Red Hat Enterprise Linux 4

Guide de référence

Red Hat Enterprise Linux 4: Guide de référence


Red Hat, Inc.

1801 Varsity Drive Raleigh NC 27606-2072 USA Téléphone : +1 919 754 3700 Téléphone : 888 733 4281 Fax : +1 919 754 3701 PO Box 1358
search Triangle Park NC 27709 États-Unis

rhel-rg(FR)-4-Impression-RHI (2004-09-30T17:13)

Le code GPG de la clé security@redhat.com est :
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Table des matières

Introduction

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

Le *Guide de référence de Red Hat Enterprise Linux* contient des informations utiles sur le système Red Hat Enterprise Linux. Depuis les concepts fondamentaux tels que la structure des systèmes de fichiers, jusqu'à certains points plus délicats concernant la sécurité du système et le contrôle de l'authentification, nous espérons que ce guide sera pour vous une précieuse ressource.

Ce guide vous convient tout particulièrement si vous souhaitez en savoir plus sur la manière dont fonctionne votre système Red Hat Enterprise Linux. Il examine en effet les sujets suivants :

- Le processus de démarrage
- La structure des systèmes de fichiers
- Le système X Window
- Les services de réseau
- Les outils de sécurité

1. Modifications apportées à ce manuel

La structure de ce manuel a été réorganisée dans un souci de clarté. Le manuel a également été mis à jour de manière à inclure les nouvelles fonctionnalités de Red Hat Enterprise Linux 4. Ci-après figure une liste des modifications apportées :

Un nouveau chapitre dédié à Samba

Le nouveau chapitre dédié à *Samba* examine les différents démons Samba et les options de configuration. Il convient de remercier ici tout particulièrement **John Terpstra** pour sa contribution qui a permis de boucler ce chapitre.

Un nouveau chapitre sur SELinux

Le nouveau chapitre sur *SELinux* examine différents fichiers et des options de configurations variées pour SELinux. Il convient de remercier ici tout particulièrement **Karsten Wade** pour sa contribution qui a permis de boucler ce chapitre.

Mise à jour du chapitre Système de fichiers `proc`

Le chapitre sur le système de fichiers `proc` inclut des informations mises à jour par rapport au noyau 2.6. Il convient de remercier ici tout particulièrement **Arjan van de Ven** pour sa contribution qui a permis de boucler ce chapitre.

Mise à jour du chapitre Système de fichiers réseau (NFS)

Le chapitre *Système de fichiers réseau (NFS)* a été révisé et réorganisé afin d'inclure NFSv4.

Mise à jour du chapitre Système X Window

Le chapitre *Système X Window* a été révisé afin d'inclure des informations sur la version X11R6.8 développée par l'équipe X.Org.

Avant d'entamer la lecture de ce guide, vous devriez connaître le contenu du *Guide d'installation de Red Hat Enterprise Linux* en ce qui concerne les problèmes d'installation, celui du manuel intitulé *Introduction à l'administration système de Red Hat Enterprise Linux* par rapport aux concepts d'administration de base, celui du *Guide d'administration système de Red Hat Enterprise Linux* en matière d'instructions générales de personnalisation et finalement celui du *Guide de sécurité de Red*

Hat Enterprise Linux pour ce qui est des instructions associées à la sécurité. Le présent guide contient des informations sur des sujets d'intérêt pour les utilisateurs expérimentés.

Les versions HTML, PDF et RPM des manuels sont disponibles sur le CD-ROM de documentation de Red Hat Enterprise Linux et en ligne à l'adresse suivante : http://www.redhat.com/docs/.

Remarque

Bien que ce manuel reflète les informations les plus courantes possibles, il est recommandé de lire les *notes de mise à jour de Red Hat Enterprise Linux* afin d'obtenir des informations qui n'étaient pas disponibles avant la version finale de notre documentation. Ces dernières se trouvent sur le CD-ROM #1 de Red Hat Enterprise Linux et en ligne à l'adresse suivante : http://www.redhat.com/docs/.

2. Informations spécifiques aux architectures

À moins que cela ne soit indiqué différemment, toutes les informations contenues dans ce manuel s'appliquent uniquement au processeur x86 et aux processeurs comprenant les technologies Intel® Extended Memory 64 Technology (Intel® EM64T) et AMD64. Afin d'obtenir des informations spécifiques aux architectures, reportez-vous au *Guide d'installation de Red Hat Enterprise Linux* correspondant à votre architecture.

3. Documentation appropriée à vos besoins

Il est essentiel que vous disposiez d'une documentation appropriée à votre niveau de maîtrise de Linux. En effet, dans le cas contraire, vous vous sentirez peut-être dépassé par le contenu ou vous ne pourrez pas trouver les informations nécessaires pour répondre à vos questions. Le *Guide de référence de Red Hat Enterprise Linux* traite des aspects et des options les plus techniques de votre système Red Hat Enterprise Linux. Cette section vous aidera à décider si ce manuel est la source d'informations dont vous avez besoin ou si au contraire vous devriez consulter d'autres guides Red Hat Enterprise Linux, y compris les ressources disponibles en ligne.

Passons en revue les trois catégories d'utilisateurs de Red Hat Enterprise Linux et déterminons la documentation et les sources d'informations dont ils ont besoin. Commençons par déterminer votre niveau d'expérience. Ci-dessous figurent trois catégories de base :

Débutant

Ce type d'utilisateur n'a jamais, ou presque jamais, utilisé un système d'exploitation Linux (ou analogue). Il peut éventuellement avoir déjà utilisé d'autres systèmes d'exploitation (tels que Windows). Est-ce votre cas ? Si oui, passez directement à la Section 3.1.

Expérimenté

Ce type d'utilisateur a déjà installé et utilisé Linux (mais pas Red Hat Enterprise Linux) avec succès auparavant, ou dispose d'une expérience équivalente avec d'autres systèmes d'exploitation de type Linux. Est-ce votre cas ? Si oui, reportez-vous à la Section 3.2.

Chevronné

Ce type d'utilisateur a déjà installé et utilisé Red Hat Enterprise Linux avec succès précédemment. Est-ce votre cas ? Si oui, reportez-vous à la Section 3.3.

3.1. Documentation pour les débutants

Pour un nouveau-venu au monde de Linux, 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 impressionnante. Ces informations permettent d'acquérir de solides bases sur le fonctionnement de Linux, avant d'approfondir des sujets plus avancés.

Commencez par vous procurer la documentation adéquate. Nous ne soulignerons jamais assez l'importance de cette étape. En effet, sans documentation vous ne pourrez qu'être frustré en raison de votre incapacité à faire fonctionner le système Red Hat Enterprise Linux comme vous le souhaiteriez.

Ci-après figure une liste du type de documentation Linux que vous devriez avoir sous la main :

- *Bref historique de Linux* — De nombreux aspects de Linux sont le fruit de précédents historiques. La culture Linux repose également sur des événements, besoins et demandes du passé. Ainsi, une compréhension élémentaire de l'histoire de Linux vous aidera à trouver comment résoudre de nombreux problèmes potentiels avant même d'y être confronté.
- *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)* — Ce document est probablement l'élément le plus important de 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 un grand nombre de commandes volumineuses (et complexes) qui font tout le travail. Si vous ne disposez pas d'exemples illustrant cette approche de Linux, vous risquez d'être effrayé rien que par le nombre de commandes disponibles sur votre système Red Hat Enterprise Linux.

  Souvenez-vous qu'il n'est pas nécessaire de mémoriser toutes les commandes Linux qui existent. Différentes techniques permettent de trouver la commande précise dont vous avez besoin 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 exactes pour exécuter la commande.

Le *Guide d'installation de Red Hat Enterprise Linux* et le *Guide étape par étape de Red Hat Enterprise Linux* constituent d'excellentes références qui vous aideront à réaliser avec succès l'installation et la configuration initiale d'un système Red Hat Enterprise Linux. Le manuel *Introduction à l'administration système de Red Hat Enterprise Linux* est un excellent point de départ pour ceux qui souhaitent apprendre les principes de base de l'administration système. Nous vous conseillons de commencer par ces livres afin d'acquérir la base de vos connaissances sur Red Hat Enterprise Linux. Il ne vous faudra pas beaucoup de temps avant que des concepts plus compliqués ne deviennent très clairs, car vous aurez compris les idées générales de Linux.

Outre les manuels Red Hat Enterprise Linux, d'autres sources de documentation sont disponibles à un prix modique voire gratuitement. Parmi celles-ci figurent les ressources metionnées ci-après.

3.1.1. Sites Web de Linux — Introduction

- http://www.redhat.com/ — Sur 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 Enterprise Linux, le Forum Aux Questions (FAQ), 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 la base de données de connaissances pour l'assistance (Red Hat Support Knowledge Base), etc.
- http://www.linuxheadquarters.com/ — Le site Web du siège social de Linux contient de nombreux guides 'étape par étape' d'une utilisation facile qui examinent différents outils de Linux.

3.1.2. Groupes de discussion Linux — Introduction

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 expérimentés de Linux sont bien connus pour l'aide qu'ils apportent aux débutants afin de leur permettre de comprendre Linux — en particulier si les questions sont bien formulées et adressées au forum approprié. Si vous n'avez pas accès à une application qui permet de faire partie de ces groupes, vous pouvez accéder aux informations sur le Web à l'adresse suivante : http://groups.google.com/. Il existe des dizaines de groupes de discussion concernant Linux, dont :

- 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 spécifiques à Red Hat Enterprise Linux.
- linux.redhat.install — Un endroit idéal pour poser vos questions concernant l'installation ou voir comment d'autres personnes résolvent des problèmes similaires aux vôtres.
- linux.redhat.misc — Un bon forum où poser des questions ou demander de l'aide sur des sujets peu traditionnels.
- linux.redhat.rpm — Une bonne adresse si vous n'arrivez pas à atteindre des objectifs particuliers avec **RPM**.

3.2. Documentation 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 d'administration système de Red Hat Enterprise Linux* est conçu pour expliquer les différentes configurations du système Red Hat Enterprise Linux afin de pouvoir choisir celle répondant le mieux à vos objectifs. Ce guide vous permettra d'acquérir des connaissances sur des options de configuration spécifiques et vous expliquera comment les appliquer.

Lorsque vous installez des logiciels qui ne figurent pas dans le *Guide d'administration système de Red Hat Enterprise 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 suivante : http://www.redhat.com/mirrors/LDP/HOWTO/HOWTO-INDEX/howtos.html, traitent des aspects particuliers de Linux allant des modifications ésotériques du noyau de bas niveau à l'utilisation de Linux pour des stations de radioamateurs.

Si vous vous posez des questions sur des points plus précis et sur des aspects spécifiques du système Red Hat Enterprise Linux, le *Guide de référence de Red Hat Enterprise Linux* représente une excellente source d'informations.

Si vous êtes préoccupé par la sécurité, le *Guide de sécurité de Red Hat Enterprise Linux* représente une excellente ressource — expliquant les meilleures stratégies et pratiques pour sécuriser Red Hat Enterprise Linux.

3.3. Documentation pour les utilisateurs chevronnés

Si vous vous posez des questions sur des points plus précis et sur des aspects spécifiques du système Red Hat Enterprise Linux, le *Guide de référence de Red Hat Enterprise Linux* représente une excellente source d'informations.

Si vous utilisez Red Hat Enterprise Linux depuis longtemps, vous savez probablement que le meilleur moyen de comprendre un programme consiste à lire son code source et/ou ses fichiers de configura-

tion. L'un des principaux avantages de Red Hat Enterprise Linux est que le code source est toujours disponible.

Évidemment, comme nous ne sommes pas tous des programmeurs, le code source ne sera pas forcément d'une grande aide. Toutefois, si vous avez les connaissances et les aptitudes nécessaires pour le comprendre, le code source peut répondre à toutes vos interrogations.

4. Conventions de documentation

En lisant ce manuel, vous verrez que certains mots sont représentés avec des polices différentes au niveau du type, de la taille et de l'utilisation de caractères gras. Cette présentation est systématique ; différents mots sont représentés dans le même style pour indiquer leur appartenance à une certaine catégorie. Parmi les types de mots représentés de cette façon figurent :

`commande`

Les commandes de Linux (et les commandes d'autres systèmes d'exploitation, lorsqu'elles sont utilisées) sont représentées de cette façon. Ce style vous indique que vous pouvez saisir le mot ou l'expression sur la ligne de commande et appuyer sur [Entrée] pour invoquer une commande. Une commande contient parfois des mots qui, individuellement, seraient représentés différemment (comme les noms de fichiers). Dans ces cas précis, ils sont considérés comme une partie de la commande ; toute la phrase sera donc affichée comme une commande. Par exemple :

Utilisez la commande `cat testfile` pour afficher le contenu d'un fichier nommé `testfile`, dans le répertoire de travail courant.

`nom de fichier`

Les noms de fichiers, de répertoires, les chemins d'accès et les noms de paquetages RPM sont représentés de cette façon. Ce style devrait indiquer qu'un fichier ou un répertoire de ce nom existe dans votre système. Par exemple :

Le fichier `.bashrc` dans votre répertoire personnel contient des définitions et alias de shell bash pour votre utilisation personnelle.

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

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

application

Ce style indique que le programme est une application d'utilisateur final (par opposition aux logiciels de système). Par exemple :

Utilisez **Mozilla** pour parcourir le Web.

[touche]

Une touche du clavier est représentée de cette façon. Par exemple :

Pour utiliser la fonctionnalité d'achèvement [Tab], saisissez un caractère, puis appuyez sur la touche [Tab]. Votre terminal affichera la liste des fichiers du répertoire qui commencent avec cette lettre.

[combinaison]-[touche]

Une combinaison de touches est représentée de cette façon. Par exemple :

La combinaison [Ctrl]-[Alt]-[Retour arrière] vous déconnecte de votre session graphique et revient sur l'écran de connexion graphique ou la console.

texte trouvé sur une interface GUI

Un titre, un mot ou une phrase figurant sur l'écran ou dans la fenêtre d'une interface GUI est représenté de cette façon. Lorsque vous voyez du texte dans ce style, il est utilisé pour identifier un écran GUI ou un élément sur un écran GUI particulier (comme du texte associé avec une case à cocher ou un champ de saisie). Par exemple :

Cochez la case **Nécessite un mot de passe** si vous voulez que votre écran de veille demande un mot de passe avant de s'arrêter.

premier niveau d'un menu sur un écran ou une fenêtre GUI

Ce style vous indique que le mot représente le premier élément d'un menu déroulant. Cliquez sur le mot de l'écran GUI pour afficher le reste du menu. Par exemple :

Sous **Fichier** d'un terminal GNOME, vous trouverez l'option **Nouvel onglet** vous permettant d'ouvrir plusieurs invites du shell dans la même fenêtre.

Si vous devez saisir une séquence de commandes depuis un menu GUI, ces dernières apparaîtront de la façon suivante :

Cliquez sur **Menu principal** (sur le tableau de bord) => **Programmation** => **Emacs** pour lancer l'éditeur de texte **Emacs**.

bouton dans un écran ou une fenêtre GUI

Ce style indique que le texte se trouve sur un bouton à cliquer dans un écran GUI. Par exemple :

Cliquez sur le bouton **Précédent** pour revenir à la dernière page Web que vous avez affichée.

`sortie d'ordinateur`

Ce style indique du texte affiché dans une invite du shell tel que des messages d'erreur et des réponses de commandes. Par exemple :

Utilisez la commande `ls` pour afficher le contenu d'un répertoire. Par exemple :

```
Desktop                about.html       logs          paulwesterberg.png
Mail                   backupfiles      mail          reports
```

La sortie produite en réponse à cette commande (dans ce cas, le contenu du répertoire) est affichée de cette façon.

`invite`

L'invite est la façon utilisée par l'ordinateur pour vous indiquer qu'il est prêt à recevoir votre saisie. Elle est représentée comme ci-dessous. Par exemple :

```
$

#

[stephen@maturin stephen]$

leopard login:
```

`saisie de l'utilisateur`

Le texte que l'utilisateur doit saisir, que ce soit en ligne de commande ou dans une zone de texte dans un écran GUI, est affiché de cette façon. Dans l'exemple ci-dessous, **`text`** est affiché de la manière suivante :

Vous devez saisir la commande **`text`** à l'invite `boot:` pour démarrer votre système dans le programme d'installation en mode texte.

remplaçable

Le texte utilisé pour les exemples et qui doit être remplacé par des données saisies par l'utilisateur est affiché de cette façon. Dans l'exemple ci-dessous, <*version-number*> est affiché de la manière suivante :

Le répertoire de la source du noyau est `/usr/src/`<*version-number*>`/`, où <*version-number*> représente la version du noyau installée sur ce système.

De plus, nous utilisons différentes stratégies pour attirer votre attention sur certaines informations. Suivant l'importance de l'information pour votre système, ces éléments seront présentés sous forme de symbole indiquant une remarque, une astuce, un point important, un message d'attention ou un avertissement. Par exemple :

Remarque

N'oubliez pas que Linux est sensible à la casse. Autrement dit, rose n'est ni ROSE ni rOsE.

Astuce

Le répertoire `/usr/share/doc` contient de la documentation supplémentaire pour les paquetages installés sur votre système.

Important

Si vous modifiez le fichier de configuration de DHCP, les changements ne prendront pas effet tant que vous n'aurez pas redémarré le démon DHCP.

Attention

N'effectuez pas de tâches quotidiennes en tant que root — utilisez un compte utilisateur ordinaire à moins que vous n'ayez besoin d'utiliser le compte super-utilisateur pour des tâches d'administration système.

Avertissement

Faites attention à ne supprimer que les partitions Red Hat Enterprise Linux nécessaires. La suppression d'autres partitions pourrait provoquer la perte de données ou la corruption d'un environnement système.

5. Activation de votre abonnement

Avant de pouvoir accéder aussi bien aux informations relatives à la maintenance des logiciels et des services qu'à la documentation d'assistance faisant partie de votre abonnement, vous devez activer ce dernier en vous enregistrant avec Red Hat. Pour ce faire, suivez les étapes suivantes :

- Saisie d'un nom de connexion Red Hat
- Saisie d'un numéro d'abonnement
- Connexion de votre système

Lors du premier démarrage de votre installation de Red Hat Enterprise Linux, vous serez invité à vous enregistrer avec Red Hat à l'aide de l'**Agent de paramétrage**. En suivant les invites fournies par l'**Agent de paramétrage**, vous pouvez accomplir les étapes nécessaires pour vous enregistrer et activer votre abonnement.

Dans le cas où vous ne parviendriez pas à effectuer votre enregistrement avec l'**Agent de paramétrage** (qui demande un accès au réseau), vous pouvez vous rendre à l'adresse suivante : http://www.redhat.com/register/ et vous enregistrer en ligne avec Red Hat.

5.1. Saisie d'un nom de connexion Red Hat

Si vous n'avez pas de nom de connexion Red Hat (login), vous pouvez en créer un lorsque l'**Agent de paramétrage** vous le demande ou vous pouvez le faire en ligne à l'adresse suivante :

```
https://www.redhat.com/apps/activate/newlogin.html
```

Un nom de connexion Red Hat vous permet d'accéder aux éléments suivants :

- Mises à jour de logiciels, errata et maintenance via Red Hat Network
- Ressources d'assistance technique, documentation et base de connaissances de Red Hat

Si vous avez oublié votre nom de connexion Red Hat, vous pouvez le rechercher en ligne à l'adresse suivante :

```
https://rhn.redhat.com/help/forgot_password.pxt
```

5.2. Saisie d'un numéro d'abonnement

Votre numéro d'abonnement est situé dans le paquetage fourni avec votre commande. S'il ne contient pas de numéro d'abonnement, ce dernier a déjà été activé pour vous et vous pouvez sauter cette étape.

Vous pouvez donner votre numéro d'abonnement lorsque l'**Agent de paramétrage** vous le demande ou vous pouvez le fournir à l'adresse suivante : http://www.redhat.com/register/.

5.3. Connexion de votre système

Le client d'enregistrement Red Hat Network vous aide à connecter votre système afin que vous soyez en mesure d'obtenir des mises à jour et de gérer vos systèmes. Vous pouvez vous connecter de trois manières :

1. Avec l'**Agent de paramétrage** — Cochez les options **Send hardware information** (envoyer les informations matérielles) et **Send system package list** (envoyer la liste des paquetages du système) lorsqu'elles apparaissent.

2. Une fois que l'**Agent de paramétrage** a fini son travail — Depuis le **menu principal**, sélectionnez **Outils de système**, puis **Red Hat Network**.
3. Une fois que l'**Agent de paramétrage** a fini son travail — Saisissez la commande suivante sur la ligne de commande en étant connecté en tant que super-utilisateur :
   - `/usr/bin/up2date --register`

6. Utilisation de la souris

Red Hat Enterprise Linux utilise habituellement une souris à trois boutons. Si vous avez une souris à deux boutons, vous devriez avoir sélectionné l'émulation de souris à trois boutons durant le processus d'installation. Si vous utilisez l'émulation de souris à trois boutons, cliquer simultanément sur les deux boutons revient à cliquer sur le bouton central (que vous n'avez pas).

Dans ce document, si le système vous demande de cliquer à un endroit, il est entendu qu'il s'agit du bouton gauche. Si vous devez utiliser le bouton central ou celui de droite, cela vous sera précisé. (Si vous avez configuré votre souris pour un gaucher, inversez ces instructions.)

L'expression « glisser et poser » (ou déplacement par glissement) vous est peut-être familière. Si vous devez glisser et poser un élément sur votre bureau d'interface graphique, cliquez sur cet élément et maintenez le bouton de la souris appuyé. Glissez ensuite l'élément, tout en maintenant la touche appuyée, vers son nouvel emplacement. Relâchez ensuite le bouton et posez l'élément.

7. Fonction « Copier-coller » avec X

Il est facile de copier et coller du texte à l'aide de votre souris et du système X Window. Pour copier du texte, il vous suffit de cliquer et glisser votre souris sur le texte pour le mettre en surbrillance. Pour coller du texte, il suffit de cliquer avec le bouton central de la souris à l'endroit où vous souhaitez le placer.

8. Prochainement

Le *Guide de référence de Red Hat Enterprise Linux* fait partie de l'engagement de Red Hat à fournir une assistance utile et opportune aux utilisateurs de Red Hat Enterprise Linux. Les prochaines éditions contiendront 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 Red Hat Enterprise Linux — ainsi que vos capacités à l'exploiter au maximum de ses possibilités.

Pour nous permettre de remplir notre engagement, votre contribution est importante.

8.1. Faites-nous part de vos commentaires !

Si vous trouvez une erreur, une faute de frappe dans le *Guide de référence de Red Hat Enterprise Linux* ou si vous avez songé à une manière d'améliorer ce manuel, faites-nous part de vos commentaires. Soumettez un rapport par l'entremise de Bugzilla (http://bugzilla.redhat.com/bugzilla) dans la catégorie *rhel-rg*.

N'oubliez pas de mentionner la référence du manuel :

```
rhel-rg(FR)-4-Impression-RHI (2004-09-30T17:13)
```

Nous pourrons ainsi connaître la version du guide à laquelle vous faites référence.

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

I. Références pour le système

Pour gérer un système efficacement, vous devez absolument connaître ses composants et leur agencement. Cette section présente des aspects importants du système. Elle examine le processus de démarrage, la structure de base des systèmes de fichiers, l'emplacement des systèmes de fichiers et des fichiers systèmes essentiels et les concepts de base expliquant les notions d'utilisateurs et de groupes. De plus, le système X Window est expliqué en détail.

Table des matières

Chapitre 1.

Processus de démarrage, Init et arrêt

Un des aspects importants et performants de Red Hat Enterprise Linux est la méthode flexible et pouvant être configurée par l'utilisateur qui est employée pour le démarrage du système d'exploitation. Les utilisateurs peuvent configurer librement de nombreux aspects du processus de démarrage, y compris la possibilité de spécifier les programmes lancés au démarrage. De même, l'arrêt du système met fin nettement aux processus et ce, de manière organisée et configurable ; bien que la personnalisation de ce processus ne soit que rarement nécessaire.

La compréhension des processus de démarrage et d'arrêt vous permettra non seulement de personnaliser, mais également de résoudre plus rapidement les problèmes liés au démarrage ou à l'arrêt de votre système.

1.1. Processus de démarrage

Vous trouverez ci-dessous les étapes de base du processus de démarrage d'un système x86 :

1. Le BIOS du système examine le système et lance le chargeur de démarrage de l'Étape 1 sur le bloc de démarrage maître (MBR) du disque dur principal.
2. Le chargeur de démarrage de l'Étape 1 se charge en mémoire et lance le chargeur de démarrage de l'Étape 2 à partir de la partition `/boot/`.
3. Le chargeur de démarrage de l'Étape 2 charge en mémoire le noyau qui à son tour charge tous les modules nécessaires et monte la partition root en lecture-seule.
4. Le noyau passe le contrôle du processus de démarrage au programme `/sbin/init`.
5. Le programme `/sbin/init` charge tous les services et les outils de l'espace utilisateur et monte toutes les partitions répertoriées dans `/etc/fstab`.
6. L'utilisateur voit alors s'afficher un écran de connexion pour le système Linux qui vient d'être démarré.

Étant donné que la configuration du processus de démarrage est plus courante que la personnalisation du processus d'arrêt, le reste de ce chapitre examinera en détail le fonctionnement du processus de démarrage et vous expliquera comment l'adapter à vos besoins spécifiques.

1.2. Examen détaillé du processus de démarrage

Le début du processus de démarrage varie en fonction de la plate-forme matérielle utilisée. Toutefois, une fois le noyau trouvé et chargé par le chargeur de démarrage, le processus de démarrage par défaut est identique pour toutes les architectures. Ce chapitre se concentre principalement sur l'architecture x86.

1.2.1. Le BIOS

Lors du démarrage d'un ordinateur x86, le processeur recherche le programme *BIOS* (de l'anglais *Basic Input/Output System*) dans la mémoire morte (ROM) de la carte mère et l'exécute. Le BIOS est le plus bas niveau d'interface pour les périphériques et contrôle la première étape du processus de démarrage. C'est la raison pour laquelle le BIOS est enregistré en lecture-seule dans la mémoire morte et peut ainsi être utilisé à tout moment.

D'autres plates-formes utilisent différents programmes pour réaliser des tâches de bas niveau plus ou moins équivalentes à celles effectuées par le BIOS sur un système x86. Par exemple, les ordinateurs basés sur Itanium utilisent le *Shell EFI* (de l'anglais *Extensible Firmware Interface*).

Une fois chargé, le BIOS teste le système, recherche et vérifie les périphériques et trouve ensuite un périphérique valide qui sera utilisé pour amorcer le système. Normalement, il vérifie d'abord les lecteurs de disquettes et les lecteurs CD-ROM présents afin de trouver un support amorçable ; s'il n'en trouve aucun, il cherche sur les disques durs du système. Dans la plupart des cas, l'ordre des unités recherchées lors du démarrage peut être contrôlé par un paramètre du BIOS ; il cherche sur le périphérique IDE maître sur le bus IDE principal. Le BIOS charge ensuite en mémoire tout programme résidant sur le premier secteur de ce périphérique appelé bloc de démarrage maître ou *MBR*(de l'anglais *Master Boot Record*). Le MBR a une taille de 512 octets seulement et contient des instructions de codes machine, appelée chargeur de démarrage, qui sont nécessaires pour démarrer l'ordinateur ainsi que la table des partitions. Une fois que le BIOS trouve et charge en mémoire le programme du chargeur de démarrage, il lui cède le contrôle du processus de démarrage.

1.2.2. Le chargeur de démarrage

Cette section examine le chargeur de démarrage par défaut pour la plate-forme x86, à savoir GRUB. Selon l'architecture du système, le processus de démarrage peut varier légèrement. Reportez-vous à la Section 1.2.2.1 pour obtenir un bref aperçu des chargeurs de démarrage autres que ceux utilisés pour x86. Pour obtenir de plus amples informations sur la configuration et l'utilisation de GRUB, consultez le Chapitre 2.

Un chargeur de démarrage pour la plate-forme x86 fonctionne au minimum en deux étapes. La première est un petit binaire de code machine sur le MBR. Son seul rôle est de localiser le chargeur de démarrage pour l'Étape 2 et d'en charger la première partie en mémoire.

GRUB a l'avantage de pouvoir lire les partitions ext2 et ext3[1] et de charger son fichier de configuration — `/boot/grub/grub.conf`— au moment du démarrage. Pour obtenir de plus amples informations sur la façon de modifier ce fichier, reportez-vous à la Section 2.7.

Astuce

Si vous mettez à niveau le noyau en utilisant l'application **Agent de mise à jour Red Hat**, le fichier de configuration du chargeur de démarrage sera mis à jour automatiquement. De plus amples informations sur Red Hat Network se trouvent en ligne à l'adresse suivante : https://rhn.redhat.com/.

Une fois que le chargeur de démarrage Étape 2 est en mémoire, il affiche l'écran graphique indiquant à l'utilisateur les différents systèmes d'exploitation ou noyaux qu'il doit charger en fonction de sa configuration. Sur cet écran, l'utilisateur peut, à l'aide des touches fléchées, choisir le système d'exploitation ou le noyau qu'il souhaite charger et valider ce choix en appuyant sur la touche [Entrée]. Si l'utilisateur n'appuie sur aucune touche avant qu'un certain laps de temps - configurable - ne se soit écoulé, le chargeur de démarrage chargera la sélection par défaut.

Remarque

Si la prise en charge par le noyau de Symmetric Multi-Processor (SMP) est installée, plusieurs options seront proposées lors du premier démarrage de votre système. Dans une telle situation,

1. GRUB lit les systèmes de fichiers ext3 en tant que ext2, en abandonnant le fichier journal. Reportez-vous au chapitre intitulé *Le système de fichiers ext3* du *Guide d'administration système de Red Hat Enterprise Linux* pour de plus amples informations sur le système de fichiers ext3.

GRUB affiche `Red Hat Enterprise Linux (<kernel-version>-smp)`, qui est le noyau SMP et `Red Hat Enterprise Linux (<kernel-version>)`, qui est pour des processeurs simples (où *<kernel-version>* correspond à la version du noyau).

Si vous rencontrez des problèmes en utilisant le noyau SMP, sélectionnez le noyau non-SMP au redémarrage.

Une fois que le chargeur de démarrage Étape 2 a déterminé le noyau à lancer, il localise le binaire de noyau correspondant dans le répertoire `/boot/`. Le binaire du noyau est baptisé d'après le format—fichier `/boot/vmlinuz-`*<kernel-version>* (où *<kernel-version>* correspond à la version du noyau spécifiée dans les paramètres du chargeur de démarrage).

Pour obtenir des instructions sur la manière d'utiliser le chargeur de démarrage pour transmettre au noyau des arguments en ligne de commande, reportez-vous au Chapitre 2. Pour des informations sur la manière de changer le niveau d'exécution à l'invite du chargeur de démarrage, reportez-vous à la Section 2.8.

Le chargeur de démarrage place alors plusieurs images *initramfs* appropriées (ou une seule) en mémoire. Ensuite, par l'intermédiaire de `cpio`, le noyau décompresse ces images présentes dans la mémoire et les met sur `/boot/`, un système de fichiers virtuel basé sur la RAM. Les images `initramfs` sont utilisées par le noyau pour charger les pilotes et modules nécessaires au démarrage du système. Ce processus s'avère particulièrement important si votre système dispose de disques durs SCSI ou s'il utilise le système de fichiers ext3.

Une fois que le noyau et une ou plusieurs images `initramfs` sont chargées en mémoire, le chargeur de démarrage cède le contrôle du processus de démarrage au noyau.

Pour obtenir une présentation plus détaillé du chargeur de démarrage GRUB, reportez-vous au Chapitre 2.

1.2.2.1. Chargeurs de démarrage pour d'autres architectures

Une fois que le noyau se charge et qu'il passe les commandes à `init`, les mêmes événements se produisent sur toutes les architectures. La différence essentielle entre le processus de démarrage de chaque architecture réside dans le choix de l'application utilisée pour trouver et charger le noyau.

Par exemple, l'architecture Itanium utilise le chargeur de démarrage ELILO, l'architecture eServer pSeries d'IBM utilise YABOOT et les systèmes IBM s390 et eServer zSeries utilisent le chargeur de démarrage z/IPL.

Consultez le *Guide d'installation de Red Hat Enterprise Linux* spécifique à ces plates-formes pour obtenir de plus amples informations sur la manière de configurer leurs chargeurs de démarrage.

1.2.3. Le noyau

Lors du chargement du noyau, ce dernier non seulement initialise et configure immédiatement la mémoire de l'ordinateur, mais il configure également les divers composants matériels reliés au système, y compris tous les processeurs, les sous-systèmes d'E/S ainsi que les périphériques de stockage. Il recherche ensuite la ou les image(s) `initrd` compressée(s) dans un emplacement prédéterminé de la mémoire, effectue la décompression directement sur `/sysroot/` et finalement charge tous les pilotes nécessaires. Ensuite, il initialise les dispositifs virtuels associés aux systèmes de fichiers, tels que LVM ou RAID logiciel, avant d'achever les processus `initramfs` et de libérer toute la mémoire que l'image du disque occupait.

Le noyau crée alors un dispositif root, monte la partition root en lecture-seule et libère la mémoire non-utilisée.

À ce stade, le noyau est chargé en mémoire et est désormais opérationnel. Toutefois, en l'absence de toute application offrant à l'utilisateur la possibilité de donner des informations utiles au système, on ne peut pas faire grand chose avec ce système.

Afin de configurer l'environnement utilisateur, le noyau exécute le progamme `/sbin/init`.

1.2.4. Le programme `/sbin/init`

Le programme `/sbin/init` (aussi appelé `init`) coordonne le reste du processus de démarrage et configure l'environnement de l'utilisateur.

Lorsque la commande `init` est lancée, elle devient le parent ou grand-parent de tous les processus qui sont lancés automatiquement sur le système. Tout d'abord, elle exécute le script `/etc/rc.d/rc.sysinit` qui définit le chemin d'accès de l'environnement, démarre swap, contrôle les systèmes de fichiers et exécute toutes les autres étapes nécessaires à l'initialisation du système. Par exemple, la plupart des systèmes utilisant une horloge, `rc.sysinit` lit le fichier de configuration `/etc/sysconfig/clock` pour initialiser l'horloge matérielle. Autre exemple : s'il existe des processus de port série spéciaux qui doivent être initialisés, `rc.sysinit` exécute le fichier `/etc/rc.serial`.

Ensuite la commande `init` exécute le script `/etc/inittab` qui décrit la manière selon laquelle le système devrait être configuré à chaque niveau d'exécution, *SysV init runlevel*. Les niveaux d'exécution sont des états ou *modes* définis par les services énumérés dans le répertoires `/etc/rc.d/rc<x>.d/` de SysV, où *<x>* correspond au numéro du niveau d'exécution. Pour obtenir de plus amples informations sur les niveaux d'exécution (ou SysV init runlevels), reportez-vous à la Section 1.4.

Ensuite, la commande `init` configure la bibliothèque de fonctions sources, `/etc/rc.d/init.d/functions`, pour le système. Celle-ci indique comment démarrer ou arrêter un programme et comment déterminer le PID d'un programme.

Le programme `init` démarre l'ensemble des processus d'arrière-plan en consultant le répertoire `rc` approprié au niveau d'exécution spécifié comme valeur par défaut dans `/etc/inittab`. Les répertoires `rc` sont numérotés de façon à correspondre au niveau d'exécution qu'ils représentent. Par exemple, `/etc/rc.d/rc5.d/` est le répertoire correspondant au niveau d'exécution 5.

