Red Hat Linux 7.1

Guide de référence officiel Red Hat Linux

ISBN: N/A


Red Hat, Inc.

2600 Meridian Parkway
Durham , NC 27713 USA

Research Triangle Park, NC 27709 USA

rhl-rg(IT)-7.1-Print-RHI (2001-02-21T10:50-0500)

Imprimé au Canada, en Irlande et au Japon

Table des matières

Red Hat Linux 7.1

Introduction

Bienvenue dans le *Guide de référence officiel Red Hat Linux*.

Le *Guide de référence officiel Red Hat Linux* contient des informations utiles sur le système Red Hat Linux. Depuis les concepts fondamentaux tels que la structure des systèmes de fichiers de Red Hat Linux, jusqu'à certains points plus précis concernant le partitionnement de disque et le contrôle de l'authentification, nous espérons que ce guide sera pour vous un auxiliaire précieux.

Ce guide vous convient si vous voulez en savoir plus sur la manière dont fonctionne votre système Red Hat Linux. Il présente notamment les fonctions suivantes :

- *Concepts de partitionnement* — Il s'agit d'une présentation des partitions de disque et des stratégies sous-jacentes à la "recherche d'un emplacement" pour plusieurs systèmes d'exploitation sur des disques durs.
- *Démarrage de Red Hat Linux* — Des informations sur les niveaux d'exécution, les répertoires `rc.d` et le mode de démarrage de vos applications préférées à l'amorçage du système.
- *Sécurité du système et du réseau* — Découvrez les méthodes les plus utilisées par les pirates informatiques pour compromettre votre système et apprenez à prévenir les problèmes de sécurité.
- *Concepts RAID* — Prenez une unité de disque, ajoutez-en une autre, puis une autre…, affichez-les comme une unité logique unique et vous allierez la puissance aux performances.
- *Installation du serveur Web sécurisé* — Apprenez à ajouter des fonctions de chiffrage à votre serveur Apache.

Avant d'entamer ce guide, vous devriez connaître les aspects concernant l'installation reportés dans *Guide d'installation officiel Red Hat Linux pour x86*, les concepts de base de Linux contenus dans le *Guide de démarrage officiel Red Hat Linux* et les instructions générales de personnalisation décrites dans le *Guide de personnalisation officiel Red Hat Linux*. Le *Guide de référence officiel Red Hat Linux* contient des informations sur des sujets avancés qui ne concernent pas forcément tous les utilisateurs.

Les versions HTML et PDF des manuels officiels de Red Hat Linux sont disponibles en ligne à l'adresse http://www.redhat.com/support/manuals.

Documentation appropriée

Il est essentiel que vous disposiez d'une documentation appropriée en fonction de votre niveau de maîtrise de Linux. Quel que soit votre niveau d'expérience de Linux, vous risquez de "décrocher" si vous ne disposez pas d'une documentation adéquate. Le *Guide de référence officiel Red Hat Linux* traite des aspects et des options les plus techniques de votre système Red Hat Linux. Cette section vous aidera à trouver les informations que vous cherchez, dans les manuels Red Hat Linux ou sur le Web.

Passons en revue trois catégories d'utilisateurs de Red Hat Linux, et déterminons la documentation dont ils ont besoin. Commençons par déterminer votre niveau d'expérience. Voici les trois catégories de base :

Débutant

N'a jamais, ou presque, utilisé un système d'exploitation Linux (ou analogue). Peut éventuellement avoir déjà utilisé d'autres systèmes d'exploitation (tels que Windows). Est-ce votre cas ? Si oui, reportez-vous à la *Documentation pour les débutants*.

Expérimenté

A déjà installé et utilisé Linux (mais pas Red Hat Linux) avec succès auparavant. Ou alors, dispose d'une expérience équivalente avec d'autres systèmes d'exploitation de type Linux. Est-ce votre cas ? Si oui, reportez-vous à la documentation *Pour les utilisateurs expérimentés*.

Chevronné

A déjà installé et utilisé Red Hat Linux avec succès précédemment. Est-ce votre cas ? Si oui, reportez-vous à la *Documentation pour les utilisateurs chevronnés*.

Documentation pour les débutants

La quantité d'informations disponibles sur des sujets de base tels que l'impression, le démarrage du système ou le partitionnement du disque dur est impressionante. Ces informations vous donnent un aperçu du fonctionnement de Linux, indispensable pour approfondir ensuite ces sujets.

Commencez par vous procurer la documentation adéquate ! On ne le soulignera jamais assez ; sans documentation vous ne pourrez qu'être frustré de votre incapacité à faire fonctionner le système Red Hat Linux comme vous le voulez.

Voici le type de documentation Linux que vous devriez avoir sous la main :

- *Bref historique de Linux* —De nombreux aspects de Linux sont le fruit d'une évolution. Il existe également une culture Linux qui, une fois encore, puise largement dans son histoire passée. Quelques connaissances concernant l'histoire de Linux vous seront utiles, en particulier pour apprendre à résoudre beaucoup de problèmes potentiels avant leur apparition.
- *Explication du fonctionnement de Linux* — S'il n'est pas indispensable de maîtriser tous les aspects du noyau Linux, il est utile de savoir de quoi Linux est fait. Ce point est particulièrement important si vous avez déjà travaillé avec d'autres systèmes d'exploitation ; certaines de vos certitudes quant au fonctionnement des ordinateurs peuvent ne pas être transposables à Linux.
- *Aperçu des commandes (avec des exemples)* — C'est probablement ce que vous trouverez de plus important dans la documentation de Linux. La philosophie de conception sous-jacente à Linux est qu'il est préférable d'utiliser de nombreuses petites commandes interconnectées de différentes manières plutôt que d'avoir quelques commandes volumineuses (et complexes) qui font tout le

travail. Si vous ne disposez pas d'exemples illustrant l'approche de Linux, vous risquez d'être effrayé rien que par le nombre de commandes disponibles sur votre système Red Hat Linux.

Souvenez-vous que vous ne devez pas connaître toutes les commandes Linux existantes. Différentes techniques permettent de trouver la commande requise pour l'accomplissement d'une tâche. Vous devez simplement comprendre le fonctionnement de Linux de façon générale, ce que vous devez accomplir et comment accéder à l'outil qui vous fournira les instructions nécessaires à l'exécution de la commande.

Le *Guide d'installation officiel Red Hat Linux pour x86* est une excellente référence qui vous assistera dans l'installation et la configuration initiale de Red Hat Linux. Le *Guide de démarrage officiel Red Hat Linux* couvre l'histoire de Linux, les commandes de base du système, GNOME, KDE, RPM et bien d'autres concepts fondamentaux. Ces deux livres vous aideront à construire vos connaissances de base sur Red Hat Linux. Bientôt les concepts compliqués vous seront plus clairs car vous aurez compris les idées principales de Linux.

Outre les manuels Red Hat Linux, bien d'autres sources de documentations sont disponibles à un prix réduit ou gratuitement :

Introduction aux sites Web de Linux

- http://www.redhat.com — Dans le site Web de Red Hat vous trouverez des liens qui vous permettront de consulter le Projet de documentation Linux (LDP, Linux Documentation Project), les versions en ligne des manuels Red Hat Linux, le forum aux questions, une base de données qui vous assiste dans la recherche d'un Groupe d'Utilisateurs Linux près de chez vous, les informations techniques contenues dans le Red Hat Support Knowledge Base etc.
- http://www.linuxheadquarters.com — Le site Web du "quartier général" de Linux contient de nombreux guides qui expliquent différents outils de Linux.

Introduction aux groupes de discussion Linux

Vous pouvez participer aux groupes de discussion en suivant les interventions d'autres personnes, en posant des questions ou en essayant de répondre aux questions posées. Les utilisateurs de Linux sont passés maîtres dans l'art d'aider les néophytes à comprendre Linux — en particulier si les questions sont bien formulées. Si vous n'avez pas accès à une application qui permet d'entrer dans ces groupes, vous pouvez accéder à ces informations sur le Web à l'adresse http://www.deja.com. Il existe des dizaines de groupes de discussion concernant Linux. En voici des exemples :

- linux.help — Un excellent site où vous obtiendrez de l'aide de la part d'autres utilisateurs Linux.
- linux.redhat — Ce groupe de discussion aborde des thèmes spécifique à Red Hat Linux.
- linux.redhat.install — Posez vos questions concernant l'installation ou voyez comment d'autres personnes résolvent des problèmes similaires aux vôtres.
- linux.redhat.misc — Pour des questions ou des demandes d'aide particulières.

- linux.redhat.rpm — Une bonne adresse si vous n'arrivez pas à atteindre des objectifs particuliers avec RPM.

Livres sur Linux pour les utilisateurs débutants

- *Red Hat Linux for Dummies, 2ème édition* de Jon "maddog" Hall, édité par IDG
- *Special Edition Using Red Hat Linux* de Alan Simpson, John Ray et Neal Jamison; édité par Que
- *Running Linux* de Matt Welsh et Lar Kaufman, édité par O'Reilly & Associates
- *Red Hat Linux 7 Unleashed* de William Ball et David Pitts, édité par Sams

Les livres ci-dessus sont d'excellentes sources d'information sur le fonctionnement de base du système Red Hat Linux. Pour des informations plus approfondies, reportez-vous aux livres mentionnés dans les différents chapitre de ce manuel, en particulier dans la section *Autres Ressources*.

Pour les utilisateurs expérimentés

Si vous avez utilisé d'autres distributions Linux, vous connaissez probablement déjà les commandes les plus utilisées. Vous avez peut être installé votre système Linux et téléchargé des logiciels que vous avez trouvés sur Internet. Une fois Linux installé, les procédures de configuration peuvent toutefois poser problème.

Le *Guide de personnalisation officiel Red Hat Linux* est conçu pour vous suggérer la ou les configurations du système Red Hat Linux les plus adéquates à vos objectifs. Ce manuel donne des options de configuration spécifiques et vous explique comment les appliquer.

Lorsque vous installez des logiciels qui ne figurent pas dans le *Guide de personnalisation officiel Red Hat Linux*, il est souvent utile de voir ce que d'autres personnes ont fait dans des circonstances similaires. Les documents HOWTO du Projet de documentation Linux, disponibles à l'adresse http://www.redhat.com/mirrors/LDP/HOWTO/HOWTO-INDEX/howtos.html, traitent des aspects particuliers de Linux, à partir des modifications ésotériques du noyau de bas niveau, jusqu'à l'utilisation de Linux pour des stations de radio-amateurs.

Documentation pour les utilisateurs chevronnés

Si vous utilisez Red Hat Linux depuis longtemps, vous savez probablement que le meilleur moyen de comprendre un programme est de lire son code souce et/ou ses fichiers de configuration. L'un des plus gros avantages de Red Hat Linux est que le code source est toujours disponible.

Evidemment, nous ne sommes pas tous des programmateurs de language C. Toutefois, si vous avez les connaissances et les capacités pour le comprendre, le code source peut dissiper tous vos doutes.

Conventions

En lisant ce manuel vous remarquerez que certains mots sont écrits avec des polices et des tailles de caractères différentes. Cette méthode de mise en relief est systématique. Des mots différents sont écrits avec le même style pour indiquer qu'ils appartiennent à une même catégorie. En voici des exemples :

`commande`

Cette catégorie comprend les commandes Linux et les commandes d'autres systèmes d'exploitation. Ce style indique que vous pouvez entrez le mot ou la phrase sur la ligne de commande et appuyer sur [Entrée]. Parfois, une commande contient des mots qui devraient être écrits avec des styles différents (tels que les noms de fichier). Dans ces cas, ils sont considérés comme faisant partie d'une même commande. Par exemple :

Utilisez la commande `cat testfile` pour afficher le contenu d'un fichier appelé `testfile` dans le répertoire actuel.

`nom de fichier`

Les noms de fichier, de répertoires, les chemins d'accès et les paquetages RPM. Le style appliqué indique qu'un fichier ou un répertoire particulier est ainsi appelé dans votre système Red Hat Linux. Par exemple :

Le fichier `.bashrc` contenu dans votre répertoire personnel comprend des définitions et des alias de shell bash.

Le fichier `/etc/fstab` contient des informations sur les différents systèmes de fichiers et périphériques du système.

Le répertoire `/usr/share/doc` contient de la documentation sur différents programmes.

Installez le RPM `webalizer` si vous voulez utiliser un programme d'analyse de fichiers journaux de serveur Web.

application

Ce style indique que le programme est une application destinée à l'utilisateur final (par opposition aux logiciel du système). Par exemple :

Utilisez Netscape Navigator pour surfer sur le Web.

[touche]

Ce style est utilisé pour les touches de clavier. Par exemple :

Pour utiliser le complément des commandes et noms de fichiers au moyen de la touche [Tab], entrez un caractère et appuyez sur [Tab]. Votre écran affichera la liste des fichiers contenus dans le répertoire actuel qui commencent avec cette lettre.

[combinaison]-[touches]

Ce style indique une combinaison de touches. Par exemple :

La combinaison des touches [Ctrl]-[Alt]-[Retour arrière] arrête le système X Window.

texte trouvé dans une interface graphique

Ce style est utilisé pour mettre en relief des mots ou des phrases contenues dans une fenêtre ou un écran d'une interface graphique (tels que des mots associés à une case à cocher ou à un champ). Par exemple :

Dans l'écran de GNOME appelé **Centre de contrôle**, vous pouvez personnaliser votre gestionnaire de fenêtres GNOME.

Sélectionnez la case à cocher **Mot de passe requis** si vous voulez que votre économiseur d'écran demande un mot de passe avant de s'arrêter.

premier mot du menu d'une fenêtre ou d'un écran de l'interface graphique

Ce style indique que le mot se trouve au premier niveau d'un menu déroulant. Si vous cliquez sur ce mot, le menu s'ouvre. Par exemple :

Le menu **Paramètres** de GNOME contient les entrées de menu suivantes : **Préférences**, **R.A.Z. Terminal**, **Réinitialiser et effacer** et **Sélection de la couleur**.

Si vous devez sélectionner une séquence de commandes à l'intérieur d'un menu de l'interface graphique, celles-ci seront affichées comme dans l'exemple suivant :

Cliquez sur **Programmes**=>**Applications**=>**Emacs** pour démarrer l'éditeur de texte Emacs.

bouton d'un écran ou d'une fenêtre graphique

Ce style indique que le texte se trouve sur un bouton cliquable d'un écran graphique. Par exemple :

Cliquez sur **Précédent** pour retourner à la dernière page Web que vous avez visitée.

`message ordinateur`

Ce style est utilisé pour indiquer le texte que l'ordinateur affiche sur la ligne de commande. Vous verrez des réponses à des commandes que vous avez tapées, des messages d'erreur et des invites interactives durant les scripts ou les programmes affichés de cette façon. Par exemple :

Entrez la commande `ls` pour afficher le contenu d'un répertoire :

```
$ ls
Desktop              axhome          logs          nirvana.gif
Mail                 backupfiles     mail          reports
```

Les informations reçues en réponse à la commande (ici le contenu du répertoire) sont affichées dans ce style.

`invite`

Ce style est utilisé pour les invites de l'ordinateur. Une invite est un moyen utilisé par l'ordinateur pour indiquer à l'utilisateur qu'il peut écrire quelque chose. Examples:

```
$
#
[truk@bleach truk]$
leopard login:
```

`saisie manuelle`

Texte que l'utilisateur doit taper, soit sur une ligne de commande, soit dans une case de texte d'un écran graphique. Dans l'exemple ci-dessous, **`text`** est affiché dans ce style :

Pour que le système démarre le programme d'installation en mode texte, entrez la commande **`text`** à l'invite `boot :`

Dans l'exemple ci-dessous, le mot **`root`** est affiché comme quelque chose que l'utilisateur doit entrer :

Si vous devez vous connecter en tant que root au démarrage du système et que vous utilisez l'écran de connexion graphique, entrez **`root`** à l'invite `Login`. Ensuite, entrez le mot de passe de l'utilisateur root à l'invite `Password`.

entrée de glossaire

Les mots contenus dans le glossaire seront affichés dans ce style à l'intérieur du corps du document. Par exemple :

Le **démon** lpd gère les demandes d'impression.

Dans ce cas, le style du mot **démon** vous indique qu'une définition du terme est disponible dans le glossaire.

De plus, différentes stratégies sont utilisées dans tout le manuel pour attirer votre attention, telles que Remarque, Attention et Avertissement. Par exemple :

Remarque

Souvenez-vous que Linux différencie les lettres majuscules des lettres minuscules. En d'autres termes, une rose n'est pas une ROSE ni une rOsE.

N’effectuez pas les tâches de routine en tant que root — utilisez un compte utilisateur à moins que vous ne deviez utiliser le compte root pour l’administration de votre système.

Si vous optez pour un partitionnement non manuel, une installation de classe Serveur supprimera toutes les partitions existantes sur tous les disques durs installés. Ne choisissez pas ce type d’installation si vous voulez conserver vos données.

Utilisation de la souris

Red Hat Linux prévoit l’utilisation d’une souris à trois boutons. Si vous avez une souris à deux boutons, vous devez avoir sélectionné Emulation de souris à trois boutons durant l’installation. Pour émuler le troisième bouton, appuyez simultanément sur les deux boutons de la souris.

Dans ce manuel, s’il vous est demandé de cliquer avec la souris sur quelque chose, il est sous-entendu que vous devez utiliser le bouton de gauche. Si vous devez cliquer avec le bouton du milieu ou sur celui de droite, cela vous sera spécifié. (Evidemment le tout s’intervertit si votre souris est configuré pour un utilisateur gaucher.)

Les mots "glisser et poser" vous sont peut-être familiers. S’il vous est demandé de glisser et poser un élément de votre bureau graphique, cliquez sur l’élément et gardez le bouton de la souris appuyé. Tout en appuyant sur le bouton de la souris, faites glisser l’élément vers le nouvel emplacement. Une fois que vous avez atteint l’emplacement, lâchez le bouton pour poser l’élément.

Copier et coller du texte avec X Window

L’opération de copier et coller est très simple si l’on utilise une souris et un système X Window. Mettez en surbrillance le texte que vous voulez copier. Ensuite, cliquez avec le bouton du milieu de la souris à l’endroit où vous voulez que le texte soit copié.

Prochainement

Le *Guide de référence officiel Red Hat Linux* fait partie de l'engagement pris par Red Hat dans le but de fournir une assistance utile et ponctuelle aux utilisateurs de Red Hat Linux. Les prochaines éditions reporteront de plus amples informations sur les changements de la structure et de l'organisation du système, de nouveaux outils de sécurité plus performants et d'autres ressources qui vous aideront à accroître la puissance de votre système — ainsi que vos capacités d'utilisation.

Voici comment vous pouvez nous aider !

Vos réactions sont les bienvenues

Si vous trouvez une faute de frappe dans le *Guide de référence officiel Red Hat Linux* ou si vous avez songé à une manière d'améliorer ce manuel, nous aimerions connaître vos remarques. Signalez l'erreur dans Bugzilla à l'adresse (http://bugzilla.redhat.com/bugzilla).

N'oubliez pas de mentionner la référence du manuel :

```
rhl-rg(IT)-7.1-Print-RHI (2001-02-21T10:50-0500)
```

Nous saurons ainsi quelle version de guide est en votre possession.

Si vous avez la moindre suggestion susceptible d'améliorer la documentation, tâchez d'en donner une description aussi détaillée que possible. Si vous avez détecté une erreur, incluez le numéro de section et une partie du texte qui l'entoure, de façon à ce que nous puissions la trouver aisément.

Enregistrez-vous pour bénéficier de l'assistance

Si vous disposez d'une édition officielle de Red Hat Linux 7.1, songez à vous enregistrer pour bénéficier des avantages auxquels vous avez droit en tant que client Red Hat.

Vous bénéficierez de certains ou de tous les avantages suivants, selon le produit Red Hat Linux officiel que vous aurez acheté :

- Assistance technique officielle de Red Hat — Obtenez de l'aide sur l'installation auprès de l'équipe d'assistance de Red Hat, Inc..
- Mettez facilement à jour vos paquetages et recevez des notices de sécurité adaptées à votre système. Pour plus de détails, visitez le site http://www.redhat.com/network.
- Accès FTP prioritaire— Finies les visites nocturnes à des sites miroir saturés. En tant que propriétaire de Red Hat Linux 7.1, vous pouvez bénéficier d'un accès gratuit à priority.redhat.com, le service FTP pour les clients privilégiés de Red Hat qui offre des connexions à haute bande passante jour et nuit.

- *Le bulletin d'information Red Hat officiel* — Recevez tous les mois les dernières nouvelles directement de Red Hat.

Pour bénéficier de l'assistance, inscrivez-vous au site http://www.redhat.com/apps/activate. A l'intérieur de votre boîte Red Hat Linux officielle, vous trouverez une carte rouge et blanche sur laquelle est reporté votre identificateur produit.

Pour plus d'informations sur l'assistance technique Red Hat Linux officielle, reportez-vous à l'appendice *Obtention de l'assistance technique* contenue dans le *Guide d'installation officiel Red Hat Linux pour x86*.

Bonne chance et merci d'avoir choisi Red Hat Linux!!

L'équipe de documentation Red Hat

Partie I Références liées au système

1 Structure d’un système de fichiers

1.1 Pourquoi partager une structure commune ?

La structure du système de fichiers d’un système d’exploitation est son niveau d’organisation le plus bas. Presque toutes les façons dont un système d’exploitation interagit avec ses utilisateurs, ses applications et son modèle de sécurité dépendent de la façon dont il stocke ses fichiers dans un périphérique de stockage de base (généralement une unité de disque dur). Il est impératif, et ce pour nombre de raisons, que les utilisateurs, ainsi que les programmes au moment de leur installation et par la suite, puissent compter sur une ligne directrice commune afin de savoir où lire et écrire leur fichier binaire, leur configuration, leur journal et les autres fichiers nécessaires.

Les systèmes de fichiers peuvent être définis selon deux types différents de catégories logiques de fichiers :

- Fichier partageable/fichier non partageable
- Fichier variable/fichier statique

Les fichiers **partageables** sont accessibles à partir de différents hôtes, alors que les fichiers **non partageables** ne sont pas disponibles aux autres hôtes. Les fichiers **variables** peuvent être modifiés à tout moment, sans que l’intervention de l’administrateur système (active ou passive) ne soit nécessaire, alors que les fichiers **statiques**, tels que la documentation ou les fichiers binaires, ne peuvent être changés sans l’action directe de l’administrateur système ou d’un agent mis en place par ce dernier afin d’accomplir cette tâche.

Nous définissons ces fichiers de cette manière en raison des différents types d’autorisations données aux répertoires qui les contiennent. La façon dont le système d’exploitation et ses utilisateurs utilisent les fichiers détermine le répertoire où ces fichiers doivent être placés, selon qu’il est monté pour la lecture seule ou pour la consultation et la modification, ainsi que le niveau d’accès permis pour chaque fichier. Le niveau le plus élevé de cette organisation est crucial car, s’il est mal organisé ou n’est pas doté d’une structure très utilisée, l’accès aux sous-répertoires sous-jacents pourrait être limité ou des problèmes de sécurité pourraient survenir.

Toutefois, le fait d’avoir une structure ne signifie pas grand chose à moins qu’elle ne soit un standard. En effet, des structures concurrentes peuvent créer plus de problèmes qu’elles n’en règlent. Pour cette raison, Red Hat a choisi la structure de système de fichiers la plus utilisée et l’a étendue légèrement pour la prise en charge de fichiers spéciaux spécifiques à Red Hat Linux.

1.2 Aperçu du FHS

Red Hat adhère au **FHS** (**Filesystem Hierarchy Standard** / standard en matière de hiérarchie du système de fichiers), document de collaboration définissant les noms et les emplacements de nombreux

fichiers et répertoires. Nous continuerons à respecter cette norme pour garantir la conformité de Red Hat Linux.

Le document FHS actuel est la référence faisant autorité pour tout système de fichiers compatible avec le standard FHS. Toutefois, celui-ci comprend de nombreuses zones indéfinies ou extensibles. Cette section donne un aperçu de la norme et une description des éléments du système de fichiers non couverts par celle-ci.

La norme complète peut être consultée à l'adresse suivante :

http://www.pathname.com/fhs

La conformité avec la norme signifie beaucoup, mais les deux aspects les plus importants sont la compatibilité avec d'autres systèmes également conformes et la possibilité de monter la partition `/usr` en lecture seule (car elle contient des fichiers exécutables courants et n'a pas pour vocation d'être modifiée par les utilisateurs). Du fait que la partition `/usr` peut être montée en lecture seule, il est possible de monter `/usr` depuis le CD-ROM ou un autre ordinateur par le biais d'un NFS en lecture seule.

1.2.1 Organisation de FHS

Les répertoires et les fichiers mentionnés ici sont un petit sous-ensemble de ceux qui sont spécifiés par le document FHS. Consultez le document FHS le plus récent pour obtenir des renseignements complets.

Le répertoire `/dev`

Le répertoire `/dev` contient des entrées de système de fichiers représentant des périphériques connectés au système. Ces fichiers sont essentiels au bon fonctionnement du système.

Le répertoire `/etc`

Le répertoire `/etc` est réservé aux fichiers de configuration locaux sur votre ordinateur. Tous les fichiers binaires qui se trouvaient auparavant dans `/etc` devraient dorénavant aller dans `/sbin` ou, si possible, dans `/bin`.

Les répertoires `X11` et `skel` doivent être des sous-répertoires de `/etc` :

```
/etc
  |- X11
  |- skel
```

Le répertoire `X11` est destiné aux fichiers de configuration X11, tels que `XF86Config`. Le répertoire `skel` est consacré aux fichiers utilisateur "squelette", utilisés pour remplir un répertoire personnel lors de la création d'un nouvel utilisateur.

Le répertoire /lib

Le répertoire /lib ne devrait contenir que les bibliothèques nécessaires à l'exécution de fichiers binaires dans /bin et /sbin. Ces images de bibliothèques partagées sont particulièrement importantes pour le démarrage du système et l'exécution de commandes dans le système de fichiers racine.

Le répertoire /mnt

Le répertoire /mnt se réfère aux systèmes de fichiers montés de façon temporaire, tels que les CD-ROM et les disquettes.

Le répertoire /opt

Le répertoire /opt fournit un endroit pour stocker des paquetages de logiciels d'applications statiques de grande taille.

Lorsque l'on veut éviter de mettre les fichiers d'un paquetage donné dans le système de fichiers, /opt fournit un système organisationnel logique et prévisible sous le répertoire du paquetage en question. Cela donne à l'administrateur système une façon facile de déterminer le rôle de chaque fichier d'un paquetage donné.

Par exemple, si sample est le nom d'un paquetage logiciel situé dans /opt, alors tous ses fichiers pourraient être placés dans des répertoires à l'intérieur de /opt/sample, tels que /opt/sample/bin pour les fichiers binaires et /opt/sample/man pour les pages de manuel.

Les paquetages de grande taille qui contiennent de nombreux sous-paquetages différents exécutant chacun une tâche spécifique, vont également dans le répertoire /opt, leur donnant ainsi une façon standard de s'organiser. Pour reprendre notre exemple, le paquetage sample pourrait contenir différents outils allant chacun dans un sous-répertoire qui lui est propre, tel que /opt/sample/tool1 et /opt/sample/tool2, qui à son tour peut avoir ses propres répertoires bin, man ou autres répertoires semblables.

Le répertoire /sbin

Le répertoire /sbin est conçu pour les fichiers exécutables qui ne sont utilisés que par les utilisateurs racine. Les fichiers exécutables dans /sbin ne sont utilisés que pour démarrer et monter /usr et exécuter des opérations de remise en état du système. FHS indique ce qui suit:

> "/sbin contient généralement des fichiers essentiels pour le démarrage du système, en plus des fichiers binaires figurant dans /bin. Tout ce qui est exécuté après /usr est supposé monté (lorsqu'il n'y a pas de problème) et doit être placé dans /usr/sbin. Les fichiers binaires d'administration du système exclusivement locaux doivent être placés dans le répertoire /usr/local/sbin."

Au minimum, les programmes suivants doivent être dans /sbin :

```
arp, clock, getty, halt, init, fdisk,
fsck.*, ifconfig, lilo, mkfs.*, mkswap, reboot,
route, shutdown, swapoff, swapon, update
```

Le répertoire /usr

Le répertoire /usr est destiné aux fichiers pouvant être partagés sur l'ensemble d'un site. Le répertoire /usr a généralement sa propre partition et devrait être montable en lecture seule. Les répertoires suivants doivent être des sous-répertoires de /usr :

```
/usr
  |- bin
  |- doc
  |- etc
  |- games
  |- include
  |- kerberos
  |- lib
  |- libexec
  |- local
  |- man
  |- sbin
  |- share
  |- src
  |- X11R6
```

Le répertoire bin contient des fichiers exécutables, doc contient des pages de documentation, etc contient des fichiers de configuration pour l'ensemble du système, games est pour les jeux, include contient des fichiers d'en-tête C, kerberos contient des fichiers binaires et d'autres éléments pour Kerberos et, enfin, lib contient des fichiers objet et des bibliothèques qui ne sont pas destinés à être utilisés directement par les utilisateurs ou les scripts shell. Le répertoire libexec contient de petits programmes d'aide appelés par d'autres programmes, sbin est pour les fichiers binaires d'administration du système (ceux qui n'appartiennent pas à /sbin), share contient des fichiers qui ne sont pas spécifiques à l'architecture, src est pour le code source et X11R6 est pour le système X Window (XFree86 sur Red Hat Linux).

Le répertoire /usr/local

FHS indique ce qui suit :

> "La hiérarchie /usr/local est destinée à être installée par l'administrateur système lors de l'installation locale du logiciel. Elle doit être à l'abri de toute réécriture lors de la mise à jour du logiciel système. Elle peut être utilisée pour des programmes et des données partageables entre un groupe d'ordinateurs, mais ne figurant pas dans /usr."

Le répertoire `/usr/local` est semblable, de par sa structure, au répertoire `/usr`. Il contient les sous-répertoires suivants, qui sont semblables, de par leur fonction, à ceux qui se trouvent dans le répertoire `/usr` :

```
/usr/local
       |- bin
       |- doc
       |- etc
       |- games
       |- info
       |- lib
       |- man
       |- sbin
       |- src
```

Le répertoire `/var`

Comme FHS exige que vous soyez en mesure de monter `/usr` en lecture seule, tous les programmes qui écrivent des fichiers journaux ou ont besoin de répertoires `spool` ou `lock` devraient probablement les écrire dans le répertoire `/var`. FHS indique que `/var` est pour :

> "… les fichiers de données variables. Ceci comprend les répertoires et fichiers spool, les données administratives et de journalisation, de même que les fichiers transitoires et temporaires."

Les répertoires suivants peuvent être des sous-répertoires de `/var` :

```
/var
  |- arpwatch
  |- cache
  |- db
  |- ftp
  |- gdm
  |- kerberos
  |- lib
  |- local
  |- lock
  |- log
  |- named
  |- nis
  |- opt
  |- preserve
  |- run
  +- spool
       |- anacron
       |- at
```

```
        |- cron
        |- fax
        |- lpd
        |- mail
        |- mqueue
        |- news
        |- rwho
        |- samba
        |- slrnpull
        |- squid
        |- up2date
        |- uucp
        |- uucppublic
        |- vbox
        |- voice
    |- tmp
    |- www
    |- yp
```

Les fichiers journaux tels que `messages` et `lastlog` vont dans `/var/log`. Le répertoire `/var/lib/rpm` contient aussi les bases de données système RPM. Les fichiers lock vont dans `/var/lock`, généralement dans des répertoires spécifiques aux programmes qui utilisent ces fichiers. Le répertoire `/var/spool` comprend des sous-répertoires pour divers systèmes ayant besoin de stocker des fichiers de données.

1.2.2 `/usr/local` dans Red Hat Linux

Dans Red Hat Linux, l'usage prévu pour `/usr/local` est légèrement différent de celui qui est spécifié par FHS. FHS indique que `/usr/local` devrait se trouver là où vous stockez des logiciels devant rester à l'abri des mises à jour du logiciel système. Du fait que les mises à jour du système à partir de Red Hat s'effectuent en toute sécurité à l'aide du système RPM et de Gnome-RPM, il ne vous est pas nécessaire de protéger des fichiers en les plaçant dans `/usr/local`. Il vous est plutôt recommandé d'utiliser `/usr/local` pour y placer les logiciels locaux de votre ordinateur.

Par exemple, imaginons que vous ayez monté `/usr` par le biais d'un NFS en lecture seule à partir d'un hôte appelé `jake`. Si vous désirez installer un paquetage ou un programme, mais que vous n'avez pas l'autorisation d'apporter des modifications dans `jake`, vous devriez alors l'installer sous `/usr/local`. De cette façon, si vous réussissez par la suite à convaincre l'administrateur système de `jake` d'installer le programme dans `/usr`, vous pourrez le désinstaller du répertoire `/usr/local`.

1.3 `/proc` et ses "fichiers"

Le répertoire `/proc` contient des "fichiers" spéciaux qui permettent d'extraire des informations du noyau ou de lui en envoyer.

Cependant, le répertoire `/proc` est beaucoup plus puissant que vous ne le croyez. Au moyen des divers "fichiers" de ce répertoire (qui en réalité ne sont pas du tout des fichiers, mais bien des interfaces dans le noyau), l'administrateur système peut utiliser `/proc` comme méthode facile pour accéder aux informations sur l'état du noyau, les caractéristiques de l'ordinateur, l'état des divers processus et plus encore. En utilisant `cat` combinée aux interfaces situées dans `/proc`, vous disposez d'un accès instantané à une multitude de renseignements sur tout le système. Par exemple, si vous voulez voir de quelle façon les registres sont actuellement attribués dans votre système :

```
[truk@tictactoe /proc]$ cat iomem
00000000-0009fbff : System RAM
0009fc00-0009ffff : reserved
000a0000-000bffff : Video RAM area
000c0000-000c7fff : Video ROM
000f0000-000fffff : System ROM
00100000-07ffffff : System RAM
  00100000-002553d7 : Kernel code
  002553d8-0026d91b : Kernel data
e0000000-e3ffffff : VIA Technologies, Inc. VT82C597 [Apollo VP3]
e4000000-e7ffffff : PCI Bus #01
  e4000000-e4003fff : Matrox Graphics, Inc. MGA G200 AGP
  e5000000-e57fffff : Matrox Graphics, Inc. MGA G200 AGP
e8000000-e8ffffff : PCI Bus #01
  e8000000-e8ffffff : Matrox Graphics, Inc. MGA G200 AGP
ea000000-ea00007f : Digital Equipment Corporation DECchip 21140
  ea000000-ea00007f : eth0
ffff0000-ffffffff : reserved
[truk@tictactoe /proc]$
```

Ou alors (chose encore plus utile), si vous étiez connecté à un ordinateur inconnu et vouliez connaître son type d'unité centrale et sa vitesse, vous pourriez utiliser la commande suivante :

```
cat /proc/cpuinfo
```

D'autres renseignements importants concernant le système peuvent être obtenus grâce, entre autre, à `cmdline`, `meminfo`, `partitions` et `version`.

Les répertoires dans `/proc` symbolisent un ensemble d'informations sur une application ou un processus donné. Par exemple, le répertoire `/proc/sys/kernel` est rempli de renseignements sur le noyau, tels que le nombre maximum de threads (`threads-max`) et le nombre maximum de messages (`msgmax`).

1.4 Emplacement de fichiers Red Hat Linux spéciaux

En plus des fichiers relatifs à RPM se trouvant dans `/var/lib/rpm` (voir le chapitre RPM dans le *Guide de personnalisation officiel Red Hat Linux* pour avoir plus de détails sur RPM), il existe deux autres emplacements spéciaux réservés à la configuration et l'exploitation de Red Hat Linux.

Les outils de configuration fournis avec Red Hat Linux installent de nombreux fichiers script, bitmap et texte dans `/usr/lib/rhs`. Puisque ces fichiers sont générés par des logiciels sur votre système, il est préférable de n'en modifier aucun manuellement.

L'autre emplacement spécial (`/etc/sysconfig`) stocke des informations de configuration. De nombreux scripts lancés au démarrage utilisent les fichiers de ce répertoire. Ces fichiers peuvent être modifiés manuellement, mais peuvent aussi être configurés au moyen de Linuxconf, d'un outil du tableau de contrôle ou d'un autre outil de configuration. Reportez-vous au *Guide de personnalisation officiel Red Hat Linux* pour avoir des instructions sur l'utilisation de Linuxconf.

2 Utilisateurs et groupes

Le contrôle des **utilisateurs** et **groupes** est au coeur de l'administration de système de Red Hat Linux.

Les utilisateurs peuvent autant être des personnes physiques (comptes réservés à un utilisateur physique défini) que des personnes logiques (les comptes existent pour des applications de façon à pouvoir exécuter des tâches particulières). Ces deux types d'utilisateurs, réel ou logique, ont un **Identificateur Utilisateur** et **Identificateur Groupe**. Les Identificateurs utilisateurs sont généralement uniques (mais il n'est pas nécessaire qu'ils le soient).

Les **Groupes** sont toujours des expressions logiques de l'organisation. Les utilisateurs forment des groupes, et les groupes constituent la fondation de l'ensemble des utilisateurs, leur donnant la permission de lire, écrire ou exécuter un fichier donné.

Lors de sa création, tout fichier est assigné à un utilisateur et à un groupe, ainsi qu'à une modalité de lecture, d'écriture et de permission d'exécution pour le créateur du fichier, pour le groupe ou pour tout autre utilisateur de cet hôte. L'utilisateur et le groupe d'un fichier, ainsi que les permissions sur ce fichier, peuvent être modifiés par le root et par le créateur du fichier.

La bonne gestion des utilisateurs et groupes, ainsi que l'assignation et la révocation des permissions, est l'une des tâches les plus importantes de tout gestionnaire de système. Heureusement, Red Hat Linux rend cette tâche aussi facile que possible tout en préservant la sécurité des fichiers de l'hôte.

2.1 Outils pour l'administration des utilisateurs et des groupes

La gestion des utilisateurs et des groupes est généralement laborieuse ; toutefois, Red Hat Linux comprend quelques outils et conventions qui facilitent la gestion des utilisateurs et des groupes.

Si vous pouvez utiliser `useradd` pour créer un nouvel utilisateur à l'invite du shell, la manière la plus simple de gérer des utilisateurs et des groupes consiste à utiliser Linuxconf (pour obtenir plus de détails sur Linuxconf, reportez-vous au *Guide de personnalisation officiel Red Hat Linux*).

2.2 Utilisateurs standard

Dans la Table 2–1, *Utilisateurs standard*, vous trouverez les utilisateurs standard configurés par le processus d'installation (il s'agit essentiellement du fichier `/etc/passwd`). L'**id du groupe** (GID) figurant dans ce tableau correspond au *groupe principal* pour l'utilisateur. Reportez-vous à la Section 2.4, *Groupes propres à l'utilisateur* pour plus de détails sur l'utilisation des groupes.

Table 2–1 Utilisateurs standard

Utilisateur	UID	GID	Répertoire personnel	Shell
root	0	0	/root	/bin/bash
bin	1	1	/bin	
daemon	2	2	/sbin	
adm	3	4	/var/adm	
lp	4	7	/var/spool/lpd	
sync	5	0	/sbin	/bin/sync
shutdown	6	0	/sbin	/sbin/shutdown
halt	7	0	/sbin	/sbin/halt
mail	8	12	/var/spool/mail	
news	9	13	/var/spool/news	
uucp	10	14	/var/spool/uucp	
operator	11	0	/root	
games	12	100	/usr/games	
gopher	13	30	/usr/lib/gopher-data	
ftp	14	50	/var/ftp	
nobody	99	99	/	

2.3 Groupes standard

Dans la Table 2–2, *Groupes standard*, vous trouverez les groupes standard tels que définis par le processus d'installation (il s'agit essentiellement du fichier `/etc/group`).

Table 2–2 Groupes standard

Groupe	GID	Membres
root	0	root
bin	1	root, bin, daemon

Groupe	GID	Membres
daemon	2	root, bin, daemon
sys	3	root, bin, adm
adm	4	root, adm, daemon
tty	5	
disk	6	root
lp	7	daemon, lp
mem	8	
kmem	9	
wheel	10	mail
mail	12	mail
news	13	news
uucp	14	uucp
man	15	
games	20	
gopher	30	
dip	40	
ftp	50	
nobody	99	
users	100	

2.4 Groupes propres à l’utilisateur

Red Hat Linux utilise un système de **groupe propre à l’utilisateur** (**UPG**), qui facilite considérablement l’utilisation de groupes UNIX. Le système UPG n’ajoute ni ne modifie rien à la manière standard dont UNIX manipule les groupes. Il propose simplement une nouvelle convention pour la manipulation des groupes. Chaque fois que vous créez un nouvel utilisateur, par défaut, il correspond à un groupe unique. Le système fonctionne comme suit :

Groupe propre à l’utilisateur

Chaque utilisateur a son propre groupe principal qui est le seul auquel il appartienne.

umask = 002

L'umask UNIX traditionnel est 022, ce qui empêche d'autres utilisateurs *et d'autres membres du groupe principal d'un utilisateur* de modifier les fichiers d'un utilisateur. Du fait que chaque utilisateur a son propre groupe privé dans le système UPG, cette "protection de groupe" n'est pas nécessaire. Un umask égal à 002 empêche les utilisateurs de modifier les fichiers privés d'autres utilisateurs. L'umask est défini dans `/etc/profile`.

Bit setgid sur des répertoires

Si vous définissez le bit setgid sur un répertoire (avec `chmod g+s` *`directory`*), le groupe des fichiers créés dans ce répertoire sera celui du répertoire.

La plupart des organisations de TI aiment créer un groupe pour chaque projet majeur et assigner les personnes aux groupes dont elles doivent faire partie. La gestion de fichiers a cependant toujours été difficile du fait que, lorsque quelqu'un crée un fichier, celui-ci est la propriété du groupe principal auquel la personne appartient. Lorsqu'une même personne travaille sur plusieurs projets, il devient difficile d'associer les bons fichiers au bon groupe de propriété. Dans le système UPG, les groupes sont automatiquement assignés à des fichiers, projet par projet, ce qui facilite considérablement la gestion des projets de groupe.

Supposons que vous ayez un grand projet baptisé *devel*, dans le cadre duquel de nombreuses personnes éditent des fichiers *devel* figurant dans un répertoire. Créez un groupe appelé `devel`, attribuez la propriété (`chgrp`) du répertoire `devel` au groupe `devel`, puis ajoutez tous les utilisateurs *devel* au groupe `devel`.

Vous pouvez ajouter un utilisateur à un groupe à l'aide de Linuxconf (voir *Guide de personnalisation officiel Red Hat Linux*). Si vous préférez utiliser la ligne de commande, exécutez la commande `/usr/sbin/groupadd` *`groupname`* pour créer un groupe. La commande `/usr/bin/gpasswd -a` *`loginname groupname`* ajoutera un utilisateur *loginname* à un groupe. (Pour obtenir plus d'informations sur leurs options, voir les pages `groupadd` et `gpasswd` du manuel.) Le fichier `/etc/group` contient les informations concernant les groupes pour votre système.

Si vous avez créé le groupe `devel`, ajouté des utilisateurs au groupe `devel`, changé le groupe du répertoire `devel` en `devel` et défini le bit setgid pour le répertoire `devel`, tous les utilisateurs *devel* pourront éditer les fichiers *devel* et créer de nouveaux fichiers dans le répertoire `devel`. Les fichiers qu'ils créent garderont toujours leur statut de groupe `devel`, de façon à ce que les autres utilisateurs *devel* puissent toujours les éditer.

Si vous avez plusieurs projets tels que *devel*, et des utilisateurs travaillant sur plusieurs projets, ces derniers ne devront jamais changer d'umask ou de groupe pour passer d'un projet à l'autre. Le bit setgid sur le répertoire principal de chaque projet "sélectionne" le groupe approprié.

Du fait que le répertoire personnel de chaque utilisateur appartient à l'utilisateur et à son groupe privé, la définition du bit setgid sur le répertoire personnel apporte une sécurité. Toutefois, par défaut, les fichiers sont créés avec le groupe principal de l'utilisateur, de sorte que le bit setgid serait redondant.

2.4.1 Exposé raisonné concernant le groupe propre à l'utilisateur

Bien que l'UPG ne soit pas une nouveauté dans Red Hat Linux 7.1, bon nombre de personnes se posent des questions à son sujet, notamment quant à son utilité. Voici un exposé raisonné relatif à ce système.

- Vous souhaitez qu'un groupe de personnes travaillent sur une série de fichiers se trouvant dans le répertoire `/usr/lib/emacs/site-lisp`. Vous faites confiance à quelques personnes capables, selon vous, de faire quelques manipulations, mais pas à toutes.
- Tout d'abord, vous créez un groupe `emacs` en tapant :

  ```
  /usr/sbin/groupadd emacs
  ```

  Ensuite vous saisissez :

  ```
  chown -R root.emacs /usr/lib/emacs/site-lisp
  ```

  Pour associer les contenus du répertoire au groupe `emacs` et ajouter les utilisateurs appropriés à ce groupe :

  ```
  /usr/bin/gpasswd -a <username> emacs
  ```

- Pour permettre aux utilisateurs de créer réellement des fichiers dans le répertoire, vous tapez :

  ```
  chmod 775 /usr/lib/emacs/site-lisp
  ```

- Mais, lorsqu'un utilisateur crée un nouveau fichier, ce dernier est attribué au groupe par défaut de l'utilisateur (généralement `users`). Pour empêcher ceci, entrez :

  ```
  chmod 2775 /usr/lib/emacs/site-lisp
  ```

  qui entraîne la création de tout ce qui figure dans le répertoire avec le groupe `emacs`.
- Mais le nouveau fichier doit être du mode 664 pour qu'un autre utilisateur du groupe emacs puis l'éditer. A cette fin, vous créez l'umask 002 par défaut.
- Cela fonctionne assez bien, si ce n'est que le groupe par défaut est `users`, tous les membres de "users" (généralement tout le monde) peuvent écrire dans chaque fichier du répertoire personnel.
- Pour éviter cela, vous pouvez attribuer à chaque utilisateur un groupe privé par défaut.

A ce stade, en créant l'umask 002 par défaut et en attribuant à chacun un groupe privé par défaut, vous pouvez aisément constituer des groupes dont les utilisateurs puissent bénéficier dans devoir faire

appel à des solutions magiques. Créez simplement le groupe, ajoutez les utilisateurs et appliquez les commandes `chown` et `chmod` ci-dessus aux répertoires du groupe.

3 Processus de démarrage, Init et arrêt

Ce chapitre contient des informations qui expliquent ce qui se passe lorsque vous démarrez ou arrêtez votre système Red Hat Linux.

3.1 Introduction

Une des caractéristiques les plus importantes de Red Hat Linux concerne sa méthode ouverte de démarrer et d'arrêter le système d'exploitation ; il charge des programmes spécifiques et utilise leur configuration particulière, permet de changer ces configurations afin de contrôler le processus de démarrage et arrête le tout de façon gracieuse et organisée. Contrairement aux autres systèmes d'exploitation qui essaient de contrôler la façon dont s'amorce l'ordinateur ou vous empêchent de spécifier les paramètres d'arrêt, Red Hat Linux vous donne un accès complet à toutes les étapes du processus.

Au-delà de la question du contrôle du processus de démarrage ou d'arrêt, la nature ouverte de Red Hat Linux fait en sorte qu'il est beaucoup plus facile de déterminer avec précision la source de nombreux problèmes associés au démarrage ou à l'arrêt de l'ordinateur. Comprendre ce processus est donc très utile et ce, même pour la résolution de problèmes mineurs.

3.2 Dans les coulisses du processus de démarrage

Remarque

Cette section porte principalement sur le processus de démarrage x86. Le processus de démarrage de votre ordinateur peut varier légèrement en fonction de son architecture. Toutefois, le processus de démarrage par défaut de Red Hat Linux est identique pour toutes les architectures après que le noyau a été trouvé et chargé par l'ordinateur. Reportez-vous à la Section 3.8, *Différences du processus de démarrage d'autres architectures* pour obtenir plus de renseignements au sujet de processus de démarrage non x86.

Lorsque l'on démarre un ordinateur, le processeur recherche le **BIOS** (Basic Input/Output System) à la fin de la mémoire du système et l'exécute. Le programme du BIOS est écrit en lecture seulement dans la mémoire permanente et peut toujours être utilisé. Le BIOS est le plus bas niveau d'interface pour les périphériques et contrôle la première étape du processus de démarrage.

Le BIOS teste le système, recherche et vérifie les périphériques et recherche ensuite une unité qui sera utilisée pour amorcer le système. Normalement, il vérifie le lecteur de disquette (ou le lecteur de CD-ROM sur de nombreux ordinateurs plus récents) afin de trouver un support amorçable, s'il y en a un, puis se tourne vers le disque dur. L'ordre des unités utilisées pour le démarrage est généralement

contrôlé par une configuration particulière du BIOS sur le système. Après avoir installé Red Hat Linux sur le disque dur de l'ordinateur, le BIOS cherche un **bloc de démarrage maître** (MBR) en commençant par le premier secteur du premier disque dur, charge son contenu dans la mémoire et lui donne le contrôle.

Ce code MBR cherche ensuite la première partition active et lit son enregistrement d'amorçage. Cet enregistrement contient les instructions sur la façon de charger **LILO** (*LI*nux *LO*ader), le chargeur de démarrage. Le MBR charge LILO, qui prend alors la relève (si LILO est installé dans le MBR). Dans la configuration par défaut de Red Hat Linux, LILO utilise les paramètres dans le MBR pour afficher les options de démarrage et permet à l'utilisateur de spécifier quel système d'exploitation doit être lancé.

Cela entraîne la question suivante : "Comment LILO fait-il dans le MBR pour savoir ce qu'il faut faire lorsque le MBR est lu?". Les instructions pour LILO sont en fait déjà écrites à cet endroit par l'entremise de `lilo` et du fichier de configuration `/etc/lilo.conf`.

3.2.1 Options dans `/etc/lilo.conf`

En général, vous n'avez pas à changer le bloc de démarrage maître sur votre disque dur à moins d'avoir besoin d'amorcer un système d'exploitation venant tout juste d'être installé ou de vouloir utiliser un nouveau noyau. Si vous devez créer un nouveau bloc de démarrage maître au moyen de LILO, mais utilisant une configuration différente, vous devrez modifier `/etc/lilo.conf` et exécuter `lilo` encore une fois.

Si vous prévoyez de modifier `/etc/lilo.conf`, assurez-vous de faire une copie de sauvegarde du fichier avant d'y apporter des changements. De plus, assurez-vous d'avoir une disquette d'amorçage fonctionnel à votre disposition, de sorte que vous puissiez démarrer le système et apporter des modifications au MBR s'il y a des problèmes. Lisez les pages de manuel concernant `mkbootdisk` pour en savoir plus sur la création d'une disquette d'amorçage.

Le fichier `/etc/lilo.conf` est utilisé par `lilo` pour déterminer quel(s) système(s) d'exploitation utiliser ou avec quel noyau commencer, ainsi que pour savoir où l'installer (exemple : `/dev/hda` pour le premier disque dur IDE). Un fichier `/etc/lilo.conf` échantillon ressemble à ceci :

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
```

```
prompt
timeout=50
message=/boot/message
lba32
default=linux

image=/boot/vmlinuz-2.4.0-0.43.6
 label=linux
 initrd=/boot/initrd-2.4.0-0.43.6.img
 read-only
 root=/dev/hda5

other=/dev/hda1
 label=dos
```

Cet exemple montre un système qui est configuré pour amorcer deux systèmes d'exploitation : Red Hat Linux et DOS. Voici plus de détails sur certaines des lignes de ce fichier (votre fichier `/etc/lilo.conf` pourrait être légèrement différent) :

- `boot=/dev/hda` indique à LILO de regarder sur le premier disque dur du premier contrôleur IDE.
- `map=/boot/map` localise le fichier map. Pour une utilisation normale, ce nom ne devrait pas être modifié.
- `install=/boot/boot.b` indique à LILO d'installer le fichier spécifié en tant que nouveau secteur de démarrage. Pour une utilisation normale, cela ne devrait pas être modifié. Si la ligne `install` manque, LILO prendra par défaut `/boot/boot.b` en tant que fichier à utiliser.
- L'existence de `prompt` indique à LILO de vous afficher tout ce qui est défini dans la ligne `message`. Bien qu'il ne soit pas recommandé d'éliminer la ligne `prompt`, si vous le faites, vous pourrez tout de même obtenir une invite en appuyant sur la touche [Shift] pendant que votre ordinateur commence l'amorçage.
- `timeout=50` définit combien de temps LILO doit attendre que l'utilisateur entre une commande avant d'amorcer la ligne d'entrée `default`. Cette période de temps est mesurée en dixièmes de seconde et est réglée sur 50 par défaut.
- `message=/boot/message` se réfère à l'écran que LILO affiche pour vous laisser sélectionner le système d'exploitation ou le noyau à amorcer.
- `lba32` décrit la géométrie du disque dur à LILO. Une autre ligne commune que l'on retrouve à cet endroit est `linear`. Vous ne devriez pas changer cette ligne à moins d'être sûr de ce que vous faites. Autrement, vous pourriez mettre votre ordinateur dans un état où il lui est impossible d'être redémarré.

- `default=linux` se réfère au système d'exploitation par défaut que LILO doit amorcer au moyen des options énumérées sous cette ligne. Le nom `linux` fait référence à la ligne `label` située sous chacune des options de démarrage.
- `image=/boot/vmlinuz-2.4.0-0.43.6` spécifie le noyau Linux à amorcer au moyen de cette option.
- `label=linux` donne le nom de l'option du système d'exploitation sur l'écran LILO. Dans ce cas, il s'agit également du nom auquel fait référence la ligne `default`.
- `initrd=/boot/initrd-2.4.0-0.43.6.img` se réfère à l'image **disque RAM initial** qui est utilisée lors du démarrage pour initialiser et lancer les périphériques qui font en sorte qu'il est possible d'amorcer le noyau. Le disque RAM initial est un ensemble de pilotes nécessaires au fonctionnement de l'unité de disque dur et tout ce qui sert à charger le noyau. Vous ne devriez jamais essayer de partager des disques RAM initiaux entre différents ordinateurs à moins que la configuration de leur matériel ne soit identique (et même dans ce cas, c'est une bien mauvaise idée).
- `read-only` spécifie que la partition root (voir la ligne `root` en-dessous) ne peut être modifiée elle ne peut qu'être lue.
- `root=/dev/hda5` indique à LILO quelle partition de disque utiliser en tant que partition root.

LILO affiche ensuite l'écran Red Hat Linux initial sur lequel apparaissent les systèmes d'exploitation ou les noyaux qui, selon la configuration choisie, doivent être amorcés. Si vous n'avez installé que Red Hat Linux et n'avez rien changé dans `/etc/lilo.conf`, vous ne verrez que l'option linux. Si vous avez configuré LILO de façon à ce qu'il amorce également d'autres systèmes d'exploitation, cet écran vous donnera la possibilité de choisir quel système amorcer. Utilisez les flèches de direction pour choisir le système d'exploitation désiré et appuyez sur [Entrée].

Si vous désirez avoir une invite pour donner des commandes à LILO, appuyez sur [Cntl]-[X]. LILO affiche alors une invite `LILO:` sur l'écran et attend pendant une période de temps préétablie que l'utilisateur entre une commande (cette période d'attente de LILO est déterminée par la ligne `timeout` dans le fichier `/etc/lilo.conf`). Si le fichier `/etc/lilo.conf` est programmé pour donner un choix de systèmes d'exploitation à LILO, à ce moment vous pourrez taper l'étiquette de l'un où l'autre des systèmes d'exploitation que vous désirez amorcer.

Si LILO amorce Linux, il charge d'abord le noyau dans la mémoire, un fichier `vmlinuz` (avec un numéro de version, tel que `vmlinuz-2.4.0-xx` par exemple) qui se trouve dans le répertoire `/boot`. Ensuite, le noyau donne le contrôle à `init`.

Ainsi, le noyau étant chargé dans la mémoire et opérationnel, Linux est déjà amorcé, bien qu'à un niveau encore très bas. Cependant, comme aucune application n'utilise le noyau et que l'utilisateur ne peut donner d'informations utiles au système, on ne peut en faire grand chose. Le programme `init` résout ce problème en démarrant les divers services qui permettent au système de jouer son rôle.

3.2.2 Init

Le noyau trouve `init` dans `/sbin` et l'exécute ; `init` coordonne ensuite le reste du processus de démarrage.

Lorsque `init` est lancé, il devient l'élément parent ou grand-parent de tous les processus qui sont lancés automatiquement sur votre système Red Hat Linux. D'abord, il exécute le script `/etc/rc.d/rc.sysinit`, qui établit les chemins d'exécution par défaut, initialise le swap, vérifie les systèmes de fichiers, etc. Bref, `rc.sysinit` s'occupe de tout ce dont a besoin votre système lors de son initialisation. Exemple : sur un système en réseau, `rc.sysinit` utilise l'information contenue dans le fichier `/etc/sysconfig/network` pour initialiser le processus réseau. La plupart des systèmes utilisent une horloge, donc `rc.sysinit` utilise le fichier `/etc/sysconfig/clock` sur ceux-ci pour initialiser l'horloge. Si vous avez des processus de port série spéciaux à initialiser, `rc.sysinit` peut aussi exécuter `rc.serial`.

Ensuite, `init` exécute le script `/etc/inittab`, qui décrit comment le système doit être configuré dans chaque **niveau d'exécution** et définit le niveau d'exécution par défaut. (Voir la Section 3.4, *Niveaux d'exécution d'Init* pour avoir plus de détails sur les niveaux d'exécution d'init.) Ce fichier établit notamment que `/sbin/update` doit être exécuté chaque fois qu'un niveau d'exécution commence. Le programme `update` sert à recopier périodiquement les tampons mémoire vers les disques.

Lorsque le niveau d'exécution change, `init` utilise les scripts dans `/etc/rc.d/init.d` pour faire démarrer ou arrêter différents services, tels que votre serveur Web, votre serveur DNS, etc. Premièrement, `init` définit la bibliothèque de fonctions source pour le système (`/etc/rc.d/init.d/functions` habituellement), qui explique comment démarrer ou arrêter un programme et comment trouver l'identification des paramètres d'un programme. Puis, `init` détermine le niveau d'exécution en cours ainsi que le niveau précédent.

Ensuite, `init` lance toutes les tâches de fond nécessaires pour que le système puisse s'exécuter en cherchant dans le répertoire `rc` approprié pour ce niveau d'exécution (`/etc/rc.d/rc<x>.d`, où `<x>` est numéroté de 0 à 6). `init` exécute chacun des scripts kill (leur nom de fichier commencent par un `K`) avec un paramètre `stop`. Par la suite, `init` exécute tous les scripts de démarrage (leur nom de fichier commencent par un `S`) dans le répertoire approprié du niveau d'exécution avec un `start` afin que tous les services et applications soient lancés correctement. En fait, vous pouvez exécuter ces scripts de façon manuelle après que le système a fini l'amorçage au moyen de commandes telles que `/etc/rc.d/init.d/httpd stop` ou `service httpd stop` si vous êtes l'utilisateur root. Cela arrêtera le serveur `httpd`.

Remarque

Il est préférable d'être l'utilisateur root pour lancer des services manuellement. Si vous obteniez une erreur en exécutant `service httpd stop`, vous pourriez ne pas avoir spécifié l'accès à `/sbin` dans `/root/.bashrc` (ou le bon fichier `.rc` pour votre shell préféré). Vous pouvez alors entrer la commande complète de `/sbin/service httpd stop` ou ajouter `export PATH="$PATH:/sbin"` à votre fichier shell `.rc`. Si vous modifiez le fichier de configuration du shell, sortez et reconnectez-vous en tant qu'utilisateur root afin que le fichier de configuration du shell modifié soit appliqué.

Aucun des scripts qui lancent et arrêtent les services n'est réellement situé dans `/etc/rc.d/rc<x>.d`. Tous les fichiers dans `/etc/rc.d/rc<x>.d` sont des **liens symboliques** qui pointent vers les scripts, qui sont situés dans `/etc/rc.d/init.d`. Un lien symbolique n'est autre qu'un fichier qui pointe vers un autre fichier. Dans le cas présent, on en fait usage car ils peuvent être créés et éliminés sans avoir aucun effet sur les scripts eux-mêmes, qui arrêtent ou démarrent les services. Les liens symboliques sont numérotés et ont un ordre particulier afin qu'ils s'exécutent dans cet ordre. Il vous est possible de changer l'ordre dans lequel les services sont arrêtés ou démarrés en changeant le nom du lien symbolique se référant au script qui démarre ou arrête un service donné. Vous pouvez donner aux liens symboliques le même numéro qu'un autre lien si vous voulez que ce service démarre ou arrête juste avant ou juste après cet autre service.

Exemple : pour le niveau d'exécution 5, `init` cherche dans le répertoire `/etc/rc.d/rc5.d` et pourrait trouver ce qui suit (votre système et votre configuration peuvent varier) :

```
K01pppoe -> ../init.d/pppoe
K05innd -> ../init.d/innd
K10ntpd -> ../init.d/ntpd
K15httpd -> ../init.d/httpd
K15mysqld -> ../init.d/mysqld
K15pvmd -> ../init.d/pvmd
K16rarpd -> ../init.d/rarpd
K20bootparamd -> ../init.d/bootparamd
K20nfs -> ../init.d/nfs
K20rstatd -> ../init.d/rstatd
K20rusersd -> ../init.d/rusersd
K20rwalld -> ../init.d/rwalld
K20rwhod -> ../init.d/rwhod
K25squid -> ../init.d/squid
K28amd -> ../init.d/amd
K30mcserv -> ../init.d/mcserv
```

```
K34yppasswdd -> ../init.d/yppasswdd
K35dhcpd -> ../init.d/dhcpd
K35smb -> ../init.d/smb
K35vncserver -> ../init.d/vncserver
K45arpwatch -> ../init.d/arpwatch
K45named -> ../init.d/named
K50snmpd -> ../init.d/snmpd
K54pxe -> ../init.d/pxe
K55routed -> ../init.d/routed
K60mars-nwe -> ../init.d/mars-nwe
K61ldap -> ../init.d/ldap
K65kadmin -> ../init.d/kadmin
K65kprop -> ../init.d/kprop
K65krb524 -> ../init.d/krb524
K65krb5kdc -> ../init.d/krb5kdc
K75gated -> ../init.d/gated
K80nscd -> ../init.d/nscd
K84ypserv -> ../init.d/ypserv
K90ups -> ../init.d/ups
K96irda -> ../init.d/irda
S05kudzu -> ../init.d/kudzu
S06reconfig -> ../init.d/reconfig
S08ipchains -> ../init.d/ipchains
S10network -> ../init.d/network
S12syslog -> ../init.d/syslog
S13portmap -> ../init.d/portmap
S14nfslock -> ../init.d/nfslock
S18autofs -> ../init.d/autofs
S20random -> ../init.d/random
S25netfs -> ../init.d/netfs
S26apmd -> ../init.d/apmd
S35identd -> ../init.d/identd
S40atd -> ../init.d/atd
S45pcmcia -> ../init.d/pcmcia
S55sshd -> ../init.d/sshd
S56rawdevices -> ../init.d/rawdevices
S56xinetd -> ../init.d/xinetd
S60lpd -> ../init.d/lpd
S75keytable -> ../init.d/keytable
S80isdn -> ../init.d/isdn
S80sendmail -> ../init.d/sendmail
S85gpm -> ../init.d/gpm
S90canna -> ../init.d/canna
S90crond -> ../init.d/crond
S90FreeWnn -> ../init.d/FreeWnn
```

```
S90xfs -> ../init.d/xfs
S95anacron -> ../init.d/anacron
S97rhnsd -> ../init.d/rhnsd
S99linuxconf -> ../init.d/linuxconf
S99local -> ../rc.local
```

Ces liens symboliques indiquent à `init` qu'il doit arrêter `pppoe`, `innd`, `ntpd`, `httpd`, `mysqld`, `pvmd`, `rarpd`, `bootparamd`, `nfs`, `rstatd`, `rusersd`, `rwalld`, `rwhod`, `squid`, `amd`, `mcserv`, `yppasswdd`, `dhcpd`, `smb`, `vncserver`, `arpwatch`, `named`, `snmpd`, `pxe`, `routed`, `mars-nwe`, `ldap`, `kadmin`, `kprop`, `krb524`, `krb5kdc`, `gated`, `nscd`, `ypserv`, `ups`, et `irda`. Une fois tous ces processus arrêtés, `init` cherche dans le même répertoire et trouve des scripts de démarrage pour `kudzu`, `reconfig`, `ipchains`, `portmap`, `nfslock`, `autofs`, `random`, `netfs`, `apmd`, `identd`, `atd`, `pcmcia`, `sshd`, `rawdevices`, `xinetd`, `lpd`, `keytable`, `isdn`, `sendmail`, `gpm`, `canna`, `crond`, `FreeWnn`, `xfs`, `anacron`, `rhnsd`, et `linuxconf`. La dernière chose que fait `init` est d'exécuter `/etc/rc.d/rc.local` afin de lancer tout script spécial configuré pour cet ordinateur hôte. A ce stade, le système est considéré comme opérationnel au niveau d'exécution 5.

Lorsqu'`init` a parcouru tous les niveaux d'exécution, le script `/etc/inittab` lance un processus `getty` pour chaque console virtuelle (invites de connexion) et pour chaque niveau d'exécution (les niveaux d'exécution 2 à 5 obtiennent les six consoles, alors que le niveau d'exécution 1, qui est un mode mono-utilisateur, n'en obtient qu'une ; les niveaux 0 et 6 n'obtiennent aucune console virtuelle). Fondamentalement, `getty` ouvre des terminaux, définit leur mode, imprime l'invite d'ouverture de session, obtient le nom d'utilisateur et initialise ensuite un processus d'ouverture de session pour cet utilisateur. Cela permet à l'utilisateur de s'authentifier auprès du système et de commencer à l'utiliser.

De plus, `/etc/inittab` indique à `init` comment interpréter la combinaison des touches [Ctrl]-[Alt]-[Suppr] sur la console. Comme Red Hat Linux doit être correctement arrêté et redémarré, `init` reçoit la directive d'exécuter la commande `/sbin/shutdown -t3 -r now` lorsqu'un utilisateur appuie sur ces touches. Aussi, `/etc/inittab` indique ce que `init` devrait faire en cas de panne d'alimentation, si un système d'alimentation sans coupure est branché à l'ordinateur.

Au niveau d'exécution 5, `/etc/inittab` exécute un script appelé `/etc/X11/prefdm`. Le script `prefdm` exécute le gestionnaire d'affichage X préféré (`gdm` si vous utilisez GNOME, `kdm` si vous utilisez KDE ou `xdm` si vous utilisez AnotherLevel) en fonction de ce qui est contenu dans le répertoire `/etc/sysconfig/desktop`.

A ce stade, le système devrait afficher une invite de connexion. Tout cela s'est produit en quelques secondes seulement.

3.2.3 Init SysV

Comme nous l'avons vu, le programme `init` est exécuté par le noyau au démarrage. Il est chargé de lancer tous les processus normaux qui ont besoin de démarrer avec le système. Ces derniers incluent

notamment les processus getty qui vous permettent de vous connecter, les démons NFS ou FTP et tout ce que vous aimeriez exécuter lors du démarrage de votre ordinateur.

init SysV est le processus init standard de l'univers Linux pour le contrôle de l'exécution de logiciels au démarrage car il est facile à utiliser, plus puissant et plus flexible que le programme `init` BDS traditionnel.

init SysV est aussi différent de init BDS du fait que ses fichiers de configuration sont dans `/etc/rc.d` au lieu d'être situés directement dans `/etc`. Dans `/etc/rc.d`, vous trouverez `rc`, `rc.local`, `rc.sysinit` et les répertoires suivants :