En démarrant au niveau d'exécution 5, le programme `init` examine le répertoire `/etc/rc.d/rc5.d/` afin de déterminer les processus à arrêter et à démarrer.

Ci-dessous figure un exemple de listing pour un répertoire `/etc/rc.d/rc5.d/` :

```
K05innd -> ../init.d/innd
K05saslauthd -> ../init.d/saslauthd
K10dc_server -> ../init.d/dc_server
K10psacct -> ../init.d/psacct
K10radiusd -> ../init.d/radiusd
K12dc_client -> ../init.d/dc_client
K12FreeWnn -> ../init.d/FreeWnn
K12mailman -> ../init.d/mailman
K12mysqld -> ../init.d/mysqld
K15httpd -> ../init.d/httpd
K20netdump-server -> ../init.d/netdump-server
K20rstatd -> ../init.d/rstatd
K20rusersd -> ../init.d/rusersd
K20rwhod -> ../init.d/rwhod
K24irda -> ../init.d/irda
K25squid -> ../init.d/squid
K28amd -> ../init.d/amd
K30spamassassin -> ../init.d/spamassassin
K34dhcrelay -> ../init.d/dhcrelay
```

```
K34yppasswdd -> ../init.d/yppasswdd
K35dhcpd -> ../init.d/dhcpd
K35smb -> ../init.d/smb
K35vncserver -> ../init.d/vncserver
K36lisa -> ../init.d/lisa
K45arpwatch -> ../init.d/arpwatch
K45named -> ../init.d/named
K46radvd -> ../init.d/radvd
K50netdump -> ../init.d/netdump
K50snmpd -> ../init.d/snmpd
K50snmptrapd -> ../init.d/snmptrapd
K50tux -> ../init.d/tux
K50vsftpd -> ../init.d/vsftpd
K54dovecot -> ../init.d/dovecot
K61ldap -> ../init.d/ldap
K65kadmin -> ../init.d/kadmin
K65kprop -> ../init.d/kprop
K65krb524 -> ../init.d/krb524
K65krb5kdc -> ../init.d/krb5kdc
K70aep1000 -> ../init.d/aep1000
K70bcm5820 -> ../init.d/bcm5820
K74ypserv -> ../init.d/ypserv
K74ypxfrd -> ../init.d/ypxfrd
K85mdmpd -> ../init.d/mdmpd
K89netplugd -> ../init.d/netplugd
K99microcode_ctl -> ../init.d/microcode_ctl
S04readahead_early -> ../init.d/readahead_early
S05kudzu -> ../init.d/kudzu
S06cpuspeed -> ../init.d/cpuspeed
S08ip6tables -> ../init.d/ip6tables
S08iptables -> ../init.d/iptables
S09isdn -> ../init.d/isdn
S10network -> ../init.d/network
S12syslog -> ../init.d/syslog
S13irqbalance -> ../init.d/irqbalance
S13portmap -> ../init.d/portmap
S15mdmonitor -> ../init.d/mdmonitor
S15zebra -> ../init.d/zebra
S16bgpd -> ../init.d/bgpd
S16ospf6d -> ../init.d/ospf6d
S16ospfd -> ../init.d/ospfd
S16ripd -> ../init.d/ripd
S16ripngd -> ../init.d/ripngd
S20random -> ../init.d/random
S24pcmcia -> ../init.d/pcmcia
S25netfs -> ../init.d/netfs
S26apmd -> ../init.d/apmd
S27ypbind -> ../init.d/ypbind
S28autofs -> ../init.d/autofs
S40smartd -> ../init.d/smartd
S44acpid -> ../init.d/acpid
S54hpoj -> ../init.d/hpoj
S55cups -> ../init.d/cups
S55sshd -> ../init.d/sshd
S56rawdevices -> ../init.d/rawdevices
S56xinetd -> ../init.d/xinetd
S58ntpd -> ../init.d/ntpd
S75postgresql -> ../init.d/postgresql
```

```
S80sendmail -> ../init.d/sendmail
S85gpm -> ../init.d/gpm
S87iiim -> ../init.d/iiim
S90canna -> ../init.d/canna
S90crond -> ../init.d/crond
S90xfs -> ../init.d/xfs
S95atd -> ../init.d/atd
S96readahead -> ../init.d/readahead
S97messagebus -> ../init.d/messagebus
S97rhnsd -> ../init.d/rhnsd
S99local -> ../rc.local
```

Comme le montre ce listing, aucun des scripts qui lancent et arrêtent vraiment les services n'est réellement situé dans le répertoire `/etc/rc.d/rc5.d/`. Tous les fichiers dans `/etc/rc.d/rc5.d/` sont en fait des *liens symboliques* qui pointent vers les scripts situés dans le répertoire `/etc/rc.d/init.d/`. Des liens symboliques sont utilisés dans chacun des répertoires `rc` afin que les niveaux d'exécution puissent être reconfigurés en créant, modifiant et supprimant les liens symboliques, et ce, sans affecter les scripts auxquels ils font référence.

Le nom de chaque lien symbolique commence soit par `K`, soit par `S`. Les liens `K` correspondent à des processus arrêtés à ce niveau d'exécution, tandis que les liens `S` correspondent à des processus démarrés à ce niveau d'exécution.

La commande `init` arrête tout d'abord tous les liens symboliques `K` du répertoire en émettant la commande `/etc/rc.d/init.d/<command> stop`, *<command>* correspondant au processus à arrêter. Elle démarre ensuite tous les liens symboliques `S` en émettant la commande `/etc/rc.d/init.d/<command> start`.

Astuce

Une fois que le système a terminé son démarrage, il est possible d'établir une connexion en tant que super-utilisateur et d'exécuter ces mêmes scripts pour démarrer et arrêter des services. Par exemple, la commande `/etc/rc.d/init.d/httpd stop` arrêtera le Serveur HTTP Apache.

Chacun des liens symboliques est numéroté de façon à établir l'ordre de démarrage. L'ordre dans lequel les services sont démarrés ou arrêtés peut être modifié en changeant ce numéro. Plus le numéro est bas, plus le démarrage se produira tôt. Les liens symboliques disposant du même numéro sont démarrés par ordre alphabétique.

Remarque

Une des dernières choses que le programme `init` exécute est le fichier `/etc/rc.d/rc.local`. Ce dernier est utilisé pour la personnalisation du système. Reportez-vous à la Section 1.3 pour de plus amples informations sur l'utilisation du fichier `rc.local`.

Une fois que la commande `init` a progressé dans le répertoire `rc` approprié pour le niveau d'exécution, le script `/etc/inittab` crée un processus `/sbin/mingetty` pour chaque console virtuelle (invites de connexion) assignée au niveau d'exécution. Les niveaux d'exécution de 2 à 5 ont tous six consoles virtuelles, tandis que le niveau d'exécution 1 (mode mono-utilisateur) n'a lui qu'une seule console virtuelle et que les niveaux d'exécution 0 et 6 n'en ont eux aucune. Le processus `/sbin/mingetty` ouvre des chemins de communication vers les périphériques *tty*[2],

2. Consultez la Section 5.3.11 pour obtenir des informations supplémentaires sur les périphériques `tty`.

définit leurs modes, affiche l'invite de connexion, accepte le nom et le mot de passe de l'utilisateur, puis commence le processus de connexion.

Au niveau d'exécution 5, `/etc/inittab` exécute un script appelé `/etc/X11/prefdm`. Le script `prefdm` exécute le gestionnaire d'affichage X préféré [3] — `gdm`, `kdm` ou `xdm`, en fonction de ce qui est contenu dans le fichier `/etc/sysconfig/desktop`.

Une fois l'ensemble du processus terminé, le système fonctionne à un niveau d'exécution 5 et affiche un écran de connexion.

1.3. Exécution de programmes supplémentaires au démarrage

Le script `/etc/rc.d/rc.local` est exécuté par la commande `init` au démarrage ou lors de la modification des niveaux d'exécution. L'ajout de commandes à la fin de ce script est une façon simple d'exécuter des tâches nécessaires comme le démarrage de services spéciaux ou l'initialisation de périphériques sans devoir écrire des scripts d'initialisation compliqués dans le répertoire `/etc/rc.d/init.d/` et sans devoir créer de liens symboliques.

Le script `/etc/rc.serial` est utilisé si des ports série doivent être configurés au démarrage. Ce script exécute les commandes `setserial` pour la configuration des ports série du système. Consultez les pages de manuel de `setserial` pour obtenir de plus amples informations.

1.4. Niveaux d'exécution de SysV Init

Le système de niveaux d'exécution SysV init fournit un processus standard pour contrôler les programmes lancés et arrêtés par `init` lors de l'initialisation d'un niveau d'exécution. SysV init a été choisi parce qu'il est non seulement plus facile à utiliser et mais également parce que'il est plus flexible que le processus init BSD traditionnel.

Les fichiers de configuration de SysV init se trouvent dans le répertoire `/etc/rc.d/`. Dans ce répertoire, se trouvent les scripts `rc`, `rc.local`, `rc.sysinit` et, de manière optionnelle, les scripts `rc.serial` ainsi que les répertoires suivants :

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

Le répertoire `init.d/` contient les scripts utilisés par la commande `/sbin/init` lors du contrôle des services. Chacun des répertoires numérotés représentent les six niveaux d'exécution configurés par défaut sous Red Hat Enterprise Linux.

1.4.1. Niveaux d'exécution (Runlevels)

L'idée derrière les niveaux d'exécution de SysV init se résume au principe que divers systèmes peuvent être utilisés de différentes manières. Par exemple, un serveur fonctionne plus efficacement lorsqu'il n'est pas dépendant de l'utilisation des ressources du système par le système X Window. En d'autres occasions, il se peut qu'un administrateur système doive faire fonctionner le système à un niveau d'exécution inférieur afin d'effectuer des tâches de diagnostic ; comme par exemple pour résoudre la corruption de disques à un niveau d'exécution 1.

3. Consultez la Section 7.5.2 pour obtenir davantage d'informations sur les gestionnaires d'affichage.

Les caractéristiques d'un niveau d'exécution donné déterminent les services qui seront arrêtés ou démarrés par `init`. Par exemple, le niveau d'exécution 1 (mode mono-utilisateur) arrête tout service réseau alors que le niveau d'exécution 3 lui, démarre ces mêmes services. En déterminant le démarrage ou l'arrêt de services spécifiques à un niveau d'exécution donné, `init` peut rapidement changer le mode de l'ordinateur sans que l'utilisateur n'ait à arrêter ou démarrer ces services manuellement.

Les niveaux d'exécution suivants sont définis par défaut sous Red Hat Enterprise Linux :

- `0` — Arrêt
- `1` — Mode texte mono-utilisateur
- `2` — Pas utilisé
- `3` — Mode texte multi-utilisateurs complet
- `4` — Pas utilisé
- `5` — Mode graphique multi-utilisateurs complet (avec un écran de connexion de type X Window)
- `6` — Redémarrage

En général, les utilisateurs font fonctionner Red Hat Enterprise Linux à un niveau d'exécution 3 ou 5 — les deux niveaux correspondant à des modes multi-utilisateurs complets. Parfois, les utilisateurs personnalisent les niveaux d'exécution 2 et 4 pour leurs besoins spécifiques, puisque ces derniers ne sont pas utilisés.

Le niveau d'exécution par défaut du système se trouve dans `/etc/inittab`. Pour trouver le niveau d'exécution par défaut d'un système, recherchez la ligne semblable à celle reproduite ci-dessous, au début de `/etc/inittab` :

```
id:5:initdefault:
```

Dans l'exemple ci-dessus, le niveau d'exécution par défaut est 5, comme l'indique le chiffre qui suit le premier signes des deux-points (:). Si vous désirez le changer, modifiez `/etc/inittab` en étant connecté en tant que super-utilisateur.

Avertissement

Faites très attention lorsque vous éditez `/etc/inittab`. De simples fautes de frappe peuvent empêcher votre système de démarrer. Si cela se produit, vous devrez utiliser une disquette d'amorçage pour votre système ou passer en mode mono-utilisateur ou en mode de secours pour redémarrer l'ordinateur et réparer le fichier.

Pour plus d'informations sur le mode mono-utilisateur et le mode de secours, reportez-vous au chapitre intitulé *Mode de secours* du *Guide d'administration système de Red Hat Enterprise Linux*.

Il est possible de changer le niveau d'exécution par défaut au moment du démarrage en modifiant les arguments transmis par le chargeur de démarrage au noyau. Pour obtenir des informations sur la manière de modifier le niveau d'exécution au démarrage, reportez-vous à la Section 2.8.

1.4.2. Utilitaires de niveaux d'exécution

Une des meilleures façons de configurer les niveaux d'exécution consiste à utiliser un des *utilitaires initscript*. Ces outils sont conçus pour simplifier le maintien des fichiers dans la hiérarchie du répertoire SysV init et pour éviter aux administrateurs système de manipuler directement les nombreux liens symboliques des sous-répertoires `/etc/rc.d/`.

Red Hat Enterprise Linux offrent trois utilitaires de ce type :

- `/sbin/chkconfig` — L'utilitaire `/sbin/chkconfig` est un simple outil de ligne de commande permettant de maintenir la hiérarchie du répertoire `/etc/rc.d/init.d`.
- **/sbin/ntsysv** — l'utilitaire **/sbin/ntsysv** basé sur ncurses fournit une interface interactive de mode texte, que certains utilisateurs trouvent plus simple à utiliser que `chkconfig`.
- L'**Outil de configuration des services** — Le programme graphique **Outil de configuration des services** (`system-config-services`) est un utilitaire flexible permettant de configurer les niveaux d'exécution.

Veuillez vous reporter au chapitre intitulé *Contrôle de l'accès aux services* du *Guide d'administration système de Red Hat Enterprise Linux* pour obtenir de plus amples informations sur ces outils.

1.5. Arrêt

Pour arrêter Red Hat Enterprise Linux, le super-utilisateur peut exécuter la commande `/sbin/shutdown`. La page de manuel relative à `shutdown` contient une liste complète des options ; ceci étant, les deux options les plus courantes sont les suivantes :

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

Après avoir tout arrêté, l'option `-h` éteindra l'ordinateur et l'option `-r` le redémarrera.

Les utilisateurs de console PAM peuvent utiliser les commandes `reboot` et `halt` pour éteindre l'ordinateur en étant à un niveau d'exécution entre 1 et 5. Pour obtenir davantage d'informations sur les utilisateurs de console PAM, consultez la Section 16.7.

Si l'ordinateur ne s'éteint pas automatiquement, ne le faites pas manuellement avant qu'un message confirmant l'arrêt du système n'apparaisse à l'écran.

Si vous n'attendez pas ce message, il se peut que toutes les partitions du disque dur n'aient pas été complètement démontées, ce qui pourrait entraîner la corruption de systèmes de fichiers.

Chapitre 2.

Chargeur de démarrage GRUB

Lorsqu'un ordinateur avec Red Hat Enterprise Linux est allumé, le système d'exploitation est chargé en mémoire par un programme spécial appelé un *chargeur de démarrage*. Un chargeur de démarrage existe généralement sur le disque dur principal du système (ou sur d'autres supports) et a pour seule responsabilité de charger en mémoire le noyau Linux ainsi que les fichiers dont il a besoin ou (dans certains cas) d'autres systèmes d'exploitation.

2.1. Chargeurs de démarrage et architecture système

Chaque architecture pouvant exécuter Red Hat Enterprise Linux utilise un chargeur de démarrage différent. Le tableau suivant montre les chargeurs de démarrage disponibles pour chaque architecture.

Architecture	Chargeur de démarrage
AMD64 AMD®	GRUB
iSeries™ eServer™ IBM®	OS/400®
pSeries™ eServer™ IBM®	YABOOT
S/390® IBM®	z/IPL
zSeries® eServer™ IBM®	z/IPL
Itanium™ Intel®	ELILO
x86	GRUB

Tableau 2-1. Chargeurs de démarrage par architecture

Ce chapitre examine les commandes et options de configuration du chargeur de démarrage GRUB inclus dans Red Hat Enterprise Linux pour l'architecture x86.

2.2. GRUB

Le *GNU GRand Unified Boot loader* (ou GRUB) est un programme permettant à l'utilisateur de sélectionner le système d'exploitation ou noyau qui doit être chargé au démarrage du système. Il permet également à l'utilisateur de transmettre des arguments au noyau.

2.2.1. GRUB et le processus de démarrage x86

Cette section examine de façon plus détaillée le rôle spécifique que GRUB joue lors du démarrage d'un système x86. Pour obtenir un aperçu du processus de démarrage global, reportez-vous à la Section 1.2.

GRUB se charge en mémoire en suivant les étapes suivantes :

1. *Le chargeur de démarrage Étape 1 (ou primaire) est lu en mémoire par le BIOS à partir du MBR*[1]. Le chargeur de démarrage primaire existe sur moins de 512 octets d'espace disque dans

1. Pour en savoir plus sur le BIOS et le MBR, reportez-vous à la Section 1.2.1.

le MBR et peut charger aussi bien le chargeur de démarrage Étape 1.5 que le chargeur de démarrage Étape 2.

2. *Le chargeur de démarrage Étape 1.5 est lu en mémoire par le chargeur de démarrage Étape 1, si cela est nécessaire.* Selon le matériel, une étape intermédiaire est parfois nécessaire pour arriver au chargeur de démarrage Étape 2. Ceci peut être le cas si la partition `/boot/` se situe au-dessus de la tête de cylindre 1024 du disque dur ou lorsque le mode LBA (Logical Block Addressing) est utilisé. Le chargeur de démarrage Étape 1.5 se trouve sur la partition `/boot/` ou sur une petite portion du MBR et de la partition `/boot/`.
3. *Le chargeur de démarrage Étape 2 (ou secondaire) est lu et stocké en mémoire.* Le chargeur de démarrage secondaire affiche le menu et l'environnement de commandes de GRUB. Cette interface permet à l'utilisateur de sélectionner le système d'exploitation ou le noyau particulier à démarrer, de transmettre des arguments au noyau ou de vérifier des paramètres système.
4. *Le chargeur de démarrage secondaire lit et stocke en mémoire le système d'exploitation ou le noyau ainsi que le contenu de `/boot/sysroot/`.* Une fois que GRUB détermine le système d'exploitation ou noyau spécifique à démarrer, il le charge en mémoire et cède le contrôle de la machine à ce système d'exploitation.

La méthode utilisée pour démarrer Red Hat Enterprise Linux est appelée *chargement direct* car le chargeur de démarrage charge directement le système d'exploitation. Il n'y a pas d'intermédiaire entre le chargeur de démarrage et le noyau.

Il est possible que le processus de démarrage utilisé par d'autres systèmes d'exploitation soit différent. Par exemple, le système d'exploitation Microsoft® Windows®, ainsi que d'autres systèmes d'exploitation, sont chargés en utilisant le *chargement en chaîne*. Avec cette méthode, le MBR pointe simplement vers le premier secteur de la partition contenant le système d'exploitation où il trouve les fichiers nécessaires au démarrage proprement dit de ce système d'exploitation.

GRUB prend en charge les méthodes de chargement direct et en chaîne, ce qui lui permet de lancer tout système d'exploitation.

Avertissement

Lors de l'installation, les programmes d'installation DOS et Windows de Microsoft écrasent complètement le MBR, détruisant ainsi tout chargeur de démarrage existant. Si vous créez un système à double démarrage, nous vous conseillons d'installer en premier le système d'exploitation Microsoft.

2.2.2. Caractéristiques de GRUB

GRUB contient un certain nombre de caractéristiques qui le rendent plus intéressant que d'autres chargeurs de démarrage disponibles pour l'architecture x86. Vous trouverez ci-dessous une liste de certaines des caractéristiques les plus importantes :

- *GRUB offre un véritable environnement pré-système d'exploitation à base de commandes sur les ordinateurs x86.* Cette fonctionnalité permet à l'utilisateur de bénéficier d'une flexibilité maximale pour le chargement de systèmes d'exploitation avec des options spécifiées ou pour obtenir des informations sur le système. Pendant des années, de nombreuses architectures autres que l'architecture x86 ont utilisé des environnements pré-système d'exploitation qui permettent de démarrer le système depuis une ligne de commande.
- *GRUB prend en charge le mode Logical Block Addressing (LBA).* Le mode LBA, qui place la conversion d'adressage utilisée pour localiser des fichiers dans le micrologiciel du disque, est utilisé sur de nombreux périphériques IDE et sur tous les périphériques SCSI. Avant l'arrivée du mode LBA, les chargeurs de démarrage pouvaient se heurter à la limitation du BIOS par rapport au 1024ème

cylindre, créant ainsi des situations dans lesquelles le BIOS se trouvait dans l'incapacité de trouver des fichiers au-delà de cette tête de cylindre du disque. La prise en charge du mode LBA permet à GRUB de procéder à l'amorçage de systèmes d'exploitation résidant sur des partitions situées au-delà de la limite du 1024ème cylindre, à condition que votre BIOS prenne en charge le mode LBA. La plupart des révisions modernes du BIOS prennent en charge le mode LBA.

- *GRUB peut lire les partitions ext2.* Cette fonctionnalité permet à GRUB d'accéder à son fichier de configuration, `/boot/grub/grub.conf`, chaque fois que le système démarre, évitant ainsi à l'utilisateur d'écrire une nouvelle version du chargeur de démarrage Étape 1 sur le MBR lors de toute modification de la configuration. L'utilisateur ne devra réinstaller GRUB sur le MBR que si l'emplacement physique de la partition `/boot/` est déplacé sur le disque. Pour en savoir plus sur l'installation de GRUB sur le MBR, reportez-vous à la Section 2.3.

2.3. Installation de GRUB

Si GRUB n'est pas installé au cours du processus d'installation, vous pouvez l'installer ultérieurement. Une fois installé, il devient automatiquement le chargeur de démarrage par défaut.

Avant d'installer GRUB, vérifiez que vous disposez du paquetage GRUB le plus récent ou utilisez le paquetage GRUB des CD-ROM d'installation. Pour obtenir des instructions sur l'installation de paquetages, reportez-vous au chapitre intitulé *Gestion des paquetages avec RPM* du *Guide d'administration système de Red Hat Enterprise Linux*.

Une fois le paquetage GRUB installé, ouvrez une invite de shell root et lancez la commande `/sbin/grub-install <location>`, où `<location>` correspond à l'emplacement où le chargeur de démarrage GRUB Étape 1 doit être installé. Par exemple, la commande suivante installe GRUB sur le MBR du périphérique IDE maître sur le bus IDE primaire :

```
/sbin/grub-install /dev/hda
```

Lors du prochain démarrage de votre système, le menu du chargeur de démarrage graphique de GRUB apparaîtra avant le chargement du noyau en mémoire.

Important

Si GRUB est installé sur une matrice RAID 1, il est possible que le système ne puisse plus démarrer dans le cas d'une défaillance de disque. Une solution qui n'est pas supportée, est offerte en ligne à l'adresse suivante :

http://www.dur.ac.uk/a.d.stribblehill/mirrored_grub.html

2.4. Terminologie relative à GRUB

Un des points fondamentaux à maîtriser avant d'utiliser GRUB est la façon dont le programme fait référence aux périphériques, tels que votre disque dur et les partitions. Ces informations sont très importantes lorsque vous configurez GRUB pour qu'il démarre plusieurs systèmes d'exploitation.

2.4.1. Noms des périphériques

Lorsque vous faites référence à un périphérique spécifique avec GRUB, utilisez le format suivant (notez que les parenthèses et les virgules sont très importantes dans la syntaxe) :

`(<type-of-device><bios-device-number>,<partition-number>)`

L'élément <*type-of-device*> spécifie le type de périphérique à partir duquel GRUB démarre. Les deux options les plus courantes sont `hd` pour un disque dur et `fd` pour une disquette de 3,5 pouces. Un autre type de périphérique moins couramment utilisé est également disponible, à savoir `nd` pour un disque réseau. Des instructions relatives à la configuration de GRUB pour qu'il démarre sur le réseau existent en ligne à l'adresse suivante : http://www.gnu.org/software/grub/manual/.

<*bios-device-number*> correspond au numéro du périphérique BIOS. Le disque dur IDE primaire est numéroté `0` et un disque dur IDE secondaire est numéroté `1`. Cette syntaxe est équivalente à celle utilisée pour les périphériques par le noyau. Par exemple, la lettre `a` dans `hda` pour le noyau est analogue au `0` dans `hd0` pour GRUB, le `b` dans `hdb` est analogue au `1` dans `hd1`, et ainsi de suite.

<*partition-number*> se rapporte au numéro d'une partition sur un périphérique. Comme pour l'élément <*bios-device-number*>, la numérotation des partitions commence par `0`. Toutefois, les partitions BSD sont désignées par des lettres, où `a` correspond à `0`, `b` correspond à `1`, et ainsi de suite.

Astuce

Le système de numérotation de GRUB pour les périphériques commence toujours par `0` et non pas `1`. Le non respect de cette distinction est la source d'une des erreurs les plus courantes commises par les nouveaux utilisateurs.

Par exemple, si un système possède plusieurs disques durs, GRUB fait référence au premier disque dur en tant que `(hd0)` et au deuxième en tant que `(hd1)`. De la même manière, GRUB fait référence à la première partition du premier disque en tant que `(hd0,0)` et à la troisième partition sur le second disque dur en tant que `(hd1,2)`.

GRUB fait appel aux règles suivantes pour nommer les périphériques et les partitions :

- Peu importe si vos disques durs sont IDE ou SCSI. Le nom de tous les disques durs commence par `hd`. Les lecteurs de disquette quant à eux commencent par `fd`.
- Pour indiquer un périphérique en entier sans spécifier ses partitions, il suffit de retirer la virgule et le numéro de la partition. Ceci est important lorsque l'on souhaite que GRUB configure le bloc de démarrage maître pour un disque donné. Par exemple, `(hd0)` indique le MBR sur le premier périphérique et `(hd3)` indique le MBR sur le quatrième.
- Si un système est doté de plusieurs lecteurs de disque, il est très important de connaître l'ordre de démarrage défini dans le BIOS. Cette tâche est relativement simple si vous ne possédez que des disques IDE ou SCSI, mais s'il existe un mélange de périphériques, il est alors critique que le type de lecteur lisant la partition boot soit démarrer en premier.

2.4.2. Noms de fichiers et listes des blocs

Lorsque des commandes saisies pour GRUB référencent un fichier, comme une liste de type menu, il est impératif de spécifier le chemin absolu du fichier immédiatement après avoir désigné le périphérique et la partition.

L'exemple suivant illustre la structure d'une telle commande :

(<*device-type*><*device-number*>,<*partition-number*>)<*/path/to/file*>

Dans cet exemple, remplacez <*device-type*> par `hd`, `fd` ou `nd`. Remplacez <*device-number*> par le nombre entier du périphérique. Remplacez <*/path/to/file*> par le chemin absolu du périphérique de niveau supérieur.

Il est également possible d'indiquer à GRUB des fichiers qui n'apparaissent pas en fait dans le système de fichiers, tel qu'un chargeur de chaîne qui apparaît dans les tout premiers blocs d'une partition. Pour

charger de tels fichiers, vous devez fournir une *liste de blocs* (blocklist) qui indique bloc par bloc, l'emplacement du fichier sur la partition. Étant donné qu'un fichier est souvent constitué de plusieurs blocs, les listes de blocs utilisent une syntaxe particulière. Chaque bloc contenant le fichier est spécifié par un nombre de blocs décalé, suivi du nombre de blocs existant après ce point de décalage précis. Les décalages des blocs sont énumérés séquentiellement dans une liste délimitée par des virgules.

Prenons l'exemple de la liste de blocs ci-dessous pour illustrer cette notion :

```
0+50,100+25,200+1
```

Cette liste de blocs indique à GRUB qu'il doit utiliser un fichier commençant au premier bloc de la partition et qui utilise les blocs 0 à 49, 99 à 124 et 199.

Il est très utile de savoir comment écrire des listes de blocs, particulièrement lorsque GRUB doit charger des systèmes d'exploitation qui utilisent le chargement en chaîne. Vous pouvez laisser tomber le décalage de blocs si vous commencez au bloc 0. Par exemple, le fichier de chargement en chaîne sur la première partition du premier disque dur devrait s'appeler ainsi :

```
(hd0,0)+1
```

Vous pouvez également utiliser la commande `chainloader` suivante avec un mode d'indication de liste de blocs similaire à la ligne de commande GRUB après avoir spécifié le bon périphérique et la bonne partition et en étant connecté en tant que root :

```
chainloader +1
```

2.4.3. Le système de fichiers racine et GRUB

L'utilisation du terme *système de fichiers root* a un sens différent dans GRUB. Il est important de se rappeler que le système de fichiers root de GRUB n'a rien à voir avec le système de fichiers root de Linux.

Le système de fichiers root de GRUB est le niveau supérieur du périphérique spécifié. Par exemple, le fichier image `(hd0,0)/grub/splash.xpm.gz` est situé au sein du répertoire `/grub/` au niveau supérieur (ou root) de la partition `(hd0,0)` (qui est en fait la partition `/boot/` du système).

Ensuite, la commande `kernel` est exécutée avec l'emplacement du fichier noyau spécifié en option. Une fois que le noyau Linux démarre, il monte le système de fichiers root auquel les utilisateurs Linux sont habitués. Le système de fichiers root de GRUB monté au départ et ses montages sont oubliés ; en effet, ils ne servaient qu'au démarrage du fichier noyau.

Pour de plus amples informations, lisez les notes relatives aux commandes `root` et `kernel` contenues dans la Section 2.6.

2.5. Interfaces GRUB

GRUB offre trois interfaces, qui fournissent différents niveaux de fonctionnalités. Chacune de ces interfaces permet aux utilisateurs de démarrer le noyau Linux ou d'autres systèmes d'exploitation.

Les interfaces sont les suivantes :

Remarque

Les interfaces GRUB mentionnées ci-après sont accessibles en appuyant sur une touche quelconque seulement pendant trois secondes après l'affichage de l'écran menu de GRUB.

Interface Menu

L'interface par défaut qui s'affiche lorsque GRUB est configuré par le programme d'installation se présente ainsi : un menu des différents systèmes d'exploitation ou noyaux pré-configurés est affiché sous la forme d'une liste, organisée par nom. Utilisez les flèches du clavier pour choisir une sélection différente de celle retenue par défaut, puis appuyez sur la touche [Entrée] pour démarrer le système d'exploitation ou le noyau choisi. Sinon, un délai d'attente est déterminé et, dans le cas où aucun choix n'est fait avant l'écoulement de ce dernier, GRUB procède au démarrage de l'option par défaut.

Appuyez sur la touche [e] pour accéder à l'interface éditeur d'entrées ou sur la touche [c] pour charger une interface de ligne de commande.

Pour plus d'informations sur la configuration de cette interface, consultez la Section 2.7.

Interface éditeur d'entrées de menu

Pour accéder à l'éditeur d'entrée de menu, appuyez sur la touche [e] depuis le menu du chargeur de démarrage. Les commandes de GRUB relatives à cette entrée sont présentées ci-après. Ces lignes de commande peuvent être modifiées par les utilisateurs avant le démarrage du système d'exploitation en ajoutant une ligne de commande ([o] insère la nouvelle ligne après la ligne actuelle et [O] l'insère avant), en modifiant une ligne de commande ([e]) ou finalement en supprimant une ligne de commande ([d]).

Une fois que vos modifications sont effectuées, appuyez sur la touche [b] pour exécuter les commandes et démarrer le système d'exploitation. La touche [Échap] elle, permet d'annuler ces modifications et recharge l'interface menu standard. Finalement, la touche [c] elle, charge l'interface de la ligne de commande.

Astuce

Pour obtenir des informations sur le moyen de changer les niveaux d'exécution à l'aide de l'éditeur d'entrées du menu de GRUB, reportez-vous à la Section 2.8.

Interface de ligne de commande

L'interface de ligne de commande est certes la plus élémentaire des interfaces GRUB, mais c'est celle qui fournit le plus grand niveau de contrôle. La ligne de commande permet de taper toute commande GRUB pertinente et de l'exécuter en appuyant sur la touche [Entrée]. Cette interface présente certaines fonctionnalités avancées de type shell parmi lesquelles figurent la touche [Tab] pour l'achèvement automatique de ligne en fonction du contexte et les combinaisons de touches avec [Ctrl] lors de la saisie de commandes, telles que [Ctrl]-[a] pour se déplacer au début de la ligne et [Ctrl]-[e] pour aller directement à la fin de la ligne. De plus, les flèches, les touches [Début], [Fin] et [Suppr] fonctionnent de la même façon que sous le shell `bash`.

Pour obtenir une liste des commandes les plus courantes, reportez-vous à la Section 2.6.

2.5.1. Ordre de chargement des interfaces

Lorsque GRUB charge le chargeur de démarrage Étape 2 (ou secondaire), il essaie d'abord de trouver son fichier de configuration. Une fois que celui-ci a été localisé, l'écran de l'interface menu s'affiche. Si l'utilisateur appuie sur une touche dans les trois secondes qui suivent, GRUB construit une liste de type menu et affiche l'interface menu. En revanche, si aucune touche n'est utilisée, l'entrée du noyau par défaut du menu GRUB est retenue.

Si le fichier de configuration est introuvable ou s'il est impossible de le lire, GRUB charge l'interface de ligne de commande permettant à l'utilisateur de saisir manuellement les commandes nécessaires pour achever le processus de démarrage.

Si le fichier de configuration n'est pas valide, GRUB affiche l'erreur et attend une commande. Ceci aide l'utilisateur à déterminer exactement là où le problème est survenu. Appuyez sur une touche quelconque pour recharger l'interface menu, d'où il est alors possible d'éditer l'option du menu et d'apporter les corrections nécessaires en fonction de l'erreur rapportée par GRUB. Si la correction apportée ne résout pas le problème, GRUB rapporte une erreur et charge de nouveau l'interface menu.

2.6. Commandes GRUB

GRUB permet un certain nombre de commandes utiles dans son interface ligne de commande. Certaines de ces commandes acceptent une option après leur nom. Pour être acceptées, ces options doivent être séparées de la commande et des autres options présentes par un espace.

Ci-après figure une liste de commandes utiles :

- `boot` — Démarre le dernier système d'exploitation ou le chargeur de chaîne qui a été chargé.
- `chainloader` <*`/path/to/file`*> — Charge le fichier indiqué comme chargeur de chaîne (où <*`/path/to/file`*> représente le chemin d'accès au fichier). Si le fichier se situe sur le premier secteur de la partition spécifiée, utilisez la notation de type liste de blocs, `+1`, au lieu du nom de fichier.

  Ci-après figure un exemple de la commande `chainloader` :

  ```
  chainloader +1
  ```

- `displaymem` — Affiche l'utilisation actuelle de mémoire, sur la base des informations fournies par le BIOS. Cette commande est pratique pour déterminer la quantité de mémoire vive dont le système dispose, avant de le démarrer.
- `initrd` <*`/path/to/initrd`*> — Permet aux utilisateurs de spécifier un disque RAM initial à utiliser pour l'amorçage (où <*`/path/to/initrd`*> correspond au chemin d'accès à initrd). Un fichier `initrd` est nécessaire lorsque le noyau a besoin de certains modules pour démarrer correctement, comme lorsque la partition root est formatée avec le système de fichiers ext3.