```
init.d
rc0.d
rc1.d
rc2.d
rc3.d
rc4.d
rc5.d
rc6.d
```

init SysV représente chacun des niveaux d'exécution d'init avec un répertoire séparé, au moyen de liens symboliques dans chaque répertoire, afin que `init` puisse arrêter ou démarrer les services au fur et à mesure que le système passe d'un niveau d'exécution à l'autre.

Pour résumer le tout, la chaîne des événements d'un démarrage init SysV se présente comme suit :

- Le noyau recherche `init` dans `/sbin`.
- `init` exécute le script `/etc/rc.d/rc.sysinit`.
- `rc.sysinit` prend en charge la plupart des processus du chargeur de démarrage et exécute ensuite `rc.serial` (s'il existe).
- `init` exécute tous les scripts pour le niveau d'exécution par défaut.
- `init` exécute `/etc/rc.d/rc.local`.

Le niveau d'exécution par défaut est défini dans `/etc/inittab`. Vous devriez avoir une ligne près du début qui ressemble à ceci :

```
id:3:initdefault:
```

Dans cet exemple, le niveau d'exécution par défaut est 3, soit le chiffre qui suit le premier deux-points. Si vous désirez le changer, vous pouvez modifier manuellement `/etc/inittab`. Soyez très prudent lorsque vous apportez des changements au fichier `inittab`. Si vous faites une erreur, vous pouvez la corriger en redémarrant l'ordinateur, en allant dans l'invite `boot:` avec [Ctrl]-[X] et en tapant :

```
boot:  linux single
```

Ceci *devrait* vous permet de démarrer en mode mono-utilisateur afin de modifier à nouveau `inittab` et de rétablir les valeurs initiales.

Maintenant, nous aborderons la question des informations contenues dans les fichiers qui se trouvent dans `/etc/sysconfig` et qui définissent les paramètres utilisés par les différents services au moment de leur démarrage.

3.3 Information Sysconfig

Ce qui suit souligne certains fichiers situés dans `/etc/sysconfig` : leur fonction et leur contenu. Cette information n'est pas complète car nombre de ces fichiers ont une série d'options qui ne sont utilisées que dans des circonstances spécifiques et plutôt rares.

3.3.1 Fichiers dans `/etc/sysconfig`

Les fichiers suivants se trouvent généralement dans `/etc/sysconfig` :

- `amd`
- `apmd`
- `authconfig`
- `cipe`
- `clock`
- `desktop`
- `firewall`
- `harddisks`
- `hwconf`
- `i18n`
- `init`
- `irda`
- `keyboard`
- `kudzu`
- `mouse`
- `network`
- `pcmcia`
- `rawdevices`

- `sendmail`
- `soundcard`
- `ups`
- `vncservers`

Il est possible qu'il en manque quelques-uns sur votre ordinateur si le programme correspondant nécessitant ce fichier n'est pas installé.

Jetons un coup d'oeil à chacun d'entre eux.

`/etc/sysconfig/amd`

Le fichier `/etc/sysconfig/amd` contient différents paramètres utilisés par `amd` pour permettre le montage et le démontage automatiques de systèmes de fichiers.

`/etc/sysconfig/apmd`

Le fichier `/etc/sysconfig/apmd` est utilisé par `apmd` en tant que configuration pour indiquer ce qu'il faut démarrer, arrêter ou changer en cas de suspension ou de reprise. Il est configuré pour activer ou désactiver `apmd` pendant le démarrage, selon que votre matériel prend ou non en charge la technologie **APM** (**Advanced Power Management** / gestion d'é,nergie avancée) ou que vous décidez de ne pas l'utiliser. `apm` est un démon de contrôle qui fonctionne avec le code de gestion d'énergie au sein du noyau Linux. Il peut notamment vous avertir lorsque le niveau de la batterie est bas, si vous utilisez Red Hat Linux sur un ordinateur portable.

`/etc/sysconfig/authconfig`

Le fichier `/etc/sysconfig/authconfig` définit le type d'autorisation à utiliser sur l'ordinateur hôte. Il contient une ou plusieurs des lignes suivantes :

- `USEMD5=<`*`valeur`*`>`, où `<`*`valeur`*`>` est un des éléments suivants :
  - `yes` — MD5 est utilisé pour l'authentification.
  - `no` — MD5 n'est pas utilisé pour l'authentification.

- `USEKERBEROS=<`*`valeur`*`>`, où `<`*`valeur`*`>` est l'un des éléments suivants :
  - `yes` — Kerberos est utilisé pour l'authentification.
  - `no` — Kerberos n'est pas utilisé pour l'authentification.

- `USELDAPAUTH=<`*`valeur`*`>`, où `<`*`valeur`*`>` est l'un des éléments suivants :

- yes — LDAP est utilisé pour l'authentification.
- no — LDAP n'est pas utilisé pour l'authentification.

/etc/sysconfig/cipe

Le fichier /etc/sysconfig/cipe configure cipe lorsqu'il est lancé.

Il peut contenir les exemples de valeurs suivants :

- DEVICE=eth0, qui spécifie la carte réseau que cipe utilisera.
- PORT=9999, qui désigne le numéro de port UDP que le processus cipe doit utiliser aux deux extrémités.
- PEER=0.0.0.0, qui spécifie l'adresse réelle de l'extrémité cipe distante. Vous pouvez configurer cette adresse de façon dynamique en y inscrivant une valeur de 0.0.0.0.
- IPADDR=0.0.0.0, qui spécifie l'adresse virtuelle de l'extrémité locale du tunnel cipe.
- PTPADDR=0.0.0.0, qui spécifie l'adresse virtuelle de l'extrémité distante du tunnel cipe.

/etc/sysconfig/clock

Le fichier /etc/sysconfig/clock contrôle l'interprétation des valeurs que lit l'horloge du système. Les versions précédentes de Red Hat Linux utilisaient les valeurs suivantes (qui sont déconseillées) :

- CLOCKMODE=<*valeur*>, où <*valeur*> estl'un des éléments suivants :
  - GMT — indique que l'horloge est réglée sur l'heure universelle (l'heure de Greenwich).
  - ARC — indique que le décalage de 42 ans de la console ARC est activé (pour les systèmes fondés sur Alpha seulement).

Actuellement, les bonnes valeurs sont :

- UTC=<*valeur*>, où <*valeur*> est une des valeurs booléennes suivantes :
  - true — indique que l'horloge est réglée sur l'heure universelle. Toute autre valeur signifie qu'elle est réglée sur l'heure locale.
- ARC=<*valeur*>, où <*valeur*> est l'un des éléments suivants :
  - true — indique que le décalage de 42 ans de la console ARC est activé. Toute autre valeur indique que l'époque UNIX normale est supposée (uniquement pour les systèmes de type Alpha).

- `ZONE=<filename>` — indique le fichier de fuseau horaire sous `/usr/share/zoneinfo`, dont `/etc/localtime` est une copie, par exemple :

```
ZONE="Amérique/New York"
```

/etc/sysconfig/desktop

Le fichier `/etc/sysconfig/desktop` spécifie le gestionnaire de bureau devant être exécuté, tel que :

```
DESKTOP="GNOME"
```

/etc/sysconfig/firewall

Le fichier `/etc/sysconfig/firewall` contient les différentes configurations de coupe-feu. Par défaut, ce fichier est créé, mais il est vide.

/etc/sysconfig/harddisks

Le fichier `/etc/sysconfig/harddisks` vous permet de régler le(s) disque(s) dur(s).

N'apportez aucun changement à ce fichier de façon non réfléchie. Si vous modifiez les valeurs par défaut qui y sont enregistrées, vous pourriez altérer toutes les données qui sont sur le(s) disque(s) dur(s).

Le fichier `/etc/sysconfig/harddisks` peut contenir ce qui suit :

- `USE_DMA=1`, où la valeur 1 active DMA. Toutefois, avec certaines combinaisons circuits/disque dur, cette DMA pourrait entraîner une corruption de données. *Vérifiez la documentation concernant votre disque dur ou auprès du fabricant avant de l'activer.*
- `Multiple_IO=16`, où la valeur 16 autorise plusieurs secteurs par interruption d'entrée/sortie. Lorsqu'elle est activée, cette fonction réduit le temps de gestion du système d'exploitation de 30 à 50 %. *Utilisez-la avec prudence.*
- `EIDE_32BIT=3` active le support E/S (E)IDE 32-bits pour une carte d'interface.
- `LOOKAHEAD=1` active l'anticipation en lecture du lecteur.
- `EXTRA_PARAMS=` spécifie l'endroit où peuvent être ajoutés des paramètres supplémentaires.

/etc/sysconfig/hwconf

Le fichier /etc/sysconfig/hwconf affiche la liste de tout le matériel que kudzu a détecté sur votre ordinateur, ainsi que l'information sur les pilotes utilisés, l'ID du fabricant et du périphérique. Le programme kudzu détecte et configure le matériel nouveau ou modifié d'un ordinateur. Le fichier /etc/sysconfig/hwconf n'est pas destiné à être modifié manuellement. Si vous le faites, certains périphériques pourraient soudainement apparaître comme ajoutés ou supprimés.

/etc/sysconfig/i18n

Le fichier /etc/sysconfig/i18n définit la langue par défaut, telle que :

```
LANG="fr_FR"
```

/etc/sysconfig/init

Le fichier /etc/sysconfig/init contrôle l'aspect et le fonctionnement du système durant la séquence de démarrage.

Les valeurs suivantes peuvent être utilisées :

- BOOTUP=<*valeur*>, où <*valeur*> est l'un des éléments suivants :
  - BOOTUP=color signifie un affichage couleur standard au démarrage ; la réussite ou l'échec du démarrage des périphériques et des services sont indiqués par des couleurs différentes.
  - BOOTUP=verbose signifie un affichage dans l'ancien style, ce qui offre plus d'informations qu'un simple message de réussite ou d'échec.
  - Toute autre chose signifie un nouvel affichage, mais sans mise en forme ANSI.

- RES_COL=<*valeur*>, où <*valeur*> est le numéro de la colonne de l'écran à laquelle commencer les étiquettes d'état. La valeur par défaut est 60.
- MOVE_TO_COL=<*valeur*>, où <*valeur*> déplace le curseur sur la valeur dans la ligne RES_COL. Indique, par défaut, une sortie de séquences ANSI par écho -e.
- SETCOLOR_SUCCESS=<*valeur*>, où <*valeur*> configure la couleur indiquant la réussite. Indique, par défaut, une sortie de séquences ANSI par écho -e, définissant la couleur sur vert.
- SETCOLOR_FAILURE=<*valeur*>, où <*valeur*> configure la couleur indiquant l'échec. Indique, par défaut, une sortie de séquences ANSI par écho -e, définissant la couleur sur rouge.
- SETCOLOR_WARNING=<*valeur*>, où <*valeur*> configure la couleur indiquant un avertissement. Indique, par défaut, une sortie de séquences ANSI par écho -e, définissant la couleur sur jaune.

- `SETCOLOR_NORMAL=<valeur>`, où `<valeur>` configure la couleur sur 'normal'. Indique, par défaut, une sortie de séquences ANSI par écho `-e`.
- `LOGLEVEL=<valeur>`, où `<valeur>` définit le niveau de connexion initial de la console pour le noyau. La valeur par défaut est 7 : 8 signifie tout (y compris le débogage) ; 1 ne signifie rien d'autre que les panics du noyau. `syslogd` écrasera ceci au démarrage.
- `PROMPT=<valeur>`, où `<valeur>` est une des valeurs booléennes suivantes :
  - `yes` — active le contrôle du mode interactif au clavier.
  - `no` — désactive le contrôle du mode interactif au clavier.

`/etc/sysconfig/irda`

Le fichier `/etc/sysconfig/irda` contrôle la configuration des périphériques à infrarouge de votre système lors du démarrage.

Les valeurs suivantes peuvent être utilisées :

- `IRDA=<valeur>`, où `<valeur>` est une des valeurs booléennes suivantes :
  - `yes` — `irattach` s'exécute et vérifie de façon périodique si certains périphériques essaient de se connecter au port infrarouge, tel qu'un ordinateur bloc-notes qui tente d'effectuer une connexion réseau. Pour que des périphériques à infrarouge fonctionnent sur votre système, cette ligne doit être réglée sur `yes`.
  - `no` — `irattach` ne s'exécute pas et empêche toute communication avec les périphériques à infrarouge.

- `DEVICE=<valeur>`, où `<valeur>` est le périphérique (généralement le port série) qui gère les connexions à infrarouge.
- `DONGLE=<valeur>`, où `<valeur>` spécifie le type de clé électronique utilisée pour les communications par infrarouges. Ce paramètre existe pour les gens qui utilisent des clés électroniques série plutôt que de vrais ports infrarouges. Une clé électronique est un dispositif qui est branché à un port série traditionnel pour la communication par infrarouges. Cette ligne est, par défaut, réglée sur l'inactivité car les ordinateurs bloc-notes ayant de vrais ports infrarouges sont beaucoup plus fréquents que ceux qui ont des clés électroniques ajoutées.
- `DISCOVERY=<valeur>`, où `<valeur>` est une des valeurs booléennes suivantes.
  - `yes` — lance `irattach` en mode découverte, ce qui signifie qu'il cherche activement d'autres périphériques à infrarouge. Cette fonction doit être activée pour que l'ordinateur

puisse chercher de façon active une connexion infrarouge (c'est-à-dire un élément qui ne prend pas l'initiative de connexion).

– `no` — `irattach` ne s'exécute pas en mode découverte.

/etc/sysconfig/keyboard

Le fichier `/etc/sysconfig/keyboard` contrôle le comportement du clavier. Les valeurs suivantes peuvent être utilisées :

- `KEYBOARDTYPE=sun|pc`, qui n'est utilisée que sur les systèmes SPARC. `sun` signifie qu'un clavier Sun est connecté à `/dev/kbd` et `pc` signifie qu'un clavier PS/2 est connecté à un port PS/2.
- `KEYTABLE=<`*`file`*`>`, où `<`*`file`*`>` est le nom d'un fichier de clavier. Par exemple : `KEYTABLE="us"`. Les fichiers pouvant être utilisés comme fichier de clavier commencent dans `/usr/lib/kbd/keymaps/i386` et se ramifient en différents topogrammes de clavier à partir de là, tous étiquetés `<`*`file`*`>.kmap.gz`. Le premier fichier qui se trouve sous `/usr/lib/kbd/keymaps/i386` et qui correspond au paramètre `KEYTABLE` est utilisé.

/etc/sysconfig/kudzu

Le fichier `/etc/sysconfig/kuzdu` vous permet de spécifier la détection sécuritaire du matériel de votre ordinateur par `kudzu` lors du démarrage. Une détection sécuritaire désactive la détection de ports série et de moniteurs DDC.

- `SAFE=<`*`valeur`*`>`, où `<`*`valeur`*`>` est l'un des éléments suivants :
  – `yes` — `kuzdu` exécute une détection sécuritaire.
  – `no` — `kuzdu` exécute une détection normale.

/etc/sysconfig/mouse

Le fichier `/etc/sysconfig/mouse` sert à spécifier des renseignements sur la souris disponible. Les valeurs suivantes peuvent être utilisées :

- `FULLNAME=<`*`valeur`*`>`, où `<`*`valeur`*`>` se réfère au nom complet de la souris utilisée.
- `MOUSETYPE=<`*`valeur`*`>`, où `<`*`valeur`*`>` est l'un des éléments suivants :
  – `microsoft` — une souris Microsoft™.
  – `mouseman` — une souris MouseMan™.
  – `mousesystems` — une souris Mouse Systems™.

  - `ps/2` — une souris PS/2.
  - `msbm` — une souris bus Microsoft™.
  - `logibm` — une souris bus Logitech™.
  - `atibm` — une souris bus ATI™.
  - `logitech` — une souris Logitech™.
  - `mmseries` — un ancien modèle de souris MouseMan™.
  - `mmhittab` — une souris mmhittab.

- `XEMU3=<valeur>`, où `<valeur>` est une des valeurs booléennes suivantes :
  - `yes` — la souris n'a que deux boutons, mais trois boutons de souris devraient être simulés.
  - `no` — la souris a déjà trois boutons.

- `XMOUSETYPE=<valeur>`, où `<valeur>` se réfère au type de souris utilisée lors de l'exécution de X Window. Les options dans ce cas sont les mêmes que pour la définition `MOUSETYPE` dans ce même fichier.

De plus, `/dev/mouse` est un lien symbolique qui pointe vers le périphérique de souris réel.

`/etc/sysconfig/network`

Le fichier `/etc/sysconfig/network` est utilisé pour spécifier des informations sur la configuration réseau désirée. Les valeurs suivantes peuvent être utilisées :

- `NETWORKING=<valeur>`, où `<valeur>` est une des valeurs booléennes suivantes :
  - `yes` — la connexion au réseau devrait être configurée.
  - `no` — la connexion au réseau ne devrait pas être configurée.

- `HOSTNAME=<valeur>`, où `<valeur>` devrait être un **nom de domaine complet**, tel que `hôte.domaine.com`, mais vous pouvez choisir le nom d'hôte que vous voulez.

Remarque

Pour assurer la compatibilité avec des logiciels plus anciens que certaines personnes risqueraient d'installer (tels que `trn`), le fichier `/etc/HOSTNAME` devrait contenir la même valeur qu'ici.

- `GATEWAY=<`*`valeur`*`>`, où `<`*`valeur`*`>` est l'adresse IP de la passerelle du réseau.
- `GATEWAYDEV=<`*`valeur`*`>`, où `<`*`valeur`*`>` est le périphérique de passerelle, tel que `eth0`.
- `NISDOMAIN=<`*`valeur`*`>`, où `<`*`valeur`*`>` est le nom de domaine NIS.

`/etc/sysconfig/pcmcia`

Le fichier `/etc/sysconfig/pcmcia` est utilisé pour spécifier des informations de configuration de la carte PCMCIA. Les valeurs suivantes peuvent être utilisées :

- `PCMCIA=<`*`valeur`*`>`, où `<`*`valeur`*`>` est un des éléments suivants :
  - `yes` — le support PCMCIA doit être activé.
  - `no` — le support PCMCIA ne doit pas être activé.

- `PCIC=<`*`valeur`*`>`, où `<`*`valeur`*`>` est un des éléments suivants :
  - `i82365` — l'ordinateur a un circuit de socket PCMCIA de type i82365.
  - `tcic` — l'ordinateur a un circuit de socket PCMCIA de type tcic.

- `PCIC_OPTS=<`*`valeur`*`>`, où `<`*`valeur`*`>` correspond aux paramètres de synchronisation du pilote de support (i82365 ou tcic).
- `CORE_OPTS=<`*`valeur`*`>`, où `<`*`valeur`*`>` est la liste d'options `pcmcia_core`.
- `CARDMGR_OPTS=<`*`valeur`*`>`, où `<`*`valeur`*`>` est la liste d'options pour le `cardmgr` PCMCIA (telles que : `-q`, mode silencieux ; `-m`, recherche des modules de noyau chargeables dans le répertoire spécifié ; etc.). Veuillez lire la page de manuel `cardmgr` pour avoir plus de détails.

`/etc/sysconfig/rawdevices`

Le fichier `/etc/sysconfig/rawdevices` est utilisé pour configurer les liaisons des raw device, comme par exemple :

```
/dev/raw/raw1 /dev/sda1
/dev/raw/raw2 8 5
```

/etc/sysconfig/sendmail

Le fichier `/etc/sysconfig/sendmail` permet d'envoyer des messages à un ou plusieurs destinataires, en acheminant les messages sur les réseaux nécessaires. Le fichier définit les valeurs par défaut pour l'exécution du programme Sendmail. Ses valeurs par défaut font qu'il s'exécute comme démon en tâche de fond et qu'il contrôle sa file d'attente une fois par heure si quelque chose a été sauvegardé.

Les valeurs suivantes peuvent être utilisées :

- `DAEMON=<valeur>`, où `<valeur>` est une des valeurs booléennes suivantes :
  - `yes` — Sendmail doit être configuré pour contrôler le port 25 afin de détecter le courrier entrant. `yes` implique l'utilisation des options `-bd` de Sendmail.
  - `no` — Sendmail ne devrait pas être configuré pour contrôler le port 25 afin de détecter le courrier entrant.

- `QUEUE=1h` qui est donné à Sendmail en tant que `-q$QUEUE`. L'option `-q` n'est pas donnée à Sendmail si le fichier `/etc/sysconfig/sendmail` existe et que `QUEUE` est vide ou non défini.

/etc/sysconfig/soundcard

Le fichier `/etc/sysconfig/soundcard` est généré par `sndconfig` et ne devrait pas être modifié. Le seul rôle de ce fichier est de déterminer l'entrée de carte de menu à afficher par défaut lors de la prochaine exécution de `sndconfig`. Les informations de configuration de la carte son se trouvent dans le fichier `/etc/modules.conf`.

Il peut contenir ce qui suit :

- `CARDTYPE=<valeur>`, où `<valeur>` est indiqué avec, par exemple, `SB16` pour une carte son Soundblaster 16.

/etc/sysconfig/ups

Le fichier `/etc/sysconfig/ups` est utilisé pour spécifier des informations concernant tout **système d'alimentation sans coupure** (**UPS**) branché au système. Un UPS peut être très utile à Red Hat Linux car il donne le temps nécessaire pour éteindre l'ordinateur lors de pannes de courant. Les valeurs suivantes peuvent être utilisées :

- SERVER=<*valeur*>, où <*valeur*> est un des éléments suivants :
  - yes — un dispositif UPS est branché à votre système.
  - no — aucun dispositif UPS n'est branché à votre système.

- MODEL=<*valeur*>, où <*valeur*> doit être un des éléments suivants ou doit être réglé sur NONE si aucun dispositif UPS n'est branché à votre système :
  - apcsmart — pour un périphérique SmartUPS™ APC ou semblable.
  - fentonups — pour un UPS Fenton™.
  - optiups — pour un dispositif UPS OPTI™.
  - bestups — pour un UPS Best Power™.
  - genericups — pour un UPS générique.
  - ups-trust425+625 — pour un UPS Trust™.

- DEVICE=<*valeur*>, où <*valeur*> spécifie où le dispositif UPS est branché, tel que /dev/ttyS0.
- OPTIONS=<*valeur*>, où <*valeur*> est une commande spéciale qui doit être passée au dispositif UPS.

/etc/sysconfig/vncservers

Le fichier /etc/sysconfig/vncservers configure comment le serveur **VNC** (**Virtual Network Computing**) démarre. VNC est un système d'affichage à distance qui vous permet de visualiser un environnement bureau sur l'ordinateur où il est exécuté ainsi que sur différents réseaux (d'un LAN à Internet) et utilise une vaste gamme d'architectures d'ordinateur.

Il peut contenir ce qui suit :

- VNCSERVERS=<*valeur*>, où <*valeur*> est réglé sur quelque chose qui ressemble à "1:root".

3.3.2 Fichiers dans /etc/sysconfig/network-scripts/

Les fichiers suivants se trouvent généralement dans /etc/sysconfig/network-scripts, où <*if-name*> correspond au nom de l'interface réseau :

- `/etc/sysconfig/network-scripts/ifup`
- `/etc/sysconfig/network-scripts/ifdown`
- `/etc/sysconfig/network-scripts/network-functions`
- `/etc/sysconfig/network-scripts/ifcfg-<`*`if-name`*`>`
- `/etc/sysconfig/network-scripts/ifcfg-<`*`if-name`*`>-<`*`clone-name`*`>`
- `/etc/sysconfig/network-scripts/chat-<`*`if-name`*`>`
- `/etc/sysconfig/network-scripts/dip-<`*`if-name`*`>`
- `/etc/sysconfig/network-scripts/ifup-post`

Examinons-les un par un.

`/etc/sysconfig/network-scripts/ifup` et `/etc/sysconfig/network-scripts/ifdown`

Il s'agit de liens symboliques respectivement vers `/sbin/ifup` et `/sbin/ifdown`. Ce sont les deux seuls scripts dans ce répertoire qui doivent être appelés directement ; ces derniers appellent ensuite les autres scripts au besoin. Ces liens symboliques ne sont là que pour des raisons historiques et seront probablement supprimés dans les futures versions. Par conséquent, seuls `/sbin/ifup` et `/sbin/ifdown` devraient être utilisés actuellement.

Ces scripts prennent normalement un argument : le nom du périphérique (tel que `eth0`). Ils sont appelés au moyen d'un deuxième argument de `boot` au cours de la séquence de démarrage de façon à ce que les périphériques ne devant pas être lancés au démarrage (`ONBOOT=no`, [voir ci-dessous]) puissent être ignorés à ce moment.

`/etc/sysconfig/network-scripts/network-functions`

Ce n'est pas réellement un fichier public. Il contient des fonctions que les scripts utilisent pour appeler et renvoyer des interfaces. Il contient, en particulier, l'essentiel du code pour la prise en charge des configurations d'interface alternatives et la notification de modification d'interface par le biais de `netreport`, programme qui indique aux scripts de gestion du réseau d'envoyer un signal SIGIO au processus qui appelle `netreport` lorsque des changements sont apportés à l'état de l'interface réseau.

`/etc/sysconfig/network-scripts/ifcfg-<`*`if-name`*`>` et `/etc/sysconfig/network-scripts/ifcfg-<`*`if-name`*`>:<`*`clone-name`*`>`

Le premier fichier définit une interface alors que le second ne contient que les parties de la définition qui sont différentes dans une interface "alias" (ou alternative). Les deux nécessitent que soit spécifié `<`*`if-name`*`>` (nom d'une interface réseau). Exemple : les numéros de réseau peuvent être différents,

mais tout le reste doit être identique, de sorte que seuls les numéros de réseau figureraient dans le fichier clone alors que les informations de périphériques seraient dans le fichier `ifcfg` de base.

Les éléments pouvant être définis dans un fichier `ifcfg` dépendent du type d'interface.

Les valeurs suivantes sont communes :

- `DEVICE=<`*`name`*`>`, où `<`*`name`* est le nom du périphérique physique (à l'exception des périphériques PPP attribués de façon dynamique là où est le "nom logique").
- `IPADDR=<`*`addr`*`>`, où `<`*`addr`*`>` est l'adresse IP.
- `NETMASK=<`*`mask`*`>`, où `<`*`mask`*`>` est la valeur du masque réseau.
- `NETWORK=<`*`addr`*`>`, où `<`*`addr`*`>` est l'adresse du réseau.
- `BROADCAST=<`*`addr`*`>`, où `<`*`addr`*`>` est l'adresse de diffusion.
- `GATEWAY=<`*`addr`*`>`, où `<`*`addr`*`>` est l'adresse de la passerelle.
- `ONBOOT=<`*`réponse`*`>`, où `<`*`réponse`*`>` est un des éléments suivants :
  - `yes` — ce périphérique doit être activé au démarrage
  - `no` — ce périphérique ne doit pas être activé au démarrage.
- `USERCTL=<`*`réponse`*`>`, où `<`*`réponse`*`>` est un des éléments suivants :
  - `yes` — les utilisateurs non root peuvent contrôler ce périphérique.
  - `no` — les utilisateurs non root ne peuvent contrôler ce périphérique.
- `BOOTPROTO=<`*`proto`*`>`, où `<`*`proto`*`>` est un des éléments suivants.
  - `none` — aucun protocole de démarrage ne doit être utilisé.
  - `bootp` — le protocole de démarrage doit être utilisé.
  - `dhcp` — le protocole DHCP doit être utilisé.

Les valeurs suivantes sont communes à tous les fichiers SLIP :

- `PERSIST=<`*`réponse`*`>`, où `<`*`réponse`*`>` est un des éléments suivants :
  - `yes` — ce périphérique doit rester actif en permanence, même s'il est désactivé après qu'un modem se soit déconnecté.
  - `no` — ce périphérique ne doit pas être actif en permanence.

- `MODEMPORT=<`*`port`*`>`, où `<`*`port`*`>` correspond au nom de périphérique du port modem (exemple : "`/dev/modem`").

- `LINESPEED=<`*`baud`*`>`, où `<`*`baud`*`>` est la vitesse de transmission du modem (exemple : "`115200`").
- `DEFABORT=<`*`réponse`*`>`, où `<`*`réponse`*`>` est un des éléments suivants :
  - `yes` — insère des chaînes d'abandon par défaut lors de la création ou de l'édition de scripts pour cette interface.
  - `no` — n'insère pas de chaînes d'abandon lors de la création ou de l'édition de scripts pour cette interface.

`/etc/sysconfig/network-scripts/chat-<`*`if-name`*`>`

Ce fichier est un script chat pour les connexions SLIP et a pour but d'établir des connexions. Pour les périphériques SLIP, un script DIP est écrit à partir du script chat.

`/etc/sysconfig/network-scripts/ifup-post`

Ce fichier est appelé lorsqu'un périphérique réseau (à l'exception d'un périphérique SLIP) intervient. Il appelle `/etc/sysconfig/network-scripts/ifup-routes` pour établir des routes statiques qui dépendent de ce périphérique, établit des alias pour ce périphérique et définit le nom d'hôte si ce n'est déjà fait ; un nom d'hôte peut être trouvé pour l'IP de ce périphérique. `ifup-post` envoie SIGIO à tout programme ayant demandé une notification d'événements de réseau.

Au besoin, ce fichier pourrait être étendu pour définir la configuration du service de noms, appeler des scripts arbitraires, etc.

3.4 Niveaux d'exécution d'Init

L'idée derrière l'utilisation de différents services à des niveaux d'exécution différents se résume principalement au principe que divers systèmes peuvent être utilisés de différentes façons. Certains services ne peuvent être utilisés tant que le système n'a pas un état ou un **mode** bien précis, tel que de permettre l'utilisation à plus d'un utilisateur ou d'avoir une connexion réseau disponible. Vous pourriez parfois désirer utiliser le système à un mode plus bas, pour tester des problèmes relatifs au réseau au niveau 2 ou laisser le système au niveau d'exécution 3 sans exécuter de session X Window par exemple. Dans ces cas, l'exécution de services qui dépendent d'un mode du système plus élevé pour fonctionner n'a pas de sens car ils ne fonctionneront pas correctement de toute manière. En ayant défini chaque service pour qu'il s'exécute lorsque son niveau d'exécution particulier est atteint, vous vous assurez d'obtenir un processus de démarrage ordonné et vous pouvez changer rapidement le mode de l'ordinateur sans vous préoccuper des services devant être lancés ou arrêtés manuellement.

En général, Red Hat Linux fonctionne en niveau d'exécution 3 — mode multi-utilisateurs complet. Les niveaux d'exécution suivants sont définis dans Red Hat Linux :

- `0` — Arrêt
- `1` — Mode mono-utilisateur
- `2` — Mode multi-utilisateurs, sans connexion au réseau
- `3` — Mode multi-utilisateurs complet
- `4` — Non utilisé
- `5` — Mode multi-utilisateurs complet (avec écran de connexion de type X Window)
- `6` — Redémarrage

Le niveau d'exécution par défaut pour le démarrage et l'arrêt d'un système est configuré dans `/etc/inittab`. Pour obtenir plus de détails sur `/etc/inittab`, reportez-vous à la Section 3.2.3, *Init SysV*.

Si votre ordinateur ne démarre pas en raison d'un `/etc/inittab` incorrect ou ne vous laisse pas vous connecter parce que votre `/etc/passwd` est corrompu ou parce que vous avez oublié votre mot de passe, démarrez en mode mono-utilisateur en tapant **`linux single`** à l'invite `boot:` de LILO. Un système très dépouillé démarrera et vous disposerez d'un shell à partir duquel vous pourrez résoudre le problème.

3.5 Utilitaires de gestion des scripts Init

L'utilitaire `chkconfig` dans `/sbin` offre un outil de ligne de commande simple permettant de maintenir la hiérarchie de répertoires `/etc/rc.d/init.d`. Il libère les administrateurs système de la tâche de devoir manipuler directement les nombreux liens symboliques dans les répertoires sous `/etc/rc.d`.

De plus, l'utilitaire `ntsysv` dans `/usr/sbin` offre une interface orientée écran que vous trouverez peut-être plus facile à utiliser que l'interface de ligne de commande de `chkconfig`. Ces deux utilitaires doivent être exécutés en tant que root.

Veuillez lire les pages de manuel `chkconfig` et `ntsysv` pour obtenir plus d'informations.

3.6 Exécution de programmes au démarrage

Le fichier `/etc/rc.d/rc.local` est exécuté par `init` au démarrage, après accomplissement de toutes les autres tâches d'initialisation et chaque fois que vous modifiez des niveaux d'exécution. Vous pouvez y ajouter des commandes d'initialisation supplémentaires. Par exemple, il se pourrait que vous vouliez démarrer des démons supplémentaires ou initialiser une imprimante.

En outre, si vous avez besoin d'une configuration de port série, vous pouvez créer et modifier `/etc/rc.serial` qui sera exécuté automatiquement au démarrage. Ce script peut exécuter toute

une série de commandes `setserial` afin de configurer spécialement les ports série du système. Lisez les pages de manuel `setserial` pour plus de détails.

Le fichier `/etc/rc.d/rc.local` par défaut crée simplement une jolie bannière de connexion avec votre version de noyau et votre type d'ordinateur.

3.7 Arrêt

Pour arrêter Red Hat Linux, entrez la commande `shutdown`. Vous pouvez lire les pages de manuel `shutdown` pour avoir des renseignements complets à ce sujet, mais les deux utilisations les plus courantes sont :

```
/sbin/shutdown -h now
/sbin/shutdown -r now
```

Vous devez exécuter `shutdown` en tant qu'utilisateur root. L'option `-h` arrête l'ordinateur et l'option `-r` le redémarre.

Bien que les commandes `reboot` et `halt` puissent maintenant invoquer la commande `shutdown` si elles sont exécutées alors que le système est en niveaux d'exécution 1-5, ce n'est pas une bonne habitude à prendre car les systèmes de type Linux ne disposent pas tous de cette fonction.

Si l'ordinateur ne s'éteint pas par lui-même, vous ne devriez pas l'éteindre avant de voir apparaître le message qui vous indique que le système est arrêté ou qu'il a terminé son processus d'arrêt.

Si vous n'attendez pas ce message, cela signifie que vous éteignez l'ordinateur avant que les partitions du disque dur n'aient terminé d'être démontées. Cela peut provoquer la corruption du système de fichiers, à, tel point que votre système pourrait ne pas redémarrer à la prochaine tentative. Soyez patient lorsque vous arrêtez votre système.

3.8 Différences du processus de démarrage d'autres architectures

Chaque architecture d'ordinateur prise en charge par Red Hat Linux démarre le système d'exploitation de façon différente. Cependant, une fois que le noyau a commencé le démarrage et qu'il passe les commandes à `init`, les mêmes événements se produisent sur toutes les architectures de la même

façon. La seule différence est la manière dont Red Hat Linux trouve le noyau pour le charger afin de lancer `init`.

Consultez les informations d'installation des différentes architectures pour en savoir plus sur les diverses méthodes de démarrage.

4 Protocole LDAP (Lightweight Directory Access Protocol)

4.1 Qu'est-ce que le protocole LDAP ?

LDAP est une norme ouverte proposée pour les services d'annuaire globaux ou locaux sur réseau et/ou Internet. Dans ce sens, un annuaire a beaucoup en commun avec un annuaire téléphonique. Si le protocole LDAP peut traiter d'autres informations, il est surtout utilisé actuellement pour associer des noms à des numéros de téléphone et des adresses électroniques. Les répertoires sont conçus pour prendre en charge un volume important de requêtes, tandis que les données qu'ils contiennent ne sont pas sujettes à de fréquentes modifications.

Le protocole LDAP est beaucoup plus utile qu'un annuaire papier car, par sa conception, il est destiné à prendre en charge la propagation vers des serveurs LDAP sur tout Internet, un peu comme le **DNS** (**service de noms de domaines**). Les serveurs DNS connectent les ordinateurs les uns aux autres sur la base des noms de domaines ou des services demandés depuis un domaine, comme par exemple l'échange de courrier. Sans les serveurs DNS, les noms d'hôte ne pourraient pas être transformés en adresses IP, qui sont nécessaires à la communication TCP/IP. A l'avenir, le protocole LDAP pourrait offrir le même genre d'accès global à de nombreux types d'informations de répertoire : actuellement, le protocole LDAP est plus généralement utilisé au sein de grandes organisations, telles que des écoles ou entreprises, pour des services d'annuaire.

Le protocole LDAP est un système client/serveur. Un client LDAP se connecte à un serveur LDAP, puis émet ou saisit une requête pour obtenir des informations ou fournit au serveur des informations à entrer dans l'annuaire. Le serveur répond à la requête, la renvoie à un autre serveur LDAP ou accepte les informations afin de les incorporer dans l'annuaire.

Le protocole LDAP est parfois appelé **X.500 Lite**. X.500 est une norme internationale pour les annuaires. Elle est complète mais complexe et requiert d'importantes ressources de calcul et la pile OSI complète. Par contre, le protocole LDAP peut s'exécuter aisément sur un PC avec une connexion TCP/IP. Le protocole LDAP peut accéder à des répertoires X.500, mais ne prend pas en charge toutes les fonctions de X.500.

Ce chapitre décrit la configuration et l'utilisation de OpenLDAP, une implémentation "open source" de LDAP. OpenLDAP comprend `slapd`, un serveur LDAP autonome, `slurpd`, un serveur de duplication LDAP autonome, des bibliothèques implémentant le protocole LDAP, des utilitaires, des outils, des exemples de clients.

4.2 Avantages et inconvénients de LDAP

Le principal avantage du protocole LDAP réside dans la possibilité de consolider certains types d'informations au sein de votre organisation. Par exemple, toutes les listes d'utilisateurs au sein de l'organisation peuvent être fusionnées dans un annuaire LDAP. Cet annuaire peut être interrogé par toute application compatible avec LDAP ayant besoin de ces informations. Il peut également être utilisé par des utilisateurs ayant besoin d'informations d'annuaire.

Parmi les autres avantages du protocole LDAP figurent sa facilité d'implémentation (par rapport à X.500) et son API (Application Programming Interface, interface de programmation d'application) bien définie qui augure une croissance future du nombre d'applications compatibles avec LDAP et de passerelles LDAP.

Du côté des inconvénients, si vous voulez utiliser le protocole LDAP, il faut disposer d'applications compatibles avec LDAP ou avoir accès à des passerelles LDAP. Comme mentionné plus haut, l'utilisation du protocole LDAP est appelée à se développer ; toutefois, actuellement, les applications compatibles avec LDAP pour Linux ne sont pas légion. De même, le protocole LDAP ne prenant pas en charge certains contrôles d'accès, il ne prend donc pas en charge autant de fonctions de sécurité que X.500.

4.3 Utilisations du protocole LDAP

Plusieurs applications Netscape, dont Netscape Roaming Access, sont compatibles avec LDAP. Sendmail est capable d'utiliser le protocole LDAP pour rechercher des adresses. Votre organisation peut utiliser le protocole LDAP comme annuaire et/ou service de noms interne (à la place de NIS ou de tableaux bidimensionnels). Vous pouvez même utiliser un serveur LDAP personnel pour conserver une trace de votre propre carnet d'adresses électronique (reportez-vous à la Section 4.11, *Autres ressources*).

LDAP étant un protocole ouvert et configurable, vous pouvez l'utiliser pour stocker presque tous les types d'informations en relation avec une structure organisatrice.

4.3.1 Applications LDAP

Il existe plusieurs applications clients LDAP qui simplifient l'affichage et le changement des informations LDAP :

- Navigateur LDAP/Editeur — Un outil convivial entièrement écrit en langage Java, pour un déploiement facile sur plusieurs plate-formes. Vous le trouverez à l'adresse suivante : http://www.iit.edu/~gawojar/ldap
- GQ — Client LDAP basé sur GTK, fourni avec la distribution sous emballage Red Hat Linux 7.1 ou à l'adresse : http://biot.com/gq

- kldap — Client LDAP pour le projet KDE , disponible à l'adresse : http://www.mount-point.ch/oliver/kldap

4.3.2 LDAP et PAM

Le protocole LDAP peut être utilisé comme service d'authentification via le module `pam_ldap`. Le protocole LDAP est généralement utilisé comme serveur d'authentification central, de sorte que les utilisateurs disposent d'une identité de connexion unifiée couvrant les connexions aux consoles, les serveurs POP, les serveurs IMAP, les ordinateurs sous Samba connectés au réseau et même les ordinateurs sous Windows NT/2000. Grâce au protocole LDAP, toutes ces situations de connexion peuvent reposer sur la même combinaison ID utilisateur/mot de passe. Le module `pam_ldap` fait partie du paquetage `nss_ldap`.

4.4 Terminologie LDAP

Une **entrée** est une unité dans un annuaire LDAP. Une entrée est identifiée ou référencée par son **Distinguished Name** (DN) unique.

Une entrée a des **attributs** ; les attributs sont des éléments d'information directement associés à l'entrée. Par exemple, une organisation peut être une entrée LDAP. Parmi les attributs associés à l'organisation figurent son numéro de fax, son adresse, etc. Des personnes peuvent également constituer des entrées dans l'annuaire LDAP. Parmi les attributs utilisés pour les personnes figurent les numéros de téléphone et adresses électroniques.

Certains attributs sont obligatoires, tandis que d'autres sont facultatifs. Une **classe d'objets** définit les attributs obligatoires et les attributs facultatifs. Vous trouverez des définitions de classe d'objets dans le fichier `slapd.oc.conf`.

LDAP Data Interchange Format (LDIF, format d'échange de données LDAP) est un format de texte ASCII pour les entrées LDAP. Les fichiers qui échangent des données avec des serveurs LDAP doivent être au format LDIF. Une entrée LDIF ressemble à ceci :

```
[<id>]
dn: <distinguished name>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
<attrtype>: <attrvalue>
```

Une entrée peut contenir autant de paires <attrtype>: <attrvalue> que nécessaire. Une ligne vide indique que l'entrée est terminée et qu'une autre entrée va commencer.

Vos paires *<attrtype>* et *<attrvalue>* *doivent* être définies par un schéma avant de pouvoir être utilisé. Vous ne pouvez pas les définir simplement dans un fichier LDIF et utiliser un serveur LDAP sans que les données correspondantes dans ses fichiers schéma ne puissent utiliser cette information.

Tout ce qui est contenu dans < > est variable et vous pouvez le paramétrer lorsque vous ajoutez une entrée LDAP, à l'exception de *<id>*. *<id>* est un nombre qui est habituellement paramétreé par les outils LDAP lorsque vous ajoutez une entrée, et vous n'aurez sans doute jamais la nécessité d'en paramétrer aucun manuellement.

4.5 Mises à jour de OpenLDAP 2.0

OpenLDAP 2.0 représente la plus importante mise à jour de l'application, grâce à :

- *Support LDAPv3* — Fonctionne maintenant avec SASL, TLS et SSL, en autres améliorations, et est entièrement compatible avec RFC 2251-2256; de nombreux changements depuis LDAPv2 ont pour but de faire de LDAP un protocole plus sûr.
- *Support IPv6* — Supporte maintenant la nouvelle génération de protocoles Internet.
- *LDAP sur IPC* — OpenLDAP peut communiquer à l'intérieur d'un système particulier sans avoir besoin d'un réseau, ce qui le rend plus sûr.
- *Mise à jour de l'API C* — Améliore la connection et l'utilisation de l'application pour les programmeurs.
- *Support LDIFv1* — Entièrement compatible avec la version 1 de Full Data Interchange Format (LDIF) de LDAP.
- *Serveur LDAP autonome amélioré* — Comprend un système de contrôle d'accès mis à jour, un pool de conversation, des outils améliorés et bien plus.

4.6 Fichiers OpenLDAP

Les fichiers de configuration OpenLDAP sont installés dans le répertoire `/etc/openldap`. Si vous appliquez la commande `ls` à `/etc/openldap`, vous obtenez quelque chose comme ceci :

```
ldap.conf        ldapsearchprefs.conf  schema
ldapfilter.conf  ldaptemplates.conf    slapd.conf
```

4.6.1 Editer `/etc/openldap/slapd.conf`

Le fichier `slapd.conf`, qui se trouve dans `/etc/openldap`, contient les informations de configuration nécessaires à votre serveur LDAP `slapd`. Il vous faudra éditer ce fichier pour le rendre spécifique à vos domaine et serveur.

La ligne de suffixe nomme le domaine pour lequel le serveur LDAP fournira les informations. La ligne de suffixe devrait être changée depuis :

```
suffix          "dc=your-domain, dc=com"
```

il reflète votre nom de domaine. Par exemple :

```
suffix          "dc=acmewidgets, dc=com"
```

ou

```
suffix          "dc=acmeuniversity, dc=edu"
```

L'entrée `rootdn` est le nom de domaine pour un utilisateur non restreint par les paramètres de contrôle d'accès ou de limite administrative définis pour les opérations sur l'annuaire LDAP. On peut se représenter l'utilisateur rootdn comme l'utilisateur root pour l'annuaire LDAP. La ligne rootdn doit être modifiée de :

```
rootdn          "cn=root, dc=your-domain, dc=com"
```

en quelque chose comme :

```
rootdn          "cn=root, dc=redhat, dc=com"
```

ou

```
rootdn          "cn=ldapmanager, dc=my_organization, dc=org"
```

Modifiez la ligne rootpw de :

```
rootpw          secret
```

en quelque chose comme :

```
rootpw          {crypt}s4L9sOIJo4kBM
```

Dans l'exemple ci-dessus, vous utilisez un mot de passe root crypté, ce qui vaut beaucoup mieux que de laisser un mot de passe root en texte en clair dans le fichier `slapd.conf`. Vous pouvez utiliser Perl pour créer cette chaîne cryptée :

```
perl -e "print crypt('passwd','a_salt_string');"
```

Dans la ligne Perl précédente, `salt_string` est une chaîne salt de deux caractères, et `passwd` est la version en texte en clair du mot de passe.

Vous pourriez également copier une entrée `passwd` de `/etc/passwd`, mais ceci ne fonctionnera pas si l'entrée `passwd` est un mot de passe MD5 (valeur par défaut dans Red Hat Linux 7.1).

4.6.2 Le répertoire `schema`

Nouveauté de OpenLDAP version 2, le répertoire `schema` contient les différentes définitions LDAP, précédemment situées dans les fichiers `slapd.at.conf` et `slapd.oc.conf`. Toutes les **définitions de syntaxe d'attribut et les définitions de classe d'objets** se trouvent maintenant dans les différents fichiers schéma. Les différents fichiers schéma sont référencés dans `/etc/openldap/slapd.conf` en utilisant les lignes `include`, comme le montre l'exemple suivant :

```
include  /etc/openldap/schema/core.schema
include  /etc/openldap/schema/cosine.schema
include  /etc/openldap/schema/inetorgperson.schema
include  /etc/openldap/schema/nis.schema
include  /etc/openldap/schema/rfc822-MailMember.schema
include  /etc/openldap/schema/autofs.schema
include  /etc/openldap/schema/kerberosobject.schema
```

Ne modifiez aucun des éléments schéma définis dans les fichiers schéma installés par OpenLDAP.

Vous pouvez étendre le schéma utilisé par OpenLDAP pour prendre en charge des types d'attributs et classes d'objets supplémentaires, en utilisant comme guide les fichiers schéma de défaut. Pour ce faire, créez un fichier `local.schema` dans le répertoire `/etc/openldap/schema`. Référencez ce nouveau schéma dans `slapd.conf`, en ajoutant la ligne suivante sous vos lignes schéma de défaut :

```
include  /etc/openldap/schema/local.schema
```

Ensuite, définissez vos nouveaux types d'attributs et classes d'objets dans le fichier `local.schema`. De nombreuses organisations utilisent des types d'attributs et classes d'objets existants dans les fichiers schéma installés par défaut, et les modifient pour les utiliser dans le fichier `local.schema`. Ceci peut vous aider à apprendre la syntaxe de schéma tout en répondant aux besoins immédiats de votre organisation.

Ce chapitre a pour but de vous montrer comment étendre les schémas pour répondre à certaines nécessités spécifiques. Pour plus d'informations sur l'écriture de nouveaux fichiers schéma, consultez http://www.openldap.org/doc/admin/schema.html.

4.7 Démons et utilitaires OpenLDAP

Le paquetage OpenLDAP contient deux démons : `slapd` et `slurpd`.

Le démon `slapd` est le démon LDAP autonome que vous devez exécuter pour prendre en charge LDAP.

Le démon `slurpd` contrôle la duplication des annuaires LDAP sur un réseau. `Slurpd` envoie des modifications de l'annuaire LDAP maître aux annuaires LDAP esclaves. Vous ne devrez pas exécuter `slurpd` à moins d'avoir plusieurs serveurs LDAP connectés à votre réseau. Si vous avez deux serveurs LDAP ou plus, vous devrez exécuter `slurpd` pour préserver la synchronisation des annuaires LDAP.

OpenLDAP contient également certains utilitaires dans `/usr/bin` pour l'ajout, la modification et la suppression d'entrées dans un annuaire LDAP :

- `ldapmodify` — Modifie des entrées dans une base de données LDAP, acceptant la saisie via un fichier ou une saisie standard.
- `ldapadd` — Permet d'ajouter des entrées à votre annuaire, acceptant la saisie via un fichier ou une saisie standard ; `ldapadd` est en réalité un lien vers `ldapmodify -a`.
- `ldapsearch` — Recherche des entrées dans le répertoire LDAP à l'aide d'une invite shell.
- `ldapdelete` — Efface les entrées du répertoire LDAP, acceptant la saisie via un fichier ou une invite shell.

A l'exception de `ldapsearch`, chacun de ces utilitaires est plus facile à utiliser en référençant un fichier avec les changements à effectuer, qu'en tapant les commandes l'une après l'autre. Les pages du manuel consacrées à chacun d'eux comprennent la syntaxe de ces fichiers.

Pour importer ou exporter des blocs d'informations avec un répertoire `slapd` ou exécuter des tâches administratives similaires, plusieurs utilitaires, situés dans `/usr/sbin`, sont nécessaires :

- `slapadd` — Ajoute des entrées depuis un fichier LDIF ou un répertoire LDAP. Par exemple, exécuter `/usr/sbin/slapadd -l` *`ldif`* ou *`ldif`* est le nom du fichier LDIF contenant de nouvelles entrées.
- `slapcat` — Retire les entrées d'un répertoire LDAP et les sauvegarde dans un fichier LDIF. Par exemple, exécuter `/usr/sbin/slapcat -l` *`ldif`* où *`ldif`* est le nom du fichier cible qui contient les entrées du répertoire LDAP.
- `slapindex` — Réindexe la base données `slapd` basée sur le contenu de l'actuelle base de données. Exécuter `/usr/sbin/slapindex` pour commencer à réindexer.
- `slappasswd` — Génère une valeur de mot de passe utilisateur à utiliser avec `ldapmodify` ou une valeur `rootpw` dans `/etc/openldap/slapd.conf`. Exécuter `/usr/sbin/slappasswd` pour créer le mot de passe.

AVERTISSEMENT

Assurez-vous d'avoir arrêté `slapd` avant d'utiliser `slapadd`, `slapcat` ou `slapindex`. Sinon vous risquez d'endommager votre base de données LDAP.

Pour plus d'informations sur l'utilisation de ces outils, consultez les pages du manuel qui y sont consacrées.

4.8 Modules pour l'ajout de fonctionnalités à LDAP

Red Hat Linux contient les paquetages suivants, qui ajoutent des fonctionnalités à LDAP .

`nss_ldap` est un module LDAP pour **Solaris Nameservice Switch** (NSS). NSS est un ensemble d'extensions de bibliothèque C nécessaire pour accéder aux informations de l'annuaire LDAP au lieu de ou en plus du service de noms **Network Information Service** (NIS) et/ou des tableaux bidimensionnels. Le module `nss_ldap` est nécessaire pour utiliser LDAP comme serveur de noms natif.

Le module `pam_ldap` est nécessaire pour intégrer l'authentification LDAP dans l'API des modules d'authentification enfichables (PAM). Si vous utilisez `pam_ldap`, les utilisateurs peuvent authentifier et modifier leur mot de passe à l'aide d'annuaires LDAP. Les modules `nss_ldap` et `pam_ldap` sont fournis dans le paquetage `nss_ldap`.

Red Hat Linux comprend également des modules LDAP pour le serveur Web Apache. Le module `auth_ldap` est destiné à l'authentification de clients HTTP par rapport aux entrées utilisateur dans un annuaire LDAP. Le module `php-ldap` ajoute le support LDAP à PHP4, un langage de script encapsulé dans du HTML. Les modules `auth_ldap` et `php-ldap` doivent être compilés dans Apache comme **objets partagés dynamiques** (DSO).

4.9 HowTo de LDAP : présentation rapide

Cette section fournit une présentation rapide des opérations à accomplir pour faire fonctionner un annuaire LDAP.

1. Assurez-vous que le RPM `openldap` et tout autre RPM en rapport avec LDAP sont installés.
2. Reportez-vous soit au Quick Start Guide du site OpenLDAP (http://www.openldap.org/doc/admin/quickstart.html — commencez par "Create configuration file for slapd", du fait que les fichiers LDAP sont déjà installés), soit au Linux-LDAP HOWTO (http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html) pour obtenir des instructions concernant l'utilisation de LDAP sur votre système. L'un et l'autre couvrent le reste de ces étapes.

3. Editez le fichier `slapd.conf` pour l'adapter à votre système. (Pour obtenir plus d'informations sur l'édition de `slapd.conf`, consultez la Section 4.6.1, *Editer `/etc/openldap/slapd.conf`*.)
4. Lancez `slapd` en tapant `/etc/rc.d/init.d/ldap start`. (Après avoir correctement configuré LDAP, utilisez Linuxconf ou `ntsysv` pour configurer LDAP de façon à lancer le système.)
5. Créez votre annuaire LDAP (des exemples d'entrées LDAP figurent sur le site Web de PADL Software à l'adresse http://www.padl.com/ldap_examples.html).
6. Ajoutez des entrées à votre annuaire LDAP à l'aide de `ldapadd` ou d'un script.
7. Utilisez `ldapsearch` pour vérifier si `slapd` fonctionne.
8. A ce stade, votre annuaire LDAP devrait exister. L'étape suivante consiste à configurer vos applications compatibles LDAP de manière à ce qu'elles puissent utiliser l'annuaire LDAP.

4.10 Configuration de votre système pour l'authentification à l'aide de OpenLDAP

Cette section donne un bref aperçu de la manière de configurer votre système Red Hat Linux pour l'authentification à l'aide de OpenLDAP. A moins que vous ne soyez un expert de OpenLDAP, vous aurez probablement besoin de plus de documentation que vous n'en trouverez ici. Reportez-vous aux références de la Section 4.11, *Autres ressources* pour plus d'informations.

4.10.1 Installez les paquetages LDAP nécessaires

Tout d'abord, assurez-vous que les paquetages appropriés sont installés tant sur le serveur LDAP que sur les ordinateurs clients LDAP. Le serveur LDAP a besoin du paquetage `openldap`.

Les ordinateurs clients LDAP ont besoin des paquetages suivants : `openldap`, `auth_ldap`, et `nss_ldap`.

4.10.2 Editez les fichiers de configuration

Editer `/etc/openldap/slapd.conf`

Editez le fichier `slapd.conf` pour vous assurer qu'il correspond aux besoins spécifiques de votre organisation.

Pour obtenir des informations sur l'édition de `slapd.conf`, consultez Section 4.6.1, *Editer `/etc/openldap/slapd.conf`*.

Editer `ldap.conf`

Editez les fichiers `ldap.conf` dans `/etc` et dans `/etc/openldap` sur le serveur LDAP et les clients.

Editez `/etc/ldap.conf`, le fichier de configuration pour `nss_ldap` et `pam_ldap`, pour refléter votre organisation et votre base de recherche. Le fichier `/etc/openldap/ldap.conf` est le fichier de configuration pour les outils de la ligne de commande comme `ldapsearch`, `ldapadd`, etc. ; il devra aussi être édité pour le paramétrage de votre LDAP. Les ordinateurs clients auront besoin de ces deux fichiers modifiés.

Editer `/etc/nsswitch.conf`

Pour utiliser `nss_ldap`, vous devrez ajouter `ldap` dans les champs appropriés dans `/etc/nsswitch.conf`. (Soyez attentifs lorsque vous éditez ce fichier, soyez sûrs de ce que vous faites.) Par exemple :

```
passwd: files ldap
shadow: files ldap
group: files ldap
```

PAM et LDAP

Pour faire en sorte que des applications compatibles avec PAM standard utilisent LDAP pour l'authentification, exécutez `authconfig` et sélectionnez **Use LDAP** (la technologie PAM dépasse la portée de cette présentation du protocole LDAP ; dès lors, si vous avez besoin d'aide, consultez Chapitre 8, *Modules d'authentification enfichables (PAM)* et/ou les pages de manuel sur PAM).

4.10.3 Faites migrer vos anciennes informations d'authentification vers le format LDAP

Le répertoire `/usr/share/openldap/migration` contient un ensemble de scripts shell et Perl pour la migration de vos anciennes informations d'authentification vers le format LDAP (Perl doit naturellement être installé sur votre système pour que vous puissiez utiliser ces scripts).

Tout d'abord, modifiez le fichier `migrate_common.ph` de manière à ce qu'il reflète votre domaine. Le domaine DNS par défaut devrait être changé de :

```
$DEFAULT_MAIL_DOMAIN = "padl.com";
```

en quelque chose comme :

```
$DEFAULT_MAIL_DOMAIN = "votre_société.com";
```

La base par défaut devrait également être changée de :

```
$DEFAULT_BASE = "dc=padl,dc=com";
```

en quelque chose comme :

```
$DEFAULT_BASE = "dc=votre_société,dc=com";
```

Ensuite, vous devez choisir le script à utiliser. Le tableau ci-dessous vous y aidera :

Table 4–1 Scripts de migration LDAP

Service de noms existant	LDAP fonctionne-t-il ?	Utilisez ce script :
`/etc` tableaux bidimensionnels	oui	`migrate_all_online.sh`
`/etc` tableaux bidimensionnels	non	`migrate_all_offline.sh`
NetInfo	oui	`migrate_all_netinfo_online.sh`
NetInfo	non	`migrate_all_netinfo_offline.sh`
NIS (YP)	oui	`migrate_all_nis_online.sh`
NIS (YP)	non	`migrate_all_nis_offline.sh`

Exécutez le script approprié en fonction de votre service de noms existant.

Les fichiers `README` et `migration-tools.txt` du répertoire `/usr/share/openldap/migration` fournissent plus de détails sur la migration d'informations.

4.11 Autres ressources

Vous pouvez trouver sur le Web de nombreuses informations utiles sur LDAP. Consultez ces sources, en particulier le site Web OpenLDAP et le HOWTO LDAP, avant de commencer à configurer LDAP sur votre système.

4.11.1 Documentation installée

- La page du manuel `ldap` constitue un bon point de départ pour commencer à connaître LDAP. Vous trouverez aussi des pages du manuel consacrées aux démons et utilitaires de LDAP. Si vous avez besoin de plus d'informations, consultez les pages `ldapmodify`, `ldapsearch`, et semblables.

- `/usr/share/doc/openldap-`*`version`* — Contient un document `README` général et des informations variées.

4.11.2 Sites web utiles

- http://www.openldap.org — Accueil du projet OpenLDAP, l'effort collectif pour développer une "suite LDAP d'applications et d'outils de développement robuste, attractive du point de vue commercial, offrant de bonnes fonctionnalités et libre."
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — document HOWTO LDAP Linux, parcourant l'installation de l'authentification à la connexion.
- http://www.padl.com — Outils de développement de `nss_ldap` et `pam_ldap`, entre autres outils LDAP utiles.
- http://www.innosoft.com/ldapworld — Contient des informations concernant LDAP RFCs et des précisions sur la version 3 de LDAP.
- http://www.kingsmountain.com/ldapRoadmap.shtml — La Road Map de Jeff Hodges contient des liens vers différentes FAQ et des nouvelles importantes concernant le protocole LDAP.
- http://www.rudedog.org/auth_ldap — L'accueil du module d'authentification `auth_ldap` pour Apache.
- http://www.stanford.edu/~bbense/Inst.html — Discute l'utilisation de LDAP avec Sendmail.
- http://www.webtechniques.com/archives/2000/05/wilcox — Un regard utile sur les groupes de gestion LDAP.
- http://www.ldapman.org/articles — Articles offrant une bonne introduction à LDAP, ainsi que des méthodes de création d'arborescence de répertoires et des structures de répertoire de personnalisation.

4.11.3 Livres sur le thème

- *Implementing LDAP* de Mark Wilcox, édité par Wrox Press, Inc.
- *Understanding and Deploying LDAP Directory Services* de Tim Howes, édité par Macmillan Technical Publishing

5 Eléments de base de CCVS (Credit Card Verification System)

Le système CCVS utilise votre ordinateur et un modem pour simuler un terminal de lecture de carte de crédit (également **POS** - Point of Sale terminal, terminal de point de vente).

CCVS est sûr, sécurisé et facile à utiliser. Ecrit en C ANSI et conforme aux normes POSIX, CCVS est portable et conçu pour être aisément intégré à des systèmes d'exploitation modernes, des langages de programmation et des applications Internet. Conçu pour faciliter l'écriture de scripts et la programmation, CCVS peut être utilisé pour automatiser des traitements par lots ou améliorer des applications nécessitant un traitement de cartes de crédit.

CCVS peut être utilisé ailleurs qu'aux Etats-Unis si le représentant de vos services bancaires ou commerçant peut prendre en charge l'un des protocoles compatibles avec CCVS. Si vous êtes situé au Canada, CCVS prend en charge le protocole NDC, pouvant être utilisé par n'importe quelle banque au Canada. Si vous vous trouvez ailleurs qu'aux Etats-Unis ou au Canada, consultez le représentant de vos services de commerce. Le protocole pris en charge par CCVS qui a le plus de chances d'être pris en charge par une institution financière en dehors des Etats-Unis est le protocole Visa 2nd Generation "K Format" (VITAL).

5.1 Utilisation de CCVS

CCVS fournit des liens entre une application de e-commerce et une passerelle de paiement par carte de crédit. Si le mode d'utilisation de CCVS dépend du protocole qu'utilise votre passerelle de paiement, dans de nombreux cas CCVS peut être utilisé en n'apportant que peu de modifications au système existant. Pour des informations plus détaillées sur les différents protocoles pris en charge par CCVS, reportez-vous à l'adresse http://www.redhat.com/products/software/ecommerce/ccvs/support/docs/protocol-specific.html.

Voici des exemples d'utilisation de CCVS :

- CCVS peut, par exemple, être utilisé dans un système pour téléopératrices prenant des commandes sur catalogue. Les extensions Tcl de CCVS permettent de créer une interface utilisateur graphique Tcl/Tk simple pour les téléopératrices. Celles-ci peuvent alors utiliser de simples terminaux X Window ; tous les logiciels fonctionneront sur le serveur central. Il suffit d'installer CCVS sur un ordinateur ; les opératrices ne doivent pas attendre qu'une ligne se libère — toutes leurs transactions passent par le même appel téléphonique.
- CCVS peut être utilisé pour faciliter la facturation automatique. Par exemple, un fournisseur d'accès Internet peut avoir une base de données de sa clientèle stockée sur un serveur de base de données. L'administrateur de base de données du fournisseur d'accès pourrait écrire un script Perl,

combinant le module Perl CCVS avec un module pour le système de base de données. Ce script pourrait ensuite être exécuté mensuellement. Le script lira les données client, traitera la facturation mensuellement et mettra à jour les enregistrements de la base de données pour indiquer qu'un paiement a eu lieu.

- CCVS peut être utilisé pour effectuer les processus de paiement pour une boutique sur le Web qui utilise un centre téléphonique pour gérer les commandes par téléphone. Les commandes sont ainsi acheminées à travers le Web par le moyen d'une application CGI standard ou par un agent de vente utilisant un programme Java personnalisé fonctionnant sur LAN, et peuvent utiliser la même connexion pour l'acheminement et le paiement. De plus, les fonctionnalités de l'Address Verification System, système de vérification des adresses (AVS) de CCVS peuvent être utilisées pour prévenir la fraude dans les deux méthodes de commande, sans avoir le souci d'implémenter cette fonctionnalité séparément pour chaque application, ce qui permet de gagner du temps sur le développement.

Ce ne sont là que quelques exemples des fonctions de CCVS. CCVS permet d'améliorer n'importe quel aspect des opérations nécessitant un traitement de carte de crédit. Parmi les nombreuses fonctions de CCVS figurent les suivantes :

- Bibliothèque en langage C avec une API documentée permettant aux utilisateurs d'intégrer CCVS sans problème à des applications existantes.
- Une extension Tcl permet d'utiliser CCVS avec un système Tcl côté serveur tel que NeoWebScript.
- Un module Perl 5.0 permet à CCVS de fonctionner avec le langage de programmation CGI le plus utilisé actuellement.
- Il est possible de créer rapidement des interfaces graphiques personnalisées à l'aide de Tcl/Tk — le temps de développement est généralement inférieur à un jour.
- Les modules Python, PHP3 et Java permettent à CCVS de fonctionner avec d'autres langages de programmation courants.
- Programmes CLI (Command Line Interface, interface de ligne de commande) pour une utilisation interactive. Appelez des programmes à partir de tout shell UNIX et programmes dans votre langage UNIX favori.
- Protection contre la fraude AVS permettant aux commerçants de vérifier si les cartes de crédit n'ont pas été volées. De nombreuses chambres de compensation offrent de meilleurs taux aux commerçants utilisant AVS, même pour des commandes prises au téléphone.
- Prise en charge de plusieurs comptes commerçants, permettant aux utilisateurs d'ouvrir leur propre centre commercial virtuel comprenant un nombre illimité de vitrines de magasin. Un **compte commerçant** est un type de compte bancaire particulier permettant à une entreprise d'accepter de ses

clients des paiements par carte de crédit ; le compte commerçant retient le déroulement des transactions de carte de crédit.

- Capacité d'exécuter plusieurs transactions au cours d'une seule session, approchant les performances de lignes louées (deux secondes par transaction !) sans coût supplémentaire ni complexité insurmontable.
- Réconfort d'être en mesure de tester et d'effectuer la programmation de développement sur le produit sans devoir prélever des montants sur des cartes de crédit réelles.

5.2 Processus de vérification de carte de crédit

Comment ce petit bout de plastique indique-t-il que vous pouvez réellement vous offrir ce téléviseur grand écran ?

Tout d'abord, le consommateur présente ses informations de carte de crédit au commerçant. Ce dernier transmet ces données, en même temps que son code d'identification commerçant, à une chambre de compensation. La chambre de compensation peut être la banque ayant ouvert le compte de carte de crédit du commerçant ; il s'agit cependant le plus souvent d'une société ayant conclu un contrat avec la banque du commerçant pour compenser le montant en échange de frais fixes, additionnés d'un pourcentage sur chaque montant traité.

Les données sont transmises par une lecture de la carte et des références du commerçant par téléphone, à l'aide d'un terminal POS pour carte de crédit, ou bien en utilisant CCVS ou un autre composant logiciel pour transmettre les informations par ordinateur.

La chambre de compensation contacte la banque ayant émis la carte de crédit du consommateur et vérifie si le montant chargé est acceptable. S'il est accepté, la Chambre de compensation envoie un message de confirmation au commerçant. Au même moment, le crédit disponible sur carte de crédit du client est gelé à concurrence du montant de transaction.

A la fin de la journée de travail, le commerçant (en réalité, son ordinateur ou le terminal de carte de crédit) appelle la chambre de compensation et vérifie toutes les transactions de la journée pour s'assurer que le système du commerçant et la chambre de compensation sont d'accord sur les transactions effectuées pendant la journée. Une fois que le commerçant et la chambre de compensation sont d'accord sur les transactions du jour, la chambre de compensation entame le processus de transfert de l'argent de la banque émettrice de la carte de crédit sur le compte bancaire du commerçant.

5.3 Ce qu'il vous faut pour utiliser CCVS

Pour utiliser CCVS, il vous faut un modem et un compte commerçant. Vous devez également appliquer quelques instructions afin que CCVS fonctionne correctement.

5.3.1 Modems

Il vous faut au moins un modem dédié à l'utilisation de CCVS. Les protocoles de carte de crédit ne prenant pas en charge les fonctions de compression ou de correction d'erreur durant la connexion du modem, il n'est pas possible de les utiliser. Nous pouvons vous communiquer des informations sur la manière de désactiver de telles fonctions sur les modems suivants :

- Hayes Optima
- US Robotics Courier
- US Robotics Sportster
- Chase Research PCI-RAS

Remarque

Utilisez un ou plusieurs modems de la liste ci-dessus !

Si vous utilisez un modem non pris en charge (autre que les quatre modems précités), vous aurez peut-être des difficultés à le faire fonctionner avec CCVS. Consultez également les listes de compatibilité matérielle de Red Hat Linux à l'adresse http://hardware.redhat.com pour vous assurer que votre modem fonctionnera avec Red Hat Linux.

Si le modem que vous voulez utiliser ne figure pas dans cette liste, consultez le manuel du modem pour rechercher la chaîne permettant de désactiver la compression et la correction d'erreur, de même que celle permettant de réinitialiser le modem pour une utilisation normale. Vous devrez fournir ces deux chaînes lors de la configuration de CCVS.

5.3.2 Comptes commerçants

Si vous configurez juste un compte commerçant ou si vous modifiez un compte commerçant existant pour utiliser CCVS, il est possible que votre fournisseur de compte commerçant y voie une preuve que CCVS peut fonctionner avec le protocole qu'il utilise. Des lettres de spécification pour des protocoles spécifiques sont disponibles à l'adresse http://www.redhat.com/products/software/ecommerce/ccvs/support/certifications.html. Imprimez toutes les pages de la lettre correspondant au protocole que vous allez utiliser et montrez-les à votre fournisseur de compte commerçant.

Votre fournisseur de compte commerçant doit utiliser l'un des protocoles pris en charge par CCVS :

- le protocole ETC PLUS de First Data Corporation (également appelé FDR7, ETC+, ETC7, Omaha)
- le protocole South Platform de First Data Corporation (également appelé "Nabanco")

- le protocole MAPP de Global Payment Systems (également appelé "St. Louis")
- le protocole NDC de Global Payment Systems (également appelé "Atlanta")
- le protocole VITAL de Visa International (également appelé VisaNet, Visa 2nd generation, "K format")
- le protocole UTF de Paymentech (également appelé GENSAR)
- le protocole NOVA Information Systems

Si votre fournisseur de compte commerçant accepte l'un de ces protocoles, vous pourrez utiliser CCVS.

Après avoir identifié le protocole que vous allez utiliser, consultez les informations le concernant à l'adresse http://www.redhat.com/products/software/ecommerce/ccvs/support/docs/protocol-specific.html avant d'entamer le processus de configuration de CCVS. Le *CCVS Protocol Guide*, accessible à l'adresse mentionnée, décrit les fonctionnalités prises en charge par les divers protocoles.

5.3.3 Instructions relatives à l'utilisation de CCVS sur votre système

Les exigences suivantes permettent de faire fonctionner CCVS sans problème et efficacement. Veillez à appliquer toutes ces instructions avant d'essayer d'utiliser CCVS.

Utilisation exclusive des modems pendant l'exécution de CCVS

N'exécutez pas d'autres applications logicielles susceptibles d'accéder au modem pendant que vous exécutez CCVS ; elles risquent d'interférer avec le fonctionnement de CCVS en empêchant le modem de fonctionner et les chiffres des cartes de crédit d'être traités.

Permissions, privilèges et accès au modem

La plupart des autorisations nécessaires pour CCVS sont configurées pour vous durant le processus d'installation par la création d'un groupe spécial nommé "ccvs". Il y a toutefois certains problèmes impliquant des autorisations système dont il faut être conscient. Cette section traite de toutes ces questions.

Toutes les opérations relatives à une configuration particulière de CCVS doivent être effectuées depuis un seul compte utilisateur. Un seul compte est requis, de sorte que toutes les propriétés et autorisations relatives au fichier soient correctement définies et protégées. Ce compte utilisateur doit être ajouté au groupe ccvs (par vous ou votre administrateur système) avant d'exécuter le programme de configuration.

Une fois que l'utilisateur a été ajouté au groupe ccvs, exécutez le programme de configuration de CCVS (`ccvs_configure`) sous l'identité de cet utilisateur. Après avoir exécuté le programme de configuration, ce même utilisateur doit exécuter les commandes de CCVS pour cette configuration.

Si vous voulez que CCVS fonctionne avec un modem, les utilisateurs du groupe ccvs doivent également être ajoutés au groupe uucp. Il se peut que l'adhésion au groupe ne soit pas suffisante pour pouvoir utiliser les modems ; dans ce cas, vérifiez que les membres du groupe CCVS ont eux-aussi accès au port série des modems que CCVS doit utiliser.

Si vous utilisez PHP avec CCVS, vous devrez activer le serveur Web pour exécuter des commandes CCVS. Pour ce faire, vous devrez faire de l'utilisateur du serveur Web un membre du groupe ccvs. Habituellement, l'utilisateur du serveur Web devra également être membre du groupe uucp.

Si vous n'utilisez pas PHP mais souhaitez que votre serveur Web soit capable d'exécuter CCVS, vous avez à votre disposition d'autres options (par exemple, `suexec`, `setuid`) que de faire de l'utilisateur du serveur Web un membre du groupe ccvs. Vous pouvez le configurer à votre guise, à moins que vous n'utilisiez PHP.

Versions du logiciel

CCVS requiert Tcl, version 7.6 ou postérieure, pour exécuter l'interface graphique incluse ou pour utiliser les API Tcl/Tk incluses afin de développer votre propre frontal graphique. Tcl version 8.3 est inclus dans Red Hat Linux 7.1.

CCVS requiert Perl, version 5.0 ou postérieure pour utiliser les API Perl incluses. Perl version 5.6 est également inclus dans Red Hat Linux 7.1.

5.4 Installation de CCVS

Les RPM de CCVS sont disponibles sur le CD-ROM Linux Applications Library Workstation.

Vous pouvez utiliser RPM, Gnome-RPM ou Kpackage pour installer les paquetages CCVS :

- `CCVS` — Programmes principaux de CCVS
- `CCVS-devel` — Kit de développement C
- `CCVS-perl` — Interface Perl pour CCVS
- `CCVS-python` — Interface Python pour CCVS
- `CCVS-php3` — Interface PHP3 pour CCVS
- `CCVS-tcl` — Interface Tcl pour CCVS
- `CCVS-java` — Interface Java pour CCVS (incluse comme code source)
- `CCVS-examples` — Echantillon de code source, nécessaire pour le développement

5.5 Avant de configurer CCVS

Avant de configurer CCVS, vous devez être en mesure de répondre à certaines questions sur votre système et sur la manière dont vous voulez le faire. Pour préparer le processus de configuration, procédez comme suit :

1. Lisez l'ensemble de la documentation et des errata fournis avec le programme. Consultez la Section 5.11, *Autres resources* pour trouver l'emplacement de la documentation concernant CCVS installée et en ligne.

2. Complétez `setup.txt`. Le fichier `setup.txt` est un document expliquant les diverses informations nécessaires lors de la configuration de CCVS en vue de l'utilisation de protocoles particuliers. Si vous complétez `setup.txt`, vous disposerez de toutes les informations nécessaires pour le processus de configuration à votre disposition. Elles figurent dans le répertoire `/usr/share/doc/CCVS-<version>`. Le fichier `setup.txt` est également disponible à l'adresse http://www.redhat.com/products/software/ecommerce/ccvs/support/docs/setup.txt.

Remarque

Dans le fichier de configuration, vous êtes invité à entrer des informations spécifiques au protocole. Vous devez uniquement fournir des informations pour le protocole que vous allez utiliser. Il est inutile de compléter les informations pour les autres protocoles.

---

3. Le programme d'installation de CCVS vous posera plusieurs questions sur votre modem ; munissez-vous des informations appropriées. Actuellement, CCVS ne fournit de la documentation que sur les chaînes init des modems suivants :

Hayes Optima ou ACCURA

```
\r~~~\rAT &D3 X4 E0 &K0 &Q0
```

U.S. Robotics Sportster ou Courier

```
\r~~~\rAT E0 L0 M1 V1 X4 &K0 &M0 +FCLASS=0
```

Chase Research PCI-RAS

```
\r~~~\rAT E0 %C0 \\N0
```

Si vous utilisez l'un des modems pris en charge, le programme de configuration vous demandera uniquement de confirmer la chaîne init. Si votre modem ne figure pas dans cette liste, parcourez son manuel pour trouver la chaîne qui désactive toutes les fonctions de compression et de correction d'erreur, de même que la chaîne qui réinitialise votre modem pour une utilisation normale. Vous devrez définir ces deux chaînes de modem durant le processus de configuration.

5.6 Configuration de CCVS

Vous devez configurer CCVS pour votre système, soit en mode de démonstration, soit pour le traitement de données réelles.

Utilisez la commande `su` pour basculer vers le compte utilisateur que vous avez créé (un membre du groupe ccvs) pour cette configuration.

Exécutez le programme de configuration de CCVS avec la commande suivante :

```
/usr/sbin/ccvs_configure
```

Le reste de cette section vous mènera à travers le programme de configuration de CCVS. Le système devrait afficher une fenêtre d'accueil. Appuyez sur [Entrée] pour lire la licence du logiciel CCVS. Vous pouvez utiliser les commandes de défilement et de pagination standard de `more` (ou le programme de pagination défini par votre variable d'environnement $PAGER) pour lire la licence.

Après avoir lu la licence et quitté le pager, vous verrez s'afficher le message :

```
Type "accept" to accept this license, or anything else to exit.
```

Tapez **`accept`** pour accepter les termes de la licence et continuer la configuration de CCVS. Toute autre commande vous permettra de sortir du programme.

L'écran suivant apparaîtra :

```
This program creates the configuration file for CCVS functions.
To do this, you will require the following information:
 1: The clearing protocol you will be using. This may be MAPP,
ETC+, or any of the other protocols which CCVS supports. There
is also a demo protocol; if you have downloaded the free demo of
CCVS, you will be using the demo protocol.
 2: The unique number which identifies you to the clearing
house. This may be your merchant account number or a terminal id
number, depending on what protocol you will be using. This number
will be supplied when you set up your merchant account.
 3: Your modem type, and the serial port your modem is attached
to. You will also need modem configuration strings. (We can
supply modem configuration strings for many popular modems.)
 4: The location of your data directory. This is where the
configuration file and data directories will be placed.
 5: Other information as needed for particular protocols. This
information will generally be supplied when you set up your
merchant account.

We supply a worksheet which you can use to organize all this
information, including the details for each protocol. See the
```

```
file "setup.txt" in /usr/share/doc/CCVS-<version>.

The configuration program is running as user "<username>".
It is important that this be the same user which the actual CCVS
software will run as. (We recommend creating a special user
account for just this purpose.)

Do you wish to continue configuring CCVS as user "<username>"?

[Enter Y to continue, or N to stop here:]
```

Appuyez sur [Y] pour continuer. Si vous exécutez `ccvs_configure` en tant que root, l'erreur suivante apparaîtra. Dans ce cas, tapez `su` dans l'utilisateur CCVS, comme utilisateur ccvs par défaut, et ré-exécutez `ccvs_configure`.

```
The configuration program may not be run as root. You must run
this as the same user which the actual CCVS software will run as.
(We recommend creating a special user account for just this
purpose.)
```

Lorsque vous continuez, le programme vous affichera des invites demandant des informations. Vous pouvez revenir à une invite précédente à n'importe quel moment en tapant `.` (un point) tout seul et en pressant [Entrée].

```
Do you want to configure CCVS for the free demo, or a working
merchant account? (If you have not purchased a license for CCVS,
only the demo configuration is available.)

[Enter Y to use the demo configuration, N for a real configuration,
or . to exit:]
```

A moins d'avoir acheté une clé logicielle et une licence pour CCVS, entrez [Y]. Cela installe une configuration de démonstration, qui n'appelle pas le modem ou n'utilise pas de compte commerçant réel. Si vous avez acheté une licence et êtes prêt à installer une configuration opérationnelle, entrez [N].

```
Where do you want to place the CCVS configuration files and
transaction queues? This should be a directory name which is
writable by the current user.
The default is "/var/ccvs".
Enter directory, or Return for default value, or . by itself to
back up.
>
```

A moins d'avoir des raisons spécifiques pour déplacer les fichiers de configuration CCVS et les files d'attente de transaction, laissez-les à leurs emplacements par défaut. Si vous devez les déplacer, songez que vous devrez également définir une variable d'environnement.

```
What do you want to name this configuration? This should be a
short filename.
The default is "ccvs".
Enter name, or Return for default value, or . by itself to back
up.
>
```

Par exemple, vous pourriez avoir une configuration appelée **`tshirt`** pour un commerçant vendant des T-shirts, et une autre appelée **`music`** pour un vendeur de partitions musicales. Le nom entré ici est celui utilisé pour opérer une distinction entre les deux configurations.

La version de démonstration de CCVS ne requiert pas d'autre information ; si vous l'avez choisie, vous allez voir immédiatement :

```
Writing "/var/ccvs/ccvs.conf"...

The CCVS system is now configured.
```

Vous pouvez à présent commencer à tester le logiciel de démonstration. La démo agit exactement comme le logiciel CCVS complet, sinon qu'elle n'appelle pas le modem ni ne communique avec un processeur commerçant réel.

Si vous avez une licence pour la version complète de CCVS et avez choisi d'installer une configuration réelle, vous verrez s'afficher à la place quelque chose comme ceci :

```
Which protocol and merchant processor will you be using?

Credit card clearing protocols:
  1: ETC PLUS (FDR7/ETC7/FDR "Omaha"): First Data Corporation
  2: South Platform (FDR "Nabanco"): First Data Corporation
  3: MAPP: Global Payment Systems "St. Louis"
  4: NDC: Global Payment Systems "Atlanta" / NDC
  5: VITAL (Visa 2nd generation, K format): Visa/Total System Services
  6: UTF: Paymentech Inc.
  7: NOVA: NOVA Information Systems

[Enter a number, or . by itself to back up:]
```

Sélectionnez le protocole pour lequel vous avez une licence CCVS et un compte commerçant valide.

```
What is the number of your merchant account?
Enter number, or . by itself to back up.
>
```

Ce chiffre doit être fourni avec votre compte commerçant.

```
What is your CCVS software customer number?
Enter number, or . by itself to back up.
>
```

Ce numéro est fourni avec votre licence CCVS.

```
What is your CCVS software license key?
Enter number, or . by itself to back up.
>
```

Ce numéro aura également été fourni avec votre licence CCVS.

```
What is the phone number of your merchant processor?
Enter number, or . by itself to back up.
>
```

Des questions supplémentaires peuvent également se poser du fait qu'elles sont requises par des protocoles particuliers. Si vous avez complété, dans la feuille de travail `setup.txt`, la section relative à votre protocole, vous devriez être prêt à répondre à ces questions. Par exemple, VITAL poursuit avec quelques invites supplémentaires concernant votre nom commercial, votre adresse, votre banque, etc. Vous devriez déjà avoir trouvé ces informations lors de la création de votre compte commerçant VITAL. C'est là l'objectif du fichier feuille de travail `setup.txt` que vous devriez avoir complété avant de lancer le programme de configuration CCVS. Pour plus d'informations concernant l'utilisation de `setup.txt`, consultez la Section 5.5, *Avant de configurer CCVS*.

Vous devez à présent entrer des informations sur la manière de communiquer avec votre modem. Les informations de configuration du modem sont très importantes. Veillez à entrer des informations correctes pour la configuration de votre système ; CCVS ne fonctionnera pas si le modem est incorrectement configuré.

```
Do you want to configure a pool of several modems? (If you answer
yes, all the modems must be exactly the same make and model. If
you want to use just one modem, answer no.)

[Enter Y or N, or . to back up:]
```

Si vous avez plusieurs modems identiques, vous pouvez configurer CCVS pour qu'il les utilise tous, comme un groupe. Chaque processus CCVS nécessitant un modem utilisera l'un de ceux du groupe, à supposer que l'un d'entre eux soit disponible. Plusieurs configurations de CCVS peuvent ainsi partager un ensemble de modems. Vous pouvez également déterminer une configuration simple avec deux modems, de façon à ce que les autorisations et le traitement par lots puissent se produire en même temps.

```
What serial port is your modem connected to? (Do not include the
"/dev/" prefix.) The default is ttyS0. The modem should be
```

```
connected and ready now, so that the serial port can be tested.

Enter port name, or Return for default value, or . by itself to
back up.
>
```

Le programme teste le port série que vous entrez ; si vous en configurez plusieurs, il teste chacun d'eux. N'incluez pas le préfixe `/dev/`. Cette étape peut prendre jusqu'à trente secondes si le modem ne répond pas.

```
What type of modem do you have? This information makes it
possible to suggest modem configuration strings. If your modem
is not listed, you can choose "none of the above"; but you will
then have to create your own configuration strings, which is a
difficult process.

 1: USR Sportster/Courier
 2: Hayes Optima
 3: Chase Research PCI-RAS
 4: None of the above

[Enter a number, or . by itself to back up:]
```

Vous serez invité à entrer les chaînes d'initialisation, de numérotation et de raccrochage du modem (si vous configurez un groupe de modems, ils doivent être tous identiques, de manière à ce qu'ils utilisent tous les mêmes chaînes). Si CCVS connaît les chaînes appropriées pour votre modem, elles sont suggérées et vous pouvez simplement appuyer sur [Entrée].

```
The modem initialization string should set the modem to do no
protocol
negotiation. What string do you want to use?
A string which works for your modem is:
 \r~~~\rAT E0 L0 M1 V1 X4 &K0 &M0 +FCLASS=0
Enter string, or Return for suggested value.
>

The modem dial string should dial the modem. (Do not include a
phone number.)
What string do you want to use?
A string which works for your modem is:
 ATDT
Enter string, or Return for suggested value.
>

The modem hang-up string should hang the modem up if it's
connected. What string do you want to use?
```

```
A string which works for your modem is:
 ~~~+++~~~~~~~~~~\rATH0\r~~~
Enter string, or Return for suggested value.
>

Initialize: \r~~~\rAT E0 L0 M1 V1 X4 &K0 &M0 +FCLASS=0
Dial: ATDT
Hang up: ~~~+++~~~~~~~~~~\rATH0\r~~~
Are these the values you want?

[Enter Y to accept, N to change, . to back up.]
```

Vous ne verrez peut-être pas exactement le même écran que celui illustré ci-dessous du fait que les valeurs par défaut suggérées varieront en fonction du modem sélectionné.

La question suivante a trait à la vitesse :

```
What baud rate do you want to use? You should use the
default unless you have explicit information that another
value is appropriate.
The default baud rate is 1200.

Enter rate, or Return for default value, or . by itself to
back up.
>
```

Lorsque vous aurez terminé d'entrer les informations de configuration, vous verrez :

```
Writing "/var/ccvs/ccvs.conf"...

The CCVS system is now configured.
```

5.7 Comptes commerçants multiples

Si vous devez prendre en charge plus de comptes commerçants, suivez de nouveau simplement la procédure de configuration. Utilisez un autre nom de configuration pour chaque compte commerçant.

Différentes configurations peuvent partager le même port série ou le même groupe de ports série. Les modems seront utilisés dans l'ordre d'arrivée.

5.8 Démarrage de CCVS

Pour exécuter CCVS pour une application particulière, vous devez être connecté par une commande `su` au compte ayant créé cette configuration. Si vous utilisez un compte utilisateur ccvs dans ce but et que vous êtes déjà connecté au système en tant qu'autre utilisateur, tapez `su ccvs` pour passer au bon utilisateur.

En tant qu'utilisateur du compte, pour exécuter CCVS, vous devez démarrer le démon `ccvsd` pour chaque compte commerçant. De plus, vous devrez exécuter le programme `cvupload` sur une base régulière. En utilisant `cron` pour exécuter `cvupload`, vous accomplirez cette tâche tous les jours. Pour plus d'informations concernant les processus d'automatisation, reportez-vous aux pages `cron` du manuel.

5.8.1 Le démon ccvsd

Pour exécuter CCVS, vous devez exécuter le démon `ccvsd`. Le démon `ccvsd` établit en réalité les appels téléphoniques et conduit les transactions. La commande `ccvsd` doit être suivie par le nom du compte que vous avez spécifié lors de la configuration du compte.

Par exemple, si vous voulez démarrer le traitement des transactions pour le revendeur de partitions musicales mentionné durant le programme de configuration, et si vous avez installé le logiciel à son emplacement par défaut `/usr/sbin`, entrez la commande suivante pour lancer `ccvsd`:

```
/usr/sbin/ccvsd music
```

Chaque fois que vous ajoutez un compte commerçant, vous devez lancer `ccvsd` pour ce compte, si vous voulez traiter des transactions pour ce compte.

Pour plus d'informations sur `ccvsd`, reportez-vous à la page de manuel `ccvsd`.

5.8.2 Commande cvupload

Certaines transactions (telles les autorisations) interviennent au moment où la carte de crédit est présentée. D'autres transactions (telles les ventes et les retours) sont enregistrées et ne sont pas traitées immédiatement. Ces transactions sont réparties par lots, puis traitées en groupe.

CCVS utilise le programme `cvupload` pour exécuter ce traitement par lots. Nous vous recommandons d'appeler `cvupload` comme tâche `cron` (au moins) quotidienne, de sorte que `cvupload` s'exécute automatiquement chaque jour, sans intervention de votre part.

Par exemple, pour effectuer le traitement périodique pour le vendeur de partitions musicales, il faut entrer la commande suivante :

```
/usr/sbin/cvupload music
```

Pour plus d'informations sur `cvupload`, reportez-vous à la page de manuel `cvupload`.

5.9 Considérations sur des langages de programmation spécifiques

- C — La bibliothèque C de CCVS est incluse dans le paquetage `CCVS-devel` . Lors de la compilation de programmes en langage C utilisant CCVS, ajoutez l'option `-lccvs` sur la ligne du lien.
- Java — Consultez la page http://www.redhat.com/products/software/ecommerce/ccvs/support/docs/AdminJava.html pour plus d'informations sur la conception de l'interface Java de CCVS. Le code source pour l'interface Java est compris dans le paquetage `CCVS-java`.
- Perl — L'interface Perl est fournie dans le paquetage `CCVS-perl`.
- Python — L'interface Python est fournie dans le paquetage `CCVS-python`.
- PHP — Le paquetage `CCVS-php3` fournit l'interface PHP3.
- Tcl — L'interface Tcl est incluse dans le paquetage `CCVS-tcl`.

5.10 Assistance pour CCVS

Il est possible d'acheter l'assistance pour CCVS auprès de Red Hat. Lorsque vous achetez une clé pour activer CCVS, veillez à passer en revue les options d'assistance disponibles. Consultez la page http://www.redhat.com/products/software/ecommerce/ccvs pour plus d'informations sur l'achat d'une clé et d'options d'assistance CCVS.

Si vous avez besoin d'assistance, veillez à réunir les informations suivantes avant de contacter les services d'assistance :

- Nom de votre société
- Version de CCVS que vous utilisez
- Votre numéro de commerçant
- Votre numéro de client CCVS
- Votre système d'exploitation et sa version

Red Hat, par l'intermédiaire de l'assistance technique, s'efforcera de résoudre tous les problèmes directement en rapport avec CCVS. Nous ne pouvons pas offrir d'assistance pour les produits d'autres éditeurs, sauf pour les questions ayant trait à leur intégration avec CCVS.

5.11 Autres resources

D'autres informations concernant CCVS sont disponibles.

5.11.1 Documentation installée

- `/usr/share/doc/CCVS–<version>` — Contient les fichiers `CHANGES`, `LICENSE`, et `README` , ainsi que la feuille de travail `setup.txt` qui vous aidera à rassembler les informations nécessaires avant d'exécuter le programme de configuration.
- Tapez `man ccvs` pour obtenir une description des différents états de transaction CCVS, les codes erreurs, et bien plus encore. Les pages du manuel pour `ccvsd`, `cvreport`, et `cvupload` décrivent un certain nombre d'options qui peuvent être utilisées avec ces commandes.

5.11.2 Sites Web utiles

- http://www.redhat.com/products/software/ecommerce/ccvs — Ce site fournit des liens vers de nombreuses autres resources CCVS comme des FAQ, des explications techniques et des informations générales concernant CCVS.
- http://www.redhat.com/products/software/ecommerce/ccvs/support/documentation.html — Contient des liens vers plusieurs guides, rédigés expressément pour expliquer les différentes manières d'utiliser CCVS. Ces manuels en ligne traitent de tout, de l'installation à la configuration de CCVS, jusqu'à la description complète des API pour les différentes langues qui peuvent être utilisées.

6 Sendmail

6.1 Introduction à Sendmail

Sendmail est un **agent de transfert** (**MTA**) très utilisé sur Internet. Il traite un grand pourcentage de tous les courriers envoyés par Internet en se déplaçant d'un hôte à l'autre. Il existe d'autres agents de transfert de courrier (fonctionnant avec Red Hat Linux), mais la plupart des administrateurs préfèrent utiliser Sendmail, vu sa puissance, son caractère modifiable et sa conformité avec les standards Internet.

La tâche principale de Sendmail, comme des autres agents de transfert de courrier, est de tansmettre de façon sûre le courrier d'un hôte à l'autre, en utilisant généralement **Simple Mail Transfer Protocol** (**SMTP**). Cela dit, Sendmail offre de grandes capacités de configuration et permet ainsi de contrôler presque tous les aspects de la manipulation de courrier.

Les origines de Sendmail peuvent être suivies depuis la naissance du courrier, jusqu'à dix ans avant la naissance de ARPANET, le précurseur d'Internet. A cette époque, la boîte aux lettres de tous les utilisateurs était un fichier en lecture seule, et les applications de courrier ne faisaient rien de plus qu'ajouter du texte à ce fichier. Chaque utilisateur devait parcourir son fichier de courrier pour trouver un vieux message, et lire un nouveau message était une corvée. Le premier vrai transfert de courrier d'un hôte à un autre a eu lieu en 1972, lorsque le courrier a commencé à être acheminé par FTP sur un protocole de réseau NCP. Cette méthode de communication, plus facile, s'est rapidement diffusée, au point de devenir, en moins d'un an, le plus important agent de transfert de ARPANET. Toutefois, le manque de standardisation entre les protocoles rendaient l'envoi de courrier beaucoup plus difficile depuis certains systèmes. Cette situation s'est prolongée jusqu'à la standardisation de ARPANET sur TCP/IP en 1982. Un nouveau protocole, SMTP, spécialisé dans le transport de courrier est apparu. Ces développements, ainsi que le remplacement des fichiers HOSTS par DNS, permirent de proposer des agents de transfert du courrier offrant de grandes fonctionnalités. Sendmail, né d'un système de livraison de courrier précédent appelé Delivermail, est rapidement devenu standard, alors qu'Internet commençait à s'étendre et à être de plus en plus utilisé.

Il est important d'être conscient de ce qu'est Sendmail ainsi que de ce qu'il peut faire et non. A l'heure où les applications sont monolithiques et qu'elles jouent de multiples rôles, vous pourriez penser que Sendmail est la seule application dont vous avez besoin pour exécuter un serveur de courrier électronique dans votre organisation. Techniquement, c'est vrai. Sendmail peut stocker du courrier dans les répertoires de vos utilisateurs et accepter du courrier via la ligne de commande. Mais les utilisateurs d'aujourd'hui ont besoin de bien plus qu'une simple livraison de courrier. Ils veulent presque toujours interagir avec leur courrier en utilisant un **mail user agent** (**MUA**) qui fonctionne avec **Post Office Protocol** (**POP**), **Internet Message Access Protocol** (**IMAP**), voire même avec le Web. Ces autres protocoles peuvent fonctionner avec Sendmail et SMTP, mais en réalité ils existent pour différentes raisons et peuvent opérer indépendamment l'un de l'autre.

Ce chapitre a pour but de traiter de ce que Sendmail peut faire et non. Consultez les excellentes sources d'informations (en ligne ou non) concernant Sendmail, de façon à le configurer pour qu'il corresponde à vos exigences. Vous devriez cependant savoir quels sont les fichiers installé avec Sendmail par défaut sur votre système, comment effecuer des changements simples de configuration, comment arrêter la réception par Sendmail de courrier non sollicité (spam), et comment étendre Sendmail à l'aide de **Lightweight Directory Access Protocol** (**LDAP**).

6.2 Installation de Sendmail par défaut

Bien que vous puissiez télécharger le code source de Sendmail et construire votre propre exemplaire, de nombreux utilisateurs préfèrent installer Sendmail via RPM depuis le CD-ROM (au moment de l'installation de Red Hat Linux ou plus tard).

L'application Sendmail est située dans `/usr/sbin`.

Un fichier de configuration commenté pour Sendmail (`sendmail.cf`) est installé dans `/etc`. Vous ne devriez pas éditer directement le fichier `sendmail.cf`, à moins de savoir exactement ce que vous faites, car il est très long et complexe. Par contre, pour apporter des changements à la configuration de Sendmail, éditez le fichier `/etc/mail/sendmail.cf` et utilisez le processeur de macros `m4` fourni pour créer un nouveau `/etc/sendmail.cf` (prenez soin de sauvegarder l'original avant de modifier `/etc/sendmail.cf`). Vous trouverez plus d'informations sur la configuration de Sendmail dans la Section 6.3, *Changements communs de configuration*.

Plusieurs fichiers de configuration de Sendmail sont installés dans `/etc/mail`, y compris :

- `access` — Précise quels systèmes peuvent utiliser Sendmail pour transférer le courrier.
- `domaintable` — Vous permet de fournir la configuration du nom de domaine.
- `local-host-names` — L'endroit où vous insérez tous les alias de votre ordinateur.
- `mailertable` — Précise les instructions qui remplacent le suivi dans des domaines particuliers.
- `virtusertable` — Vous permet de créer un formulaire d'alias de domaine spécifique offrant la possibilité de recevoir plusieurs domaines virtuels sur une machine.

Plusieurs fichiers de configuration de `/etc/mail`, comme `access`, `domaintable`, `mailertable` et `virtusertable`, doivent en réalité stocker leurs informations dans des fichiers de base de données pour que Sendmail puisse utiliser les changements de configuration. Pour insérer dans leurs fichiers de base de données les changements que vous faites à cette configuration, exécutez une commande de syntaxe `makemap hash /etc/mail/`*`name`* `< /etc/mail/`*`name`* où *name* est le nom du fichier de configuration à convertir.

Par exemple, si vous voulez que tous les messages adressés à un compte `domain.com` soient livrés à `bob@otherdomain.com`, il vous faut ajouter une ligne au fichier `virtusertable` :

```
@domain.com       bob@otherdomain.com
```

Ensuite, pour ajouter cette nouvelle information au fichier `virtusertable.db`, exécutez `make-map hash /etc/mail/virtusertable < /etc/mail/virtusertable` comme root. Vous créerez ainsi un nouveau `virtusertable.db` contenant la nouvelle configuration.

6.3 Changements communs de configuration

Un fichier par défaut `sendmail.cf` sera installé dans `/etc`. La configuration par défaut devrait fonctionner sur la plupart des sites exclusivement SMTP. Elle ne fonctionnera *pas* pour les sites UUCP (UNIX to UNIX Copy) ; si vous devez utiliser des transferts de courrier UUCP, vous devez générer un nouveau `sendmail.cf`.

Remarque

Contrairement à tous les serveurs qui sont pris en charge automatiquement, le serveur **IMAP** (Internet Message Access Protocol) ne l'est pas. Si votre ISP utilise un serveur IMAP et non un serveur SMTP, il vous faut installer le paquetage IMAP. Sans cela votre système ne saura pas comment transmettre les informations au serveur IMAP ni comment récupérer votre courrier.

Si vous devez générer un nouveau fichier `/etc/sendmail.cf` pour configurer Sendmail, vous devriez utiliser le macro processeur `m4`. Si vous éditez `/etc/mail/sendmail.mc` pour ajouter des fonctions à Sendmail, sauvegardez votre fichier `/etc/sendmail.cf` actuel, générez-en un nouveau en exécutant la commande `m4 /etc/mail/sendmail.mc > /etc/sendmail.cf`, et ajoutez tout changement du fichier `/etc/sendmail.cf` que vous avez sauvegardé dans le nouveau fichier `/etc/sendmail.cf`. Après avoir créé le nouveau `/etc/sendmail.cf`, redémarrez Sendmail pour qu'il prenne effet. La façon la plus simple de faire cela est de taper la commande `/sbin/service sendmail restart` comme root.

Le processeur `m4` est installé par défaut avec Sendmail et se trouve dans le paquetage `sendmail-cf` situé dans `/usr/lib/sendmail-cf`.

Avant d'éditer les fichiers dans les sous-répertoires de `/usr/lib/sendmail-cf`, nous vous conseillons de consulter le fichier `/usr/lib/sendmail-cf/README`, car ils peuvent modifier la configuration des futurs fichiers `/etc/sendmail.cf`.

AVERTISSEMENT

N'utilisez pas Linuxconf pour configurer Sendmail! Le module Linuxconf `mailconf`, conçu pour faciliter l'édition de `/etc/sendmail.cf`, est dépassé et contient des informations désuètes concernant les ensembles de règles utilisées pour la configuration de Sendmail.

La configuration la plus courante de Sendmail est d'utiliser un seul ordinateur comme passerelle de courrier pour tous les ordinateurs de votre réseau. Une entreprise pourrait par exemple vouloir avoir un ordinateur appelé `mail.bigcorp.com` s'occupant de tout le courrier. Il suffit d'ajouter sur cet ordinateur, dans `/etc/mail/local-host-names`, les noms des ordinateurs pour lesquels `mail.bigcorp.com` gèrera le fichier. Voici un exemple :

```
# sendmail.cw - contient tous les alias de votre ordinateur
torgo.bigcorp.com
poodle.bigcorp.com
devel.bigcorp.com
```

Sur les autres ordinateurs, `torgo`, `poodle`, et `devel`, il faut éditer `/etc/sendmail.cf` pour se "masquer" comme `mail.bigcorp.com` afin d'envoyer le courrier et de retransmettre du courrier local à `bigcorp.com`. Cherchez les lignes `DH` et `DM` dans `/etc/sendmail.cf` et éditez-les comme :

```
# who I send unqualified names to
# (null means deliver locally)
DRmail.bigcorp.com

# who gets all local email traffic
DHmail.bigcorp.com

# who I masquerade as (null for no masquerading)
DMbigcorp.com
```

Dans ce type de configuration, tout le courrier envoyé apparaîtra comme s'il était envoyé depuis `bigcorp.com`, et tout le courrier envoyé depuis `torgo.bigcorp.com` ou d'autres hôtes sera expédié à `mail.bigcorp.com`.

Si vous configurez votre système pour masquer un autre utilisateur, tout courrier envoyé de votre systàme à votre système sera envoyé à l'ordinateur en lequel vous êtes masqué. Dans l'exemple précédant, les fichiers de connexion qui sont régulièrement envoyés à `root@poodle.bigcorp.com` depuis le démon `cron` seraient envoyés à `root@mail.bigcorp.com`.

6.4 Arrêter les spam

Le courrier **spam** peut être défini comme du courrier inutile et non désiré reçu par un utilisateur qui ne connaît probablement pas l'expéditeur et n'a sans doute jamais demandé cette communication. Il s'agit d'un courrier très gênant et coûteux qui abuse des standards de communication de l'Internet.

Heureusement, Sendmail a (relativement) facilité le blocage des nouvelles techniques d'envoi de spam utilisées. Il bloque également un grand nombre des méthodes les plus répandues par défaut. Il vous faudrait donc les activer consciencieusement en modifiant votre fichier `/etc/mail/sendmail.cf` pour prédisposer votre système. Par exemple, faire suivre des messages SMTP, également appelés **SMTP relaying**, a été désactivé depuis la version 8.9 de Sendmail. Avant ce changement, Sendmail contraignait votre hôte de courrier (`x.org`) à accepter les messages d'une partie (`y.com`) et à les envoyer vers d'autres parties (`z.net`). Maintenant vous devez dire explicitement à Sendmail de permettre à un domaine de relayer le courrier à travers votre domaine. Pour activer les changements, il suffit d'éditer `/etc/mail/relay-domains` et de relancer Sendmail en tapant la commande `/sbin/service sendmail restart` en tant que root.

Vos utilisateurs pourraient cependant souvent être bombardés par des spams d'autres serveurs Internet hors de votre contrôle. Vous pouvez dans ce cas utiliser le contrôle d'accès de Sendmail que vous trouverez dans le fichier `/etc/mail/access`. En tant que root, il vous suffit d'ajouter les domaines que vous voulez bloquer ou à qui vous voulez autoriser l'accès, comme :

```
badspammer.com       550 Go away and don't spam us anymore
tux.badspammer.com   OK
10.0                 RELAY -relayer
```

`/etc/mail/access` étant une banque de données, vous devez utiliser makemap pour activer vos changements en reconfigurant la banque de données. Cette opération est facile à entreprendre en exécutant la commande `makemap hash /etc/mail/access < /etc/mail/access` en tant que root.

Cet exemple vous montre que tout courrier électronique qui vous est envoyé depuis `badspammer.com` sera bloqué par le code d'erreur de circonstance 550 RFC 821 et renverra un message à l'expéditeur du spam ; si le courrier est expédié depuis le sous-domaine `tux.badspammer.com`, il sera accepté. La dernière ligne montre que tout message envoyé depuis le réseau 10.0.*.* peut être relayé par votre serveur de courrier.

Comme vous pouvez vous en douter, ceci n'est qu'un échantillon des capacités de Sendmail en ce qui concerne le bloquage et l'autorisation d'accès. Pour obtenir plus d'informations sur ce sujet, consultez `/usr/share/doc/sendmail/README.cf` et les exemples.

6.5 Utiliser Sendmail avec LDAP

Comme nous l'avons déjà vu dans le Chapitre 4, *Protocole LDAP (Lightweight Directory Access Protocol)*, LDAP est un outil rapide et puissant pour chercher des informations spécifiques concernant un utilisateur précis du groupe. Vous pouvez par exemple utiliser un serveur LDAP pour chercher l'adresse électronique d'un utilisateur dans le répertoire d'une entreprise en utilisant son nom. Dans ce type d'implémentation, LDAP diffère largement de Sendmail : LDAP stocke les informations utilisateur de façon hiérarchique, tandis que Sendmail ne donne les réponses de LDAP que dans les messages pré-adressés.

Toutefois, Sendmail utilise LDAP pour remplacer séparément les fichiers maintenus de façon séparée, comme `aliases` et `virtusertables`, sur les différents serveurs de messagerie électronique qui fonctionnent ensemble pour gérer une organisation moyenne ou de la taille d'une entreprise. En résumé, vous pouvez utiliser LDAP pour extraire le niveau d'acheminement du courrier de Sendmail et ses fichiers de configuration séparés en une puissante grappe LDAP améliorée par de nombreuses applications.

La version actuelle de Sendmail contient le support de LDAP. Pour étendre votre serveur Sendmail à l'aide de LDAP, équipez-vous d'un serveur LDAP, OpenLDAP par exemple, correctement configuré et en exécution. Il vous faudra ensuite éditer votre `/etc/mail/sendmail.mc` pour comprendre :

```
LDAPROUTE_DOMAIN('yourdomain.com')dnl
FEATURE('ldap_routing')dnl
```

Remarque

Il ne s'agit là que d'une configuration de base de Sendmail à partir de LDAP. Votre configuration devrait être différente, car elle dépend de votre implémentation de LDAP, en particulier si vous voulez configurer plusieurs ordinateurs Sendmail pour utiliser un serveur LDAP commun.

Pour obtenir des instructions plus détaillées concernant la configuration de l'acheminement du courrier LDAP ainsi que des exemples, consultez : `/usr/share/doc/sendmail/README.cf`.

Ensuite, recréez votre fichier `/etc/sendmail.cf` en exécutant `m4` et relançant Sendmail. Pour obtenir plus d'instructions sur ce sujet, consultez la Section 6.3, *Changements communs de configuration.*

Pour obtenir plus d'informations sur LDAP, reportez-vous au Chapitre 4, *Protocole LDAP (Lightweight Directory Access Protocol).*

6.6 Autres ressources

Au début, de nombreux utilisateurs trouvent Sendmail difficile à configurer, surtout à cause du grand nombre d'options qu'il propose. Une documentation supplémentaire peut se révéler très utile, en particulier pour la configuration des options.

6.6.1 Documentation installée

Les meilleures sources d'information sur la configuration de Sendmail se trouvent dans les paquetages `sendmail` et `sendmail-cf`.

- `/usr/share/doc/sendmail/README.cf` — contient des informations sur `m4`, sur l'emplacement des fichiers de Sendmail, sur les protocoles de messagerie électronique pris en charge, sur le mode d'accéder aux fonctions améliorées et plus encore.
- `/usr/share/doc/sendmail/README` — Contient des informations concernant la structure du répertoire Sendmail, le support de protocole IDENT, des détails sur les autorisations de répertoire et les problèmes que ces autorisations causent souvent lorsqu'elles sont mal configurées.

6.6.2 Sites Web utiles

- http://www.sendmail.net — Nouveautés, interviews et articles concernant Sendmail, et vous permettant d'avoir une vision plus large des différentes options disponibles.
- http://www.sendmail.org — Offre une présentation technique détaillée des fonctionalités de Sendmail et des exemples de configuration.

6.6.3 Bibliographie

- *Sendmail* de Bryan Costales et Eric Allman, édité par O'Reilly & Associates — Une bonne référence sur Sendmail rédigée par le créateur de Delivermail et Sendmail.

Partie II Références liées à la sécurité

7 Red Hat : la sécurité

Au-delà de l'installation et de la configuration adéquates de votre système Red Hat Linux, il est impératif d'en assurer la sécurité en fonction d'un niveau de risque acceptable qui tient compte de son rôle, de son importance et de son utilisation. La sécurité est un sujet très complexe qui implique l'émergence constante de nouveaux problèmes et de problèmes potentiels.

En raison de la nature floue et compliquée de la sécurité, de nombreux administrateurs système et utilisateurs font l'erreur de se pencher sur de petits problèmes isolés et d'ignorer des questions beaucoup plus sérieuses qui posent des risques plus élevés. La véritable sécurité d'un système va plus loin que la simple installation de la toute dernière mise à jour, la configuration d'un fichier donné ou la gestion attentive de l'accès des utilisateurs aux ressources du système. C'est une façon d'analyser les menaces auxquelles pourrait faire face votre système et de déterminer jusqu'où vous irez pour les éviter.

A moins qu'il ne soit éteint, aucun système n'est totalement en sécurité (et même dans ce cas, il pourrait toujours courir le risque d'être volé). Lorsqu'un système est allumé, il est susceptible à tout moment d'être victime d'une attaque, allant du virus de macro inoffensif au virus détruisant le matériel entier d'un ordinateur, en passant par l'élimination de données. Tout n'est pas perdu cependant. Au moyen d'une bonne planification et de bons outils, il vous est possible d'utiliser votre ordinateur pendant des années et de n'avoir aucun problème de sécurité. Les sections qui suivent ont été conçues pour vous aider à définir une manière d'aborder la sécurité d'un système et les menaces potentielles auxquelles il fait face. Elles permettent de considérer divers outils de sécurité, leus coûts et leurs avantages lors de l'utilisation de Red Hat Linux.

7.1 Le dilemme incontournable de la sécurité

Tous les utilisateurs de systèmes d'exploitation, quels qu'ils soient, font face à un dilemme commun lorsque vient le temps de créer un paradigme de sécurité pour leur système. D'une part, ils essaient d'éviter de le rendre sûr au point qu'il soit incapable d'exécuter des applications correctement et, de l'autre, d'éviter qu'il ne le soit pas assez et que n'importe qui puisse (et cela se produira) en faire tout ce qu'il veut, tel que d'éliminer le travail des autres ou de commettre des actes encore plus graves.

La solution parfaite à ce dilemme n'existe pas. Certains systèmes, en raison de la nature de leur fonction ou de l'importance des données qu'ils protègent, correspondent à la première prémisse du dilemme alors que d'autres, que ce soit en raison du grand nombre de leurs utilisateurs ou du fait qu'ils sont des ordinateurs de tests, correspondent à la seconde prémisse.

La chose la plus importante à faire lorsque vous configurez la sécurité de votre système est de déterminer où il se situe sur le spectre du dilemme de la sécurité. Il se pourrait que la politique de votre entreprise s'en charge pour vous ou alors que vous soyez un chercheur muni d'un système qui n'est jamais connecté aux réseaux publics et auquel personne d'autre que vous n'a physiquement accès ou encore que vous soyez un utilisateur à la maison ayant une connexion à large bande et que vous soyez

préoccupé (avec raison) par ce que des utilisateurs malicieux de par le monde pourraient bien faire pour endommager vos données.

Peu importe le scénario correspondant à votre situation, vous avez la responsabilité de déterminer l'exposition aux risques de votre système et les objectifs qu'il doit atteindre. Puis, après avoir déterminé le tout, utilisez ces renseignements comme guide pour la configuration et le maintien des lignes directrices de sécurité de votre système.

7.2 Manière active et manière passive d'aborder la sécurité

Les manières d'aborder la sécurité peuvent être divisées en deux types : **active** ou **passive**. Une manière **active** consiste à prévenir toute brèche du modèle de sécurité d'un système, alors qu'une manière **passive** fait plutôt référence aux gestes posés pour contrôler la sécurité du système basée sur le modèle de sécurité en question.

Tout utilisateur devrait employer les deux méthodes car elles se renforcent mutuellement. En effet, le fait de savoir au moyen du journal du serveur qu'un utilisateur donné essaie de déjouer votre système de sécurité (manière passive d'aborder la sécurité) pourrait faire en sorte que vous installiez une application qui bloque les utilisateurs et les empêche carrément d'obtenir une invite de connexion pour commencer (manière active). De même, le fait que vous n'utilisiez pas de mots de passe masqués pour protéger votre système, (approche active) pourrait vous mener à vérifier vigoureusement les changements apportés aux fichiers clés de votre système avec un outil tel que Tripwire (manière passive). Pour obtenir plus de renseignements sur Tripwire, reportez-vous au Chapitre 10, *Installation et configuration de Tripwire*.

Red Hat Linux comprend toute une série d'outils qui vous aideront à mettre en pratique ces deux approches de la sécurité. Dans les deux cas, vous devez toutefois utiliser une méthodologie appropriée afin d'éviter que la protection de votre système ne dépende trop étroitement des outils que vous utiliserez.

7.2.1 Outils et méthodes pour la manière active d'aborder la sécurité

La plupart des outils de sécurité pour Red Hat Linux fonctionnent de façon à protéger activement le système. Voici quelques-uns des outils source ouverte les plus communs et les plus utiles :

- *Utilitaires masqués* — ensemble d'outils conformes aux normes de l'industrie pour gérer les utilisateurs locaux et les groupes d'un système au moyen de mots de passe cryptés.
- *Kerberos 5* — système sécurisé qui fournit des services d'authentification réseau. Il empêche l'utilisation de mots de passe en texte clair envoyés par réseau pour accéder à des services. (Voir

le Chapitre 9, *Utilisation de Kerberos 5 sur Red Hat Linux* pour avoir plus de détails sur Kerberos 5.)

- *OpenSSL* — vous aide à protéger toute une série de services pouvant être pris en charge par un logiciel de cryptographie. (Voir le *Guide de personnalisation officiel Red Hat Linux* pour en savoir plus sur OpenSSL.)
- *OpenSSH* — ensemble de programmes utilitaires qui peuvent très bien remplacer des outils omniprésents, quoique non sécurisés, tels que `telnet` et `ftp` avec des `ssh` et `scp` puissants et sécurisés. (Voir le *Guide de personnalisation officiel Red Hat Linux* pour plus de renseignements sur OpenSSH.)

Voici quelques méthodes qui impliquent une manière active d'aborder la sécurité :

- *Limitez le nombre d'utilisateurs pouvant exécuter des commandes en tant qu'utilisateur root* — que ce soit de façon intentionnelle ou non, un pourcentage élevé des problèmes de sécurité sont le résultat, bien qu'indirect parfois, de personnes connaissant le mot de passe root ou ayant reçu la permission par le biais de `sudo` d'exécuter une commande au niveau root.
- *Connaître tous les paquetages logiciels installés sur votre système et demeurer au fait des faiblesses en matière de sécurité récemment découvertes* — vous ne saurez quels paquetages surveiller à moins de savoir lesquels sont installés sur votre système, ni ne saurez qu'ils ont besoin d'être mis à jour à moins de consulter régulièrement des sources d'information sur le sujet, telles que Red Hat Network.
- *Limitez les services en exécution sur le système à ceux dont vous avez vraiment besoin* — en fait, plus vous en avez en cours, plus vous risquez qu'on les attaque ou qu'on y accède sans autorisation. Gardez les ressources du système (et évitez ainsi de devoir maintenir des choses qui ne vous servent pas) et enlevez les paquetages que vous n'utilisez pas. Ou alors, la moindre des choses à faire serait d'exécuter un outil tel que `ntsysv` afin d'empêcher que les services inutiles ne s'exécutent avec le système au démarrage. (Voir *Contrôler l'accès aux services* dans le *Guide de personnalisation officiel Red Hat Linux*.)
- *Exigez de vos utilisateurs qu'ils créent des mots de passe et qu'ils les changent souvent* — la plupart des problèmes de sécurité commencent par un accès non autorisé au système. Il est possible de réduire ce risque en demandant à vos utilisateurs de pratiquer, eux-aussi, des méthodes actives de sécurité et de protéger leurs clés du système.
- *Assurez-vous que les autorisations d'accès aux fichiers ne sont pas inutilement ouvertes* — aucun fichier, ou presque, ne devrait pouvoir être modifié de tous.

7.2.2 Outils et méthodes pour la manière passive d'aborder la sécurité

Bien que la plupart des outils de sécurité pour Red Hat Linux soient destinés à la manière active d'aborder la sécurité, quelques outils font de la manière passive un fardeau d'administration beaucoup moins lourd.

- *Tripwire* — application conçue pour vous informer de tout changement apporté à des répertoires ou systèmes de fichiers spécifiés. De cette façon, vous saurez au moins si des utilisateurs non autorisés ont accès à votre système ou s'ils effectuent des changements non désirés aux fichiers importants. (Voir le Chapitre 10, *Installation et configuration de Tripwire* pour obtenir plus de renseignements sur Tripwire.)
- *COPS* — ensemble d'outils de sécurité conçus pour remplir différentes fonctions, allant de la vérification des ports ouverts sur un ordinateur hôte donné à la recherche de mots de passe utilisateur trop faciles.

Voici quelques méthodes qui impliquent une manière passive d'aborder la sécurité :

- *Prendre l'habitude de contrôler les journaux système* — par défaut, Red Hat Linux enregistre une énorme quantité de données utiles dans les journaux système situés dans le répertoire `/var/log` et plus particulièrement dans le fichier `messages`. Une simple commande exécutée en tant qu'utilisateur root, telle que `grep "session opened for user root" /var/log/messages | less` vous permet de faire une vérification partielle très efficace de votre système et de contrôler qui y accède en tant qu'utilisateur root. Cela vous donne notamment la possibilité de réduire rapidement le nombre d'utilisateurs possibles pouvant avoir changé un fichier donné qui ne peut être modifié que par des utilisateurs root en comparant tout simplement l'heure à laquelle le fichier en question a été changé avec les heures de début de session dans le fichier `/var/log/messages`. Il est à noter toutefois que cette méthode n'est pas à toute épreuve et qu'une personne ayant la possibilité de modifier un important système de fichiers pourrait également avoir le droit d'apporter des changements à `/var/log/messages` et ainsi d'effacer ses traces.

7.3 Préparation d'une politique de sécurité

Tout système, qu'il s'agisse d'un ordinateur utilisé par une seule personne ou d'un serveur d'entreprise utilisé par des milliers de travailleurs, devrait avoir une politique de sécurité. Une politique de sécurité est un ensemble de lignes directrices servant à déterminer si des tâches données ou des applications doivent ou non être exécutées ou utilisées sur un système, en fonction des objectifs qui lui sont attribués.

Les politiques de sécurité peuvent varier grandement d'un système à l'autre, mais l'important est d'en avoir une pour votre système, qu'elle soit écrite noir sur blanc dans le manuel des politiques de l'entreprise ou tout simplement mémorisée.

Toute politique de sécurité devrait tenir compte des éléments suivants lors de sa conception :

- *Simplicité plutôt que complexité* — plus votre politique de sécurité est simple et directe, plus vous avez de chance que ses lignes directrices soient suivies et que votre système soit sécurisé.
- *Facilité plutôt que difficulté d'entretien* — les méthodes et les outils de sécurité, comme toute chose, peuvent changer en fonction des nouveaux défis et besoins. Votre politique de sécurité doit être conçue de façon à minimiser l'impact que pourraient avoir de tels changements sur le système et ses utilisateurs.
- *Promouvoir la liberté au moyen de la confiance en l'intégrité du système plutôt qu'une utilisation étouffante du système* — évitez d'utiliser des méthodes et outils de sécurité qui diminuent inutilement l'utilité de votre système pour le rendre plus sûr. Les méthodes et outils de sécurité de qualité doivent toujours, dans la mesure du possible, être positifs et rendre le système sécurisé tout en offrant le plus de choix possibles aux utilisateurs.
- *Reconnaître ses faiblesses plutôt que d'avoir un faux sentiment de sécurité* — l'une des meilleures façons d'attirer les problèmes de sécurité est de croire que votre système ne pourrait jamais en être victime. Alors, soyez vigilent en tout temps et ne vous reposez jamais sur vos lauriers.
- *Vous concentrer sur les vrais problèmes plutôt que de vous préoccuper de problèmes virtuels* — consacrez votre temps et vos efforts à la résolution des problèmes réels les plus importants et passez aux autres ensuite. Vos efforts doivent d'abord servir à colmater les plus grandes lacunes. Pour vous aider à déterminer ce sur quoi vous devriez vous pencher en premier, vous pourriez consulter le site Web http://www.sans.org/topten.htm ou d'autres sites semblables, qui soulignent des problèmes de sécurité précis posant un risque réel et vous indiquent comment faire pour les régler.
- *Agir immédiatement plutôt que d'attendre à plus tard* — réglez les problèmes dès que vous les trouvez et que vous jugez qu'ils posent des risques. Ne croyez pas que cela peut attendre. Il n'y a pas de meilleur moment que le moment présent pour le faire, surtout lorsque votre système est en jeu.

Si vous vous rendez compte que votre politique de sécurité est trop restrictive et qu'elle vous empêche d'utiliser votre système comme vous l'entendez, vous devriez peut-être songer à accroître l'accès au système. De même, si vous vous apercevez que la sécurité de votre système est compromise, vous devriez revoir votre politique et restreindre l'accès au système. Par-dessus tout, il ne faut pas oublier qu'une politique de sécurité n'est pas une idée ou un document statique. Elle doit être modifiée en fonction des besoins et des objectifs changeants des utilisateurs. Réévaluez-la continuellement et demandez-vous si elle correspond aux exigences du monde actuel.

7.4 Au-delà de la protection root

De nombreux utilisateurs mettent principalement l'accent sur la réduction du nombre d'utilisateurs ayant l'accès root à leur système. Quoique ce soit une excellente et importante première étape, il faut faire bien plus pour assurer la sécurité d'un système. En réalité, la sécurité n'est qu'une partie de cette question beaucoup plus vaste qu'est la stabilité du système. Les problèmes de sécurité s'entremêlent souvent à des problèmes de stabilité plus importants et un système efficace doit d'abord et avant tout avoir un juste équilibre entre les méthodes et les outils utilisés pour la sécurité et une prise de conscience que ces problèmes peuvent provoquer des dommages de différentes façons.

Premièrement, si votre système est utilisé par de nombreux utilisateurs qui peuvent parfois changer, assurez-vous d'éliminer les comptes des anciens utilisateurs dès qu'ils ne servent plus ou, encore mieux, créez une liste à cocher précise faisant état des mesures à prendre lorsqu'un compte utilisateur ou un groupe n'est plus requis.

Limitez l'accès physique à votre système. Si vous y avez des fichiers d'une certaine importance et qu'une personne désire les trouver, cette dernière pourrait décider qu'il est plus simple de le faire en se sauvant carrément avec le disque dur et en essayant d'y entrer à son rythme ailleurs. Vous pouvez rendre la vie difficile à ce genre d'individu en lui cachant l'aspect physique de l'ordinateur qu'il désire trafiquer.

Avant tout, essayez d'imaginer les façons les plus élémentaires de déjouer vos méthodes de sécurité. Dites-vous qu'il est inutile de ne protéger qu'une seule voie d'accès à votre système et d'en laisser d'autres, plus susceptibles d'être attaquées, à découvert. Evidemment, tout cela dépend de vous ou des besoins de vos utilisateurs, mais assurez-vous toutefois de ne pas vous concentrez seulement sur une seule faiblesse de votre système.

7.5 L'importance des mots de passe sécurisés

Les mots de passe sont les clés d'accès de votre système. Il va sans dire qu'ils doivent être le plus sécurisés possible afin d'empêcher que des utilisateurs accèdent au système sans autorisation, premier pas vers de plus grands problèmes de sécurité. L'utilisation de mots de passe assez efficaces pour contrecarrer une attaque est une étape cruciale et simple qui peut vous préserver de nombreux problèmes futurs.

Trop nombreux sont les mots de passe des utilisateurs faciles à deviner. Red Hat Linux fournit différentes façons d'accorder l'autorisation au système, telles que les mots de passe cryptés qui utilisent `crypt`, les mots de passe masqués (dont on parle plus longuement à la Section 12.1, *Utilitaires masqués*), Kerberos 5, etc. Chaque fois que vous sélectionnez un mot de passe faisant partie d'un système d'authentification, la sécurité même de cette authentification est partiellement à la merci de la complexité du mot de passe choisi.

Pourquoi faut-il toujours essayer de créer des mots de passe difficiles à deviner ? En peu de mots, les prix du matériel informatique puissant ne cessent de diminuer alors que les outils et les méthodes de qualité, offerts gratuitement, pour déjouer les mots de passe ne cessent d'augmenter. En raison de la façon de stocker les mots de passe de nombreux modèles d'authentification simples, si un individu réussit à accéder au fichier contenant les mots de passe des utilisateurs d'un système, il peut généralement en deviner un assez rapidement en comparant les mots de passe cryptés à une liste de mots du dictionnaire. Bien que les modèles d'authentification reconnaissent ce genre d'attaque et essaient différentes méthodes pour en réduire le nombre, aucune d'entre elles n'est à l'épreuve de tout. Aussi, vous devriez accorder une très grande importance aux mots de passe que vous utilisez et à la fréquence avec laquelle vous les changez, particulièrement pour le compte root.

Un bon mot de passe a les qualités suivantes :

- *Avoir au moins huit caractères* — plus le mot de passe est court, plus il est facile de le déjouer.
- *Etre composé de caractères, de chiffres et de symboles* — les chiffres et les symboles cachés au milieu des lettres (ou vice versa) font augmenter les options possibles pour un caractère donné, ce qui renforce le mot de passe dans son ensemble.
- *Etre unique* — sélectionnez des mots de passe différents pour chacune des utilisations que vous en faites. Si tous vos mots de passe sont identiques ou très semblables, les brèches dans la sécurité de votre système se multiplieront.

Vous devriez éviter d'utiliser des mots de passe qui :

- *sont des mots d'un dictionnaire* — en utilisant des mots de passe tirés d'un dictionnaire, vous rendez la tâche beaucoup plus facile aux personnes qui essaient de percer votre système. Ne le faites pas et ne changez pas les modèles d'authentification qui empêchent les utilisateurs de choisir des mots du dictionnaire pour qu'ils puissent le faire.
- *sont liés à vos renseignements personnels* — si vous utilisez votre date d'anniversaire, le nom de votre conjoint ou la marque de votre voiture comme mot de passe, vous vous attirez des problèmes. Réfléchissez à tous vos mots de passe et demandez-vous si l'une ou l'autre des personnes que vous connaissez pourrait les deviner. Si vous avez le moindre doute, n'utilisez pas ces mots de passe.
- *ne peuvent être tapés rapidement* — si votre mot de passe est compliqué au point où vous devez toujours vous arrêter et chercher chaque touche pour le taper, des regards indiscrets pourraient facilement repérer l'emplacement des touches à l'aide de vos doigts et deviner votre mot de passe. Si vous tenez absolument à l'utiliser, entraînez-vous à le taper lorsque vous êtes seul, pour augmenter votre vitesse d'exécution.

7.6 Sécurité réseau

Si vous utilisez votre système Red Hat Linux sur un réseau (tel qu'un réseau local d'entreprise, un réseau étendu ou Internet), vous devriez savoir qu'il fait face à un degré de risque plus élevé que s'il

n'était connecté à aucun réseau. Au-delà des simples attaques envers les fichiers de mots de passe et des utilisateurs qui y accèdent sans autorisation, la présence de votre système sur un réseau plus vaste accroît les possibilités de problèmes de sécurité et les différentes formes qu'ils peuvent prendre.

Un certain nombre de mesures de sécurité pour réseau ont été incluses dans Red Hat Linux et de nombreux outils de sécurité source ouverte sont également compris dans la distribution de base. Néanmoins, en dépit de votre préparation, des problèmes de sécurité pourraient tout de même survenir, en raison, d'une part, de la topologie de votre réseau ou, de l'autre, d'une douzaine d'autres facteurs. Pour vous aider à déterminer la source des problèmes de sécurité sur réseau et les méthodes pour les résoudre, vous devez essayer d'imaginer dans quelles circonstances ces problèmes peuvent se produire, comme par exemple :

- *La recherche de données d'authentification* — plusieurs méthodes d'authentification dans Linux et les autres systèmes d'exploitation nécessitent que vous envoyiez vos informations d'authentification "sans protection", c'est-à-dire que votre nom d'utilisateur et votre mot de passe sont envoyés sur le réseau en texte en clair ou non cryptés. Il existe une panoplie d'outils offerts à ceux qui ont accès à votre réseau (ou Internet, si vous l'utilisez pour accéder à votre système) qui leur permettent de rechercher ou de détecter votre mot de passe en enregistrant toutes les données transférées sur le réseau et en les passant au crible pour y trouver des instructions d'accès. Cette méthode peut être utilisée pour trouver *toute* information envoyée sans être cryptée, même votre mot de passe root. Il est impératif d'appliquer et d'utiliser des outils tels que Kerberos 5 et OpenSSH pour éviter que vos mots de passe ou vos données importantes ne soient envoyées sans cryptographie. Si, pour une raison donnée, ces outils ne peuvent être utilisés sur votre système, ne vous connectez jamais en tant qu'utilisateur root, à moins d'être à la console.

- *L'attaque frontale* — les attaques DoS (refus de service) et autres du même genre, peuvent aller jusqu'à endommager un système sécurisé en l'inondant de requêtes incorrectes ou difformes qui l'accablent ou créent des processus qui mettent le système et ses données, ainsi que d'autres systèmes qui communiquent avec lui, en danger. Plusieurs protections sont disponibles pour vous aider à arrêter une attaque et minimiser les dommages. Toutefois, l'idéal pour faire face aux attaques frontales est d'analyser en profondeur la façon dont les systèmes non sécurisés communiquent avec votre système sécurisé, de mettre des barrières entre eux et de préparer une riposte rapide à tout événement pour limiter les possibilités de rupture ou de dommages.