  Ci-après figure un exemple de la commande `initrd` :

  ```
  initrd /initrd-2.6.8-1.523.img
  ```

- `install` <*`stage-1`*> <*`install-disk`*> <*`stage-2`*> `p` *`config-file`* — Installe GRUB dans le MBR du système.
  - <*`stage-1`*> — Précise un périphérique, une partition et un fichier où l'image du premier chargeur de démarrage peut être trouvée, tel que `(hd0,0)/grub/stage1`.
  - <*`install-disk`*> — Spécifie le disque où le chargeur de démarrage Étape 1 doit être installé, comme par exemple `(hd0)`.
  - <*`stage-2`*> — Indique au chargeur de démarrage Étape 2, l'emplacement du chargeur de démarrage Étape 1 comme par exemple, `(hd0,0)/grub/stage2`.
  - `p` <*`config-file`*> — Indique à la commande `install` de rechercher le fichier de configuration du menu spécifié par <*`config-file`*>, comme, par exemple, `(hd0,0)/grub/grub.conf`.

Avertissement

La commande `install` écrase toutes les informations déjà présentes sur le MBR.

- `kernel <`*`/path/to/kernel`*`> <`*`option-1`*`> <`*`option-N`*`>` ... — Indique le fichier noyau à charger lors du démarrage du système d'exploitation. Remplacez `<`*`/path/to/kernel`*`>` par le chemin absolu de la partition spécifiée par la commande root. Remplacez `<`*`option-1`*`>` par les options du noyau Linux, comme par exemple, `root=/dev/hda5` pour spécifier le périphérique sur lequel la partition root du système se trouve. Plusieurs options peuvent être transmises au noyau dans une liste délimitée par des espaces.

  Un exemple de la commande `kernel` ressemble à l'extrait suivant :

  ```
  kernel /vmlinuz-2.4.21 root=/dev/hda5
  ```

  L'option de l'exemple précédent indique que le système de fichiers root de Linux se trouve sur la partition `hda5`.

- `root (<`*`device-type`*`><`*`device-number`*`>,<`*`partition`*`>)` — Configure la partition root de GRUB, comme, par exemple, `(hd0,0)` et monte la partition.

  Un exemple de la commande `root` ressemble à l'extrait suivant :

  ```
  root (hd0,0)
  ```

- `rootnoverify (<`*`device-type`*`><`*`device-number`*`>,<`*`partition`*`>)` — Configure la partition root de GRUB, tout comme la commande `root`, mais ne monte pas la partition.

D'autres commandes sont également disponibles ; tapez `help --all` pour obtenir une liste complète de commandes. Pour une description de toutes les commandes GRUB, reportez-vous à la documentation disponible en ligne à l'adresse suivante : http://www.gnu.org/software/grub/manual/.

2.7. Fichier de configuration du menu de GRUB

Le fichier de configuration (`/boot/grub/grub.conf`) utilisé pour créer la liste des systèmes d'exploitation à démarrer dans l'interface menu, permet à l'utilisateur de sélectionner un groupe prédéterminé de commandes à exécuter. Les commandes fournies dans la Section 2.6 peuvent être utilisées, ainsi que certaines commandes spéciales qui ne sont disponibles que dans le fichier de configuration.

2.7.1. Structure des fichiers de configuration

Le fichier de configuration de l'interface menu de GRUB est `/boot/grub/grub.conf`. Les commandes servant à la définition des préférences générales pour l'interface menu sont placées au début du fichier, suivies des différentes strophes (aussi appelées stanzas) pour chacun des systèmes d'exploitation ou noyaux énumérés dans le menu.

L'extrait ci-dessous correspond à un fichier de configuration élémentaire du menu de GRUB servant au démarrage de Red Hat Enterprise Linux ou de Microsoft Windows 2000 :

```
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux AS (2.6.8-1.523)
        root (hd0,0)
        kernel /vmlinuz-2.6.8-1.523 ro root=/dev/VolGroup00/LogVol00 rhgb quiet
        initrd /initrd-2.6.8-1.523.img

# section to load Windows
title Windows
        rootnoverify (hd0,0)
        chainloader +1
```

Ce fichier invite GRUB à construire un menu avec Red Hat Enterprise Linux comme le système d'exploitation par défaut, réglé pour un démarrage automatique après 10 secondes. Deux sections sont disponibles, une entrée pour chacun des systèmes d'exploitation, avec les commandes spécifiques à la table de partitions de chaque système.

Remarque

Notez bien que le paramètre par défaut est spécifié sous la forme d'un chiffre. Ceci se rapporte à la première ligne `title` du fichier de configuration de GRUB. Si vous voulez que `Windows` soit le paramètre par défaut dans l'exemple précédent, changez la valeur `default=0` en `default=1`.

La configuration du fichier de configuration d'un menu GRUB pour le démarrage de multiples systèmes d'exploitation va au-delà de la portée de ce chapitre. Ainsi, pour obtenir une liste des ressources supplémentaires, reportez-vous à la Section 2.9.

2.7.2. Directives des fichiers de configuration

Les commandes suivantes sont des directives utilisées couramment dans le fichier de configuration du menu de GRUB :

- `chainloader <`*`/path/to/file`*`>` — Charge le fichier indiqué comme chargeur de chaîne. Remplacez `<`*`/path/to/file`*`>` par le chemin absolu du chargeur de chaîne. Si le fichier se trouve sur le premier secteur de la partition donnée, utilisez la notation de liste de blocs, `+1`.
- `color <`*`normal-color`*`> <`*`selected-color`*`>` — Permet de définir les couleurs spécifiques à utiliser dans le menu, où deux couleurs sont configurées, une pour le premier plan et une pour l'arrière-plan. Utilisez des noms de couleur simples tels que `red/black` (rouge/noir). Par exemple : `color red/black green/blue`
- `default=<`*`integer`*`>` — Remplacez `<`*`integer`*`>` par le numéro du titre de l'entrée par défaut qui sera chargée si le délai imparti pour le choix d'une option du menu est dépassé.
- `fallback=<`*`integer`*`>` — Remplacez `<`*`integer`*`>` par le numéro du titre de l'entrée à essayer en cas d'échec de la première tentative.
- `hiddenmenu` — Empêche l'affichage de l'interface menu de GRUB, chargeant l'entrée par défaut (`default`) lorsque la durée d'attente initiale (`timeout`) est dépassée. L'utilisateur peut visualiser le menu standard de GRUB en appuyant sur la touche [Échap].
- `initrd <`*`/path/to/initrd`*`>` — Permet à l'utilisateur de spécifier un disque RAM initial à utiliser pour l'amorçage. Remplacez `<`*`/path/to/initrd`*`>` par le chemin absolu du disque RAM initial.
- `kernel <`*`/path/to/kernel`*`> <`*`option-1`*`> <`*`option-N`*`>` — Spécifie le fichier noyau à charger lors du démarrage du système d'exploitation. Remplacez `<`*`/path/to/kernel`*`>` par le chemin absolu de la partition spécifiée dans la directive root. Plusieurs options peuvent être transmises au noyau lors de son chargement.
- `password=<`*`password`*`>` — Interdit à tout utilisateur ne connaissant pas le mot de passe d'éditer les entrées relatives à l'option de ce menu.

  Il est possible éventuellement, d'indiquer un autre fichier de configuration de menu après la commande `password=<`*`password`*`>`. Dans ce cas, GRUB redémarrera le chargeur de démarrage Étape 2 et utilisera l'autre fichier de configuration spécifié pour construire le menu. Si ce fichier alternatif n'est pas indiqué dans cette commande, tout utilisateur en possession du mot de passe sera à même d'éditer le fichier de configuration actuel.

Pour davantage d'informations sur la sécurisation de GRUB, reportez-vous au chapitre intitulé *Sécurité du poste de travail* du *Guide de sécurité de Red Hat Enterprise Linux*.

- `root (<device-type><device-number>,<partition>)` — Configure la partition root de GRUB, comme, par exemple, `(hd0,0)` et monte la partition.
- `rootnoverify (<device-type><device-number>,<partition>)` — Configure la partition root de GRUB, tout comme la commande `root`, mais ne monte pas la partition.
- `timeout=<integer>` — Spécifie la durée, en secondes, qui peut s'écouler avant que GRUB ne charge l'entrée indiquée dans la commande `default`.
- `splashimage=<path-to-image>` — Précise l'emplacement de l'image de fond utilisée lors du démarrage de GRUB.
- `title group-title` — Définit le titre à utiliser avec un groupe donné de commandes utilisé pour charger un système d'exploitation ou un noyau.

Pour ajouter des commentaires plus lisibles au fichier de configuration du menu, commencez la ligne par le symbole dièse (`#`).

2.8. Changement de niveau d'exécution au démarrage

Sous Red Hat Enterprise Linux, il est possible de changer le niveau d'exécution par défaut au démarrage.

Pour changer le niveau d'exécution d'une session à démarrage unique, utilisez les instructions suivantes :

- Appuyez sur une touche quelconque, lorsque l'écran menu de GRUB apparaît au démarrage, pour accéder au menu de GRUB (seulement possible dans les trois secondes suivant l'affichage de l'écran menu)
- Appuyez sur la touche [a] pour ajouter un élément à la commande `kernel`.
- Ajoutez `<espace><runlevel>` à la fin de la ligne des options de démarrage afin de démarrer au niveau d'exécution (ou runlevel) souhaité. Par exemple, l'entrée suivante engendrera un processus de démarrage au niveau d'exécution 3.

```
grub append> ro root=/dev/VolGroup00/LogVol00 rhgb quiet 3
```

2.9. Ressources supplémentaires

Ce chapitre a seulement pour intention de présenter GRUB. Consultez les ressources suivantes si vous souhaitez en savoir plus sur le fonctionnement de GRUB.

2.9.1. Documentation installée

- `/usr/share/doc/grub-<version-number>` — Ce répertoire contient un certain nombre d'informations sur l'utilisation et la configuration de GRUB. `<version-number>` correspond à la version installée du paquetage GRUB.
- `info grub` — La page d'information de GRUB contient des leçons, ainsi qu'un manuel de référence pour les utilisateurs et les programmeurs et un Forum Aux Questions (FAQ) sur GRUB et son utilisation.

2.9.2. Sites Web utiles

- http://www.gnu.org/software/grub/ — La page d'accueil du projet GRUB de GNU. Ce site contient des informations concernant l'état du développement de GRUB ainsi qu'un FAQ.
- http://www.redhat.com/mirrors/LDP/HOWTO/mini/Multiboot-with-GRUB.html — Ce document examine les différentes utilisations possibles de GRUB, y compris le démarrage de systèmes d'exploitation autres que Linux.
- http://www.linuxgazette.com/issue64/kohli.html — Un article d'introduction traitant de la configuration de GRUB sur un système, et ce, à partir des toutes premières étapes. Il inclut entre autres un aperçu des options de la ligne de commande de GRUB.

2.9.3. Livre sur le sujet

- *Guide de sécurité de Red Hat Enterprise Linux* ; Red Hat, Inc. — Le chapitre *Sécurité du poste de travail* explique, de manière concise, comment sécuriser le chargeur de démarrage GRUB.

Chapitre 3.

Structure d'un système de fichiers

3.1. 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 manières selon lesquelles un système d'exploitation interagit avec ses utilisateurs, ses applications et son modèle de sécurité dépendent de la façon dont il stocke ses fichiers sur des périphériques de stockage. Le fait d'avoir une structure de système de fichiers commune garantit que les utilisateurs et les programmes puissent non seulement avoir accès aux fichiers mais qu'ils puissent également y enregistrer des données.

Les systèmes de fichiers réduisent les fichiers en deux catégories logiques :

- Fichiers partageables contre fichiers non-partageables
- Fichiers variables contre fichiers statiques

Les fichiers *partageables* sont accessibles aussi bien localement qu'à partir d'hôtes distants, alors que les fichiers *non-partageables* sont seulement disponibles localement. Les fichiers *variables*, comme des documents, peuvent être modifiés à tout moment. Les fichiers *statiques*, tels que les fichiers binaires, ne peuvent être changés sans l'action directe de l'administrateur système.

Les fichiers sont considérés de la sorte en raison des différents types d'autorisations données aux répertoires qui les contiennent. La façon selon laquelle le système d'exploitation et ses utilisateurs intergassient avec un fichier donné détermine le répertoire dans lequel ce dernier est placé, selon qu'il est monté avec des permissions en lecture-seule ou en lecture-écriture et selon le niveau d'accès octroyé à chaque utilisateur sur le fichier en question. Le niveau le plus élevé de cette organisation est crucial. En effet, l'accès aux sous-répertoires peut être limité ou des problèmes de sécurité pourraient survenir si le niveau le plus élevé est mal organisé ou s'il ne suit pas une structure rigide.

3.2. Aperçu de FHS (Filesystem Hierarchy Standard)

Red Hat Enterprise Linux utilise la structure de système de fichiers *FHS* (de l'anglais *Filesystem Hierarchy Standard*), un document de collaboration définissant les noms, les emplacements et les permissions de nombreux types de fichiers et répertoires.

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

La conformité avec la norme a de nombreuses implications, mais les deux aspects les plus importants sont la compatibilité avec d'autres systèmes également conformes et la possibilité de monter une partition `/usr/` en lecture-seule car elle contient des fichiers exécutables courants et n'a pas pour vocation d'être modifiée par les utilisateurs. Étant donné que le répertoire `/usr/` peut être monté en lecture-seule, le montage peut être effectué depuis le CD-ROM ou depuis un autre ordinateur par le biais d'un montage NFS en lecture-seule.

3.2.1. Organisation de FHS

Les répertoires et les fichiers mentionnés ici représentent 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.

La norme complète est disponible en ligne à l'adresse suivante : http://www.pathname.com/fhs/.

3.2.1.1. Le répertoire `/boot/`

Le répertoire `/boot/` contient des fichiers statiques requis pour démarrer le système, comme le noyau Linux. Ces fichiers sont essentiels pour que le système démarre correctement.

 **Avertissement**

Ne supprimez le répertoire `/boot/` sous aucun prétexte. En effet, sa suppression empêcherait votre système de démarrer.

3.2.1.2. 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.

3.2.1.3. Le répertoire `/etc/`

Le répertoire `/etc/` est réservé aux fichiers de configuration locaux sur votre ordinateur. Aucun fichier binaire ne devrait être stocké dans `/etc/`. Tous les fichiers binaires qui se trouvaient auparavant dans `/etc/` devraient être maintenant stockés dans `/sbin/` ou dans `/bin/`.

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

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

Le répertoire `/etc/X11/` est destiné aux fichiers de configuration du système X Window, tels que `xorg.conf`. Le répertoire `/etc/skel/` est pour les fichiers utilisateur "squelette" qui sont utilisés pour remplir un répertoire personnel lors de la création d'un nouvel utilisateur.

3.2.1.4. 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.

3.2.1.5. Le répertoire `/media/`

Le répertoire `/media/` contient des sous-répertoires utilisés comme points de montage pour des supports amovibles, tels que les disquettes 3,5 pouces, les CD-ROM et les disques Zip.

3.2.1.6. Le répertoire `/mnt/`

Le répertoire `/mnt/` est réservé aux systèmes de fichiers montés de façon temporaire, tels que les montages NFS de systèmes de fichiers. Pour tout support amovible, utilisez le répertoire `/media/`.

Remarque

Ce répertoire ne doit pas être utilisé par des programmes d'installation.

3.2.1.7. Le répertoire `/opt/`

Le répertoire `/opt/` fournit du stockage pour des paquetages logiciels d'applications statiques de grande taille.

Un paquetage qui place des fichiers dans le répertoire `/opt/` crée un répertoire portant le même nom que le paquetage. Celui-ci contient les fichiers qui autrement seraient éparpillés dans tout le système de fichiers, offrant ainsi à l'administrateur système un moyen facile de déterminer le rôle de chaque fichier d'un paquetage donné.

Par exemple, si `sample` était le nom d'un paquetage logiciel situé dans le répertoire `/opt/`, 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, se trouvent 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, comme `/opt/sample/tool1/` et `/opt/sample/tool2/`, qui à son tour peut avoir ses propres répertoires `/bin/`, `/man/` et autres répertoires semblables.

3.2.1.8. Le répertoire `/proc/`

Le répertoire `/proc/` contient des fichiers spéciaux qui extraient des informations à partir du noyau ou envoient des informations au noyau.

Étant donné l'immense variété de données disponibles dans `/proc/` et les nombreuses manières selon lesquelles ce répertoire peut être utilisé pour communiquer avec le noyau, un chapitre entier a été consacré à ce sujet. Pour obtenir de plus amples informations, consultez le Chapitre 5.

3.2.1.9. Le répertoire `/sbin/`

Le répertoire `/sbin/` est conçu pour les fichiers exécutables qui sont utilisés par le super-utilisateur. Les fichiers exécutables dans `/sbin/` ne sont utilisés que pour démarrer et exécuter des opérations de remise en état du système. FHS indique ce qui suit :

> "`/sbin/` contient généralement des fichiers essentiels pour le démarrage, la restauration et/ou la réparation du système, en plus des fichiers binaires figurant dans `/bin/`. Tous les programmes exécutés après que `/usr/` soit monté (lorsqu'il n'y a pas de problème) sont généralement placés dans `/usr/sbin/`. Les programmes d'administration système installés localement doivent être placés dans le répertoire `/usr/local/sbin/`."

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

```
arp, clock,halt,
init, fsck.*, grub,
ifconfig, mingetty, mkfs.*,
mkswap, reboot, route,
shutdown, swapoff, swapon
```

3.2.1.10. Le répertoire `/srv/`

Le répertoire `/srv/` contient des données spécifiques au site qui sont fournie par votre système exécutant Red Hat Enterprise Linux. Ce répertoire donne aux utilisateurs l'emplacement de fichiers de données pour un service spécifique, tel que FTP, WWW ou CVS. Des données ne se rapportant qu'à un utilisateur spécifique devraient aller dans le répertoire `/home/`.

Remarque

Veuillez prendre note du fait que des fichiers actuellement placés dans `/var/` *pourraient* être déplacés vers `/srv/` dans de futures versions.

3.2.1.11. Le répertoire `/sys/`

Le répertoire `/sys/` utilise le nouveau système de fichiers virtuel `sysfs` spécifique au noyau 2.6. Avec la prise en charge améliorée pour des périphériques matériels enfichables à chaud dans le noyau 2.6, le répertoire `/sys/` contient des informations semblables à celles contenues dans `/proc/`, mais affiche une vue hiérarchisée des informations spécifiques aux périphériques pour ce qui est des périphériques enfichables à chaud.

Pour voir comment certains périphériques USB et FireWire sont montés, reportez-vous aux pages de manuel de `/sbin/hotplug` et `/sbin/udev`.

3.2.1.12. Le répertoire `/usr/`

Le répertoire `/usr/` est destiné aux fichiers pouvant être partagés parmi plusieurs machines. Le répertoire `/usr/`, monté en lecture-seule, réside généralement sur sa propre partition. Au minimum, les répertoires suivants devraient être des sous-répertoires de`/usr/` :

```
/usr
  |- bin/
  |- etc/
  |- games/
  |- include/
  |- kerberos/
  |- lib/
  |- libexec/
  |- local/
  |- sbin/
  |- share/
  |- src/
  |- tmp -> ../var/tmp/
  |- X11R6/
```

Sous le répertoire `/usr/`, le sous-répertoire `bin/` contient des fichiers exécutables, `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 en relation avec Kerberos et finalement, `lib/` contient des fichiers objet et des bibliothèques qui ne sont pas conçu pour 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 système (ceux qui n'appartiennent pas au répertoire `/sbin/`), `share/` contient des fichiers qui ne sont pas spécifiques à une architecture particulière, `src/` est pour le code source et `X11R6/` est pour le système X Window (XFree86 sur Red Hat Enterprise Linux).

3.2.1.13. Le répertoire `/usr/local/`

Selon FHS :

> "La hiérarchie `/usr/local/` est destinée à être utilisée par l'administrateur système lors de l'installation locale de logiciels. Elle doit être protégée contre tout écrasement lors de la mise à jour des logiciels du 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/
       |- etc/
       |- games/
       |- include/
       |- lib/
       |- libexec/
       |- sbin/
       |- share/
       |- src/
```

Dans Red Hat Enterprise Linux, l'utilisation prévue pour `/usr/local/` est légèrement différente de celle qui est spécifiée par le document FHS. Selon ce dernier, `/usr/local/` devrait se trouver là où sont stockés des logiciels devant rester à l'écart des mises à niveaux logicielles du système. Étant donné que les mises à niveau logicielles s'effectuent en toute sécurité à l'aide du gestionnaire de *RPM* (*Red Hat Package Manager*), il n'est pas nécessaire de protéger des fichiers en les plaçant dans `/usr/local/`. À la place, le répertoire `/usr/local/` est utilisé pour des logiciels locaux de votre ordinateur.

Par exemple, si le répertoire `/usr/` est monté en tant que partage NFS en lecture-seule à partir d'un hôte distant, il est toujours possible d'installer un paquetage ou programme sous le répertoire `/usr/local/`.

3.2.1.14. Le répertoire `/var/`

FHS exigeant que Linux monte `/usr/` en lecture-seule, tous les programmes qui écrivent des fichiers journaux ou ont besoin des répertoires `spool/` ou `lock/` devraient les écrire dans le répertoire `/var/`. FHS stipule que `/var/` est pour :

> ...les fichiers de données variables. Parmi ces derniers figurent 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
  |- account/
  |- arpwatch/
  |- cache/
  |- crash/
  |- db/
  |- empty/
  |- ftp/
  |- gdm/
  |- kerberos/
  |- lib/
  |- local/
  |- lock/
  |- log/
  |- mail -> spool/mail/
  |- mailman/
  |- named/
  |- nis/
  |- opt/
  |- preserve/
  |- run/
  +- spool/
       |- at/
       |- clientmqueue/
       |- cron/
       |- cups/
       |- exim/
       |- lpd/
       |- mail/
       |- mailman/
       |- mqueue/
       |- news/
       |- postfix/
       |- repackage/
       |- rwho/
       |- samba/
       |- squid/
       |- squirrelmail/
       |- up2date/
       |- uucp
       |- uucppublic/
       |- vbox/
  |- tmp/
  |- tux/
  |- www/
  |- yp/
```

Les fichiers journaux du système, tels que `messages/` et `lastlog/` vont dans le répertoire `/var/log/`. Le répertoire `/var/lib/rpm/` contient les bases de données système du RPM. Les fichiers de verrouillage (lock) vont dans le répertoire `/var/lock/`, généralement dans des répertoires spécifiques aux programmes qui utilisent ce type de fichiers. Le répertoire `/var/spool/` a des sous-répertoires pour les programmes dans lesquels des fichiers de données sont stockés.

3.3. Emplacement des fichiers spéciaux sous Red Hat Enterprise Linux

Red Hat Enterprise Linux étend légèrement la structure FHS pour prendre en charge les fichiers spéciaux.

La plupart des fichiers appartenant au RPM se trouvent dans le répertoire `/var/lib/rpm/`. Afin d'obtenir de plus amples informations sur le RPM, reportez-vous au chapitre intitulé *Gestion de paquetages avec RPM* du *Guide d'administration système de Red Hat Enterprise Linux*.

Le répertoire `/var/spool/up2date/` contient des fichiers utilisés par l'**Agent de mise à jour Red Hat**, y compris des informations d'en-tête RPM. Cet emplacement peut également être utilisé pour stocker temporairement des RPM téléchargés lorsque vous mettez à jour votre système. Pour obtenir davantage d'informations sur Red Hat Network, reportez-vous à la documentation en ligne disponible à l'adresse suivante : https://rhn.redhat.com/.

Un autre emplacement spécifique à Red Hat Enterprise Linux est le répertoire `/etc/sysconfig/`. Ce répertoire stocke un grand nombre d'informations de configuration. De nombreux scripts lancés au démarrage utilisent les fichiers de ce répertoire. Consultez le Chapitre 4 pour obtenir plus d'informations sur le contenu de ce répertoire et le rôle de ces fichiers dans le processus de démarrage.

Enfin, un dernier répertoire à connaître est le répertoire `/initrd/`. Il est vide, mais est utilisé comme point de montage critique pendant le processus de démarrage.

Avertissement

Ne supprimez le répertoire `/initrd/` sous aucun prétexte. Sa suppression empêcherait votre système de démarrer, avec comme explication un message d'erreur de type panique du noyau.

Chapitre 4.

Répertoire `/sysconfig/`

Le répertoire `/etc/sysconfig/` contient de nombreux fichiers de configuration différents pour Red Hat Enterprise Linux.

Ce chapitre souligne certains des fichiers présents dans le répertoire `/etc/sysconfig/`, leur fonction et leur contenu. Ces informations ne prétendent pas être exhaustives car nombre de ces fichiers sont une série d'options qui ne sont utilisées que dans des circonstances bien spécifiques et plutôt rares.

4.1. Fichiers contenus dans le répertoire `/etc/sysconfig/`

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

- `amd`
- `apmd`
- `arpwatch`
- `authconfig`
- `autofs`
- `clock`
- `desktop`
- `devlabel`
- `dhcpd`
- `exim`
- `firstboot`
- `gpm`
- `harddisks`
- `hwconf`
- `i18n`
- `init`
- `ip6tables-config`
- `iptables-config`
- `irda`
- `keyboard`
- `kudzu`
- `mouse`
- `named`
- `netdump`
- `network`
- `ntpd`

- pcmcia
- radvd
- rawdevices
- samba
- sendmail
- selinux
- spamassassin
- squid
- system-config-securitylevel
- system-config-users
- system-logviewer
- tux
- vncservers
- xinetd

Remarque

Si certains des fichiers énumérés ci-dessus ne sont pas présents dans le répertoire /etc/sysconfig/, le programme correspondant n'est peut-être pas installé.

La section suivante fournit une description de ces fichiers. Les fichiers qui ne sont pas mentionnés ici ainsi que les options de fichiers supplémentaires se trouvent dans le fichier /usr/share/doc/initscripts-<*version-number*>/sysconfig.txt (remplacez <*version-number*> par le numéro de version du paquetage initscripts). Il peut également s'avérer utile d'examiner les scripts d'initialisation dans le répertoire /etc/rc.d/.

4.1.1. /etc/sysconfig/amd

Le fichier /etc/sysconfig/amd contient différents paramètres utilisés par amd ; ces derniers permettent le montage automatique et le démontage de systèmes de fichiers.

4.1.2. /etc/sysconfig/apmd

Le fichier /etc/sysconfig/apmd est utilisé par apmd pour configurer les paramètres d'alimentation spécifiques qui doivent être démarrés/arrêtés/modifiés en cas de suspension ou de reprise des opérations. Ce fichier configure le mode de fonctionnement de apmd selon que le matériel prend en charge ou non la gestion avancée de l'énergie (ou *APM* de l'anglais *Advanced Power Management*) ou selon que l'utilisateur a configuré le système pour utiliser cette fonctionnalité. Le démon apm est un programme de contrôle qui fonctionne avec le code de gestion d'énergie au sein du noyau Linux. Il est capable d'avertir les utilisateurs d'ordinateurs portables lorsque le niveau de la batterie est bas ou lorsqu'il y a un problème avec des paramètres liés à la source d'énergie.

4.1.3. /etc/sysconfig/arpwatch

Le fichier /etc/sysconfig/arpwatch est utilisé pour transmettre des arguments au démon arpwatch lors du démarrage. Le démon arpwatch maintient une table d'adresses Ethernet MAC et leurs parités d'adresses IP. Par défaut, ce fichier attribue la propriété du processus arpwatch à l'utilisateur pcap et envoie tout message à la file d'attente de messages de root. Pour obtenir de plus amples informations sur les paramètres que vous pouvez utiliser dans ce fichier, reportez-vous à la page de manuel de arpwatch.

4.1.4. /etc/sysconfig/authconfig

Le fichier /etc/sysconfig/authconfig détermine l'autorisation devant être utilisée sur l'hôte. Il contient une ou plusieurs des lignes suivantes :

- USEMD5=<*value*>, où <*value*> correspond à un des éléments ci-dessous :
  - yes — MD5 est utilisé pour l'authentification.
  - no — MD5 n'est pas utilisé pour l'authentification.

- USEKERBEROS=<*value*>, où <*value*> correspond à un des éléments ci-dessous :
  - yes — Kerberos est utilisé pour l'authentification.
  - no — Kerberos n'est pas utilisé pour l'authentification.

- USELDAPAUTH=<*value*>, où <*value*> correspond à un des éléments ci-dessous :
  - yes — LDAP est utilisé pour l'authentification.
  - no — LDAP n'est pas utilisé pour l'authentification.

4.1.5. /etc/sysconfig/autofs

Le fichier /etc/sysconfig/autofs définit les options personnalisées pour le montage automatique des périphériques. Il contrôle le fonctionnement des démons automount qui montent automatiquement des systèmes de fichiers lorsqu'ils sont utilisés et les démontent après une certaine période d'inactivité. Les systèmes de fichiers peuvent inclure des systèmes de fichiers réseau, des CD-ROM, des disquettes et bien d'autres supports.

Le fichier /etc/sysconfig/autofs peut contienir les éléments suivants :

- LOCALOPTIONS="<*value*>", où "<*value*>" représente une chaîne permettant de définir les règles automount spécifiques à la machine. La valeur par défaut est une chaîne vide ("").
- DAEMONOPTIONS="<*value*>", où "<*value*>" représente la durée du délai d'attente exprimée en secondes, avant que le périphérique ne soit démonté. La valeur par défaut est de 60 secondes ("--timeout=60").
- UNDERSCORETODOT=<*value*>, où <*value*> est une valeur binaire qui contrôle si les soulignements faisant partie dses noms de fichiers doivent être convertis en points. Par exemple, auto_home en auto.home et auto_mnt en auto.mnt. La valeur par défaut est 1 (vrai).
- DISABLE_DIRECT=<*value*>, où <*value*> est un binaire qui contrôle si la prise en charge du montage direct doit être désactivée, étant donné que l'implémentation de Linux ne se conforme

pas au comportement de automonteur de Microsystems. La valeur par défaut de 1 (vrai) permet la compatibilité avec la syntaxe de spécification des options de l'automonteur de Sun.

4.1.6. /etc/sysconfig/clock

Le fichier /etc/sysconfig/clock contrôle l'interprétation des valeurs lues à partir de l'horloge matérielle du système.

Les valeurs correctes sont les suivantes :

- UTC=<*value*>, où <*value*> correspond à l'une des valeurs booléennes suivantes :
  - true ou yes — Indique que l'horloge matérielle est réglée sur l'heure universelle (celle du méridien de Greenwich).
  - false ou no — Indique que l'horloge matérielle est réglée sur l'heure locale.

- ARC=<*value*>, où <*value*> correspond à :
  - true ou yes — Ces valeurs indiquent que le décalage de 42 ans de la console ARC est activé. Ce paramétrage ne s'applique qu'aux systèmes Aplha basés sur ARC ou AlphaBIOS.
  - false ou no — Ces valeurs indiquent que l'époque UNIX normale est utilisée.

- SRM=<*value*>, où <*value*> correspond à :
  - true ou yes — Ces valeurs indiquent que l'époque 1900 de la console SRM est activée. Ce paramétrage ne s'applique qu'aux systèmes Alpha basés sur SRM.
  - false ou no — Ces valeurs indiquent que l'époque UNIX normale est utilisée.

- ZONE=<*filename*> — Indique le fichier de fuseau horaire dans /usr/share/zoneinfo dont /etc/localtime est une copie, comme par exemple :
  ZONE="America/New York"

Des versions précédentes de Red Hat Enterprise Linux utilisaient les valeurs suivantes (qui ne sont désormais plus valables) :

- CLOCKMODE=<*value*>, où <*value*> correspond à l'une des valeurs suivantes :
  - GMT — Indique que l'horloge est réglée sur l'heure universelle (UTC : Universal Time Clock ou GMT : Greenwich Mean Time).
  - ARC — Indique que le décalage de 42 ans de la console ARC est activé (pour les systèmes basés sur Alpha seulement).

4.1.7. /etc/sysconfig/desktop

Le fichier /etc/sysconfig/desktop spécifie le bureau pour les nouveaux utilisateurs et le gestionnaire d'affichage à exécuter au niveau d'exécution 5.

Les valeurs correctes sont les suivantes :

- DESKTOP="<*value*>", où "<*value*>" correspond à l'une des valeurs suivantes :
  - GNOME — Sélectionne l'environnement de bureau GNOME.
  - KDE — Sélectionne l'environnement de bureau KDE.

- DISPLAYMANAGER="<*value*>", où "<*value*>" correspond à l'une des valeurs suivantes :
  - GNOME — Sélectionne le gestionnaire d'affichage GNOME.
  - KDE — Sélectionne le gestionnaire d'affichage KDE.
  - XDM — Sélectionne le gestionnaire d'affichage X.

Pour de plus amples informations, reportez-vous au Chapitre 7.

4.1.8. /etc/sysconfig/devlabel

Le fichier /etc/sysconfig/devlabel représente le fichier de configuration de devlabel. Il ne devrait pas être modifié manuellement, mais plutôt, configuré à l'aide de la commande /sbin/devlabel.

Afin d'obtenir des instructions sur l'utilisation de la commande devlabel, reportez-vous au chapitre intitulé *Noms de périphériques déterminés par l'utilisateur* dans le *Guide d'administration système de Red Hat Enterprise Linux*.

4.1.9. /etc/sysconfig/dhcpd

Le fichier /etc/sysconfig/dhcpd est utilisé pour transmettre des arguments au démon dhcpd lors du démarrage. Le démon dhcpd met en oeuvre les protocoles DHCP (Dynamic Host Configuration Protocol) et BOOTP (Internet Bootstrap Protocol). DHCP et BOOTP assignent des noms d'hôtes aux ordinateurs sur le réseau. Pour de plus amples informations sur les paramètres pouvant être utilisés dans ce fichier, consultez la page de manuel relative à dhcpd.

4.1.10. /etc/sysconfig/exim

Le fichier /etc/sysconfig/exim permet d'envoyer des messages à un ou plusieurs clients, en acheminant les messages sur les réseaux nécessaires, quels qu'ils soient. Le fichier définit les valeurs par défaut pour l'exécution de exim. Ses valeurs par défaut sont définies de sorte qu'il soit exécuté comme un démon en tâche de fond et que sa file d'attente soit contrôlée une fois par heure, au cas où quelque chose aurait été sauvegardé.

Parmi ces valeurs figurent :

- DAEMON=<*value*>, où <*value*> correspond à une des valeurs suivantes :
  - yes — exim doit être configuré de sorte qu'il contrôle le port 25 afin de détecter le courrier entrant. La valeur yes implique l'utilisation des options -bd de l'application exim.
  - no — exim ne doit pas être configuré pour contrôler le port 25 afin de détecter le courrier entrant.

- QUEUE=1h qui est donné à exim en tant que -q$QUEUE. L'option -q n'est pas donnée à exim si /etc/sysconfig/exim existe et si la valeur de QUEUE est vide ou non-définie.

4.1.11. /etc/sysconfig/firstboot

Lors du premier démarrage du système, le programme `/sbin/init` appelle le script `etc/rc.d/init.d/firstboot` qui à son tour lance l'**Agent de paramétrage**. Cette application permet à l'utilisateur d'installer les dernières mises à jour ainsi que les applications et la documentation supplémentaires.

Le fichier `/etc/sysconfig/firstboot` indique à l'application **Agent de paramétrage** de ne pas s'exécuter lors de prochains démarrages. Pour la lancer lors du prochain démarrage du système, supprimez `/etc/sysconfig/firstboot` et exécutez `chkconfig --level 5 firstboot on`.

4.1.12. /etc/sysconfig/gpm

Le fichier `/etc/sysconfig/gpm` est utilisé pour transmettre des arguments au démon `gpm` lors du démarrage. Le démon `gpm` est le serveur souris qui permet l'accélération de la souris et le collage en cliquant sur le bouton central de la souris. Pour obtenir de plus amples informations sur les paramètres pouvant être utilisés dans ce fichier, consultez la page de manuel de `gpm`. Par défaut, la directive `DEVICE` a la valeur `/dev/input/mice`.