- *L'exploitation de bogues et de pseudo-problèmes de sécurité* — on trouve parfois des bogues dans les logiciels qui, s'ils sont exploités, pourraient créer de graves dommages à un système non protégé. C'est pour cette raison qu'il est recommandé d'exécuter le moins de processus root possible. De plus, utilisez les différents outils mis à votre disposition, tels que Red Hat Network pour obtenir des renseignements sur la mise à jour des paquetages et sur des questions de sécurité importantes, afin de résoudre certains problèmes de sécurité dès qu'ils sont découverts. Assurez-vous également qu'aucun programme ne s'exécute inutilement lors du démarrage de votre système. Moins vous lancez de programmes, moins les bogues de sécurité possibles peuvent vous frapper.

7.7 Autres ressources

Les informations en matière de sécurité changent constamment et les sites Web représentent une façon commode d'obtenir des nouvelles récentes à ce sujet. Pour être au fait des nouveautés ou pour trouver plus de renseignements sur diverses questions de sécurité concernant Red Hat Linux, vous pouvez visiter régulièrement le site de Linux ou des sites généraux sur la sécurité. En outre, si vous avez besoin d'idées pour la création d'une politique de sécurité solide qui tient compte des besoins particuliers de votre système, utilisez un bon livre sur la sécurité.

7.7.1 Sites Web utiles

- http://www.redhat.com/support/errata — consultez la section Support du site de Red Hat pour obtenir des conseils sur la sécurité ou les mises à jour affichées pour chaque version de Red Hat Linux.
- http://www.cert.org — le site Web CERT offre une liste très à jour des divers incidents et vulnérabilités en matière de sécurité, tels que des informations sur les différentes questions de sécurité et la façon de remettre sur pied un système qui a été exposé à une attaque.
- http://www.sans.org — le site Web SANS (System Administration, Networking and Security Institute) offre des avertissements de sécurité sous forme compréhensible, telles que des liens pratiques vers des RPM mis à jour (lorsque disponibles).
- http://www.linuxsecurity.com — ce site Web de Linux, spécifique à la question de la sécurité, renferme des liens Linux relatifs à la sécurité, de la documentation et plus encore.
- http://www.securityportal.com — le site Security Portal contient une série de nouvelles récentes sur la sécurité, des solutions spécifiques à Linux et des documents qui expliquent comment créer de meilleures méthodes et politiques de sécurité.

7.7.2 Livres sur le sujet

- *Securing and Optimizing Linux: Edition Red Hat* de Gerhard Mourani, édité par OpenNA — ce livre peut aussi être téléchargé gratuitement au format PDF à l'adresse suivante : http://www.openna.com.
- *Secrets & Lies* de Bruce Schneier, édité par John Wiley & Sons, Inc. — une analyse complète et pragmatique de la question actuelle de la sécurité des ordinateurs.

8 Modules d'authentification enfichables (PAM)

Les programmes qui donnent des privilèges aux utilisateurs doivent authentifier correctement (vérifier l'identité de) chaque utilisateur. Lorsque vous ouvrez une session sur un système, il vous est nécessaire de fournir votre nom d'utilisateur et votre mot de passe. Le processus d'ouverture de session les utilise ensuite pour authentifier le nom de connexion et s'assurer que vous êtes bien la personne que vous prétendez être. Outre les mots de passe, il existe aussi d'autres formes d'authentification et les mots de passe peuvent être stockés de diverses façons.

Les modules d'authentification enfichables (PAM) permettent à l'administrateur système de définir une politique d'authentification sans avoir à recompiler les programmes d'authentification. Grâce aux PAM, il est possible de contrôler de quelle façon des modules d'authentification donnés sont connectés à un programme en ne modifiant que le fichier de configuration PAM de ce programme dans `/etc/pam.d`.

La plupart des utilisateurs de Red Hat Linux n'auront jamais besoin de modifier les fichiers de configuration PAM de leurs programmes. En effet, lorsque vous utilisez RPM pour installer des programmes qui ont besoin d'une authentification, les changements nécessaires pour l'utilisation de mots de passe d'authentification au moyen de PAM se font automatiquement. Toutefois, si vous devez personnaliser votre configuration, vous devez bien comprendre la structure des fichiers de configuration PAM. Vous trouverez plus de renseignements à ce sujet à la Section 8.2.2, *Modules PAM*.

8.1 Avantages des PAM

Lorsqu'un PAM est utilisé correctement, il offre de nombreux avantages à l'administrateur système, tels que :

- Un modèle d'authentification pouvant être utilisé par un vaste éventail d'applications.
- La mise en oeuvre de PAM qui peuvent ainsi être utilisés pas différentes applications sans qu'il ne soit nécessaire de recompiler ces dernières pour la prise en charge spécifique de ces PAM.
- Flexibilité et contrôle de l'authentification pour l'administrateur et le développeur d'applications.
- Les développeurs d'applications n'ont pas à créer leurs programmes de façon à ce qu'ils utilisent un modèle d'authentification particulier, ce qui leur permet de consacrer tous leurs efforts à d'autres détails de leurs programmes.

8.2 Fichiers de configuration PAM

Le répertoire `/etc/pam.d` contient les fichiers de configuration PAM. Dans les versions précédentes, on utilisait `/etc/pam.conf`. Le fichier `pam.conf` peut encore être lu si aucune entrée `/etc/pam.d/` n'est trouvée, mais son utilisation est déconseillée.

Chaque application (ou *service*, comme les applications destinées à être utilisées par de nombreux utilisateurs sont communément appelées) a son propre fichier. Chaque fichier est composé de cinq éléments différents : un **nom de service**, un **type de module**, un **indicateur de contrôle**, un **chemin d'accès du module** et des **arguments**.

8.2.1 Noms de service PAM

Le nom de service d'une application utilisant un PAM est le nom de son fichier de configuration dans `/etc/pam.d`. Tout programme utilisant un PAM définit son propre nom de service.

Par exemple, le programme `login` définit le nom de service `login`, `ftpd` `ftp`, etc.

En général, le nom de service correspond au nom du programme utilisé pour *accéder* au service et non pas au nom du programme utilisé pour *fournir* le service.

8.2.2 Modules PAM

Il y a quatre types de module PAM pour contrôler l'accès à un service donné :

- Les modules `auth`, qui fournissent l'authentification même (en demandant par exemple un mot de passe et en le vérifiant) et établissent des certificats d'identité, tels qu'une inscription à un groupe ou des tickets Kerberos.
- Les modules `account`, qui se chargent de la vérification nécessaire afin de s'assurer que l'authentification est permise (si le compte est encore valide, si l'utilisateur est autorisé à ouvrir une session à cette heure de la journée, etc.).
- Les modules `password`, qui sont utilisés pour définir des mots de passe.
- Les modules `session`, qui sont utilisés après l'authentification d'un utilisateur. Un module `session` permet à une personne d'utiliser son compte (pour, par exemple, monter son répertoire personnel ou activer sa boîte aux lettres).

Ces modules peuvent être *superposés* ou placés les uns à la suite des autres de façon à utiliser plusieurs modules à la fois. L'ordre d'une superposition de modules est très important dans le processus d'authentification car il permet à l'administrateur système de demander que de nombreuses conditions soient remplies avant d'accorder l'authentification à un utilisateur.

Par exemple, `rlogin` utilise normalement un minimum de quatre méthodes d'authentification, les unes à la suite des autres, comme vous pouvez le constater en jetant un coup d'oeil à son fichier de configuration PAM :

```
auth       required     /lib/security/pam_nologin.so
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_env.so
auth       sufficient   /lib/security/pam_rhosts_auth.so
auth       required     /lib/security/pam_stack.so service=system-auth
account    required     /lib/security/pam_stack.so service=system-auth
password   required     /lib/security/pam_stack.so service=system-auth
session    required     /lib/security/pam_stack.so service=system-auth
```

Avant d'accorder `rlogin` à un utilisateur, PAM s'assure que `/etc/nologin` n'existe pas, que l'utilisateur n'essaie pas de se connecter à distance en tant qu'utilisateur root et que toute variable d'environnement peut être chargée. Ensuite, une authentification `rhosts` réussie doit être faite avant que la connexion ne soit accordée. Si l'authentification `rhosts` échoue, une authentification standard au moyen d'un mot de passe est lancée.

Il est possible d'ajouter des modules d'authentification enfichables à tout moment et on peut ensuite créer des applications les reconnaissant pour les utiliser. Par exemple, si vous élaborez une méthode de création de mot de passe unique et écrivez un module d'authentification enfichable pour la prendre en charge, tous les programmes reconnaissant les PAM pourront utiliser ce nouveau module et cette méthode de mot de passe à l'instant sans qu'ils n'aient besoin d'être recompilés ou modifiés. Comme vous pouvez l'imaginer, ceci est très utile car vous pouvez combiner (et tester) rapidement des méthodes d'authentification à différents programmes sans devoir les recompiler.

La documentation sur l'écriture de modules est comprise avec le système dans `/usr/share/doc/pam-<`*`version-number`*`>`.

8.2.3 Indicateurs de contrôle PAM

Lors d'une vérification, tous les modules PAM produisent un résultat qui en indique la réussite ou l'échec. Les indicateurs de contrôle indiquent aux PAM quoi faire de ce résultat. Comme les modules peuvent être mis dans un ordre bien précis, les indicateurs de contrôle vous donnent la possibilité de définir l'importance de certains modules par rapports à ceux qui viennent après eux.

Prenons, encore une fois, l'exemple du fichier de configuration PAM de `rlogin` :

```
auth       required     /lib/security/pam_nologin.so
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_env.so
auth       sufficient   /lib/security/pam_rhosts_auth.so
auth       required     /lib/security/pam_stack.so service=system-auth
account    required     /lib/security/pam_stack.so service=system-auth
password   required     /lib/security/pam_stack.so service=system-auth
```

```
session    required     /lib/security/pam_stack.so service=system-auth
```

Une fois qu'un type de module a été spécifié, les indicateurs de contrôle décident quelle importance doit être attribuée au module en question en fonction de l'objectif général qui est d'accorder l'accès du programme à un utilisateur.

Quatre types d'indicateurs de contrôle sont définis par la norme PAM :

- Les modules ayant l'indication `required` doivent être vérifiés avec succès pour que l'authentification soit accordée. Si la vérification d'un module portant l'indication `required` échoue, l'utilisateur n'en est pas averti tant que tous les modules du même type n'auront pas été vérifiés.
- Les modules ayant l'indication `requisite` doivent également être vérifiés avec succès pour que l'authentification soit accordée. Cependant, si la vérification d'un de ces modules échoue, l'utilisateur en est averti sur-le-champ au moyen d'un message lui indiquant l'échec du premier module `required` *ou* `requisite`.
- La vérification des modules ayant l'indication `sufficient` est ignorée en cas d'échec, mais, si la vérification est réussie et qu'aucun module `required` précédent n'a échoué, aucun autre module de ce type ne sera vérifié et ce type de module sera considéré comme étant vérifié dans l'ensemble.
- Les modules ayant l'indication `optional` ne sont pas cruciaux pour la réussite ou l'échec de l'authentification de ce type de module. Ils ne jouent un rôle que lorsque aucun autre module de ce type n'a réussi ou échoué. Dans ce cas, le succès ou l'échec d'un module portant l'indication `optional` détermine l'authentification PAM générale pour ce type de module.

Il existe maintenant pour PAM une syntaxe d'indicateurs de contrôle plus récente qui offre encore plus de contrôle. Veuillez lire les documents PAM qui se trouvent dans `/usr/share/doc/pam–<`*`version-number`*`>` pour en savoir plus sur cette nouvelle syntaxe.

8.2.4 Chemins d'accès des modules PAM

Les chemins d'accès indiquent à PAM où trouver les modules enfichables à utiliser avec le type de module spécifié. Normalement, le chemin d'accès complet menant au module est indiqué, tel que `/lib/security/pam_stack.so`. Cependant, si le chemin d'accès complet n'est pas donné (autrement dit, si le chemin d'accès ne commence pas par un `/`), on considère alors que le module indiqué est situé dans `/lib/security`, l'emplacement par défaut des modules PAM.

8.2.5 Arguments PAM

PAM utilise des arguments pour passer des informations à un module enfichable pendant le processus d'authentification d'un type de module donné. Ces arguments permettent aux fichiers de configuration PAM de programmes particuliers d'utiliser le même module PAM, mais de différentes façons.

Par exemple, le module `pam_userdb.so` utilise des fichiers cachés stockés dans un fichier de la base de données Berkeley pour authentifier les utilisateurs. (La base de données Berkeley est une base de données source ouverte conçue pour être utilisée dans de nombreuses applications afin de contrôler différents types d'informations.) Le module prend un argument `db` qui spécifie le fichier de la base de données à utiliser et qui peut être différent pour divers services.

Donc, la ligne `pam_userdb.so` dans un fichier de configuration PAM ressemble à ceci (sur une seule ligne):

```
auth      required  /lib/security/pam_userdb.so db=chemin
d'accès/au/fichier
```

Les arguments non valides sont ignorés et n'ont aucun effet sur la réussite ou l'échec du module PAM. Lorsqu'un argument non valide est passé, une erreur est généralement écrite dans `/var/log/messages`. Toutefois, comme la méthode de signalisation est contrôlée par le module PAM, c'est à ce dernier d'enregistrer correctement l'erreur.

8.2.6 Exemples de fichiers de configuration PAM

Un fichier de configuration PAM ressemble à ceci :

```
#%PAM-1.0
auth      required  /lib/security/pam_securetty.so
auth      required  /lib/security/pam_unix.so shadow nullok
auth      required  /lib/security/pam_nologin.so
account   required  /lib/security/pam_unix.so
password  required  /lib/security/pam_cracklib.so
password  required  /lib/security/pam_unix.so shadow nullok use_authtok
session   required  /lib/security/pam_unix.so
```

La première ligne est un commentaire (toute ligne commençant par un # est un commentaire). Les lignes deux à quatre superposent trois modules à utiliser pour l'authentification de connexion.

```
auth      required  /lib/security/pam_securetty.so
```

La deuxième ligne sert à s'assurer que, *si* l'utilisateur essaie de se connecter en tant qu'utilisateur root, le terminal sur lequel il se connecte fait partie de la liste se trouvant dans le fichier `/etc/securetty`, *si* ce fichier existe.

```
auth      required  /lib/security/pam_unix.so shadow nullok
```

La troisième ligne fait en sorte que le mot de passe de l'utilisateur soit demandé et vérifié.

```
auth      required  /lib/security/pam_nologin.so
```

La quatrième ligne vérifie si le fichier `/etc/nologin` existe. Si c'est le cas et que l'utilisateur n'est pas un utilisateur root, l'authentification échoue.

Notez que les trois modules `auth` sont vérifiés, *même si le premier module* `auth` *échoue*. Cette stratégie empêche que l'utilisateur sache pour quelle raison son authentification n'est pas acceptée. S'il savait pourquoi son authentification est refusée, il pourrait avoir plus de facilité à déjouer le processus d'authentification au prochain essai. Vous pouvez modifier cette méthode en changeant `required` par `requisite`. Si un module ayant l'indication `requisite` obtient un résultat négatif, PAM échoue immédiatement sans appeler d'autres modules.

```
account   required  /lib/security/pam_unix.so
```

La cinquième ligne active la vérification des comptes lorsque nécessaire. Par exemple, si des mots de passe masqués ont été activés, le module `pam_unix.so` vérifie si le compte est périmé ou si l'utilisateur a changé son mot de passe pendant le délai de grâce alloué.

```
password  required  /lib/security/pam_cracklib.so
```

La sixième ligne teste les mots de passe récemment modifiés afin de déterminer s'ils peuvent être détectés facilement par un programme de détermination de mots de passe utilisant un dictionnaire.

```
password  required  /lib/security/pam_unix.so shadow nullok use_authtok
```

La septième ligne spécifie que le module `pam_unix.so` doit être utilisé si le programme `login` change le mot de passe de l'utilisateur. (Cela ne se produit que lorsqu'un module `auth` détermine que le mot de passe doit être changé — quand un mot de passe masqué est périmé, par exemple.)

```
session   required  /lib/security/pam_unix.so
```

La huitième et dernière ligne indique que le module `pam_unix.so` doit être utilisé pour gérer la session. En ce moment, ce module ne fait rien du tout ; il pourrait être remplacé par tout autre module nécessaire ou complété par la superposition de modules.

Notez que l'ordre des lignes à l'intérieur de chaque fichier compte. Bien que l'ordre dans lequel les modules `required` sont appelés a peu d'importance, il y a d'autres indicateurs de contrôle disponibles et, alors que `optional` est rarement utilisé, `sufficient` et `requisite` redonnent une importance à l'ordre.

Dans le prochain exemple, nous examinerons la configuration `auth` de `rlogin` :

```
#%PAM-1.0
auth      required    /lib/security/pam_nologin.so
auth      required    /lib/security/pam_securetty.so
auth      required    /lib/security/pam_env.so
auth      sufficient  /lib/security/pam_rhosts_auth.so
auth      required    /lib/security/pam_stack.so service=system-auth
```

Premièrement, `pam_nologin.so` vérifie si `/etc/nologin` existe. S'il existe, seuls les utilisateurs root peuvent obtenir l'accès.

```
auth      required    /lib/security/pam_securetty.so
```

Deuxièmement, `pam_securetty.so` empêche les connexions root sur des terminaux non sécurisés. Ceci a pour effet de refuser toute tentative de `rlogin` root. Si vous désirez les autoriser (dans ce cas, vous avez intérêt à être protégé par un excellent coupe-feu ou à ne pas être connecté à Internet), lisez la Section 8.4, *Utilisation de `rlogin`, `rsh` et `rexec` avec PAM*.

```
auth      required    /lib/security/pam_env.so
```

Troisièmement, le module `pam_env.so` charge les variables d'environnement spécifiées dans `/etc/security/pam_env.conf`.

```
auth      sufficient  /lib/security/pam_rhosts_auth.so
```

Quatrièmement, si `pam_rhosts_auth.so` procède à l'authentification de l'utilisateur au moyen de `.rhosts` dans le répertoire personnel de l'utilisateur, PAM authentifie immédiatement `rlogin` sans passer à l'authentification normale par mot de passe avec `pam_stack.so`. Si `pam_rhosts_auth.so` échoue lors de l'authentification de l'utilisateur, cette tentative non réussie est ignorée.

```
auth      required    /lib/security/pam_stack.so service=system-auth
```

Cinquièmement, si `pam_rhosts_auth.so` ne réussit pas à authentifier l'utilisateur, le module `pam_stack.so` lance une authentification normale avec mot de passe et l'argument `service=system-auth` lui est passé.

Remarque

Si vous ne voulez pas qu'une invite de mot de passe apparaisse lorsque la vérification `securetty` échoue et détermine que l'utilisateur essaie de se connecter à distance comme utilisateur root, vous pouvez changer le module `pam_securetty.so` de `required` à `requisite`. Autrement, si vous désirez autoriser la connexion root à distance (ce qui n'est pas du tout une bonne idée), vous n'avez qu'à mettre un # devant cette ligne pour l'annuler.

8.3 Mots de passe masqués

Si vous utilisez des mots de passe masqués, `pam_unix.so` détecte automatiquement s'ils sont en usage et les utilise pour authentifier l'utilisateur.

Veuillez consulter la Section 12.1, *Utilitaires masqués* pour avoir plus de renseignements sur les mots de passe masqués.

8.4 Utilisation de `rlogin`, `rsh` et `rexec` avec PAM

Pour des raisons de sécurité, `rexec`, `rsh` et `rlogin` ne sont pas activés par défaut dans Red Hat Linux 7.1 . Vous devriez plutôt utiliser la suite d'outils OpenSSH. Vous trouverez plus d'informations au sujet de cette suite d'outils au Chapitre 11, *Protocole SSH* et dans le *Guide de personnalisation officiel Red Hat Linux*.

Si vous devez utiliser `rexec`, `rsh` et `rlogin` et ce en tant que root, vous devez apporter quelques modifications au fichier `/etc/securetty`. Ces trois outils possèdent tous des fichiers de configuration PAM ayant besoin du module PAM `pam_securetty.so`. Par conséquent, vous devez modifier `/etc/securetty` pour autoriser l'accès root.

Avant de pouvoir vous connecter en tant que root au moyen de ces outils, vous devez les définir correctement. D'abord, installez le RPM `rsh-server`, qui est inclus dans Red Hat Linux 7.1. Reportez-vous au *Guide de personnalisation officiel Red Hat Linux* si vous avez besoin d'aide sur l'utilisation de RPM.

Ensuite, exécutez `ntsysv` et activez `rexec`, `rsh` et `rlogin`. Lisez les pages de manuel `ntsysv` si vous désirez en savoir plus sur cet outil.

Enfin, redémarrez `xinetd` avec `/sbin/service xinetd restart` pour activer les changements `ntsysv` apportés. A ce stade, tous les utilisateurs, sauf les utilisateurs root, peuvent utiliser `rexec`, `rsh` et `rlogin`.

Pour faire en sorte que les utilisateurs root puissent également les utiliser, ajoutez le nom des outils que vous voulez autoriser dans `/etc/securetty`. Aussi, si vous désirez permettre la connexion root au moyen de `rexec`, `rsh` et `rlogin`, ajoutez les lignes suivantes à `/etc/securetty` :

```
rexec
rsh
rlogin
```

Pour permettre la connexion root au moyen de ces outils par le biais du protocole `telnet` (très mauvaise idée, mais nécessaire dans certains environnements), ajoutez aussi ces quelques lignes :

```
pts/0
pts/1
```

8.5 Autres ressources

Dans ce chapitre, nous n'avons parlé que d'une partie des éléments concernant PAM. De nombreuses autres sources d'informations existent également et peuvent être très utiles pour vous aider à configurer et utiliser PAM sur votre système.

8.5.1 Documentation installée

- Page de manuel `pam` — très bonne introduction à PAM, couvrant la structure et le but des fichiers de configuration PAM.
- `/usr/share/doc/pam–<version-number>` — contient une excellente documentation HTML sur PAM, dont un *Guide de l'administrateur système*, un *Manuel pour programmeurs de modules* et un *Manuel pour développeurs d'applications*. Il contient également une copie de DCE-RFC 86.0, la norme PAM.

8.5.2 Sites Web utiles

- http://www.kernel.org/pub/linux/libs/pam — site Web de la distribution principale pour le projet Linux-PAM, qui offre des informations sur différents modules PAM et applications en usage ou en cours de développement, un forum aux questions et de la documentation supplémentaire au sujet de PAM.

En plus de ces sources d'informations, nous vous suggérons aussi de lire le plus d'exemples possibles de fichiers de configuration lorsque vous commencez à utiliser PAM. De nombreux sites Web en donnent, aussi bien pour les administrateurs désireux de changer les paramètres par défaut des fichiers de configuration que pour les développeurs d'applications voulant utiliser PAM dans leurs programmes.

9 Utilisation de Kerberos 5 sur Red Hat Linux

Kerberos est un système sécurisé permettant de fournir des services d'authentification de réseau. L'authentification signifie :

- que les identités des entités sur le réseau sont vérifiées,
- que le trafic sur le réseau émane de la source qui prétend l'avoir envoyé,
- que Kerberos utilise des mots de passe pour vérifier l'identité des utilisateurs, mais les mots de passe ne sont jamais envoyés sur le réseau sans avoir été préalablement codés.

9.1 Pourquoi utiliser Kerberos ?

La plupart des systèmes de réseau conventionnels utilisent des systèmes d'authentification par mot de passe. Lorsqu'un utilisateur doit s'authentifier auprès d'un service fonctionnant sur un serveur de réseau, il entre son mot de passe pour chaque service requérant une authentification. Son mot de passe est diffusé sur le réseau et le serveur utilise ce mot de passe pour vérifier l'identité de l'utilisateur.

La transmission des mots de passe sous forme de texte en clair effectuée de cette manière, tout en étant une pratique courante, représente un risque énorme sur le plan de la sécurité. Tout pirate de système ayant accès au réseau et à un analyseur de paquets (généralement appelé "sniffer" de paquets) peut intercepter tout mot de passe envoyé de cette manière.

Le principe de base ayant présidé à la conception de Kerberos est de veiller à ce que les mots de passe ne soient *jamais* envoyés sur un réseau sans avoir été préalablement codés et, de préférence, ne soient jamais envoyés du tout. L'utilisation appropriée de Kerberos éliminera le risque de "sniffers" de paquets interceptant des mots de passe sur votre réseau.

9.2 Pourquoi ne pas utiliser Kerberos ?

Si Kerberos permet d'éliminer une menace commune pour la sécurité, pourquoi n'est-il pas systématiquement utilisé sur tous les réseaux ? Plusieurs raisons font que Kerberos peut être difficile à implémenter :

- Il n'existe pas de solution rapide pour la migration de mots de passe utilisateur d'une base de données de mots de passe UNIX standard (par exemple `/etc/passwd` ou `/etc/shadow`) vers une base de données de mots de passe Kerberos. Consultez la Question 2.23 du site http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#pwconvert ou la section Section 9.8, *Autres ressources* pour obtenir des informations plus détaillées sur ce point.

- PAM (Pluggable Authentication Module, module d'authentification enfichable) est utilisé par la plupart des serveurs fonctionnant avec Red Hat Linux. Pour plus d'informations sur ce point, reportez-vous à la Section 9.7, *Kerberos et les modules d'authentification enfichables (PAM)*.
- Pour qu'une application utilise Kerberos, ses sources doivent être modifiées afin de faire les appels appropriés dans les bibliothèques Kerberos. Pour certaines applications, ceci peut exiger un effort de programmation trop important. Pour d'autres, des modifications doivent être apportées au protocole utilisé entre les serveurs de réseau et leurs clients ; une fois encore, il se peut que l'effort requis soit trop important. En outre, il peut être impossible de faire fonctionner avec Kerberos certaines applications dont les sources ne sont pas accessibles.
- Kerberos suppose que vous utilisez des hôtes sécurisés sur un réseau non sécurisé. Son but principal est d'empêcher d'envoyer des mots de passe en texte clair dans le réseau. Si quelqu'un d'autre que l'utilisateur normal a physiquement accès à l'un des hôtes, et en particulier à celui qui délivre les tickets d'authentification, tout le système d'authentification Kerberos est menacé d'être compromis.
- Enfin, si vous décidez d'utiliser Kerberos sur votre réseau, sachez qu'il s'agit d'un pari du type "tout ou rien". Si l' *un* des services transmettant des mots de passe sous forme de texte en clair est encore utilisé, il reste possible d'intercepter des mots de passe et votre réseau ne tirera aucun avantage de l'utilisation de Kerberos. Pour sécuriser votre réseau avec Kerberos, vous devez **faire fonctionner avec Kerberos** *toutes* les applications qui envoient des mots de passe sous forme de texte en clair ou arrêter de les utiliser sur votre réseau.

9.3 Terminologie Kerberos

Comme tout système, Kerberos dispose de sa propre terminologie. Avant d'évoquer la manière dont il fonctionne, voici une liste des termes avec lesquels vous devrez vous familiariser :

cache de certificat d'identité ou fichier de ticket

Fichier contenant les clés nécessaires au cryptage des communications entre un utilisateur et divers services réseau. Kerberos 5 fournit un environnement permettant d'utiliser d'autres types de cache (par exemple, une mémoire partagée), mais les fichiers sont mieux pris en charge.

ciphertext

Données cryptées.

clé

Bloc de données utilisé pour le cryptage et le décryptage de données. Il est impossible de décrypter des données cryptées sans disposer de la clé appropriée, à moins d'être un génie en devinettes.

client

Entité sur le réseau (utilisateur, hôte ou application) pouvant obtenir un ticket Kerberos.

KDC (Key Distribution Center, centre distributeur de tickets)

Ordinateur émettant des tickets Kerberos, généralement exécuté sur le même hôte que le Serveur d'émission de tickets.

key table ou keytab

Fichier contenant une liste cryptée des "principaux" et de leurs clés respectives. Les serveurs extraient les clés dont ils ont besoin des fichiers keytab au lieu d'utiliser `kinit`. Le fichier keytab par défaut est `/etc/krb5.keytab`. La commande `kadmind` est le seul service connu utilisant n'importe quel autre fichier (il utilise `/var/kerberos/krb5kdc/kadm5.keytab`).

principal

Utilisateur ou service pouvant effectuer une authentification à l'aide de Kerberos. Un nom de principal a la forme "*root*[/*instance*]*@REALM*". Pour un utilisateur ordinaire, *root* correspond à l'ID de connexion. L'*instance* est facultative. Si le principal a une instance, il est séparé du root par une barre oblique ("/"). La chaîne vide ("") est une instance valide (qui diffère de l'instance *NULL* par défaut) mais son utilisation peut être source de confusion. Tous les éléments principaux d'une zone ont leur propre *clé*, dérivée de leur mot de passe (pour les utilisateurs) ou définie de façon aléatoire (pour les services).

Service

Programme ou ordinateur accessible via le réseau.

Service d'émission de tickets (TGS, ticket granting service)

Délivre les tickets pour un service demandé que l'utilisateur doit employer pour accéder au service en question. TGS fonctionne en réalité sur le même hôte que KDC.

texte en clair

Données non cryptées.

ticket

Ensemble temporaire de certificats d'identité électroniques indiquant l'identité d'un client pour un service particulier.

Ticket d'émission de tickets (TGT, ticket granting ticket)

Ticket spécial permettant au client d'obtenir des tickets supplémentaires sans les demander au KDC.

zone

Réseau utilisant Kerberos, composé d'un ou plusieurs serveurs (également appelés KDC) et d'un nombre (potentiellement très important) de clients.

9.4 Fonctionnement de Kerberos

Vous connaissez à présent quelques termes propres à Kerberos. Voici une explication simplifiée du fonctionnement d'un système d'authentification Kerberos :

Sur un réseau "normal" utilisant des mots de passe pour authentifier les utilisateurs, lorsqu'un utilisateur demande un service réseau nécessitant une authentification, il est invité à entrer son mot de passe. Celui-ci est transmis sous forme de texte en clair via le réseau, et l'accès au service réseau est autorisé.

Comme mentionné plus haut, le problème central résolu par Kerberos a trait à la manière d'utiliser les mots de passe d'authentification sans qu'ils transitent sur le réseau. Sur un réseau "kerbérisé", la base de données Kerberos contient les principaux et leurs clés (pour les utilisateurs, les clés sont dérivées des mots de passe). La base de données Kerberos contient également des clés pour tous les services réseau.

Lorsqu'un utilisateur d'un réseau "kerbérisé" se connecte sur son poste de travail, son principal est envoyé au KDC comme une demande de TGT. Cette demande peut être émise par le programme de connexion (de sorte qu'elle est transparente pour l'utilisateur) ou par le programme `kinit` une fois l'utilisateur connecté.

Le KDC vérifie la présence du principal dans sa base de données. Si le principal est trouvé, le KDC crée un TGT, le crypte à l'aide de la clé de l'utilisateur, puis le renvoie à ce dernier.

Le programme de connexion ou `kinit` décrypte le TGT à l'aide de la clé de l'utilisateur (qu'il recompose à partir du mot de passe). Défini pour expirer après un certain laps de temps, le TGT est stocké dans un cache de certificats d'identité. Un délai d'expiration est défini de manière à ce qu'un TGT compromis ne puisse être utilisé que pendant une certaine période de temps, généralement de huit heures (à la différence d'un mot de passe compromis qui peut être utilisé tant qu'il n'a pas été modifié). L'utilisateur n'a pas à entrer à nouveau son mot de passe tant que le TGT n'a pas expiré ou tant qu'il ne se déconnecte pas.

Lorsque l'utilisateur doit accéder à un service réseau, le TGT demande un ticket au TGS (Ticket Granting Service, service d'émission de tickets) fonctionnant sur le KDC. Le TGS émet un ticket pour le service souhaité, qui permet d'authentifier l'utilisateur.

Bien entendu, cette explication est très sommaire. Pour une explication plus approfondie du fonctionnement de Kerberos, reportez-vous à la Section 9.8, *Autres ressources*.

Remarque

Le bon fonctionnement de Kerberos dépend de certains services réseau. Premièrement, Kerberos a besoin d'une (vague) synchronisation d'horloge entre les ordinateurs du réseau. Si vous n'avez pas installé de programme de synchronisation d'horloge pour le réseau, vous allez devoir le faire. Etant donné que certains aspects de Kerberos reposent sur le DNS (Domain Name Service), veillez à ce que les entrées DNS et les hôtes sur votre réseau soient tous correctement configurés. Pour plus d'informations sur ces questions, reportez-vous au *Kerberos V5 System Administrator's Guide*, disponible aux formats PostScript et HTML dans `/usr/share/doc/krb5-server-<version-number>`.

9.5 Installation d'un serveur Kerberos sur Red Hat Linux 7.1

Si vous installez Kerberos, commencez par installer le(s) serveur(s). Si vous devez installer des serveurs esclaves, vous trouverez des détails relatifs à la configuration des relations entre les serveurs maître et esclaves dans le *Guide d'Installation de Kerberos 5* (dans le répertoire `/usr/share/doc/krb5-server-<version-number>`).

Pour installer un serveur Kerberos :

1. Assurez-vous que votre serveur est synchronisé est que le DNS est activé, puis installez Kerberos 5. Portez une attention particulière à la synchronisation entre le serveur Kerberos et ses clients. Si les montres du serveur et des clients diffèrent de plus de 5 minutes (vous pouvez configurer ce montant de défaut dans Kerberos 5), les clients Kerberos ne pourront pas authentifier leur serveur. Cette synchronisation de l'heure est nécessaire pour empêcher un attaquant d'utiliser un vieil authentificateur pour se masquer en utilisateur autorisé.

   Vous devriez installer un Protocole de temps de réseau (NTP) compatible avec le réseau client/serveur fonctionnant avec Red Hat Linux même si vous n'utilisez pas Kerberos. Red Hat Linux 7.1 contient le paquetage `ntp` qui fournit une installation facile. Pour plus d'informations sur NTP, reportez-vous à l'adresse http://www.eecis.udel.edu/~ntp.

2. Installez les paquetages `krb5-libs`, `krb5-server`, et `krb5-workstation` sur l'ordinateur dédié qui exécutera votre KDC. Cet ordinateur doit être sécurisé — idéalement, il ne devrait rien exécuter d'autre que le KDC.

   Pour disposer d'un utilitaire graphique permettant d'administrer Kerberos, installez également le paquetage `gnome-kerberos`. `gnome-kerberos` contient `krb5`, un outil pour la gestion de

tickets doté d'une interface graphique, et `gkadmin`, un outil pour la gestion de zones Kerberos également doté d'une interface graphique.

3. Modifiez les fichiers de configuration `/etc/krb5.conf` et `/var/kerberos/krb5kdc/kdc.conf` afin qu'ils reflètent le nom de votre zone (realm) et les mappages domaine-zone. Il est possible de créer une zone simple en remplaçant des instances de *EXAMPLE.COM* et *example.com* par votre nom de domaine (en respectant la casse) et en remplaçant le nom du KDC, *kerberos.example.com*, par celui de votre serveur Kerberos. Par convention, tous les noms de zone sont en majuscules et tous les noms d'hôte DNS et noms de domaine sont en minuscules. Pour plus de détails sur les formats de ces fichiers, reportez-vous aux pages du manuel les concernant.

4. Créez la base de données à l'aide de l'utilitaire `kdb5_util` à l'invite du shell :

```
/usr/kerberos/sbin/kdb5_util create -s
```

La commande `create` crée la base de données qui servira à stocker des clés pour votre zone Kerberos. Le commutateur `-s` force la création d'un fichier **stash** dans lequel est stockée la clé du serveur maître. A défaut de fichier stash dans lequel lire la clé, le serveur Kerberos (`krb5kdc`) invite l'utilisateur à entrer le mot de passe du serveur maître (permettant de regénérer la clé) à chaque démarrage.

5. Modifiez le fichier `/var/kerberos/krb5kdc/kadm5.acl`. `kadmind` utilise ce fichier pour déterminer les principaux ayant accès à la base de données Kerberos, ainsi que leur type d'accès. La plupart des organisations s'en tireront avec une seule ligne :

```
*/admin@EXAMPLE.COM  *
```

La plupart des utilisateurs seront représentés dans la base de données par un seul principal (avec une instance *NULL*, c'est-à-dire *joe@EXAMPLE.COM*). Avec cette configuration, les utilisateurs disposant d'un second principal avec une instance de *admin* (par exemple, *joe/admin@EXAMPLE.COM*) pourront contrôler totalement la base de données Kerberos de la zone.

Une fois `kadmind` démarré sur le serveur, n'importe quel utilisateur sera en mesure d'accéder à ses services en exécutant `kadmin` ou `gkadmin` sur n'importe quel client ou serveur de la zone. Toutefois, seuls les utilisateurs figurant dans le fichier `kadm5.acl` pourront modifier la base de données à leur guise, à l'exception de leur propre mot de passe.

Remarque

Les utilitaires `kadmin` et `gkadmin` communiquent avec le serveur `kadmind` via le réseau. Bien entendu, vous devez créer un principal avant de vous connecter au serveur sur le réseau pour l'administrer ; pour ce faire, utilisez la commande `kadmin.local` : elle est conçue spécialement pour être utilisée sur le même hôte que KDC et n'utilise pas Kerberos pour l'authentification.

Tapez la commande `kadmin.local` dans le terminal KDC pour créer le premier principal.

```
/usr/kerberos/sbin/kadmin.local -q "addprinc username/admin"
```

6. Démarrez Kerberos à l'aide des commandes suivantes :

```
/sbin/service krb5kdc start
/sbin/service kadmin start
/sbin/service krb524 start
```

7. Ajoutez des principaux pour les utilisateurs utilisant la commande `addprinc` de `kadmin` ou **Principal** de `gkadmin` =>option de menu **Add**. `kadmin` (et `kadmin.local` sur le maître KDC) est une interface de ligne de commande du système d'administration Kerberos. En tant que telle, de nombreuses commandes sont disponibles après le lancement du programme `kadmin`. Pour plus d'informations sur ce sujet, consultez la page `kadmin` du manuel.

8. Vérifiez si votre serveur émet des tickets. Commencez par exécuter `kinit` pour obtenir un ticket et stockez-le dans un fichier de cache de certificat d'identité. Utilisez ensuite `klist` pour afficher la liste des certificats d'identité dans votre cache et `kdestroy` pour supprimer le cache et les certificats d'identité qu'il contient.

Remarque

Par défaut, `kinit` essaie de vous authentifier à l'aide du nom de connexion sous lequel vous vous êtes connecté à votre système. Si cet utilisateur ne correspond pas à un principal figurant dans la base de données Kerberos, vous obtiendrez un message d'erreur. Dans ce cas, donnez simplement à `kinit` le nom de votre principal comme argument dans la ligne de commande. (`kinit` *`principal`*).

Une fois les étapes ci-dessus accomplies, votre serveur Kerberos doit être opérationnel. Il vous reste à présent à installer vos clients Kerberos.

9.6 Installation d'un client Kerberos 5 sur Red Hat Linux 7.1

L'installation d'un client Kerberos 5 est moins compliquée que l'installation d'un serveur. Vous devez, au minimum, installer les paquetages clients et fournir aux clients un fichier de configuration `krb5.conf` valide. Les versions "kerbérisées" de `rsh` et `rlogin` nécessiteront en outre certains changements de configuration.

1. Assurez-vous d'avoir installé une synchronisation d'heure entre les clients Kerberos et KDC. Pour plus d'informations sur ce sujet, reportez-vous à la section Section 9.5, *Installation d'un serveur Kerberos sur Red Hat Linux 7.1*. De plus, DNS devrait fonctionner correctement sur le client Kerberos avant l'installation des programmes client Kerberos.

2. Installez les paquetages `krb5-libs` et `krb5-workstation` sur tous les clients de votre zone. Vous devrez fournir votre propre version de `/etc/krb5.conf` pour les postes de travail clients ; habituellement, ce peut être le fichier `krb5.conf` utilisé par le KDC.

3. Avant qu'un poste de travail particulier de votre zone ne puisse permettre aux utilisateurs de se connecter à l'aide d'un `rsh` et d'un `rlogin` "kerbérisés", il faut que le paquetage `xinetd` soit installé sur ce poste de travail et que celui-ci ait son propre hôte principal dans la base de données Kerberos. Les programmes `kshd` et `klogind` du serveur devront également pouvoir accéder aux clés correspondant au principal de leur service.

   Utilisez `kadmin` pour ajouter un principal hôte pour le poste de travail. Dans ce cas, l'instance sera le nom d'hôte du poste de travail. Etant donné que vous ne devrez plus entrer le mot de passe pour ce principal et que vous ne souhaitez probablement pas vous donner la peine de trouver un mot de passe approprié, vous pouvez utiliser l'option `-randkey` afin que la commande `addprinc` de kadmin crée le principal et lui attribue une clé aléatoire :

   ```
   addprinc -randkey host/blah.example.com
   ```

   Le principal étant créé, vous pouvez à présent extraire les clés du poste de travail en exécutant `kadmin` *sur le poste de travail lui-même*, et en utilisant la commande `ktadd` de `kadmin` :

   ```
   ktadd -k /etc/krb5.keytab host/blah.example.com
   ```

   Pour pouvoir utiliser les versions "kerbérisées" de `rsh` et `rlogin`, vous devez utiliser ntsysv ou `chkconfig` afin d'activer `klogin`, `eklogin` et `kshell`.

4. D'autres services réseau "kerbérisés" devront également être démarrés. Pour disposer d'une connexion `telnet` "kerbérisée", vous devez utiliser ntsysv ou `chkconfig` pour activer `ktelnet`.

Pour disposer également d'un accès FTP, créez et extrayez une clé pour un principal à l'aide d'un root ftp, ainsi que l'instance définie sur le nom d'hôte du serveur FTP. Utilisez ensuite ntsysv ou `chkconfig` pour activer `gssftp`.

Le serveur IMAP inclus dans le paquetage `imap` utilise une authentification GSS-API à l'aide de Kerberos 5 s'il trouve la clé appropriée dans `/etc/krb5.keytab`. Le root pour le principal doit être `imap` . Le serveur CVS utilise un principal avec un root `cvs` et est, pour le reste, identique à un `pserver`.

Voilà tout ce dont vous avez besoin pour installer une zone Kerberos simple.

9.7 Kerberos et les modules d'authentification enfichables (PAM)

Actuellement, les services "kerbérisés" n'utilisent pas du tout les PAM — un serveur "kerbérisé" ignore complètement les PAM. Les applications utilisant des PAM peuvent se servir de Kerberos pour vérifier les mots de passe si le module `pam_krb5` (contenu dans le paquetage `pam_krb5`) est installé. Le paquetage `pam_krb5` contient des exemples de fichier de configuration qui permettent à des services tels que `login` et `gdm` d'authentifier des utilisateurs et d'obtenir des certificats d'identité initiaux à l'aide de leurs mots de passe. Pour autant que l'accès aux serveurs de réseau s'effectue toujours à l'aide de services "kerbérisés" (ou de services utilisant GSS-API, par exemple IMAP), le réseau peut être considéré comme raisonnablement sûr.

Un administrateur prudent n'ajoutera pas la vérification de mot de passe Kerberos aux services réseau, car la plupart des protocoles utilisés par ces services ne cryptent pas le mot de passe avant de l'envoyer sur le réseau — ce que vous souhaitez sans doute éviter.

9.8 Autres ressources

Comprendre, implémenter et configurer Kerberos peut constituer un défi pour les nouveaux utilisateurs. Pour plus d'informations et d'exemples sur l'utilisation de Kerberos, reportez-vous aux sources d'information suivantes :

9.8.1 Documentation installée

- `/usr/share/doc/krb5-server-<`*`version-number`*`>` — Les *Guide d'installation Kerberos V5* et *Guide de l'administrateur de système Kerberos V5*, aux formats PostScript et HTML, sont installés dans `krb5-server`.
- `/usr/share/doc/krb5-workstation-<`*`version-number`*`>` — Le *Guide de l'utilisateur Kerberos V5 UNIX*, aux formats PostScript et HTML, est installé dans `krb5-workstation`.

9.8.2 Sites Web utiles

- http://web.mit.edu/kerberos/www — Page d'accueil de Kerberos sur le site Web du MIT.
- http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html — Le Forum Aux Questions (FAQ) de Kerberos.
- ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS — Lien vers une version PostScript de *Kerberos: An Authentication Service for Open Network Systems* par Jennifer G. Steiner, Clifford Neuman, et Jeffrey I. Schiller, document original décrivant Kerberos.
- http://web.mit.edu/kerberos/www/dialogue.html — *Designing an Authentication System: a Dialogue in Four Scenes* écrit par Bill Bryant en 1988, puis modifié par Theodore Ts'o en 1997. Ce document relate une conversation entre deux développeurs réfléchissant à la création d'un système d'authentification de type Kerberos. La présentation sous forme de dialogue et l'approche progressive de la question en font un bon point de départ pour les néophytes.
- http://www.ornl.gov/~jar/HowToKerb.html — Conseil pratique concernant la "kerbérisation" de votre réseau

10 Installation et configuration de Tripwire

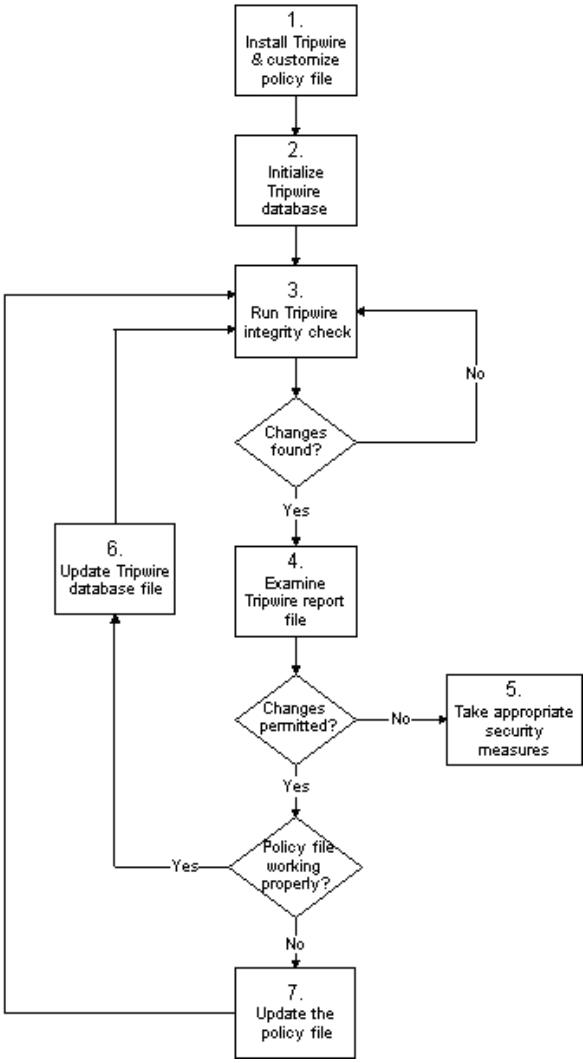
Le logiciel Tripwire aide à assurer l'intégrité de répertoires et de systèmes de fichiers importants en identifiant tout changement apporté à ceux-ci. Les options de configuration de Tripwire comprennent notamment l'envoi de messages d'alerte par courrier électronique lorsqu'un fichier spécifique est modifié et la vérification automatique de l'intégrité du système par l'entremise de `cron`. L'utilisation de Tripwire pour détecter des intrusions dans le système et analyser les dommages causés, vous aide à contrôler les changements apportés au système et accélère la vitesse de sa remise en état lorsqu'il est victime d'une violation, en réduisant le nombre de fichiers devant être restaurés pour le réparer.

Tripwire compare des fichiers et des répertoires avec des informations, telles que des emplacements de fichier, des dates de modification de fichier et d'autres données de ce genre, contenues dans une base de données référentielle. Il crée cette base de données en faisant un instantané de répertoires et de fichiers spécifiques dont l'état est certain et sécuritaire. (Pour avoir un maximum de sécurité, Tripwire devrait être installé et sa base de données référentielle créée avant que le système ne coure le risque d'être victime d'une intrusion.) Une fois la base de données référentielle créée, Tripwire compare le système en cours avec cette base de données et produit un rapport des modifications, des suppressions et des ajouts effectués.

10.1 Comment utiliser Tripwire

L'organigramme suivant illustre comment utiliser Tripwire :

Figure 10–1 Comment utiliser Tripwire



Suivez les étapes suivantes pour installer, utiliser et maintenir correctement Tripwire :

1. *Installation de Tripwire et personnalisation du fichier de politiques* — si ce n'est déjà fait, installez le RPM `tripwire` (voir la Section 10.2.1, *Instructions d'installation du RPM*). Ensuite, personnalisez les exemples de fichiers de configuration (`/etc/tripwire/twcfg.txt`) et de politiques (`/etc/tripwire/twpol.txt`) et exécutez le script de configuration (`/etc/tripwire/twinstall.sh`). Pour plus de détails, reportez-vous à la Section 10.2.2, *Instructions à suivre après l'installation*.

2. *Initialisation de la base de données de Tripwire* — créez une base de données des fichiers système critiques devant être contrôlés en fonction des directives contenues dans le tout nouveau fichier de politiques Tripwire signé (`/etc/tripwire/tw.pol`). Consultez la Section 10.7, *Initialisation de la base de données* pour en savoir plus.

3. *Exécution d'une vérification d'intégrité Tripwire* — comparez la base de données de Tripwire nouvellement créée avec les fichiers système pour vérifier s'il en manque ou si certains d'entre eux ont été modifiés. Reportez-vous à la Section 10.8, *Exécution d'une vérification d'intégrité* pour avoir plus de renseignements à ce sujet.

4. *Analyse d'un fichier rapport de Tripwire* — visualisez un fichier rapport Tripwire au moyen de `twprint` afin d'identifier les violations d'intégrité du système. Pour en savoir plus, reportez-vous à la la Section 10.9, *Impression des rapports*.

5. *Prise de mesures appropriées* — si les fichiers contrôlés ont été modifiés de façon non voulue, deux choix s'offrent à vous : vous pouvez remplacer les fichiers originaux par des copies de sauvegarde ou tout simplement réinstaller le programme.

6. *Mise à jour du fichier de la base de données de Tripwire* — si les violations de l'intégrité du système sont intentionnelles, dans le cas où vous avez modifié un fichier volontairement ou remplacé un programme donné par exemple, vous devez indiquer au fichier de la base de données Tripwire de ne plus souligner ces violations dans les rapports suivants. Pour plus de détails, veuillez lire la Section 10.10, *Mise à jour de la base de données après une vérification d'intégrité*.

7. *Mise à jour du fichier de politiques de Tripwire* — si vous avez besoin de changer la liste des fichiers contrôlés par Tripwire ou la façon dont les violations d'intégrité sont traitées, vous devez mettre à jour votre exemple de fichier de politiques (`/etc/tripwire/twpol.txt`), régénérer une copie signée (`/etc/tripwire/tw.pol`) et mettre à jour votre base de données Tripwire. Pour plus de renseignements là-dessus, reportez-vous à la Section 10.11, *Mise à jour du fichier de politiques*.

Pour obtenir des instructions plus détaillées sur ces différentes étapes, consultez les sections de ce chapitre les concernant.

10.2 Instructions d'installation

Une fois installé, Tripwire doit être initialisé correctement afin de contrôler de façon efficace vos fichiers. Les sections qui suivent expliquent comment installer le programme (s'il n'est pas déjà sur votre système) et comment initialiser la base de données de Tripwire.

10.2.1 Instructions d'installation du RPM

La façon la plus simple d'installer Tripwire est d'installer le RPM `tripwire` lors du processus d'installation de Red Hat Linux 7.1. Toutefois, si Red Hat Linux 7.1 est déjà installée, vous pouvez utiliser RPM, Gnome-RPM ou Kpackage pour installer le RPM Tripwire à partir des CD-ROMs de Red Hat Linux 7.1. Les étapes suivantes illustrent le processus d'installation faisant usage de RPM :

1. Localisez le répertoire `RedHat/RPMS` sur le CD-ROM de Red Hat Linux 7.1.
2. Localisez le RPM binaire `tripwire` en tapant `ls -l tripwire*` dans le répertoire `RedHat/RPMS`.
3. Entrez `rpm -Uvh <`*`nom`*`>` (où <*nom*> correspond au nom du RPM Tripwire trouvé à l'étape 2).
4. Une fois le RPM `tripwire` installé, suivez les instructions ci-dessous, qui soulignent ce qui doit être fait après l'installation.

Remarque

La documentation fournie et le fichier `README` sont situés dans `/usr/share/doc/tripwire-<`*`version-number`*`>`. Ces documents contiennent d'importantes informations sur le fichier de politiques par défaut et d'autres sujets.

10.2.2 Instructions à suivre après l'installation

Le RPM `tripwire` installe les fichiers du programme nécessaires au bon fonctionnement du logiciel. Une fois Tripwire installé, vous devez le configurer pour votre système, comme l'expliquent les étapes suivantes :

1. Si vous savez déjà quelles modifications doivent être apportées au fichier de configuration (`/etc/tripwire/twcfg.txt`) et au fichier de politiques (`/etc/tripwire/twpol.txt`), effectuez-les maintenant.

Remarque

Bien que vous deviez modifier les fichiers de configuration et de politiques pour personnaliser Tripwire selon vos besoins spécifiques, la modification de ces fichiers n'est pas obligatoire pour pouvoir utiliser Tripwire. Cependant, si vous prévoyez de les modifier, vous devez apporter les changements avant d'exécuter le script de configuration (`/etc/tripwire/twinstall.sh`) car si vous le faites après l'exécution du script de configuration, vous devrez l'exécuter à nouveau avant d'initialiser le fichier de la base de données. Rappelez-vous que vous *pouvez* modifier les fichiers de configuration et de politiques *après* avoir initialisé le fichier de la base de données et exécuté une vérification d'intégrité.

---

2. Entrez `/etc/tripwire/twinstall.sh` à la ligne de commande en tant que root et appuyez sur la touche [Entrée] pour exécuter le script de configuration. Le script `twinstall.sh` vous fait parcourir le processus permettant de définir des phrases d'accès, générer des clés cryptographiques qui protègent les fichiers de configuration et de politiques de Tripwire et de signer ces fichiers. Reportez-vous à la Section 10.6, *Sélection des phrases d'accès* pour avoir plus de renseignements concernant la définition des phrases d'accès.

Remarque

Une fois codés et signés, le fichier de configuration (`/etc/tripwire/tw.cfg`) et le fichier de politiques (`/etc/tripwire/tw.pol`), générés lors de l'exécution du script `/etc/tripwire/twinstall.sh`, ne doivent pas être renommés ou déplacés.

---

3. Initialisez le fichier de la base de données de Tripwire en entrant la commande `/usr/sbin/tripwire --init` à la ligne de commande.

4. Effectuez une première vérification d'intégrité du système pour comparer la nouvelle base de données de Tripwire avec vos fichiers système, au moyen de la commande `/usr/sbin/tripwire --check` à la ligne de commande et vérifiez s'il y a des erreurs dans le rapport généré.

Une fois ces étapes réalisées avec succès, Tripwire possède l'instantané référentiel de votre système de fichiers dont il a besoin pour contrôler les changements apportés aux fichiers importants. De plus, le

RPM `tripwire` ajoute un fichier appelé `tripwire-check` au répertoire `/etc/cron.daily`, qui a pour but d'effectuer automatiquement une vérification d'intégrité journalière.

10.3 Emplacements des fichiers

Avant de commencer à utiliser Tripwire, vous devez savoir où se trouvent les fichiers importants de cette application. Tripwire stocke ses fichiers à différents endroits en fonction de leur rôle :

- Le répertoire `/usr/sbin` stocke les programmes `tripwire`, `twadmin` et `twprint`.
- Le répertoire `/etc/tripwire` contient la clé du site et la clé locale (fichier `*.key`), le script d'initialisation (`twinstall.sh`), ainsi que les fichiers de configuration et de politiques et leur exemple.
- Le répertoire `/var/lib/tripwire` contient la base de données Tripwire des fichiers de votre système (`*.twd`) et un répertoire `report` dans lequel les rapports Tripwire sont enregistrés. Les rapports Tripwire, appelés *`nom_hôte-date_du_rapport-heure_du_rapport`*`.twr`, établissent les différences entre la base de données de Tripwire et les fichiers de votre système.

10.4 Composants de Tripwire

Le fichier de politiques de Tripwire est un fichier texte qui contient des commentaires, des règles, des directives et des variables. Ce fichier dicte la façon dont Tripwire doit vérifier votre système. Chaque règle dans le fichier de politiques spécifie un objet système devant être contrôlé. Les règles indiquent également quels changements rapporter ou ignorer.

Les objets système sont les fichiers et les répertoires que vous désirez contrôler. Chaque objet est identifié par un nom. Une propriété fait référence à une caractéristique unique d'un objet que le logiciel Tripwire peut surveiller. Les directives contrôlent le traitement conditionnel d'ensembles de règles dans un fichier de politiques. Durant l'installation, le fichier texte de politiques (`/etc/tripwire/twpol.txt`) est chiffré et renommé, devenant ainsi le fichier de politiques actif (`/etc/tripwire/tw.pol`).

Lorsqu'il est initialisé pour la première fois, Tripwire utilise les règles du fichier de politiques signé pour créer le fichier de la base de données (`/var/lib/tripwire/`*`nom_d'hôte`*`.twd`). Le fichier de la base de données est un instantané référentiel du système à un moment où son état est certain et sécuritaire. Tripwire compare ce fichier référentiel avec le système en cours pour déterminer si des changements ont eu lieu. Cette comparaison est appelée **vérification d'intégrité**.

Lorsque vous effectuez une vérification d'intégrité, Tripwire produit des fichiers rapport, situés dans le répertoire `/var/lib/tripwire/report`. Ces fichiers rapport indiquent toutes les modifications apportées aux fichiers violant les règles du fichier de politiques trouvées lors de la vérification d'intégrité.

Le fichier de configuration de Tripwire (`/etc/tripwire/tw.cfg`) stocke des informations spécifiques au système, telles que l'emplacement des fichiers de données de Tripwire. Tripwire génère les informations nécessaires au fichier de configuration lors de l'installation, mais l'administrateur système peut changer les paramètres du fichier de configuration en tout temps après cela. Notez qu'un fichier de configuration modifié doit être signé, tout comme le fichier de politiques d'ailleurs, afin de pouvoir être utilisé par défaut.

Les variables **POLFILE**, **DBFILE**, **REPORTFILE**, **SITEKEYFILE** et **LOCALKEYFILE** du fichier de configuration spécifient les emplacements du fichier de politiques, du fichier de la base de données, des fichiers rapport et des fichiers des clés du site et locale. Ces variables sont définies par défaut au moment de l'installation. Si vous modifiez le fichier de configuration et laissez l'une de ces variables non définie, le fichier de configuration sera considéré comme non valide par Tripwire. Cela cause d'ailleurs une erreur lors de l'exécution de `tripwire` et la fermeture du programme.

Veuillez prendre note que le fichier de configuration modifié doit être signé, tout comme le fichier de politiques, afin de pouvoir être utilisé par Tripwire. Reportez-vous à la Section 10.11.1, *Signature du fichier de configuration* pour avoir les instructions concernant la signature du fichier de configuration.

10.5 Modification du fichier de politiques

Vous pouvez spécifier la façon dont Tripwire contrôle votre système en modifiant le fichier de politiques de Tripwire (`twpol.txt`). Si vous modifiez ce fichier en fonction de la configuration particulière de votre système, vous augmentez l'efficacité des rapports de Tripwire car vous minimisez les fausses alertes concernant des fichiers ou des programmes que vous n'utilisez pas, mais que Tripwire identifie comme étant modifiés ou manquants.

Localisez le fichier de politiques par défaut dans `/etc/tripwire/twpol.txt`. Un exemple de fichier de politiques (situé dans `/usr/share/doc/tripwire-<`*`numéro-version`*`>/policyguide.txt`) est aussi inclus pour vous aider à apprendre le langage des politiques. Lisez le fichier d'exemples de politiques pour avoir des instructions sur la façon de modifier le fichier de politiques par défaut.

Si vous modifiez le fichier de politiques immédiatement après avoir installé le paquetage `tripwire`, assurez-vous de taper `/etc/tripwire/twinstall.sh` pour exécuter le script de configuration. Ce script signe le fichier de politiques modifié et le renomme `tw.pol`. Il s'agit du fichier de politiques actif utilisé par le programme `tripwire` lorsqu'il est exécuté.

Si vous modifiez l'exemple de fichier de politiques après avoir exécuté le script de configuration, veuillez lire la Section 10.11, *Mise à jour du fichier de politiques* pour savoir comment le signer et le faire devenir le fichier `tw.pol` requis.

Remarque

Si vous modifiez l'exemple de fichier de politiques, il n'est pas utilisé par Tripwire tant qu'il n'est pas signé, chiffré et devenu le nouveau fichier `/etc/tripwire/tw.pol` (voir la Section 10.11, *Mise à jour du fichier de politiques*).

10.6 Sélection des phrases d'accès

Les fichiers Tripwire sont signés ou chiffrés au moyen de la clé locale et de la clé du site, qui empêchent ainsi que les fichiers de configuration, de politiques, de la base de données et des rapports ne soient visualisés ou modifiés par des individus connaissant les phrases d'accès locale ou du site. Cela signifie qu'un intrus ayant l'accès root à votre système ne peut modifier les fichiers Tripwire pour effacer ses traces sans avoir également les phrases d'accès. Lorsque vous choisissez des phrases d'accès, vous devez utiliser un minimum de 8 caractères alphanumériques et symboliques pour chaque phrase. La longueur maximum d'une phrase d'accès est de 1023 caractères. Les guillemets ne devraient pas être utilisés comme caractères pour les phrases d'accès. De plus, assurez-vous que vos phrases d'accès sont complètement différentes du mot de passe root du système.

La clé locale et la clé du site devraient toutes deux avoir leur propre phrase d'accès. La phrase d'accès de la clé du site protège la clé du site, utilisée pour signer les fichiers de configuration et de politiques de Tripwire, alors que la clé locale signe les fichiers de la base de données et des rapports de Tripwire.

Mettez vos phrases d'accès en lieu sûr. *Il n'existe aucune façon de déchiffrer un fichier signé si vous oubliez ou perdez vos phrases d'accès.* Si cela devait se produire, les fichiers seraient alors inutilisables et vous devriez exécuter à nouveau le script de configuration, ce qui initialise encore une fois la base de données de Tripwire.

10.7 Initialisation de la base de données

Lorsque la base de donnée est initialisée, Tripwire crée un ensemble d'objets du système de fichiers en se basant sur les règles contenues dans le fichier de politiques. Cette base de données est utilisée comme référence lors des vérifications d'intégrité.

Pour initialiser la base de données de Tripwire, utilisez la commande suivante :

```
/usr/sbin/tripwire --init
```

De nombreuses minutes peuvent s'écouler avant que la commande ne soit exécutée.

10.8 Exécution d'une vérification d'intégrité

Lors d'une vérification d'intégrité, Tripwire compare les objets actuels du système de fichiers avec leurs propriétés, qui sont enregistrées dans la base de données. Les violations sont imprimées sur la sortie standard et enregistrées dans un fichier rapport accessible par la suite au moyen de `twprint`. Pour plus de détails sur la visualisation des rapports de Tripwire, consultez la Section 10.9, *Impression des rapports*.

Une option de configuration de messagerie électronique dans le fichier de politiques permet d'envoyer des messages à des adresses spécifiques lorsque certaines violations de l'intégrité du système sont découvertes. Reportez-vous à la Section 10.12, *Tripwire et courrier électronique* pour savoir comment faire.

Utilisez la commande suivante pour effectuer une vérification d'intégrité :

```
/usr/sbin/tripwire --check
```

En général, cette commande prend un peu de temps avant d'être exécutée, en raison du nombre de fichiers à contrôler.

10.9 Impression des rapports

La commande `twprint -m r` affiche le contenu d'un rapport Tripwire en texte en clair. Vous devez préciser à `twprint` quel rapport afficher.

Une commande `twprint` pour imprimer des rapports Tripwire ressemble à ce qui suit (sur une seule ligne) :

```
/usr/sbin/twprint -m r --twrfile
          /var/lib/tripwire/report/<nom>.twr
```

L'option `-m r` de cette commande indique à `twprint` de décoder un rapport Tripwire. L'option `--twrfile` indique à `twprint` d'utiliser un fichier rapport Tripwire spécifique.

Le nom du rapport Tripwire que vous voulez visualiser contient le nom de l'hôte que Tripwire a contrôlé pour générer le rapport, ainsi que la date et l'heure de sa création. Vous pouvez consulter des rapports enregistrés précédemment en tout temps. Pour cela, vous n'avez qu'à taper `ls /var/lib/tripwire/report` pour faire apparaître une liste de rapports Tripwire.

Les rapports Tripwire peuvent être assez longs, selon le nombre de violations trouvées ou d'erreurs générées. Voici à quoi peut ressembler le début d'un de ces rapports :

```
Tripwire(R) 2.3.0 Integrity Check Report
```

```
Report generated by:          root
Report created on:            Fri Jan 12 04:04:42 2001
Database last updated on:     Tue Jan  9 16:19:34 2001

===============================================================================
Report Summary:
===============================================================================
Host name:                    some.host.com
Host IP address:              10.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/some.host.com.twd
Command line used:            /usr/sbin/tripwire --check

===============================================================================
Rule Summary:
===============================================================================
-------------------------------------------------------------------------------
Section: Unix File System
-------------------------------------------------------------------------------
  Rule Name                Severity Level    Added    Removed  Modified
  ---------                --------------    -----    -------  --------
  Invariant Directories    69                0        0        0
  Temporary directories    33                0        0        0
* Tripwire Data Files      100               1        0        0
  Critical devices         100               0        0        0
  User binaries            69                0        0        0
  Tripwire Binaries        100               0        0        0
```

10.9.1 Utilisation de `twprint` pour visualiser la base de données de Tripwire

Vous pouvez également utiliser `twprint` pour visualiser la base de données complète ou certaines informations sur des fichiers de votre choix dans la base de données de Tripwire. C'est très pratique pour avoir une idée de la quantité d'informations contrôlées par Tripwire sur votre système.