4.1.13. /etc/sysconfig/harddisks

Le fichier `/etc/sysconfig/harddisks` permet de régler le ou les disque(s) dur(s). Un administrateur peut également utiliser `/etc/sysconfig/hardiskhd[a-h]` pour configurer les paramètres de disques durs spécifiques.

Avertissement

Réfléchissez bien avant d'apporter toute modification à ce fichier. En modifiant les valeurs par défaut contenues dans ce fichier, vous risquez de corrompre toutes les données stockées sur le ou les disque(s) dur(s).

Le fichier `/etc/sysconfig/harddisks` peut contenir les éléments suivants :

- `USE_DMA=1`, où la valeur 1 active l'accès direct à la mémoire (ou DMA). Néanmoins, avec certaines combinaisons jeux de puces/disque dur, cet accès direct (DMA) peut entraîner une corruption des données. *Avant de l'activer, consultez bien la documentation de votre disque dur ou demandez conseil au fabricant.* Par défaut, cette entrée est spécifiée en tant que commentaire et par conséquent désactivée.
- `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 de 30 à 50%. *Utilisez cette fonction avec prudence.* Par défaut, cette entrée est spécifiée en tant que commentaire et par conséquent désactivée.
- `EIDE_32BIT=3` active le la prise en charge des E/S (E)IDE 32-bit par une carte pour l'interface. Par défaut, cette entrée est spécifiée en tant que commentaire et par conséquent désactivée.
- `LOOKAHEAD=1` active l'anticipation en lecture du disque. Par défaut, cette entrée est spécifiée en tant que commentaire et par conséquent désactivée.
- `EXTRA_PARAMS=` précise l'endroit où des paramètres supplémentaires peuvent être ajoutés. Par défaut, aucun paramètre n'est énuméré.

4.1.14. /etc/sysconfig/hwconf

Le fichier /etc/sysconfig/hwconf affiche la liste de tout le matériel que kudzu a détecté sur l'ordinateur, ainsi que des informations sur les pilotes utilisés, l'ID du fabricant et du périphérique. Le programme kudzu détecte et configure le matériel nouveau et/ou changé sur un système. Le fichier /etc/sysconfig/hwconf n'est pas supposé être modifié manuellement. Dans le cas où il le serait, certains périphériques pourraient soudainement apparaître comme étant des p'eriphériques ajoutés ou supprimés.

4.1.15. /etc/sysconfig/i18n

Le fichier /etc/sysconfig/i18n règle la langue par défaut, toute langue prise en charge et la police de caractères par défaut. Par exemple :

```
LANG="en_US.UTF-8"
SUPPORTED="en_US.UTF-8:en_US:en"
SYSFONT="latarcyrheb-sun16"
```

4.1.16. /etc/sysconfig/init

Le fichier /etc/sysconfig/init contrôle l'aspect et le fonctionnement du système pendant le processus de démarrage.

Les valeurs suivantes peuvent être utilisées :

- BOOTUP=<*value*>, où <*value*> correspond à un des éléments suivants :
  - color — L'affichage couleur standard au démarrage, où la réussite ou l'échec de l'exécution des périphériques et des services est représentée par des couleurs différentes.
  - verbose — Un affichage de style ancien qui fournit des informations plus détaillées qu'un simple message de réussite ou d'échec.
  - Toute autre valeur indique un nouvel affichage, mais sans formatage ANSI.

- RES_COL=<*value*>, où <*value*> correspond au numéro de la colonne de l'écran où commencer les étiquettes d'état. La valeur par défaut est 60.
- MOVE_TO_COL=<*value*>, où <*value*> déplace le curseur sur la valeur indiquée dans la ligne RES_COL via la commande echo -en.
- SETCOLOR_SUCCESS=<*value*>, où <*value*> configure la couleur indiquant la réussite via la commande echo -en. Vert (green) est la couleur par défaut.
- SETCOLOR_FAILURE=<*value*>, où <*value*> configure la couleur indiquant un échec via la commande echo -en. Rouge (red) est la couleur par défaut.
- SETCOLOR_WARNING=<*value*>, où <*value*> configure la couleur indiquant un avertissement via la commande echo -en. Jaune (yellow) est la couleur par défaut.
- SETCOLOR_NORMAL=<*value*>, où <*value*> configure la couleur sur 'normal' via la commande echo -en.
- LOGLEVEL=<*value*>, où <*value*> définit le niveau de journalisation initial de la console pour le noyau. La valeur par défaut est 3 ; 8 signifie tout (y compris le débogage) alors que 1 signifie seulement les paniques du noyau. Le démon syslogd écrase ce paramètre lorsqu'il est lancé.
- PROMPT=<*value*>, où <*value*> correspond à l'une des valeurs booléennes suivantes :
  - yes — Active le contrôle du mode interactif au clavier.

- no — Désactive le contrôle du mode interactif au clavier.

4.1.17. /etc/sysconfig/ip6tables-config

Le fichier /etc/sysconfig/ip6tables-config stocke des informations utilisées par le noyau pour configurer des services de filtrage de paquets IPv6 au moment du démarrage ou chaque fois que le service ip6tables est lancé.

Ne modifiez pas ce fichier manuellement à moins que vous ne soyez familier avec la manière de construire des règles ip6tables. Il est possible de créer des règles manuellement à l'aide de la commande /sbin/ip6tables. Une fois créées, ajoutez les règles dans le fichier /etc/sysconfig/ip6tables en tapant la commande suivante :

```
/sbin/service ip6tables save
```

Une fois que ce fichier existe, toutes les règles de pare-feu sauvegardées ici seront conservées lors d'un redémarrage du système ou lors du redémarrage d'un service.

Pour de plus amples informations sur ip6tables, consultez le Chapitre 18.

4.1.18. /etc/sysconfig/iptables-config

Le fichier /etc/sysconfig/iptables stocke des informations utilisées par le noyau pour configurer des services de filtrage de paquets au démarrage ou chaque fois que le service est lancé.

Il est déconseillé de modifier ce fichier manuellement à moins que vous ne sachiez exactement comment construire des règles iptables. La manière la plus simple d'ajouter des règles consiste à utiliser l'**Outil de configuration du niveau de sécurité** (system-config-securitylevel) pour créer un pare-feu. En utilisant ces applications, ce fichier sera automatiquement modifié à la fin du processus.

Il est également possible de créer des règles manuellement à l'aide de la commande /sbin/iptables. Une fois créée(s), ajoutez la ou le(s) règle(s) au fichier /etc/sysconfig/iptables en tapant la commande suivante :

```
/sbin/service iptables save
```

Une fois que ce fichier existe, toutes les règles de pare-feu sauvegardées ici seront conservées lors d'un redémarrage du système ou lors du redémarrage d'un service.

Pour de plus amples informations sur iptables, consultez le Chapitre 18.

4.1.19. /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=<*value*>, où <*value*> correspond à une des valeurs booléennes suivantes :
  - yes — irattach est exécuté et vérifie de façon périodique si un périphérique quelconque essaie de se connecter au port infrarouge, comme par exemple, un autre ordinateur portable qui tente d'effectuer une connexion réseau. Pour que des périphériques à infrarouge fonctionnent sur le système. cette ligne doit avoir la valeur yes.

  - `no` — `irattach` n'est pas exécutée, empêchant ainsi toute communication avec les périphériques à infrarouge.

- `DEVICE=<value>`, où `<value>` correspond au périphérique (habituellement un port série) qui traite les connexions à infrarouge. Une entrée pour un périphérique série pourrait être `/dev/ttyS2`.
- `DONGLE=<value>`, où `<value>` spécifie le type de clé électronique utilisée pour une communication par infrarouge. Ce paramètre existe pour les personnes utilisant une clé électronique série plutôt que de vrais ports infrarouge. Une clé électronique est un dispositif qui est branché à un port série traditionnel pour la communication par infrarouge. Cette ligne est, par défaut, décommentée car les ordinateurs potables dotés de vrais ports à infrarouge sont beaucoup plus fréquents que ceux dotés de clés électroniques ajoutées. Une entrée pour une clé électronique pourrait être `actisys+`.
- `DISCOVERY=<value>`, où `<value>` correspond à 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 que l'élément ne prend pas l'initiative de la connexion).
  - `no` — Ne lance pas `irattach` en mode découverte.

4.1.20. `/etc/sysconfig/keyboard`

Le fichier `/etc/sysconfig/keyboard` contrôle le comportement du clavier. Il est possible d'utiliser les valeurs suivantes :

- `KEYBOARDTYPE="sun|pc"`, où la valeur `sun` signifie qu'un clavier Sun est relié à `/dev/kbd` et la valeur `pc` indique qu'un clavier PS/2 est connecté à un port PS/2.
- `KEYTABLE=<file>`, où `<file>` représente le nom d'un fichier tableau de touches (keytable).

  Comme, par exemple : `KEYTABLE="us"`. Les fichiers pouvant être utilisés comme fichiers de clavier commencent dans `/lib/kbd/keymaps/i386` et se ramifient de là, en différents types de claviers, portant tous l'étiquette `<fichier>.kmap.gz`. Le premier fichier qui se trouve sous `/lib/kbd/keymaps/i386` et qui correspond au paramètre `KEYTABLE` est utilisé.

4.1.21. `/etc/sysconfig/kudzu`

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

- `SAFE=<value>`, où `<value>` correspond à une des valeurs suivantes :
  - `yes` — `kuzdu` exécute une détection sécuritaire.
  - `no` — `kuzdu` exécute une détection normale.

4.1.22. /etc/sysconfig/mouse

Le fichier /etc/sysconfig/mouse est utilisé pour spécifier des informations sur la souris disponible. Les valeurs suivantes peuvent être utilisées :

- FULLNAME="<*value*>", où "<*value*>" fait référence au nom complet du type de souris utilisée.
- MOUSETYPE="<*value*>", où "<*value*>" correspond à un des éléments suivants :
  - imps2 — Une souris générique USB à roue.
  - 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="<*value*>", où "<*value*>" correspond à 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="<*value*>", où "<*value*>" fait référence au type de souris utilisé lors de l'exécution de X. Les options ici sont les mêmes que le paramétrage de MOUSETYPE contenus dans ce même fichier.
- DEVICE=<*value*>, où <*value*> indique périphérique de souris.

  Un exemple de valeur comme /dev/input/mice est un lien symbolique qui pointe vers le périphérique de souris spécifique.

4.1.23. /etc/sysconfig/named

Le fichier /etc/sysconfig/named est utilisé pour transmettre des arguments au démon named au moment du démarrage. Le démon named est un serveur *Domain Name System* (*DNS*) qui met en oeuvre le *Berkeley Internet Name Domain* (*BIND*) version 9. Ce serveur maintient une table dont les noms d'hôtes sont attachés à des adresses IP sur le réseau.

Actuellement, seules les valeurs suivantes peuvent être utilisées :

- ROOTDIR="<*/some/where*>", où <*/some/where*> fait référence au chemin d'accès du répertoire d'un environnement chroot sous lequel named sera exécuté. Cet environnement chroot doit préalablement être configuré. Tapez info chroot pour obtenir de plus amples informations sur la manière de procéder.
- OPTIONS="<*valeur*>", où <*value*> correspond à toute option listée dans la page de manuel relative à named, à l'exception de **-t**. Au lieu de **-t**, utilisez la ligne de commande ROOTDIR ci-dessus.

Pour obtenir de plus amples informations sur les différents paramètres pouvant être utilisés dans ce fichier, consultez la page de manuel relative à named. Pour des renseignements détaillés sur la façon de configurer un serveur BIND DNS, reportez-vous au Chapitre 12. Par défaut, le fichier ne contient aucun paramètre. Par défaut, ce fichier ne contient aucun paramètre.

4.1.24. /etc/sysconfig/netdump

Le fichier /etc/sysconfig/netdump est le fichier de configuration du service /etc/init.d/netdump. Le service netdump envoie à la fois des données 'oops' et des surplus de mémoire sur le réseau. En général, netdump n'est pas un service nécessaire ; ainsi, ne le lancez que si vous en avez absolument besoin. Pour de plus amples informations sur les paramètres que vous pouvez utiliser dans ce fichier, consultez la page de manuel relative à netdump.

4.1.25. /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=<*value*>, où <*value*> correspond à une des valeurs booléennes suivantes :
  - yes — La mise en réseau devrait être configurée.
  - no — La mise en réseau ne devrait pas être configurée.

- HOSTNAME=<*value*>, où <*value*> devrait être le *le nom de domaine complet* (*FQDN* de l'anglais Fully Qualified Domain Name), comme par exemple hostname.domain.com, mais vous pouvez tout à fait utiliser le nom d'hôte de votre choix.

  

  Remarque

  Pour assurer la compatibilité avec des logiciels plus anciens que certains utilisateurs devraient installer (comme par exemple, trn), le fichier /etc/HOSTNAME devrait contenir les mêmes valeurs que celles définies ici.

- GATEWAY=<*value*>, où <*value*> est l'adresse IP de la passerelle réseau.
- GATEWAYDEV=<*value*>, où <*value*> est le périphérique de passerelle, comme par exemple, eth0.
- NISDOMAIN=<*value*>, où <*value*> est le nom de domaine NIS.

4.1.26. /etc/sysconfig/ntpd

Le fichier /etc/sysconfig/ntpd est utilisé pour transmettre des arguments au démon ntpd au moment du démarrage. Le démon ntpd paramètre et maintient l'horloge du système pour qu'elle soit synchronisée avec un serveur de temps standard Internet. Il implémente la version 4 du protocole NTP (de l'anglais Network Time Protocol). Pour de plus amples informations sur les paramètres que vous pouvez utiliser dans ce fichier, consultez la page suivante à l'aide de votre navigateur Web : /usr/share/doc/ntp-<*version*>/ntpd.htm (où <*version*> correspond au numéro de la version de ntpd). Par défaut, ce fichier attribue la propriété du processus ntpd à l'utilisateur ntp.

4.1.27. /etc/sysconfig/pcmcia

Le fichier /etc/sysconfig/pcmcia est utilisé pour préciser des informations de configuration pour la carte PCMCIA. Il est possible d'utiliser les valeurs suivantes :

- PCMCIA=<*value*>, où <*value*> correspond à un des éléments suivants :
  - yes — La prise en charge PCMCIA doit être activée.
  - no — La prise en charge PCMCIA ne doit pas être activée.

- PCIC=<*value*>, où <*value*> correspond à un des éléments suivants :
  - i82365 — L'ordinateur a un jeu de puces de socket PCMCIA de type i82365.
  - tcic — L'ordinateur a un jeu de puces de socket PCMCIA de type tcic.

- PCIC_OPTS=<*value*>, où <*value*> correspond aux paramètres de synchronisation du pilote de socket (i82365 ou tcic).
- CORE_OPTS=<*value*>, où <*value*> correspond à la liste d'options pcmcia_core.
- CARDMGR_OPTS=<*value*>, où <*value*> correspond à la liste d'options pour le cardmgr PCMCIA (comme par exemple, -q pour le mode silencieux ; -m pour la cherche des modules de noyau chargeables dans le répertoire spécifié, etc.). Lisez la page de manuel relative à cardmgr pour obtenir de plus amples informations.

4.1.28. /etc/sysconfig/radvd

Le fichier /etc/sysconfig/radvd est utilisé pour transmettre des arguments au démon radvd au moment du démarrage. Le démon radvd est à l'écoute des requêtes du routeur et envoie des annonces pour le protocole IP version 6. Ce service permet aux hôtes sur un réseau de modifier de façon dynamique leurs routeurs par défaut, sur la base de ces annonces de routeur. Pour obtenir de plus amples informations sur les paramètres que vous pouvez utiliser dans ce fichier, consultez la page de manuel relative à radvd. Par défaut, ce fichier attribue la propriété du processus radvd à l'utilisateur radvd.

4.1.29. /etc/sysconfig/rawdevices

Le fichier /etc/sysconfig/rawdevices est utilisé pour configurer les liaisons des périphériques bruts (aussi appelés raw devices), comme par exemple :

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

4.1.30. /etc/sysconfig/samba

Le fichier /etc/sysconfig/samba est utilisé pour transmettre des arguments aux démons smbd et nmbd au moment du démarrage. Le démon smbd offre une connectivité de partage de fichiers pour les clients Windows sur le réseau. Le démon nmbd offre NetBIOS sur les services de nommage IP. Pour de plus amples informations sur les paramètres pouvant être utilisés dans ce fichier, consultez la page de manuel relative à smbd. Par défaut, ce fichier règle le fonctionnement de smbd et nmbd en mode démon.

4.1.31. /etc/sysconfig/selinux

Le fichier /etc/sysconfig/selinux contient les options de configuration élémentaires pour SELinux. Ce dernier est un lien symbolique vers /etc/selinux/config. Pour obtenir de plus amples informations sur SELinux, reportez-vous au Chapitre 21.

4.1.32. /etc/sysconfig/sendmail

Le fichier /etc/sysconfig/sendmail permet d'envoyer des messages à un ou plusieurs clients, en acheminant les messages sur les réseaux nécessaires, quels qu'ils soient. Le fichier définit les valeurs par défaut pour que l'application Sendmail soit exécutée. Ses valeurs par défaut sont déterminées de sorte que l'application soit exécutée comme un démon en tâche de fond et qu'elle contrôle sa file d'attente une fois par heure, au cas où quelque chose aurait été sauvegardé.

Parmiles valeurs figurent :

- DAEMON=<*value*>, où <*value*> correspond à une des valeurs suivantes :
  - yes — **Sendmail** doit être configuré pour contrôler le port 25 afin de détecter le courrier entrant. La valeur yes implique l'utilisation des options -bd.
  - no — **Sendmail** ne doit 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.

4.1.33. /etc/sysconfig/spamassassin

Le fichier /etc/sysconfig/spamassassin est utilisé pour transmettre des arguments au démon spamd (une version 'démonisée' de Spamassassin) lors du démarrage. Spamassassin est une application de messagerie pour le filtrage de pourriel (spam). Pour obtenir une liste des options disponibles, consultez la page de manuel de spamd. Par défaut, il configure spamd de sorte qu'il soit exécuté en mode démon, qu'il crée des préférences utilisateur et qu'il crée automatiquement des listes blanches (expéditeurs de courrier en gros autorisés).

Pour de plus amples informations sur Spamassassin, consultez la Section 11.4.2.6.

4.1.34. /etc/sysconfig/squid

Le fichier /etc/sysconfig/squid est utilisé pour transmettre des arguments au démon squid au moment du démarrage. Le démon squid est un serveur proxy de cache pour des applications clientes par le Web. Pour de plus amples informations sur la configuration d'un serveur proxy squid, ouvrez le répertoire /usr/share/doc/squid-<*version*>/ à l'aide de votre navigateur (remplacez <*version*> par le numéro de la version squid installée sur votre système). Par défaut, ce fichier règle le démarrage de squid en mode démon et détermine la durée devant s'écouler avant un arrêt automatique.

4.1.35. /etc/sysconfig/system-config-securitylevel

Le fichier /etc/sysconfig/system-config-securitylevel contient toutes les options choisies par l'utilisateur lors de la dernière exécution de l'**Outil de configuration du niveau de sécurité** (system-config-securitylevel). Il est fortement déconseillé aux utilisateurs de modifier ce fichier manuellement. Pour obtenir de plus amples informations sur l'**Outil de configuration**

du niveau de sécurité, consultez le chapitre intitulé *Configuration de base du pare-feu* du *Guide d'administration système de Red Hat Enterprise Linux*.

4.1.36. /etc/sysconfig/system-config-users

Le fichier `/etc/sysconfig/system-config-users` est le fichier de configuration pour l'application graphique **Gestionnaire d'utilisateurs**. Ce fichier est utilisé pour filtrer les utilisateurs du système tels que `root`, `daemon` ou `lp`. Ce fichier peut être édité depuis le menu déroulant **Préférences => Filtrer les utilisateurs et les groupes du système** dans le **Gestionnaire d'utilisateurs** et ne devrait jamais être modifié manuellement. Pour de plus amples informations sur l'utilisation de cette application, consultez le chapitre intitulé *Configuration des utilisateurs et des groupes* du *Guide d'administration système de Red Hat Enterprise Linux*.

4.1.37. /etc/sysconfig/system-logviewer

Le fichier `/etc/sysconfig/system-logviewer` est le fichier de configuration pour l'application graphique et interactive d'affichage de journal, **Afficheur de journal**. Ce fichier peut être édité depuis le menu déroulant **Éditer => Préférences** dans l'**Afficheur de journal** et ne doit pas être modifié manuellement. Pour de plus amples informations sur l'utilisation de cette application, consultez le chapitre intitulé *Fichiers journaux* du *Guide d'administration système de Red Hat Enterprise Linux*.

4.1.38. /etc/sysconfig/tux

Le fichier `/etc/sysconfig/tux` est le fichier de configuration de Red Hat Content Accelerator (précédemment appelé TUX), le serveur Web basé sur le noyau. Pour de plus amples informations sur la configuration de Red Hat Content Accelerator,ouvrez `/usr/share/doc/tux-<version>/tux/index.html` à l'aide de votre navigateur (remplacez `<version>` par le numéro de la version de TUX installée sur votre système). Les paramètres disponibles pour ce fichier sont énumérés dans `/usr/share/doc/tux-<version>/tux/parameters.html`.

4.1.39. /etc/sysconfig/vncservers

Le fichier `/etc/sysconfig/vncservers` configure la façon dont le serveur *Virtual Network Computing* (ou *VNC*) démarre.

VNC est un système d'affichage à distance qui vous permet de visualiser un environnement de bureau non seulement sur l'ordinateur où il est exécuté mais également sur différents réseaux présents sur des architectures variées.

Ce dernier peut contenir les éléments suivants :

- `VNCSERVERS=<value>`, où `<value>` est réglée sur une valeur de type `"1:fred"`, pour indiquer qu'un serveur VNC devrait être démarré par l'utilisateur fred sur l'écran :1. L'utilisateur fred doit avoir configuré un mot de passe VNC en utilisant la commande `vncpasswd` avant d'essayer de se connecter au serveur VNC distant.

Remarquez bien que lors de l'utilisation d'un serveur VNC, la communication que vous établissez avec le serveur n'est pas cryptée. Il est par conséquent vivement déconseillé de l'utiliser sur un réseau non sécurisé. Pour des instructions spécifiques sur l'utilisation de SSH pour sécuriser la communication avec le serveur VNC, lisez les informations disponibles en ligne à l'adresse suivante : http://www.uk.research.att.com/archive/vnc/sshvnc.html. Pour de plus amples informations sur SSH, reportez-vous au Chapitre 20 du *Guide d'administration système de Red Hat Enterprise Linux*.

4.1.40. /etc/sysconfig/xinetd

Le fichier /etc/sysconfig/xinetd est utilisé pour transmettre des arguments au démon xinetd au moment du démarrage. Le démon xinetd lance des programmes qui fournissent des services Internet lorsqu'une requête est reçue sur le port pour ce service. Pour des plus amples informations sur les paramètres que vous pouvez utiliser dans ce fichier, consultez la page de manuel de xinetd. Pour des plus amples informations sur le service xinetd, consultez la Section 17.3.

4.2. Répertoires contenus dans le répertoire /etc/sysconfig/

Les répertoires suivants se trouvent normalement dans /etc/sysconfig/.

- apm-scripts — Ce répertoire contient le script APM suspendre/reprendre. Il est déconseillé d'éditer directement ce fichier. Si vous devez le personnaliser, il suffit de créer un fichier nommé /etc/sysconfig/apm-scripts/apmcontinue qui estinvoqué à la fin du script. Vous pouvez également contrôler le script en éditant /etc/sysconfig/apmd.
- cbq — Ce répertoire contient les fichiers de configuration nécessaires pour le *Class Based Queuing* (rangement selon la classe) pour la gestion de la largeur de bande sur les interfaces réseau. CBQ organise le trafic des utilisateurs en une hiérarchie de classes basée sur une combinaison quelconque des éléments adresse IP, protocoles et types d'applications.
- networking/ — Ce répertoire est utilisé par l'**Outil d'administration réseau** (sytem-config-network) et son contenu ne devrait pas être modifié manuellement. Pour de plus amples informations sur la configuration des interfaces réseau à l'aide de l'**Outil d'administration réseau**, consultez le chapitre intitulé *Configuration réseau* du *Guide d'administration système de Red Hat Enterprise Linux*.
- network-scripts — Ce répertoire contient les fichiers de configuration relatifs au réseau ci-dessous :
  - Les fichiers de configuration réseau pour chaque interface réseau configurée, comme par exemple, ifcfg-eth0 pour l'interface Ethernet eth0.
  - Les scripts utilisés pour activer et désactiver des interfaces réseau, comme par exemple, ifup et ifdown.
  - Les scripts utilisés pour activer et désactiver des interfaces réseau ISDN, comme par exemple, ifup-isdn et ifdown-isdn
  - Divers scripts de fonctions réseau partagés, qu'il est vivement déconseillé de modifier directement.

  Pour de plus amples informations sur le répertoire network-scripts/, consultez le Chapitre 8.
- rhn/ — Ce répertoire contient les fichiers de configuration ainsi que les clés GPG pour Red Hat Network. Aucun fichier de ce répertoire ne devrait être édité manuellement. Pour de plus amples informations sur Red Hat Network, consultez son site Web de Red Hat Network à l'adresse suivante : https://rhn.redhat.com/.

4.3. Ressources supplémentaires

L'intention de ce chapitre est seulement de fournir une introduction aux fichiers contenus dans le répertoire /etc/sysconfig/. Pour obtenir des renseignements plus détaillés, consultez la source d'informations mentionnée ci-dessous.

4.3.1. Documentation installée

- /usr/share/doc/initscripts-<*version-number*>/sysconfig.txt — Ce fichier contient une liste plus complète des fichiers se trouvant dans le répertoire /etc/sysconfig/ et des options qu'ils acceptent. L'élément <*version-number*> dans le chemin d'accès vers ce fichier correspond à la version installée du paquetage initscripts.

Chapitre 5.

Système de fichiers `proc`

Le noyau de Linux a deux fonctions principales : contrôler l'accès aux périphériques physiques de l'ordinateur d'une part et programmer à quel moment et de quelle façon les processus vont interagir avec ces périphériques d'autre part. Le répertoire `/proc/` — également appelé le système de fichiers `proc` — contient une hiérarchie de fichiers spéciaux qui représentent l'état actuel du noyau ; permettant ainsi aux applications et aux utilisateurs d'obtenir un aperçu du système du point du vue du noyau.

Le répertoire `/proc/` contient de nombreuses informations relatives à la configuration matérielle du système et aux processus en cours d'exécution. De plus, certains des fichiers situés dans l'arborescence du répertoire `/proc/` peuvent être manipulés par les utilisateurs ainsi que par les applications afin de transmettre des changements de configuration au noyau.

5.1. Système de fichiers virtuel

Sous Linux, toutes les données sont stockées en tant que fichiers. La plupart des utilisateurs sont familiers avec les deux principaux types de fichiers : texte et binaire. Mais le répertoire `/proc/` contient un autre type de fichier nommé *fichier virtuel*. Telle est la raison pour laquelle on fait souvent référence à `/proc/` en tant que *système de fichiers virtuel*.

Ces fichiers virtuels ont des qualités uniques. La plupart d'entre eux ont une taille égale à zéro octet ; pourtant, lorsqu'on les affiche, on constate qu'ils contiennent parfois une grande quantité d'informations. De plus, la plupart du temps, les paramètres concernant la date et l'heure des fichiers virtuels reflètent la date et l'heure actuelles, ce qui prouve qu'ils sont constamment mis à jour.

Des fichiers virtuels tels que `/proc/interrupts`, `/proc/meminfo`, `/proc/mounts` et `/proc/partitions` fournissent un aperçu du matériel d'un système à un moment donné. D'autres tels que le fichier `/proc/filesystems` et le répertoire `/proc/sys/` fournissent des informations sur la configuration du système et sur les interfaces.

Dans un souci d'organisation, les fichiers qui contiennent des informations sur un sujet similaire sont groupés dans des répertoires et sous-répertoires virtuels. Par exemple, `/proc/ide/` contient des informations se rapportant à tous les périphériques IDE. De même, les répertoires de processus contiennent des données concernant tous les processus en cours d'exécution sur le système.

5.1.1. Affichage de fichiers virtuels

En appliquant les commandes `cat`, `more` ou `less` aux fichiers du répertoire `/proc/`, les utilisateurs ont immédiatement accès à un grand nombre d'informations sur le système. Par exemple, pour afficher le type d'unité centrale dont dispose l'ordinateur, tapez `cat /proc/cpuinfo` et une sortie semblable à l'extrait ci-dessous s'affichera :

```
processor : 0
vendor_id : AuthenticAMD
cpu family : 5
model  : 9
model name : AMD-K6(tm) 3D+ Processor
stepping : 1
cpu MHz  : 400.919
cache size : 256 KB
fdiv_bug : no
hlt_bug  : no
```

```
f00f_bug : no
coma_bug : no
fpu  : yes
fpu_exception : yes
cpuid level : 1
wp  : yes
flags  : fpu vme de pse tsc msr mce cx8 pge mmx syscall 3dnow k6_mtrr
bogomips : 799.53
```

Lors de l'affichage de différents fichiers virtuels du système de fichiers `/proc/`, certaines informations sont facilement compréhensibles alors que d'autres ne le sont pas. C'est en partie la raison poue laquelle il existe des utilitaires dont la fonction consiste à extraire des données de fichiers virtuels pour les afficher ensuite de façon compréhensible. Parmi ces utilitaires figurent par exemple : `lspci`, `apm`, `free` et `top`.

Remarque

Certains des fichiers virtuels du répertoire `/proc/` ne peuvent être lus que par l'utilisateur root.

5.1.2. Modification de fichiers virtuels

D'une manière générale, la plupart des fichiers virtuels du répertoire `/proc/` sont en lecture-seule. Toutefois, certains peuvent être utilisés pour régler des paramètres dans le noyau. C'est le cas en particulier des fichiers du sous-répertoire `/proc/sys/`.

Pour modifier la valeur d'un fichier virtuel, utilisez la commande `echo` et le signe supérieur (>) afin de réacheminer la nouvelle valeur vers le fichier. Par exemple, pour modifier votre nom d'hôte à la volée, tapez :

```
echo www.example.com > /proc/sys/kernel/hostname
```

D'autres fichiers servent de commutateur binaire ou booléen. Par exemple, la saisie de `cat /proc/sys/net/ipv4/ip_forward`, renvoie comme sortie un `0` ou un `1`. Le `0` indique que le noyau ne réachemine pas les paquets réseau. En utilisant la commande `echo` pour changer la valeur du fichier `ip_forward` en `1` afin que les paquets soient immédiatement réacheminés.

Astuce

La commande `/sbin/sysctl` permet également de modifier les paramètres du sous-répertoire `/proc/sys/`. Pour obtenir davantage d'informations sur cette commande, reportez-vous à la Section 5.4.

Pour obtenir une liste de certains des fichiers de configuration du noyau qui sont disponibles dans `/proc/sys/`, consultez la Section 5.3.9.

5.2. Fichiers de niveau supérieur dans le système de fichiers proc

Ci-dessous figure une liste de certains des fichiers virtuels les plus utiles qui se trouvent au niveau supérieur du répertoire /proc/.

Remarque

Dans la plupart des cas, le contenu des fichiers répertoriés dans cette section sera différent de celui des fichiers présents sur votre ordinateur. En effet, une bonne partie des informations est spécifique au matériel sur lequel Red Hat Enterprise Linux est exécuté pour ces besoins de documentation.

5.2.1. /proc/apm

Ce fichier qui fournit des informations sur l'état du système de *gestion de la consommation d'énergie (APM)* (de l'anglais Advanced Power Management) est utilisé par la commande apm. Si le système sans batterie est connecté à une source d'alimentation de courant alternatif, ce fichier virtuel sera similaire à l'extrait ci-dessous :

```
1.16 1.2 0x07 0x01 0xff 0x80 -1% -1 ?
```

L'exécution de la commande apm -v sur un tel système renvoie une sortie semblable à celle reproduite ci-dessous :

```
APM BIOS 1.2 (kernel driver 1.16ac)
AC on-line, no system battery
```

Pour les systèmes n'utilisant pas de batterie comme source d'alimentation, apm ne peut guère faire plus que de mettre l'ordinateur en mode veille. La commande apm est beaucoup plus utile sur les portables. Ci-dessous se trouve l'exemple d'une sortie renvoyée par la commande cat /proc/apm exécutée sur un ordinateur portable lorsqu'il est branché à une prise de courant :

```
1.16 1.2 0x03 0x01 0x03 0x09 100% -1 ?
```

Lorsque ce portable est débranché de sa source d'alimentation pendant quelques minutes, le contenu du fichier apm change de la manière suivante :

```
1.16 1.2 0x03 0x00 0x00 0x01 99% 1792 min
```

La commande apm -v va à présent générer des données plus utiles, comme par exemple :

```
APM BIOS 1.2 (kernel driver 1.16)
AC off-line, battery status high: 99% (1 day, 5:52)
```

5.2.2. /proc/buddyinfo

Ce fichier est utilisé essentiellement pour diagnostiquer des problèmes de fragmentation de mémoire. En utilisant l'algorithme d'allocation de mémoire buddy (aussi appelé algorithme des 'frères siamois') chaque colonne représente le nombre de pages d'un certain ordre (d'une certaine taille) qui sont disponibles à tout moment donné. Par exemple, pour la zone DMA (direct memory access ou accès direct à la mémoire), il y a 90 morceaux de mémoire de 2^ (0*PAGE_SIZE). De même, il y a 6 morceaux de 2^(1*PAGE_SIZE) et 2 morceaux de 2^(2*PAGE_SIZE) disponibles.

La rangée DMA référence les 16 premiers méga-octets sur un système, la rangée Normal référence toute la mémoire entre les deux et finalement la rangée HighMem elle référence toute la mémoire supérieure à 4 Go sur un système.

Ci-dessous figure un exemple de sortie typique d'un fichier /proc/buddyinfo :

```
Node 0, zone      DMA     90      6      2      1      1      ...
Node 0, zone   Normal   1650    310      5      0      0      ...
Node 0, zone  HighMem      2      0      0      1      1      ...
```

5.2.3. /proc/cmdline

Ce fichier montre les paramètres transmis au noyau au moment du démarrage. Un exemple de fichier /proc/cmdline ressemble à l'exemple ci-dessous :

```
ro root=/dev/VolGroup00/LogVol00 rhgb quiet 3
```

Cet extrait indique que le noyau est monté en lecture-seule (comme l'indique la mention (ro)), qu'il se trouve sur le premier volume logique (LogVol00) du premier groupe de volumes (/dev/VolGroup00). Le volume logique LogVol00 est l'équivalent d'une partition de disque dans un système n'utilisant pas la gestion de volumes logiques LVM (ou Logical Volume Management), de même que /dev/VolGroup00 est semblable au concept de partition /dev/hda1, mais de manière beaucoup plus extensible.

Consultez l'adresse suivante : http://www.tldp.org/HOWTO/LVM-HOWTO/index.html pour obtenir de plus amples informations sur LVM utilisé avec Red Hat Enterprise Linux.

Ensuite, rhgb signale que le paquetage rhgb a été installé et que le démarrage en mode graphique et pris en charge à condition que /etc/inittab indique un niveau d'exécution (runlevel) par défaut équivalent à id:5:initdefault:.

Finalement, quiet indique que tous les messages prolixes du noyau sont supprimés au démarrage.