Pour visualiser la base de données complète de Tripwire, entrez cette commande :

```
/usr/sbin/twprint -m d --print-dbfile | less
```

Vous obtenez ainsi une grande quantité de données et les premières lignes que vous voyez ressemblent à ceci :

```
Tripwire(R) 2.3.0 Database
```

```
Database generated by:        root
Database generated on:        Tue Jan  9 13:56:42 2001
Database last updated on:     Tue Jan  9 16:19:34 2001

===============================================================
Database Summary:
===============================================================
Host name:                    some.host.com
Host IP address:              10.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/some.host.com.twd
Command line used:            /usr/sbin/tripwire --init

===============================================================
Object Summary:
===============================================================
---------------------------------------------------------------
# Section: Unix File System
---------------------------------------------------------------
     Mode        UID          Size       Modify Time
     ------      ----------   ---------- ----------
 /
     drwxr-xr-x  root (0)     XXX        XXXXXXXXXXXXXXXXX
 /bin
     drwxr-xr-x  root (0)     4096       Mon Jan  8 08:20:45 2001
 /bin/arch
     -rwxr-xr-x  root (0)     2844       Tue Dec 12 05:51:35 2000
 /bin/ash
     -rwxr-xr-x  root (0)     64860      Thu Dec  7 22:35:05 2000
 /bin/ash.static
     -rwxr-xr-x  root (0)     405576     Thu Dec  7 22:35:05 2000
```

Pour avoir des renseignements sur un fichier en particulier, contrôlé par Tripwire, tel que `/etc/hosts`, tapez une commande `twprint` différente :

```
/usr/sbin/twprint -m d --print-dbfile /etc/hosts
```

Voici à quoi ressemble le résultat :

```
Object name:  /etc/hosts

Property:               Value:
-------------           -----------
```

```
Object Type             Regular File
Device Number           773
Inode Number            216991
Mode                    -rw-r--r--
Num Links               1
UID                     root (0)
GID                     root (0)
```

Consultez la page de manuel `twprint` pour connaître d'autres options.

10.10 Mise à jour de la base de données après une vérification d'intégrité

Lorsque Tripwire décèle des violations du système à la suite d'une vérification d'intégrité, vous devez d'abord déterminer si ces violations sont causées par des brèches du système de sécurité ou si elles sont provoquées de façon autorisée. Si, par exemple, vous avez récemment installé une application ou modifié des fichiers système critiques, Tripwire rapporte (avec raison) ces violations lors de la vérification d'intégrité. Dans ce cas précis, vous devez mettre à jour votre base de données Tripwire de sorte que ces changements ne soient plus considérés comme des violations du système. Toutefois, si des changements non autorisés ont été apportés à des fichiers système et provoquent des violations lors de la vérification d'intégrité, vous devez alors restaurer les fichiers originaux à partir d'une copie de sauvegarde ou réinstaller le programme.

Pour mettre à jour votre base de données Tripwire, afin qu'elle accepte les violations trouvées dans un rapport, vous devez spécifier quel rapport vous désirez utiliser pour la mise à jour de la base de données. Assurez-vous toujours d'utiliser le rapport le plus récent lorsque vous donnez la commande d'intégrer ces violations valides à la base de données. Tapez la commande suivante (sur une seule ligne), où *nom* correspond au nom du rapport à utiliser :

```
/usr/sbin/tripwire --update --twrfile
          /var/lib/tripwire/report/<nom>.twr
```

Tripwire affiche le rapport au moyen de l'éditeur de texte par défaut (spécifié dans le fichier de configuration de Tripwire à la ligne **EDITOR**). C'est à ce moment que vous avez la possibilité de désélectionner les fichiers que vous ne désirez pas inclure dans la mise à jour de la base de données Tripwire. Il est important que vous ne permettiez qu'aux violations autorisées du systèmes d'être changées dans la base de données.

Tous les fichiers proposés pour la mise à jour de la base de données Tripwire sont précédés d'un `[x]`. Si vous voulez exclure spécialement une violation valide afin qu'elle ne fasse pas partie de la mise à jour de la base de données Tripwire, enlevez le `x`. Pour accepter le changement d'un fichier précédé d'un `x`, écrivez le fichier dans l'éditeur de texte et quittez-le. Ce faisant, vous indiquez à Tripwire de

modifier sa base de données et de ne plus rapporter les fichiers indiqués comme étant des violations du système.

Par exemple, l'éditeur de texte par défaut de Tripwire est `vi`. Pour écrire le fichier dans `vi` et apporter les changements à la base de données de Tripwire lorsque vous faites sa mise à jour à l'aide d'un rapport donné, tapez `:wq` dans le mode de commande de `vi` et appuyez sur la touche [Entrée]. On vous demande alors de fournir votre phrase d'accès. Ensuite, un nouveau fichier de la base de données est créé pour inclure les violations valides du système.

Une fois la nouvelle base de données Tripwire créée, les violations d'intégrité venant tout juste d'être autorisées ne seront plus indiquées lors des vérifications d'intégrité successives.

10.11 Mise à jour du fichier de politiques

Si vous désirez changer les fichiers que Tripwire enregistre dans sa base de données ou modifier la sévérité avec laquelle les violations sont rapportées, vous devez modifier le fichier de politiques de Tripwire.

Premièrement, apportez tous les changements nécessaires à l'exemple de fichier de politiques (`/etc/tripwire/twpol.txt`). L'un des changements couramment apportés à ce fichier est d'indiquer (mettre un # devant) tous les fichiers qui n'existent pas sur le système, de sorte qu'ils ne puissent provoquer un message d'erreur `file not found` dans les rapports de Tripwire. Si, par exemple, votre système ne possède pas le fichier `/etc/smb.conf`, vous pouvez spécifier à Tripwire de ne pas essayer de le trouver en mettant un # devant sa ligne dans `twpol.txt`, comme ceci :

```
#     /etc/smb.conf                       -> $(SEC_CONFIG) ;
```

Ensuite, vous devez indiquer à Tripwire de générer un nouveau fichier `/etc/tripwire/tw.pol` signé et puis un fichier mis à jour de la base de données en fonction des nouvelles informations contenues dans le fichier de politiques. Imaginons que `/etc/tripwire/twpol.txt` est le fichier de politiques modifié. Il faudrait alors utiliser la commande suivante :

```
/usr/sbin/twadmin --create-polfile -S site.key /etc/tripwire/twpol.txt
```

Puis, on vous demande la phrase d'accès du site, après quoi le fichier `twpol.txt` est analysé et signé.

Il est très important que vous mettiez à jour votre base de données Tripwire après la création d'un nouveau fichier `/etc/tripwire/tw.pol`. La façon la plus efficace pour faire cette opération est d'éliminer votre base de données Tripwire existante et d'en créer une nouvelle au moyen du nouveau fichier de politiques.

Si votre fichier de base de données Tripwire s'appelle `wilbur.domain.com.twd`, entrez cette commande :

```
rm /var/lib/tripwire/wilbur.domain.com.twd
```

Ensuite, entrez la commande suivante pour créer une nouvelle base de données :

```
/usr/sbin/tripwire --init
```

Une nouvelle base de donnée est ainsi créée selon les les instructions renfermées dans le nouveau fichier de politiques. Pour vous assurer que la base de données a été modifiée correctement, faites une première vérification d'intégrité manuellement et visualisez le contenu du rapport produit. Consultez la Section 10.8, *Exécution d'une vérification d'intégrité* et la Section 10.9, *Impression des rapports* pour avoir des instructions plus spécifiques là-dessus.

10.11.1 Signature du fichier de configuration

Le fichier texte contenant les changements du fichier de configuration (généralement `/etc/tripwire/twcfg.txt`) doit être signé afin qu'il remplace le fichier `/etc/tripwire/tw.cfg` et qu'il soit utilisé par Tripwire lors de l'exécution des vérifications d'intégrité. Tripwire ne reconnaît aucun changement de configuration tant que le fichier texte de configuration n'est pas correctement signé et utilisé à la place du fichier `/etc/tripwire/tw.pol`.

Si votre fichier texte de configuration modifié est `/etc/tripwire/twcfg.txt`, tapez la commande suivante pour le signer et faire en sorte qu'il remplace le fichier `/etc/tripwire/tw.pol` existant :

```
/usr/sbin/twadmin --create-cfgfile -S site.key /etc/tripwire/twcfg.txt
```

Etant donné que le fichier de configuration ne modifie pas les politiques Tripwire ou les fichiers qu'il contrôle, il est inutile de régénérer la base de données des fichiers système contrôlés.

10.12 Tripwire et courrier électronique

Tripwire peut envoyer des messages électroniques d'alerte si un type de règle spécifié contenu dans le fichier de politiques est enfreint. Pour configurer Tripwire de sorte qu'il exécute cette fonction, vous devez d'abord connaître l'adresse électronique du destinataire des messages en cas de violation et le nom de la règle que vous voulez surveiller. Notez également que sur les systèmes importants ayant plusieurs administrateurs système, vous pouvez faire en sorte que des groupes d'individus différents soient avertis selon les violations commises ou que personne ne soit averti lors de violations mineures.

Une fois que vous savez qui avertir et pour quelles raisons, ajoutez une ligne **emailto=** dans la section des directives des règles de chaque règle désirée. Vous n'avez qu'à ajouter une virgule après la ligne **severity=** d'une règle désirée et entrer **emailto=** sur la ligne suivante, suivi des adresses électroniques des personnes à qui vous voulez qu'un rapport de violation pour cette règle soit envoyé. Les messages seront envoyés à plus d'une personne si plus d'une adresse est spécifiée et que les adresses sont séparées par un point-virgule.

Par exemple, si vous désirez avertir deux administrateurs, Sam et Bob, lorsqu'un programme de connexion au réseau est modifié, changez la directive de la règle des programmes de connexion au réseau dans le fichier de politiques de sorte qu'elle ressemble à ceci :

```
(
  rulename = "Networking Programs",
  severity = $(SIG_HI),
  emailto = bob@domain.com;sam@domain.com
)
```

Après la génération d'un nouveau fichier de politiques signé à partir du fichier `/etc/tripwire/twpol.txt`, des messages sont envoyés aux adresses électroniques indiquées dès qu'il y a violation des règles spécifiées. Si vous désirez avoir plus de détails sur la façon de signer votre fichier de politiques, reportez-vous à la Section 10.11, *Mise à jour du fichier de politiques*.

10.12.1 L'envoi d'un message électronique test

Afin de vous assurer que la configuration de l'envoi de messages électroniques d'avertissement est correcte et que Tripwire est en mesure d'envoyer les messages, utilisez la commande suivante :

```
/usr/sbin/tripwire --test --email vos@adresses_électroniques
```

Un message est ainsi envoyé immédiatement par le programme `tripwire` aux adresses électroniques indiquées.

10.13 Autres ressources

Tripwire peut également accomplir des tâches dont nous n'avons pas parlé au cours de ce chapitre. Aussi, pour en apprendre davantage sur Tripwire, nous vous invitons à consulter les sources d'informations supplémentaires énumérées ci-dessous.

10.13.1 Documentation déjà installée

- `/usr/share/doc/tripwire-<version-number>` — excellent point de départ pour apprendre à personnaliser les fichiers de configuration et de politiques dans le répertoire `/etc/tripwire`.
- De plus, lisez les pages de manuel `tripwire`, `twadmin` et `twprint` pour obtenir de l'aide sur l'utilisation de ces programmes utilitaires.

10.13.2 Sites Web utiles

- http://www.tripwire.org — site Web du projet source ouverte Tripwire, où vous trouverez les toutes dernières nouvelles sur cette application et une liste de questions fréquemment posées.

11 Protocole SSH

Ce chapitre parle des avantages du protocole SSH™, de la séquence d'événements se produisant lors d'une connexion sécurisée à un système distant, des différentes couches de SSH et des méthodes pour assurer que les utilisateurs qui se connectent à votre système utilisent le protocole SSH.

Les méthodes communément utilisées pour se connecter à distance à un autre système au moyen d'un shell (`telnet`, `rlogin` ou `rsh`) ou pour copier des fichiers entre ordinateurs hôtes (`ftp` ou `rcp`) ne sont pas sécurisées et devraient donc être évitées. Vous devriez plutôt vous connecter à un ordinateur hôte distant au moyen d'un shell sécurisé ou d'un réseau privé virtuel chiffré. En utilisant des méthodes sécurisées pour vous connecter à distance à d'autres systèmes, vous réduisez les risques en matière de sécurité, pour votre système et le système distant.

11.1 Introduction

SSH (ou *S*ecure *SH*ell) est un protocole servant à créer une connexion sécurisée entre deux systèmes. Grâce à SSH, un ordinateur client peut initier une connexion avec un ordinateur serveur et profiter des mesures de sécurité suivantes :

- Après avoir effectué une connexion initiale, le client peut s'assurer de se connecter au même serveur lors des sessions suivantes.
- Le client peut transmettre ses données d'authentification au serveur, telles que son nom d'utilisateur et son mot de passe, en format crypté.
- Toutes les données envoyées et reçues pendant la connexion sont transférées de façon chiffrée, ce qui les rend extrêmement difficiles à déchiffrer et à lire.
- Le client a la possibilité d'utiliser des applications X11[1] lancées à partir de l'invite shell. Cette technique fournit une interface graphique sécurisée (appelée **retransmission X11**).

Un serveur peut aussi tirer parti du protocole SSH, particulièrement s'il exécute de nombreux services. Si vous utilisez la **retransmission de port**, des protocoles normalement non sécurisés (comme POP par exemple) peuvent être chiffrés et envoyés en toute sécurité à des ordinateurs distants. Il est relativement facile avec SSH de crypter différents types d'informations échangées lors des communications qui sont habituellement envoyées de manière non sécurisée sur les réseaux publics.

La Red Hat Linux 7.1 contient le serveur OpenSSH (`openssh-server`) et les paquetages client (`openssh-clients`), ainsi que le paquetage OpenSSH général (`openssh`) qui doit être installé

[1] X11 fait référence au système d'affichage de fenêtres X11R6, généralement appelé X. Red Hat Linux comprend XFree86, un système X Window sources ouvertes très utilisé, basé sur X11R6.

sur l'un des deux ordinateurs pour que le tout fonctionne. Veuillez vous reporter au *Guide de personnalisation officiel Red Hat Linux* pour avoir les instructions d'installation et d'utilisation d'OpenSSH sur votre système Red Hat Linux.

Les paquetages OpenSSH nécessitent le paquetage OpenSSL (`openssl`). OpenSSL installe de nombreuses bibliothèques cryptographiques importantes qui aident OpenSSH à chiffrer les communications. Vous devez installer le paquetage `openssl` avant d'installer tout autre paquetage OpenSSH.

Un grand nombre de programmes client et serveur peuvent utiliser le protocole SSH, dont de nombreuses applications sources ouvertes et disponibles gratuitement. Il existe plusieurs versions de clients SSH pour les principaux systèmes d'exploitation utilisés aujourd'hui. Donc, même si un utilisateur se connectant à votre système n'utilise pas Red Hat Linux, il peut tout de même avoir recours à un client SSH fait pour son propre système d'exploitation.

11.1.1 Pourquoi utiliser SSH ?

L'interception de paquets, la mystification[2]DNS et IP, ainsi que la diffusion de fausses informations de routage ne sont que quelques exemples des menaces qui planent lors des communications en réseau. En d'autres termes, nous pourrions catégoriser ces menaces de la façon suivante :

- *Interception d'une communication entre deux systèmes* — ce scénario implique la présence d'un troisième élément quelque part sur le réseau entre les deux systèmes connectés qui copie l'information échangée entre eux. Celui-ci peut copier et garder l'information ou alors la modifier avant de l'envoyer au destinataire prévu.
- *Usurpation de l'identité d'un hôte* — grâce à cette technique, un système intercepteur prétend être le destinataire désiré d'un message. Si cela fonctionne, le client ne s'en rend pas compte et continue de lui envoyer toute l'information, comme s'il était connecté au bon destinataire.

Dans les deux cas, l'information est interceptée (probablement pour des raisons hostiles). Le résultat peut être catastrophique, peu importe qu'il soit obtenu par l'interception de tous les paquets sur un réseau local d'entreprise ou au moyen d'un serveur DNS piraté qui pointe vers un hôte mal intentionné.

L'utilisation du protocole SSH pour effectuer une connexion shell à distance ou copier des fichiers permet de faire diminuer sensiblement ces menaces à la sécurité. La signature numérique d'un serveur fournit la vérification pour son identité. En outre, la communication complète entre un système client et un système serveur ne peut être utilisée si elle est interceptée car tous les paquets sont chiffrés. De plus, il n'est pas possible d'usurper l'identité d'un des deux systèmes, parce que les paquets sont chiffrés et leurs clés ne sont connues que par les systèmes local et distant.

2 La mystification est l'acte de laisser croire aux autres que l'on est un système précis sans l'être véritablement.

11.2 Séquence des événements d'une connexion SSH

Pour aider à protéger l'intégrité d'une communication SSH entre deux ordinateurs hôtes, une certaine série d'événements doit être utilisée.

D'abord, une **couche transport** sécurisée doit être créée pour que le client sache qu'il communique bien avec le bon serveur. Ensuite, la communication est chiffrée entre le client et le serveur au moyen d'un chiffre symétrique.

Puis, une fois la connexion sécurisée établie avec le serveur, le client peut s'authentifier auprès de celui-ci sans craindre que ses informations ne puissent être compromises. Sur Red Hat Linux, OpenSSH utilise par défaut des clés DSA ou RSA et la version 2.0 du protocole SSH pour l'authentification.

Enfin, après l'authentification du client auprès du serveur, de nombreux services différents peuvent être utilisés de façon sécurisée au cours de la connexion, tels qu'une session shell interactive, des applications X11 et des ports TCP/IP tunnellisés.

L'ensemble du processus de connexion se fait sans que le système local n'ait à faire de nombreuses opérations supplémentaires. En effet, SSH semblera familier, à bien des égards, aux utilisateurs habitués aux méthodes de connexion moins sécurisées.

Dans l'exemple qui suit, l'utilisateur 1 (user1) sur le système client veut initier une connexion SSH à un système serveur. L'adresse IP de ce serveur est 10.0.0.2, mais on pourrait également utiliser son nom de domaine. Le nom de connexion de l'utilisateur 1 sur le serveur est user2. La commande `ssh` est écrite de la façon suivante :

```
[user1@machine1 user1]$ ssh user2@10.0.0.2
```

Le client OpenSSH demande la phrase d'accès de la clé privée de l'utilisateur pour déchiffrer la clé privée utilisée pour procéder à l'authentification. Cependant, la phrase d'accès de la clé privée n'est pas envoyée au moyen de la connexion sécurisée en cours entre le client et le serveur. Elle est plutôt utilisée pour ouvrir le fichier `id_dsa` et générer une signature qui est ensuite envoyée au serveur. Si le serveur a une copie de la clé publique de l'utilisateur pouvant être utilisée pour vérifier la signature, l'utilisateur est alors authentifié.

Dans cet exemple, l'utilisateur utilise une clé DSA (des clés RSA, notamment, peuvent aussi être utilisées) et reçoit l'invite suivante :

```
Enter passphrase for DSA key '/home/user1/.ssh/id_dsa':
```

Si l'authentification par clé publique échoue, pour une raison ou une autre (il se pourrait que la phrase d'accès ait été mal tapée ou que les renseignements d'authentification n'existent pas encore sur le serveur), un autre type d'authentification est généralement lancé. Dans notre exemple, le serveur

OpenSSH permet à l'utilisateur 1 de s'authentifier au moyen du mot de passe de l'utilisateur 2 (user2) car la signature envoyée ne correspond pas à la clé publique stockée par l'utilisateur 2 :

```
user2@machine2's password:
```

En introduisant le bon mot de passe, l'utilisateur reçoit une invite shell. Bien entendu, l'utilisateur 2 doit déjà avoir un compte sur l'ordinateur 10.0.0.2 pour que l'authentification par mot de passe réussisse.

```
Last login: Mon Apr 15 13:27:43 2001 from machine1
[user2@machine2 user2]$
```

A ce stade, l'utilisateur peut interagir avec le shell de la même façon qu'avec `telnet` ou `rsh`, sauf que la communication est chiffrée.

D'autres outils SSH, tels que `scp` et `sftp`, fonctionnent de façon semblable aux outils non sécurisés `rcp` et `ftp`. Veuillez lire le *Guide de personnalisation officiel Red Hat Linux* pour avoir des instructions et des exemples sur l'utilisation de ces outils et d'autres commandes SSH.

11.3 Couches de sécurité SSH

Le protocole SSH permet à tout programme client et serveur créé selon les spécifications du protocole de communiquer de façon sécurisée et d'être utilisé de manière interchangeable.

A l'heure actuelle, il existe deux types différents de protocole SSH. La version 1 contient de nombreux algorithmes de chiffrement brevetés (toutefois, bon nombre de ces brevets sont périmés) et un trou de sécurité qui donne la possibilité éventuelle d'insérer des données dans le flot de données. Il vous est vivement recommandé d'utiliser des serveurs et clients compatibles avec la version 2 de SSH, si cela vous est possible.

OpenSSH comprend le support pour la version 2 (et des clés de chiffrement DSA disponibles gratuitement). Conjugué aux bibliothèques de chiffrement OpenSSL, OpenSSH offre une gamme complète de fonctions de sécurité.

Les deux versions (1 et 2) du protocole SSH utilisent des couches de sécurité semblables pour renforcer l'intégrité des communications sous différents aspects. Chaque couche fournit son propre type de protection, ce qui, lorsque utilisé de concert avec d'autres types, renforce la sécurité des communications et les rend plus facile à utiliser.

11.3.1 Couche transport

Le rôle principal d'une couche transport est de faciliter une communication sécurisée entre deux ordinateurs hôtes au moment de l'authentification et par la suite également. Elle utilise généralement le protocole TCP/IP, et accomplit sa tâche en s'occupant du chiffrement et du déchiffrement des données,

en s'assurant que le serveur est le bon ordinateur pour l'authentification et en offrant la protection nécessaire aux paquets de données lors de leur envoi et de leur réception. En outre, la couche transport peut également faire la compression des données pour accélérer la vitesse de transfert de l'information.

Lorsqu'un client communique avec un serveur au moyen d'un protocole SSH, de nombreux éléments importants sont négociés afin que les deux systèmes puissent créer correctement la couche transport :

- l'échange des clés
- l'algorithme de clé publique à utiliser
- l'algorithme de chiffrement symétrique à utiliser
- l'algorithme d'authentification de message à utiliser
- l'algorithme repère (hash) à utiliser

Durant l'échange des clés, le serveur s'identifie au client au moyen d'une **clé hôte**. Evidemment, si le client communique pour la première fois avec ce serveur, la clé du serveur lui est inconnue. OpenSSH contourne ce problème en permettant au client d'accepter la clé hôte du serveur lors de leur première connexion SSH. Ensuite, lors des connexions suivantes, la clé hôte du serveur peut être vérifiée au moyen d'une version enregistrée sur le client, ce qui permet au client de s'assurer qu'il communique bien avec le serveur désiré.

La méthode de vérification de la clé hôte utilisée par SSH n'est pas parfaite car, à ce stade, un individu pourrait se faire passer pour le serveur lors de la première connexion sans que le système local puisse nécessairement différencier le serveur désiré de l'individu voulant se faire passer pour lui. Toutefois, d'ici à ce qu'une meilleure méthode de distribution de la clé hôte soit disponible, cette méthode initiale non sécurisée est mieux que rien.

Le protocole SSH est conçu pour fonctionner avec la plupart des types d'algorithme de clé publique ou de format de codage. Après la création de deux valeurs lors de l'échange initial des clés (une valeur repère utilisée pour les échanges et une valeur secrète partagée), les deux systèmes commencent immédiatement à calculer de nouveaux algorithmes et de nouvelles clés pour protéger l'authentification et les données qui seront envoyées au cours de la connexion.

11.3.2 Authentification

Une fois que la couche transport a créé un tunnel sécurisé pour envoyer les informations entre les deux systèmes, le serveur indique au client quelles sont les différentes méthodes d'authentification prises

en charge, telles que l'utilisation d'une signature chiffrée privée ou l'entrée d'un mot de passe. Le client doit ensuite essayer de s'authentifier au serveur au moyen d'une des méthodes spécifiées.

Etant donné que les serveurs peuvent être configurés de façon à permettre différents types d'authentification, cette méthode donne aux deux parties un niveau de contrôle optimal. Le serveur peut décider quelles méthodes d'authentification prendre en charge en fonction de son modèle de sécurité et le client peut choisir l'ordre des méthodes d'authentification à utiliser parmi celles qui sont disponibles. Grâce à la nature sécurisée de la couche transport SSH, même les méthodes d'authentification qui, de prime abord, semblent non sécurisées, telles que l'authentification d'ordinateur hôte, peuvent être utilisées en toute sécurité.

La plupart des utilisateurs exigeant un shell sécurisé procèdent à l'authentification au moyen d'un mot de passe. Contrairement aux autres modèles d'authentification, les mots de passe sont transmis sur les réseaux en texte clair. Cependant, comme ce mot de passe est complètement chiffré, il peut être envoyé sans problème sur n'importe quel réseau.

11.3.3 Connexion

Après avoir effectué avec succès l'authentification au moyen de la couche transport SSH, des **canaux** multiples sont ouverts en transformant la connexion simple entre les deux systèmes en connexion multiplex[3]. Chaque canal peut ainsi s'occuper de la communication d'une session de terminal différente, du transfert d'informations X11 ou de tout autre service séparé essayant d'utiliser la connexion SSH.

Le client et le serveur peuvent tous deux créer un nouveau canal et chaque canal reçoit un numéro différent aux deux extrémités (serveur ou client). Lorsque l'une d'elle essaie d'ouvrir un nouveau canal, le numéro de cette extrémité pour ce canal est envoyé avec la requête. Cette information est stockée à l'autre extrémité et utilisée pour diriger un type spécifique de communication d'un service à ce canal. Ainsi, des types différents de session ne peuvent se nuire entre eux et les canaux peuvent être fermés sans interrompre la connexion SSH principale entre les deux systèmes.

Les canaux prennent aussi en charge le contrôle du flot de données, ce qui leur permet d'envoyer et de recevoir des données de façon ordonnée. Ce faisant, aucune donnée n'est envoyée par le canal tant que l'hôte n'a pas reçu un message lui indiquant que le canal est en mesure d'en recevoir.

Les canaux sont particulièrement utiles avec la retransmission X11 et la retransmission de port TCP/IP par SSH. Des canaux séparés peuvent être configurés différemment, pour utiliser une quantité maximum de paquets différente ou pour transférer un type spécifique de données. Cela permet à SSH de faire preuve de souplesse lors de l'acheminement des données sur divers types de connexion à distance, tels que les liaisons sur des réseaux publics ou les connexions rapides sur des réseaux locaux d'entreprise, sans avoir à changer l'infrastructure de base du protocole. Le client et le serveur négocient automatiquement la configuration de chaque canal à l'intérieur de la connexion pour l'utilisateur.

[3] Une connexion multiplex envoie plusieurs signaux sur un support commun et partagé. Avec le protocole SSH, divers canaux sont envoyés sur une connexion sécurisée commune.

11.4 Fichiers de configuration d'OpenSSH

OpenSSH est constitué de deux ensembles de fichiers de configuration différents, un pour les programmes client (`ssh`, `scp` et `sftp`) et l'autre pour le service (`sshd`), situés dans deux emplacements distincts.

Les informations de configuration SSH qui s'appliquent à l'ensemble du système sont stockées dans le répertoire `/etc/ssh` :

- `primes` — contient les groupes Diffie-Hellman utilisés pour l'échange de clés Diffie-Hellman. En fait, cet échange de clés crée une valeur secrète partagée qui ne peut être déterminée par aucune des parties seules et est utilisée pour accorder l'authentification hôte. Ce fichier est crucial pour la création d'une couche transport sécurisée.
- `ssh_config` — fichier de configuration client SSH pour l'ensemble du système, utilisé pour diriger le client SSH. Si un utilisateur possède son propre fichier de configuration disponible dans son répertoire personnel (`~/.ssh/config`), ses valeurs remplaceront celles qui sont stockées dans `/etc/ssh/ssh_config`.
- `sshd_config` — fichier de configuration pour `sshd`.
- `ssh_host_dsa_key` — clé DSA privée utilisée par `sshd`.
- `ssh_host_dsa_key.pub` — clé DSA privée utilisée par `sshd`.
- `ssh_host_key` — clé RSA privée utilisée par `sshd` pour la version 1 du protocole SSH.
- `ssh_host_key.pub` — clé RSA publique utilisée par `sshd` pour la version 1 du protocole SSH.
- `ssh_host_rsa_key` — clé RSA privée utilisée par `sshd` pour la version 2 du protocole SSH.
- `ssh_host_rsa_key.pub` — clé RSA publique utilisée par `sshd` pour la version 2 du protocole SSH.

Les informations de configuration SSH spécifiques à l'utilisateur sont stockées dans son répertoire personnel à l'intérieur du sous répertoire `.ssh` :

- `authorized_keys2` — ce fichier contient une liste de clés publiques "autorisées". Si un utilisateur se connecte et prouve qu'il connaît la clé privée correspondant à l'une de ces clés, il obtient l'authentification. Notez qu'il ne s'agit que d'une méthode d'authentification facultative.
- `id_dsa` — contient l'identité d'authentification DSA de l'utilisateur.
- `id_dsa.pub` — clé DSA publique de l'utilisateur.
- `known_hosts2` — stocke les clés hôte des serveurs auxquels l'utilisateur s'est connecté au moyen du protocole SSH, lorsque l'utilisateur choisit de les enregistrer. Si un serveur change volontairement sa clé hôte, à la suite d'une réinstallation de Red Hat Linux par exemple, l'utilisateur

reçoit un message lui indiquant que la clé hôte enregistrée dans le fichier `known_hosts2` correspondant à ce serveur est inexacte. Ensuite, l'utilisateur doit éliminer la clé de cet hôte du fichier `known_hosts`, afin d'y stocker la nouvelle clé de ce système. Le fichier `known_hosts2` est très important pour assurer que le client se connecte au bon serveur. Si une clé hôte a changé et que vous n'êtes pas absolument certain de la raison pour laquelle elle a changé, vous devriez communiquer avec l'administrateur système de cet hôte et vous assurer que cet hôte n'a pas été compromis.

Veuillez lire les pages de manuel concernant `ssh` et `sshd` pour avoir plus de détails sur les différentes directives disponibles dans les fichiers de configuration SSH.

11.5 Beaucoup plus qu'un shell sécurisé

Une interface sécurisée en ligne de commande n'est que la première des nombreuses façons dont SSH peut être utilisé. En ayant la quantité nécessaire de bande passante, les sessions X11 peuvent être dirigées sur un canal SSH ou bien, en utilisant la retransmission TCP/IP, les connexions par port entre systèmes, considérées auparavant comme étant non sécurisés, peuvent être appliquées à des canaux SSH spécifiques.

11.5.1 Retransmission X11

Ouvrir une session X11 par le biais d'une connexion SSH établie est aussi facile que d'exécuter un programme X lorsque l'on exécute déjà un client X sur son propre ordinateur hôte. Lorsqu'un programme X est exécuté à partir de l'invite shell sécurisée, le client et le serveur SSH créent un nouveau canal sécurisé au sein de la connexion SSH en cours et les données du programme X sont ensuite envoyées à l'ordinateur client par ce canal, comme si la connexion au serveur X se faisait via un terminal local.

Comme vous pouvez l'imaginer, la retransmission X11 peut être très utile. Vous pourriez, par exemple, l'utiliser pour créer une session interactive sécurisée au moyen de l'interface utilisateur graphique `up2date` sur le serveur pour mettre à jour des paquetages de votre choix (si les paquetages Red Hat Network nécessaires sont installés sur le serveur). Pour ce faire, vous n'avez qu'à vous connecter au serveur au moyen de `ssh` et taper :

```
up2date
```

On vous demande alors de donner votre mot de passe root pour ce serveur, puis l'agent de mise à jour Red Hat apparaît et vous pouvez mettre à jour vos paquetages sur le serveur comme si vous étiez confortablement assis devant cet ordinateur.

Cependant, le temps-système de traitement nécessaire pour chiffrer et déchiffrer les données sécurisées envoyées par le canal et la quantité supplémentaire de bande passante requise pour envoyer des données d'application X par le canal, peuvent être assez élevés. Il est donc nécessaire de tester

correctement le tout, afin de s'assurer que le programme X est toujours utilisable, en fonction des caractéristiques de votre matériel et de votre bande passante.

11.5.2 Retransmission TCP/IP

La retransmission TCP/IP fonctionne de concert avec le client SSH qui demande qu'un port donné sur le client ou le serveur soit mappé sur la connexion SSH en cours.

Pour mapper un port local d'un ordinateur client à un port distant sur un serveur, vous devez d'abord connaître les numéros de port des deux ordinateurs. Vous pouvez même mapper deux ports différents et non standard l'un à l'autre.

Pour créer un canal de retransmission TCP/IP en mode de réception des connexions sur l'ordinateur hôte local, utilisez la commande suivante (tout doit être sur une seule ligne) :

```
ssh -L <port-local>:<nomhôte-distant>:<port-distant>
      <nomutilisateur>@<nomhôte>
```

Remarque

Afin de pouvoir définir la retransmission TCP/IP pour qu'elle puisse être en mode réception des ports inférieurs à 1024, il est nécessaire d'avoir un accès super-utilisateur, tout comme pour l'exécution de services en mode de réception des ports inférieurs à 1024.

Par exemple, si vous voulez vérifier votre courrier sur un serveur appelé mail.domain.com au moyen du protocole POP et que SSH est disponible sur ce serveur, vous pouvez utiliser la commande suivante pour définir la retransmission TCP/IP :

```
ssh -L 1100:mail.domain.com:110 mail.domain.com
```

Une fois la retransmission TCP/IP en place entre les deux ordinateurs, vous pouvez diriger votre client POP mail pour qu'il utilise l'hôte local comme serveur POP et 1100 comme port pour vérifier le nouveau courrier. Ainsi, toute requête envoyée au port 1100 de votre système sera redirigée en toute sécurité au serveur mail.domain.com.

Si mail.domain.com n'exécute aucun démon de serveur SSH, mais que vous pouvez tout de même vous connecter par SSH à un ordinateur tout près, au moyen d'un pare-feu par exemple, vous pouvez quand même utiliser SSH pour rendre sécurisée la partie de la connexion POP qui est faite sur un réseau public. Dans ce cas, la commande est légèrement différente :

```
ssh -L 1100:mail.domain.com:110 other.domain.com
```

Dans cet exemple, vous transférez votre requête POP du port 1100 de votre ordinateur au moyen de la connexion SSH au port 22 de other.domain.com. Ensuite, other.domain.com se connecte au port 110

de mail.domain.com pour vous permettre de vérifier votre courrier. Seule la connexion entre vous et other.domain.com est sécurisée, mais dans nombre de cas, cela suffit pour acheminer des informations sur un réseau public de façon sécurisée et pour vous offrir plus de sécurité qu'auparavant.

Bien entendu, dans cet exemple et celui qui le précède, vous devez être en mesure de faire l'authentification auprès du serveur SSH pour pouvoir utiliser la retransmission TCP/IP. Assurez-vous d'abord de pouvoir exécuter des commandes SSH normales avant de vous lancer dans l'aventure de la retransmission TCP/IP.

La retransmission TCP/IP peut être très utile pour obtenir des informations de façon sécurisée à travers un pare-feu. Si le pare-feu est configuré de façon à permettre le trafic SSH par son port standard (22), mais bloque l'accès aux autres ports, une connexion entre deux ordinateurs hôtes qui utilisent des ports bloqués est tout de même possible en redirigeant leur communication sur une connexion SSH établie entre eux.

Remarque

Cela peut par contre être très risqué. L'utilisation de la retransmission TCP/IP pour transférer des connexions de cette façon permet à tout utilisateur sur le système client de se connecter au service auquel vous transférer des connexions, ce qui peut être dangereux et peut compromettre votre système client.

Vérifiez auprès de l'administrateur système qui s'occupe du pare-feu avant d'utiliser la retransmission TCP/IP pour le contourner. Les administrateurs système préoccupés par la retransmission TCP/IP n'ont qu'à désactiver cette fonction en définissant un paramètre `No` pour la ligne **AllowTcpForwarding** dans `/etc/ssh/sshd_config` et redémarrer le service `sshd`.

11.6 Exiger SSH pour les connexions à distance

Afin que le protocole SSH soit vraiment efficace et protège vos connexions réseau, vous devez absolument cesser d'utiliser des protocoles de connexion non sécurisés, tels que `telnet` et `rsh`. Autrement, le mot de passe d'un utilisateur pourrait être protégé au moyen de `ssh`, mais être capté lors d'une connexi ultérieure de ce même utilisateur au moyen de `telnet`.

Pour désactiver des méthodes de connexion non sécurisées sur votre système, utilisez `ntsysv` ou `chkconfig` qui vous permettent d'empêcher qu'elles ne soient lancées au démarrage du système. Pour configurer les services qui doivent être lancés au démarrage aux niveaux 2, 3 et 5, à l'aide de `ntsysv`, entrez cette commande :

```
/usr/sbin/ntsysv 235
```

Au sein de `ntsysv`, vous pouvez désactiver des services en les dessélectionnant. La [barre d'espacement] fait passer un service de l'état actif à l'état inactif. Vous devriez au moins dessélectionner `telnet`, `rsh`, `ftp` et `rlogin`. Lorsque c'est fait, sélectionnez le bouton **OK** pour enregistrer les modifications apportées à `ntsysv`. Reportez-vous à la page de manuel `ntsysv` pour en savoir plus sur cette fonction.

Les changements apportés au moyen de `ntsysv` ne seront appliqués qu'après avoir redémarré le système ou avoir changé les niveaux d'exécution. Si vous désactivez des services utilisés avec `xinetd`, vous devez redémarrer `xinetd`. Par défaut, `rlogin`, `rsh` et `telnet` sont contrôlés par `xinetd`. Pour redémarrer `xinetd`, vous n'avez qu'à taper ceci :

```
/sbin/service xinetd restart
```

Quant aux services qui ne sont pas utilisés avec `xinetd`, vous devez les arrêter manuellement, à moins que vous ne fassiez redémarrer votre système après avoir utilisé `ntsysv`. Pour arrêter un service, utilisez une commande comme celle-ci :

```
/sbin/service <nom-du-service> stop
```

Ainsi, après avoir redémarré `xinetd` et arrêté tous les services que vous avez configurés de façon à ce qu'ils ne soient pas lancés automatiquement lors du démarrage de votre système, les méthodes de connexion désactivées ne seront plus acceptées par votre système. Si vous désactivez toutes les méthodes de connexion à distance autres que le démon service `sshd`, les utilisateurs devront nécessairement utiliser une application client SSH pour se connecter au serveur.

12 Contrôle des accès et des privilèges

Selon une politique de sécurité courante, la sécurité du système se base sur l'incapacité des utilisateurs ou des groupes à faire plus que ce qu'ils ne devraient. La plupart des changements quotidiens concernent le contrôle correct des accès et des privilèges accordés aux groupes et aux utilisateurs. (Voir le Chapitre 2, *Utilisateurs et groupes* pour plus d'informations sur la création et la configuration correctes des utilisateurs et des groupes.)

Toutefois, bien des organisations utilisant Red Hat Linux requièrent une sécurité accrue ou des configurations particulières qui permettent d'obtenir un accès plus ou moins élevé aux applications ou aux périphériques du système. Cette section fournit des méthodes qui permettent d'obtenir un niveau d'accès et de privilèges approprié à ses propres besoins.

12.1 Utilitaires masqués

Si vous êtes dans un environnement multi-utilisateur et n'utilisez ni PAM ni Kerberos, vous devriez envisager d'utiliser des utilitaires masqués (aussi connus sous le nom de **mots de passe masqués**) car ils offrent une protection accrue des fichiers d'authentification de votre système. Pendant l'installation de Red Hat Linux, les mots de passe masqués et les **mots de passe MD5** (une méthode alternative et sans doute plus sûre de cryptage des mots de passe pour le stockage sur votre système) sont activés par défaut.

Les mots de passe masqués offrent d'autres avantages par rapport au système standard de stockage des mots de passe sur UNIX et Linux, notamment :

- Une méthode permettant d'améliorer la sécurité du système en déplaçant les mots de passe cryptés (se trouvant normalement dans `/etc/passwd`) vers `/etc/shadow` qui n'est lisible que par root.
- Des informations concernant le vieillissement du mot de passe (le temps qui s'est écoulé depuis la dernière modification du mot de passe).
- Un contrôle sur la durée de validité du mot de passe (le moment où l'utilisateur doit le modifier).
- La possibilité d'utiliser le fichier `/etc/login.defs` pour imposer une règle de sécurité, en particulier une règle concernant le vieillissement du mot de passe.

Le paquetage `shadow-utils` contient des utilitaires qui gèrent :

- la conversion des mots de passes normaux en mots de passe masqués et vice-versa (`pwconv`, `pwunconv`),
- la vérification du mot de passe, du groupe et des fichiers masqués associés (`pwck`, `grpck`),

- des méthodes standard d'ajout, de suppression et de modification des comptes utilisateurs (`useradd`, `usermod` et `userdel`),
- des méthodes standard d'ajout, de suppression et de modification des groupes utilisateurs (`groupadd`, `groupmod` et `groupdel`),
- des méthodes standard d'administration du fichier `/etc/group` au moyen de la commande `gpasswd`.

Remarque

Ces utilitaires offrent d'autres avantages :

- Les utilitaires fonctionneront parfaitement que les mots de passe masqués soient activés ou non.
- Les utilitaires ont été légèrement modifiés pour gérer le schéma du groupe propre à l'utilisateur de Red Hat. Pour obtenir un description de ces modifications, reportez-vous à la page du manuel qui reporte la commande `useradd`. Pour plus de détails sur les groupes propres à l'utilisateur, passez à la Section 2.4, *Groupes propres à l'utilisateur*.
- Le script `adduser` a été remplacé par un lien symbolique à script `/usr/sbin/useradd`.
- Les outils composant le paquetage `shadow-utils` ne sont pas compatibles avec Kerberos et LDAP. Les nouveaux utilisateurs seront uniquement locaux. Pour plus d'informations sur Kerberos et LDAP, reportez-vous au Chapitre 9, *Utilisation de Kerberos 5 sur Red Hat Linux* et au Chapitre 4, *Protocole LDAP (Lightweight Directory Access Protocol)*.

12.2 Configuration de l'accès à la console

Lorsque des utilisateurs normaux (non root) se connectent localement à un ordinateur, ils se voient attribuer deux types d'autorisation spéciale :

1. Ils peuvent exécuter certains programmes qu'ils ne pourraient pas exécuter autrement.
2. Ils peuvent accéder à certains fichiers (normalement des fichiers de périphériques spéciaux utilisés pour accéder à des disquettes, CD-ROM, etc.) auxquels ils ne pourraient pas accéder autrement.

Du fait qu'il y a plusieurs consoles sur un ordinateur, et que plusieurs utilisateurs peuvent être connectés localement à l'ordinateur en même temps, il faut que l'un d'eux "gagne" le combat pour accéder à

ces fichiers. Le premier utilisateur se connectant à la console est propriétaire de ces fichiers. Une fois que le premier utilisateur se déconnecte, le second utilisateur à s'être connecté devient propriétaire des fichiers.

Par contre, *chaque* utilisateur se connectant à la console sera autorisé à exécuter des programmes dont l'usage est normalement réservé à l'utilisateur root. Ceci sera effectué sous forme graphique si X Window est en cours d'exécution, ce qui permet d'inclure ces actions en tant qu'éléments de menu dans une interface utilisateur graphique. Tels qu'ils sont livrés, les programmes accessibles depuis la console sont `shutdown`, `halt`, `poweroff` et `reboot`.

12.2.1 Désactivation de Shutdown via Ctrl-Alt-Suppr

Par défaut, `/etc/inittab` spécifie que votre système est configuré pour s'arrêter et redémarrer en réponse à la combinaison de touches [Ctrl]-[Alt]-[Suppr]. Pour désactiver complètement cette fonction, commentez la ligne suivante dans `/etc/inittab`:

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Sinon, vous pouvez décider de ne donner qu'à certains utilisateurs non root l'autorisation d'arrêter le système au moyen de la combinaison de touches [Ctrl]-[Alt]-[Suppr]. Pour limiter cette autorisation à quelques utilisateurs, suivez la procédure ci-dessous :

1. Ajoutez l'option `-a` à la ligne `/etc/inittab` ci-dessus :

   ```
   ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
   ```

   `-a` demande à `shutdown` de chercher le fichier `/etc/shutdown.allow`, que vous devrez créer à l'étape suivante.

2. Créez un fichier nommé `shutdown.allow` dans `/etc`. Le fichier `shutdown.allow` doit contenir les noms d'utilisateurs de tous les utilisateurs qui ont l'autorisation d'arrêter le système en utilisant la combinaison de touches [Ctrl]-[Alt]-[Suppr]. Le fichier `/etc/shutdown.allow` est une liste qui, sur chacune de ses lignes, reporte un nom d'utilisateur :

   ```
   stephen
   jack
   sophie
   ```

Dans ce fichier `shutdown.allow` d'exemple, stephen, jack et sophie sont autorisés à arrêter le système via la combinaison de touches [Ctrl]-[Alt]-[Suppr]. Lorsque cette combinaison est utilisée, le fichier `shutdown -a` contenu dans `/etc/inittab` contrôle si des utilisateurs dans `/etc/shutdown.allow` (ou root) sont connectés à une console virtuelle. Si l'un d'entre eux l'est, la procédure d'arrêt se poursuit ; dans le cas contraire, un message d'erreur sera transmis à la console du système.

Pour plus d'informations sur `shutdown.allow`, reportez-vous à la page du manuel sur la commande `shutdown`.

12.2.2 Désactivation de l'accès aux programmes de la console

Pour désactiver l'accès des utilisateurs aux programmes de la console, entrez en tant que root la commande ci-dessous :

```
rm -f /etc/security/console.apps/*
```

Dans les environnements où la console est normalement sécurisée (mots de passe BIOS et LILO définis, combinaison de touches [Ctrl]-[Alt]-[Suppr] désactivée, commutateurs d'alimentation et de réinitialisation désactivés, etc.), il n'est peut-être pas souhaitable d'autoriser l'accès d'utilisateurs arbitraires à la console où ils peuvent exécuter les programmes `poweroff`, `halt` et `reboot`, accessibles par défaut.

Pour désactiver tout accès des utilisateurs de console aux programmes de la console, entrez en tant que root les commandes ci-dessous :

```
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

12.2.3 Désactivation de tout accès à la console

Le module PAM `pam_console.so` gère les autorisations et l'authentification des fichiers de la console (pour plus d'informations sur la configuration de PAM, reportez-vous au Chapitre 8, *Modules d'authentification enfichables (PAM)*). Pour désactiver tout accès à la console, y compris aux programmes et aux fichiers, dans le répertoire `/etc/pam.d`, ajoutez un commentaire à toutes les lignes faisant référence à `pam_console.so`. Le script suivant se chargera de cette tâche :

```
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo $i
done
```

12.2.4 Définition de la console

Le module `pam_console.so` utilise le fichier `/etc/security/console.perms` pour définir les autorisations d'accès à la console des utilisateurs. La syntaxe de ce fichier est très flexible ; vous pouvez éditer le fichier afin que ces instructions ne soient plus applicables. Toutefois, le fichier par défaut contient une ligne ressemblant à ceci :

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

Lorsque les utilisateurs se connectent, ils sont liés à une sorte de terminal, soit un serveur X portant un nom tel que `:0` ou `mymachine.example.com:1.0` ; soit un périphérique tel que `/dev/ttyS0`

ou `/dev/pts/2`. Par défaut, il convient de définir que les consoles virtuelles locales et les serveurs X locaux permettent d'héberger une console systè, mais si vous voulez considérer le terminal série à côté de vous sur le port `/dev/ttyS1` comme pouvant également le faire, vous pouvez modifier cette ligne comme suit :

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9] /dev/ttyS1
```

12.2.5 Rendre des fichiers accessibles depuis la console

`/etc/security/console.perms` contient des lignes telles que :

```
<floppy>=/dev/fd[0-1]* \
    /dev/floppy/*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
    /dev/mixer* /dev/sequencer \
    /dev/sound/*
<cdrom>=/dev/cdrom* /dev/cdwriter*
```

Si nécessaire, vous pouvez également ajouter vos propres lignes. Vérifiez que chaque ligne que vous ajoutez se réfère au périphérique approprié. Par exemple, vous pouvez ajouter la ligne suivante :

```
<scanner>=/dev/sga
```

(Assurez-vous, naturellement, que `/dev/sga` est réellement votre scanner et non, par exemple, votre disque dur).

Ceci est la première partie. La seconde partie consiste à définir le sort de ces fichiers. Examinez la dernière section de `/etc/security/console.perms`:

```
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <sound>  0640 root
<console> 0600 <cdrom>  0600 root.disk
```

et ajoutez la ligne ci-dessous :

```
<console> 0600 <scanner> 0600 root
```

Ensuite, lorsque vous vous connecterez à la console, vous recevrez la propriété du périphérique `/dev/sga` et vos autorisations seront 0600 (lecture et écriture réservées pour vous). Lorsque vous vous déconnecterez, le périphérique sera la propriété du root et disposera toujours des autorisations 0600 (lecture et écriture réservées au root).

12.2.6 Activation de l'accès à la console pour d'autres applications

Pour rendre d'autres applications accessibles aux utilisateurs de la console, vous devrez simplement travailler un petit peu plus.

Tout d'abord, l'accès à la console ne fonctionne *que* pour les applications résidant dans `/sbin` ou `/usr/sbin`, de sorte que l'application que vous voulez exécuter doit s'y trouver également. Après l'avoir vérifié, suivez la procédure ci-dessous :

1. Créez un lien entre le nom de votre application, tel que notre programme d'exemple *`foo`*, et l'application `/usr/bin/consolehelper` :

```
cd /usr/bin
ln -s consolehelper foo
```

2. Créez le fichier `/etc/security/console.apps/`*`foo`*:

```
touch /etc/security/console.apps/foo
```

3. Créez un fichier de configuration PAM pour le service *foo* dans `/etc/pam.d/`. Nous vous suggérons de commencer avec une copie du service d'arrêt du fichier de configuration PAM, puis de la modifier si vous voulez en modifier le comportement :

```
cp /etc/pam.d/halt /etc/pam.d/foo
```

Désormais, lorsque vous exécutez `/usr/bin/foo`, cette action appelle `consolehelper` qui, avec l'aide de `/usr/sbin/userhelper`, authentifiera l'utilisateur en demandant le mot de passe utilisateur si `/etc/pam.d/foo` est une copie de `/etc/pam.d/shutdown` ; (dans le cas contraire, il fait précisément ce qui est spécifié dans `/etc/pam.d/foo`), puis exécute `/usr/sbin/foo` avec des autorisations root.

12.3 Groupe `floppy`

Si, pour une raison quelconque, l'accès à la console n'est pas approprié pour vous, et si vous devez donner à des utilisateurs non root l'accès à l'unité de disquette de votre système, vous pouvez le faire à l'aide du groupe `floppy`. Ajoutez simplement les utilisateurs au groupe `floppy` à l'aide de l'outil de votre choix. Voici un exemple montrant comment `gpasswd` peut être utilisé pour ajouter l'utilisateur fred au groupe `floppy` :

```
[root@bigdog root]# gpasswd -a fred floppy
Adding user fred to group floppy
[root@bigdog root]#
```

L'utilisateur fred pourra désormais accéder au lecteur de disquette du système.

Partie III Références liées à Apache

13 Utilisation d’Apache comme serveur Web sécurisé

13.1 Introduction

Ce chapitre fournit des informations de base sur le mode d’installation du serveur Apache World Wide Web (WWW ou Web) avec le module de sécurité mod_ssl ainsi qu’avec la bibliothèque et l’ensemble de programmes OpenSSL. La combinaison de ces trois éléments fournis dans Red Hat Linux sera appelée dans ce manuel secure Web server ou plus simplement serveur sécurisé.

Les serveurs Web fournissent des pages Web en réponse aux demandes des navigateurs. Netscape Navigator et Microsoft Internet Explorer sont deux exemples de navigateurs très connus. Les serveurs et les navigateurs Web communiquent en utilisant le protocole HTTP, le protocole standard pour les communications de type Web. Lorsqu’un utilisateur clique sur une page Web, une demande d’afficher le contenu correspondant au lien est envoyée au serveur Web. Le serveur Web reçoit la demande et fournit le contenu requis, tel qu’une page HTML, un script CGI ou une page Web créée de façon dynamique depuis une base de données. Si un serveur Web ne peut fournir le contenu demandé, il envoie un message d’erreur. Apache, le serveur Web fourni dans Red Hat Linux, est le serveur Web le plus utilisé sur Internet (connectez-vous à l’adresse http://www.netcraft.net/survey) .

Le serveur Apache a une structure modulaire. Il est en effet composé de plusieurs morceaux de code qui correspondent à différents aspects ou fonctions du serveur. Cette modularité est voulue. Ainsi, les développeurs peuvent écrire leur propre morceau de code. Ce code, appelé module, peut ensuite être facilement intégré dans le serveur Web Apache.

Le module mod_ssl est un module de sécurité pour le serveur Web Apache. Le module mod_ssl utilise les outils fournis par le projet OpenSSL pour ajouter une fonction importante à Apache — la capacité de crypter des communications. Par contraste, avec le HTTP "normal" les communications entre un navigateur et un serveur Web sont échangées en texte clair, au risque d’être interceptées et lues en cours de route.

Le projet OpenSSL comprend un ensemble de programmes qui applique les protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security), de même qu’une bibliothèque de cryptographie générale. Le protocole SSL est actuellement utilisé pour la transmission de données sécurisée sur Internet ; le protocole TLS est une norme Internet proposée pour permettre des communications privées (sécurisées) et fiables sur Internet. Les outils de OpenSSL sont utilisés par le module mod_ssl pour sécuriser les communications Web.

Ce chapitre ne prétend pas constituer une documentation exhaustive ni exclusive pour aucun de ces programmes. Dans la mesure du possible, ce guide indique où trouver une documentation plus approfondie sur certains aspects.

Ce chapitre explique comment installer ces programmes. Il décrit également les démarches nécessaires pour générer une clé privée et une demande de certificat, explique comment générer votre propre certificat autographe et comment installer un certificat à utiliser avec votre serveur Web sécurisé.

13.2 Remerciements

Le secure Web server comprend les éléments suivants :

- Logiciel développé par le groupe Apache en vue de son utilisation dans le projet de serveur HTTP Apache (http://httpd.apache.org)
- Module de sécurité mod_ssl développé par Ralf S. Engelschall (http://www.modssl.org)
- Ensemble de programmes OpenSSL, développé par Mark J. Cox, Ralf S. Engelschall, Dr. Stephen Henson et Ben Laurie (http://www.openssl.org)
- Logiciel basé sur un projet de serveur HTTP Apache-SSL développé par Ben Laurie (http://www.apache-ssl.org)
- Logiciel basé sur un logiciel cryptographique SSLeay écrit par Eric Young et Tim Hudson

Red Hat remercie les auteurs des contributions apportées à ce produit.

13.3 Paquetages de sécurité

Pour installer le serveur sécurisé vous devez installer au moins trois paquetages :

`apache`

Le paquetage `apache` contient le démon `httpd` ainsi que les utilitaires, les fichiers de configuration, les icônes, les modules Apache, les pages de manuel et autres fichiers utilisés par le serveur Apache.

`mod_ssl`

Le paquetage `mod_ssl` contient le module mod_ssl, qui fournit un bon système de chiffrement pour le serveur Apache via les protocoles SSL et TLS.

`openssl`

Le paquetage `openssl` contient l'ensemble de programmes OpenSSL. Celui-ci applique les protocoles SSL et TLS et contient une bibliothèque de chiffrement générale.

D'autres paquetages fournis dans Red Hat Linux ont des fonctions de sécurité (mais ne sont pas requis pour que le serveur fonctionne) :

`apache-devel`

Le paquetage `apache-devel` contient les fichiers à inclure Apache, des fichiers d'en-tête et l'utilitaire APXS. Vous en avez besoin si vous souhaitez charger des modules supplémentaires, autres que ceux fournis avec ce produit. Reportez-vous à la Section 14.3, *Ajout de modules au serveur* pour plus d'informations sur le chargement de modules dans le secure Web server à l'aide de la fonctionnalité DSO d'Apache.

Si vous n'avez pas l'intention de charger d'autres modules dans le secure Web server, il est inutile d'installer ce paquetage.

`apache-manual`

Le paquetage `apache-manual` contient le *Guide de l'utilisateur Apache 1.3* du projet Apache au format HTML. Ce manuel est également disponible sur le Web à l'adresse http://httpd.apache.org/docs/ .

Paquetages OpenSSH

Le paquetage `openssh` fournit le jeu d'outils de connectivité réseau OpenSSH permettant de se connecter à un ordinateur distant et d'exécuter des commandes sur celui-ci. Les outils OpenSSH cryptent tous les trafics (y compris les mots de passe), ce qui vous permet d'éviter tout détournement de connexion, indiscrétion et autre attaque portée contre les communications entre votre ordinateur et l'ordinateur distant.

Le paquetage `openssh` contient les fichiers de base requis par les programmes du client OpenSSH et le serveur OpenSSH. Le paquetage `openssh` contient également `scp`, un programme de remplacement sécurisé de `rcp` (pour copier des fichiers entre différents ordinateurs) et `ftp` (pour transférer des fichiers d'un ordinateur à un autre).

Le paquetage `openssh-askpass` prend en charge l'affichage d'une fenêtre de dialogue qui demande un mot de passe en cours d'utilisation de l'agent OpenSSH avec authentification RSA.

Le paquetage `openssh-askpass-gnome` contient une fenêtre de dialogue de l'environnement GNOME qui s'affiche lorsque OpenSSH demande un mot de passe. Si vous utilisez GNOME et les utilitaires OpenSSH, installez ce paquetage.

Le paquetage `openssh-server` contient le démon de shell sécurisé `sshd` et les fichiers relatifs. Le démon de shell sécurisé est le côté serveur de la suite OpenSSH et doit être installé sur votre hôte si vous voulez permettre à des clients SSH de s'y connecter.

Le paquetage `openssh-clients` contient les programmes client nécessaires pour établir des connexions chiffrées avec des serveurs SSH, tels que `ssh`, un remplacement sécurisé pour `rsh`, `slogin`, un remplacement sécurisé pour `rlogin` (pour les connexions à distance) et `telnet` (pour communiquer avec un autre hôte par le biais du protocole TELNET).

Pour plus d'informations sur OpenSSH, consultez le Chapitre 11, *Protocole SSH* et le site OpenSSH à l'adresse http://www.openssh.com .

openssl-devel

Le paquetage openssl-devel contient les bibliothèques statiques et les fichiers à inclure nécessaires pour compiler des applications qui prennent en charge divers algorithmes de chiffrement et protocoles. N'installez ce paquetage que si vous développez des applications qui comprennent le support SSL — vous n'avez pas besoin de ce paquetage pour utiliser SSL.

stunnel

Le paquetage stunnel fournit le wrapper Stunnel SSL. Stunnel prend en charge le cryptage SSL de connexions TCP, de sorte qu'il peut assurer le chiffrement de démons et protocoles non compatibles SSL (tels que POP, IMAP et LDAP) sans qu'il soit nécessaire de modifier le code du démon.

La Table 13–1, *Paquetages de sécurité* affiche l'emplacement des paquetages du serveur sécurisé et des paquetages supplémentaires relatifs à la sécurité au sein des groupes de paquetages fournis par Red Hat Linux. Ce tableau vous indique également si les paquetages sont facultatifs ou non pour l'installation d'un serveur Web sécurisé.

Table 13–1 Paquetages de sécurité

Nom du paquetage	Groupe où il est situé	Facultatif ?
apache	Environnement Système/Démons	non
mod_ssl	Environnement Système/Démons	non
openssl	Environnement Système/Bibliothèques	non
apache-devel	Développement/Bibliothèques	oui
apache-manual	Documentation	oui
openssh	Applications/Internet	oui
openssh-askpass	Applications/Internet	oui
openssh-askpass-gnome	Applications/Internet	oui
openssh-clients	Applications/Internet	oui
openssh-server	Environnement Système/Démons	oui
openssl-devel	Développement/Bibliothèques	oui
stunnel	Applications/Internet	oui

13.4 Comment installer le serveur sécurisé

Vous pouvez installer le secure Web server de l'une des façons suivantes :

- *Lors d'une nouvelle installation de Red Hat Linux* — comme le secure Web server est fourni avec le système d'exploitation Red Hat Linux, la méthode la plus simple pour l'installer est de le faire pendant l'installation de Red Hat Linux. Si vous vous apprêtez à faire l'installation complète de Red Hat Linux, utilisez cette méthode pour installer également votre serveur sécurisé. Reportez-vous à la Section 13.5, *Installation du serveur sécurisé avec Red Hat Linux* pour avoir plus de renseignements sur cette méthode.
- *Lors de la mise à jour de Red Hat Linux au moyen du programme d'installation* — si une version antérieure de Red Hat Linux est installée sur votre système et que vous procédez à la mise à jour vers la version 7.1de Red Hat Linux, vous pouvez en profiter pour installer les paquetages du serveur sécurisé pendant le processus de mise à jour. Reportez-vous à la Section 13.6, *Mise à jour d'une version antérieure de Red Hat Linux* pour en savoir plus sur cette méthode.
- *Installation du serveur sécurisé lorsque Red Hat Linux 7.1 est déjà installé* — si vous avez déjà installé la version 7.1 de Red Hat Linux, mais n'avez pas installé les paquetages du serveur sécurisé et décidez de les installer à un autre moment, vous pouvez le faire au moyen de RPM, Gnome-RPM ou Kpackage. Les paquetages du serveur sécurisé sont ainsi installés à partir d'un cédérom Red Hat Linux. Reportez-vous à la Section 13.7, *Installation du serveur sécurisé après avoir installé Red Hat Linux* pour savoir comment installer le serveur sécurisé après avoir déjà installé Red Hat Linux.

Mise à jour d'Apache

Lorsque vous installez le secure Web server et que vous procédez à la mise à jour d'une version antérieure d'Apache (y compris toute version précédente d'un produit de serveur sécurisé Red Hat), vous devez bien comprendre certaines choses concernant le processus de mise à jour d'Apache. Si vous procédez à la mise à jour d'Apache reportez-vous à la Section 13.8, *Mise à jour d'une version antérieure d'Apache* avant de commencer le processus d'installation.

13.5 Installation du serveur sécurisé avec Red Hat Linux

Si vous installez simultanément Red Hat Linux et le secure Web server, suivez les instructions du manuel d'installation relatives à votre architecture. Si vous prévoyez utiliser votre système Red Hat

Linux comme serveur sécurisé, vous choisirez probablement d'exécuter une installation de la classe Serveur ou Personnalisée. Voici les différentes classes d'installation possibles :

- Si vous optez pour une installation de la classe Serveur, les paquetages `apache`, `mod_ssl` et `openssl` sont sélectionnés automatiquement. Les paquetages `stunnel` et `openssh`, qui assurent les fonctions de sécurité, sont également sélectionnés.
- Si vous optez pour une installation de la classe Poste de travail (ou de la classe Ordinateur portable, si elle disponible pour votre système), les paquetages du serveur sécurisé et les paquetages de sécurité ne sont pas sélectionnés automatiquement pour l'installation, mais vous pouvez choisir de les installer durant le processus de personnalisation de la sélection des paquetages.
- Si vous optez pour une installation de la classe Personnalisée, vous pouvez sélectionner les paquetages du serveur sécurisé et les paquetages relatifs à la sécurité de votre choix car vous avez le contrôle total des paquetages à installer.

Après avoir sélectionné la classe d'installation, continuez de suivre les instructions d'installation pour le partitionnement et la configuration du système. Lorsque vous atteignez la section relative à la sélection des groupes de paquetages ou des composants, sélectionnez le groupe de paquetages **Serveur Web**. **Serveur Web** inclut les paquetages `apache` et `mod_ssl` que vous devez installer pour exécuter le serveur sécurisé. Du fait que `openssl` est une dépendance pour le paquetage `mod_ssl`, `openssl` est également sélectionné pour l'installation.

Si vous voulez installer n'importe lequel des paquetages supplémentaires de sécurité décrits à la Section 13.3, *Paquetages de sécurité*, vous devez l'indiquer au programme d'installation. Pour ce faire, sélectionnez l'option **Sélection individuelle des paquetages** dans l'écran **Sélection des groupes de paquetages**.

Sélectionnez les paquetages de sécurité que vous voulez installer en fonction des instructions fournies dans le manuel d'installation. Pour vous aider à les localiser plus facilement, un tableau indiquant leur emplacement est fourni à la Table 13–1, *Paquetages de sécurité*.

Après avoir vérifié que les paquetages nécessaires sont sélectionnés, poursuivez le processus d'installation. Lorsque vous avez terminé d'installer Red Hat Linux et le serveur sécurisé, reportez-vous à la Section 13.9, *Aperçu des certificats et de la sécurité*.

13.6 Mise à jour d'une version antérieure de Red Hat Linux

Si vous avez déjà une version précédente de Red Hat Linux sur votre système, vous pourriez décider de faire une mise à jour et de passer à la version 7.1 de Red Hat Linux plutôt que de faire une installation complète. Si vous optez pour la mise à jour, vous devez choisir **Mise à jour** au lieu de choisir une classe d'installation. Suivez les instructions adaptées à votre architecture pour la mise à jour de votre

système, contenues dans le manuel d'installation. Pendant la mise à jour, vous devrez vous assurer que les paquetages du serveur sécurisé sont sélectionnés par le programme d'installation.

Lorsque vous procédez à une mise à jour de votre système Red Hat Linux, le programme d'installation vérifie les paquetages déjà installés. Ces paquetages sont automatiquement mis à jour en fonction des versions incluses dans la version 7.1 de Red Hat Linux pendant le processus. Toutefois, si un paquetage donné n'est pas installé, le programme d'installation n'installe pas sa nouvelle version, à moins que vous ne personnalisiez votre mise à jour.

Si vous procédez à la mise à jour de Red Hat Linux 7.0 ou d'une version ultérieure et que les paquetages du secure Web server sont déjà installés, le processus de mise à jour met à jour les paquetages du serveur sécurisé. Par contre, si vous procédez à la mise à jour de Red Hat Linux 7.0 ou d'une version ultérieure et que les paquetages du secure Web server ne sont pas déjà installés, vous devez sélectionner les paquetages `apache`, `mod_ssl` et `openssl` durant le processus de personnalisation des paquetages. Reportez-vous à la Section 13.6.1, *Personnalisation de la mise à jour pour installer le serveur sécurisé* pour savoir comment trouver les paquetages que vous devez choisir.

Si vous procédez à la mise à jour de la version américaine et canadienne de Red Hat Linux Professional, vous devez personnaliser votre mise à jour et choisir les paquetages du serveur sécurisé pour l'installation. Il se pourrait que `apache` soit déjà installé, mais `mod_ssl` et `openssl` ne le sont pas car ils n'étaient pas inclus dans Red Hat Linux avant la version 7.0. Vous devez donc personnaliser la mise à jour de façon à inclure au moins `mod_ssl` et `openssl`. Reportez-vous à la Section 13.6.1, *Personnalisation de la mise à jour pour installer le serveur sécurisé* pour savoir comment trouver les paquetages que vous devez choisir.

Si vous procédez à la mise à jour de la version internationale de Red Hat Linux Professional et que les paquetages `apache`, `mod_ssl` et `openssl` sont installés, alors le programme d'installation les sélectionne et les met à jour automatiquement.

Si vous procédez à la mise à jour de la version internationale de Red Hat Linux Professional et que les paquetages `apache`, `mod_ssl` ou `openssl` ne sont pas installés, alors vous devez personnaliser votre mise à jour et sélectionner ces paquetages pour l'installation. Reportez-vous à la Section 13.6.1, *Personnalisation de la mise à jour pour installer le serveur sécurisé* pour savoir comment trouver les paquetages que vous devez choisir.

13.6.1 Personnalisation de la mise à jour pour installer le serveur sécurisé

Si vous avez besoin de personnaliser le processus de mise à jour, suivez les instructions fournies dans le manuel d'installation. En fait, il suffit de choisir **Mise à jour** comme **Type d'installation** et ensuite de sélectionner **Personnalisation des paquetages à mettre à jour**. Puis vous devez sélectionner les

paquetages à mettre à jour, comme expliqué dans le manuel d'installation. Pour vous aider à sélectionner les paquetages, la Table 13–1, *Paquetages de sécurité* fournit l'emplacement de chaque paquetage du serveur sécurisé et indique s'il est facultatif ou non.

Une fois terminé, reportez-vous à la Section 13.8, *Mise à jour d'une version antérieure d'Apache* si vous désirez également procéder à la mise à jour d'une version d'Apache. Si, au contraire, vous ne mettez pas à jour Apache, reportez-vous à la Section 13.9, *Aperçu des certificats et de la sécurité*.

13.7 Installation du serveur sécurisé après avoir installé Red Hat Linux

Si vous avez procédé à l'installation de la version 7.1 de Red Hat Linux sans toutefois avoir installé le serveur sécurisé, il est possible de le faire plus tard. La façon la plus simple est d'utiliser RPM, Gnome-RPM ou Kpackage pour installer les paquetages RPM fournis sur le CD-ROM Red Hat Linux.

13.7.1 Arrêtez tout processus de serveur Web

Avant de commencer l'installation du secure Web server, vous devez arrêter tout serveur Web en cours sur votre système. Si un serveur Web Apache est en cours, utilisez l'une des deux commandes suivantes pour l'arrêter :

```
/etc/rc.d/init.d/httpsd stop
/etc/rc.d/init.d/httpd stop
```

13.7.2 Utilisation de Gnome-RPM ou de Kpackage

Si vous avez GNOME ou KDE, vous pouvez utiliser une interface graphique, telle que Gnome-RPM ou Kpackage, pour installer les paquetages du serveur sécurisé.

Plus d'informations sur l'utilisation de Gnome-RPM sont fournies dans le *Guide de démarrage officiel Red Hat Linux*. Les instructions sur l'utilisation de Kpackage sont fournies à la page Web *Kpackage Handbook* qui est à l'adresse http://www.general.uwa.edu.au/u/toivo/kpackage .

Après avoir installé les paquetages nécessaires, l'étape suivante est la création de votre clé pour obtenir un certificat. Veuillez poursuivre à la Section 13.9, *Aperçu des certificats et de la sécurité*.

13.7.3 Utilisation de RPM

Les paquetages du secure Web server sont fournis au format RPM, ce qui vous permet de les installer au moyen de RPM. Reportez-vous au *Guide de personnalisation officiel Red Hat Linux* pour en savoir plus sur RPM et à la Table 13–1, *Paquetages de sécurité* si vous ne savez pas avec certitude quels paquetages installer.

Une fois les paquetages du serveur sécurisé installés, reportez-vous à la Section 13.8, *Mise à jour d'une version antérieure d'Apache* si vous mettez également à jour une version d'Apache. Dans le cas contraire, poursuivez à la Section 13.9, *Aperçu des certificats et de la sécurité*.

13.8 Mise à jour d'une version antérieure d'Apache

Pendant l'installation des paquetages du serveur sécurisé, vous devez savoir deux choses si vous procédez à la mise à jour d'Apache :

- Dans la version d'Apache comprise dans Red Hat Linux 7.1, le `DocumentRoot` est `/var/www/html`.
- Si vous avez personnalisé votre fichier de configuration Apache (`httpd.conf`), vous désirez peut-être savoir ce qu'il adviendra de vos personnalisations durant le processus de mise à jour.

13.8.1 Où se trouve le DocumentRoot ?

Le `DocumentRoot` est le répertoire de votre système qui contient la plupart des pages Web servies par votre serveur Web Apache. Le `DocumentRoot` est défini par une directive de configuration dans le fichier de configuration d'Apache, `httpd.conf`. Si vous ne connaissez pas bien la directive de configuration `DocumentRoot`, reportez-vous à la Section 14.2.28, *`DocumentRoot`* pour obtenir une explication plus détaillée.

Dans les versions Red Hat Linux antérieures à 7.0, l'Apache fourni par Red Hat Linux utilisait `/home/httpd/html` comme `DocumentRoot`. Dans la version par défaut (non sécurisée) du fichier de configuration d'Apache, le `DocumentRoot` est `/usr/local/apache/htdocs`. Il est aussi possible que vous (ou l'un de vos prédécesseurs) ayez utilisé un `DocumentRoot` complètement différent. Dans la 7.1 Red Hat Linux toutefois, le `DocumentRoot` par défaut est `/var/www/html`.

Cela a-t-il de l'importance pour vous ? Oui, si vous avez utilisé Apache avec un `DocumentRoot` différent et que vous voulez servir les mêmes pages Web avec la nouvelle configuration d'Apache. Toutes les pages Web qui étaient précédemment servies à partir d'un `DocumentRoot` différent ne seront pas trouvées (ou servies) par la version d'Apache fournie avec Red Hat Linux 7.1 dans sa configuration par défaut. Vous devez donc prendre l'une des mesures suivantes :

Déplacez tous les fichiers de l'ancien `DocumentRoot` (`/home/httpd/html`, `/usr/local/apache/htdocs`, ou ailleurs) vers le nouveau `DocumentRoot` (`/var/www/html`).

ou

Modifiez le fichier de configuration d'Apache et changez toutes les références menant au `DocumentRoot` par l'ancien chemin d'accès du répertoire.

La solution à choisir dépend de la configuration de votre système. Généralement, si vous auto-montez `/home` sur votre système, vous préférerez ne pas avoir votre `DocumentRoot` dans `/home`. D'un

autre côté, si vous n'avez pas beaucoup d'espace dans `/var`, vous préférerez probablement ne pas avoir votre `DocumentRoot` dans `/var`. Vous ou votre administrateur système devrez choisir la meilleure solution en fonction de la configuration de votre système et des besoins de votre serveur Web. La configuration par défaut du secure Web server a pour but de satisfaire aux besoins de la plupart des Webmasters ; malheureusement, il n'est pas possible de le configurer pour qu'il soit adapté à toutes les situations.

13.8.2 Qu'advient-il de mon ancien fichier de configuration ?

Si vous aviez installé une autre version d'Apache et personnalisé ses fichiers de configuration, ceux-ci seront enregistrés, dans le même répertoire, avec une extension `.rpmsave` durant l'installation d'Apache. Si vous aviez installé une autre version d'Apache sans jamais modifier ses fichiers de configuration, ceux-ci seront écrasés durant l'installation de ce produit.

Après avoir installé Apache, vous pouvez couper et coller vos personnalisations à partir de vos anciens fichiers de configuration Apache dans le nouveau fichier de configuration `httpd.conf` installé pour votre serveur sécurisé. Veuillez noter que si vous utilisez l'outil de configuration Apache, vous devez modifier `httpd.conf` manuellement. Reportez-vous au *Guide de personnalisation officiel Red Hat Linux* pour avoir plus de renseignements sur l'outil de configuration Apache.

13.9 Aperçu des certificats et de la sécurité

Votre secure Web server permet d'offrir un niveau de sécurité en conjuguant le protocole SSL (Secure Sockets Layer) à (dans la plupart des cas) un certificat numérique d'un fournisseur de certificats (CA). Le protocole SSL se charge des communications chiffrées et de l'authentification mutuelle entre les navigateurs et votre secure Web server, alors que le certificat numérique approuvé par un CA fournit l'authentification pour votre secure Web server (la réputation du fournisseur de certificats est à la base du certificat d'identité accordé à votre organisation). Lorsque votre navigateur communique au moyen du chiffrement de SSL, le préfixe https:// est placé devant l'adresse Web (URL) dans la barre de navigation.

Le chiffrement dépend du type de clés (imaginez-les comme des chaînes secrètes de codage et décodage en format de données). Pour le chiffrement conventionnel ou symétrique, les deux extrémités de la transaction ont la même clé, qu'elles utilisent pour décoder leurs transmissions. Pour le chiffrement public ou asymétrique, deux clés coexistent : une clé publique et une clé privée. La clé privée d'un individu ou d'une organisation doit rester secrète, alors que la clé publique doit être publiée. Les données codées au moyen de la clé publique ne peuvent être décodées qu'avec la clé privée ; les données codées avec la clé privée ne peuvent être décodées qu'avec la clé publique.

Pour définir votre serveur sécurisé, vous utiliserez le chiffrement public afin de créer une paire de clés publique et privée. Dans la plupart des cas, vous enverrez votre demande de certificat (y compris votre clé publique), une preuve d'identité de votre entreprise et le paiement à un fournisseur de certificats.

Celui-ci vérifiera la demande de certificat, votre identité et vous enverra ensuite un certificat pour votre secure Web server.

Un serveur sécurisé utilise un certificat pour s'identifier auprès des navigateurs Web. Vous pouvez générer votre propre certificat (appelé certificat autographe) ou obtenir un certificat d'un fournisseur de certificats. Un certificat d'un fournisseur de bonne réputation garantit qu'un site Web est bel et bien associé à une entreprise ou à une organisation donnée.

Autrement, vous pouvez créer votre propre certificat autographe. Notez cependant qu'il est préférable de ne pas utiliser un certificat autographe dans des environnements de production. Ces certificats ne sont pas acceptés automatiquement par le navigateur d'un utilisateur ; le navigateur demande d'abord à l'utilisateur s'il veut accepter le certificat et créer une connexion sécurisée. Reportez-vous à la Section 13.11, *Types de certificats* pour en savoir davantage sur les différences entre les certificats autographes et les certificats signés par des CA.

Une fois que vous avez un certificat, autographe ou signé par un CA de votre choix, vous devez l'installer sur votre secure Web server.

13.10 Utilisation des clés et certificats préexistants

Si vous possédez déjà une clé et un certificat (si vous procédez à l'installation du secure Web server pour remplacer le produit de serveur Web sécurisé d'une autre société, par exemple), vous pourrez probablement utiliser votre clé et votre certificat existants avec le secure Web server. Dans les deux cas suivants cependant, vous ne pouvez pas les utiliser :

- *Si vous changez votre adresse IP ou votre nom de domaine* — vous ne pouvez utiliser votre ancienne clé ou votre ancien certificat si vous changez votre adresse IP ou votre nom de domaine. Les certificats sont accordés pour une paire d'adresse IP et de nom de domaine spécifique. Si vous y apportez des changements, vous devez obtenir un nouveau certificat.
- *Vous avez un certificat de VeriSign et voulez changer votre logiciel serveur* — VeriSign est un fournisseur de certificats très utilisé. Si vous possédez déjà un certificat VeriSign pour autre chose, vous avez peut-être considéré la possibilité de l'utiliser pour votre nouveau secure Web server. Toutefois, vous ne le pourrez pas car VeriSign accorde ses certificats pour une combinaison de logiciel serveur et adresse IP/nom de domaine précise.

  Si vous changez l'un de ces paramètres (comme par exemple si vous avez utilisé un autre produit de serveur Web sécurisé auparavant et que vous voulez maintenant utiliser le secure Web server), le certificat VeriSign reçu pour être utilisé avec la configuration précédente ne fonctionnera pas avec la nouvelle configuration. Vous devrez obtenir un nouveau certificat.

Si vous possédez une clé et un certificat que vous pouvez utiliser, vous n'avez pas à générer une nouvelle clé pour obtenir un nouveau certificat. Cependant, il se pourrait que vous ayez besoin de déplacer et de renommer les fichiers qui contiennent votre clé et votre certificat.

Déplacez le fichier de la clé existante vers :

```
/etc/httpd/conf/ssl.key/server.key
```

Déplacez le fichier du certificat existant vers :

```
/etc/httpd/conf/ssl.crt/server.crt
```

Après avoir terminé de déplacer votre clé et votre certificat, passez à la Section 13.15, *Test du certificat*.

Si vous effectuez une mise à jour du serveur Web sécurisé Red Hat version 1.0 ou 2.0, votre ancienne clé (`httpsd.key`) et votre ancien certificat (`httpsd.crt`) se trouvent dans `/etc/httpd/conf/`. Vous devez les déplacer et les renommer pour que le secure Web server puisse les utiliser. Utilisez les deux commandes suivantes pour déplacer et renommer les fichiers de votre clé et de votre certificat :

```
mv /etc/httpd/conf/httpsd.key /etc/httpd/conf/ssl.key/server.key
mv /etc/httpd/conf/httpsd.crt /etc/httpd/conf/ssl.crt/server.crt
```

Lancez ensuite votre secure Web server comme indiqué à la Section 14.1, *Démarrage et arrêt* `httpd`. Si vous procédez à la mise à jour d'une version antérieure du secure Web server, vous ne devriez pas avoir besoin d'obtenir un nouveau certificat.

13.11 Types de certificats

Si vous avez installé le secure Web server au moyen du programme d'installation de Red Hat Linux, une clé et un certificat de test ont été générés et enregistrés dans les répertoires appropriés. Toutefois, avant de commencer à utiliser votre serveur sécurisé, vous devez générer votre propre clé et obtenir un certificat qui identifie correctement votre serveur.

Vous avez besoin d'une clé et d'un certificat pour utiliser votre secure Web server — ceci signifie que vous pouvez générer un certificat autographe ou acheter un certificat signé par un fournisseur de certificats. Quelles différences y a-t-il entre les deux ?

Un certificat signé par un fournisseur de certificats offre deux avantages très importants pour votre serveur :

- Les navigateurs le reconnaissent automatiquement (de façon générale) et permettent la création d'une connexion sécurisée sans demander l'autorisation à l'utilisateur.
- Lorsqu'un fournisseur de certificats émet un certificat signé, il garantit l'identité de l'organisation qui fournit les pages Web au navigateur.

Si votre serveur sécurisé offre l'accès à un grand public, votre secure Web server nécessite un certificat signé par un fournisseur de certificats, de sorte que les gens qui visitent votre site Web soient assurés que le site en question est bien la propriété de l'organisation qui prétend le posséder. Les fournisseurs

de certificats vérifient toujours l'identité des organisations demandant des certificats avant de les signer.

La plupart des navigateurs Web qui prennent en charge le protocole SSL ont une liste des fournisseurs de certificats acceptés automatiquement. Si un navigateur Web tombe sur un certificat signé par un fournisseur ne faisant pas partie de cette liste, il demande à l'utilisateur de décider s'il doit accepter ou refuser la connexion.

Vous pouvez générer un certificat autographe pour votre secure Web server, mais sachez que ce dernier n'offre pas les mêmes avantages qu'un certificat signé par un fournisseur. Un certificat autographe n'est pas accepté automatiquement par les navigateurs des utilisateurs et ne fournit aucune garantie quant à l'identité de l'organisation propriétaire d'un site Web, contrairement au certificat signé par un fournisseur qui assure ces deux éléments importants pour un serveur sécurisé. Si votre serveur sécurisé doit être utilisé dans un environnement de production, il vous est conseillé d'obtenir un certificat signé par un fournisseur de certificats.

La marche à suivre pour obtenir un certificat signé par un fournisseur est relativement facile. En voici un bref aperçu :

1. Créez une paire de clés privée et publique de chiffrement.
2. Créez une demande de certificat fondée sur la clé publique. La demande de certificat contient des informations sur votre serveur et la société qui l'héberge.
3. Envoyez votre demande de certificat et les documents qui prouvent votre identité à un fournisseur de certificats. Nous ne pouvons vous dire quel fournisseur choisir. En effet, votre décision peut dépendre de divers facteurs, tels que vos expériences passées ou celles de vos collègues ou encore de questions purement financières.

   Pour consulter une liste de CA, cliquez sur le bouton **Sécurité** sur la barre d'outils de votre navigateur ou sur l'icône cadenas dans le coin inférieur gauche de votre écran et cliquez ensuite sur **Signataires** pour visualiser la liste de tous les fournisseurs de certificats dont la signature est acceptée par votre navigateur Web. Vous pouvez aussi chercher sur le Web pour trouver des fournisseurs. Une fois que vous avez arrêté votre choix sur l'un d'eux, vous devez suivre les instructions fournies par celui-ci pour obtenir un certificat.
4. Lorsque le fournisseur de certificats est satisfait et a vérifié que vous êtes bien celui que vous prétendez être, il vous envoie un certificat numérique.
5. Installez ce certificat sur votre serveur Web et commencez à faire des transactions sécurisées.

Que vous décidiez de fournir votre propre certificat autographe ou de vous en procurer un auprès d'un fournisseur, la première étape est la même et consiste à générer une clé. Reportez-vous à la Section 13.12, *Génération d'une clé* pour savoir comment générer une clé.

13.12 Génération d'une clé

D'abord, allez au répertoire `/etc/httpd/conf`. Enlevez la fausse clé et le faux certificat générés lors de l'installation au moyen des commandes suivantes :

```
rm ssl.key/server.key
rm ssl.crt/server.crt
```

Puis, vous devez créer votre propre clé aléatoire. Entrez la commande suivante :

```
make genkey
```

Votre système affiche ensuite un message qui ressemble à ceci :

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.......++++++
.....................................................................++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

Vous devez maintenant entrer un mot de passe. Pour plus de sécurité, votre mot de passe devrait contenir au moins huit caractères, inclure des chiffres ou des signes de ponctuation et ne devrait pas être un mot tiré du dictionnaire. De plus, n'oubliez pas que votre mot de passe est sensible à la casse.

Remarque

Vous devrez entrer ce mot de passe chaque fois que vous lancez votre secure Web server, alors tâchez de ne pas l'oublier.

Puis, vous devez entrer à nouveau le mot de passe, pour assurer qu'il n'y a pas d'erreurs. Lorsque c'est fait, un fichier appelé `server.key` est créé et contient votre clé.

Il est à noter que si vous ne voulez pas entrer un mot de passe chaque fois que vous lancez votre serveur sécurisé, vous devez utiliser les deux commandes suivantes à la place de `make genkey` pour la création de la clé. Ces deux commandes doivent être écrites en entier sur une seule et même ligne.

Cette commande :

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

sert à créer votre clé. Ensuite utilisez la commande suivante :

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

pour vous assurer que les autorisations sont bien définies sur votre clé.

Après avoir utilisé les deux commandes mentionnées précédemment, vous n'avez plus à entrer de mot de passe lorsque vous lancez le secure Web server.

La désactivation de la fonction de mot de passe de votre serveur Web sécurisé représente un risque pour sa sécurité. Nous ne vous recommandons PAS de désactiver la fonction de mot de passe de votre secure Web server.

Les problèmes liés à la non-utilisation de mots de passe affectent directement la sécurité de l'ordinateur hôte. Par exemple, si un individu sans scrupules compromet la sécurité UNIX normale sur l'ordinateur hôte, cet individu pourrait obtenir votre clé privée (le contenu de votre fichier `server.key`). Cette clé pourrait ensuite être utilisée pour publier des pages Web comme si elles venaient de votre propre serveur Web.

Si les mesures de sécurité UNIX sont maintenues rigoureusement sur l'ordinateur hôte (c'est-à-dire que toute mise à jour du système d'exploitation est installée dès que possible, qu'aucun service inutile ou risqué n'est en cours d'exécution, etc.) le mot de passe du secure Web server peut sembler superflu. Cependant, comme votre secure Web server ne devrait pas être redémarré très souvent, l'opération supplémentaire qu'est l'entrée d'un mot de passe est un effort minime qui peut s'avérer très utile dans la plupart des cas.

Le fichier `server.key` doit être la propriété unique de l'utilisateur root de votre système et ne devrait être accessible à aucun autre utilisateur. Faites une copie de sauvegarde de ce fichier et gardez-la en lieu sûr. Cette copie de sauvegarde est nécessaire car si vous perdez le fichier `server.key` après l'avoir utilisé pour créer votre demande de certificat, votre certificat ne fonctionnera plus et le fournisseur de certificats ne pourra vous dépanner. La seule solution à ce problème est de demander (et de payer) un nouveau certificat.

Si vous prévoyez acheter un certificat auprès d'un fournisseur, poursuivez à la Section 13.13, *Création d'une demande de certificat à envoyer à un CA*. Si vous préférez générer votre propre certificat autographe, poursuivez à la Section 13.14, *Création d'un certificat autographe*.

13.13 Création d'une demande de certificat à envoyer à un CA

Après avoir créé une clé, vous devez créer une demande de certificat que vous enverrez ensuite au fournisseur de certificats de votre choix. Pour ce faire, tapez la commande suivante :

```
make certreq
```

Votre système affiche le résultat suivant et vous demande votre mot de passe (à moins d'avoir désactivé cette option) :

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

Entrez le mot de passe que vous avez choisi lors de la création de votre clé. Le système affiche ensuite quelques instructions et vous demande de lui fournir toute une série de renseignements. Ceux-ci seront ajoutés à la demande de certificat. Voici un exemple de l'écran qui affiche les questions :

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:North Carolina
Locality Name (eg, city) []:Durham
Organization Name (eg, company) [Internet Widgits]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.mydomain.com
Email Address []:admin@mydomain.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Les réponses par défaut sont mises entre parenthèses `[]` immédiatement après chaque requête d'information. Par exemple, la première information demandée est le nom du pays où le certificat sera utilisé, ce qui est indiqué comme suit :

```
Country Name (2 letter code) [AU]:
```

Le résultat par défaut, entre parenthèses, est **AU**. Pour accepter cette valeur par défaut, vous n'avez qu'à appuyer sur [Entrée] ou alors écrivez le code de deux lettres de votre pays.

Vous devez également indiquer les autres informations demandées (`State or Province Name`, `Locality Name`, `Organization Name`, `Organizational Unit Name`, `Common Name`, et `Email address`). Toutes ces informations ne nécessitent pas vraiment d'explication, mais vous devez tout de même suivre les lignes directrices suivantes :

- N'abrégez pas le nom de l'endroit ou du pays. Ecrivez-le en entier (par exemple, St-Louis devrait être écrit Saint-Louis).
- Lorsque vous envoyez votre demande de certificat à un fournisseur de certificats, assurez-vous de donner les bonnes informations, et ce pour tous les champs, particulièrement pour `Organization Name` et `Common Name`. Les fournisseurs de certificats vérifient les informations contenues dans la demande pour déterminer si le nom DNS que vous avez indiqué sous le champ `Common Name` appartient bien à votre organisation. Les fournisseurs de certificats refusent les demandes contenant des informations qu'elles considèrent comme non valides.
- Pour le champ `Common Name`, assurez-vous d'inscrire le nom *réel* de votre secure Web server (un nom DNS valide) et non pas l'alias du serveur s'il en a un.
- Le champ `Email Address` doit contenir l'adresse électronique du Webmaster ou de l'administrateur système.
- Evitez les caractères spéciaux comme @, #, &, !, etc. Certains fournisseurs de certificats refusent les demandes qui contiennent de tels caractères. Aussi, si le nom de votre société contient une esperluette (&), épelez-la en entier ("et" au lieu de "&").
- N'utilisez pas les champs supplémentaires (`A challenge password` et `An optional company name`). Pour continuer sans entrer d'informations dans ces champs, appuyez sur la touche [Entrée] pour accepter la valeur nulle par défaut des deux champs.

Lorsque vous avez terminé d'entrer les informations, un fichier appelé `server.csr` est créé. Ce fichier est votre demande de certificat, prêt à être envoyé au fournisseur de certificats.

Si vous avez déjà choisi un fournisseur de certificats, suivez les instructions fournies sur son site Web. Celles-ci vous indiqueront comment lui envoyer votre demande de certificat, les autres renseignements requis et votre paiement.

Si vous répondez aux exigences du fournisseur de certificats, celui-ci vous enverra (généralement par courrier électronique) un certificat. Enregistrez-le (ou alors copiez-le et collez-le) sous `/etc/httpd/conf/ssl.crt/server.crt`.

13.14 Création d'un certificat autographe

Vous pouvez créer votre propre certificat autographe. Prenez note qu'un certificat autographe ne fournit pas les mêmes garanties qu'un certificat signé par un fournisseur de certificats. Consultez la Section 13.11, *Types de certificats* pour plus de détails sur les certificats.

Pour pouvoir créer votre propre certificat autographe, vous devez d'abord créer une clé aléatoire (voir les instructions dans la Section 13.12, *Génération d'une clé*). Puis, lorsque vous avez votre clé, utilisez la commande suivante :

```
make testcert
```

Vous voyez ensuite apparaître ce qui suit et une invite de mot de passe à l'écran (à moins d'avoir désactivé cette fonction) :

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

Le cas échéant, entrez votre mot de passe et répondez aux questions qui s'affichent. Voici à quoi ressemble l'écran qui contient les questions et quelques exemples de réponses (vous devez fournir les bonnes informations sur votre société et votre hôte) :

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:North Carolina
Locality Name (eg, city) []:Durham
Organization Name (eg, company) [Internet Widgits]:My Company, Inc.
Organizational Unit Name (eg, section) []:Documentation
Common Name (your name or server's hostname) []:myhost.mydomain.com
Email Address []:myemail@mydomain.com
```

Après avoir répondu correctement aux questions, un certificat autographe est créé et placé dans `/etc/httpd/conf/ssl.crt/server.crt`. Vous devez redémarrer votre serveur sécurisé une fois le certificat créé. Reportez-vous à la Section 14.1, *Démarrage et arrêt `httpd`* pour obtenir des informations sur le redémarrage de votre serveur Web sécurisé.

13.15 Test du certificat

Lorsque le serveur sécurisé est installé par le programme d'installation Red Hat Linux, une clé aléatoire et un certificat générique sont installés aux fins de test. Vous pouvez connecter votre serveur sécurisé au moyen de ce certificat. Par contre, vous ne pourrez vous en servir que pour des tests. Si vous désirez faire autre chose vous devez vous procurer un certificat d'un fournisseur de certificats

ou créer un certificat autographe. Reportez-vous à la Section 13.11, *Types de certificats* si vous avez besoin d'explication sur les différents types de certificats disponibles.

Si vous possédez un certificat signé par un fournisseur ou un certificat autographe, vous devriez avoir un fichier appelé `/etc/httpd/conf/ssl.key/server.key` qui contient votre clé et un fichier appelé `/etc/httpd/conf/ssl.crt/server.crt` qui contient votre certificat. Si votre clé ou votre certificat se trouvent ailleurs, replacez-les dans ces répertoires. Si vous avez changé les emplacements par défaut ou les noms de fichier pour le secure Web server dans les fichiers de configuration d'Apache, vous devriez mettre ces deux fichiers dans les bons répertoires en fonction des modifications apportées.

Maintenant, arrêtez et démarrez votre serveur de la façon indiquée à la Section 14.1, *Démarrage et arrêt `httpd`*. Si votre fichier de clé est chiffré, on vous demande votre mot de passe. Entrez-le et le serveur devrait démarrer.

Pointez votre navigateur Web vers votre page d'accueil. Votre adresse pour avoir accès au secure Web server ressemblera à ceci :

```
https://votre_domaine
```

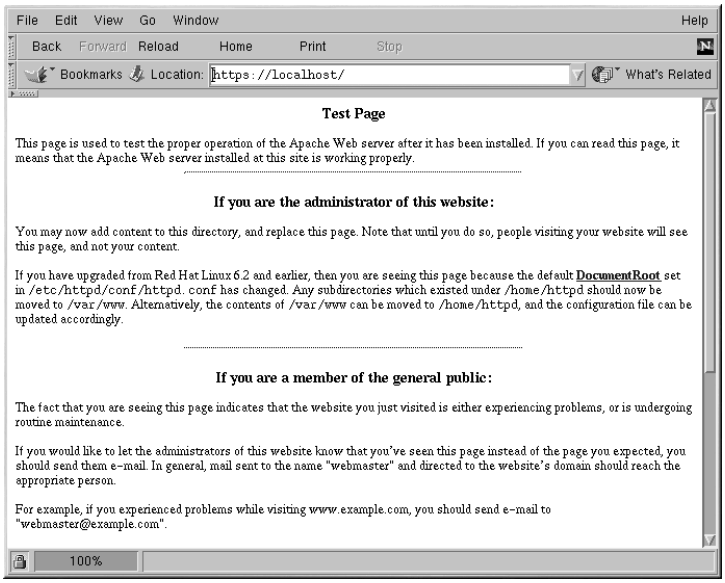
Remarque

Remarquez le "s" après "http". Le préfixe https: est utilisé pour les transactions HTTP sécurisées.

Si vous utilisez un certificat signé par un fournisseur de certificats reconnu, votre navigateur l'acceptera probablement de façon automatique (sans vous demander quoi que ce soit) et créera une connexion sécurisée. Toutefois, votre navigateur n'acceptera pas automatiquement un certificat de test ou un certificat autographe car ils ne sont pas signés par un fournisseur de certificats. Si vous n'utilisez pas un certificat signé par un fournisseur, suivez les instructions fournies par votre navigateur pour accepter le certificat. Vous pouvez vous contenter d'accepter les valeurs par défaut en cliquant sur le bouton **Suivant** jusqu'à ce que les boîtes de dialogue soient terminées.

Une fois que votre navigateur accepte le certificat, votre secure Web server affiche une page d'accueil par défaut (voir Figure 13–1, *Page d'accueil par défaut*).

Figure 13–1 Page d'accueil par défaut



13.16 Accès au serveur sécurisé

Pour accéder à votre serveur sécurisé, on utilise une adresse Web comme celle-ci :

```
https://votre_domaine
```

Notez que les adresses devant se connecter à votre secure Web server doivent commencer par le préfixe https: à la place du préfixe http: plus couramment utilisé.

Pour accéder à votre serveur non sécurisé, on utilise une adresse Web comme celle-ci :

```
http://votre_domaine
```

Le port standard pour les communications Web sécurisées est le port 443. Le port standard pour les communications Web non sécurisées est le port 80. La configuration par défaut du secure Web server définit qu'il est en mode réception sur les deux ports standard. Ainsi, vous n'avez pas à spécifier le numéro de port dans une adresse Web (le numéro est pris pour acquis).

Cependant, si vous configurez votre serveur pour qu'il soit en mode réception sur un port non standard (c'est-à-dire autre que 80 ou 443), vous devez spécifier le numéro de port dans chaque adresse Web devant se connecter au serveur sur le port non standard.

Par exemple, vous pourriez avoir configuré votre serveur de façon à avoir un hôte virtuel non sécurisé sur le port 12331. Le numéro de port doit alors être spécifié dans toute adresse Web devant se connecter à cet hôte virtuel. Voici un exemple d'adresse Web devant se connecter au serveur Web non sécurisé en mode réception sur le port 12331 :

```
http://votre_domaine:12331
```

Certains exemples d'adresse Web utilisés dans ce manuel doivent être modifiés, selon que vous accédez à votre secure Web server ou à votre serveur Web non sécurisé. Veuillez considérer tous les exemples d'adresses Web donnés dans ce manuel comme des exemples généraux et non comme des instructions explicites fonctionnant dans toutes les situations.

13.17 Autres ressources

Si vous avez suivi correctement toutes les étapes indiquées dans le Chapitre 13, *Utilisation d'Apache comme serveur Web sécurisé* et avez tout de même eu des problèmes, la première chose à faire est de consulter la section Errata du site Web Red Hat à l'adresse http://www.redhat.com/support/errata .

Si vous avez acheté un produit Red Hat officiel qui comprend le support, vous avez droit à l'assistance technique. Assurez-vous de visiter le site Web Red Hat de l'assistance à l'adresse http://www.redhat.com/support afin de vous y enregistrer.

Peut-être désirerez-vous vous inscrire à la liste des participants serveur-sécurisé-redhat. Vous pouvez le faire à l'adresse suivante : http://www.redhat.com/mailing-lists .

Vous pouvez aussi vous inscrire à la liste des participants serveur-sécurisé-redhat par courrier électronique. Pour ce faire, vous n'avez qu'à écrire à l'adresse électronique `redhat-secure-server-request@redhat.com` et indiquer le mot "subscribe" (sans les guillemets) dans la ligne objet.

13.17.1 Documentation déjà installée

Si vous avez installé le paquetage `apache-manual`, vous avez accès sur votre ordinateur à de la documentation au format HTML au sujet d'Apache, à partir de l'adresse Web suivante : http://localhost/manual/ .

La documentation mod_ssl est fournie à l'adresse Web http://localhost/manual/mod/mod_ssl/ .

13.17.2 Sites Web utiles

Vous trouverez des trucs, des questions fréquemment posées et des documents HowTo sur le site Web de Red Hat à l'adresse http://www.redhat.com/support/docs/howto .

La base centralisée de connaissances sur Apache de Red Hat Linux est disponible à l'adresse http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html .

Le site Web d'Apache fournit de la documentation complète sur le serveur Web Apache à l'adresse http://httpd.apache.org/docs .

Le site Web mod_ssl (http://www.modssl.org) est sans contredit la meilleure source d'informations sur mod_ssl . Le site est riche en documentation et contient notamment un *Manuel de l'utilisateur* à l'adresse http://www.modssl.org/docs .

13.17.3 Livres sur le sujet

Apache: The Definitive Guide, 2e édition, de Ben Laurie et Peter Laurie, édité par O'Reilly & Associates, Inc.

14 Directives et modules Apache

La configuration par défaut d'Apache fonctionne en principe pour la plupart des utilisateurs. Il est possible que vous ne deviez jamais modifier aucune directive de configuration d'Apache. Si vous tenez à modifier des options de configuration par défaut, vous devez en connaître la fonction et savoir où les trouver. Ce chapitre traite des options de configuration qui vous sont accessibles.

AVERTISSEMENT

Si vous avez l'intention d'utiliser l'outil de configuration Apache, un utilitaire graphique fourni par Red Hat Linux, ne modifiez pas le fichier de configuration `httpd.conf` de votre serveur Web Apache. Inversement, si vous voulez modifier manuellement `httpd.conf`, n'utilisez pas l'outil de configuration Apache.

Pour obtenir plus d'informations concernant l' outil de configuration Apache, consultez le *Guide de personnalisation officiel Red Hat Linux*.

Après avoir installé le paquetage `apache` vous pouvez obtenir la documentation sur le serveur Web Apache à l'adresse http://votre_domaine/manual/ ou consulter la documentation à l'adresse http://httpd.apache.org/docs/ s. La documentation sur le serveur Web Apache contient une liste exhaustive et des descriptions complètes de toutes les options de configuration d'Apache. Pour plus de commodité, ce guide fournit de brèves descriptions des directives de configuration utilisées par Red Hat Linux.

Lorsque vous examinez le fichier de configuration de votre serveur Web, sachez que votre configuration par défaut comprend un serveur Web non sécurisé et un serveur Web sécurisé. Le serveur Web sécurisé fonctionne comme un hôte virtuel configuré dans le fichier de configuration `httpd.conf`. Pour plus d'informations sur les hôtes virtuels, reportez-vous à la Section 14.4, *Utilisation d'hôtes virtuels*.

Remarque

Nous n'incluons pas d'extensions FrontPage, la licence de Microsoft(TM) interdit l'inclusion de telles extensions dans des produits d'autres éditeurs.

14.1 Démarrage et arrêt `httpd`

Durant le processus d'installation, un script shell appelé `httpd` a été sauvegardé dans `/etc/rc.d/init.d`. Pour arrêter et démarrer manuellement votre serveur, exécutez `httpd` avec les arguments `stop` ou `start`.

Pour démarrer votre serveur, tapez la commande :

```
/etc/rc.d/init.d/httpd start
```

Si vous exécutez Apache comme serveur sécurisé, une invite vous demandera votre mot de passe. Votre serveur démarrera dès que vous l'aurez tapé.

Pour arrêter votre serveur, tapez la commande :

```
/etc/rc.d/init.d/httpd stop
```

La commande `restart` est la façon la plus rapide d'arrêter et de redémarrer votre serveur. La commande `restart` arrête puis redémarre votre serveur. Une invite vous demandera alors votre mot de passe, si vous exécutez Apache en tant que serveur sécurisé. La commande `restart` ressemble à ceci :

```
/etc/rc.d/init.d/httpd restart
```

Si vous venez de finir de modifier quelque chose dans votre fichier `httpd.conf`, il n'est pas nécessaire d'arrêter et de redémarrer votre serveur. Vous devriez par contre utiliser la commande `reload`. Lorsque vous utilisez `reload`, vous ne devez pas taper votre mot de passe (qui est nécessaire si vous exécutez Apache en tant que serveur sécurisé). Votre mot de passe sera masqué durant les rechargements, mais pas durant les arrêts et redémarrage. La commande `reload` ressemble à ceci :

```
/etc/rc.d/init.d/httpd reload
```

Par défaut, le processus `httpd` démarre automatiquement au lancement de votre ordinateur. Si vous exécutez Apache en tant que serveur sécurisé, une invite vous demandera le mot de passe après le lancement de l'ordinateur, à moins que vous n'ayez désactivé cette protection.

14.2 Directives de configuration dans `httpd.conf`

Le fichier de configuration du serveur Web Apache est `/etc/httpd/conf/httpd.conf`. Le fichier `httpd.conf` est bien commenté et parle de lui-même. Sa configuration par défaut fonctionnera pour la plupart des clients. Vous ne devrez donc probablement pas changer ses directives dans `httpd.conf`. Vous pourriez cependant vouloir vous familiariser avec les options de configuration les plus importantes.

Les fichiers vides `srm.conf` et `access.conf` se trouvent également dans le répertoire `/etc/httpd/conf`. Les fichiers `srm.conf` et `access.conf` était auparavant utilisés, avec `httpd.conf`, comme des fichiers de configuration pour Apache.

Si vous voulez configurer Apache, il vous suffit de modifier `httpd.conf` et de recharger (ou d'arrêter et rallumer) le processus `httpd`. La Section 14.1, *Démarrage et arrêt `httpd`* illustre comment recharger, arrêter et relancer Apache.

Avant de modifier `httpd.conf`, copiez avant tout le fichier original comme `httpd.confold` (ou tout autre nom). Si vous commettez ensuite une erreur durant la modification du fichier de configuration, vous devrez utiliser la copie de sauvegarde.

Si vous commettez une erreur et que votre server Web ne fonctionne pas correctement, la première chose à vérifier est ce que vous avez modifié dans le fichier `httpd.conf`. Vérifiez si vous n'avez pas commis de faute de frappe. La seconde chose à vérifier est le journal des erreurs du serveur Web (`/var/log/httpd/error_log`). Le journal des erreurs peut vous sembler difficile à interpréter si vous manquez d'expérience. Toutefois, si vous venez de rencontrer un problème, les dernières entrées du journal des erreurs devraient fournir certaines indications sur ce qu'il s'est passé.

Les sections suivantes contiennent de brèves descriptions des directives incluses dans le fichier `httpd.conf`, dans l'ordre dans lequel elles se présentent. Ces descriptions ne sont pas exhaustives. Pour plus d'informations, reportez-vous à la documentation d'Apache fournie au format HTML à l'adresse http://*votre_domaine*/manual/ ou à la documentation en ligne du groupe Apache à l'adresse http://httpd.apache.org/docs/ . Pour plus d'informations sur les directives mod_ssl, reportez-vous à la documentation incluse au format HTML à l'adresse http://*votre_domaine*/manual/mod/mod_ssl/, ou consultez le *document mod_ssl User Manual* à l'adresse http://www.modssl.org/docs/2.7/ .

14.2.1 `ServerType`

Votre `ServerType` peut être `inetd` ou `standalone`. Par défaut, votre serveur est paramétré sur `ServerType standalone`.

`ServerType standalone` signifie que le serveur est démarré une fois, après quoi il s'occupe de toutes les connexions. `ServerType inetd` signifie qu'une nouvelle instance du serveur est démarrée pour chaque connexion HTTP. Chaque instance du serveur prend en charge la connexion, puis s'arrête une fois la connexion terminée. Comme vous pouvez l'imaginer, `inetd` n'est pas très efficace. Un autre problème est que `inetd` risque de ne pas fonctionner correctement, selon le groupe Apache. Enfin, du fait que Red Hat Linux 7.1 utilise `xinetd`, une configuration supplémentaire sera nécessaire pour faire en sorte que `xinetd` démarre le serveur. C'est pourquoi il est préférable de laisser le `ServerType` de votre secure Web server paramétré sur `standalone`.

14.2.2 ServerRoot

Le `ServerRoot` est le répertoire de niveau supérieur qui contiendra les fichiers du serveur. Les serveurs tant sécurisé que non sécurisé sont paramétrés pour utiliser le `ServerRoot /etc/httpd`.

14.2.3 LockFile

`LockFile` est le chemin d'accès du fichier de blocage utilisé lorsque le serveur Apache est compilé avec `USE_FCNTL_SERIALIZED_ACCEPT` ou `USE_FLOCK_SERIALIZED_ACCEPT`. `LockFile` doit normalement conserver sa valeur par défaut.

14.2.4 PidFile

`PidFile` est le nom du fichier dans lequel le serveur consigne son identifiant de processus (pid). Votre serveur Web est paramétré pour consigner son pid dans `/var/run/httpd.pid`.

14.2.5 ScoreBoardFile

The `ScoreBoardFile` stocke les informations internes au processus serveur utilisées pour la communication entre le processus serveur père et ses processus fils. Le `ScoreBoardFile` de votre serveur Web est défini sur `/var/run/httpd.scoreboard`.

14.2.6 ResourceConfig

La directive `ResourceConfig` donne pour instruction au serveur de lire un fichier pour plus de directives. Un commentaire est ajouté à la directive `ResourceConfig` car votre serveur Web utilise `httpd.conf` uniquement pour les directives de configuration.

14.2.7 AccessConfig

La directive `AccessConfig` donne pour instruction au serveur de lire le fichier dont le nom figure après `AccessConfig` après avoir lu le fichier nommé `ResourceConfig`. La directive `AccessConfig` est identifiée comme un commentaire parce que votre serveur Web utilise uniquement `httpd.conf` pour les directives de configuration.

14.2.8 Timeout

`Timeout` définit, en secondes, le temps pendant lequel votre serveur attend des réceptions et des émissions en cours de communication. Plus spécifiquement, `Timeout` définit le temps pendant lequel le serveur attend de recevoir une demande GET, le temps pendant lequel il attend de recevoir des paquets TCP sur une requête POST ou PUT et le temps pendant lequel il attend entre des ACK répondant aux paquets TCP. `Timeout` est défini sur 300 secondes, ce qui convient dans la plupart des cas.

14.2.9 KeepAlive

KeepAlive définit si votre serveur autorisera des connexions persistantes (c'est-à-dire plusieurs demandes par connexion). KeepAlive peut être utilisé pour empêcher tout client de consommer trop de ressources du serveur. Par défaut, KeepAlive est défini sur on, ce qui signifie que votre serveur autorise les connexions persistantes. Vous pouvez le définir sur off, ce qui désactive les connexions persistantes. Reportez-vous à la Section 14.2.10, *MaxKeepAliveRequests* pour connaître une manière apparentée de limiter le nombre de demandes par connexion.

14.2.10 MaxKeepAliveRequests

Cette directive définit le nombre maximum de demandes autorisées par connexion persistante. Le groupe Apache recommande d'utiliser un paramétrage élevé, qui améliorera les performances de votre serveur. Par défaut, MaxKeepAliveRequests est paramétré sur 100, ce qui convient dans la plupart des cas.

14.2.11 KeepAliveTimeout

KeepAliveTimeout définit la durée en secondes pendant laquelle votre serveur attendra, après avoir servi une demande, la demande suivante, avant d'interrompre la connexion. Une fois une demande reçue, c'est la directive Timeout qui s'applique à la place.

14.2.12 MinSpareServers et MaxSpareServers

Le serveur Web Apache s'adapte de façon dynamique à la charge reçue en maintenant un nombre de processus serveur de rechange approprié en fonction du trafic. Le serveur vérifie le nombre de processus attendant une requête et en supprime s'ils sont plus nombreux que MaxSpareServers ou en crée s'ils sont moins nombreux que MinSpareServers.

La valeur MinSpareServers par défaut de votre serveur est 5 ; la valeur MaxSpareServers par défaut de votre serveur est 20. Ces paramètres par défaut doivent être appropriés dans presque toutes les situations. Ne définissez pas une valeur très élevée pour MinSpareServers car cela créera une charge de traitement importante sur le serveur, même si le trafic est faible.

14.2.13 StartServers

StartServers définit le nombre de processus créés au démarrage. Du fait que le serveur Web supprime et crée des processus serveur, de façon dynamique en fonction de la charge du trafic, il est inutile de modifier ce paramètre. Votre serveur Web est réglé pour lancer huit processus serveur au démarrage.

14.2.14 MaxClients

`MaxClients` définit une limite au nombre total de processus serveur (c'est-à-dire le nombre de clients connectés simultanément) pouvant s'exécuter en même temps. Conservez une valeur élevée pour `MaxClients` (par défaut, la valeur du serveur est réglée sur 150) car personne d'autre ne sera autorisé à se connecter une fois ce nombre atteint. Vous ne pouvez pas définir pour `MaxClients` une valeur supérieure à 256 sans recompiler Apache. La principale raison d'être de `MaxClients` est d'éviter qu'un serveur Web surchargé ne perturbe votre système d'exploitation.

14.2.15 MaxRequestsPerChild

`MaxRequestsPerChild` définit le nombre total de demandes que chaque processus serveur fils sert avant de disparaître. La principale raison justifiant de définir `MaxRequestsPerChild` consiste à éviter des pertes de mémoire induites par les processus longs. La valeur par défaut de `MaxRequestsPerChild` pour votre serveur est `100`.

14.2.16 Listen

`Listen` identifie les ports sur lesquels votre serveur Web accepte les demandes entrantes. Votre secure Web server est paramétré pour écouter sur le port 80 pour les communications Web non sécurisées et (dans les balises d'hôte virtuel définissant le serveur sécurisé) sur le port 443 pour les communications Web sécurisées.

Si vous paramétrez Apache pour écouter sur un port dont le numéro est inférieur à 1024, le processus `httpd` devra démarrer avec les droits de root. Pour les ports dont le numéro est égal ou supérieur à 1024, `httpd` peut démarrer comme utilisateur normal.

`Listen` peut également être utilisée pour spécifier des adresses IP particulières sur lesquelles le serveur acceptera des connexions.

14.2.17 BindAddress

`BindAddress` permet de spécifier les adresses IP pour lesquelles votre serveur réagira. Utilisez plutôt la directive `Listen` si vous avez besoin de cette fonctionnalité. La commande `BindAddress` n'est pas utilisée par votre serveur Web ; par défaut, elle est identifiée comme un commentaire dans `httpd.conf`.

14.2.18 LoadModule

`LoadModule` est utilisée pour charger des modules DSO (Dynamic Shared Object, objet partagé dynamique). Pour plus d'informations sur le support DSO de secure Web server, y compris la manière précise d'utiliser la directive `LoadModule`, reportez-vous à la Section 14.3, *Ajout de modules au serveur*. L'ordre des modules étant important, ne les déplacez pas.

14.2.19 IfDefine

Les balises <IfDefine> et </IfDefine> entourent des directives de configuration. Elles s'appliquent si le "test" indiqué dans la balise <IfDefine> est vrai ; les directives sont ignorées si le test est faux.

Le test dans les balises <IfDefine> est un nom de paramètre (par exemple, HAVE_PERL). Si le paramètre est défini (c'est-à-dire spécifié comme argument de la commande de démarrage du serveur), le test est vrai. Dans ce cas, votre secure Web server est démarré, le test est vrai et les directives contenues dans les balises IfDefine sont appliquées.

Par défaut, les balises <IfDefine HAVE_SSL> entourent les balises d'hôtes virtuels pour votre serveur sécurisé. Les balises <IfDefine HAVE_SSL> entourent également les directives LoadModule et AddModule pour le ssl_module.

14.2.20 ClearModuleList

ClearModuleList est située immédiatement avant la longue liste de directives AddModule. ClearModuleList efface la liste de modules actifs dans le serveur. Ensuite, la liste de directives AddModule recrée la liste, immédiatement après ClearModuleList.

14.2.21 AddModule

AddModule est la directive utilisée pour créer une liste complète de tous les modules disponibles. Vous utiliserez la directive AddModule si vous ajoutez votre propre module comme DSO. Pour plus d'informations sur la manière dont AddModule est utilisé pour la prise en charge de DSO, reportez-vous à la Section 14.3, *Ajout de modules au serveur*.

14.2.22 ExtendedStatus

ExtendedStatus contrôle le fait qu'Apache génère des informations d'état sommaires (off) ou détaillées (on) lorsque le module de commande server-status est appelé. Server-status est appelé à l'aide des balises Location ; pour plus d'informations sur l'appel de server-status, reportez-vous à la Section 14.2.71, *Location* .

14.2.23 Port

Normalement, Port définit le port sur lequel votre serveur écoute. Toutefois, le secure Web server contrôle plusieurs ports par défaut, du fait que la directive Listen est également utilisée. Lorsque les directives Listen sont activées, votre serveur contrôle tous ces ports. Pour plus d'informations sur Listen, reportez-vous à la description de la directive Listen.

La commande `Port` est également utilisée pour spécifier le numéro de port utilisé pour créer un nom autorisé pour votre serveur. Reportez-vous à la Section 14.2.39, *`UseCanonicalName`* pour plus d'informations sur le nom canonique de votre serveur.

14.2.24 `User`

La directive `User` définit l'ID utilisateur utilisé par le serveur pour répondre aux demandes. Le paramétrage de `User` détermine l'accès au serveur. Tous les fichiers inaccessibles à cet utilisateur seront également inaccessibles aux visiteurs de votre site Web. La valeur par défaut pour `User` est `apache`.

`User` devrait avoir pour seuls privilèges la possibilité d'accéder à des fichiers supposés visibles par le monde extérieur. `User` est également le propriétaire de tous les processus CGI engendrés par le serveur. `User` ne devrait pas être autorisé à exécuter un code non destiné à constituer une réponse à des demandes HTTP.

Remarque

A moins d'être absolument certain de savoir ce que vous faites, ne paramétrez pas `User` sur root. Le fait d'utiliser root comme valeur pour `User` risque d'ouvrir une brèche importante dans la sécurité de votre serveur Web.

Le processus `httpd` parent commence par s'exécuter comme root en cours de fonctionnement normal, puis est immédiatement transmis à l'utilisateur apache. Le serveur doit démarrer comme root parce qu'il doit se relier à un port sous 1024 (le port par défaut pour les communications Web sécurisées est le port 443 ; le port par défaut pour les communications Web non sécurisées est le port 80). Les ports sous 1024 étant réservés à l'usage du système, ils ne peuvent être utilisés que par quelqu'un connecté en tant que root. Une fois que le serveur s'est connecté à son port, il transmet le processus au `User` avant d'accepter la moindre demande de connexion.

14.2.25 `Group`

La directive `Group` est similaire à `User`. `Group` définit le groupe sous lequel le serveur répondra à des demandes. La valeur de `Group` par défaut est également `apache`.

14.2.26 `ServerAdmin`

`ServerAdmin` indique l'adresse électronique de l'administrateur du serveur Web. Cette adresse électronique apparaîtra dans les messages d'erreur sur les pages Web générées par le serveur afin que les utilisateurs puissent signaler un problème en envoyant un message électronique à l'administrateur du serveur. La valeur par défaut de ServerAdmin est `root@localhost`.

Généralement, une bonne manière de configurer `ServerAdmin` consiste à utiliser la valeur `webmaster@votre_domaine.com`. Ensuite, créez un alias pour `webmaster` au nom de la personne responsable du serveur Web, dans `/etc/aliases`. Enfin, exécutez `/usr/bin/newaliases` pour ajouter le nouvel alias.

14.2.27 ServerName

`ServerName` permet de définir un nom pour votre serveur, qui diffère du nom réel de votre hôte. Par exemple, vous pouvez utiliser www.votre_domaine.com alors que le nom réel de votre serveur est foo.votre_domaine.com. Notez que `ServerName` doit être un nom DNS (Domain Name Service) valide de la machine sur laquelle tourne le serveur.

Si vous spécifiez un `ServerName`, assurez-vous que son adresse IP et son nom de serveur sont inclus dans votre fichier `/etc/hosts`.

14.2.28 DocumentRoot

`DocumentRoot` est le répertoire contenant la plupart des fichiers HTML qui seront servis en réponse aux demandes. La valeur de `DocumentRoot` par défaut pour les serveurs Web sécurisés et non sécurisés est `/var/www/html`. Par exemple, le serveur pourrait recevoir une demande pour le document suivant :

```
http://votre_domaine/foo.html
```

Le serveur recherchera le fichier suivant dans le répertoire par défaut :

```
/var/www/html/foo.html
```

Si vous voulez modifier le `DocumentRoot` afin qu'il ne soit pas partagé par les serveurs Web sécurisés et non sécurisés, reportez-vous à la Section 14.4, *Utilisation d'hôtes virtuels*.

14.2.29 Directory

Les balises `<Directory /path/to/directory>` et `</Directory>` sont utilisées pour entourer un groupe de directives de configuration devant uniquement s'appliquer à ce répertoire et tous ses sous-répertoires. Toute directive applicable à un répertoire peut être utilisée à l'intérieur des balises `<Directory>`. Les balises `<File>` peuvent être utilisées de la même manière, appliquées à un fichier spécifique.

Par défaut, des paramètres très restrictifs sont appliqués au répertoire racine, à l'aide des directives `Options` (voir Section 14.2.30, *`Options`*) et `AllowOverride` (voir Section 14.2.31, *`AllowOverride`*). Dans cette configuration, il faut explicitement attribuer ces paramètres à tout répertoire du système ayant besoin de paramètres plus permissifs.

Les balises `Directory` permettent de définir le `DocumentRoot` (désigné comme `"/"`) avec des paramètres moins rigides, de manière à ce qu'il puisse servir des demandes HTTP.

Le répertoire `cgi-bin` est configuré pour permettre l'exécution de scripts CGI avec l'option `ExecCGI`. Si vous devez exécuter un script CGI dans un autre répertoire, vous devez définir `ExecCGI` pour ce répertoire. Par exemple, si votre répertoire `cgi-bin` est `/var/www/cgi-bin` mais que vous voulez exécuter des scripts CGI depuis `/home/mon_répertoire_cgi`, ajoutez une directive `ExecCGI` à un ensemble de directives `Directory` tel que le suivant dans votre fichier `httpd.conf` :

```
<Directory /home/my_cgi_directory>
    Options +ExecCGI
</Directory>
```

Pour permettre l'exécution de scripts CGI dans `/home/my_cgi_directory`, il vous faudra entreprendre des démarches supplémentaires au paramétrage de `ExecCGI`. Vous devrez aussi décommander la directive `AddHandler` pour identifier les fichiers qui ont une extension `.cgi` (scripts CGI). Vous trouverez des instructions sur le paramétrage de `AddHandler` dans la Section 14.2.65, *`AddHandler`* . Les permissions pour les scripts CGI et le chemin d'accès aux scripts doivent être paramétrés à 0755. Enfin, le script et le répertoire doivent être détenus par le même utilisateur.

14.2.30 `Options`

La directive `Options` contrôle les fonctions du serveur disponibles dans un répertoire particulier. Par exemple, en vertu des paramètres restrictifs spécifiés pour le répertoire racine, `Options` est défini uniquement sur `FollowSymLinks`. Aucune fonction n'est activée, à l'exception du fait que le serveur est autorisé à suivre les liens symboliques dans le répertoire racine.

Par défaut, dans votre répertoire `DocumentRoot`, `Options` est paramétré pour inclure `Indexes`, `Includes` et `FollowSymLinks`. `Indexes` permet au serveur de générer le contenu d'un répertoire si aucun `DirectoryIndex` (c'est-à-dire `index.html`, etc.) n'est spécifié. `Includes` signifie que des fichiers à inclure côté serveur sont autorisés. `FollowSymLinks` permet au serveur de suivre des liens symboliques dans ce répertoire.

Vous devez également inclure des instructions `Options` pour les répertoires à l'intérieur de directives d'hôtes virtuels si vous voulez que vos hôtes virtuels reconnaissent ces `Options`.

Par exemple, les fichiers à inclure côté serveur sont déjà activés dans le répertoire `/var/www/html` en raison de la présence de la ligne `Options Includes` dans la section des directives `Location "/"`. Toutefois, si vous voulez qu'un hôte virtuel reconnaisse que les fichiers à inclure côté serveur sont autorisés dans `/var/www/html`, vous devez inclure une section telle que la suivante à l'intérieur des balises de votre hôte virtuel :

```
<Directory /var/www/html>
Options Includes
</Directory>
```

14.2.31 AllowOverride

La directive `AllowOverride` définit si des `Options` peuvent être invalidées par les instructions d'un fichier `.htaccess`. Par défaut, `DocumentRoot` est paramétré pour ne pas autoriser la prise en compte des instructions de fichiers `.htaccess` .

14.2.32 Order

La directive `Order` contrôle simplement l'ordre dans lequel les directives `Allow` et `Deny` sont analysées. Votre serveur est configuré pour analyser les directives `Allow` avant les directives `Deny` pour votre répertoire `DocumentRoot`.

14.2.33 Allow

`Allow` spécifie quel demandeur peut accéder à un répertoire donné. Le demandeur peut être `all`, un nom de domaine, une adresse IP, une adresse IP partielle, une paire réseau/masque réseau, etc. Votre répertoire `DocumentRoot` est configuré pour `Allow` (permettre) les demandes de `all` (tous).

14.2.34 Deny

`Deny` fonctionne exactement comme `allow`, mais vous spécifiez à qui l'accès est refusé. Votre `DocumentRoot` n'est pas configuré pour `deny` (refuser) les demandes de quiconque.

14.2.35 UserDir

`UserDir` est le nom du sous-répertoire, au sein du répertoire de départ personnel de chaque utilisateur, où devraient être placés les fichiers HTML personnels devant être servis par le serveur Web. Par défaut, le sous-répertoire est `public_html`. Par exemple, le serveur pourrait recevoir la demande suivante :

```
http://votre_domaine/~utilisateur/foo.html
```

Le serveur rechercherait le fichier :

```
/home/utilisateur/public_html/foo.html
```

Dans l'exemple ci-dessus, `/home/utilisateur` est le répertoire personnel de l'utilisateur (notez que le chemin d'accès par défaut aux répertoires personnels des utilisateurs peut être différent sur votre système).

Assurez-vous que les autorisations relatives aux répertoires personnels des utilisateurs sont correctement définies. Les répertoires personnels des utilisateurs doivent être définis sur 0755. Les bits de lecture (r) et d'exécution (x) doivent être définis sur les répertoires `public_html` de l'utilisateur (0755 fonctionnera). Les fichiers qui seront servis dans les répertoires `public_html` des utilisateurs doivent être définis sur au moins 0644.

14.2.36 DirectoryIndex

`DirectoryIndex` est la page servie par défaut lorsqu'un utilisateur demande un index de répertoire en insérant une barre oblique (/) à la fin de l'URL.

Lorsqu'un utilisateur demande la page http://*votre_domaine*/*ce_répertoire*/, il obtient soit la page `DirectoryIndex`, si elle existe, soit la liste du contenu du répertoire générée par le serveur. La valeur par défaut pour `DirectoryIndex` est `index.html index.htm index.shtml index.php index.php4 index.php3 index.cgi`. Le serveur essaie de trouver l'un de ces fichiers et retourne le premier qu'il trouve. S'il ne trouve aucun de ces fichiers et si `Options Indexes` est paramétré pour ce répertoire, le serveur génère et retourne une liste, au format HTML, des fichiers et sous-répertoires contenus dans le répertoire.

14.2.37 AccessFileName

`AccessFileName` nomme le fichier que le serveur doit utiliser pour les informations de contrôle d'accès dans chaque répertoire. Par défaut, votre serveur Web est paramétré pour utiliser `.htaccess`, s'il existe, afin d'accéder aux informations de contrôle d'accès dans chaque répertoire.

Juste après la directive `AccessFileName`, une série de balises `Files` appliquent un contrôle d'accès à tout fichier commençant par `.ht`. Ces directives refusent l'accès Web à tous les fichiers `.htaccess` (ou d'autres commençant par `.ht`) pour des raisons de sécurité.

14.2.38 CacheNegotiatedDocs

Par défaut, votre serveur Web demande aux serveurs proxy de ne pas mettre en cache des documents négociés sur la base du contenu (c'est-à-dire qui peuvent changer avec le temps ou suite à l'entrée du demandeur). Si vous annulez le commentaire de `CacheNegotiatedDocs`, vous désactivez cette fonction et les serveurs proxy seront autorisés à mettre en cache les documents à partir de ce moment.

14.2.39 UseCanonicalName

`UseCanonicalName` est paramétré par défaut sur `on`. `UseCanonicalName` permet au serveur de créer une URL qui se référence elle-même, en utilisant `ServerName` et `Port`. Lorsque le serveur fait référence à lui-même en réponse aux demandes des clients, il utilise cette URL. Si vous paramétrez `UseCanonicalName` sur `off`, le serveur utilisera plutôt la valeur figurant dans la demande du client pour pointer sur lui-même.

14.2.40 TypesConfig

`TypesConfig` nomme le fichier qui définit la liste par défaut des correspondances de type MIME (extensions de nom de fichier associées à des types de contenu). Le fichier `TypesConfig` par défaut

est `/etc/mime.types`. Au lieu d'éditer `/etc/mime.types`, il est recommandé d'ajouter des types MIME à l'aide de la directive `AddType`.

14.2.41 DefaultType

`DefaultType` définit un type de contenu par défaut pour le serveur Web à utiliser pour des documents dont les types MIME ne peuvent pas être déterminés. Par défaut, votre serveur Web suppose que tout fichier au contenu indéterminé est de type texte brut.

14.2.42 IfModule

Les balises `<IfModule>` et `</IfModule>` entourent des directives conditionnelles. Les directives contenues à l'intérieur des balises `IfModule` sont traitées dans l'un des deux cas suivants. Les directives sont traitées si le module contenu dans la balise de début `<IfModule>` est compilé dans le serveur Apache. Si un point d'exclamation ("!") est inclus devant le nom du module, les directives ne sont traitées que si le module dans la balise de départ `<IfModule>` n'est *pas* compilé.

Le fichier `mod_mime_magic.c` est utilisé dans ces balises `IfModule`. Le module mod_mime_magic est comparable à la commande UNIX `file`, qui examine quelques octets du contenu d'un fichier, puis utilise des "nombres magiques" et d'autres indices pour déterminer le type MIME du fichier.

Si le module mod_mime_magic est compilé dans Apache, ces balises `IfModule` indiquent au module mod_mime_magic où se trouve le fichier de définition des indices : `share/magic` dans ce cas.

Le module mod_mime_magic n'est pas compilé par défaut. Si vous voulez l'utiliser, reportez-vous à la Section 14.3, *Ajout de modules au serveur* pour plus de détails sur la manière d'ajouter des modules à votre serveur.

14.2.43 HostnameLookups

`HostnameLookups` peut être défini sur `on`, `off` ou `double`. Si vous autorisez `HostnameLookups` (en le paramétrant sur `on`), votre serveur résoudra automatiquement l'adresse IP pour chaque connexion demandant un document de votre serveur Web. La résolution de l'adresse IP signifie que votre serveur établit une ou plusieurs connexions avec le DNS pour rechercher le nom d'hôte correspondant à une adresse IP particulière. Si vous paramétrez `HostnameLookups` en `double`, votre serveur établira un DNS double inversé. En d'autres termes, après la recherche inverse (IP vers nom), une recherche en avant (nom vers IP) est lancée sur le résultat. Cette double recherche doit ramener à l'adresse IP de départ.

Généralement, vous devez laisser `HostnameLookups` paramétré sur `off`, du fait que les demandes de DNS ajoutent une charge à votre serveur et peuvent le ralentir. Si votre serveur est occupé, les effets de `HostnameLookups` peuvent être sensibles.

`HostnameLookups` pose également une question pour Internet dans son ensemble. Les connexions individuelles établies pour rechercher chaque nom d'hôte s'additionnent. C'est pourquoi, pour le bien

de votre propre serveur Web, de même que pour celui d'Internet dans son ensemble, laissez `HostnameLookups` paramétré sur `off`.

14.2.44 ErrorLog

`ErrorLog` nomme le fichier dans lequel sont consignées les erreurs du serveur. Comme cette directive l'indique, le fichier journal des erreurs relatif à votre serveur Web se trouve dans `/var/log/httpd/error_log`.

Le journal des erreurs est intéressant si votre serveur Web génère des erreurs ou des pannes dont vous ne connaissez pas la cause.

14.2.45 LogLevel

`LogLevel` définit le niveau de détail des messages d'erreur des journaux des erreurs. `LogLevel` peut être défini (du moins détaillé au plus détaillé) sur `emerg`, `alert`, `crit`, `error`, `warn`, `notice`, `info` ou `debug`. Par défaut, le `LogLevel` de votre serveur Web est défini sur `warn`.

14.2.46 LogFormat

Les directives `LogFormat` de votre fichier `httpd.conf` définissent un format pour les messages d'erreur ; ce format devrait rendre votre journal des accès plus lisible.

14.2.47 CustomLog

`CustomLog` identifie le fichier journal et le format de fichier journal. Dans la configuration par défaut de votre secure Web server, `CustomLog` définit le fichier journal dans lequel sont consignés les accès à votre serveur Web : `/var/log/httpd/access_log`. Vous devez connaître l'emplacement de ce fichier pour pouvoir générer des statistiques concernant les performances d'accès à votre serveur Web.

`CustomLog` définit également le format du fichier journal ordinaire. Le format du fichier journal ordinaire ressemble à ceci :