5.2.4. /proc/cpuinfo

Ce fichier virtuel identifie le type de processeur utilisé par votre système. L'extrait ci-dessous montre un exemple de la sortie typique de /proc/cpuinfo :

```
processor : 0
vendor_id : GenuineIntel
cpu family : 15
model  : 2
model name : Intel(R) Xeon(TM) CPU 2.40GHz
stepping : 7
cpu MHz  : 2392.371
cache size : 512 KB
physical id : 0
siblings : 2
runqueue : 0
fdiv_bug : no
hlt_bug  : no
f00f_bug : no
coma_bug : no
fpu  : yes
fpu_exception : yes
cpuid level : 2
wp  : yes
```

```
flags  : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm
bogomips : 4771.02
```

- `processor` — Fournit à chaque processeur un numéro d'identification. Sur les systèmes dotés d'un seul processeur, seul le numéro `0` sera présent.
- `cpu family` — Identifie avec certitude le type de processeur dont votre système dispose. Si vous disposez d'un système Intel, placez simplement ce numéro devant "86" afin de déterminer la valeur. Cela est particulièrement utile si vous essayez d'identifier l'architecture d'un système plus ancien, comme 586, 486 ou 386. Comme certains paquetages RPM sont compilés pour chacune de ces architectures particulières, cette valeur vous indique également quel paquetage installer.
- `model name` — Affiche le nom communément utilisé du processeur, de même que son nom de projet.
- `cpu MHz` — Indique la vitesse précise en mégahertz du processeur, au centième près.
- `cache size` — Indique la quantité de mémoire cache de niveau 2 disponible pour le processeur.
- `siblings` — Affiche le nombre de CPU de la même famille sur le même CPU physique pour les architectures qui utilisent l'hyperthreading.
- `flags` — Définit un certain nombre de caractéristiques du processeur, telles que la présence d'une unité de virgule flottante (ou FPU, de l'anglais Floating Point Unit) et la capacité à traiter des instructions MMX.

5.2.5. `/proc/crypto`

Ce fichier dresse la liste de tous les chiffres de cryptographie utilisés par le noyau Linux, y compris des informations supplémentaires pour chacun d'eux. Un exemple de fichier `/proc/crypto` ressemble à l'exemple ci-dessous :

```
name         : sha1
module       : kernel
type         : digest
blocksize    : 64
digestsize   : 20

name         : md5
module       : md5
type         : digest
blocksize    : 64
digestsize   : 16
```

5.2.6. `/proc/devices`

Ce fichier affiche les divers périphériques d'entrée-sortie de caractères et périphériques blocs actuellement configurés (il ne contient pas les périphériques dont les modules ne sont pas chargés). Ci-dessous figure un exemple de ce fichier :

```
Character devices:
  1 mem
  4 /dev/vc/0
  4 tty
  4 ttyS
```

```
  5 /dev/tty
  5 /dev/console
  5 /dev/ptmx
  7 vcs
 10 misc
 13 input
 29 fb
 36 netlink
128 ptm
136 pts
180 usb

Block devices:
  1 ramdisk
  3 ide0
  9 md
 22 ide1
253 device-mapper
254 mdp
```

La sortie de `/proc/devices` inclut le nombre ainsi que le nom principal du périphérique ; elle est répartie en deux sections principales : `Character devices` (périphériques d'entrée-sortie de caractères) et `Block devices` (périphériques blocs).

Les *périphériques d'entrée-sortie de caractères* sont semblables aux *périphériques blocs*, à l'exception de deux points essentiels :

1. Les périphériques d'entrée-sortie de caractères ne nécessitent pas de tamponnement. Les périphériques blocs ont un tampon disponible, ce qui leur permet de classer les demandes avant de les traiter. Ceci est très important pour les périphériques conçus pour stocker des informations — tels que les disques durs — parce que la possibilité de classer les informations avant de les écrire sur le périphérique permet de les placer de façon plus efficace.
2. Les périphériques d'entrée-sortie de caractères envoient des données sans taille préconfigurée. Les périphériques blocs peuvent envoyer et recevoir les informations par blocs d'une taille configurée individuellement pour chaque périphérique.

Pour davantage d'informations sur les périphériques, consultez la documentation installée dont la référence figure ci-dessous :

`/usr/share/doc/kernel-doc-<`*version*`>/Documentation/devices.txt`

5.2.7. `/proc/dma`

Ce fichier contient une liste des canaux ISA DMA (accès direct à la mémoire) enregistrés qui sont utilisés. Un exemple de fichier `/proc/dma` ressemble à l'exemple ci-dessous :

```
 4: cascade
```

5.2.8. `/proc/execdomains`

Ce fichier fournit la liste des *domaines d'exécution* actuellement pris en charge par le noyau Linux, ainsi que la gamme des personnalités qu'ils prennent en charge.

```
0-0   Linux           [kernel]
```

Considérez les domaines d'exécution comme étant la "personnalité" d'un système d'exploitation donné. Parce que d'autres formats binaires, tels que Solaris, UnixWare et FreeBSD peuvent être utilisés avec Linux, les programmeurs peuvent, en changeant la personnalité d'une tâche, changer la façon dont le système d'exploitation traite certains appels système de ces binaires. À l'exception du domaine d'exécution PER_LINUX, différentes personnalités peuvent être mises en oeuvre en tant que modules dynamiquement chargeables.

5.2.9. /proc/fb

Ce fichier contient une liste des périphériques de mémoire vidéo (frame buffer), comportant le numéro de chaque périphérique et le pilote qui le contrôle. La sortie de /proc/fb pour les systèmes qui contiennent des périphériques de mémoire vidéo ressemble généralement à l'exemple ci-dessous :

```
0 VESA VGA
```

5.2.10. /proc/filesystems

Ce fichier affiche une liste des types de systèmes de fichiers actuellement pris en charge par le noyau. Ci-dessous figure un exemple de sortie d'un fichier /proc/filesystems générique :

```
nodev   sysfs
nodev   rootfs
nodev   bdev
nodev   proc
nodev   sockfs
nodev   binfmt_misc
nodev   usbfs
nodev   usbdevfs
nodev   futexfs
nodev   tmpfs
nodev   pipefs
nodev   eventpollfs
nodev   devpts
        ext2
nodev   ramfs
nodev   hugetlbfs
        iso9660
nodev   mqueue
        ext3
nodev   rpc_pipefs
nodev   autofs
```

La première colonne indique si le système de fichiers est monté sur un périphérique bloc. Ceux commençant par nodev ne sont pas montés sur un périphérique. La seconde colonne répertorie les noms de systèmes de fichiers pris en charge.

La commande mount tourne en boucle dans ces systèmes de fichiers lorsqu'aucun d'eux n'est spécifié comme argument.

5.2.11. /proc/interrupts

Ce fichier enregistre le nombre d'interruptions par IRQ sur l'architecture x86. Un fichier `/proc/interrupts` standard ressemble à l'extrait suivant :

```
           CPU0
  0:   80448940          XT-PIC  timer
  1:     174412          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          1          XT-PIC  rtc
 10:     410964          XT-PIC  eth0
 12:      60330          XT-PIC  PS/2 Mouse
 14:    1314121          XT-PIC  ide0
 15:    5195422          XT-PIC  ide1
NMI:          0
ERR:          0
```

Dans le cas d'un ordinateur ayant plusieurs processeurs, le fichier peut être légèrement différent :

```
           CPU0       CPU1
  0: 1366814704          0          XT-PIC  timer
  1:        128        340    IO-APIC-edge  keyboard
  2:          0          0          XT-PIC  cascade
  8:          0          1    IO-APIC-edge  rtc
 12:       5323       5793    IO-APIC-edge  PS/2 Mouse
 13:          1          0          XT-PIC  fpu
 16:   11184294   15940594   IO-APIC-level  Intel EtherExpress Pro 10/100 Ethernet
 20:    8450043   11120093   IO-APIC-level  megaraid
 30:      10432      10722   IO-APIC-level  aic7xxx
 31:         23         22   IO-APIC-level  aic7xxx
NMI:          0
ERR:          0
```

La première colonne fait référence au numéro de l'IRQ. Chaque unité centrale du système a sa propre colonne et son propre nombre d'interruptions par IRQ. La colonne suivante indique le type d'interruption et la dernière colonne contient le nom du périphérique situé à cette IRQ.

Chaque type d'interruptions - spécifiques à l'architecture - présentées dans ce fichier ont une signification légèrement différente. Pour les ordinateurs x86, les valeurs suivantes sont courantes :

- `XT-PIC` — Correspond aux anciennes interruptions des ordinateurs AT.
- `IO-APIC-edge` — Représente le signal de voltage sur ces transitions d'interruption allant de faible à élevé, créant une *dénivellation*, là où l'interruption a lieu ; il n'est signalé qu'une seule fois. Des interruptions de ce genre, de même que l'interruption `IO-APIC-level`, ne se rencontrent que sur des systèmes ayant des processeurs de la gamme 586 ou d'une gamme supérieure.
- `IO-APIC-level` — Génère des interruptions lorsque le signal de voltage est élevé, jusqu'à ce qu'il redevienne faible.

5.2.12. /proc/iomem

Ce fichier montre la topologie actuelle de la mémoire du système pour chacun des périphériques physiques :

```
00000000-0009fbff : System RAM
0009fc00-0009ffff : reserved
000a0000-000bffff : Video RAM area
```

```
000c0000-000c7fff : Video ROM
000f0000-000fffff : System ROM
00100000-07ffffff : System RAM
  00100000-00291ba8 : Kernel code
  00291ba9-002e09cb : 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 [FasterNet]
  ea000000-ea00007f : tulip
ffff0000-ffffffff : reserved
```

La première colonne affiche les registres de mémoire utilisés par chacun des différents types de mémoire. La seconde colonne indique le type de mémoire situé dans ces registres et précise notamment les registres de mémoire spécifiques qui sont utilisés par le noyau dans la mémoire vive du système ou, si la carte de l'interface réseau a plusieurs ports Ethernet, les registres de mémoire affectés à chaque port.

5.2.13. /proc/ioports

La sortie de `/proc/ioports` fournit une liste des fourchettes relatives aux ports actuellement enregistrés et utilisés pour les communications d'entrée et de sortie avec un périphérique. Ce fichier peut être assez long. L'exemple suivant affiche une partie d'une liste :

```
0000-001f : dma1
0020-003f : pic1
0040-005f : timer
0060-006f : keyboard
0070-007f : rtc
0080-008f : dma page reg
00a0-00bf : pic2
00c0-00df : dma2
00f0-00ff : fpu
0170-0177 : ide1
01f0-01f7 : ide0
02f8-02ff : serial(auto)
0376-0376 : ide1
03c0-03df : vga+
03f6-03f6 : ide0
03f8-03ff : serial(auto)
0cf8-0cff : PCI conf1
d000-dfff : PCI Bus #01
e000-e00f : VIA Technologies, Inc. Bus Master IDE
  e000-e007 : ide0
  e008-e00f : ide1
e800-e87f : Digital Equipment Corporation DECchip 21140 [FasterNet]
  e800-e87f : tulip
```

La première colonne indique la plage d'adresses de port d'E/S réservées au périphérique spécifié dans la seconde colonne.

5.2.14. /proc/kcore

Ce fichier qui représente la mémoire physique du système est stocké dans le format fichier core. Contrairement à la plupart des fichiers de /proc/, le fichier kcore affiche une taille. Cette valeur qui est donnée en octets est égale à la taille de la mémoire vive (RAM) utilisée plus 4 Ko.

Le contenu de ce fichier, conçu pour être examiné par un débogueur tel que gdb, est codé.

Attention

N'affichez pas le fichier virtuel /proc/kcore. Dans le cas contraire, le contenu de ce fichier submergera votre terminal de texte. Si vous ouvrez ce fichier par accident, appuyez sur les touches [Ctrl]-[C] pour arrêter le processus, puis tapez reset pour faire revenir l'invite de ligne de commande.

5.2.15. /proc/kmsg

Ce fichier est utilisé pour contenir des messages générés par le noyau. Ces messages sont ensuite récupérés par d'autres programmes, tels que /sbin/klogd ou /bin/dmesg.

5.2.16. /proc/loadavg

Ce fichier fournit un aperçu dans le temps de la moyenne de charge relative au CPU et aux ES, ainsi que des données supplémentaires utilisées par la commande uptime et par d'autres commandes. Un fichier /proc/loadavg peut ressembler à l'exemple suivant :

```
0.20 0.18 0.12 1/80 11206
```

Les trois premières colonnes mesurent l'utilisation du CPU et des ES au cours des périodes de temps allant de la dernière minutes, des cinq dernières minutes et des dix dernières minutes. La quatrième colonne indique le nombre de processus actuellement en cours d'exécution ainsi que le nombre total de processus. La dernière colonne affiche l'ID du dernier processus utilisé.

5.2.17. /proc/locks

Ce fichier affiche les fichiers actuellement verrouillés par le noyau. Le contenu de ce fichier comprend des données internes de débogage du noyau et peut varier énormément en fonction de l'utilisation du système. Ci-après figure un exemple de fichier /proc/locks d'un système peu chargé :

```
1: POSIX  ADVISORY  WRITE 3568 fd:00:2531452 0 EOF
2: FLOCK  ADVISORY  WRITE 3517 fd:00:2531448 0 EOF
3: POSIX  ADVISORY  WRITE 3452 fd:00:2531442 0 EOF
4: POSIX  ADVISORY  WRITE 3443 fd:00:2531440 0 EOF
5: POSIX  ADVISORY  WRITE 3326 fd:00:2531430 0 EOF
6: POSIX  ADVISORY  WRITE 3175 fd:00:2531425 0 EOF
7: POSIX  ADVISORY  WRITE 3056 fd:00:2548663 0 EOF
```

Chaque verrouillage a sa propre ligne qui commence par un numéro unique. La deuxième colonne indique la classe de verrouillage utilisée dans laquelle FLOCK représente les verrouillages de fichiers UNIX de type plus ancien d'un appel système flock alors que POSIX représente les verrouillages POSIX plus récents de l'appel système lockf.

La troisième colonne peut avoir deux valeurs : ADVISORY ou MANDATORY. La valeur ADVISORY signifie que le verrouillage n'empêche pas les autres personnes d'avoir accès aux données ; il ne

fait qu'empêcher d'autres tentatives de verrouillage. La valeur `MANDATORY` quant à elle, signifie qu'aucun accès aux données n'est autorisé tant que le verrouillage est en place. La quatrième colonne spécifie si le verrouillage autorise son détenteur à avoir un accès `READ` (lecture) ou `WRITE` (écriture) au fichier. La cinquième colonne montre l'ID du processus qui détient le verrouillage. La sixième colonne montre l'ID du fichier verrouillé, selon le format suivant : *PÉRIPHÉRIQUE-PRINCIPAL*:*PÉRIPHÉRIQUE-MINEUR*:*NUMÉRO-INODE*. La septième et la huitième colonnes précisent le début et la fin de la région verrouillée du fichier.

5.2.18. `/proc/mdstat`

Ce fichier contient les informations courantes sur les configurations RAID à disques multiples. Si votre système ne dispose pas de ce genre de configuration, votre fichier `/proc/mdstat` ressemblera à l'extrait suivant :

```
Personalities :
read_ahead not set
unused devices: <none>
```

Ce fichier garde l'état reproduit ci-dessus, sauf si vous créez un périphérique RAID logiciel ou `md`. Dans ce cas, vous pouvez afficher `/proc/mdstat` pour connaître l'état actuel de vos périphériques RAID `md`*X*.

Le fichier `/proc/mdstat` ci-dessous montre un système contenant `md0` configuré comme un périphérique RAID 1 et effectuant la re-synchronisation des disques :

```
Personalities : [linear] [raid1]
read_ahead 1024 sectors
md0: active raid1 sda2[1] sdb2[0] 9940 blocks [2/2] [UU] resync=1% finish=12.3min
algorithm 2 [3/3] [UUU]
unused devices: <none>
```

5.2.19. `/proc/meminfo`

Ci-dessous figure l'un des fichiers les plus communément utilisés du répertoire `/proc/` en raison des nombreuses informations importantes qu'il fournit sur l'utilisation de la mémoire vive du système.

L'échantillon ci-dessous du fichier virtuel `/proc/meminfo` provient d'un système ayant 256 Mo de mémoire vive et 512 Mo d'espace :

```
MemTotal:       255908 kB
MemFree:         69936 kB
Buffers:         15812 kB
Cached:         115124 kB
SwapCached:          0 kB
Active:          92700 kB
Inactive:        63792 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:       255908 kB
LowFree:         69936 kB
SwapTotal:      524280 kB
SwapFree:       524280 kB
Dirty:               4 kB
Writeback:           0 kB
Mapped:          42236 kB
Slab:            25912 kB
Committed_AS:   118680 kB
```

```
PageTables:       1236 kB
VmallocTotal:  3874808 kB
VmallocUsed:      1416 kB
VmallocChunk:  3872908 kB
HugePages_Total:     0
HugePages_Free:      0
Hugepagesize:     4096 kB
```

La plupart des informations de cet exemple sont utilisées par les commandes `free`, `top` et `ps`. En fait, la sortie de la commande `free` est même similaire en apparence au contenu et à la structure de `/proc/meminfo`. Mais si vous examinez directement `/proc/meminfo`, vous y trouverez davantage d'informations :

- `MemTotal` — Quantité totale de mémoire vive (exprimée en Ko).
- `MemFree` — Quantité de mémoire vive (exprimée en Ko), non-utilisée par le système.
- `Buffers` — Quantité de mémoire vive (exprimée en Ko), utilisée pour les tampons de fichiers.
- `Cached` — Quantité de mémoire vive (exprimée en Ko), utilisée comme mémoire cache.
- `SwapCached` — Quantité de mémoire vive (exprimée en Ko), utilisée comme mémoire cache.
- `Active` — Quantité totale de mémoire tampon ou de mémoire cache de pages (exprimée en Ko), en utilisation active. Il s'agit de la mémoire qui a récemment été utilisée et qui n'est généralement pas récupérée à d'autres fins.
- `Inactive` — Quantité totale de mémoire tampon ou de mémoire cache de pages (exprimée en Ko) qui est libre et disponible. Il s'agit de la mémoire qui n'a pas récemment été utilisée et qui peut être récupérée à d'autres fins.
- `HighTotal` et `HighFree` — Quantité totale et libre de mémoire qui n'est pas directement mappée dans l'espace du noyau. La valeur `HighTotal` peut varier en fonction du type de noyau utilisé.
- `LowTotal` et `LowFree` — Quantité totale et libre de mémoire qui est directement mappée dans l'espace du noyau. La valeur `LowTotal` peut varier en fonction du type de noyau utilisé.
- `SwapTotal` — Quantité totale de mémoire swap disponible (exprimée en Ko).
- `SwapFree` — Quantité totale de mémoire swap libre (exprimée en Ko).
- `Dirty` — Quantité totale de mémoire (exprimée en Ko), en attente d'écriture sur le disque.
- `Writeback` — Quantité totale de mémoire tampon (exprimée en Ko), en cours d'écriture active sur le disque.
- `Mapped` — Quantité totale de mémoire tampon (exprimée en Ko) qui a été utilisée pour établir la correspondance avec les périphériques, fichiers ou bibliothèques à l'aide de la commande `mmap`.
- `SwapCached` — Quantité de mémoire vive (exprimée en Ko), utilisée comme mémoire cache.
- `Committed_AS` — Quantité totale de mémoire (exprimée en Ko) qui est estimée nécessaire pour finir la charge de travail. Cette valeur correspond à celle du pire scénario et inclut également la mémoire de swap.
- `PageTables` — Quantité totale de mémoire (exprimée en Ko) dédiée au niveau le plus bas du tableau des pages.
- `VMallocTotal` — Quantité totale de mémoire (exprimée en Ko) de l'espace total alloué à l'adressage virtuel.
- `VMallocUsed` — Quantité totale de mémoire (exprimée en Ko), de l'espace d'adressage virtuel utilisé.
- `VMallocChunk` —Plus grand bloc contigu de mémoire (exprimée en Ko) d'espace d'adressage virtuel disponible.

- `HugePages_Total` — Nombre total de hugepages pour le système. Ce nombre est obtenu en divisant `Hugepagesize` par les méga-octets mis à part pour les hugepages spécifiées dans `/proc/sys/vm/hugetlb_pool`. *Cette statistique apparaît uniquement sur les architectures x86, Itanium et AMD64.*
- `HugePages_Free` — Nombre total de hugepages disponibles pour le système. *Cette statistique apparaît uniquement sur les architectures x86, Itanium et AMD64.*
- `Hugepagesize` — Taille de chaque unité de hugepages en kilo-octets. Par défaut, la valeur est de 4096 Ko pour les noyaux à processeur unique sur les architectures 32 bit. Pour SMP, les noyaux hugemem et AMD64, la valeur par défaut est de 2048 Ko. Pour les architectures Itanium, la valeur par défaut est de 262144 Ko. *Ce genre de statistique apparaît uniquement sur les architectures x86, Itanium et AMD64.*

5.2.20. `/proc/misc`

Ce fichier affiche la liste des pilotes divers enregistrés sur le périphérique principal divers, portant le numéro 10 :

```
 63 device-mapper
175 agpgart
135 rtc
134 apm_bios
```

La première colonne correspond au nombre mineur de chaque périphérique et la deuxième indique le pilote utilisé.

5.2.21. `/proc/modules`

Ce fichier affiche une liste de tous les modules qui ont été chargés dans le noyau. Son contenu varie en fonction de la configuration et de l'utilisation du système, mais il devrait être organisé de façon semblable à la sortie du fichier exemple `/proc/modules` ci-dessous :

Remarque

Cet exemple a été reformaté pour le rendre lisible. La plupart de ces informations peuvent être affichées à l'aide de commande `/sbin/lsmod` .

```
nfs      170109  0 -          Live 0x129b0000
lockd    51593   1 nfs,       Live 0x128b0000
nls_utf8 1729    0 -          Live 0x12830000
vfat     12097   0 -          Live 0x12823000
fat      38881   1 vfat,      Live 0x1287b000
autofs4  20293   2 -          Live 0x1284f000
sunrpc   140453  3 nfs,lockd, Live 0x12954000
3c59x    33257   0 -          Live 0x12871000
uhci_hcd 28377   0 -          Live 0x12869000
md5      3777    1 -          Live 0x1282c000
ipv6     211845 16 -          Live 0x128de000
ext3     92585   2 -          Live 0x12886000
jbd      65625   1 ext3,      Live 0x12857000
dm_mod   46677   3 -          Live 0x12833000
```

La première colonne contient le nom du module.

La deuxième colonne fait référence à la taille de la mémoire du module (exprimée en octets).

La troisième colonne énumère le nombre d'instances du module qui sont actuellement chargées. Une valeur de zéro correspond à un module qui n'est pas chargé.

La quatrième colonne indique si le module dépend de la présence d'un ou d'autres module(s) pour son fonctionnement et en dresse la liste.

La cinquième colonne dresse énumère le statut de la charge du module dans : `Live`, `Loading` ou `Unloading`, sont les seules valeurs possibles.

La sixième colonne énumère le décalage actuel de la mémoire du noyau pour les modules chargés. Ce genre d'information peut être utile à des fins de débogage ou pour des outils de profilage tels que `oprofile`.

5.2.22. `/proc/mounts`

Ce fichier fournit une liste de tous les montages utilisés par le système :

```
rootfs / rootfs rw 0 0
/proc /proc proc rw,nodiratime 0 0
none /dev ramfs rw 0 0
/dev/mapper/VolGroup00-LogVol00 / ext3 rw 0 0
none /dev ramfs rw 0 0
/proc /proc proc rw,nodiratime 0 0
/sys /sys sysfs rw 0 0
none /dev/pts devpts rw 0 0
usbdevfs /proc/bus/usb usbdevfs rw 0 0
/dev/hda1 /boot ext3 rw 0 0
none /dev/shm tmpfs rw 0 0
none /proc/sys/fs/binfmt_misc binfmt_misc rw 0 0
sunrpc /var/lib/nfs/rpc_pipefs rpc_pipefs rw 0 0
```

Cette sortie est semblable au contenu de `/etc/mtab`, mis à part que `/proc/mount` est plus actuel.

La première colonne spécifie le périphérique monté et la deuxième indique le point de montage. La troisième colonne donne le type de système de fichiers et la quatrième indique s'il est monté en lecture-seule (`ro`) ou en lecture et écriture (`rw`). Les cinquième et sixième colonnes sont des valeurs fictives conçues pour correspondre au format utilisé dans `/etc/mtab`.

5.2.23. `/proc/mtrr`

Ce fichier fait référence aux MTRR (Memory Type Range Registers) utilisés avec le système. Si l'architecture de votre système prend en charge les MTRR, votre fichier `/proc/mtrr` pourrait alors avoir l'aspect suivant :

```
reg00: base=0x00000000 (   0MB), size= 256MB: write-back, count=1
reg01: base=0xe8000000 (3712MB), size=  32MB: write-combining, count=1
```

Les MTRR sont utilisés avec les processeurs de la famille P6 d'Intel (Pentium II et supérieur) pour contrôler l'accès du processeur aux plages de mémoire. En utilisant une carte vidéo sur un bus PCI ou AGP, un fichier `/proc/mtrr` correctement configuré peut augmenter les performances de plus de 150%.

Dans la plupart des cas, cette valeur est correctement configurée par défaut. Pour obtenir davantage de renseignements sur la configuration manuelle de ce fichier, reportez-vous à l'adresse suivante :

/usr/share/doc/kernel-doc-<*version*>/Documentation/mtrr.txt

5.2.24. /proc/partitions

Ce fichier contient des informations sur l'allocation de blocs aux partitions. Un échantillonnage de ce fichier depuis un système élémentaire ressemble à l'extrait ci-dessous :

```
major minor  #blocks  name

   3     0   19531250 hda
   3     1     104391 hda1
   3     2   19422585 hda2
 253     0   22708224 dm-0
 253     1     524288 dm-1
```

La plupart des informations présentées ici ne sont pas importantes pour l'utilisateur, à l'exception des colonnes suivantes :

- `major` — Indique le nombre majeur du périphérique avec cette partition. Le nombre majeur dans `/proc/partitions`, (`3`), correspond au périphérique bloc `ide0` dans `/proc/devices`.
- `minor` — Indique le nombre mineur du périphérique avec cette partition. Cet élément permet de séparer les partitions en différents périphériques physiques et fait référence au nombre situé à la fin du nom de la partition.
- `#blocks` — Répertorie le nombre de blocs de disque physique contenus dans une partition donnée.
- `name` — Indique le nom de la partition.

5.2.25. /proc/pci

Ce fichier contient une liste complète de tous les périphériques PCI du système. Selon le nombre de périphériques PCI, `/proc/pci` peut être assez long. Ci-après se trouve un exemple de ce fichier sur un système de base :

```
  Bus  0, device   0, function  0:
    Host bridge: Intel Corporation 440BX/ZX - 82443BX/ZX Host bridge (rev 3).
      Master Capable.  Latency=64.
      Prefetchable 32 bit memory at 0xe4000000 [0xe7ffffff].
  Bus  0, device   1, function  0:
    PCI bridge: Intel Corporation 440BX/ZX - 82443BX/ZX AGP bridge (rev 3).
      Master Capable.  Latency=64.  Min Gnt=128.
  Bus  0, device   4, function  0:
    ISA bridge: Intel Corporation 82371AB PIIX4 ISA (rev 2).
  Bus  0, device   4, function  1:
    IDE interface: Intel Corporation 82371AB PIIX4 IDE (rev 1).
      Master Capable.  Latency=32.
      I/O at 0xd800 [0xd80f].
  Bus  0, device   4, function  2:
    USB Controller: Intel Corporation 82371AB PIIX4 USB (rev 1).
      IRQ 5.
      Master Capable.  Latency=32.
      I/O at 0xd400 [0xd41f].
  Bus  0, device   4, function  3:
    Bridge: Intel Corporation 82371AB PIIX4 ACPI (rev 2).
      IRQ 9.
  Bus  0, device   9, function  0:
```

```
    Ethernet controller: Lite-On Communications Inc LNE100TX (rev 33).
      IRQ 5.
      Master Capable.  Latency=32.
      I/O at 0xd000 [0xd0ff].
      Non-prefetchable 32 bit memory at 0xe3000000 [0xe30000ff].
Bus  0, device  12, function  0:
  VGA compatible controller: S3 Inc. ViRGE/DX or /GX (rev 1).
      IRQ 11.
      Master Capable.  Latency=32.  Min Gnt=4.Max Lat=255.
      Non-prefetchable 32 bit memory at 0xdc000000 [0xdfffffff].
```

Cette sortie affiche une liste de tous les périphériques PCI, triés par ordre de bus, périphérique et fonction. Outre la précision du nom et de la version du périphérique, cette liste fournit des informations détaillées sur les IRQ afin que l'administrateur puisse détecter rapidement tout conflit.

Astuce

Pour obtenir une version plus lisible de ce genre d'informations, tapez :

```
/sbin/lspci -vb
```

5.2.26. /proc/slabinfo

Ce fichier fournit des informations complètes sur l'utilisation de la mémoire au niveau du bloc (ou *slab*). Les noyaux Linux supérieurs à 2.2 utilisent des *slab pools* pour gérer la mémoire au-dessus du niveau page. Les objets couramment utilisés ont leurs propres groupes d'emplacement mémoire de type bloc (ou slab pools).

Au lieu d'analyser manuellement le fichier `/proc/slabinfo` qui est très prolixe, le programme `/usr/bin/slabtop` affiche en temps réel les informations de cache de l'utilisation de mémoire en bloc par le noyau. Ce programme permet d'effectuer des configurations personnalisées, y compris le classement des colonnes et le rafraîchissement d'écran.

Une capture d'écran type de `/usr/bin/slabtop` ressemble généralement à l'exemple ci-dessous :

```
Active / Total Objects (% used)    : 133629 / 147300 (90.7%)
Active / Total Slabs (% used)      : 11492 / 11493 (100.0%)
Active / Total Caches (% used)     : 77 / 121 (63.6%)
Active / Total Size (% used)       : 41739.83K / 44081.89K (94.7%)
Minimum / Average / Maximum Object : 0.01K / 0.30K / 128.00K

 OBJS ACTIVE  USE OBJ SIZE  SLABS OBJ/SLAB CACHE SIZE NAME
44814  43159  96%    0.62K   7469        6     29876K ext3_inode_cache
36900  34614  93%    0.05K    492       75      1968K buffer_head
35213  33124  94%    0.16K   1531       23      6124K dentry_cache
 7364   6463  87%    0.27K    526       14      2104K radix_tree_node
 2585   1781  68%    0.08K     55       47       220K vm_area_struct
 2263   2116  93%    0.12K     73       31       292K size-128
 1904   1125  59%    0.03K     16      119        64K size-32
 1666    768  46%    0.03K     14      119        56K anon_vma
 1512   1482  98%    0.44K    168        9       672K inode_cache
 1464   1040  71%    0.06K     24       61        96K size-64
 1320    820  62%    0.19K     66       20       264K filp
  678    587  86%    0.02K      3      226        12K dm_io
```

```
 678    587  86%    0.02K      3      226        12K dm_tio
 576    574  99%    0.47K     72        8       288K proc_inode_cache
 528    514  97%    0.50K     66        8       264K size-512
 492    372  75%    0.09K     12       41        48K bio
 465    314  67%    0.25K     31       15       124K size-256
 452    331  73%    0.02K      2      226         8K biovec-1
 420    420 100%    0.19K     21       20        84K skbuff_head_cache
 305    256  83%    0.06K      5       61        20K biovec-4
 290      4   1%    0.01K      1      290         4K revoke_table
 264    264 100%    4.00K    264        1      1056K size-4096
 260    256  98%    0.19K     13       20        52K biovec-16
 260    256  98%    0.75K     52        5       208K biovec-64
```

Parmi certaines des statistiques les plus communément utilisées qui se trouvent dans `/proc/slabinfo` et qui sont incluses dans `/usr/bin/slabtop` figurent :

- `OBJS` — Nombre total d'objets (blocs de mémoire), incluant ceux utilisés (alloués) et d'autres libres qui ne sont pas utilisés.
- `ACTIVE` — Nombre d'objets (blocs de mémoire) qui sont utilisés (alloués).
- `USE` — Pourcentage d'objets qui sont actifs. ((ACTIVE/OBJS)(100))
- `OBJ SIZE` — Taille des objets.
- `SLABS` — Nombre total de blocs.
- `OBJ/SLAB` — Nombre d'objets tenant dans un bloc.
- `CACHE SIZE` — Taille du cache du bloc.
- `NAME` — Nom du bloc.

Pour obtenir davantage d'informations sur le programme `/usr/bin/slabtop`, reportez-vous à la page de manuel de `slabtop`.

5.2.27. `/proc/stat`

Ce fichier effectue le suivi de différentes statistiques sur le système et ce, depuis le dernier redémarrage. Le contenu de `/proc/stat`, qui peut être assez long, commence normalement de la façon suivante :

```
cpu  259246 7001 60190 34250993 137517 772 0
cpu0 259246 7001 60190 34250993 137517 772 0
intr 354133732 347209999 2272 0 4 4 0 0 3 1 1249247 0 0 80143 0 422626 5169433
ctxt 12547729
btime 1093631447
processes 130523
procs_running 1
procs_blocked 0
preempt 5651840

cpu  209841 1554 21720 118519346 72939 154 27168
cpu0 42536 798 4841 14790880 14778 124 3117
cpu1 24184 569 3875 14794524 30209 29 3130
cpu2 28616 11 2182 14818198 4020 1 3493
cpu3 35350 6 2942 14811519 3045 0 3659
cpu4 18209 135 2263 14820076 12465 0 3373
cpu5 20795 35 1866 14825701 4508 0 3615
cpu6 21607 0 2201 14827053 2325 0 3334
```

```
cpu7 18544 0 1550 14831395 1589 0 3447
intr 15239682 14857833 6 0 6 6 0 5 0 1 0 0 0 29 0 2 0 0 0 0 0 0 0 94982 0 286812
ctxt 4209609
btime 1078711415
processes 21905
procs_running 1
procs_blocked 0
```

Parmi les statistiques les plus couramment utilisées figurent :

- `cpu` — Mesure le nombre de *jiffies* (en centièmes de seconde pour des systèmes x86) que le système a passé en mode utilisateur, en mode utilisateur doté d'une priorité basse (nice), en mode système, en tâche inactive, en attente d'E/S, en interruptions IRQ (hardirq) et softirq respectivement. L'interruption IRQ (hardirq) est la réponse directe à un événement matériel. Elle ne demande qu'un travail minimal pour mettre en file d'attente le travail "lourd" que la softirq doit exécuter. L'interruption softirq tourne à une priorité plus basse que l'IRQ et par conséquent sera peut-être interrompue plus fréquemment. Le total pour tous les CPU apparaît en haut alors que chaque CPU individuel est énuméré en dessous avec ses propres statistiques. L'exemple suivant étant une configuration Intel Pentium Xeon quadruple avec activation de multi-threading, il montre logiquement quatre processeurs physiques et quatre processeurs virtuels soit un total de huit processeurs.
- `page` — Nombre de pages mémoire que le système a enregistré en entrée et en sortie.
- `swap` — Nombre de pages échangées par le système.
- `intr` — Nombre d'interruptions reçues par le système.
- `btime` — Temps du démarrage, mesuré en nombre de secondes écoulées depuis le 1er janvier 1970 ; date à laquelle on fait parfois référence en tant qu'*époque*.

5.2.28. `/proc/swaps`

Ce fichier mesure l'espace swap et son utilisation. Pour un système n'ayant qu'une seule partition swap, la sortie de `/proc/swap` peut ressembler à l'extrait ci-dessous :

```
Filename                                Type        Size    Used    Priority
/dev/mapper/VolGroup00-LogVol01         partition   524280  0       -1
```

Bien qu'il soit possible de trouver une partie de ces informations dans d'autres fichiers du répertoire `/proc/`, `/proc/swap` fournit un instantané de chaque nom de fichier swap, du type d'espace swap, de la taille totale et de l'espace utilisé (exprimée en Ko). La colonne intitulée 'priority' est utile lorsque plusieurs fichiers swap sont en cours d'utilisation. Plus la priorité est basse, plus la probabilité que le fichier swap soit utilisé est élevée.

5.2.29. `/proc/sysrq-trigger`

En utilisant la commande `echo` pour écrire dans ce fichier, un super-utilisateur distant peut exécuter la plupart des commandes de touche d'interrogation système (ou System Request Key) comme s'il se trouvait sur le terminal local. Pour pouvoir transmettre des valeurs à ce fichier à l'aide de la commande `echo`, `/proc/sys/kernel/sysrq` doit avoir une valeur autre que `0`. Pour davantage d'informations sur la touche d'interrogation système, reportez-vous à la Section 5.3.9.3.

Bien qu'il soit possible d'écrire dans ce fichier, il n'est pas possible de le lire, même en tant que super-utilisateur.

5.2.30. `/proc/uptime`

Ce fichier contient des informations sur le temps de fonctionnement du système depuis le dernier redémarrage. La sortie de `/proc/uptime` est succincte :

```
350735.47 234388.90
```

Le premier nombre indique le nombre total de secondes de fonctionnement depuis le démarrage. Le second montre la partie de cette durée, exprimée en secondes, pendant laquelle l'ordinateur était inactif.

5.2.31. `/proc/version`

Ce fichier précise les versions du noyau Linux et celle de `gcc` qui sont utilisées, de même que la version de Red Hat Enterprise Linux qui est installée sur le système :

```
Linux version 2.6.8-1.523 (user@foo.redhat.com) (gcc version 3.4.1 20040714 \
 (Red Hat Enterprise Linux 3.4.1-7)) #1 Mon Aug 16 13:27:03 EDT 2004
```

Ces informations font l'objet d'utilisations variées, y compris l'affichage des données relatives à la version lorsqu'un utilisateur se connecte.

5.3. Répertoires `/proc/`

Les groupes communs d'informations sur le noyau sont regroupés en répertoires et sous-répertoires dans `/proc/`.

5.3.1. Répertoires de processus

Chaque répertoire `/proc/` contient un certain nombre de répertoires nommés à partir de chiffres. Une liste de tels répertoires pourrait ressembler à l'exemple suivant :

```
dr-xr-xr-x    3 root     root            0 Feb 13 01:28 1
dr-xr-xr-x    3 root     root            0 Feb 13 01:28 1010
dr-xr-xr-x    3 xfs      xfs             0 Feb 13 01:28 1087
dr-xr-xr-x    3 daemon   daemon          0 Feb 13 01:28 1123
dr-xr-xr-x    3 root     root            0 Feb 13 01:28 11307
dr-xr-xr-x    3 apache   apache          0 Feb 13 01:28 13660
dr-xr-xr-x    3 rpc      rpc             0 Feb 13 01:28 637
dr-xr-xr-x    3 rpcuser  rpcuser         0 Feb 13 01:28 666
```

Ces répertoires sont appelés *répertoires de processus* car ils font référence à un ID de processus et contiennent des informations se rapportant à ce dernier. Le propriétaire et le groupe de chaque répertoire de processus prennent la valeur de l'utilisateur qui exécute le processus. Lorsque le processus est terminé, son répertoire de processus `/proc/` disparaît.

Chaque répertoire de processus contient les lignes suivantes :

- `cmdline` — Contient la commande émise au début du processus.
- `cwd` — Représente un lien symbolique vers le répertoire de travail courant pour ce processus.
- `environ` — Fournit une liste des variables d'environnement du processus. La variable d'environnement est indiquée en majuscule et la valeur en minuscule.
- `exe` — Représente un lien symbolique vers le fichier exécutable de ce processus.

- `fd` — Représente un répertoire contenant tous les descripteurs de fichiers pour un processus donné. Ces derniers sont fournis sous forme de liens numérotés :

```
total 0
lrwx------    1 root     root           64 May  8 11:31 0 -> /dev/null
lrwx------    1 root     root           64 May  8 11:31 1 -> /dev/null
lrwx------    1 root     root           64 May  8 11:31 2 -> /dev/null
lrwx------    1 root     root           64 May  8 11:31 3 -> /dev/ptmx
lrwx------    1 root     root           64 May  8 11:31 4 -> socket:[7774817]
lrwx------    1 root     root           64 May  8 11:31 5 -> /dev/ptmx
lrwx------    1 root     root           64 May  8 11:31 6 -> socket:[7774829]
lrwx------    1 root     root           64 May  8 11:31 7 -> /dev/ptmx
```

- `maps` — Contient une liste des topologies de mémoire vers les divers fichiers exécutables et les fichiers bibliothèques associés à ce processus. Selon la complexité du processus, ce fichier peut être relativement long. Un exemple de sortie du processus `sshd` commence comme l'extrait reproduit ci-dessous :

```
08048000-08086000 r-xp 00000000 03:03 391479     /usr/sbin/sshd
08086000-08088000 rw-p 0003e000 03:03 391479     /usr/sbin/sshd
08088000-08095000 rwxp 00000000 00:00 0
40000000-40013000 r-xp 00000000 03:03 293205     /lib/ld-2.2.5.so
40013000-40014000 rw-p 00013000 03:03 293205     /lib/ld-2.2.5.so
40031000-40038000 r-xp 00000000 03:03 293282     /lib/libpam.so.0.75
40038000-40039000 rw-p 00006000 03:03 293282     /lib/libpam.so.0.75
40039000-4003a000 rw-p 00000000 00:00 0
4003a000-4003c000 r-xp 00000000 03:03 293218     /lib/libdl-2.2.5.so
4003c000-4003d000 rw-p 00001000 03:03 293218     /lib/libdl-2.2.5.so
```

- `mem` — Représente la mémoire occupée par le processus. Ce fichier ne peut pas être lu par l'utilisateur.
- `root` — Représente un lien vers le répertoire root du processus.
- `stat` — Montre l'état du processus.
- `statm` — Montre l'état de la mémoire utilisée par le processus. Ci-dessous figure un exemple de fichier `/proc/statm` :

```
263 210 210 5 0 205 0
```

  Les sept colonnes font référence à différentes statistiques de mémoire pour le processus. De gauche à droite, elles indiquent les aspects suivants de la mémoire utilisée :

  1. Taille totale du programme, exprimée en Ko.
  2. Taille des portions de mémoire, exprimée en Ko.
  3. Nombre de pages partagées.
  4. Nombre de pages de code.
  5. Nombre de pages de données/pile.
  6. Nombre de pages de bibliothèque.
  7. Nombre de pages incorrectes.

- `status` — Montre l'état du processus sous une forme plus lisible que `stat` ou `statm`. Un exemple de sortie de `sshd` ressemble à l'extrait ci-dessous :

```
Name: sshd
State: S (sleeping)
Tgid: 797
Pid: 797
PPid: 1
TracerPid: 0
```

```
Uid: 0 0 0 0
Gid: 0 0 0 0
FDSize: 32
Groups:
VmSize:     3072 kB
VmLck:         0 kB
VmRSS:       840 kB
VmData:      104 kB
VmStk:        12 kB
VmExe:       300 kB
VmLib:      2528 kB
SigPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: 8000000000001000
SigCgt: 0000000000014005
CapInh: 0000000000000000
CapPrm: 00000000ffffffff
CapEff: 00000000ffffffff
```

Les informations contenues dans cette sortie incluent le nom et l'ID du processus, l'état (tel que `S (sleeping)` pour le mode veille, ou `R (running)` pour une exécution en cours), l'ID de l'utilisateur/du groupe qui exécute le processus de même que des données beaucoup plus détaillées portant sur l'utilisation de la mémoire.

5.3.1.1. /proc/self/

Le répertoire `/proc/self/` est un lien vers le processus en cours d'exécution. Cela permet à un processus de se contrôler lui-même sans avoir à connaître son ID de processus.

Dans un environnement shell, un listage du répertoire `/proc/self/` fournit le même contenu que celui du répertoire de processus pour ce processus spécifique.

5.3.2. /proc/bus/

Ce répertoire contient des informations spécifiques aux divers bus disponibles sur le système. Par exemple, sur un système standard comportant des bus PCI et USB, les données actuelles relatives à chacun de ces bus se trouvent dans un sous-répertoire de `/proc/bus/` portant le même nom, comme par exemple `/proc/bus/pci/`.

Les sous-répertoires et les fichiers disponibles sous `/proc/bus/` dépendent des périphériques connectés au système. Toutefois, chaque type de bus possède au moins un répertoire. Sous ces répertoires de bus se trouve normalement au moins un sous-répertoire nommé à partir de chiffres, tel que `001`, qui contient des fichiers binaires.

Par exemple, le sous-répertoire `/proc/bus/usb/` contient des fichiers qui référencent les différents périphériques sur tout bus USB, ainsi que les pilotes dont ils ont besoin. Ci-après figure un exemple du répertoire `/proc/bus/usb/` :

```
total 0
dr-xr-xr-x    1 root     root            0 May  3 16:25 001
-r--r--r--    1 root     root            0 May  3 16:25 devices
-r--r--r--    1 root     root            0 May  3 16:25 drivers
```

Le répertoire `/proc/bus/usb/001/` contient tous les périphériques présents sur le premier bus USB. Le fichier `devices` identifie le concentrateur root USB sur la carte mère.

Ci-après figure l'exemple d'un fichier `/proc/bus/usb/devices` :

```
T:  Bus=01 Lev=00 Prnt=00 Port=00 Cnt=00 Dev#=  1 Spd=12  MxCh= 2
B:  Alloc=  0/900 us ( 0%), #Int=  0, #Iso=  0
D:  Ver= 1.00 Cls=09(hub  ) Sub=00 Prot=00 MxPS= 8 #Cfgs=  1
P:  Vendor=0000 ProdID=0000 Rev= 0.00
S:  Product=USB UHCI Root Hub
S:  SerialNumber=d400
C:* #Ifs= 1 Cfg#= 1 Atr=40 MxPwr=  0mA
I:  If#= 0 Alt= 0 #EPs= 1 Cls=09(hub  ) Sub=00 Prot=00 Driver=hub
E:  Ad=81(I) Atr=03(Int.) MxPS=   8 Ivl=255ms
```

5.3.3. /proc/driver/

Ce répertoire contient des informations sur des pilotes spécifiques utilisés par le noyau.

À cet endroit se trouve `rtc`, un fichier commun qui fournit une sortie provenant du pilote pour l'*horloge temps réel (RTC)* (de l'anglais Real Time Clock) du système, le dispositif qui maintient l'heure lorsque le système est éteint. Ci-après figure un exemple de sortie de `/proc/driver/rtc` :

```
rtc_time        : 16:21:00
rtc_date        : 2004-08-31
rtc_epoch       : 1900
alarm           : 21:16:27
DST_enable      : no
BCD             : yes
24hr            : yes
square_wave     : no
alarm_IRQ       : no
update_IRQ      : no
periodic_IRQ    : no
periodic_freq   : 1024
batt_status     : okay
```

Pour davantage d'informations sur l'horloge temps réel (ou RTC), consultez la documentation installée dont la référence apparaît ci-dessous :

`/usr/share/doc/kernel-doc-<version>/Documentation/rtc.txt`.

5.3.4. /proc/fs

Ce répertoire montre les systèmes de fichiers spécifiques qui sont exportés. Lors de l'exécution d'un serveur NFS, la saisie de la commande `cat /proc/fs/nfs/exports` permet d'afficher les systèmes de fichiers qui sont partagés ainsi que les permissions accordées pour ces derniers. Pour obtenir davantage d'informations sur le partage des systèmes de fichiers avec NFS, consultez le Chapitre 9.

5.3.5. /proc/ide/

Ce répertoire contient des informations sur les périphériques IDE du système. Chaque canal IDE est représenté par un répertoire séparé, tel que `/proc/ide/ide0` et `/proc/ide/ide1`. De plus, un fichier `drivers` est disponible ; il fournit le numéro de version des divers pilotes utilisés sur les canaux IDE :

```
ide-floppy version 0.99.newide
ide-cdrom version 4.61
ide-disk version 1.18
```

Plusieurs jeux de puces (ou chipsets) fournissent également dans ce répertoire un fichier qui donne des renseignements supplémentaires sur les lecteurs connectés via les canaux. Par exemple, un jeu de puces générique Ultra 33 PIIX4 d'Intel produit un fichier `/proc/ide/piix` qui indique si le DMA ou l'UDMA est activé pour les périphériques présents sur les canaux IDE :

```
                                Intel PIIX4 Ultra 33 Chipset.
------------- Primary Channel ---------------- Secondary Channel -------------
                 enabled                          enabled
------------- drive0 --------- drive1 -------- drive0 ---------- drive1 ------
DMA enabled:    yes              no              yes               no
UDMA enabled:   yes              no              no                no
UDMA enabled:   2                X               X                 X
UDMA
DMA
PIO
```

En navigant dans le répertoire pour trouver un canal IDE, tel que `ide0`, vous pouvez obtenir des informations supplémentaires. Le fichier `channel` indique le numéro de canal, alors que `model` indique le type de bus pour ce canal (tel que `pci`).

5.3.5.1. Répertoires de périphériques

À l'intérieur de chaque répertoire de canal IDE se trouve un répertoire de périphérique. Le nom du répertoire de périphérique correspond à la lettre du périphérique dans le répertoire `/dev/`. Par exemple, le premier périphérique IDE sur `ide0` serait `hda`.

Remarque

Il existe un lien symbolique pour chacun de ces répertoires de périphériquedans le répertoire `/proc/ide/`.

Chaque répertoire de périphérique contient un recueil d'informations et de statistiques. Le contenu de ces répertoires varie selon le type de périphérique connecté. Parmi les fichiers les plus utiles et qui sont communs à de nombreux périphériques figurent :

- `cache` — Le cache du périphérique ;
- `capacity` — La capacité du périphérique, en blocs de 512 octets ;
- `driver` — Le pilote et la version utilisés pour contrôler le périphérique ;
- `geometry` — La géométrie physique et logique du périphérique ;
- `media` — Le type de périphérique, comme par exemple `disk`.
- `model` — Le nom ou le numéro de modèle du périphérique ;
- `settings` — Un ensemble de paramètres actuels du périphérique. Ce fichier contient généralement un certain nombre d'informations techniques utiles. Un exemple de fichier `settings` pour un disque dur IDE standard ressemble à l'extrait ci-dessous :

```
name                    value           min             max             mode
----                    -----           ---             ---             ----
acoustic                0               0               254             rw
address                 0               0               2               rw
bios_cyl                38752           0               65535           rw
```

```
bios_head           16              0           255           rw
bios_sect           63              0           63            rw
bswap               0               0           1             r
current_speed       68              0           70            rw
failures            0               0           65535         rw
init_speed          68              0           70            rw
io_32bit            0               0           3             rw
keepsettings        0               0           1             rw
lun                 0               0           7             rw
max_failures        1               0           65535         rw
multcount           16              0           16            rw
nice1               1               0           1             rw
nowerr              0               0           1             rw
number              0               0           3             rw
pio_mode            write-only      0           255           w
unmaskirq           0               0           1             rw
using_dma           1               0           1             rw
wcache              1               0           1             rw
```

5.3.6. /proc/irq/

Ce répertoire est utilisé pour paramétrer l'association IRQ-CPU, qui permet de connecter une IRQ donnée à une seule unité centrale. Il est également possible d'empêcher qu'une unité centrale gère une IRQ.

Chaque IRQ a son propre répertoire, ce qui permet une configuration individuelle de chacune d'elles. Le fichier `/proc/irq/prof_cpu_mask` est un masque de bit qui contient les valeurs par défaut pour le fichier `smp_affinity` dans le répertoire IRQ. Les valeurs de `smp_affinity` spécifient quelles unités centrales gèrent cette IRQ spécifique.

Pour obtenir davantage d'informations sur le répertoire `/proc/irq/`, reportez-vous à la documentation installée dont la référence figure suivante :

`/usr/share/doc/kernel-doc-<version>/Documentation/filesystems/proc.txt`

5.3.7. /proc/net/

Ce répertoire fournit une vision exhaustive d'un certain nombre de paramètres et de statistiques réseau. Chaque répertoire et fichier virtuel de ce répertoire décrit des aspects de la configuration réseau du système. Vous trouverez ci-dessous une liste partielle du répertoire `/proc/net/` :

- `arp` — Contient la table ARP du noyau. Ce fichier est particulièrement utile pour connecter une adresse câblée à une adresse IP sur un système.
- `atm` — Contient des fichiers avec divers paramètres et statistiques de *mode de transfert asynchrone (ATM)* (de l'anglais Asynchronous Transfer Mode). Ce répertoire est principalement utilisé pour la gestion de réseau ATM et les cartes ADSL.
- `dev` — Dresse la liste des différents périphériques réseau configurés sur le système, avec des statistiques de transmission et de réception. Ce fichier indique entre autres, le nombre d'octets que chaque interface a envoyés et reçus, le nombre de paquets entrants et sortants, le nombre d'erreurs observées, le nombre de paquets abandonnés, etc.
- `dev_mcast` — Dresse la liste des différents groupes de multidiffusion Layer2 que chaque périphérique écoute.
- `igmp` — Dresse la liste des adresses IP de multidiffusion auxquelles le système s'est joint.

- ip_conntrack — Dresse la liste des connexions réseau suivies pour les machines qui sont des connexions IP de retransmission.
- ip_tables_names — Dresse la liste des types de iptables utilisés. Ce fichier est seulement présent si les iptables sont actives sur le système et contient une ou plusieurs des valeurs suivantes : filter, mangle ou nat.
- ip_mr_cache — Affiche le cache du routeur de diffusion.
- ip_mr_vif — Dresse la liste des interfaces virtuelles de diffusion.
- netstat — Contient un ensemble large, mais détaillé, de statistiques réseau, telles que les délais d'attente TCP, les cookies SYN envoyés et reçus, etc.
- psched — Dresse la liste des paramètres du programmateur global des paquets.
- raw — Dresse la liste des statistiques brutes relatives aux périphériques.
- route — Affiche la table de routage du noyau.
- rt_cache — Contient le cache de routage actuel.
- snmp — Représente une liste de données concernant le protocole d'administration à distance de réseaux ou SNMP (de l'anglais Simple Network Management Protocol) pour divers protocoles de gestion de réseau en cours d'utilisation.
- sockstat — Fournit des statistiques sur les sockets.
- tcp — Contient des informations détaillées sur les sockets TCP.
- tr_rif — Présente la table de routage RIF du bus annulaire à jeton (token ring).
- udp — Contient des informations détaillées sur les sockets UDP.
- unix — Dresse la liste des sockets de domaine UNIX actuellement utilisés.
- wireless — Présente des données d'interface sans fil.

5.3.8. /proc/scsi/

Ce répertoire est analogue au répertoire /proc/ide/ à la différence près qu'il est réservé aux périphériques SCSI connectés.

Le fichier principal est /proc/scsi/scsi, qui contient une liste de tous les périphériques SCSI reconnus. Cette liste fournit également des informations sur le type de périphérique, ainsi que le nom de modèle, le fabricant, le canal et les données ID SCSI disponibles.

Par exemple, si un système disposait d'un CD-ROM SCSI, d'un lecteur de bande, d'un disque dur ainsi que d'un contrôleur RAID, ce fichier ressemblerait à l'extrait ci-dessous :

```
Attached devices:
Host: scsi1 Channel: 00 Id: 05 Lun: 00
  Vendor: NEC      Model: CD-ROM DRIVE:466 Rev: 1.06
  Type:   CD-ROM                           ANSI SCSI revision: 02
Host: scsi1 Channel: 00 Id: 06 Lun: 00
  Vendor: ARCHIVE  Model: Python 04106-XXX Rev: 7350
  Type:   Sequential-Access                ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 06 Lun: 00
  Vendor: DELL     Model: 1x6 U2W SCSI BP  Rev: 5.35
  Type:   Processor                        ANSI SCSI revision: 02
Host: scsi2 Channel: 02 Id: 00 Lun: 00
  Vendor: MegaRAID Model: LD0 RAID5 34556R Rev: 1.01
  Type:   Direct-Access                    ANSI SCSI revision: 02
```

Chaque pilote SCSI utilisé par le système a son propre répertoire dans `/proc/scsi/`, qui contient des fichiers spécifiques à chaque contrôleur SCSI qui utilise ce pilote. Par conséquent, dans le cas de l'exemple ci-dessus, les répertoires `aic7xxx/` et `megaraid/` sont présents, car ces deux pilotes sont utilisés. Les fichiers situés dans chacun des répertoires contiennent généralement la plage d'adresses d'E/S, les IRQ ainsi que les statistiques relatives au contrôleur SCSI qui utilise ce pilote. Chaque contrôleur peut rapporter des types et quantités d'informations différents. Le fichier du contrôleur SCSI Adaptec AIC-7880 Ultra produit dans notre exemple la sortie suivante :

```
Adaptec AIC7xxx driver version: 5.1.20/3.2.4
Compile Options:
  TCQ Enabled By Default : Disabled
  AIC7XXX_PROC_STATS     : Enabled
  AIC7XXX_RESET_DELAY    : 5

Adapter Configuration:
           SCSI Adapter: Adaptec AIC-7880 Ultra SCSI host adapter
                         Ultra Narrow Controller
    PCI MMAPed I/O Base: 0xfcffe000
 Adapter SEEPROM Config: SEEPROM found and used.
      Adaptec SCSI BIOS: Enabled
                    IRQ: 30
                   SCBs: Active 0, Max Active 1,
                         Allocated 15, HW 16, Page 255
             Interrupts: 33726
      BIOS Control Word: 0x18a6
   Adapter Control Word: 0x1c5f
   Extended Translation: Enabled
Disconnect Enable Flags: 0x00ff
     Ultra Enable Flags: 0x0020
 Tag Queue Enable Flags: 0x0000
Ordered Queue Tag Flags: 0x0000
Default Tag Queue Depth: 8
    Tagged Queue By Device array for aic7xxx host instance 1:
      {255,255,255,255,255,255,255,255,255,255,255,255,255,255,255,255}
    Actual queue depth per device for aic7xxx host instance 1:
      {1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1}

Statistics:


(scsi1:0:5:0)
  Device using Narrow/Sync transfers at 20.0 MByte/sec, offset 15
  Transinfo settings: current(12/15/0/0), goal(12/15/0/0), user(12/15/0/0)
  Total transfers 0 (0 reads and 0 writes)
             < 2K      2K+     4K+     8K+    16K+    32K+    64K+   128K+
   Reads:       0        0       0       0       0       0       0       0
  Writes:       0        0       0       0       0       0       0       0


(scsi1:0:6:0)
  Device using Narrow/Sync transfers at 10.0 MByte/sec, offset 15
  Transinfo settings: current(25/15/0/0), goal(12/15/0/0), user(12/15/0/0)
  Total transfers 132 (0 reads and 132 writes)
             < 2K      2K+     4K+     8K+    16K+    32K+    64K+   128K+
   Reads:       0        0       0       0       0       0       0       0
  Writes:       0        0       0       0       1     131       0       0
```

Cette sortie vous permet de visualiser la vitesse de transfert des différents périphériques SCSI connectés au contrôleur en fonction de l'ID de canal, ainsi que des statistiques détaillées concernant la quantité et la taille des fichiers lus ou écrits par ces périphériques. Par exemple, à partir de la sortie ci-dessus, il est possbiel de voir que ce contrôleur communique avec le CD-ROM à une vitesse de 20 Mo par seconde, alors que le lecteur de bande ne communique lui qu'à une vitesse de 10 Mo par seconde.

5.3.9. /proc/sys/

Le répertoire /proc/sys/ est différent des autres répertoires de /proc/ car il ne fournit pas seulement des informations relatives au système, il permet également d'apporter des modifications à la configuration du noyau. Ainsi, l'administrateur de l'ordinateur est en mesure d'activer et de désactiver immédiatement des fonctions du noyau.

Attention

Soyez extrêmement prudent lors de la modification de paramètres sur un système de production, en utilisant les différents fichiers du répertoire /proc/sys/. La modification d'un mauvais paramètre peut rendre le noyau instable et nécessiter le redémarrage du système.

Pour cette raison, avant de changer une valeur dans /proc/sys/, assurez-vous que les options de ce fichier sont bien valides.

Une bonne manière de déterminer si un fichier donné peut être configuré ou s'il est uniquement conçu pour fournir des informations consiste à l'afficher à l'aide de l'option -l saisie à l'invite du shell. Si le fichier peut être modifié, il peut être utilisé pour configurer le noyau. Ci-dessous figure un exemple d'affichage partiel de /proc/sys/fs :

```
-r--r--r--    1 root     root            0 May 10 16:14 dentry-state
-rw-r--r--    1 root     root            0 May 10 16:14 dir-notify-enable
-r--r--r--    1 root     root            0 May 10 16:14 dquot-nr
-rw-r--r--    1 root     root            0 May 10 16:14 file-max
-r--r--r--    1 root     root            0 May 10 16:14 file-nr
```

Dans cet exemple, les fichiers dir-notify-enable et file-max peuvent être modifiés et, par conséquent, peuvent être utilisés pour configurer le noyau. Les autres fichiers ne fournissent que des informations sur les paramètres actuels.

Pour changer une valeur dans un fichier /proc/sys/, il faut enregistrer la nouvelle valeur dans le fichier à l'aide de la commande echo. Par exemple, pour activer la touche d'interrogation système sur un noyau en cours d'exécution, tapez la commande :

```
echo 1 > /proc/sys/kernel/sysrq
```

Cette opération aura pour effet de modifier la valeur sysrq qui passera de 0 (off) à 1 (on).

Un certain nombre de fichiers de configuration /proc/sys/ contiennent plus d'une valeur. Afin de leur transmettre correctement de nouvelles valeurs, placez un espace blanc entre chaque valeur transmise à l'aide de la commande echo, comme c'est le cas dans l'exemple ci-dessous :

```
echo 4 2 45 > /proc/sys/kernel/acct
```

Remarque

Toute modification de configuration effectuée à l'aide de la commande `echo` disparaîtra lors du redémarrage du système. Pour faire en sorte que des modifications de configuration soient appliquées lors du redémarrage, reportez-vous à la Section 5.4.

Le répertoire `/proc/sys/` contient plusieurs sous-répertoires qui contrôlent différents aspects d'un noyau en cours d'exécution.

5.3.9.1. `/proc/sys/dev/`

Ce répertoire fournit des paramètres pour des périphériques particuliers du système. La plupart des systèmes ont au moins deux répertoires, à savoir `cdrom/` et `raid/`. Les noyaux personnalisés eux peuvent en avoir d'autres, tels que `parport/`, qui offre la possibilité de partager un port parallèle entre plusieurs pilotes de périphériques.

Le répertoire `cdrom/` contient un fichier appelé `info`, qui fournt un certain nombre de paramètres importants pour le CD-ROM :

```
CD-ROM information, Id: cdrom.c 3.20 2003/12/17

drive name:             hdc
drive speed:            48
drive # of slots:       1
Can close tray:         1
Can open tray:          1
Can lock tray:          1
Can change speed:       1
Can select disk:        0
Can read multisession:  1
Can read MCN:           1
Reports media changed:  1
Can play audio:         1
Can write CD-R:         0
Can write CD-RW:        0
Can read DVD:           0
Can write DVD-R:        0
Can write DVD-RAM:      0
Can read MRW:           0
Can write MRW:          0
Can write RAM:          0
```

Ce fichier peut être examiné rapidement pour découvrir les qualités d'un lecteur de CD-ROM inconnu, pour le noyau tout au moins. Si plusieurs lecteurs de CD-ROM sont disponibles sur un système, chaque périphérique dispose de sa propre colonne d'informations.

De nombreux fichiers de `/proc/sys/dev/cdrom`, tels que `autoclose` et `checkmedia`, peuvent être utilisés pour contrôler le lecteur de CD-ROM du système. Utilisez simplement la commande `echo` pour activer ou désactiver ces fonctions.

Si la prise en charge de RAID est compilée dans le noyau, un répertoire `/proc/sys/dev/raid/` sera disponible et contiendra au moins deux fichiers : `speed_limit_min` et `speed_limit_max`. Ces paramètres permettent de déterminer l'accélération des périphérique RAID pour des tâches demandant de lourdes opérations d'E/S, telles que la re-synchronisation des disques.

5.3.9.2. `/proc/sys/fs/`

Ce répertoire contient une gamme d'options et d'informations relatives à divers aspects des systèmes de fichiers, y compris des informations relatives au quota, descripteur de fichier, inode et dentry.

Le répertoire `binfmt_misc/` est utilisé pour fournir la prise en charge par le noyau de formats binaires divers.

Parmi les fichiers importants du répertoire `/proc/sys/fs/` figurent :

- `dentry-state` — Donne l'état du cache du répertoire. Le fichier ressemble à l'extrait ci-dessous :
  ```
  57411 52939 45 0 0 0
  ```
  Le premier nombre indique le nombre total d'entrées dans le cache du répertoire, alors que le deuxième indique le nombre d'entrées non-utilisées. Le troisième indique le nombre de secondes entre le moment où un répertoire a été libéré et le moment où il peut être récupéré ; le quatrième nombre mesure les pages actuellement demandées par le système. Les deux derniers nombres eux ne sont pas utilisés et n'affichent actuellement que des zéros.
- `dquot-nr` — Indique le nombre maximum d'entrées de quota de disque en cache.
- `file-max` — Indique le nombre maximum de descripteurs de fichier que le noyau attribue. L'augmentation de la valeur dans ce fichier peut aider à résoudre des erreurs causées par un manque de descripteurs de fichier disponibles.
- `file-nr` — Affiche le nombre de descripteurs de fichier alloués, le nombre de descripteurs de fichiers utilisés et le nombre maximum de descripteurs de fichier.
- `overflowgid` et `overflowuid` — Définissent respectivement l'ID groupe et l'ID utilisateur fixes et sont utilisés avec des systèmes de fichiers qui ne prennent en charge que des ID groupe et utilisateur 16 bits.
- `super-max` — Contrôle le nombre maximum de superblocs disponibles.
- `super-nr` — Affiche le nombre actuel de superblocs utilisés.

5.3.9.3. `/proc/sys/kernel/`

Ce répertoire contient divers fichiers de configuration qui affectent directement le fonctionnement du noyau. Parmi les fichiers les plus importants figurent :

- `acct` — Contrôle la suspension de la comptabilisation du processus sur la base du pourcentage d'espace libre disponible sur le système de fichiers contenant le journal. Par défaut, ce fichier ressemble à l'extrait ci-dessous :
  ```
  4 2 30
  ```
  La première valeur détermine le pourcentage nécessaire pour que la journalisation recommence alors que la deuxième valeur définit le pourcentage d'espace libre représentant le seuil à partir duquel la journalisation est suspendue. La troisième valeur définit l'intervalle en secondes selon lequel le noyau examine le système de fichiers pour voir si la journalisation devrait être suspendue ou reprise.
- `cap-bound` — Contrôle les paramètres de *délimitation des capacités* qui fournit la liste des capacités de tout processus du système. Si une capacité n'est pas incluse dans cette liste, aucun processus, quels que soient ses privilèges, ne peut l'exécuter. L'objectif est d'améliorer la sécurité du système en s'assurant que certaines choses ne puissent pas se produire, du moins au-delà d'un point donné du processus de démarrage.

  Pour obtenir une liste des valeurs pour ce fichier, consultez la documentation installée dont la référence figure ci-dessous :

  `/lib/modules/<kernel-version>/build/include/linux/capability.h`.

- ctrl-alt-del — Contrôle si [Ctrl]-[Alt]-[Suppr] redémarre correctement l'ordinateur à l'aide d'init (0) ou force un redémarrage immédiat sans synchroniser les tampons modifiés (dits dirty) vers le disque (1).
- domainname — Permet de configurer le nom de domaine du système, tel que example.com.
- exec-shield — Configure la fonction Exec Shield du noyau. Exec Shield offre une protection contre certains types d'attaques de dépassement de capacité de la mémoire tampon.

  Deux valeurs sont possibles pour ce fichier virtuel :

  - 0 — Désactive Exec Shield.
  - 1 — Active Exec Shield. Cette valeur est celle retenue par défaut.

Important

Si un système exécute des applications sensibles au niveau sécurité et que ces dernières ont été lancées alors que la fonction Exec Shield était désactivée, il est nécessaire de les redémarrées lorsqu'Exec Shield est de nouveau activée, afin que cette fonction Exec Shield puisse être appliquée.

- exec-shield-randomize — Active la fonction d'attribution d'un emplacement aléatoire à différents éléments dans la mémoire. Un tel procédé permet d'empêcher des agresseurs potentiels de localiser des programmes et démons dans la mémoire. Chaque fois qu'un programme ou démon démarre, il est stocké dans un emplacement différent de la mémoire, jamais à une adresse de mémoire statique ou absolue.

  Deux valeurs sont possibles pour ce fichier virtuel :

  - 0 — Désactive la fonction d'attribution d'un emplacement aléatoire avec Exec Shield. Cette valeur peut être utile à des fins de débogage.
  - 1 — Active la fonction d'attribution d'un emplacement aléatoire avec Exec Shield. Cette valeur est le défaut. Remarque : Le fichier exec-shield doit également être paramétré sur 1 pour que exec-shield-randomize soit activé.

- hostname — Permet de configurer le nom d'hôte du système, tel que www.example.com.
- hotplug — Configure l'utilitaire à utiliser lorsqu'un changement de configuration est détecté par le système. Il est surtout utilisé avec USB et Cardbus PCI. La valeur par défaut de /sbin/hotplug ne devrait pas être modifiée, à moins de tester un nouveau programme qui remplira cette fonction.
- modprobe — Définit l'emplacement du programme utilisé pour charger des modules du noyau. La valeur par défaut est /sbin/modprobe ce qui signifie que kmod l'appelle pour charger le module lorsqu'un thread du noyau appelle kmod.
- msgmax — Définit la taille maximum de tout message envoyé d'un processus à un autre ; sa valeur par défaut est 8192 octets. Soyez prudent lorsque vous décidez d'augmenter cette valeur car les messages mis en file d'attente entre les processus sont stockés dans la mémoire non-échangeable du noyau. Toute augmentation de msgmax augmentera également la demande de mémoire vive du système.
- msgmnb — Définit le nombre maximum d'octets dans une file d'attente de messages. La valeur par défaut est 16384.
- msgmni — Définit le nombre maximum d'identificateurs de file d'attente de messages. Par défaut, la valeur est 16.
- osrelease — Fournit le numéro de version du noyau Linux. Ce fichier ne peut être modifié qu'en changeant la source du noyau et en recompilant.