```
remotehost rfc931 authuser [date] "request" status bytes
```

remotehost

Nom d'hôte distant. Si le nom d'hôte n'est pas disponible auprès du DNS, ou si `HostnameLookups` est paramétré sur `Off`, *`remotehost`* sera l'adresse IP de l'hôte distant.

rfc931

Non utilisé. Le signe `-` figure dans le fichier journal à sa place.

authuser

Si l'authentification est requise, il s'agit du nom sous lequel l'utilisateur s'est identifié. Habituellement, il n'est pas utilisé, de sorte que vous voyez le signe `-` à sa place.

`[date]`

La date et l'heure de la demande.

`"demande"`

La chaîne de demande telle qu'elle est venue du navigateur ou du client.

`status`

Code d'état retourné au navigateur ou au client.

`octets`

Taille du document.

La commande `CustomLog` permet de configurer des fichiers journaux spécifiques pour enregistrer des pointeurs (URL de la page Web liée à une page de votre serveur Web) et/ou des agents (navigateurs utilisés pour récupérer des pages Web sur votre serveur Web). Les lignes `CustomLog` correspondantes sont identifiées comme des commentaires, comme illustré, mais vous devez supprimer le commentaire si vous voulez utiliser ces deux fichiers journaux :

```
#CustomLog /var/log/httpd/referer_log referer
#CustomLog /var/log/httpd/agent_log agent
```

Vous pouvez également définir la directive `CommonLog` pour qu'elle utilise un journal combiné en supprimant le commentaire de la ligne suivante :

```
#CustomLog /var/log/httpd/access_log combined
```

Un journal combiné ajoutera les champs du pointeur et de l'agent à la fin des champs de journal communs. Si vous voulez utiliser un journal combiné, commentez la directive `CustomLog` définissant votre journal des accès sur le format de fichier journal commun.

14.2.48 `ServerSignature`

La directive `ServerSignature` ajoute une ligne contenant la version du serveur Apache et le `ServerName` de l'hôte servant à tout document généré par le serveur (par exemple, les messages d'erreur renvoyés à des clients). `ServerSignature` est paramétré sur `on` par défaut. Vous pouvez définir la valeur `off` afin qu'aucune ligne de signature ne soit ajoutée, ou définir la valeur `EMail`. `EMail` ajoute une balise HTML `mailto:ServerAdmin` à la ligne de signature.

14.2.49 Alias

Le paramètre `Alias` permet aux répertoires de se trouver en dehors du répertoire `DocumentRoot` tout en restant accessibles au serveur Web. Toute URL se terminant par l'alias sera automatiquement convertie en chemin d'accès de l'alias. Par défaut, un alias est déjà configuré. Un répertoire `icons` est accessible par le serveur Web, mais le répertoire n'est pas le `DocumentRoot`. Le répertoire `icons`, un alias, est en réalité `/var/www/icons/`, pas `/var/www/html/icons/`.

14.2.50 ScriptAlias

Le paramètre `ScriptAlias` définit l'endroit où les scripts CGI (ou d'autres types de scripts) peuvent être trouvés. Généralement, il est préférable de ne pas laisser de scripts CGI dans `DocumentRoot`. Si des scripts CGI figurent dans `DocumentRoot`, ils pourraient être considérés comme des documents de texte. Même s'il vous est indifférent que certaines personnes peuvent voir (et utiliser) vos scripts CGI, le fait de révéler la manière dont ils fonctionnent peut permettre à des personnes peu scrupuleuses d'exploiter d'éventuelles failles de sécurité du script, menaçant ainsi la sécurité de votre serveur. Par défaut, le répertoire `cgi-bin` est un `ScriptAlias` de `/cgi-bin/`, et se trouve en réalité dans `/var/www/cgi-bin/`.

`Options ExecCGI` est sélectionné pour votre répertoire `/var/www/cgi-bin`, ce qui signifie que l'exécution de scripts CGI est autorisée dans ce répertoire.

Reportez-vous à la Section 14.2.65, *`AddHandler`* et à la Section 14.2.29, *`Directory`* pour obtenir des instructions sur la manière d'exécuter des scripts CGI dans des répertoires autres que `cgi-bin`.

14.2.51 Redirect

Lorsqu'une page Web est déplacée, la commande `Redirect` peut être utilisée pour mapper l'ancienne URL sur une autre URL. Le format est le suivant :

```
Redirect /chemin/foo.html http://nouveau_domaine/chemin/foo.html
```

Ainsi, si une demande HTTP est reçue pour une page qui se trouve habituellement à l'URL http://*votre_domaine*/*chemin*/foo.html, le serveur retourne la nouvelle URL (http://*nouveau_domaine*/*chemin*/foo.html) au client, qui essaie d'extraire le document de la nouvelle URL.

14.2.52 IndexOptions

contrôle l'aspect des listes de contenu de répertoire générées par le serveur en ajoutant des icônes et des descriptions de fichiers, etc. Si `Options Indexes` est défini (voir Section 14.2.30, *`Options`*), votre serveur Web peut générer une liste du contenu du répertoire lorsqu'il reçoit une demande HTTP telle que celle-ci :

http://*votre_domaine*/*ce_répertoire*

Tout d'abord, votre serveur Web recherche dans ce répertoire un fichier de la liste figurant après la directive `DirectoryIndex` (par exemple, `index.html`). Si votre serveur Web ne trouve pas l'un de ces fichiers, il génère une liste HTML des fichiers et sous-répertoires figurant dans ce répertoire. Vous pouvez modifier l'aspect de cette liste du contenu du répertoire à l'aide de certaines directives de `httpd.conf`, notamment `IndexOptions`.

Par défaut, `FancyIndexing` est activé. Si `FancyIndexing` est activé, le fait de cliquer sur les en-têtes de colonne de la liste modifie l'ordre d'affichage en fonction du contenu de cette colonne. Un autre clic sur le même en-tête permet de basculer de l'ordre ascendant à l'ordre descendant, et inversement. `FancyIndexing` affiche également des icônes différentes pour les différents fichiers, en fonction des extensions de fichier. Si vous utilisez la directive `AddDescription` et activez `FancyIndexing`, une brève description de fichier sera incluse dans la liste du contenu du répertoire générée par le serveur.

`IndexOptions` comprend un certain nombre d'autres paramètres qui peuvent être définis pour contrôler l'aspect des répertoires générés par le serveur. Les paramètres incluent `IconHeight` et `IconWidth`, pour faire en sorte que le serveur inclue des balises HTML `HEIGHT` et `WIDTH` pour les icônes dans les pages Web générées par le serveur ; `IconsAreLinks`, pour faire en sorte que les icônes agissent comme une partie de l'ancre du lien HTML, en même temps que le nom de fichier, et autres.

14.2.53 AddIconByEncoding

Cette directive nomme des icônes qui seront affichées par fichier, avec codage MIME, dans des listes de répertoire générées par le serveur. Par défaut, votre serveur Web montre l'icône `compressed.gif` à côté des fichiers codés MIME x-compress et x-gzip dans des listes de répertoire générées par serveur.

14.2.54 AddIconByType

Cette directive nomme des icônes qui s'afficheront à côté des fichiers avec des types MIME dans des listes de répertoire générées par serveur. Par exemple, votre serveur est paramétré pour afficher l'icône `text.gif` à côté de fichiers avec un type MIME "texte" dans des listes de répertoire générées par serveur.

14.2.55 AddIcon

`AddIcon` indique au serveur l'icône à afficher dans les listes de répertoire générées par le serveur pour certains types de fichiers ou pour des fichiers avec certaines extensions. Par exemple, votre serveur Web est paramétré pour afficher l'icône `binary.gif` pour les fichiers portant les extensions `.bin` ou `.exe`.

14.2.56 DefaultIcon

`DefaultIcon` nomme l'icône à afficher dans les listes de répertoire générées par le serveur pour les fichiers pour lesquels aucune autre icône n'est spécifiée. `unknown.gif` est la `DefaultIcon` par défaut pour ces fichiers.

14.2.57 AddDescription

Vous pouvez utiliser `AddDescription` pour afficher le texte que vous spécifiez pour certains fichiers dans les listes du contenu de répertoires générées par le serveur (vous devez également activer `FancyIndexing` comme une `IndexOptions`). Vous pouvez nommer des fichiers spécifiques, utiliser des expressions comprenant des caractères spéciaux de recherche ou des extensions de fichier pour spécifier les fichiers auxquels cette directive devrait s'appliquer. Par exemple, vous pourriez utiliser la ligne suivante :

```
AddDescription "Fichier se terminant par .ni"
```

Dans les listes de répertoire générées par serveur, les noms de tous les fichiers portant des extensions `.ni` seraient suivis de la description `Fichier se terminant par .ni`. Il faut également que `FancyIndexing` soit activé.

14.2.58 ReadmeName

nomme le fichier qui (s'il existe dans le répertoire) sera ajouté à la fin des listes de répertoire générées par serveur. Le serveur Web commencera par essayer d'inclure le fichier comme document HTML, puis essaiera de l'inclure comme texte brut. Par défaut, `ReadmeName` est paramétré sur `README`.

14.2.59 HeaderName

`HeaderName` nomme le fichier qui (s'il existe dans le répertoire) sera ajouté au début des listes de répertoire générées par serveur. Comme `ReadmeName`, le serveur essaiera, si possible, de l'inclure sous la forme d'un document HTML, ou, sinon, comme texte brut.

14.2.60 IndexIgnore

`IndexIgnore` affiche une liste d'extensions de fichier, de noms de fichier partiels, d'expressions contenant des caractères spéciaux de recherche ou de noms de fichiers complets. Le serveur Web n'inclura pas les fichiers correspondant à l'un de ces paramètres dans les listes de répertoire générées par serveur.

14.2.61 AddEncoding

`AddEncoding` nomme des extensions de nom de fichier qui devraient spécifier un type de codage particulier. `AddEncoding` permet également de donner pour instruction à certains navigateurs (pas tous) de décompresser certains fichiers pendant leur déchargement.

14.2.62 AddLanguage

`AddLanguage` associe des extensions de nom de fichiers à des langues spécifiques. Cette directive est essentiellement utile pour la négociation de contenu, lorsque le serveur retourne un document parmi d'autres, en fonction de la préférence linguistique du client telle que définie dans son navigateur.

14.2.63 LanguagePriority

`LanguagePriority` permet de définir l'ordre de préféence des langues pour le service des fichiers, qui produit un effet si le client n'a paramétré aucune préférence linguistique dans son navigateur.

14.2.64 AddType

Utilisez la directive `AddType` pour définir des paires de type MIME et d'extension de fichier. Par exemple, si vous utilisez PHP4, votre serveur Web utilise la directive `AddType` afin de reconnaître les fichiers portant l'extension PHP (`.php4`, `.php3 .phtml .php`) comme des types MIME PHP.

La ligne `AddType` suivante indique au serveur de reconnaître l'extension de fichier `.shtml` (pour fichiers à inclure côté serveur) :

```
AddType text/html .shtml
```

Vous devrez inclure la ligne ci-dessus à l'intérieur des balises de l'hôte virtuel pour tous les hôtes virtuels devant autoriser des fichiers à inclure côté serveur.

14.2.65 AddHandler

`AddHandler` mappe des extensions de fichier sur des modules de commande spécifiques. Par exemple, le module de commande `cgi-script` peut être utilisé en association avec l'extension `.cgi` pour traiter automatiquement un fichier dont le nom se termine par `.cgi` comme un script CGI. Ceci fonctionnera même pour les fichiers situés hors du répertoire `ScriptAlias` (si vous suivez les instructions fournies ici).

Vous avez une ligne CGI `AddHandler` dans votre fichier `httpd.conf` :

```
AddHandler cgi-script .cgi
```

Il faut supprimer le commentaire de la ligne. Ensuite, Apache exécutera les scripts CGI pour les fichiers se terminant par `.cgi`, même s'ils se trouvent hors du répertoire `ScriptAlias`, qui est défini par défaut pour contenir votre répertoire `/cgi-bin/` dans `/var/www/cgi-bin/`.

Vous devez également définir `ExecCGI` comme `Options` pour tout répertoire contenant un script CGI. Reportez-vous à la Section 14.2.29, *`Directory`* pour plus d'informations sur la définition de `ExecCGI` pour un répertoire. Vous devrez en outre vous assurer que les autorisations sont correctement définies pour les scripts CGI et les répertoires contenant des scripts CGI. Les scripts CGI et tout le chemin d'accès aux scripts doivent être paramétrés sur 0755. Enfin, le propriétaire du répertoire et celui du fichier de script doivent coïncider.

Vous devrez ajouter la même ligne `AddHandler` à votre configuration `VirtualHost` si vous utilisez des hôtes virtuels et voulez qu'ils reconnaissent également des scripts CGI hors de `ScriptAlias`.

Outre des scripts CGI, votre serveur Web utilise également `AddHandler` pour traiter des fichiers HTML analysés par le serveur.

14.2.66 `Action`

`Action` vous permet d'associer un type MIME à un CGI, de sorte que chaque demande d'un fichier de ce type déclenche l'exécution d'un script CGI particulier.

14.2.67 `MetaDir`

`MetaDir` spécifie le nom d'un répertoire où votre serveur Web doit rechercher des fichiers contenant des informations META (en-têtes HTTP supplémentaires) à inclure lorsqu'il sert des documents.

14.2.68 `MetaSuffix`

`MetaSuffix` spécifie le suffixe du nom du fichier contenant les informations META (en-têtes HTTP supplémentaires), qui devrait se trouver dans le répertoire `MetaDir`.

14.2.69 `ErrorDocument`

Par défaut, en cas de problème ou d'erreur, votre serveur Web renvoie un simple message d'erreur (habituellement obscur) au client ayant formulé la demande. Au lieu d'utiliser le paramétrage par défaut, vous pouvez utiliser `ErrorDocument` afin de configurer votre serveur Web pour qu'il renvoie un message personnalisé ou redirige le client vers une URL locale ou externe. `ErrorDocument` associe simplement un code de réponse HTTP à un message ou à une URL qui sera renvoyé au client.

14.2.70 `BrowserMatch`

La directive `BrowserMatch` permet à votre serveur de définir des variables d'environnement et/ou de prendre des mesures appropriées en fonction du champ d'en-tête User-Agent HTTP qui identifie le navigateur du client. Par défaut, votre serveur Web utilise `BrowserMatch` pour refuser des connexions à certains navigateurs présentant des problèmes connus de même que pour désactiver les keepalives et vidages d'en-tête HTTP pour les navigateurs ayant des problèmes avec ces actions.

14.2.71 `Location`

Les balises `<Location>` et `</Location>` permettent de spécifier un contrôle d'accès basé sur l'URL.

L'utilisation suivante des balises `Location` consiste à les placer à l'intérieur des balises `IfModule mod_perl.c`. Ces directives de configuration sont effectives si le DSO `mod_perl.so` est chargé. Reportez-vous à la Section 14.3, *Ajout de modules au serveur* pour plus d'informations sur l'ajout de modules à Apache.

Les balises `Location` nomment le répertoire `/var/www/perl` (`Alias` pour `/perl`) comme celui à partir duquel les scripts Perl seront servis. Si un document est demandé avec une URL dans le chemin de laquelle figure la chaîne `/perl`, votre serveur Web recherche le script Perl approprié dans `/var/www/perl/`.

Plusieurs autres options de `<Location>` sont identifiées comme des commentaires dans votre fichier `httpd.conf`. Si vous voulez activer leur fonctionnalité, supprimez le commentaire de la section appropriée des directives.

Immédiatement après les directives Perl décrites plus haut, votre fichier `httpd.conf` contient une section de directives permettant d'activer HTTP PUT (par exemple, la fonction de publication de Netscape Gold qui permet de publier des pages Web sur un serveur Web). Si vous voulez autoriser HTTP PUT, vous devez supprimer le commentaire de cette section toute entière :

```
#Alias /upload /tmp
#<Location /upload>
#    EnablePut On
#    AuthType Basic
#    AuthName Temporary
#    AuthUserFile /etc/httpd/conf/passwd
#    EnableDelete Off
#    umask 007
#    <Limit PUT>
#       require valid-user
#    </Limit>
#</Location>
```

Vous devrez aussi annuler les commentaires des lignes suivantes au début de `httpd.conf`, de façon à ce que le module mod_put se charge dans Apache.

```
#LoadModule put_module          modules/mod_put.so
#AddModule mod_put.c
```

Si vous voulez permettre aux personnes qui se connectent depuis votre domaine de consulter des rapports sur l'état du serveur, annulez le commentaire de la section de directives suivante :

```
#<Location /server-status>
```

```
#    SetHandler server-status
#    Order deny,allow
#    Deny from all
#    Allow from .votre_domaine.com
#</Location>
```

Vous devez remplacer `.votre_domaine.com` par votre nom de domaine de second niveau.

Si vous voulez fournir des rapports de configuration de serveur (y compris des modules installés et des directives de configuration) en réponse à des demandes en provenance de votre domaine, vous devez supprimer le commentaire des lignes suivantes :

```
#<Location /server-info>
#    SetHandler server-info
#    Order deny,allow
#    Deny from all
#    Allow from .votre_domaine.com
#</Location>
```

Une fois encore, vous devez remplacer `.votre_domaine.com`.

La section de directives suivante utilise des balises `Location` pour permettre l'accès à la documentation dans `/usr/share/doc` (par exemple, avec une URL telle que http://*votre_domaine*/doc/fichier.html) . Ces directives permettent uniquement cet accès aux demandes faites depuis l'hôte local.

Une autre utilisation des balises `Location` est définie dans une section identifiée comme un commentaire destinée à permettre un suivi des attaques dirigées contre votre serveur Web qui exploitent un vieux bogue d'avant Apache 1.1. Si vous voulez effectuer un suivi de ces demandes, supprimez le commentaire des lignes suivantes :

```
#<Location /cgi-bin/phf*>
#    Deny from all
#    ErrorDocument 403 http://phf.apache.org/phf_abuse_log.cgi
#</Location>
```

Si ces lignes ne sont pas identifiées comme des commentaires, votre serveur Web redirige toute demande se terminant par `/cgi-bin/phf*` vers un script CGI de journalisation exécuté par le groupe Apache.

14.2.72 `ProxyRequests`

Si vous supprimez le commentaire des balises `IfModule` entourant la section `ProxyRequests`, votre serveur Apache fonctionnera également comme un serveur Proxy. Vous devez également charger le module `mod_proxy`. Pour obtenir des instructions sur la manière de charger des modules, reportez-vous à la Section 14.3, *Ajout de modules au serveur*.

14.2.73 ProxyVia

La commande ProxyVia contrôle si une ligne d'en-tête HTTP Via: est envoyée en même temps que les demandes ou les réponses transitant par le serveur proxy Apache. L'en-tête Via: indique le nom d'hôte si ProxyVia a pour valeur On, le nom d'hôte et la version d'Apache s'il a pour valeur Full, toutes les lignes Via: sont transférées inchangées s'il a pour valeur Off, et les lignes Via: sont supprimées s'il a pour valeur Block.

14.2.74 Directives cache

Plusieurs directives cache sont identifiées comme des commentaires dans les balises proxy IfModule mentionnées plus haut. Si vous utilisez la fonctionnalité du serveur proxy et voulez également activer le cache proxy, supprimez le commentaire des directives cache en procédant de la manière décrite. Les paramètres par défaut pour vos directives cache doivent être appropriés pour la plupart des configurations.

CacheRoot définit le nom du répertoire qui contiendra les fichiers mis en cache. Le CacheRoot par défaut est /var/cache/httpd.

CacheSize définit la quantité d'espace que le cache peut utiliser, exprimée en Ko. La valeur de CacheSize par défaut est 5 Ko.

CacheGcInterval définit un nombre d'heures. Une fois ce délai écoulé, les fichiers du cache sont supprimés si le cache utilise un espace supérieur à celui défini pour CacheSize. La valeur par défaut de CacheGcInterval est de quatre heures.

Les documents HTML mis en cache seront retenus (sans rechargement du serveur Web dont ils proviennent) dans le cache pendant le nombre d'heures maximum défini par CacheMaxExpire. La valeur par défaut est de 24 heures.

Le paramètre CacheLastModifiedFactor affecte la création d'une date d'expiration pour un document qui a été reçu du serveur sans date d'expiration définie. La valeur par défaut de CacheLastModifiedFactor est 0.1, ce qui signifie que la date d'expiration d'un document de ce type est égale à un dixième du temps écoulé depuis la dernière modification du document.

CacheDefaultExpire est le temps d'expiration, exprimé en heures, d'un document reçu à l'aide d'un protocole ne prenant pas en charge les délais d'expiration. La valeur par défaut est d'une heure.

Tout document récupéré sur un hôte et/ou un domaine correspondant à celui défini dans NoCache ne sera pas mis en cache. Si vous avez connaissance d'hôtes ou de domaines dont vous ne voulez pas mettre les documents en cache, supprimez le commentaire devant NoCache et définissez ici leurs noms de domaine ou d'hôte.

14.2.75 NameVirtualHost

Vous devrez utiliser la directive `NameVirtualHost` pour l'adresse IP (et le numéro de port, si nécessaire) de tout hôte virtuel nommé que vous configurez. La configuration d'hôtes virtuels nommés est utilisée pour configurer plusieurs hôtes virtuels pour plusieurs domaines, lorsque vous n'avez pas (ou ne voulez pas utiliser) d'adresses IP différentes pour les différents noms de domaine pour lesquels votre serveur Web sert des documents.

Remarque

Vous ne pouvez pas utiliser d'hôtes virtuels nommés avec votre serveur sécurisé. Tout hôte virtuel nommé que vous configurez ne peut fonctionner qu'avec des connexions HTTP non sécurisées, et non avec des connexions SSL.

Vous ne pouvez pas utiliser d'hôtes virtuels nommés avec votre serveur sécurisé parce que l'établissement de liaison SSL (lorsque le navigateur accepte le certificat d'authentification du serveur Web sécurisé) intervient avant la demande HTTP qui identifie l'hôte virtuel nommé correct. Autrement dit, l'authentification intervient avant l'identification des différents hôtes virtuels nommés. Si vous voulez utiliser des hôtes virtuels avec votre serveur sécurisé, vous devez opter pour des hôtes virtuels basés sur l'adresse IP.

Si vous utilisez des hôtes virtuels basés sur le nom, supprimez le commentaire de la directive de configuration `NameVirtualHost` et ajoutez l'adresse IP correcte de votre serveur derrière `NameVirtualHost`. Ajoutez ensuite des informations supplémentaires sur les différents domaines utilisant les balises `Virtual Host` qui entourent `ServerName` pour chaque hôte virtuel, plus toutes les autres directives de configuration exclusivement applicables à cet hôte virtuel.

14.2.76 VirtualHost

Des balises `<VirtualHost>` et `</VirtualHost>` entourent toutes les directives de configuration destinées à être appliquées à un hôte virtuel. La plupart des directives de configuration peuvent être utilisées à l'intérieur de balises d'hôte virtuel, et s'appliquent exclusivement à cet hôte virtuel particulier.

Des balises `VirtualHost` identifiées comme des commentaires entourent certains exemples de directives de configuration et espaces réservés aux informations à entrer pour configurer un hôte virtuel. Reportez-vous à la Section 14.4, *Utilisation d'hôtes virtuels* pour plus d'informations sur les hôtes virtuels.

14.2.77 `SetEnvIf`

La directive de configuration Apache `SetEnvIf` permet de désactiver la fonction keep-alive HTTP et d'autoriser SSL à fermer la connexion sans générer d'alerte de notification de fermeture du navigateur client. Ce paramètre est nécessaire pour certains navigateurs qui n'interrompent pas la connexion SSL avec une grande fiabilité.

14.2.78 Directives de configuration SSL

Les directives SSL figurant dans le fichier `httpd.conf` de votre serveur sont incluses pour permettre des communications Web sécurisées à l'aide de SSL et TLS.

Pour plus d'informations sur les directives SSL, utilisez votre navigateur pour consulter la page http://*votre_domaine*/manual/mod/mod_ssl/. Pour plus d'informations sur les directives SSL, reportez-vous à la page http://www.modssl.org/docs/2.7/ssl_reference.html, un chapitre sur mod_ssl rédigé par Ralf Engelschall. Ce document, le mod_ssl *User Manual*, commence à l'URL http://www.modssl.org/docs/2.7/ et constitue une excellente référence pour mod_ssl (évidemment) et pour la cryptographie Web en général. Ce manuel contient des informations générales sur la sécurisation de votre serveur Web, au Chapitre 13, *Utilisation d'Apache comme serveur Web sécurisé*.

Remarque

Ne modifiez pas vos directives SSL si vous n'êtes pas absolument certain de savoir ce que vous faites. Pour la grande majorité des secure Web server, la configuration par défaut des directives SSL convient parfaitement.

14.3 Ajout de modules au serveur

Du fait qu'Apache 1.3 prend en charge les objets partagés dynamiques (DSO), vous pouvez aisément charger des modules SSL ou compiler vos propres modules pour le secure Web server. La prise en charge des objets partagés dynamiques signifie qu'il est possible de charger des modules lors de l'exécution. Du fait que les modules ne sont chargés que lorsque c'est nécessaire, ils n'utilisent de mémoire que s'ils sont chargés et nécessitent, globalement, moins de mémoire.

Le groupe Apache fournit une documentation DSO complète sur les objets partagés dynamiques à l'adresse http://www.apache.org/docs/dso.html. Une fois votre serveur installé, vous pouvez également consulter la page http:// *votre_domaine*/manual/mod/ afin d'obtenir une documentation sur les modules Apache au format HTML (si vous avez installé le paquetage `apache-manual`). Une description sommaire du mode de chargement des modules figure ci-après ; pour plus de détails, reportez-vous aux URL fournies.

Pour que le secure Web server utilise un module partagé de façon dynamique, celui-ci doit comprendre une ligne `LoadModule` et une ligne `AddModule` dans `httpd.conf`. Par défaut, de nombreux modules comprennent déjà ces deux lignes dans `httpd.conf` ; toutefois, seuls quelques-uns des modules les moins souvent utilisés sont identifiés comme des commentaires. Les modules identifiés comme des commentaires ont été inclus durant la compilation, mais ne sont pas chargés par défaut.

Si vous devez utiliser l'un de ces modules non chargés, reportez-vous au fichier `httpd.conf` pour voir tous les modules disponibles. A chaque module disponible correspond une ligne `LoadModule`. Par exemple, la section `LoadModule` commence par ces sept lignes :

```
#LoadModule mmap_static_module modules/mod_mmap_static.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule env_module         modules/mod_env.so
LoadModule config_log_module  modules/mod_log_config.so
LoadModule agent_log_module   modules/mod_log_agent.so
LoadModule referer_log_module modules/mod_log_referer.so
#LoadModule mime_magic_module  modules/mod_mime_magic.so
```

La plupart des lignes ne sont pas identifiées comme des commentaires, ce qui indique que le module qui y est associé a été compilé et est chargé par défaut. La première ligne est identifiée comme un commentaire, ce qui signifie que le module correspondant (`mmap_static_module`) a été compilé mais non chargé.

Pour faire en sorte que le secure Web server charge un module non chargé, commencez par supprimer le commentaire de la ligne `LoadModule` correspondante. Par exemple, si vous voulez faire en sorte que le secure Web server charge `mime_magic_module`, modifiez cette ligne `LoadModule` par rapport à l'original :

```
#LoadModule mime_magic_module modules/mod_mime_magic.so
```

Supprimez ensuite le commentaire de la ligne correspondante dans la section `AddModule` du fichier `httpd.conf`. Pour continuer avec l'exemple précédent, supprimez le commentaire de la ligne `mod_mime_magic`. La ligne originale (par défaut) ressemble à ceci :

```
#AddModule mod_mime_magic.c
```

Après avoir supprimé le commentaire des lignes `LoadModule` et `AddModule` pour le module que vous voulez charger, arrêtez, puis démarrez votre serveur Web, comme expliqué à la Section 14.1, *Démarrage et arrêt `httpd`*. Après le démarrage, le module doit se charger dans Apache.

Si vous avez votre module personnel, vous pouvez l'ajouter au fichier `httpd.conf` afin qu'il soit compilé et chargé comme un objet partagé dynamique. Pour ce faire, vous devez installer le paquetage `apache-devel`, en procédant de la manière décrite à la Chapitre 13, *Utilisation d'Apache comme serveur Web sécurisé*. Vous avez besoin du paquetage `apache-devel` parce qu'il installe les fichiers à inclure, les fichiers d'en-tête et l'outil de support APache eXtenSion (APXS). APXS utilise

les fichiers à inclure et les fichiers d'en-tête pour compiler votre module de manière à ce qu'il fonctionne avec Apache.

AVERTISSEMENT

Si vous avez l'intention d'utiliser l'outil de configuration Apache, un utilitaire graphique fourni avec Red Hat Linux, vous ne devez ni compiler les modules de votre serveur Web Apache ni éditer le fichier de configuration `httpd.conf` de votre serveur Web. Inversement, si vous voulez ajouter des modules à Apache ou éditer manuellement `httpd.conf`, n'utilisez pas l'outil de configuration Apache.

Pour plus d'informations sur l'outil de configuration Apache, reportez-vous au *Guide de personnalisation officiel Red Hat Linux*.

Si vous avez écrit votre module personnel ou emprunté celui de quelqu'un d'autre, vous devez être en mesure d'utiliser APXS pour compiler les sources de votre module en dehors de l'arbre source Apache, sans devoir utiliser d'indicateurs pour compilateur et/ou éditeur de liens. Pour plus d'informations sur APXS, reportez-vous à la documentation sur Apache à l'adresse http://httpd.apache.org/docs/dso.html.

Après avoir compilé votre module à l'aide d'APXS, placez-le dans `/usr/lib/apache`. Ensuite, votre module a besoin d'une ligne `LoadModule` et d'une ligne `AddModule` dans le fichier `httpd.conf`, comme décrit précédemment pour les modules personnels d'Apache. Après la liste `LoadModule` dans `httpd.conf`, ajoutez une ligne indiquant le fichier d'objet partagé pour votre module, comme suit :

```
LoadModule foo_module  modules/mod_foo.so
```

Vous devez modifier le nom du module et celui de votre fichier d'objet partagé de manière appropriée.

A la fin de la liste `AddModule` dans `httpd.conf`, ajoutez une ligne indiquant le fichier de code source pour votre module, comme suit :

```
AddModule mod_foo.c
```

Vous devez modifier le nom du fichier de code source de façon appropriée.

Une fois les étapes précédentes accomplies, arrêtez et démarrez votre serveur Web en procédant de la manière décrite à la Section 14.1, *Démarrage et arrêt `httpd`*. Si vous avez tout fait correctement et si votre module est codé correctement, votre serveur Web doit trouver le module et le charger au démarrage.

14.3.1 Module mod_ssl Security

Le module de sécurité mod_ssl du secure Web server est fourni comme DSO (Dynamic Shared Object, objet partagé dynamique). Ceci signifie que le serveur Web Apache peut être recompilé par des utilisateurs si la correction d'extension EAPI du module de sécurité mod_ssl doit être appliquée à Apache. Suivez les instructions relatives à la création de mod_ssl dans Apache, incluses dans la documentation mod_ssl, mais ajoutez l'indicateur suivant :

```
--with-eapi-only
```

La ligne de commande complète doit se présenter comme ceci :

```
./configure [userflags] --with-eapi-only
```

Ensuite, compilez et installez Apache.

Remarque

Red Hat ne peut pas prendre en charge des versions recompilées du serveur Web Apache. L'installation de la version livrée est prise en charge, mais si vous recompilez Apache, vous serez livré à vous-même. Ne recompilez pas Apache si vous n'êtes pas absolument certain de savoir ce que vous faites.

14.4 Utilisation d'hôtes virtuels

Si vous avez l'intention d'utiliser l'outil de configuration Apache, un utilitaire graphique fourni avec Red Hat Linux, vous ne devez ni compiler les modules de votre serveur Web Apache ni éditer le fichier de configuration `httpd.conf` de votre serveur Web. Inversement, si vous voulez ajouter des modules à Apache ou éditer manuellement `httpd.conf`, n'utilisez pas l'outil de configuration Apache.

Pour plus d'informations sur l'outil de configuration Apache, reportez-vous au *Guide de personnalisation officiel Red Hat Linux*.

Vous pouvez utiliser la fonction des hôtes virtuels d'Apache pour exécuter différents serveurs pour différentes adresses IP, différents noms d'hôtes ou différents ports sur le même ordinateur. Si l'utilisation

des hôtes virtuels vous intéresse, vous trouverez des informations exhaustives dans la documentation d'Apache installée sur votre ordinateur ou sur le Web à l'adresse http://httpd.apache.org/docs/vhosts/.

Remarque

Vous ne pouvez pas utiliser d'hôtes virtuels basés sur le nom avec secure Web server parce que l'établissement de la liaison SSL (lorsque le navigateur accepte le certificat sécurisé du serveur Web) se produit avant la demande HTTP identifiant l'hôte virtuel nommé approprié. Si vous voulez utiliser des hôtes virtuels basés sur le nom, ils ne fonctionneront qu'avec votre serveur Web non sécurisé.

Les hôtes virtuels sont configurés dans le fichier `httpd.conf`, de la manière décrite à la Section 14.2, *Directives de configuration dans `httpd.conf`*. Lisez cette section avant de commencer à changer la configuration des hôtes virtuels sur votre ordinateur.

14.4.1 Hôte virtuel du serveur Web sécurisé

La configuration par défaut de votre secure Web server utilise un serveur non sécurisé et un serveur sécurisé. Les deux serveurs utilisent la même adresse IP et le même nom d'hôte, mais contrôlent des ports différents, et le serveur sécurisé est un hôte virtuel. Cette configuration vous permet de servir des documents sécurisés et non sécurisés avec un maximum d'efficacité. Comme vous le savez, les transmissions HTTP sécurisées sont plus lentes que les non sécurisées, le nombre d'informations échangées étant beaucoup plus important dans le cas des transactions sécurisées. L'utilisation de votre serveur sécurisé pour un trafic Web non sécurisé n'est pas recommandée.

Les directives de configuration pour votre serveur sécurisé se trouvent entre des balises d'hôte virtuel dans le fichier `httpd.conf`. Si vous devez modifier la configuration de votre serveur sécurisé, il faudra modifier les directives de configuration entre les balises d'hôte virtuel dans le fichier `httpd.conf`. Si vous voulez activer certaines fonctions (par exemple, les fichiers à inclure côté serveur) pour votre serveur sécurisé, il faudra les activer entre les balises d'hôte virtuel définissant votre serveur sécurisé.

Le serveur Web non sécurisé est configuré comme hôte "non-virtuel" dans le fichier `httpd.conf`. Autrement dit, les options de configuration du serveur Web non sécurisé se trouvent en dehors des balises d'hôte virtuel dans le fichier `httpd.conf`. Si vous voulez apporter une modification à votre serveur Web non sécurisé, il faudra modifier les directives de configuration hors des balises d'hôte virtuel dans le fichier `httpd.conf`.

Par défaut, les serveurs Web sécurisé et non sécurisé partagent le même `DocumentRoot`, une directive de configuration spécifiée dans `httpd.conf`. Autrement dit, les serveurs Web sécurisé et non

sécurisé recherchent au même endroit les fichiers HTML qu'ils fournissent en réponse aux demandes. Par défaut, le `DocumentRoot` a pour valeur `/var/www/html`.

Pour modifier le `DocumentRoot` de manière à ce qu'il ne soit plus partagé par les serveurs sécurisé et non sécurisé, modifiez l'une des directives `DocumentRoot` dans `httpd.conf`. Le `DocumentRoot` situé hors des balises d'hôte virtuel définit le `DocumentRoot` pour votre serveur Web non sécurisé. Le `DocumentRoot` situé à l'intérieur des balises d'hôte virtuel qui définissent votre serveur sécurisé lui sera destiné.

Si, pour une raison quelconque, vous voulez désactiver le serveur Web non sécurisé sur votre ordinateur, vous pouvez le faire. Votre serveur sécurisé contrôle le port 443, le port par défaut pour les communications Web sécurisées, tandis que votre serveur Web non sécurisé contrôle le port 80, le port par défaut pour les communications Web non sécurisées. Pour empêcher le serveur Web non sécurisé d'accepter des connexions, recherchez, dans le fichier `httpd.conf`, la ligne suivante :

```
Port 80
```

Modifiez la ligne ci-dessus comme suit :

```
Port 443
```

Ensuite, modifiez la ligne `Listen 80`.

Une fois ces opérations accomplies, secure Web server acceptera des connexions sur le port 443, port par défaut pour des communications Web sécurisées. Toutefois, votre serveur n'acceptera plus de connexions sur le port 80, port par défaut pour les communications non sécurisées, de sorte que le serveur Web non sécurisé sera effectivement désactivé.

14.4.2 Configuration d'hôtes virtuels

La plupart des gens utiliseront probablement secure Web server sans en modifier la configuration. Pour cela, ils utiliseront la fonction d'hôtes virtuels intégrée, mais ne devront faire aucune manipulation des directives d'hôtes virtuels dans `httpd.conf`. Toutefois, si vous voulez utiliser la fonction des hôtes virtuels pour d'autres raisons, vous pouvez le faire.

Pour créer un hôte virtuel, vous devrez modifier les lignes d'hôte virtuel, fournies à titre d'exemple, dans le fichier `httpd.conf`, ou créer votre propre section d'hôte virtuel (n'oubliez pas que les hôtes virtuels nommés ne fonctionneront pas avec votre serveur sécurisé — vous devrez opter pour des hôtes virtuels basés sur l'adresse IP pour pouvoir utiliser des hôtes virtuels compatibles avec SSL ; toutefois, votre serveur non sécurisé prendra en charge tant les hôtes virtuels nommés que les hôtes virtuels basés sur l'adresse IP).

Les lignes d'exemple de l'hôte virtuel se présentent comme suit :

```
#<VirtualHost ip.address.of.host.some_domain.com>
#    ServerAdmin webmaster@host.some_domain.com
#    DocumentRoot /www/docs/host.some_domain.com
```

```
#    ServerName host.some_domain.com
#    ErrorLog logs/host.some_domain.com-error_log
#    CustomLog logs/host.some_domain.com-access_log common
#</VirtualHost>
```

Supprimez le commentaire de toutes les lignes. Ajoutez ensuite les informations correctes concernant votre ordinateur et/ou votre hôte virtuel à chaque ligne.

Dans la première ligne, remplacez `ip.address.of.host.some_domain.com` par l'adresse IP de votre serveur. Remplacez `ServerName` par un nom de DNS *valide* à utiliser pour l'hôte virtuel (autrement dit, n'inventez rien ; interrogez votre administrateur système si vous ignorez comment obtenir un nom de domaine valide).

Vous devrez aussi supprimer le commentaire de l'une des lignes `NameVirtualHost` dans le fichier `httpd.conf` :

```
#NameVirtualHost 12.34.56.78:80
#NameVirtualHost 12.34.56.78
```

Supprimez les commentaires de l'une des lignes et remplacez l'adresse IP par celle (ainsi que le port, si nécessaire) de cet hôte virtuel.

Il est possible de placer de nombreuses autres directives de configuration entre les balises de l'hôte virtuel, selon la raison pour laquelle vous configurez un hôte virtuel.

Si vous configurez un hôte virtuel et souhaitez qu'il contrôle un port non défini par défaut (80 est le port par défaut pour les communications Web non sécurisées ; 443 est le port par défaut pour les communications Web sécurisées), il faudra configurer un hôte virtuel pour ce port, puis ajouter, dans le fichier `httpd.conf`, une directive `Listen` correspondant à ce port.

Pour faire en sorte qu'un hôte virtuel travaille spécifiquement pour ce port, ajoutez le numéro de port à la première ligne de la configuration de l'hôte virtuel. La première ligne doit ressembler à ceci :

```
<VirtualHost adresse_ip_du_serveur:12331>
```

Cette ligne crée un hôte virtuel contrôlant le port 12331. Dans l'exemple précédent, remplacez `12331` par le numéro de port que vous voulez utiliser.

Sous les lignes `Listen` du fichier `httpd.conf`, ajoutez une ligne telle la suivante, qui donnera pour instruction au serveur Web de contrôler le port 12331 :