- `ostype` — Affiche le type de système d'exploitation. Par défaut, ce fichier est paramétré sur `Linux` ; cette valeur ne peut être modifiée qu'en changeant la source du noyau et en recompilant.
- `overflowgid` et `overflowuid` — Définissent respectivement l'ID groupe et l'ID utilisateur fixes ; ils sont utilisés avec des appels système sur des architectures qui ne prennent en charge que des ID groupe et utilisateur 16 bits.
- `panic` — Définit le nombre de secondes sur lequel le noyau se base pour retarder le redémarrage du sytème lorsque ce denrier subit une panique du noyau. Par défaut, la valeur est de `0`, ce qui désactive le redémarrage automatique après une panique.
- `printk` — Représente le fichier contrôlant toute une série de paramètres relatifs à l'affichage ou à la journalisation de messages d'erreur. Chaque message d'erreur rapporté par le noyau a un *niveau journal* (loglevel) qui lui est associé et qui définit son importance. Les valeurs du niveau journal s'échelonnent selon l'ordre suivant :
  - `0` — Situation d'urgence du noyau (Emergency). Le système est inutilisable.
  - `1` — Alerte du noyau (Alert). Une action immédiate est requise.
  - `2` — Condition du noyau considérée comme critique (Critical).
  - `3` — Condition générale d'erreur du noyau (Error).
  - `4` — Condition générale d'avertissement du noyau (Warning).
  - `5` — Avis du noyau d'une condition normale, mais importante (Notice).
  - `6` — Message d'information du noyau (Information).
  - `7` — Messages de niveau débogage du noyau (Debug).

  Le fichier `printk` comporte quatre valeurs :
  ```
  6     4     1     7
  ```
  Chacune de ces valeurs définit une règle différente de traitement des messages d'erreur. La première valeur, appelée *niveau journal de la console* (console loglevel), spécifie la plus basse priorité de messages qui sera affichée sur la console (veuillez noter que plus la priorité est basse, plus le numéro du niveau journal est élevé). La deuxième valeur définit le niveau journal par défaut pour les messages dépourvus de niveau journal explicite. La troisième valeur spécifie la plus basse configuration de niveau journal possible pour le niveau journal de la console. La dernière valeur définit la valeur par défaut pour le niveau journal de la console.
- Le répertoire `random/` — Stocke un certain nombre de valeurs relatives à la génération de nombres aléatoires pour le noyau.
- `rtsig-max` — Configure le nombre maximum de signaux POSIX en temps réel que le système peut avoir mis en file d'attente à tout moment donné. La valeur par défaut est `1024`.
- `rtsig-nr` — Dresse la liste du nombre actuel de signaux POSIX en temps réel mis en file d'attente par le noyau.
- `sem` — Configure les paramètres du *semaphore* au sein du noyau. Un *sémaphore* est un objet IPC System V qui est utilisé pour contrôler l'utilisation d'un processus spécifique.
- `shmall` — Définit la quantité totale de mémoire partagée, en octets, qui peut être utilisée à un moment précis sur le système. Par défaut, cette valeur est de `2097152`.
- `shmmax` — Définit la plus grande taille autorisée par le noyau d'un segment de mémoire partagée, valeur exprimée en octets. Par défaut, cette valeur est de `33554432`. Le noyau prend cependant en charge des valeurs beaucoup plus élevées.
- `shmmni` — Définit le nombre maximum de segments de mémoire partagée pour l'ensemble du système. Par défaut, cette valeur est de `4096`
- `sysrq` — Active la touche d'interrogation système (ou System Request Key), si cette valeur est autre que zéro `0`, la valeur par défaut.

La touche d'interrogation système permet l'entrée immédiate d'informations dans le noyau au moyen d'une simple combinaison de touches. Par exemple, elle peut être utilisée pour arrêter ou redémarrer immédiatement un système, synchroniser tous les systèmes de fichiers montés ou vider des informations importantes sur votre console. Pour lancer une touche d'interrogation système, tapez [Alt]-[SysRq]-[<*system request code*>]. Remplacez <*system request code*> par l'un des codes suivants :

- `r` — Désactive le mode brut du clavier et le règle sur XLATE (un mode de clavier plus limité qui ne reconnaît pas les modificateurs comme [Alt], [Ctrl] ou [Shift] pour toutes les touches).
- `k` — Arrête tous les processus actifs dans une console virtuelle. Également appelée clé d'accès sécurisé (ou *Secure Access Key*, *SAK*), cette option est souvent utilisée pour vérifier que l'invite de connexion est bien créée par `init` et qu'elle n'est pas pas une copie de cheval de Troie conçue pour intercepter les noms d'utilisateurs et les mots de passe.
- `b` — Redémarre le noyau sans préalablement démonter les systèmes de fichiers ou synchroniser les disques connectés au système.
- `c` — Plante le système sans préalablement démonter les systèmes de fichiers ou synchroniser les disques connectés au système.
- `0` — Éteint le système.
- `0` — Essaie de synchroniser les disques connectés au système.
- `u` — Essaie de démonter et de remonter tous les systèmes de fichiers en lecture-seule.
- `p` — Affiche tous les indicateurs et registres sur la console.
- `t` — Affiche une liste de processus sur la console.
- `m` — Désactive entièrement Exec Shield.
- `0` à `9` — Définit le niveau de journalisation de la console.
- `e` — Met fin à tous les processus sauf `init` à l'aide de SIGTERM.
- `i` — Met fin à tous les processus sauf `init` à l'aide de SIGKILL.
- `l` — Arrête tous les processus à l'aide de SIGKILL (y compris `init`). *Le système est inutilisable après avoir exécuté ce code SRK.*
- `h` — Affiche le texte d'aide.

Cette fonctionnalité est très utile lors de l'utilisation d'un noyau de développement ou lorsque des gels du système se produisent.

Attention

La fonctionnalité de la touche d'interrogation système est considérée comme un risque de sécurité étant donné qu'une console sans surveillance peut permettre à un agresseur d'accéder au système. Pour cette raison, elle est désactivée par défaut.

Reportez-vous à `/usr/share/doc/kernel-doc-`<*version*>`/Documentation/sysrq.txt` afin d'obtenir davantage d'informations sur la touche d'interrogation système (ou SKR de l'anglais System Request Key).

- `sysrq-key` — Définit le code de la touche d'interrogation système (`84` est la valeur par défaut).
- `sysrq-sticky` — Définit si la touche d'interrogation système est une combinaison de touches simultanée. Parmi les valeurs acceptées figurent :
  - `0` — Les touches [Alt]-[SysRq] et le code d'interrogation système doivent être appuyées en même temps. Ce chiffre représente la valeur par défaut.
  - `1` — Les touches [Alt]-[SysRq] doivent être appuyées en même temps, mais le code d'interrogation système peut être appuyé à tout moment avant que le nombre de secondes défini dans `/proc/sys/kernel/sysrq-timer` ne soit écoulé.

- `sysrq-timer` — Définit le nombre de secondes pouvant sécouler avant que le code d'interrogation système ne doive être saisi. La valeur par défaut est `10`.
- `tainted` — Indique si un module non-GPL est chargé.
  - `0` — Aucun module non-GPL n'est chargé.
  - `1` — Au moins un module sans licence GPL (y compris des modules sans licence) est chargé.
  - `2` — Au moins un module a été chargé par force à l'aide de la commande `insmod -f`.

- `threads-max` — Définit le nombre maximum d'unités d'exécution devant être utilisé par le noyau, avec une valeur par défaut de `2048`.
- `version` — Affiche la date et l'heure de la dernière compilation du noyau. Le premier champ dans ce fichier, par exemple `#3`, fait référence au nombre de fois que le noyau a été construit à partir de la source.

5.3.9.4. `/proc/sys/net/`

Ce répertoire contient des sous-répertoires relatifs à divers éléments du réseau. Diverses configurations lors de la compilation du noyau déterminent la présence ou l'absence de différents répertoires à cet endroit, comme par exemple `appletalk/`, `ethernet/`, `ipv4/`, `ipx/` et `ipv6/`. En changeant les fichiers dans ces répertoires, les administrateurs système peuvent ajuster les configurations réseau sur un système en cours d'exécution.

Étant donné le nombre important d'options réseau possibles et disponibles sous Linux, nous n'aborderons que les répertoires `/proc/sys/net/` les plus courants.

Le répertoire `/proc/sys/net/core/` contient une série de paramètres qui contrôlent l'interaction entre le noyau et les couches réseau. Les fichiers les plus importants de ce répertoire sont :

- `message_burst` — Définit la durée, en dixièmes de seconde, nécessaire pour écrire un nouveau message d'avertissement. Ceci est utilisé pour empêcher les attaques par *déni de service* (ou *DoS* de l'anglais Denial of Service). La valeur par défaut est de `50`.
- `message_cost` — Spécifie un coût pour chaque message d'avertissement. Plus la valeur de ce fichier est élevée (`5` par défaut), plus il est probable que le message d'avertissement sera ignoré. Ce paramètre est utilisé pour empêcher les attaques DoS.

  L'idée de base d'une attaque DoS est de bombarder le système de requêtes qui génèrent des erreurs et remplissent les partitions de disque de fichiers journaux ou qui accaparent toutes les ressources du système pour gérer la journalisation des erreurs. Les paramètres de `message_burst` et `message_cost` sont conçus pour être modifiés en fonction des risques acceptables de votre système par rapport au besoin d'une journalisation exhaustive.
- `netdev_max_backlog` — Définit le nombre maximum de paquets pouvant être mis en file d'attente lorsqu'une interface spécifique reçoit des paquets plus rapidement que le noyau ne peut les traiter. La valeur par défaut de ce fichier est de `300`.
- `optmem_max` — Configure la taille maximum des tampons auxiliaires qui est autorisée par socket.
- `rmem_default` — Définit la taille par défaut en octets du tampon du socket de réception.
- `rmem_max` — Définit la taille maximum en octets du tampon de réception.
- `wmem_default` — Définit la taille par défaut en octets du tampon d'envoi.
- `wmem_max` — Définit la taille maximum en octets du tampon d'envoi.

Le répertoire /proc/sys/net/ipv4/ contient des paramètres de mise en réseau supplémentaires. Bon nombre de ces paramètres, utilisés en connexion les uns avec les autres, sont très utiles pour empêcher des attaques contre le système ou pour utiliser le système en tant que routeur.

Attention

Une modification inappropriée de ces fichiers pourrait avoir un effet néfaste sur la connectivité distante au système.

Ci-dessous figure une liste regroupant certains des fichiers les plus importants du répertoire /proc/sys/net/ipv4/ :

- icmp_destunreach_rate, icmp_echoreply_rate, icmp_paramprob_rate et icmp_timeexeed_rate — Définissent le délai maximum d'envoi, en centièmes de seconde, de paquets ICMP aux hôtes sous certaines conditions. La valeur 0 éliminant tout délai, elle n'est pas recommandée.
- icmp_echo_ignore_all et icmp_echo_ignore_broadcasts — Permet au noyau d'ignorer les paquets ECHO ICMP de tous les hôtes ou uniquement ceux qui proviennent, respectivement, d'adresses de diffusion ou de multidiffusion. Une valeur de 0 permet au noyau de répondre, alors qu'une valeur de 1 elle, lui fait ignorer les paquets.
- ip_default_ttl — Définit la *durée de vie* (ou TTL de l'anglais Time To Live) par défaut, qui limite le nombre de sauts qu'un paquet peut faire avant d'atteindre sa destination. L'augmentation de cette valeur peut réduire les performances du système.
- ip_forward — Permet aux interfaces du système de réacheminer des paquets des unes vers les autres. Par défaut, ce fichier est paramétré sur 0. En paramétrant ce fichier sur 1, le réacheminement des paquets réseau est activé.
- ip_local_port_range — Spécifie la plage de ports que TCP ou UDP doivent utiliser lorsqu'un port local est requis. Le premier nombre correspond au port le plus bas devant être utilise et le second au port le plus élevé. Tout système susceptible de nécessiter un nombre de ports supérieur aux valeurs par défaut de 1024 à 4999, devrait utiliser la plage allant de 32768 à 61000.
- tcp_syn_retries — Établit une limite au nombre de fois que le système peut retransmettre un paquet SYN lorsqu'il essaie d'effectuer une connexion.
- tcp_retries1 — Détermine le nombre de retransmissions permises, essayant de répondre à une connexion entrante. 3 est la valeur par défaut.
- tcp_retries2 — Définit le nombre de retransmissions permises de paquets TCP. 15 est la valeur par défaut.

Le fichier /usr/share/doc/kernel-doc-<*version*>/Documentation/networking/ip-sysctl.txt contient une liste exhaustive des fichiers et des options disponibles dans le répertoire /proc/sys/net/ipv4/.

De nombreux autres répertoires existent dans le répertoire /proc/sys/net/ipv4/, chacun d'entre eux couvrant un aspect différent de la pile réseau. Le répertoire /proc/sys/net/ipv4/conf/ permet de configurer chaque interface du système de façon différente et d'utiliser des paramètres par défaut pour des périphériques non-configurés (dans le sous-répertoire /proc/sys/net/ipv4/conf/default/) ainsi que des paramètres qui annulent toutes les configurations spéciales (dans le sous-répertoire /proc/sys/net/ipv4/conf/all/).

Le répertoire /proc/sys/net/ipv4/neigh/ contient non seulement des paramètres nécessaires pour la communication avec un hôte connecté directement au système (que l'on appelle voisin réseau) mais également des paramètres relatifs aux systèmes qui se trouvent à plusieurs sauts de distance.

Le routage via IPV4 dispose également de son propre répertoire, appelé /proc/sys/net/ipv4/route/. Contrairement à conf/ et neigh/, le répertoire /proc/sys/net/ipv4/route/ contient des spécifications qui s'appliquent au routage avec toutes les interfaces du système. Bon nombre de ces paramètres, tels que max_size, max_delay et min_delay, font référence au contrôle de la taille du cache de routage. Pour vider le cache de routage, spécifiez une valeur quelconque dans le fichier flush.

Des informations supplémentaires sur ces répertoires et sur les valeurs possibles pour leurs fichiers de configuration se trouvent dans :

/usr/share/doc/kernel-doc-<*version*>/Documentation/filesystems/proc.txt

5.3.9.5. /proc/sys/vm/

Ce répertoire facilite la configuration du sous-système de la mémoire virtuelle (VM) du noyau Linux. Le noyau utilise de façon exhaustive et intelligente la mémoire virtuelle, que l'on appelle communément l'espace swap.

Les fichiers suivants se trouvent généralement dans le répertoire /proc/sys/vm/ :

- block_dump — Configure le débogage d'E/S par bloc lors de son activation. Toutes les opérations de lecture/écriture et de modification des blocs effectuées sur des fichiers sont journalisées en conséquence. Cette option peut être utile lors d'un diagnostic de l'accélération ou du ralentissement du disque en vue d'économiser la batterie d'un ordinateur portable. Lorsque l'option block_dump est activée, toute sortie peut être obtenue via dmesg. La valeur par défaut est 0.

  
  Astuce

  Si l'option block_dump est activée en même temps que le débogage du noyau, il est prudent d'arrêter le démon klogd étant donné qu'il crée une activité de disque erronée résultant de block_dump.

- dirty_background_ratio — Démarre la réécriture de données modifiées (dirty) en arrière plan à ce taux de mémoire totale via le démon pdflush. La valeur par défaut est 10.
- dirty_expire_centisecs — Définit lorsque des données modifiées présentes en mémoire sont suffisamment anciennes pour être vidées (writeout). Des données sales en mémoire depuis une durée supérieure à cet intervalle sont vidées lors de la prochaine activité d'un démon pdflush. La valeur par défaut exprimée en centièmes de seconde est de 3000.
- dirty_ratio — Démarre la réécriture active de données modifiées à ce taux de mémoire pour le générateur de données modifiées, via le démon pdflush. La valeur par défaut est 40.
- dirty_writeback_centisecs — Définit l'intervalle existant entre des périodes d'activité du démon pdflush qui écrit périodiquement sur le disque des données modifiées présentes dans la mémoire. La valeur par défaut exprimée en centièmes de seconde est de 500.
- laptop_mode — Minimise le nombre de fois qu'un disque dur doit être accéléré en le gardant au ralenti aussi longtemps que possible, conservant ainsi le niveau de la batterie des ordinateurs portables. Cette option permet d'augmenter l'efficacité en regroupant tous les futurs procédés d'E/S et réduisant donc la fréquence des accélérations du disque. La valeur par défaut est 0, mais cette option est automatiquement activée lorsque la batterie d'un ordinateur portable est utilisée.

  Cette valeur est contrôlée automatiquement par le démon acpid une fois que l'utilisateur est averti que l'alimentation est fournie depuis la batterie. Aucune modification ou interaction de la part de l'utilisateur n'est nécessaire si l'ordinateur portable prend en charge la norme ACPI (Advanced Configuration and Power Interface)

Pour obtenir davantage d'informations sur le sujet, consultez la documentation installée dont la référence figure ci-dessous :

`/usr/share/doc/kernel-doc-<version>/Documentation/laptop-mode.txt`

- `lower_zone_protection` — Détermine à quel point le noyau défend les zones d'allocation de mémoire basse. Cette option est efficace lorsqu'elle est utilisée sur des machines configurées avec l'activation de l'espace mémoire `highmem`. La valeur par défaut est `0`, absolument aucune protection. Toutes les autres valeurs entières sont exprimées en méga-octets et `lowmem` est par conséquent protégée contre une allocation par d'autres utilisateurs.

  Pour obtenir davantage d'informations sur le sujet, consultez la documentation installée dont la référence figure ci-dessous :

  `/usr/share/doc/kernel-doc-<version>/Documentation/filesystems/proc.txt`

- `max_map_count` — Configure le nombre maximum de zones de topologie de mémoire qu'un processus peut avoir. La valeur par défaut de `65536` est appropriée dans la plupart des cas.

- `min_free_kbytes` — Force le gestionnaire de mémoire virtuel Linux (VM Linux) à garder un certain nombre de kilo-octets libres. Le VM utilise ce nombre pour calculer une valeur `pages_min` pour chaque zone `lowmem` du système. La valeur par défaut est définie par rapport à la mémoire totale de la machine.

- `nr_hugepages` — Indique le nombre actuel de pages `hugetlb` configurées dans le noyau.

  Pour obtenir davantage d'informations sur le sujet, consultez la documentation installée dont la référence figure ci-dessous :

  `/usr/share/doc/kernel-doc-<version>/Documentation/vm/hugetlbpage.txt`

- `nr_pdflush_threads` — Indique le nombre de démons pdflush qui sont actuellement en cours d'exécution. Ce fichier est en lecture-seule et ne devrait pas être modifié par l'utilisateur. Sous de lourdes charges d'E/S, la valeur par défaut fixée à deux est révisée à la hausse par le noyau.

- `overcommit_memory` — Configure les conditions sous lesquelles une grande demande de mémoire est acceptée ou refusée. Les trois modes suivants sont disponibles :

  - `0` — Le noyau effectue le traitement de surcharge de mémoire heuristique, en estimant la quantité de mémoire disponible et en refusant les requêtes qui sont indubitablement invalides. Malheureusement, vu que la mémoire est allouée à l'aide d'un algorithme heuristique plutôt que d'un algorithme précis, ce paramètre peut parfois autoriser la surcharge de la mémoire disponible sur un système. Cette valeur est le paramètre par défaut.

  - `1` — Le noyau n'effectue aucun traitement de surcharge de mémoire. Sous cette configuration, la possibilité de surcharge de mémoire est certes augmentée mais la performance des tâches nécessitant beaucoup de mémoire (telles que celles exécutées par certains logiciels scientifiques) l'est elle aussi.

  - `2` — Le noyau refuse des requêtes de mémoire qui, accumulées, sont égales à tout le swap plus le pourcentage de RAM physique spécifié dans `/proc/sys/vm/overcommit_ratio`. Ce paramètre est le plus approprié pour les personnes qui souhaitent des risques de surcharge de mémoire moins élevés.

    

    Remarque

    Cette configuration est uniquement recommandée pour les systèmes avec des zones de swap supérieures à la mémoire physique.

- `overcommit_ratio` — Spécifie le pourcentage de RAM physique considérée lorsque `/proc/sys/vm/overcommit_memory` est réglé sur `2`. La valeur par défaut est `50`.

- `page-cluster` — Définit le nombre de pages lues en une seule tentative. La valeur par défaut est `3` et se rapporte en fait à 16 pages ; cette valeur est adéquate pour la plupart des systèmes.
- `swappiness` — Détermine la quantité de mémoire qu'une machine devrait échanger (swap). Plus la valeur est élevée, plus l'activité de va-et-vient est importante. La valeur par défaut, en tant que pourcentage, est de fixée à `60`.

Toute la documentation sur le noyau a été installée localement et se trouve à l'emplacement suivant :

`/usr/share/doc/kernel-doc-<version>/Documentation/`, qui contient des informations supplémentaires.

5.3.10. `/proc/sysvipc/`

Ce répertoire contient des informations sur les ressources IPC System V. Les fichiers de ce répertoire concernent les appels IPC System V de messages (`msg`), sémaphores (`sem`) et mémoire partagée (`shm`).

5.3.11. `/proc/tty/`

Ce répertoire contient des informations sur les *périphériques tty* disponibles et actuellement utilisés sur le système. Appelés à l'origine *périphériques téléimprimeurs* (ou télétypes), tout terminal basé sur les caractères est un périphérique tty.

Sous Linux, il existe trois types différents de périphériques tty. Les *périphériques série* sont utilisés avec les connexions série, par exemple par modem ou câble série. Les *terminaux virtuels* créent la connexion à la console commune, comme les consoles virtuelles disponibles lorsque vous appuyez sur [Alt]-[<touche-F>] sur la console système. Les *pseudo-terminaux* créent une communication à double sens utilisée par certaines applications de niveau supérieur, telles que XFree86. Le fichier `drivers` contient une liste des périphériques tty actuellement utilisés, comme dans l'exemple suivant :

```
serial               /dev/cua        5  64-127 serial:callout
serial               /dev/ttyS       4  64-127 serial
pty_slave            /dev/pts      136   0-255 pty:slave
pty_master           /dev/ptm      128   0-255 pty:master
pty_slave            /dev/ttyp       3   0-255 pty:slave
pty_master           /dev/pty        2   0-255 pty:master
/dev/vc/0            /dev/vc/0       4       0 system:vtmaster
/dev/ptmx            /dev/ptmx       5       2 system
/dev/console         /dev/console    5       1 system:console
/dev/tty             /dev/tty        5       0 system:/dev/tty
unknown              /dev/vc/%d      4    1-63 console
```

Le fichier `/proc/tty/driver/serial` répertorie les statistiques d'utilisation et l'état de chaque ligne tty série.

Pour que les périphériques tty puissent être utilisés comme des périphériques réseau, le noyau Linux applique une *procédure de transmission* sur les périphériques. Cela permet au pilote de placer un type spécifique d'en-tête sur chaque bloc de données transmis via un périphérique donné ; ainsi, l'extrémité distante de la connexion voit ce bloc de données comme un tout unique dans un flux de blocs de données. SLIP et PPP sont des procédures de transmission courantes et sont communément utilisées pour connecter des systèmes via un lien série.

Les procédures de transmission enregistrées sont stockées dans le fichier `ldiscs` et des informations détaillées sont disponibles dans le répertoire `ldisc/`.

5.4. Utilisation de la commande sysctl

La commande /sbin/sysctl est utilisée pour afficher, définir et automatiser les paramètres du noyau dans le répertoire /proc/sys/.

Pour obtenir un aperçu rapide de tous les paramètres configurables dans le répertoire /proc/sys/, tapez la commande /sbin/sysctl -a en étant connecté en tant que super-utilisateur (root). Cette dernière dresse alors une longue liste exhaustive à laquelle le court extrait figurant ci-dessous pourrait ressembler :

```
net.ipv4.route.min_delay = 2
kernel.sysrq = 0
kernel.sem = 250     32000     32     128
```

Ces informations sont les mêmes que celles obtenues en consultant chaque fichier individuellement. La seule différence réside dans l'emplacement du fichier. Par exemple, le fichier /proc/sys/net/ipv4/route/min_delay apparaît comme net.ipv4.route.min_delay où les barres obliques de répertoire sont remplacées par des points et où la partie proc.sys est implicite.

Il est possible d'utiliser la commande sysctl au lieu de echo pour affecter des valeurs aux fichiers modifiables du répertoire /proc/sys/. Par exemple, au lieu d'utiliser la commande :

```
echo 1 > /proc/sys/kernel/sysrq
```

utilisez la commande sysctl équivalente comme suit :

```
sysctl -w kernel.sysrq="1"
kernel.sysrq = 1
```

Ce type de réglage rapide des valeurs individuelles dans /proc/sys/ est certes pratique en phase de tests, mais ne fonctionne pas aussi bien sur un système de production car tous les paramètres spéciaux de /proc/sys/ sont perdus lors du redémarrage du système. Pour préserver les paramètres personnalisés, ajoutez-les au fichier /etc/sysctl.conf.

Chaque fois que le système démarre, le programme init exécute le script /etc/rc.d/rc.sysinit. Ce dernier contient une commande pour exécuter sysctl à l'aide de /etc/sysctl.conf afin de déterminer les valeurs transmises au noyau. Toute valeur ajoutée à /etc/sysctl.conf prendra effet à chaque démarrage du système.

5.5. Ressources supplémentaires

Vous trouverez ci-dessous des sources d'informations supplémentaires sur le système de fichiers proc.

5.5.1. Documentation installée

Une partie de la meilleure documentation sur le système de fichiers /proc/ est installée par défaut sur le système.

- /usr/share/doc/kernel-doc-<*version*>/Documentation/filesystems/proc.txt — Contient des informations variées, mais limitées, sur tous les aspects du répertoire /proc/.
- /usr/share/doc/kernel-doc-<*version*>/Documentation/sysrq.txt — Offre un aperçu des options de la touche d'interrogation système (ou System Request Key).
- /usr/share/doc/kernel-doc-<*version*>/Documentation/sysctl/ — Représente un répertoire contenant un certain nombre d'astuces pour sysctl, y compris pour modifier des

valeurs en rapport avec le noyau (`kernel.txt`), accéder aux systèmes de fichiers (`fs.txt`) et pour obtenir des informations sur l'utilisation de la mémoire (`vm.txt`).

- `/usr/share/doc/kernel-doc-<version>/Documentation/networking/ip-sysctl.txt` — Offre un aperçu détaillé des options de mise en réseau d'IP.

5.5.2. Site Web utile

- http://www.linuxhq.com/ — Ce site Web maintient une base de données complète sur la source, les correctifs et la documentation de nombreuses versions du noyau Linux.

Chapitre 6.

Utilisateurs et groupes

Le contrôle des *utilisateurs* et des *groupes* est un élément central de l'administration système de Red Hat Enterprise Linux.

Les *utilisateurs* peuvent être aussi bien des personnes, avec des comptes attachés à des utilisateurs physiques, que des comptes existant pour une utilisation par des applications spécifiques.

Les *groupes* sont des expressions logiques qui permettent une certaine organisation en regroupant des utilisateurs oeuvrant pour un but commun. Les utilisateurs appartenant à un groupe donné peuvent lire, écrire ou exécuter des fichiers appartenant à ce groupe.

Chaque utilisateur et chaque groupe se voit attribuer un identificateur numérique unique appelé respectivement un *userid* (*UID*) et un *groupid* (*GID*).

L'utilisateur qui crée un fichier devient le propriétaire et le groupe propriétaire du fichier. Ce fichier reçoit également des permissions séparées de lecture, d'écriture et d'exécution pour le propriétaire, le groupe ou tout autre utilisateur. Le propriétaire du fichier peut seulement être modifié par le super-utilisateur. Le groupe possédant un fichier peut être modifié par le super-utilisateur ; les permissions d'accès quant à elles peuvent être modifiées aussi bien par le super-utilisateur et que par le propriétaire du fichier.

Red Hat Enterprise Linux prend en charge les *listes de contrôle d'accès* (ou *LCA* de l'anglais Access Control List) pour les fichiers et les répertoires permettant ainsi de définir des permissions pour des utilisateurs donnés en dehors du propriétaire. Afin d'obtenir de plus amples informations sur l'utilisation des LCA, reportez-vous au chapitre intitulé *Listes de contrôle d'accès* du *Guide d'administration système de Red Hat Enterprise Linux*.

Parmi les tâches les plus importantes qu'un administrateur de système doive effectuer figurent une bonne gestion des utilisateurs et des groupes ainsi qu'une gestion efficace des permissions de fichiers. Pour obtenir des informations plus détaillées sur les stratégies de gestion des utilisateurs et des groupes, reportez-vous au chapitre intitulé *Gestion des comptes utilisateur et de l'accès aux ressources* du manuel intitulé *Introduction à l'administration système de Red Hat Enterprise Linux*.

6.1. Outils de gestion des utilisateurs et des groupes

La gestion des utilisateurs et des groupes peut être une tâche laborieuse, mais Red Hat Enterprise Linux fournit des outils et conventions facilitant cette gestion.

La manière la plus simple de gérer des utilisateurs et des groupes consiste à utiliser l'application graphique **Gestionnaire d'utilisateurs** (`system-config-users`). Pour obtenir de plus amples informations sur le **Gestionnaire d'utilisateurs**, reportez-vous au chapitre intitulé *Configuration des utilisateurs et des groupes* du *Guide d'administration système de Red Hat Enterprise Linux*.

Les outils de la ligne de commande mentionnés ci-dessous peuvent également servir à gérer les utilisateurs et les groupes :

- `useradd`, `usermod` et `userdel` — Méthodes conformes aux standards de l'industrie permettant d'ajouter, de supprimer et de modifier des comptes d'utilisateurs.
- `groupadd`, `groupmod` et `groupdel` — Méthodes conformes aux standards de l'industrie permettant d'ajouter, de supprimer et de modifier des groupes d'utilisateurs.
- `gpasswd` — Méthode conforme aux standards de l'industrie permettant d'administrer le fichier `/etc/group`.

- `pwck`, `grpck` — Outils permettant de vérifier le mot de passe, le groupe et les fichiers masqués connexes.
- `pwconv`, `pwunconv` — Outils permettant la conversion de mots de passe standard en mots de passe masqués et vice versa.

Pour obtenir un aperçu de la gestion des utilisateurs et des groupes, reportez-vous au manuel intitulé *Introduction à l'administration système de Red Hat Enterprise Linux*. Pour des informations plus détaillées sur les outils de la ligne de commande permettant de gérer les utilisateurs et les groupes, consultez le chapitre intitulé *Configuration des utilisateurs et des groupes* du *Guide d'administration système de Red Hat Enterprise Linux*.

6.2. Utilisateurs ordinaires

Le Tableau 6-1 énumère les utilisateurs ordinaires configurés dans le fichier `/etc/passwd` lors d'une installation complète (**Tout**). L'identificateur groupe (ID groupe ou GID) figurant dans ce tableau correspond au *groupe primaire* pour l'utilisateur. Reportez-vous à la Section 6.3 pour obtenir une liste des groupes ordinaires.

Utilisateur	UID	GID	Répertoire personnel	Shell
root	0	0	`/root`	`/bin/bash`
bin	1	1	`/bin`	`/sbin/nologin`
démon	2	2	`/sbin`	`/sbin/nologin`
adm	3	4	`/var/adm`	`/sbin/nologin`
lp	4	7	`/var/spool/lpd`	`/sbin/nologin`
sync	5	0	`/sbin`	`/bin/sync`
arrêt	6	0	`/sbin`	`/sbin/shutdown`
halt	7	0	`/sbin`	`/sbin/halt`
message	8	12	`/var/spool/mail`	`/sbin/nologin`
informations	9	13	`/etc/news`	
uucp	10	14	`/var/spool/uucp`	`/sbin/nologin`
opérateur	11	0	`/root`	`/sbin/nologin`
jeux	12	100	`/usr/games`	`/sbin/nologin`
gopher	13	30	`/var/gopher`	`/sbin/nologin`
ftp	14	50	`/var/ftp`	`/sbin/nologin`
personne	99	99	`/`	`/sbin/nologin`
rpm	37	37	`/var/lib/rpm`	`/sbin/nologin`
vcsa	69	69	`/dev`	`/sbin/nologin`
dbus	81	81	`/`	`/sbin/nologin`
ntp	38	38	`/etc/ntp`	`/sbin/nologin`
canna	39	39	`/var/lib/canna`	`/sbin/nologin`

Utilisateur	UID	GID	Répertoire personnel	Shell
nscd	28	28	/	/sbin/nologin
rpc	32	32	/	/sbin/nologin
postfix	89	89	/var/spool/postfix	/sbin/nologin
mailman	41	41	/var/mailman	/sbin/nologin
nommé	25	25	/var/named	/bin/false
amanda	33	6	var/lib/amanda/	/bin/bash
postgres	26	26	/var/lib/pgsql	/bin/bash
exim	93	93	/var/spool/exim	/sbin/nologin
sshd	74	74	/var/empty/sshd	/sbin/nologin
rpcuser	29	29	/var/lib/nfs	/sbin/nologin
nsfnobody	65534	65534	/var/lib/nfs	/sbin/nologin
pvm	24	24	/usr/share/pvm3	/bin/bash
apache	48	48	/var/www	/sbin/nologin
xfs	43	43	/etc/X11/fs	/sbin/nologin
gdm	42	42	/var/gdm	/sbin/nologin
htt	100	101	/usr/lib/im	/sbin/nologin
mysql	27	27	/var/lib/mysql	/bin/bash
webalizer	67	67	/var/www/usage	/sbin/nologin
mailnull	47	47	/var/spool/mqueue	/sbin/nologin
smmsp	51	51	/var/spool/mqueue	/sbin/nologin
squid	23	23	/var/spool/squid	/sbin/nologin
ldap	55	55	/var/lib/ldap	/bin/false
netdump	34	34	/var/crash	/bin/bash
pcap	77	77	/var/arpwatch	/sbin/nologin
radiusd	95	95	/	/bin/false
radvd	75	75	/	/sbin/nologin
quagga	92	92	/var/run/quagga	/sbin/login
wnn	49	49	/var/lib/wnn	/sbin/nologin
dovecot	97	97	/usr/libexec/dovecot	/sbin/nologin

Tableau 6-1. Utilisateurs ordinaires

6.3. Groupes ordinaires

Le Tableau 6-2 énumère les groupes ordinaires configurés lors d'une installation complète (**Tout**). Les groupes sont enregistrés dans le fichier `/etc/group`.

Groupe	GID	Membres
root	0	root
bin	1	root, bin, démon
démon	2	root, bin, démon
sys	3	root, bin, adm
adm	4	root, adm, démon
tty	5	
disque	6	root
lp	7	démon, lp
mem	8	
kmem	9	
wheel	10	root
message	12	mail, postfix, exim
informations	13	informations
uucp	14	uucp
man	15	
jeux	20	
gopher	30	
dip	40	
ftp	50	
verrouillage	54	
personne	99	
utilisateurs	100	
rpm	37	
utmp	22	
disquette	19	
vcsa	69	
dbus	81	
ntp	38	
canna	39	
nscd	28	
rpc	32	
postdrop	90	
postfix	89	
mailman	41	
exim	93	

Groupe	GID	Membres
nommé	25	
postgres	26	
sshd	74	
rpcuser	29	
nfsnobody	65534	
pvm	24	
apache	48	
xfs	43	
gdm	42	
htt	101	
mysql	27	
webalizer	67	
mailnull	47	
smmsp	51	
squid	23	
ldap	55	
netdump	34	
pcap	77	
quaggavt	102	
quagga	92	
radvd	75	
slocate	21	
wnn	49	
dovecot	97	
radiusd	95	

Tableau 6-2. Groupes ordinaires

6.4. Groupes propres à l'utilisateur

Red Hat Enterprise Linux utilise un système de *groupe privé d'utilisateurs* (ou *UPG* de l'anglais User Private Group) qui facilite considérablement la gestion de groupes UNIX.

Un UPG est créé chaque fois qu'un nouvel utilisateur est ajouté au système. Les UPG portent le même nom que l'utilisateur pour lequel ils ont été créés et seul cet utilisateur est un membre de l'UPG.

Grâce à l'utilisation d'UPG, il est possible de déterminer en toute sécurité des permissions par défaut pour un nouveau fichier ou répertoire afin que l'utilisateur et le *groupe de cet utilisateur* puissent modifier le fichier ou répertoire.