```
Listen 12331
```

Vous devez redémarrer `httpd` pour lancer ce nouvel hôte virtuel. Pour obtenir des instructions sur le démarrage et l'arrêt de `httpd`, reportez-vous à la Section 14.1, *Démarrage et arrêt `httpd`*.

Pour plus d'informations sur la création et la configuration d'hôtes virtuels nommés et d'hôtes virtuels basés sur l'adresse IP, consultez la page Web http://httpd.apache.org/docs/vhosts/. Reportez-vous à

la documentation relative à l'hôte virtuel du groupe Apache pour plus de détails sur l'utilisation des hôtes virtuels.

Partie IV Annexes

A Paramètres généraux et modules

Cette annexe est fournie pour illustrer *quelques-uns* des paramètres dont peuvent avoir besoin certains pilotes[1]pour des périphériques. Dans la plupart des cas, ces paramètres supplémentaires sont inutiles car le noyau est déjà en mesure d'utiliser les périphériques sans eux. Vous ne devriez utiliser les paramètres fournis dans cette annexe que lorsque vous avez de la difficulté à faire fonctionner un périphérique donné sous Red Hat Linux ou devez modifier les paramètres par défaut du système pour le périphérique.

Durant l'installation de Red Hat Linux, certaines limites sont appliquées aux systèmes de fichiers et d'autres pilotes pris en charge par le noyau. Toutefois, après l'installation, il y a une prise en charge pour tous les systèmes de fichiers disponibles sous Linux. Lors de l'installation, le noyau modularisé prend en charge des périphériques (E)IDE (notamment les lecteurs de CD-ROM ATAPI), des cartes SCSI et des cartes réseau.

Remarque

Du fait que Red Hat Linux prend en charge l'installation sur de nombreux types de matériel différents, certains pilotes (dont ceux pour les cartes SCSI, les cartes réseau et nombre de lecteurs de CD-ROM) ne sont pas intégrés dans le noyau Linux utilisé par le programme d'installation. Ils sont plutôt disponibles comme modules et chargés en fonction de vos besoins durant le processus d'installation. Le cas échéant, vous avez la possibilité de spécifier des options pour ces modules au moment de leur chargement à partir du disque du pilote.

Pour spécifier les paramètres du module lorsqu'un pilote est chargé, tapez **`linux expert`** à l'invite `boot:` et insérez le disque du pilote lorsque le programme d'installation vous le demande. Après avoir lu le disque, le programme d'installation vous demande de sélectionner le type de périphérique que vous configurez. Vous pouvez alors faire votre sélection dans cet écran pour spécifier le paramètre du module. Ensuite, le programme d'installation affiche un écran où il vous est possible d'entrer les paramètres en fonction du type spécifique de périphérique que vous êtes en train de configurer.

Une fois l'installation terminée, vous pouvez recréer un noyau incluant la prise en charge de votre configuration matérielle spécifique. Prenez note que dans la plupart des cas, un noyau personnalisé n'est pas nécessaire. Reportez-vous au *Guide de personnalisation officiel Red Hat Linux* pour avoir plus de renseignements au sujet de la recompilation de votre noyau.

1 Un **pilote** est un type de logiciel qui aide le système à utiliser un périphérique donné. Sans ce pilote, le noyau pourrait ne pas savoir comment utiliser correctement le périphérique.

A.1 Spécification des paramètres d'un module

Si vous fournissez les paramètres au moment du chargement d'un module, vous pouvez habituellement les spécifier de deux façons différentes :

- Spécifier un ensemble complet de paramètres au moyen d'une seule instruction. Par exemple, le paramètre `cdu31=0x340,0` pourrait être utilisé avec un CDU Sony 31 ou 33 sur le port 340 sans IRQ.
- Spécifier les paramètres un par un. Cette méthode est utilisée lorsqu'un ou plusieurs paramètres du premier ensemble ne sont pas nécessaires. Par exemple, `cdu31_port=0x340 cdu31a_irq=0` peut être utilisé comme paramètre pour le même lecteur de CD-ROM donné dans l'exemple précédent. On utilise un *OK* dans les tableaux CD-ROM, SCSI et Ethernet de cette annexe pour montrer où la première méthode de paramétrage s'arrête et où la seconde commence.

Remarque

N'utilisez qu'une seule méthode, et non les deux, lorsque vous chargez un module avec des paramètres particuliers.

Lorsqu'un paramètre contient une virgule, assurez-vous de *ne pas* mettre d'espace après la virgule.

A.2 Paramètres des modules pour CD-ROM

Remarque

Les lecteurs de CD-ROM répertoriés ne sont pas tous pris en charge. Veuillez consulter la liste de compatibilité des composants matériels sur le site Web de Red Hat à l'adresse http://hardware.redhat.com pour vous assurer que votre lecteur de CD-ROM est pris en charge.

Bien que les paramètres soient spécifiés une fois le disque du pilote a été chargé et le périphérique défini, l'un des paramètres les plus couramment utilisés (`hd`*`X`*`=cdrom`) *peut* être entré à l'invite de démarrage (`boot:`) lors de l'installation. Cette exception à la règle est due au fait que ce paramètre a trait à la prise en charge de CD-ROM IDE/ATAPI, faisant déjà partie du noyau.

Dans les tableaux suivants, la plupart des modules dépourvus de paramètres sont capables d'une détection automatique du matériel, ou requièrent un changement manuel de paramètres dans le code source du module et une recompilation.

Table A–1 Paramètres du matériel

Matériel	Module	Paramètres
Lecteurs de CD-ROM ATAPI/IDE		hd*X*=cdrom
Aztech CD268-01A, Orchid CD-3110, Okano/Wearnes CDD110, Conrad TXC, CyCDROM CR520, CyCDROM CR540 (non IDE)	`aztcd.o`	aztcd=*port_es*
CD-ROM Sony CDU-31A	`cdu31a.o`	cdu31a=*port_es,IRQ OU* cdu31a_port=*adr_base* cdu31a_irq=*irq*
Lecteur de CD-ROM Philips/LMS 206 avec carte adaptateur hôte cm260	`cm206.o`	cm206=*port_es,IRQ*
CD-ROM Goldstar R420	`gscd.o`	gscd=*port_es*
Interface CD-ROM de carte son ISP16, MAD16 ou Mozart (OPTi 82C928 et OPTi 82C929) avec lecteurs Sanyo/Panasonic, Sony ou Mitsumi	`isp16.o`	isp16=*port_es,IRQ,dma, lecteur_type OU* isp16_cdrom_base=*port_es* isp16_cdrom_irq=*IRQ* isp16_cdrom_dma=*dma* isp16_cdrom_type=*lecteur_type*
CD-ROM Mitsumi standard	`mcd.o`	mcd=*port_es,IRQ*
CD-ROM Mitsumi expérimental	`mcdx.o`	mcdx=*port_es_1,IRQ_1, port_es_n,IRQ_n*
Lecteur de CD-ROM de stockage optique "Dolphin" 8000 AT, Lasermate CR328A	`optcd.o`	
CD-ROM IDE port parallèle	`pcd.o`	

Matériel	Module	Paramètres
SB Pro 16 compatible	`sbpcd.o`	sbpcd=*port_es*
CDR-H94A Sanyo	`sjcd.o`	sjcd=*port_es OU* sjcd_base=*port_es*
CDU-535 et 531 de Sony (certains lecteurs Procomm)	`sonycd535.o`	sonycd535=*port_es*

Voici quelques exemples des modules utilisés :

Table A–2 Exemples de configuration de paramètres matériels

Configuration	Exemple
CD-ROM ATAPI, branché comme maître sur le deuxième canal IDE	hdc=cdrom
CD-ROM Mitsumi non IDE sur port 340, IRQ 11	mcd=0x340,11
Trois lecteurs de CD-ROM Mitsumi non IDE utilisant le pilote expérimental, les ports E/S 300, 304 et 320 avec IRQ 5, 10 et 11	mcdx=0x300,5,0x304,10,0x320,11
Sony CDU 31 ou 33 au port 340, sans IRQ	cdu31=0x340,0 *OU* cdu31_port=0x340 cdu31a_irq=0
CD-ROM Aztech sur port 220	aztcd=0x220
CD-ROM de type Panasonic sur interface SoundBlaster connecté au port 230	sbpcd=0x230,1
Phillips/LMS cm206 et cm260 à E/S 340 et IRQ 11	cm206=0x340,11
Goldstar R420 à E/S 300	gscd=0x300
Lecteur Mitsumi sur carte son MAD16 à adresse ES 330 et IRQ 1, test DMA	isp16=0x330,11,0,Mitsumi
Sony CDU 531 à adresse E/S 320	sonycd535=0x320

Remarque

La plupart des cartes Sound Blaster récentes sont livrées avec des interfaces IDE. Pour ces cartes, vous ne devez pas utiliser de paramètres `sbpcd`, mais uniquement des paramètres `hd`*X*.

A.3 Paramètres SCSI

Table A–3 Paramètres SCSI

Matériel	Module	Paramètres
Contrôleur de mémoire 3ware	`3w-xxxx.o`	
NCR53c810/820/720, NCR53c700/710/700-66	`53c7,8xx.o`	
Pilote AM53/79C974 (PC-SCSI)	`AM53C974.o`	
La plupart des cartes Buslogic (maintenant Mylex) avec numéro de référence "BT"	`BusLogic.o`	BusLogic_Options=*option,option,…*
DAC960 RAID Controller Mylex	`DAC960.o`	
SCSI fondée sur NCR53c406a	`NCR53c406a.o`	
Initio INI-9100UW	`a100u2w.o`	a100u2w=*es,IRQ,scsi_id*
AACRAID Adaptec	`aacraid.o`	
Cartes SCSI Advansys	`advansys.o`	
Adaptec AHA-152x	`aha152x.o`	aha152x=*es,IRQ,scsi_id*
AHA 154x et 631x de type Adaptec	`aha1542.o`	
Adaptec AHA 1740	`aha1740.o`	

Matériel	Module	Paramètres
Adaptec AHA-274x, AHA-284x, AHA-29xx, AHA-394x, AHA-398x, AHA-274x, AHA-274xT, AHA-2842, AHA-2910B, AHA-2920C, AHA-2930/U/U2, AHA-2940/W/U/UW/AU/, U2W/U2/U2B/, U2BOEM, AHA-2944D/WD/UD/UWD, AHA-2950U2/W/B, AHA-3940/U/W/UW/, AUW/U2W/U2B, AHA-3950U2D, AHA-3985/U/W/UW, AIC-777x, AIC-785x, AIC-786x, AIC-787x, AIC-788x, AIC-789x et AIC-3860	`aic7xxx.o`	aic7xxx=*chaîne*
Contrôleur SCSI PCI ACARD ATP870U	`atp870u.o`	
Contrôleur Compaq Smart Array 5300	`cciss.o`	
Contrôleur Compaq Smart/2 RAID	`cpqarray.o`	
Contrôleur Compaq FibreChannel	`cpqfc.o`	
Domex DMX3191D	`dmx3191d.o`	
Data Technology Corp DTC3180/3280	`dtc.o`	

Matériel	Module	Paramètres
Cartes hôtes SCSI DTP (EATA/DMA) PM2011B/9X ISA, PM2021A/9X ISA, PM2012A, PM2012B, PM2022A/9X EISA, PM2122A/9X, PM2322A/9X, SmartRAID PM3021, PM3222, PM3224	`eata.o`	eata=*port0*,*port1*,*port2*,… *options OU* eata io_port=*port0*,*port1*,*port2*,… option=*valeur*
Cartes SCSI DTP PM2011, PM2021, PM2041, PM3021, PM2012B, PM2022, PM2122, PM2322, PM2042, PM3122, PM3222, PM3332, PM2024, PM2124, PM2044, PM2144, PM3224, PM3334	`eata_dma.o`	
Cartes DTP EATA-PIO	`eata_pio.o`	
Sun Enterprise Network Array (FC-AL)	`fcal.o`	
SCSI Future Domain TMC-16*xx*	`fdomain.o`	
NCR5380 (pilote générique)	`g_NCR5380.o`	
Contrôleur ICP RAID	`gdth.o`	
I2O Block Driver	`i2o_block.o`	
Carte SCSI pour port parallèle IOMEGA MatchMaker	`imm.o`	
Carte SCSI ISA Always IN2000	`in2000.o`	in2000=*setup_chaîne*:*valeur OU* in2000 *setup_chaîne*=*valeur*
Cartes hôtes SCSI Initio INI-9X00U/UW	`initio.o`	
IBM ServeRAID	`ips.o`	
AMI MegaRAID 418, 428, 438, 466 et 762	`megaraid.o`	

Matériel	Module	Paramètres
Cartes SCSI NCR avec circuits 810/810A/815/ 825/825A/860/875/876/895	`ncr53c8xx.o`	ncr53c8xx=*option1*:*valeur1*,*option2*:*valeur2*,… *OU* ncr53c8xx="*option1*:*valeur1 option2*:*valeur2*…"
Pro Audio Spectrum/Studio 16	`pas16.o`	
PCI-2000 IntelliCache	`pci2000.o`	
PCI-2220I EIDE RAID	`pci2220i.o`	
SparcSTORAGE Array	`pluto.o`	
Carte hôte SCSI pour port parallèle IOMEGA PPA3	`ppa.o`	
Perceptive Solutions PSI-240I EIDE	`psi240i.o`	
Qlogic 1280	`qla1280.o`	
Qlogic 2*x*00	`qla2x00.o`	
QLogic Fast SCSI FASXXX ISA/VLB/PCMCIA	`qlogicfas.o`	
QLogic ISP2100 SCSI-FCP	`qlogicfc.o`	
Cartes SCSI QLogic ISP1020 Intelligent IQ-PCI, IQ-PCI-10, IQ-PCI-D	`qlogicisp.o`	
SBUS SCSI Qlogic ISP1020	`qlogicpti.o`	
Seagate ST-01/02, Future Domain TMC-8*xx*	`seagate.o`	
Future Domain TMC-885, TMC-950	`seagate.o`	controller_type=2 adresse_base=*adr_base* irq=*IRQ*
Cartes avec circuit sym53c416	`sym53c416.o`	sym53c416=*PORTBASE,[IRQ] OU* sym53c416 io=*PORTBASE* irq=*IRQ*

Matériel	Module	Paramètres
Carte hôte SCSI Trantor T128/T128F/T228	`t128.o`	
Tekram DC-390(T) PCI	`tmscsim.o`	
UltraStor 14F/34F (pas 24F)	`u14-34f.o`	
UltraStor 14F, 24F, et 34F	`ultrastor.o`	
Série WD7000	`wd7000.o`	

Voici quelques exemples des modules utilisés :

Table A–4 Exemples de configuration des paramètres SCSI

Configuration	Exemple
Adaptec AHA1522 sur port 330, IRQ 11, SCSI ID 7	aha152x=0x330,11,7
Adaptec AHA1542 sur port 330	bases=0x330
Future Domain TMC-800 à CA000, IRQ 10	type_controller=2 adresse_base=0xca000 irq=10

A.4 Paramètres Ethernet

Table A–5 Paramètres de modules Ethernet

Matériel	Module	Paramètres
3Com 3c501	`3c501.o`	3c501=*port_es,IRQ*
3Com 3c503 et 3c503/16	`3c503.o`	3c503=*port_es,IRQ OU* 3c503 io=*port_es_1,port_es_n* irq=*IRQ_1,IRQ_n*
3Com EtherLink Plus (3c505)	`3c505.o`	3c505=*port_es,IRQ OU* 3c505 io=*port_es_1,port_es_n* irq=*IRQ_1,IRQ_2*
3Com EtherLink 16	`3c507.o`	3c507=*port_es,IRQ OU* 3c507 io=*port_es* irq=*IRQ*
3Com EtherLink III	`3c509.o`	3c509=*IRQ*

Matériel	Module	Paramètres
3Com ISA EtherLink XL "Corkscrew"	`3c515.o`	
3Com EtherLink PCI III/XL Vortex (3c590, 3c592, 3c595, 3c597) Boomerang (3c900, 3c905, 3c595)	`3c59x.o`	
RTL8139, SMC EZ Card Fast Ethernet	`8139too.o`	
Apricot 82596	`82596.o`	
Ansel Communications Modèle 3200	`ac3200.o`	ac3200=*port_es*,*IRQ OU* ac3200 io=*port_es_1*,*port_es_n* irq=*IRQ_1*,*IRQ_n*
Alteon AceNIC Gigabit	`acenic.o`	
Aironet Arlan 655	`arlan.o`	
Aironet 4500 PCI-ASI-i365 sans fil	`aironet4500_card.o`	
Allied Telesis AT1700	`at1700.o`	at1700=*port_es*,*IRQ OU* at1700 io=*port_es* irq=*IRQ*
Tangent ATB-II, Novel NL-10000, Daystar Digital LT-200, Dayna DL2000, DaynaTalk PC (HL), COPS LT-95, Farallon PhoneNET PC II, III	`cops.o`	cops=*port_es*,*IRQ OU* cops io=*port_es* irq=*IRQ*
Pilote modulaire pour carte série synchrone COSA ou SRP	`cosa.o`	cosa=*port_es*,*IRQ*,*dma*
Crystal Semiconduc-torCS89[02]0	`cs89x0.o`	

Matériel	Module	Paramètres
Cartes EtherWORKS DE425 TP/COAX EISA, DE434 TP PCI, DE435/450 TP/COAX/AUI PCI DE500 10/100 PCI Kingston, LinkSys, SMC8432, SMC9332, Znyx31[45], et Znyx346 10/100 avec circuits DC21040 (pas de SROM), DC21041[A], DC21140[A], DC21142 et DC21143	`de4x5.o`	de4x5=*port_es OU* de4x5 io=*port_es* de4x5 args='eth*X[fdx]* autosense=*MEDIA_STRING*'
Ethernet Pocket Adapter D-Link DE-600	`de600.o`	
Ethernet Pocket Adapter D-Link DE-620	`de620.o`	
DIGITAL DEPCA & EtherWORKS DEPCA, DE100, DE101, DE200 Turbo, DE201Turbo DE202 Turbo TP/BNC, DE210, DE422 EISA	`depca.o`	depca=*port_es,IRQ OU* depca io=*port_es* irq=*IRQ*
Digi Intl. RightSwitch SE-X EISA et PCI	`dgrs.o`	
Davicom DM9102(A)/DM9132/ DM9801 Fast Ethernet	`dmfe.o`	
Intel EtherExpress/1000 Gigabit	`e1000.o`	
Cabletron E2100	`e2100.o`	e2100=*io_port,IRQ,mem OU* e2100 io=*port_es* irq=*IRQ* mem=*mem*

Matériel	Module	Paramètres
Intel EtherExpress Pro10	`eepro.o`	eepro=*port_es*,*IRQ OU* eepro io=*port_es* irq=*IRQ*
Pilote Intel i82557/i82558 PCI EtherExpressPro	`eepro100.o`	
Intel EtherExpress 16 (i82586)	`eexpress.o`	eexpress=*port_es*,*IRQ OU* eexpress io=*port_es* irq=*IRQ*
SMC EtherPower II 9432 PCI (série 83c170/175 EPIC)	`epic100.o`	
Racal-Interlan ES3210 EISA	`es3210.o`	
ICL EtherTeam 16i/32 EISA	`eth16i.o`	eth16i=*port_es*,*IRQ OU* eth16i ioaddr=*port_es* IRQ=*IRQ*
EtherWORKS 3 (DE203, DE204 et DE205)	`ewrk3.o`	ewrk=*port_es*,*IRQ OU* ewrk io=*port_es* irq=*IRQ*
Fujitsu FMV-181/182/183/184	`fmv18x.o`	fmv18x=*port_es*,*IRQ OU* fmv18x io=*port_es* irq=*IRQ*
Packet Engines GNIC-II Gigabit	`hamachi.o`	
Pilote modulaire pour Comtrol Hostess SV11	`hostess_sv11.o`	hostess_sv11=*port_es*,*IRQ*, *DMABIT OU* hostess_sv11 io=*port_es* irq=*IRQ* dma=*DMABIT*
HP PCLAN/plus	`hp-plus.o`	hp-plus=*port_es*,*IRQ OU* hp-plus io=*port_es* irq=*IRQ*
HP LAN Ethernet	`hp.o`	hp=*port_es*,*IRQ OU* hp io=*port_es* irq=*IRQ*

Matériel	Module	Paramètres
Cartes réseau 100VG-AnyLan HP J2585B, J2585A, J2970, J2973, J2573 Compex ReadyLink ENET100-VG4, FreedomLine 100/VG	`hp100.o`	hp100=*port_es*,*nom OU* hp100 hp100_port=*port_es* hp100_nom=*nom*
Bus annulaire à jeton (Token Ring) IBM 16/4	`ibmtr.o`	ibmtr=*port_es*,*IRQ*,*mem OU* ibmtr io=*port_es* irq=*IRQ* mem=*mem*
AT1500, HP J2405A et la plupart des clones NE2100	`lance.o`	
Mylex LNE390 EISA	`lne390.o`	
	`ltpc.o`	ltpc=*port_es*,*IRQ OU* ltpc io=*port_es* irq=*IRQ*
SBUS MyriCOM MyriNET	`myri_sbus.o`	
NatSemi DP83815 Fast Ethernet	`natsemi.o`	
NE1000 / NE2000 (non pci)	`ne.o`	ne=*port_es*,*IRQ OU* ne io=*port_es* irq=*IRQ*
Cartes PCI NE2000 RealTEk RTL-8029, Winbond 89C940, Compex RL2000, KTI ET32P2, NetVin, NV5000SC, Via 82C926 et SureCom NE34	`ne2k-pci.o`	
Novell NE3210 EISA	`ne3210.o`	
MiCom-Interlan NI5010	`ni5010.o`	
Carte NI5210 (puce Ethernet i82586)	`ni52.o`	ni52=*port_es*,*IRQ OU* ni52 io=*port_es* irq=*IRQ*
NI6510 Ethernet	`ni65.o`	

Matériel	Module	Paramètres
Ancien DEC 21040 et la plupart des Ethernet 21*40	`old_tulip.o`	old_tulip=*port_es OU* old_tulip io=*port_es*
AMD PCnet32 et AMD PCnetPCI	`pcnet32.o`	
PCI RedCreek Communications	`rcpci.o`	
Cartes RealTek utilisant les circuits Fast Ethernet RTL8129 ou RTL8139	`rtl8139.o`	
FR multi-protocoles Sangoma S502/S508	`sdla.o`	
Sangoma S502A, ES502A, S502E, S503, S507, S508 et S509	`sdladrv.o`	
SysKonnect SK-98*XX* Gigabit	`sk98lin.o`	
Carte ISA/PCI Token Ring SysKonnect, TR4/16(+) ISA ou PCI, TR4/16 PCI et cartes ISA SK NET TR4/16 plus anciennes	`sktr.o`	sktr=*port_es,IRQ,mem OU* sktr io=*port_es* irq=*IRQ* mem=*mem*
Ethercard ISA SMS Ultra et SMC EtherEZ(8K, 83c790)	`smc-ultra.o`	smc-ultra=*port_es,IRQ OU* smc-ultra io=*port_es* irq=*IRQ*
Carte Ethernet EISA SMC Ultra32 (32K)	`smc-ultra32.o`	
Cartes Ethernet série SMC 9000	`smc9194.o`	smc9194=*port_es,IRQ OU* smc9194 io=*port_es* irq=*IRQ* ifport=*[0,1,2]*
Sun BigMac Ethernet	`sunbmac.o`	
Sundance ST201 Alta	`sundance.o`	

Matériel	Module	Paramètres
Sun Happy Meal Ethernet	`sunhme.o`	
Sun Quad Ethernet	`sunqe.o`	
ThunderLAN	`tlan.o`	
Cartes Ethernet PCI Digital 21x4x Tulip PCI SMC EtherPower 10 (8432T/8432BT) PCI SMC EtherPower 10/100 (9332DST) PCI DEC EtherWorks 100/10 (DE500-XA) PCI DEC EtherWorks 10 (DE450) DEC QSILVER's, Znyx 312 etherarray Allied Telesis LA100PCI-T Danpex EN-9400, Cogent EM110	`tulip.o`	
Cartes PCI Fast Ethernet VIA Rhine avec VIA VT86c100A Rhine-II PCI ou 3043 Rhine-I D-Link DFE-930-TX PCI 10/100	`via-rhine.o`	
Carte ISA AT&T GIS (nee NCR) WaveLan	`wavelan.o`	wavelan=*[IRQ,0],io_port,NWID*
Cartes Ethernet compatibles WD8003 et WD8013	`wd.o`	wd=*port_es,IRQ,mem, mem_end OU* wd io=*port_es* irq=*IRQ* mem=*mem* mem_end=*fin*
PCI Compex RL100ATX	`winbond.o`	
Packet Engines Yellowfin	`yellowfin.o`	
Cartes de type Z8530 pour AX.25	`z85230.o`	

Voici quelques exemples des modules utilisés :

Table A–6 Exemples de configuration des paramètres Ethernet

Configuration	Exemple
Carte ISA NE2000 à l'adresse E/S 300 et IRQ 11	ne=0x300,11 ether=0x300,11,eth0
Carte Wavelan à l'E/S 390, détection automatique d'IRQ et utilisation de NWID pour 0x4321	wavelan=0,0x390,0x4321 ether=0,0x390,0x4321,eth0

A.4.1 Utilisation de plusieurs cartes Ethernet

Vous pouvez utiliser plusieurs cartes Ethernet dans un ordinateur. Si chaque carte utilise un pilote différent (par exemple, 3c509 et DE425), vous devez simplement ajouter des lignes `alias` (et éventuellement `options`) pour chaque carte dans le fichier `/etc/modules.conf`. Veuillez vous reporter au *Guide de personnalisation officiel Red Hat Linux* pour avoir plus de détails à ce sujet.

Si deux cartes Ethernet utilisent le même pilote (par exemple, deux cartes 3c509 ou une 3c595 et une 3c905), vous devez soit indiquer les adresses des deux cartes dans la ligne d'options du pilote (pour les cartes ISA), soit simplement ajouter une ligne `alias` pour chaque carte (pour les cartes PCI).

Pour plus d'informations sur l'utilisation de plusieurs cartes Ethernet, consultez la section *Linux Ethernet-HOWTO* à l'adresse http://www.redhat.com/mirrors/LDP/HOWTO/Ethernet-HOWTO.html.

B Présentation des partitions de disque

Les partitions de disque constituent un aspect courant dans le domaine de l'informatique personnelle, et ce depuis assez longtemps. Toutefois, étant donné le nombre de gens achetant des ordinateurs munis de systèmes d'exploitation préinstallés, relativement peu de personnes comprennent la manière dont les partitions fonctionnent. Ce chapitre tente d'expliquer comment fonctionnent les partitions de disque de manière à ce que l'installation de Red Hat Linux vous semble simple.

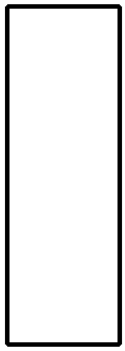
Si vous êtes relativement familiarisé avec les partitions de disque, vous pouvez passer à la Section B.1.4, *Préparation de l'espace nécessaire à Red Hat Linux* pour plus d'informations sur le processus de libération d'espace disque préalable à l'installation de Red Hat Linux. Cette section présente également le système de dénomination de partition utilisé par Linux, le partage d'espace disque avec d'autres systèmes d'exploitation et autres aspects connexes.

B.1 Concepts de base concernant le disque dur

Les disques durs ont une fonction très simple ; ils permettent de conserver des données et de les récupérer de façon fiable à la demande.

Concernant les questions telles que le partitionnement de disque, il est important de connaître un peu le matériel utilisé ; malheureusement, on a vite fait de s'enliser dans les détails. C'est pourquoi nous avons opté pour un schéma simplifié de disque dur, qui devrait vous aider à comprendre comment cela fonctionne. La Figure B–1, *Disque dur non utilisé* illustre un disque dur non encore utilisé.

Figure B–1 Disque dur non utilisé

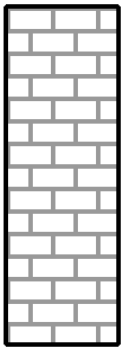


Il n’y a pas grand-chose à voir, n’est-ce pas ? Mais si nous parlons de disques durs à un niveau de base, c’est différent. Imaginons que nous voulions stocker des données sur ce disque. Dans l’état actuel des choses, cela ne fonctionnera pas. Il faut commencer par faire quelque chose …

B.1.1 Ce qui compte n’est pas tant ce que vous écrivez que la manière dont vous l’écrivez

Les vétérans de l’informatique auront probablement vite compris. Il faut **formater** le disque. Le formatage (habituellement appelé "création d’un **système de fichiers**" dans le jargon Linux) écrit des informations sur le disque, mettant de l’ordre dans l’espace vide d’un disque non formaté.

Figure B–2 Disque dur avec système de fichiers



Comme la Figure B–2, *Disque dur avec système de fichiers* l'indique, l'ordre imposé par un système de fichiers entraîne un certain nombre de compromis :

- Un petit pourcentage de l'espace disponible sur le disque est utilisé pour stocker des données en rapport avec le système de fichiers et peut être considéré comme perdu.
- Le système de fichiers fractionne l'espace restant en petits segments de taille constante. Dans l'univers Linux, ces segments sont appelés **blocs**. [1]

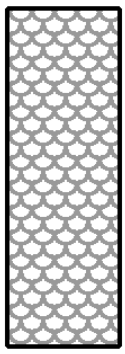
Etant donné que les systèmes de fichiers rendent possibles des choses telles que les répertoires et les fichiers, ce type de compromis est généralement considéré comme un prix modique à payer.

Il faut également noter qu'il n'y a pas de système de fichiers unique, universel ; comme l'illustre la Figure B–3, *Disque dur avec un système de fichiers différent*, un disque dur peut contenir un système de fichiers parmi de nombreux autres. Comme vous pouvez l'imaginer, les différents systèmes de fichiers ont tendance à être incompatibles ; cela signifie qu'un système d'exploitation prenant en charge un système de fichiers (ou une poignée de types de systèmes de fichiers apparentés) ne pourra

[1] Les blocs *sont* dimensionnés de façon uniforme, contrairement à ce que semblent indiquer nos illustrations. Songez également qu'une unité de disque moyenne contient des milliers de blocs. Toutefois, dans le cadre de cette présentation, il est préférable de ne pas prêter attention à ces détails.

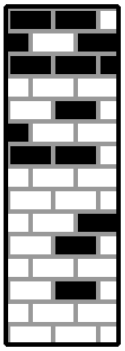
peut-être pas en prendre en charge un autre. Cette affirmation n'est cependant pas une règle absolue. Par exemple, Red Hat Linux prend en charge un vaste éventail de systèmes de fichiers (dont beaucoup sont couramment utilisés par d'autres systèmes d'exploitation), ce qui facilite l'échange de données.

Figure B–3 Disque dur avec un système de fichiers différent



Naturellement, l'écriture d'un système de fichiers sur le disque n'est qu'un début. Le but de la manoeuvre est de *stocker* et *récupérer* réellement des données. Voyons le disque après écriture de certains fichiers.

Figure B–4 Disque dur sur lequel figurent des données



Comme l'illustre la Figure B–4, *Disque dur sur lequel figurent des données*, 14 des blocs précédemment vides contiennent à présent des données. Il est impossible de déterminer le nombre de fichiers se trouvant sur cette unité ; il peut n'y en avoir qu'un seul ou jusqu'à 14, étant donné que tous les fichiers utilisent au moins un bloc. Un autre point important est que les blocs utilisés n'ont pas la forme d'une zone continue ; les blocs utilisés et inutilisés peuvent être intercalés. C'est ce qu'on appelle la **fragmentation**. Celle-ci peut jouer un rôle en cas de tentative de redimensionner une partition existante.

Comme toutes les technologies en rapport avec l'informatique, les disques durs n'ont jamais cessé d'évoluer. Ils ont en particulier évolué dans le sens d'une augmentation constante de leur taille. Il ne s'agit pas, en l'occurrence, de leur taille physique, mais de leur capacité. Et c'est précisément ce gain de capacité qui a induit une évolution dans la façon d'utiliser les disques durs.

B.1.2 Création de plusieurs partitions sur un disque

Face à l'augmentation des capacités des unités de disque, certains ont commencé à se demander si le fait de disposer de tout cet espace d'un seul tenant était une bonne idée. Ce point de vue était le fruit de plusieurs considérations tant philosophiques que techniques. Du point de vue philosophique, il apparaissait qu'au-delà d'une certaine taille, l'espace supplémentaire offert par un disque de plus

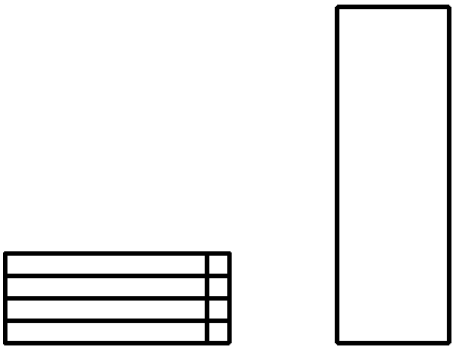
grande capacité était également source de confusion. Sur le plan technique, certains systèmes de fichiers n'étaient pas conçus pour prendre en charge des disques d'une telle capacité ; ou alors, s'ils *pouvaient* prendre en charge des unités de grande taille, la perte d'espace résultant de la place occupée par le système de fichiers devenait excessive.

La solution à ce problème consistait à diviser les disques en **partitions**. Chaque partition est accessible comme s'il s'agissait d'un disque distinct. Ceci est possible grâce à l'ajout d'une **table des partitions**.

Remarque

Si les schémas de ce chapitre montrent la table des partitions comme étant distincte du disque dur réel, ce n'est pas rigoureusement exact. En réalité, la table des partitions est stockée au tout début du disque, avant le système de fichiers et les données de l'utilisateur. C'est par souci de clarté que nous l'avons séparée du reste de l'unité sur les schémas.

Figure B–5 Disque dur avec table des partitions



Comme l'indique la Figure B–5, *Disque dur avec table des partitions*, la table des partitions est divisée en quatre sections. Chacune peut accueillir les informations nécessaires pour la définition d'une simple partition, ce qui signifie que la table des partitions ne peut pas définir plus de quatre partitions.

Chaque table des partitions contient une série d'informations sur les caractéristiques importantes de la partition telles que :

- Les points du disque où la partition commence et finit ;
- Le caractère "actif" ou non de la partition
- Le type de partition

Examinons de plus près chacune de ces caractéristiques. Les points de début et de fin de la partition définissent en réalité sa taille et son emplacement physique sur le disque. La balise "active" est utilisée par les chargeurs de démarrage de certains systèmes d'exploitation. Autrement dit, c'est le système d'exploitation se trouvant dans la partition balisée comme "active" qui sera démarré.

La notion de type de partition peut sembler un peu confuse. Le type est un nombre qui identifie l'utilisation prévue de la partition. Si cette définition semble un peu vague, c'est parce que la signification du concept de type de partition l'est également. Certains systèmes d'exploitation utilisent le type de partition pour indiquer un type de système de fichiers spécifique, marquer la partition comme étant associée à un système d'exploitation particulier, indiquer que la partition contient un système d'exploitation amorçable, voire une combinaison des trois.

La Table B–1, *Types de partition* contient la liste de quelques types de partitions communs (et obscurs), avec les valeurs numériques qui y sont associées.

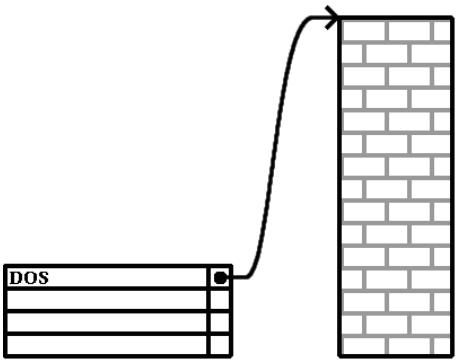
Table B–1 Types de partition

Type de partition	Valeur	Type de partition	Valeur
Vide	00	Novell Netware 386	65
DOS 12-bit FAT	01	PIC/IX	75
XENIX root	02	Old MINIX	80
XENIX usr	03	Linux/MINUX	81
DOS 16-bit <=32M	04	Linux swap	82
Etendue	05	Linux native	83
DOS 16-bit >=32	06	Linux étendue	85
OS/2 HPFS	07	Amoeba	93
AIX	08	Amoeba BBT	94
AIX amorçable	09	BSD/386	a5
OS/2 Boot Manager	0a	OpenBSD	a6

Type de partition	Valeur	Type de partition	Valeur
Win95 FAT32	0b	NEXTSTEP	a7
Win95 FAT32 (LBA)	0c	BSDI fs	b7
Win95 FAT16 (LBA)	0e	BSDI swap	b8
Win95 étendue (LBA)	0f	Syrinx	c7
Venix 80286	40	CP/M	db
Novell	51	DOS access	e1
Microport	52	DOS R/O	e3
GNU HURD	63	DOS secondary	f2
Novell Netware 286	64	BBT	ff

Maintenant, vous vous demandez peut-être comment toute cette complexité supplémentaire est normalement utilisée. Voir la Figure B–6, *Disque dur avec partition unique* pour un exemple.

Figure B–6 Disque dur avec partition unique



Très souvent, il n'y a qu'une seule partition occupant tout le disque, qui rappelle les disques pré-partitionnés d'autrefois. La table des partitions n'utilise qu'une seule entrée pointant sur le début de la partition.

Nous avons classé cette partition parmi celles de type "DOS". Comme le montre la Table B–1, *Types de partition*, bien qu'un peu simpliste, cette qualification est adéquate dans le cadre de cette présentation. Il s'agit d'un système de partition typique de la plupart des ordinateurs commercialisés avec une version de Windows préinstallée.

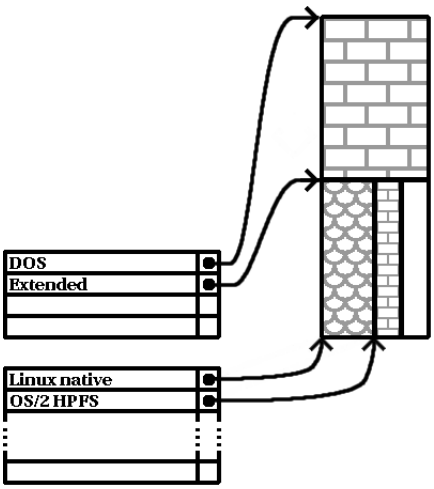
B.1.3 Partitions à l'intérieur de partitions – Aperçu des partitions étendues

Naturellement, avec le temps, il est devenu évident que quatre partitions ne suffiraient pas. Etant donné l'augmentation de la capacité des unités de disque, il devenait possible de configurer quatre partitions de taille raisonnable tout en conservant de l'espace disque. Il fallait trouver un moyen de créer plus de partitions.

Entrer dans la partition étendue. Comme indiqué dans la Table B–1, *Types de partition*, il existe un type de partition "Etendue" ; ce type de partition est au coeur des partitions étendues.

Lorsqu'une partition est créée et que son type est paramétré sur "Etendue", une table des partitions étendue est créée. Essentiellement, la partition étendue est comparable à un disque dur à part entière ; elle comprend une table des partitions qui pointe sur une ou plusieurs partitions (désormais appelées **partitions logiques**, par opposition aux quatre **partitions primaires**) entièrement contenues dans la partition étendue elle-même. La Figure B–7, *Disque dur avec partition étendue* montre un disque dur avec une partition primaire et une partition étendue contenant deux partitions logiques (de même qu'une certaine quantité d'espace disque non partitionné).

Figure B–7 Disque dur avec partition étendue



Comme le montre cette figure, il y a une différence entre une partition primaire et une partition logique ; il ne peut y avoir que quatre partitions primaires, mais le nombre de partitions logiques est illimité (toutefois, en réalité, il n'est pas conseillé de définir et d'utiliser plus de 12 partitions logiques sur un seul disque dur).

A présent que nous avons présenté les partitions en général, voyons comment utiliser ces connaissances pour installer Red Hat Linux.

B.1.4 Préparation de l'espace nécessaire à Red Hat Linux

Si vous tentez de repartitionner un disque dur, vous pouvez être confronté aux trois scénarios suivants :

- De l'espace libre non partitionné est disponible.
- Une partition non utilisée est disponible.
- De l'espace libre est disponible dans une partition.

Examinons, dans l'ordre, chacun des scénarios.

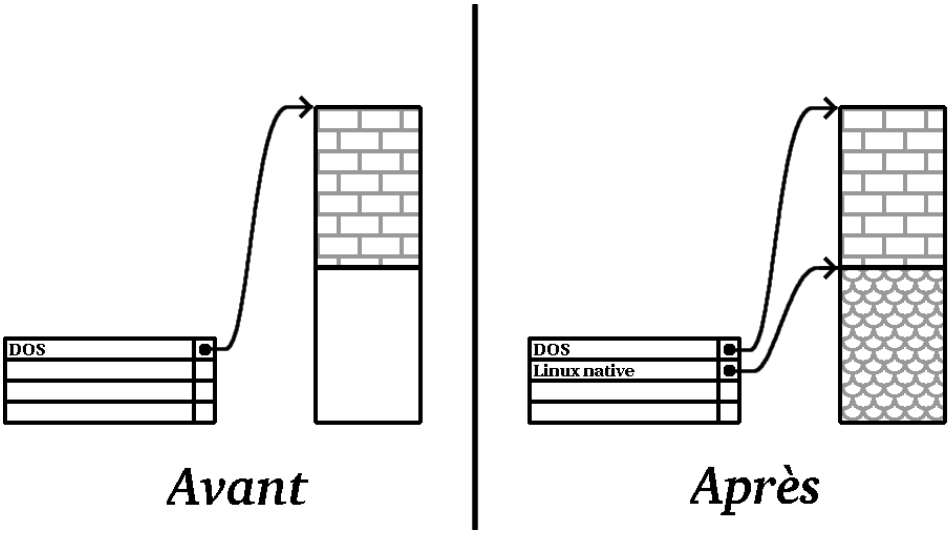
Remarque

N’oubliez pas que les illustrations suivantes, simplifiées par souci de clarté, ne reflètent pas rigoureusement le système de partitionnement que vous rencontrerez lors de l’installation réelle de Red Hat Linux.

Utilisation de l’espace libre non partitionné

Dans cette situation, les partitions déjà définies ne s’étendent pas sur tout le disque dur, laissant non attribué l’espace qui ne fait pas partie d’une partition définie. La Figure B–8, *Disque dur avec de l’espace disque non partitionné* montre à quoi cela pourrait ressembler.

Figure B–8 Disque dur avec de l’espace disque non partitionné



A y bien regarder, un disque dur non utilisé s’inscrit également dans cette catégorie ; la seule différence est que *tout* l’espace disque ne fait pas partie d’une partition définie.

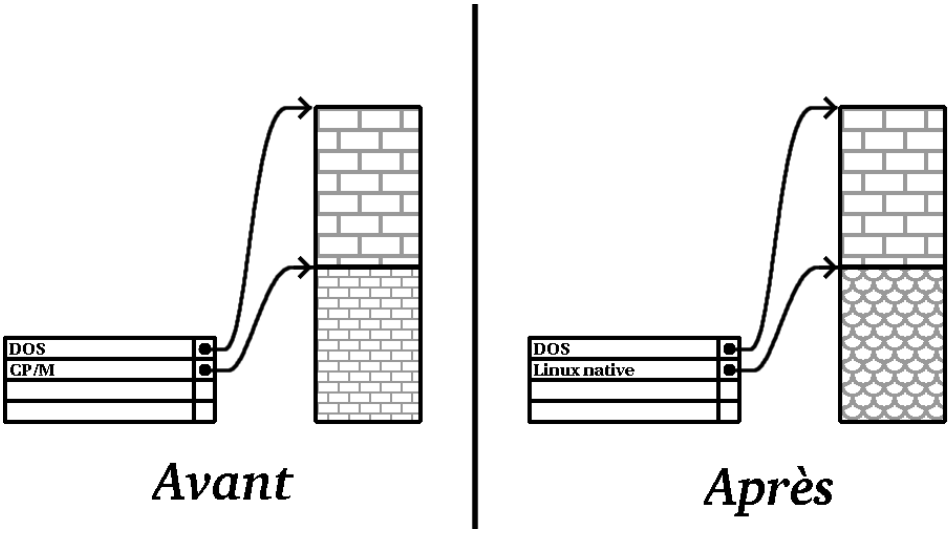
Dans tous les cas, vous pouvez simplement créer les partitions nécessaires à partir de l’espace inutilisé. Malheureusement, ce scénario, bien que très simple, est peu probable (à moins que vous n’ayez acheté un disque spécialement pour Red Hat Linux). La plupart des systèmes d’exploitation sont configurés de façon à utiliser tous l’espace disponible sur le disque (voir *Utilisation de l’espace libre d’une partition active* dans la section B.1.4).

Examinons une situation un peu plus courante.

Utilisation de l'espace d'une partition non utilisée

Dans ce cas, il se peut que vous n'utilisiez plus une ou plusieurs partitions. Peut-être avez-vous utilisé un autre système d'exploitation par le passé, et n'avez-vous plus jamais utilisé la (les) partition(s) dédiée(s) à ce système. La Figure B–9, *Disque dur avec une partition inutilisée* illustre cette situation.

Figure B–9 Disque dur avec une partition inutilisée



Si vous êtes dans cette situation, vous pouvez utiliser l'espace alloué à la partition inutilisée. Vous devez tout d'abord supprimer la partition, puis créer la (les) partition(s) Linux appropriée(s) à sa place. Vous pouvez soit supprimer la partition à l'aide de la commande DOS `fdisk`, soit procéder à une installation personnalisée de manière à ce que le système vous offre la possibilité de le faire.

Utilisation de l'espace libre d'une partition active

Il s'agit de la situation la plus courante. Il s'agit aussi, malheureusement, de la plus complexe. Le principal problème est que, même si vous avez suffisamment d'espace libre, il est actuellement alloué à une partition en cours d'utilisation. Si vous avez acheté un ordinateur avec un logiciel préinstallé, le disque dur a très probablement une partition importante contenant le système d'exploitation et les données.

Outre l'ajout d'un nouveau disque dur au système, vous avez deux possibilités :

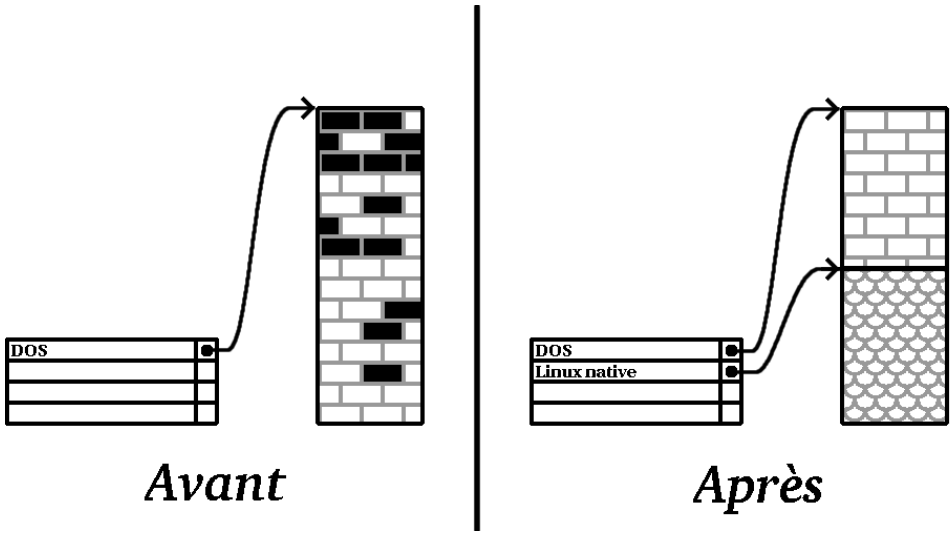
Repartitionnement destructeur

ATTENTION

Cela revient à supprimer la grande partition unique et à en créer plusieurs de plus petite taille. Comme vous pouvez l'imaginer, toutes les données de la partition d'origine seront supprimées. Ceci signifie que l'exécution d'une sauvegarde complète est nécessaire. Dans votre propre intérêt, effectuez deux sauvegardes, utilisez la fonction de vérification (si votre logiciel de sauvegarde en dispose), puis essayez de lire les données de la sauvegarde *avant* de supprimer la partition.

Après avoir créé une partition plus petite, pour le logiciel existant, vous pouvez réinstaller des logiciels, restaurer des données et poursuivre l'installation de Red Hat Linux. La Figure B–10, *Disque dur en cours de repartitionnement destructeur* illustre cette procédure.

Figure B–10 Disque dur en cours de repartitionnement destructeur



ATTENTION

Comme l'illustre la Figure B–10, *Disque dur en cours de repartitionnement destructeur* toutes les données présentes dans la partition d'origine seront perdues à défaut de sauvegarde appropriée !

Repartitionnement non destructeur

Vous exécutez ici un programme qui accomplit apparemment l'impossible : il rétrécit une grande partition sans perdre aucun des fichiers qui y sont stockés. De nombreuses personnes ont jugé cette méthode à la fois fiable et sûre. Quel logiciel utiliser pour réaliser cet exploit ? Il existe plusieurs logiciels de gestion de disque sur le marché ; vous devrez effectuer des recherches pour trouver celui correspondant le mieux à votre situation.

Si le processus de repartitionnement non destructeur est assez simple, il comporte plusieurs étapes :

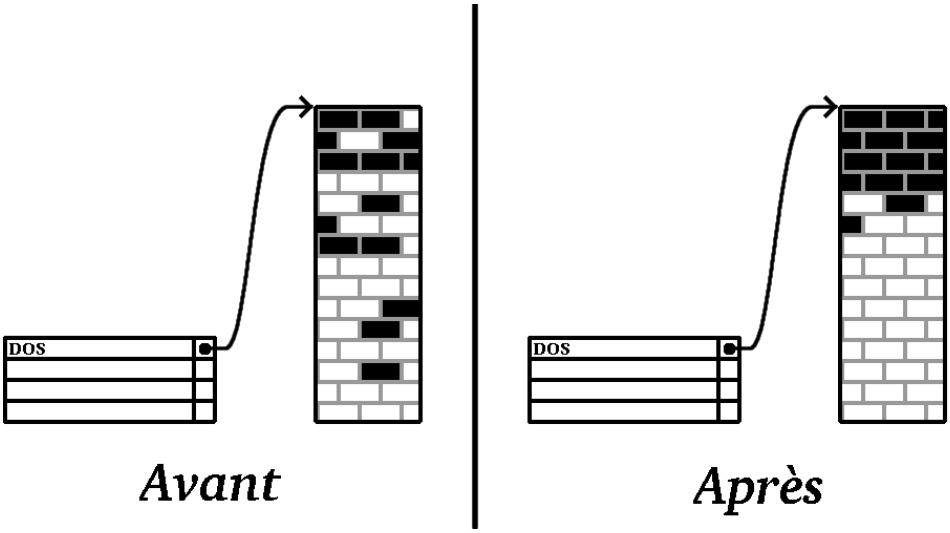
- Compression des données existantes
- Redimensionnement de la partition
- Création de nouvelle(s) partition(s)

Examinons chacune de ces étapes plus en détail.

Compression des données existantes

Comme l'illustre la Figure B–11, *Compression du disque* la première étape consiste à comprimer les données dans la partition existante. Cela permet de réorganiser les données de façon à disposer d'un maximum d'espace libre disponible à la "fin" de la partition.

Figure B–11 Compression du disque

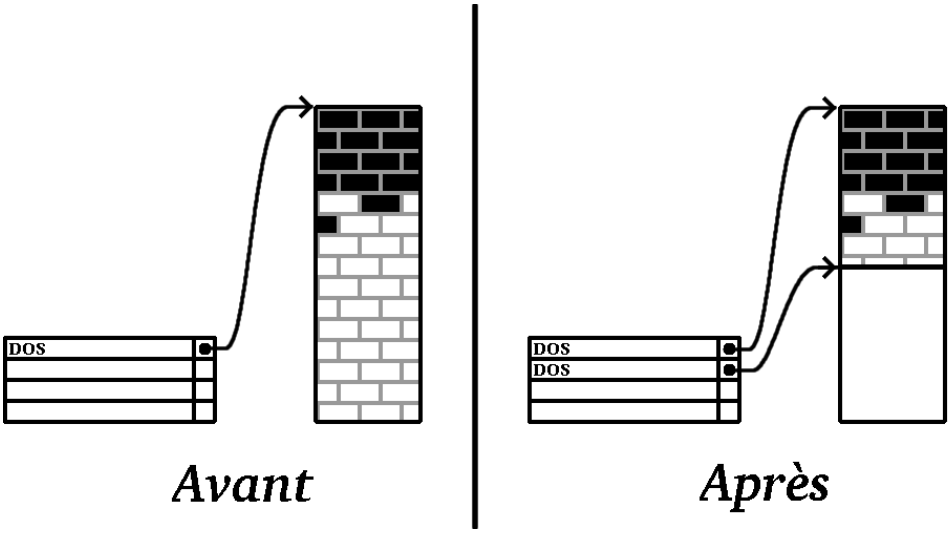


Cette étape est essentielle ; sans elle, il est possible que l'emplacement occupé par les données empêche le redimensionnement de la partition à la taille désirée. En outre, il est impossible de déplacer certaines données. Dans cette hypothèse (et ceci limite la taille des nouvelles partitions), vous risquez d'être forcé à repartitionner votre disque de façon destructive.

Redimensionnement de la partition

La Figure B–12, *Disque dur avec partition redimensionnée* montre le processus de redimensionnement réel. Si le résultat final de l'opération de redimensionnement varie en fonction du logiciel utilisé, le plus souvent, l'espace disque libéré est utilisé pour créer une partition non formatée du même type que la partition d'origine.

Figure B–12 Disque dur avec partition redimensionnée

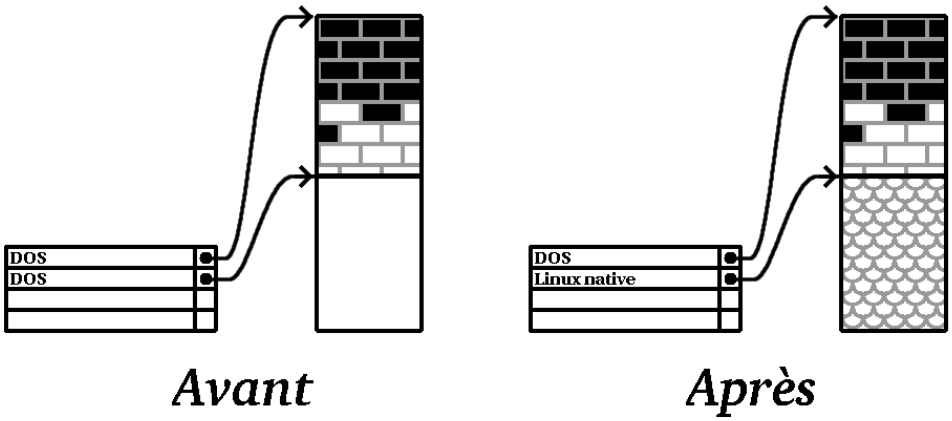


Il est important de comprendre ce que le logiciel de redimensionnement utilisé fait de l'espace libéré, de manière à pouvoir prendre les mesures appropriées. Dans le cas que nous avons illustré, il serait préférable de supprimer simplement la nouvelle partition DOS et de créer la (les) partition(s) Linux appropriée(s).

Création de nouvelle(s) partition(s)

Comme l'impliquait l'étape précédente, il peut être ou non nécessaire de créer de nouvelles partitions. Toutefois, à moins que votre logiciel de redimensionnement ne tienne compte de Linux, vous devrez probablement supprimer la partition créée durant le processus de redimensionnement. La Figure B–13, *Disque dur avec configuration de partition finale* illustre cette procédure.

Figure B–13 Disque dur avec configuration de partition finale



Remarque

Les informations suivantes sont spécifiques aux ordinateurs utilisant un processeur Intel.

Afin de simplifier cette étape pour nos clients, nous fournissons l'utilitaire DOS `fips` sur le CD 1 de Red Hat Linux/x86, dans le répertoire `dosutils`. Il s'agit d'un programme libre permettant de redimensionner les partitions de la FAT (File Allocation Table, table d'allocation des fichiers).

AVERTISSEMENT

De nombreuses personnes ont utilisé `fips` avec succès pour repartitionner leurs disques durs. Toutefois, en raison de la nature des opérations effectuées par `fips` et du vaste éventail de configurations matérielles et logicielles avec lesquelles ce programme est appelé à fonctionner, Red Hat n'est pas en mesure de garantir que `fips` fonctionnera correctement sur votre système. C'est pourquoi aucune assistance pour l'installation n'est disponible pour `fips` ; vous l'utiliserez à vos risques et périls.

Ceci dit, si vous décidez de repartitionner votre disque dur à l'aide de `fips`, vous devez *absolument* faire les deux choses suivantes :

- *Sauvegarde* — Réalisez deux copies de toutes les données importantes figurant sur votre ordinateur. Stockez ces copies sur des supports amovibles (tels qu'une bande ou des disquettes) et assurez-vous que les données sauvegardées sont accessibles avant de poursuivre.
- *Lecture de la documentation* — Lisez entièrement la documentation de `fips` figurant dans le sous-répertoire `/dosutils/fipsdocs` du CD-ROM Red Hat Linux/x86 1.

Si vous décidez d'utiliser `fips`, sachez qu'après l'exécution de `fips`, vous vous retrouverez avec *deux* partitions : celle que vous aurez redimensionnée et celle créée par `fips` à partir de l'espace libéré. Si vous avez l'intention d'utiliser cet espace pour installer Red Hat Linux, supprimez la nouvelle partition créée, soit à l'aide de la commande `fdisk` sous votre système d'exploitation actuel, soit lors de la configuration des partitions pendant une installation personnalisée.

B.1.5 Système de dénomination de partition

Linux fait référence aux partitions de disque à l'aide d'une combinaison de lettres et de chiffres qui peut sembler peu claire, en particulier si vous êtes accoutumé à appeler "disque C" le disque dur et ses partitions. Voici comment les partitions sont nommées dans l'environnement DOS/Windows :

- Chaque type de partition est vérifié pour déterminer s'il peut être lu par DOS/Windows.
- Si le type de partition est compatible, le système lui attribue une "lettre d'unité". La première lettre d'unité est "C"
- Cette lettre peut être utilisée pour désigner cette partition de même que le système de fichiers figurant dans cette partition.

Red Hat Linux utilise un système de dénomination plus flexible, fournissant plus d'informations que l'approche adoptée par d'autres systèmes d'exploitation. Le système de dénomination est basé sur les fichiers, avec des noms de fichier présentant la forme :

```
/dev/xxyN
```

Voici comment déchiffrer le système de dénomination de partition :

/dev/

Cette chaîne est le nom du répertoire dans lequel se trouvent tous les fichiers de périphérique. Etant donné que les partitions se trouvent sur des disques durs et que ceux-ci sont des périphériques, les fichiers représentant toutes les partitions possibles se trouvent dans `/dev/`.

xx

Les deux premières lettres du nom de partition indiquent le type de périphérique sur lequel se trouve la partition. Vous voyez normalement `hd` (pour les disques IDE) ou `sd` (pour les disques SCSI).

y

Cette lettre indique le périphérique sur lequel se trouve la partition. Par exemple, `/dev/hda` (premier disque dur IDE) ou `/dev/sdb` (second disque SCSI).

N

Le nombre final désigne la partition. Les quatre premières partitions (primaires ou étendues) sont numérotées de `1` à `4`. La numérotation des partitions logiques commence à `5`. Par exemple, `/dev/hda3` désigne la troisième partition primaire ou étendue du premier disque dur IDE ; `/dev/sdb6` désigne la seconde partition logique du second disque dur SCSI.

Remarque

Aucune partie de cette convention de dénomination n'est basée sur le type de partition ; à la différence de DOS/Windows, sous Red Hat Linux, *toutes* les partitions peuvent être identifiées. Ceci ne signifie évidemment pas que Red Hat Linux peut accéder aux données de chaque type de partition, même si, dans bien des cas, il est possible d'accéder aux données figurant sur une partition dédiée à un autre système d'exploitation.

Gardez ces informations à l'esprit ; elles vous aideront à comprendre le processus de configuration des partitions requises par Red Hat Linux.

B.1.6 Partitions de disque et autres systèmes d'exploitation

Si vos partitions Red Hat Linux doivent partager un disque dur avec des partitions utilisées par d'autres systèmes d'exploitation, vous n'aurez généralement pas de problèmes. Toutefois, certaines combinaisons de Linux et d'autres systèmes d'exploitation requièrent une attention particulière. Des informations sur la création de partitions de disque compatibles avec d'autres systèmes d'exploitation sont disponibles dans plusieurs HOWTO et Mini-HOWTOs, figurant sur le CD de documentation dans les répertoires `HOWTO` et `HOWTO/mini`. En particulier, les Mini-HOWTO dont les noms débutent par `Linux+` sont très utiles.

Remarque

Si Red Hat Linux/x86 doit coexister sur votre ordinateur avec OS/2, créez vos partitions de disque avec le logiciel de partitionnement d'OS/2 ; sinon, OS/2 risque de ne pas reconnaître les partitions de disque. Durant l'installation, ne créez pas de nouvelles partitions, mais définissez les types de partition appropriés pour vos partitions Linux à l'aide de la commande `fdisk`.

B.1.7 Partitions de disque et points de montage

Un aspect que de nombreux débutants dans l'utilisation de Linux trouvent confus est la manière dont les partitions sont utilisées par le système d'exploitation Linux. Sous DOS/Windows, c'est relativement simple : si vous avez plusieurs partitions, une "lettre de disque" est attribuée à chaque partition. Vous utilisez alors la lettre du disque pour faire référence aux fichiers et répertoires figurant sur une partition donnée.

La façon dont Red Hat Linux gère les partitions, et donc les disques en général, est complètement différente. En effet, vous utilisez chaque partition comme partie intégrante de l'arbre du système de fichiers de Linux. Pour ce faire, vous associez une partition à un répertoire dans le cadre d'un processus appelé **montage**. Le montage d'une partition rend son contenu disponible à partir d'un répertoire spécifié (appelé **point de montage**).

Par exemple, si une partition `/dev/hda5` était montée sur `/usr`, cela signifierait que tous les fichiers et répertoires sous `/usr` se trouveraient physiquement sur `/dev/hda5`. Ainsi le fichier `/usr/share/doc/FAQ/txt/Linux-FAQ` serait stocké sur `/dev/hda5`, tandis que le fichier `/etc/X11/gdm/Sessions/Gnome` ne le serait pas.

Si nous poursuivons avec notre exemple, il est également possible qu'un ou plusieurs répertoires sous `/usr` soient des points de montage pour d'autres partitions. Par exemple, une partition (disons `/dev/hda7`) pourrait être montée sur `/usr/local`, ce qui signifie que, par exemple, `/usr/local/man/whatis` se trouverait alors sur `/dev/hda7` plutôt que sur `/dev/hda5`.

B.1.8 Combien de partitions ?

A ce stade du processus de préparation de l'installation de Red Hat Linux, vous devez tenir compte du nombre et de la taille des partitions que doit utiliser le nouveau système d'exploitation. La question du "nombre de partitions" continue à susciter le débat au sein de la communauté des utilisateurs de Linux et, à défaut d'entrevoir la fin du débat, il est prudent de dire qu'il y a probablement autant de systèmes de partitionnement que de personnes débattant de la question.

Cela dit, nous vous conseillons, à moins que vous n'ayez de bonnes raisons de procéder autrement, de créer les partitions suivantes :

- *Une partition swap* — Les partitions swap sont utilisées pour prendre en charge la mémoire virtuelle. Autrement dit, les données sont écrites dans la partition swap lorsqu'il n'y a pas de RAM pour accueillir les données que votre système traite. Vous *devez* créer une partition swap pour pouvoir utiliser correctement Red Hat Linux. La taille minimale de la partition swap doit être égale à au moins deux fois la la mémoire vive de votre ordinateur ou à 32 Mo.
- *Une partition `/boot`* — La partition montée sur `/boot` contient le noyau du système d'exploitation (qui permet à votre système de démarrer Red Hat Linux), de même que quelques autres fichiers utilisés durant le processus d'amorçage.

N'oubliez pas de lire la Section B.1.9, *Un dernier tuyau : utilisation de LILO* — les informations qu'elle contient ont trait à la partition `/boot` !

Vu les limites de la plupart des PC BIOS, il serait préférable de créer une petite partition pour les conserver. Une partition de 32 Mo serait suffisante.

- *Une partition root (/)* — La partition root est l'endroit où se trouve le répertoire root `/`. Dans ce type de partitionnement, tous les fichiers (à l'exception de ceux stockés dans `/boot`) se trouvent sur la partition root. C'est pourquoi vous avez intérêt à choisir une partition root de grande taille. Une partition root de 1,2 Go permet d'effectuer l'équivalent d'une installation de la classe Poste de travail (avec *très* peu d'espace libre), alors qu'une partition root de 2,4 Go permet d'installer tous les paquetages. Il est évident que plus vous avez d'espace à consacrer à la partition root, mieux c'est.

Des recommandations concernant la taille des différentes partitions Red Hat Linux sont contenues dans le *Guide d'installation officiel Red Hat Linux pour x86*.

B.1.9 Un dernier tuyau : utilisation de LILO

LILO (LInux LOader) est la méthode la plus couramment utilisée pour démarrer Red Hat Linux sur les systèmes équipés d'un processeur Intel. Chargeur du système d'exploitation, LILO opère "en dehors" de tout système d'exploitation, en utilisant uniquement le système E/S de base (ou BIOS) intégré dans le matériel de l'ordinateur lui-même. Cette section décrit les interactions de LILO avec le BIOS du PC. Elle est spécifique aux ordinateurs compatibles Intel.

Limitations du BIOS affectant LILO

LILO est soumis à certaines limitations imposées par le BIOS de la plupart des ordinateurs équipés d'un processeur Intel. En particulier, la plupart des BIOS ne peuvent pas accéder à plus de deux disques durs, ni à des données stockées au-delà du cylindre 1023 de n'importe quel disque. Certains BIOS récents ne connaissent pas ces limitations.

Toutes les données auxquelles LILO doit pouvoir accéder au démarrage (notamment le noyau Linux) sont situées dans le répertoire `/boot`. Si vous vous conformez au système de partitionnement préconisé ci-dessus ou si vous procédez à une installation de classe Poste de travail ou Serveur, le répertoire `/boot` se trouvera dans une petite partition séparée. Sinon, il se trouvera dans la partition root. Dans les deux cas, la partition dans laquelle `/boot` se trouve doit être conforme aux instructions ci-dessous si vous voulez utiliser LILO pour démarrer votre système Red Hat Linux :

Sur les deux premiers disques IDE

Si vous avez deux disques IDE (ou EIDE), `/boot` doit figurer sur l'un d'eux. Cette limite de deux disques englobe également tous les lecteurs de CD-ROM IDE du contrôleur IDE principal. Ainsi, si vous avez un disque dur IDE et un lecteur de CD-ROM IDE sur le contrôleur principal, `/boot` doit être situé *uniquement* sur le premier disque dur, même si vous avez d'autres disques durs sur votre contrôleur IDE secondaire.

Sur le premier disque IDE ou SCSI

Si vous avez un disque IDE (ou EIDE) et un ou plusieurs disques SCSI, `/boot` doit être situé sur le disque IDE ou sur le disque SCSI dont l'ID est 0. Aucun autre ID SCSI ne fonctionnera.

Sur les deux premiers disques SCSI

Si vous n'avez que des disques durs SCSI, `/boot` doit être situé sur un disque dont l'ID est 0 ou 1. Aucun autre ID SCSI ne fonctionnera.

Partitionnement *entièrement* avant le cylindre 1023

Quelle que soit la configuration, la partition contenant `/boot` doit être entièrement située avant le cylindre 1023. Si la partition contenant `/boot` chevauche le cylindre 1023, vous risquez de

vous trouver dans une situation où LILO fonctionnera initialement (parce que toutes les informations nécessaires figureront avant le cylindre 1023), mais connaîtra une défaillance si un nouveau noyau doit être chargé, car celui-ci sera enregistré après le cylindre 1023.

Comme indiqué plus haut, il se peut que certains BIOS récents permettent à LILO de fonctionner avec des configurations non conformes à ces instructions. De même, certaines fonctions plus complexes de LILO peuvent être utilisées pour faire démarrer un système Linux, même si la configuration n'est pas conforme à ces instructions. Toutefois, en raison du nombre de facteurs, Red Hat ne peut pas prendre en charge un effort aussi considérable.

Remarque

Disk Druid, de même que les installations des classes Poste de travail et Serveur, tient compte de ces limitations liées au BIOS.

C Disquettes de pilotes

C.1 Utilité d'une disquette de pilotes

Lors du chargement du programme d'installation de Red Hat Linux, il se peut que le système affiche un écran vous demandant une disquette de pilote. Cet écran s'affiche généralement dans les trois cas suivants :

- si vous exécutez le programme d'installation en mode `expert`,
- si vous exécutez le programme d'installation en entrant **`linux dd`** à l'invite `boot:`
- si vous exécutez le programme d'installation sur un ordinateur n'ayant pas de périphériques PCI.

C.1.1 Qu'est-ce qu'une disquette de pilotes ?

Une disquette de pilotes ajoute une capacité de prise en charge pour du matériel qui, sans elle, ne serait pas pris en charge par le programme d'installation. La disquette de pilotes peut être créée par Red Hat ou par vous à partir de pilotes trouvés sur Internet, ou fournie par le vendeur avec le matériel acheté.

Il est en réalité inutile d'utiliser une disquette de pilotes à moins que vous n'ayez besoin d'un périphérique particulier pour installer Red Hat Linux. Vous serez probablement amené à utiliser une disquette de pilotes pour les lecteurs CD-ROM non standard ou très récents, les cartes SCSI et les cartes réseau, dès lors que ce sont les seuls périphériques utilisés durant l'installation pouvant nécessiter l'utilisation de pilotes non inclus dans les CD-ROMs de Red Hat Linux (ou disquette, si vous avez créé une disquette d'amorçage pour démarrer le processus d'installation).

Remarque

Si un périphérique non pris en charge n'est pas nécessaire pour installer Red Hat Linux sur votre système, poursuivez l'installation normale, puis ajoutez les pilotes du nouvel élément matériel une fois l'installation terminée.

C.1.2 Comment se procurer une disquette de pilotes ?

Dans le CD-ROM 1 de Red Hat Linux vous trouverez une image de disquette de pilotes (`images/drivers.img`) contenant de nombreux pilotes peu utilisés. Si vous pensez que votre système requiert certains de ces pilotes, nous vous conseillons de créer la disquette de pilotes avant de procéder à l'installation de Red Hat Linux.

Une autre façon de chercher des informations sur les disquettes de pilotes consiste à consulter le site Web de Red Hat à l'adresse http://www.redhat.com/support/errata dans la section intitulée **Bug Fixes**.

Il se peut que du matériel très connu mis en vente après la sortie d'une édition de Red Hat Linux ne fonctionne pas avec les pilotes déjà présents dans le programme d'installation ou inclus dans l'image de disquette de pilotes du CD-ROM 1 de Red Hat Linux. Dans des cas comme celui-la, vous pourriez trouver dans le site Web de Red Hat un lien à une image de disquette de pilotes que vous pouvez utiliser pour installer Red Hat Linux sur ce type de matériel.

Création d'une disquette de pilotes à partir d'un fichier d'image

Si vous avez une image de disquette de pilotes et que vous devez l'écrire sur une disquette, vous pouvez le faire en utilisant DOS ou Red Hat Linux.

Pour créer une disquette de pilotes à partir d'une image de disquette de pilotes en utilisant Red Hat Linux :

1. Insérez une disquette vierge formatée dans le premier lecteur de disquette.
2. A partir du même répertoire contenant l'image de la disquette de pilotes, tel que *dd.img*, entrez `cat`*`dd.img`* `> /dev/fd0` en étant connecté en tant que root.

Pour créer une disquette de pilotes à partir d'une image de disquette de pilotes en utilisant DOS :

1. Insérez une disquette vierge formatée dans le lecteur a: .
2. A partir du même répertoire contenant l'image de la disquette de pilotes, tel que *dd.img*, entrez `rawrite`*`dd.img`* `a:` à la ligne de commande.

C.1.3 Utilisation d'une disquette de pilotes pendant l'installation

Le fait d'avoir une disquette de pilotes ne suffit pas. Vous devez dire au programme d'installation de Red Hat Linux de charger cette disquette et de l'utiliser pendant le processus d'installation.

Remarque

Une disquette de pilotes diffère d'une disquette d'amorçage. Si vous devez démarrer votre installation à partir d'une disquette, vous devrez toujours créer cette disquette et démarrer à partir de celle-ci avant de pouvoir utiliser votre disquette de pilotes.

Si vous n'avez pas encore de disquette de démarrage de l'installation et que votre système ne gère pas le démarrage à partir du CD-ROM, créez-en une en utilisant le fichier *`filename`*`.img` approprié (tel que `boot.img`) dans le répertoire `images` du CD-ROM 1. Pour plus d'informations sur la création d'une disquette de démarrage, reportez-vous à la section sur la création des disquettes d'amorçage du *Guide d'installation officiel Red Hat Linux pour x86*

Après avoir créé votre disquette de pilotes, commencez le processus d'installation avec le CD-ROM 1 de Red Hat Linux (ou la disquette de démarrage de l'installation que vous avez créée si vous ne pouvez pas démarrer l'installation du CD-ROM), puis, entrez **`linux expert`** ou **`linux dd`** à l'invite `boot:`.

Le programme d'installation de Red Hat Linux vous demandera d'insérer la disquette de pilotes. Une fois que la disquette de pilotes est lue par le programme, les pilotes découverts sur votre système au cours du processus d'installation pourront être pris en charge.

D RAID (réseau de disques redondants)

D.1 Qu’est-ce que RAID ?

Le principe du RAID consiste à combiner plusieurs lecteurs de disque de petite taille et bon marché en un réseau permettant des performances supérieures à celles d’un lecteur de grande taille et coûteux. L’ordinateur "voit" ce réseau de lecteurs comme une unité de stockage logique ou un lecteur unique.

RAID est une méthode en vertu de laquelle les informations sont réparties sur plusieurs disques, à l’aide de techniques telles que l’**agrégat par bandes** (RAID 0) et la **mise en miroir** (RAID 1) afin d’obtenir une redondance, une moindre latence et/ou une bande passante plus importante pour la lecture et l’écriture sur les disques, et de maximiser la faculté de récupération après des pannes de disque dur.

Le concept sous-jacent de la technologie RAID est que des données peuvent être réparties sur les différents lecteurs du réseau de façon cohérente. A cette fin, les données doivent préalablement être fractionnées en "morceaux" de taille constante (souvent de 32 ou 64 Ko, même si des tailles différentes peuvent être utilisées). Chaque "morceau" est ensuite écrit, successivement, sur chaque disque. Lorsque les données doivent être lues, le processus est inversé, ce qui donne l’illusion que les multiples petits lecteurs n’en constituent en réalité qu’un seul de grande taille

D.1.1 Pourquoi utiliser un RAID ?

La technologie RAID permet d’avoir sous la main de grandes quantités de données (ce dont peuvent avoir besoin les administrateurs). Parmi les principales raisons justifiant l’utilisation du RAID figurent :

- vitesse accrue
- capacité de stockage accrue en utilisant un unique disque virtuel
- efficacité accrue pour la récupération après une défaillance de disque dur

D.1.2 RAID : matériel et logiciel

On distingue deux approches du RAID : le RAID matériel et le RAID logiciel.

RAID matériel

Le système matériel gère le sous-système RAID en toute indépendance par rapport à l’hôte et ne présente à l’hôte qu’un seul disque par réseau RAID.

Un périphérique RAID matériel peut être, par exemple celui qui, connecté à une carte SCSI, présente le réseau RAID comme une seule unité SCSI. Un système RAID externe déplace toute l’"intelligence" de traitement du réseau RAID vers un contrôleur situé dans le sous-système de disques externes. Le

sous-système tout entier est connecté à l'hôte via une carte SCSI normale, de sorte qu'il apparaît à l'hôte comme un disque unique.

Les contrôleurs RAID sont souvent fournis sous la forme de cartes qui *se comportent* comme une carte SCSI pour le système d'exploitation, mais traitent en réalité toutes les communications de l'unité. Dans ce cas, vous connectez les lecteurs au contrôleur RAID, tout comme vous le feriez avec une carte SCSI. Mais ensuite, vous les ajoutez à la configuration du contrôleur RAID et le système d'exploitation ne détecte pas la différence.

RAID logiciel

Le RAID logiciel implémente les divers niveaux du RAID dans le code du noyau, au niveau di pilote de disque. Il constitue également la solution la plus économique qui soit : des cartes contrôleur de disque onéreuses ou un châssis remplaçable à chaud [1]ne sont plus nécessaires, et le RAID logiciel fonctionne avec des disques IDE moins chers, de même qu'avec des disques SCSI. Avec les processeurs rapides disponibles aujourd'hui, les performances d'un RAID logiciel peuvent s'avérer excellentes par rapport à celles d'un RAID matériel.

Le pilote MD dans le noyau Linux est un exemple de solution RAID totalement indépendante du matériel. Les performances d'un RAID logiciel dépendent des performances et de la charge du processeur du serveur.

Pour plus d'informations sur la configuration du RAID logiciel pendant l'installation de Red Hat Linux, reportez-vous au *Guide de personnalisation officiel Red Hat Linux*.

Pour en savoir plus sur ce qu'offre le RAID logiciel, voici une courte liste de quelques-unes de ses fonctions :

- Processus de reconstruction chaîné
- Configuration complète à partir du noyau
- Portabilité des réseaux entre ordinateurs sous Linux sans reconstruction
- Reconstruction de réseau en arrière-plan à l'aide de ressources systèmes inactives
- Support de lecteur remplaçable à chaud
- Détection de processeur automatique pour tirer parti de certaines optimisations de processeur

D.1.3 Niveau et support linéaire

La technologie RAID offre également les niveaux 0, 1, 4, 5 et un support linéaire. Ces types de RAID agissent comme suit :

[1] Un châssis remplaçable à chaud permet de retirer un disque dur sans devoir arrêter le système.

- *Niveau 0* — Le RAID de niveau 0, souvent appelé "agrégat par bandes", est une technique de répartition de données axée sur les performances. Cela signifie que les données écrites sur le réseau sont fractionnées en bandes et écrites sur les disques composant le réseau. Ceci permet d'obtenir des performances d'E/S élevées à faible coût mais n'offre aucune redondance. La capacité de stockage du niveau 0 est égale à la capacité totale des disques contenus dans un RAID matériel ou à la capacité totale des partitions membres d'un RAID logiciel.
- *Niveau 1* — Le RAID de niveau 1, ou "mise en miroir de disque" a été utilisé plus longtemps que n'importe quelle forme de RAID. Le niveau 1 offre la redondance en écrivant des données sur chaque disque membre du RAID, en laissant une copie "en miroir" sur chaque disque. L'exploitation en miroir reste très utilisée en raison de sa simplicité et du haut niveau de disponibilité des données. Le niveau 1 opère avec deux disques ou plus, pouvant utiliser un accès parallèle pour atteindre des vitesses de transfert de données élevées en lecture, mais fonctionne, le plus souvent, de façon indépendante afin de permettre des vitesses d'E/S élevées. Le niveau 1 offre une excellente fiabilité pour les données et améliore les performances des applications impliquant une activité de lecture intense, mais à un coût relativement élevé. [2]La capacité du niveau 1 est égale à la capacité d'un disque miroir dans un RAID matériel ou d'une partition miroir dans un RAID logiciel.
- *Niveau 4* — Le niveau 4 utilise la parité [3]sur un seul lecteur de disque pour protéger des données. Il est plus adapté aux E/S transactionnelles qu'aux transferts de fichiers volumineux. Du fait que le disque de parité dédié entraîne, par définition, un étranglement, le niveau 4 est rarement utilisé sans technologies complémentaires telles que l'antémémoire de réécriture. Bien que le RAID de niveau 4 soit une option dans certains systèmes de partitionnement RAID, elle n'est pas autorisée dans les installations RAID de Red Hat Linux.[4]La capacité de stockage du RAID matériel niveau 4 est égale à la capacité des disques membres moins un. La capacité de stockage du RAID logiciel niveau 4 est égale à la capacité des partitions membres, moins la taille d'une partition si elles sont de même taille.
- *Niveau 5* — Type de RAID le plus répandu. En répartissant la parité sur certains lecteurs de disque membres d'un tableau, le RAID de niveau 5 élimine les étranglements en écriture propres

[2] Le RAID de niveau 1 implique un coût élevé car vous écrivez les mêmes informations sur tous les disques du réseau RAID, ce qui implique un gaspillage de l'espace disque. Par exemple, un RAID de niveau 1 peut être configuré de telle sorte que votre partition root (`/`) s'étende sur deux lecteurs de 40 Go. Vous disposez donc, au total, de 80 Go, mais ne pouvez accéder qu'à 40 de ces 80 Go. Les 40 Go restants sont utilisés comme un miroir des 40 premiers.

[3] Les informations de parité sont calculées sur la base du contenu des autres disques du réseau. Ces informations peuvent être utilisées pour reconstituer les données en cas de défaillance d'un disque du réseau. Les données reconstituées peuvent ensuite être utilisées pour satisfaire aux demandes d'E/S adressées aux disques défaillants et pour reconstituer leur contenu après qu'ils aient été réparés ou remplacés.

[4] RAID 4 occupe autant d'espace que RAID 5, mais les avantages offerts par ce dernier sont tels que RAID 4 n'est plus pris en charge.

au niveau 4. Le seul étranglement provient du processus de calcul de la parité. Grâce aux processeurs modernes et au RAID logiciel, cet étranglement n'est pas très conséquent. Comme pour le niveau 4, les résultats obtenus étant asymétriques, les performances en lecture sont sensiblement supérieures aux performances en écriture. Le niveau 5 est souvent utilisé en association avec l'antémémoire de réécriture afin de réduire l'asymétrie. La capacité de stockage du RAID matériel de niveau 5 est égale à la capacité des disques membres moins un. La capacité de stockage du RAID logiciel de niveau 5 est égale à la capacité des partitions membres, moins la taille d'une partition si elles sont de même taille.

- *RAID linéaire* — Le RAID linéaire est un simple regroupement de lecteurs visant à créer un lecteur virtuel de plus grande taille. Dans le RAID linéaire, les morceaux sont attribués de façon séquentielle, à partir de l'un des lecteurs, ne passant au lecteur suivant que lorsque le premier est totalement saturé. Ce regroupement n'offre aucun avantage en matière de performances, étant donné qu'il est improbable que des opérations d'E/S soient fractionnées entre les lecteurs. Le RAID linéaire n'offre pas non plus de redondance et, en réalité, réduit la fiabilité —— en cas de défaillance de l'un des lecteurs, tout le réseau devient inutilisable. La capacité équivaut à la capacité totale de tous les disques.

E PowerTools

E.1 Qu'est-ce que PowerTools?

Red Hat PowerTools de Red Hat est un ensemble de paquetages logiciels conçs pour le système d'exploitation Red Hat Linux 7.1. PowerTools inclut les dernières versions (à la date d'édition de ce produit) de centaines de programmes ; il ne devrait donc pas être difficile de trouver une application intéressante.

Parmi les nombreuses applications disponibles figurent programmes audio, "chat clients", outils de développement, éditeurs, gestionnaires de fichiers, émulateurs, jeux programmes graphiques, applications de productivité, paquetages mathématiques/statistiques, outils d'administration système et de gestion de réseau et autres gestionnaires de fenêtres.

Etes-vous un administrateur système ? PowerTools offre un ensemble d'outils qui peuvent vous simplifier la vie et remplacer plusieurs utilitaires de diagnostic coûteux avec une seule application. Jetez un coup d'oeil à des applications comme Ethereal pour l'analyse des protocoles de réseau, PortSentry pour empêcher la lecture des ports sur le réseau ou Postfix comme alternative à Sendmail.

Vous aimez jouer ? PowerTools contient de nombreux jeux simples et très amusants, tels que SpeedX, XFrisk et Amphetamine.

Etant donné que, grâce aux applications RPM et Gnome-RPM, l'installation et la désinstallation de paquetages logiciels est très simple, vous pouvez essayer différentes applications similaires avant de choisir celle qui vous convient le mieux.

E.2 Paquetages de PowerTools

Si vous savez déjà quel(s) paquetage(s) PowerTools installer, reportez-vous à la Section E.3, *Installation des paquetages de PowerTools* pour plus d'informations sur le mode d'installation.

Toutefois, étant donné le nombre de paquetages de PowerTools disponibles, nous vous conseillons d'examiner leur description afin de trouver plus facilement ceux qui vous intéressent le plus.

E.2.1 Lecture du contenu du CD-ROM

Vous pouvez obtenir le contenu du CD-ROM PowerTools à partir d'une invite du shell (en mode console ou fenêtre de terminal). Commencez par monter le CD-ROM PowerTools dans le lecteur de CD-ROM.

Montage du CD-ROM de PowerTools

Si votre système n'est pas configuré de façon à monter automatiquement le lecteur de CD-ROM lorsque un CD y est inséré, insérez le CD PowerTools dans le lecteur. En étant connecté en tant que root, entrez la commande suivante :

```
mount -t iso9660 /dev/cdrom /mnt/cdrom
```

Remarque

Votre système vous permet, ainsi qu'à votre administrateur système, d'autoriser d'autres utilisateurs (non connectés en tant que root) de monter le lecteur de CD-ROM. Les utilisateurs jouissent de ce privilège si l'option `user` est incluse dans la ligne `/dev/cdrom` du fichier `/etc/fstab`. N'oubliez pas, cependant, que vous devez être connecté en tant que root pour pouvoir installer des RPM PowerTools.

Lecture du fichier `CONTENTS`

Une fois le lecteur monté, changez de répertoire à l'aide de la commande suivante :

```
cd /mnt/cdrom
```

Enfin, entrez `less CONTENTS` pour afficher les applications disponibles. Le fichier `CONTENTS` contient tous les programmes du CD-ROM PowerTools classés par ordre alphabétique.

La lecture du fichier `CONTENTS` du CD-ROM PowerTools peut être une tâche difficile si l'on considère le nombre d'applications disponibles. Voici un conseil pour éviter de lire toutes les descriptions :

- *Utilisez le nom du groupe* — Chaque application est associée à un groupe particulier. Par exemple, FaxMail, utilitaire pour l'envoi de fax, fait partie du groupe Applications/Communications et Icecast, système de diffusion MP3 sur Internet, fait partie du groupe Applications/Multimédia. En effectuant une sélection des groupes, vous éviterez de devoir lire toutes les descriptions de paquetages et gagnerez ainsi du temps.
- *Recherche à l'aide de mots clés* — La commande `ls` permet d'effectuer une recherche simplifiée. Si vous cherchez un client IRC, entrez la commande `less CONTENTS` pour afficher `CONTENTS`, puis entrez **`/IRC`** et appuyez sur [Entrée]. Le premier client IRC de la liste apparaîtra à l'écran. Si celui-ci ne vous intéresse pas, appuyez sur la touche [n] jusqu'à ce que vous ne trouviez le paquetage qui vous intéresse.

Si vous avez des problèmes avec la commande `less`, entrez `man less` à l'invite pour afficher l'aide.

Démontage du CD-ROM PowerTools

Une fois que vous avez terminé d'utiliser le CD-ROM PowerTools pour installer les paquetages, vous pouvez le retirer du lecteur. Si le CD-ROM est monté dans le répertoire `/mnt/cdrom`, faites ceci :

1. Changez de répertoire en utilisant la commande `cd /mnt` de façon à vous trouver un niveau au-dessus du répertoire `/mnt/cdrom`.
2. Entrez `umount /mnt/cdrom` pour démonter le CD-ROM.
3. Entrez `eject /dev/cdrom`. Le lecteur s'ouvrira et vous pourrez retirer le CD-ROM.

E.3 Installation des paquetages de PowerTools

E.3.1 Installation de PowerTools dans un environnement graphique

Si vous utilisez GNOME ou KDE, insérez le CD-ROM dans le lecteur de CD-ROM. Le système vous invite à entrer le mot de passe root (vous devez être connecté en tant que root pour pouvoir installer des paquetages). Une fois le mot de passe root entré, le programme Gnome-RPM ou le programme de gestion de paquetages Kpackage démarre automatiquement (selon l'environnement graphique utilisé) et peut être utilisé pour installer PowerTools.

Reportez-vous au *Guide de démarrage officiel Red Hat Linux* pour obtenir des instructions spécifiques sur l'utilisation de Gnome-RPM. Visitez le site http://www.general.uwa.edu.au/u/toivo/kpackage pour obtenir plus d'informations sur l'utilisation de Kpackage.

Si vous n'utilisez ni GNOME ni KDE, utilisez l'invite du shell pour installer PowerTools.

E.3.2 Installation de PowerTools à partir de l'invite du shell

Commencez par monter le CD-ROM PowerTools dans le lecteur de CD-ROM et utilisez la commande `ls` pour afficher son contenu. Pour obtenir des information sur le montage du CD-ROM, reportez-vous à *Montage du CD-ROM de PowerTools* dans la section E.2.1.

Vous verrez les répertoires suivants : `SRPMS` et `RedHat`. Le répertoire `SRPMS` contient les RPM source de PowerTools. Le répertoire `RedHat/RPMS` contient les RPM pour les trois architectures de système d'exploitation spécifiées.

Le chemin d'accès `RedHat/RPMS` est utilisé comme exemple général. Remplacez-le par le répertoire correspondant à `RedHat/RPMS`, en fonction de votre architecture et du paquetage à installer.

Utilisez la commande `cd` pour accéder au répertoire `RedHat/RPMS` :

```
cd RedHat/RPMS
```

Affichez la liste des fichiers RPM figurant dans le répertoire à l'aide de la commande `ls` afin de voir la liste complète des paquetages RPM inclus pour les systèmes compatibles Intel.

Peut-être souhaitez-vous plus d'informations sur un paquetage spécifique avant de décider de l'installer. Vous pouvez utiliser la fonctionnalité d'interrogation de RPM pour obtenir plus d'informations sur les paquetages, par exemple sur leurs fonctions et leur origine. Reportez-vous au *Guide de personnalisation officiel Red Hat Linux* pour obtenir des instructions sur la manière d'interroger les paquetages à l'aide de l'application RPM.

Autrement, vous pouvez chercher dans le fichier `CONTENTS` les paquetages qui vous intéressent. Reportez-vous à *Lecture du fichier `CONTENTS`* dans la section E.2.1 pour obtenir plus d'informations.

Vous pouvez installer les paquetages sélectionnés à l'aide de RPM. RPM est un puissant système de gestion piloté par ligne de commande. Reportez-vous au *Guide de personnalisation officiel Red Hat Linux* pour plus d'informations sur la manière d'utiliser RPM pour installer et gérer des paquetages de PowerTools.

Une fois l'installation de vos paquetages terminée, démontez le CD-ROM. Si vous ne savez pas comment démonter le lecteur de CD-ROM, reportez-vous à *Démontage du CD-ROM PowerTools* dans la section E.2.1.

E.4 Désinstallation de PowerTools

La désinstallation des paquetages de PowerTools est similaire à la désinstallation de n'importe quel autre paquetage RPM.

Vous devez tout d'abord connaître le nom du paquetage que vous voulez désinstaller. Par exemple, pour supprimer `thrust-0.83c-11` de votre système, entrez en tant que root :

```
rpm -e thrust
```

En général, `rpm -e <nomdupaquetage>` supprime le paquetage et les fichiers y reliés de votre système. Le CD-ROM PowerTools n'est pas requis pour cette opération.

Pour plus d'informations sur l'utilisation de RPM, reportez-vous à *Guide de personnalisation officiel Red Hat Linux*.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W