Le paramètre qui détermine les permissions spécifiques à accorder à de nouveaux fichiers ou répertoires s'appelle *umask* ; ce dernier est configuré dans le fichier `/etc/bashrc`. Sur des systèmes

UNIX, `umask` a traditionnellement une valeur de `022`, permettant uniquement l'utilisateur qui a créé le fichier ou répertoire de le modifier. Sous ce système, aucun autre utilisateur, *même les membres appartenant au groupe du créateur*, n'est autorisé à apporter quelque modification que ce soit. Cependant, étant donné que chaque utilisateur a son propre groupe privé dans le système UPG, cette "protection de groupe" n'est pas nécessaire.

6.4.1. Répertoire de groupes

Dans de nombreuses sociétés du secteur informatique il est courant de créer un groupe pour chaque grand projet et d'y assigner ensuites des personnes, si ces dernières doivent avoir accès aux fichiers du projet. Avec ce système traditionnel, un fichier est créé, il est associé au groupe primaire auquel son créateur appartient. Ainsi, lorsqu'une même personne travaille sur plusieurs projets, il devient difficile d'associer les bons fichiers au bon groupe. Toutefois, en utilisant le système UPG, les groupes sont automatiquement assignés aux fichiers créés dans un répertoire avec un bit *setgid* déterminé. Ce dernier facilite considérablement la gestion des projets de groupe qui partagent un répertoire commun étant donné que tous les fichiers créés par un utilisateur au sein du répertoire appartiennent au groupe propriétaire du répertoire.

Supposons par exemple qu'un groupe de personnes travaille sur des fichiers figurant dans le répertoire `/usr/lib/emacs/site-lisp/`. Certaines personnes dignes de confiance peuvent certes être autorisées à modifier le répertoire, mais tout le monde ne peut pas jouir de ce privilège. Il est donc nécessaire de créer d'abord un groupe `emacs`, comme le fait la commande suivante :

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

Afin d'associer le contenu du répertoire au groupe `emacs`, tapez :

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

Il est maintenant possible d'ajouter les utilisateurs appropriés au groupe à l'aide de la commande `gpasswd` :

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

Afin d'autoriser les utilisateurs à créer des fichiers dans le répertoire, utilisez la commande suivante :

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

Lorsqu'un utilisateur crée un nouveau fichier, il se voit assigner le groupe privé par défaut du groupe de l'utilisateur. Ensuite, donnez une valeur au bit setgid, qui donne à tout fichier créé dans le répertoire la même permission de groupe que le répertoire lui-même (`emacs`). Utilisez la commande suivante :

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

À ce stade, comme l'umask par défaut de chaque utilisateur est 002, tous les membres du groupe `emacs` peuvent créer et modifier des fichiers dans le répertoire `/usr/lib/emacs/site-lisp/`, sans que l'administrateur n'aie à changer les permissions de fichiers chaque fois que des utilisateurs enregistrent de nouveaux fichiers.

6.5. Mots de passe masqués

Dans un environnement multi-utilisateurs, il est primordial d'utiliser des *mots de passe masqués* (fournis par le paquetage `shadow-utils`). Ce faisant, la sécurité des fichiers d'authentification du système se voit accrue. C'est pour cette raison que le programme d'installation active des mots de passe masqués par défaut.

Ci-dessous figure une liste des avantages associés aux mots de passe masqués par rapport à l'ancienne manière de stocker des mots de passe sur des systèmes basés sur UNIX :

- Amélioration de la sécurité du système en déplaçant les hachages de mots de passe cryptés d'un fichier `/etc/passwd` lisible par quiconque à un fichier `/etc/shadow` lisible uniquement par le super-utilisateur.
- Stockage d'informations sur l'expiration des mots de passe.
- Possibilité d'utiliser le fichier `/etc/login.defs` pour mettre en oeuvre les politiques de sécurité.

La plupart des utilitaires fournis par le paquetage `shadow-utils` fonctionnent correctement, que des mots de passe masqués soient activés ou non. Toutefois, comme les informations sur l'expiration des mots de passe sont stockées exclusivement dans le fichier `/etc/shadow`, aucune commande créant ou modifiant les informations sur l'expiration des mots de passe ne fonctionnera.

Ci-après figure une liste des commandes ne fonctionnant pas sans que les mots de passe masqués ne soient préalablement activés :

- `chage`
- `gpasswd`
- `/usr/sbin/usermod` options `-e` ou `-f`
- `/usr/sbin/useradd` options `-e` ou `-f`

6.6. Ressources supplémentaires

Afin d'obtenir davantage d'informations sur les utilisateurs et les groupes ainsi que sur les outils permettant leur gestion, reportez-vous aux ressources mentionnées ci-dessous.

6.6.1. Documentation installée

- Pages de manuel sur le sujet — Il existe un certain nombre de pages de manuel pour les différentes applications et divers fichiers de configuration intervenant dans la gestion des utilisateurs et des groupes. La liste suivante présente certaines des pages de manuel les plus importantes :

  Applications administratives pour les utilisateurs et les groupes :

  - `man chage` — Une commande pour modifier les politiques d'expiration des mots de passe et des comptes.
  - `man gpasswd` — Une commande pour gérer le fichier `/etc/group`.
  - `man groupadd` — Une commande pour ajouter des groupes.
  - `man grpck` — Une commande pour vérifier le fichier `/etc/group`.
  - `man groupdel` — Une commande pour supprimer des groupes.
  - `man groupmod` — Une commande pour modifier le propriétaire d'un groupe.
  - `man pwck` — Une commande pour vérifier les fichiers `/etc/passwd` et `/etc/shadow`.
  - `man pwconv` — Un outil permettant la conversion de mots de passe standard en mots de passe masqués.
  - `man pwunconv` — Un outil permettant la conversion de mots de passe masqués en mots de passe standard.

- `man useradd` — Une commande pour ajouter des utilisateurs.
- `man userdel` — Une commande pour supprimer des utilisateurs.
- `man usermod` — Une commande pour modifier des utilisateurs.

Fichiers de configuration :

- `man 5 group` — Le fichier contenant les informations de groupes pour le système.
- `man 5 passwd` — Le fichier contenant les informations d'utilisateurs pour le système.
- `man 5 shadow` — Le fichier contenant les informations d'expiration des mots de passe et des comptes pour le système.

6.6.2. Livres sur le sujet

- *Introduction à l'administration système de Red Hat Enterprise Linux* ; Red Hat, Inc. — Ce manuel offre un aperçu des concepts et techniques d'administration système. Le chapitre intitulé *Gestion des comptes utilisateur et de l'accès aux ressources* contient de nombreuses informations sur la gestion des comptes utilisateur et groupe.

- *Guide d'administration système de Red Hat Enterprise Linux* ; Red Hat, Inc. — Ce manuel contient davantage d'informations sur la gestion des utilisateurs et des groupes ainsi que sur la configuration avancée des permissions à l'aide des LCA. Reportez-vous aux chapitres intitulés *Configuration des utilisateurs et des groupes* et *Listes de contrôle d'accès* afin d'obtenir de plus amples informations.

- *Guide de sécurité de Red Hat Enterprise Linux* ; Red Hat, Inc. — Ce manuel fournit les aspects associés à la sécurité sur les comptes utilisateur, par exemple sur le choix de bons mots de passe.

Chapitre 7.

Système X Window

Alors que le coeur de Red Hat Enterprise Linux est son noyau, pour beaucoup d'utilisateurs, le visage du système d'exploitation est l'environnement graphique fourni par le *Système X Window*, également appelé *X*.

Bien avant l'apparition de nombreux systèmes d'exploitations traditionnels courants, le monde UNIX™ avait déjà connu depuis des décennies de nombreux environnements de fenêtrage. Au fil des années, X est devenu l'environnement graphique préféré des systèmes d'exploitation de type UNIX.

L'environnement graphique pour Red Hat Enterprise Linux est fourni par *X.Org Foundation*, un consortium Open Source créé pour gérer le développement et la stratégie du système X Window et des technologies connexes. X.Org est un projet de grande envergure qui se développe rapidement grâce à des centaines de développeurs résidant dans le monde entier. Il offre non seulement une prise en charge étendue pour une grande variété de périphériques et d'architectures, mais a également la capacité de tourner sur différents systèmes d'exploitation et sur des plates-formes variées. Cette version de Red Hat Enterprise Linux inclut tout particulièrement la version X11R6.8 du système X Window.

Le système X Window utilise une architecture client-serveur. Le *serveur X* (le binaire `Xorg`) est à l'écoute de connexions venant d'applications *client X* par le biais d'un réseau ou d'une interface de boucle locale. Le serveur communique avec le matériel, comme la carte vidéo, le moniteur, le clavier et la souris. Les applications client X se trouvent dans l'espace utilisateur, créant une *interface utilisateur graphique* (ou *GUI* de l'anglais Graphical User Interface) pour l'utilisateur et transmettant les requêtes de ce dernier au serveur X.

7.1. Version X11R6.8

Red Hat Enterprise Linux 4 utilise la version X11R6.8 en tant que système X Window de base doté de nombreux développements de pointe apportés à la technologie X.Org ; parmi ces derniers figurent entre autres la prise en charge de l'accélération matérielle 3D, l'extension XRender pour des polices lissées, une conception modulaire basée sur des pilotes et une prise en charge du matériel vidéo et des périphériques d'entrée modernes.

Important

Red Hat Enterprise Linux ne fournit plus les paquetages serveur XFree86™. Avant d'effectuer une mise à niveau vers la dernière version de Red Hat Enterprise Linux, assurez-vous que la carte vidéo est bien compatible avec la version X11R6.8 ; pour ce faire, consultez la liste de compatibilité matérielle de Red Hat disponible en ligne à l'adresse suivante : http://hardware.redhat.com.

Les fichiers en relation avec la version X11R6.8 se trouvent essentiellement dans deux emplacements :

/usr/X11R6/

Contient le serveur X et certaines applications client ainsi que les fichiers d'en-tête, bibliothèques, modules et documentation de X.

`/etc/X11/`

Contient tous les fichiers de configuration pour des applications client X et serveur X. Parmi ceux-ci figurent les fichiers de configuration du serveur X lui-même, le serveur de polices `fs`, les gestionnaires d'affichage X et bien d'autres composants de base.

Il est important de noter ici que le fichier de configuration pour la nouvelle architecture de polices basée sur Fontconfig est `/etc/fonts/fonts.conf` (qui remplace le fichier `/etc/X11/XftConfig`). Pour de plus amples informations sur la configuration et l'ajout de polices, reportez-vous à la Section 7.4.

Étant donné que le serveur X effectue beaucoup de tâches avancées sur une vaste gamme de matériel, il nécessite une configuration détaillée. Le programme d'installation met en place et configure X automatiquement, à moins que les paquetages de la version X11R6.8 ne soient pas sélectionnés pour l'installation. Toutefois, si le moniteur ou la carte vidéo changent, X devra être reconfiguré. Pour ce faire, la meilleure façon consiste à utiliser l'**Outil de configuration X** (`system-config-display`).

Pour lancer l'**Outil de configuration X** pendant une session active de X, cliquez sur **Menu principal** (sur le panneau) **=> Paramètres de système => Affichage**. Après l'utilisation de l'**Outil de configuration X** pendant une session X, il faudra fermer la session X en cours, puis redémarrer X pour que les changements prennent effet. Pour obtenir de plus amples informations sur l'utilisation de l'**Outil de configuration X**, reportez-vous au chapitre intitulé *Configuration du système X Window* du *Guide d'administration système de Red Hat Enterprise Linux*.

Dans certaines situations, il sera peut-être nécessaire de reconfigurer manuellement le serveur X en éditant son fichier de configuration `/etc/X11/xorg.conf`. Pour obtenir de plus amples informations sur la structure de ce fichier, reportez-vous à la Section 7.3.

7.2. Environnements de bureau et gestionnaires de fenêtres

Une fois qu'un serveur X tourne, les applications client X peuvent s'y connecter et créer une GUI pour l'utilisateur. Avec Red Hat Enterprise Linux, il existe une grande variété de GUI qui vont de l'interface rudimentaire du gestionnaire de fenêtres *Tab Window Manager* à celle hautement sophistiquée et interactive de l'environnement de bureau *GNOME*, auxquelles la plupart des utilisateurs de Red Hat Enterprise Linux sont habitués.

Afin de créer cette dernière interface très perfectionnée, deux catégories principales d'applications client X doivent être connectées au serveur X : un *environnement de bureau* et un *gestionnaire de fenêtres*.

7.2.1. Environnements de bureau

Un environnement de bureau rassemble des clients X assortis qui, lorsqu'ils sont utilisés ensemble, créent un environnement d'utilisateur graphique commun ainsi qu'une plate-forme de développement.

Les environnements de bureau contiennent des fonctions plus avancées qui permettent aux clients X et autres processus en cours de communiquer les uns avec les autres. Ce faisant, toutes les applications écrites pour cet environnement peuvent également effectuer des tâches avancées comme les opérations de glisser-déposer.

Red Hat Enterprise Linux fournit deux environnements de bureau :

- *GNOME* — L'environnement de bureau par défaut pour Red Hat Enterprise Linux qui est basé sur la boîte à outils graphique GTK+ 2.
- *KDE* — Un autre environnement de bureau basé sur la boîte à outils graphique Qt 3.

Aussi bien GNOME que KDE disposent non seulement d'applications de productivité avancées, comme des traitements de texte, des tableurs et des navigateurs Web, mais fournissent également des outils permettant de personnaliser l'apparence de la GUI. De plus, si les deux bibliothèques GTK+ 2 et Qt sont installées, les applications de KDE peuvent être exécutées dans un environnement GNOME et vice versa.

7.2.2. Gestionnaires de fenêtres

Les *gestionnaires de fenêtres* sont des programmes clients X qui font partie d'un environnement de bureau ou, dans certains cas, sont des applications à part entière. Leur objectif principal est de contrôler le positionnement, le redimensionnement et le déplacement des fenêtres graphiques. Les gestionnaires de fenêtres contrôlent également les barres de titres, le comportement de la cible de saisie (ou focus) de la fenêtre et les liaisons personnalisées des touches et des boutons souris.

Quatre gestionnaires de fenêtres sont compris dans Red Hat Enterprise Linux :

- `kwin` — Le gestionnaire de fenêtres *KWin* est le choix par défaut pour l'environnement de bureau KDE. Il s'agit d'un gestionnaire simple et efficace qui supporte des thèmes personnalisés.
- `metacity` — Le gestionnaire de fenêtres *Metacity* est le choix par défaut pour l'environnement de bureau GNOME. Il s'agit d'un gestionnaire simple et efficace qui supporte des thèmes personnalisés.
- `mwm` — Le gestionnaire de fenêtres *Motif* est un gestionnaire de fenêtres autonome doté de fonctions élémentaires. Étant donné qu'il est supposé être un gestionnaire de fenêtres autonome, il ne devrait pas être utilisé de concert avec les environnements de bureau GNOME ou KDE.
- `twm` — Le gestionnaire de fenêtres minimaliste *Tab Window Manager* qui fournit la panoplie d'outils la plus élémentaire de tous les gestionnaires de fenêtres et peut être utilisé de manière autonome ou avec un environnement de bureau. Il est installé en tant que composant de la version X11R6.8.

Ces gestionnaires de fenêtres peuvent fonctionner sans environnement de bureau afin de mieux se rendre compte de leurs différences. Pour ce faire, tapez la commande `xinit -e <path-to-window-manager>`, où `<path-to-window-manager>` correspond à l'emplacement du fichier binaire du gestionnaire de fenêtres. Vous pourrez trouver ce fichier binaire en tapant `which <window-manager-name>`, où `<window-manager-name>` correspond au nom du gestionnaire de fenêtres que vous recherchez.

7.3. Fichiers de configuration du serveur X

Le serveur X est un exécutable binaire (`/usr/X11R6/bin/Xorg`) qui charge dynamiquement à l'exécution tous les modules nécessaires du serveur X depuis le répertoire `/usr/X11R6/lib/modules/`. Certains de ces modules sont automatiquement chargés par le serveur, alors que d'autres sont facultatifs et doivent donc être spécifiés dans le fichier de configuration du serveur X.

Les fichiers de configuration du serveur X et ceux associés sont stockés dans le répertoire `/etc/X11/`. Le fichier de configuration du serveur X est `/etc/X11/xorg.conf`. Quand Red Hat Enterprise Linux est installé, les fichiers de configuration de X sont créés en utilisant les informations recueillies sur le matériel du système lors du processus d'installation.

7.3.1. `xorg.conf`

Bien qu'il soit rarement nécessaire de modifier manuellement le fichier de configuration `/etc/X11/xorg.conf`, il est utile d'avoir une certaine compréhension des différentes sections et des paramètres optionnels qui existent, surtout lors de la résolution de problèmes.

7.3.1.1. La structure

Le fichier `/etc/X11/xorg.conf` est composé de nombreuses sections différentes qui traitent d'aspects spécifiques du matériel du système.

Chaque section commence par une ligne `Section "<section-name>"` (où <section-name> correspond au titre de la section) et finit par une ligne `EndSection`. Dans chacune de ces sections se trouvent des lignes contenant des noms d'options et au moins une valeur d'option, qui peut se trouver entre guillemets (").

Les lignes commençant par un symbole dièse (#) ne sont pas lues par le serveur X et sont utilisées pour des commentaires lisibles par les utilisateurs.

Certaines options contenues dans le fichier `/etc/X11/xorg.conf` acceptent un commutateur booléen qui permet d'activer ou de désactiver la fonctionnalité. Parmi les valeurs booléennes acceptables figurent :

- `1`, `on`, `true` ou `yes` — Ces valeurs permettent d'activer l'option.
- `0`, `off`, `false` ou `no` — Ces valeurs permettent de désactiver l'option.

La liste suivante contient certaines des sections les plus importantes d'un fichier `/etc/X11/xorg.conf` typique ; ces dernières sont énumérées dans l'ordre précis dans lequel elles apparaissent dans le fichier. Des informations plus détaillées sur le fichier de configuration du serveur X sont disponibles dans la page de manuel de `xorg.conf`.

7.3.1.2. `ServerFlags`

La section facultative `ServerFlags` contient divers réglages globaux du serveur X. Tous les réglages figurant dans cette section peuvent être annulés par les options spécifiées dans la section `ServerLayout` (reportez-vous à la Section 7.3.1.3 pour de plus amples informations).

Les entrées dans la section `ServerFlags` se trouvent sur leurs propres lignes et commencent par le terme `Option` suivi d'une option spécifiée entre guillemets (").

Ci-dessous figure un exemple de section `ServerFlags` :

```
Section "ServerFlags"
      Option "DontZap" "true"
EndSection
```

Parmi certaines des options les plus utiles figurent :

- `"DontZap" "<boolean>"` — La valeur de <boolean> définie comme vraie (true) empêche l'utilisation de la combinaison de touches [Ctrl]-[Alt]-[Retour arrière] pour arrêter instantanément le serveur X.
- `"DontZoom" "<boolaen>"` — La valeur de <boolean> définie comme vraie (true) empêche la commutation entre résolutions vidéo configurées par les combinaisons de touches [Ctrl]-[Alt]-[Plus] et [Ctrl]-[Alt]-[Signe-Moins].

7.3.1.3. `ServerLayout`

La section `ServerLayout` lie les périphériques d'entrée et de sortie contrôlés par le serveur X. Au minimum, cette section doit spécifier un périphérique de sortie et au moins deux périphériques d'entrée (un clavier et une souris).

Ci-dessous figure un exemple typique de section `ServerLayout` :

```
Section  "ServerLayout"
        Identifier     "Default Layout"
        Screen      0  "Screen0" 0 0
        InputDevice    "Mouse0" "CorePointer"
        InputDevice    "Keyboard0" "CoreKeyboard"
```

```
EndSection
```

Les entrées suivantes sont couramment utilisées dans la section `ServerLayout` :

- `Identifier` — Spécifie un nom unique utilisé pour cette section `ServerLayout`.
- `Screen` — Spécifie le nom d'une section `Screen` devant être utilisée avec le serveur X. Il est possible d'avoir plus d'une option `Screen`.

  Ci-dessous figure un exemple typique d'entrée `Screen` :

  ```
  Screen      0  "Screen0" 0 0
  ```

  Dans cet exemple d'entrée, le premier nombre `Screen` (`0`) indique que le premier connecteur du moniteur ou que la *tête* de la carte vidéo utilise la configuration spécifiée dans la section `Screen` avec l'identificateur `"Screen0"`.

  Si la carte vidéo a plus d'une tête, il faudra ajouter une entrée `Screen` avec un numéro différent et un identificateur différent pour la section `Screen`.

  Les nombres figurant à la droite de `"Screen0"` donnent les coordonnées absolues X et Y pour le coin supérieur gauche de l'écran (par défaut `0 0`).
- `InputDevice` — Spécifie le nom d'une section `InputDevice` à utiliser avec le serveur X.

  Il doit y avoir au moins deux entrées `InputDevice` : une pour la souris par défaut et une pour le clavier par défaut. Les options `CorePointer` et `CoreKeyboard` indiquent qu'il s'agit du clavier et de la souris primaires.
- `Option "<option-name>"` — Correspond à une entrée facultative qui précise des paramètres supplémentaires pour cette section. Tout paramètre spécifié ici remplacent ceux mentionnés dans la section `ServerFlags`.

  Remplacez *<option-name>* par une option valide pour cette section choisie parmi celles énumérées dans la page de manuel de `xorg.conf`.

Il est possible de créer plus d'une section `ServerLayout`. Toutefois, le serveur ne lira que la section apparaissant en premier, à moins qu'une autre section `ServerLayout` ne soit spécifiée en tant qu'argument en ligne de commande.

7.3.1.4. `Files`

La section `Files` établit les chemins d'accès vers des services vitaux pour le serveur X, comme le chemin des polices.

L'exemple suivant illustre une section `Files` typique :

```
Section "Files"
        RgbPath      "/usr/X11R6/lib/X11/rgb"
        FontPath     "unix/:7100"
EndSection
```

Parmi les entrées les plus communément utilisées dans la section `Files` figurent :

- `RgbPath` — Spécifie l'emplacement de la base de données de couleurs RVB (ou RGB de l'anglais Red Green Blue). Cette base de données définit tous les noms de couleurs valides dans X et les associe aux valeurs RVB particulières.
- `FontPath` — Spécifie l'endroit où le serveur X doit se connecter pour obtenir les polices du serveur de polices `xfs`.

Par défaut, la valeur de `FontPath` est `unix/:7100`. Cette dernière instruit le serveur X qu'il doit obtenir des informations de polices en utilisant les sockets de domaine UNIX pour les communications inter-processus (IPC) sur le port 7100.

Consultez la Section 7.4 pour obtenir de plus amples informations sur X et sur les polices.

- `ModulePath` — Représente un paramètre facultatif qui spécifie d'autres répertoires stockant des modules du serveur X.

7.3.1.5. `Module`

La section `Module` spécifie les modules du répertoire `/usr/X11R6/lib/modules/` que le serveur X doit charger. Les modules fournissent au serveur X des fonctionnalités supplémentaires.

L'exemple suivant illustre une section `Module` typique :

```
Section "Module"
 Load  "dbe"
 Load  "extmod"
 Load  "fbdevhw"
 Load  "glx"
 Load  "record"
 Load  "freetype"
 Load  "type1"
 Load  "dri"
EndSection
```

7.3.1.6. `InputDevice`

Chaque section `InputDevice` configure un périphérique d'entrée pour le serveur X. Les systèmes possèdent en général au moins deux sections `InputDevice` à savoir clavier et souris.

L'exemple suivant illustre une section `InputDevice` typique :

```
Section "InputDevice"
 Identifier  "Mouse0"
 Driver      "mouse"
 Option     "Protocol" "IMPS/2"
 Option     "Device" "/dev/input/mice"
 Option     "Emulate3Buttons" "no"
EndSection
```

Parmi les entrées les plus communément utilisées dans la section `InputDevice` figurent :

- `Identifier` — Spécifie un nom unique pour cette section `InputDevice`. Cette entrée est nécessaire.
- `Driver` — Spécifie le nom du pilote de périphérique que X doit charger pour le périphérique.
- `Option` — Spécifie des options nécessaires concernant le périphérique.

  Pour une souris, ces options sont généralement :

  - `Protocol` — Spécifie le protocole utilisé par la souris, comme par exemple `IMPS/2`.
  - `Device` — Spécifie l'emplacement du périphérique physique.
  - `Emulate3Buttons` — Spécifie si une souris à deux boutons doit se comporter comme une souris à trois boutons lorsque les deux boutons sont pressés simultanément.

  Consultez la page de manuel de `xorg.conf` pour obtenir une liste des options valides pour cette section.

Par défaut, la section `InputDevice` comporte des commentaires pour permettre aux utilisateurs de configurer des options supplémentaires.

7.3.1.7. `Monitor`

La section `Monitor` permet de configurer le type de moniteur utilisé par le système. Alors qu'une section `Monitor` est le minimum requis, il est tout à fait possible d'en avoir d'autres pour chaque type de moniteur utilisé par l'ordinateur.

La meilleure façon d'effectuer la configuration d'un moniteur consiste à configurer X lors du processus d'installation ou à utiliser l'**Outil de configuration X**. Pour obtenir de plus amples informations sur l'utilisation de l'**Outil de configuration X**, reportez-vous au chapitre intitulé *Configuration du système X Window* du *Guide d'administration système de Red Hat Enterprise Linux*.

Ci-dessous figure l'exemple d'une section `Monitor` typique pour un moniteur :

```
Section "Monitor"
 Identifier   "Monitor0"
 VendorName   "Monitor Vendor"
 ModelName    "DDC Probed Monitor - ViewSonic G773-2"
 DisplaySize  320 240
 HorizSync    30.0 - 70.0
 VertRefresh  50.0 - 180.0
EndSection
```

Avertissement

Faites très attention si vous éditez manuellement les valeurs de la section `Monitor` de `/etc/X11/xorg.conf`. En effet, l'utilisation de valeurs inappropriées dans cette section peut endommager ou même détruire un moniteur. Consultez la documentation accompagnant le moniteur pour obtenir une liste des paramètres sûr disponibles pour un bon fonctionnement.

Parmi les entrées les plus communément utilisées dans la section `Monitor` figurent :

- `Identifier` — Spécifie un nom unique utilisé pour cette section `Monitor`. Cette entrée est nécessaire.
- `VendorName` — Correspond à un paramètre facultatif précisant le nom du fabricant du moniteur.
- `ModelName` — Correspond à un paramètre facultatif précisant le nom de modèle du moniteur.
- `DisplaySize` — Correspond à un paramètre facultatif précisant en millimètres, la taille physique de la partie image du moniteur.
- `HorizSync` — Spécifie la gamme de fréquences sync horizontales compatible avec le moniteur en kHz. Ces valeurs aident le serveur X à déterminer la validité des entrées `Modeline` prédéfinies ou spécifiées pour le moniteur.
- `VertRefresh` — Spécifie la gamme des fréquences de rafraîchissement verticales prise en charge par le moniteur, en kHz. Ces valeurs aident le serveur X à déterminer la validité des entrées `Modeline` prédéfinies ou spécifiées pour le moniteur.
- `Modeline` — Représente un paramètre facultatif qui spécifie les modes vidéo supplémentaires utilisés par le moniteur pour des résolutions particulières, avec certaines résolutions de sync horizontal et de rafraîchissement vertical. Pour obtenir de plus amples explications sur les entrées `Modeline`, consultez la page de manuel de `xorg.conf`.

- `Option "<option-name>"` — Représente une entrée facultative qui précise des paramètres supplémentaires pour la section. Remplacez *<option-name>* par une option valide pour cette section, choisie parmi celles énumérées dans la page de manuel de `xorg.conf`.

7.3.1.8. `Device`

Chaque section `Device` configure une carte vidéo utilisée par le système. Alors qu'une section `Device` est le minimum requis, il tout à fait possible d'en avoir d'autres pour chaque carte vidéo installée sur l'ordinateur.

La meilleure façon de configurer une carte vidéo consiste à configurer X lors du processus d'installation ou à utiliser l'**Outil de configuration X**. Pour obtenir de plus amples informations sur l'utilisation de l'**Outil de configuration X**, reportez-vous au chapitre intitulé *Configuration du système X Window* du *Guide d'administration système de Red Hat Enterprise Linux*.

Ci-après figure l'exemple d'une section `Device` typique pour une souris :

```
Section "Device"
 Identifier  "Videocard0"
 Driver      "mga"
 VendorName  "Videocard vendor"
 BoardName   "Matrox Millennium G200"
 VideoRam    8192
        Option      "dpms"
EndSection
```

Parmi les options les plus communément utilisées dans la section `Device` figurent :

- `Identifier` — Spécifie un nom unique utilisé pour la section `Device`. Cette entrée est nécessaire.
- `Driver` — Spécifie le pilote particulier que le serveur X doit charger afin que la carte vidéo puisse être utilisée. Une liste de pilotes est disponible dans le fichier `/usr/X11R6/lib/X11/Cards`, qui est installé avec le paquetage `hwdata`.
- `VendorName` — Correspond à un paramètre facultatif précisant le nom du fabricant du moniteur.
- `BoardName` — Correspond à un paramètre facultatif précisant le nom de la carte vidéo.
- `VideoRam` — Représente un paramètre facultatif précisant la quantité de mémoire RAM en kilobits, disponible sur la carte vidéo. Ce paramètre n'est nécessaire que pour les cartes vidéo que X ne peut pas détecter pour déterminer la quantité de RAM vidéo.
- `BusID` — Correspond à une entrée facultative précisant l'emplacement du bus de la carte vidéo. Cette option n'est nécessaire que pour les systèmes dotés de cartes multiples.
- `Screen` — Correspond à une entrée facultative précisant le connecteur du moniteur ou la tête de la carte vidéo que la section `Device` configure. Cette option n'est nécessaire que pour les cartes vidéo à têtes multiples.

  Si de multiples moniteurs sont connectés à des têtes différentes sur la même carte vidéo, il est nécessaire non seulement d'avoir des sections `Device` séparées mais chacune de ces sections doit également avoir une valeur `Screen` différente.

  Les valeurs associées à l'entrée `Screen` doivent être entières. La première tête de la carte vidéo à une valeur de `0`. La valeur de chaque tête supplémentaire augmente d'une unité.
- `Option "<option-name>"` — Représente une entrée facultative qui précise des paramètres supplémentaires pour la section. Remplacez *<option-name>* par une option valide pour cette section, choisie parmi celles énumérées dans la page de manuel de `xorg.conf`.

  `"dpms"` est une des options très couramment utilisé afin d'activer le paramètre de conformité aux normes Service Star de l'alimentation pour le moniteur.

7.3.1.9. `Screen`

Chaque section `Screen` lie une carte vidéo (ou tête de carte vidéo) à un moniteur en référençant la section `Device` et la section `Monitor` pour chaque. Bien qu'une section `Screen` soit le minimum requis, il est possible d'avoir d'autres instances pour chaque combinaison vidéo et moniteur existant sur l'ordinateur.

Ci-dessous figure l'exemple d'une section `Screen` typique :

```
Section "Screen"
 Identifier "Screen0"
 Device     "Videocard0"
 Monitor    "Monitor0"
 DefaultDepth     16
 SubSection "Display"
  Depth     24
  Modes    "1280x1024" "1280x960" "1152x864" "1024x768" "800x600" "640x480"
 EndSubSection
 SubSection "Display"
  Depth     16
  Modes    "1152x864" "1024x768" "800x600" "640x480"
 EndSubSection
EndSection
```

Parmi les entrées les plus communément utilisées dans la section `Screen` figurent :

- `Identifier` — Spécifie un nom unique utilisé pour cette section `Screen`. Cette entrée est nécessaire.
- `Device` — Spécifie le nom unique d'une section `Device`. Cette entrée est nécessaire.
- `Monitor` — Spécifie le nom unique d'une section `Monitor`. Cette entrée est nécessaire.
- `DefaultDepth` — Spécifie l'intensité des couleurs par défaut, en bits. Dans l'exemple précédent, la valeur par défaut de `16` fournit des milliers de couleurs. De multiples entrées `DefaultDepth` sont acceptées, mais au moins une entrée est requise.
- `SubSection "Display"` — Spécifie les modes écran disponibles à une intensité de couleur donnée. Une section `Screen` peut contenir de multiples sous-sections `Display`, mais au moins une est nécessaire pour l'intensité de couleur spécifiée dans l'entrée `DefaultDepth`.
- `Option "<option-name>"` — Représente une entrée facultative qui précise des paramètres supplémentaires pour la section. Remplacez *<option-name>* par une option valide pour cette section, choisie parmi celles énumérées dans la page de manuel de `xorg.conf`.

7.3.1.10. `DRI`

La section facultative `DRI` spécifie les paramètres pour *Direct Rendering Infrastructure* (*DRI*). DRI est une interface dont la fonction principale est de permettre aux applications logicielles 3D de profiter des capacités d'accélération matérielle 3D intégrées dans la plupart du matériel vidéo moderne. De plus, DRI peut améliorer les performances 2D grâce à l'accélération matérielle, dans le cas où elle serait prise en charge par le pilote de la carte vidéo.

Cette section n'est pas prise en compte à moins que l'interface DRI ne soit activée dans la section `Module`.

Ci-dessous figure l'exemple d'une section `DRI` typique :

```
Section "DRI"
        Group        0
        Mode         0666
EndSection
```

Étant donné que différentes cartes vidéo utilisent la DRI de différentes manières, il est déconseillé de changer les valeurs de cette section sans consulter le lien suivant : http://dri.sourceforge.net.

7.4. Polices

Red Hat Enterprise Linux utilise deux méthodes pour gérer et afficher les polices sous X. Le sous-système de polices Fontconfig qui est relativement nouveau simplifie la gestion des polices et fournit des fonctions d'affichage avancées, comme le lissage. Ce système est utilisé automatiquement pour des applications programmées à l'aide de la boîte à outils graphiques Qt 3 ou GTK+ 2.

Pour des raisons de compatibilité, Red Hat Enterprise Linux fournit le sous-système de polices original core X font subsystem . Ce système, qui a plus de 15 ans, s'articule autour du *Serveur de polices X* (*xfs*).

Cette section examine la configuration des polices pour X utilisant les deux systèmes.

7.4.1. Fontconfig

Le sous-système de polices Fontconfig permet à des applications d'accéder directement aux polices du système et utilise Xft ou tout autre mécanisme de rendu des polices de Fontconfig avec un lissage avancé. Des applications graphiques peuvent utiliser la bibliothèque Xft avec Fontconfig afin de créer du texte à l'écran.

Au fil du temps, le sous-système de polices Fontconfig/Xft remplacera le sous-système de polices core X font subsystem.

Important

Le sous-système de polices Fontconfig ne peut pas encore être utilisé avec **OpenOffice.org** qui utilise sa propre technologie de rendu des polices.

Il est important de noter ici que Fontconfig utilise le fichier de configuration `/etc/fonts/fonts.conf` et que ce dernier ne doit pas être modifié manuellement.

Astuce

En raison de la transition vers le nouveau système de polices, les applications GTK+ 1.2 ne sont affectées par aucun changement apporté par le bais du dialogue **Préférences de polices** (accessible en sélectionnant le bouton **Menu principal** [sur le panneau] => **Préférences** => **Polices**). Pour ces applications, une police peut être configurée en ajoutant les lignes suivantes au fichier `~/.gtkrc.mine` :

```
style "user-font" {

fontset = "<font-specification>"

}

widget_class "*" style "user-font"
```

Remplacez `<font-specification>` par la spécification de police dans le style utilisé par les applications X classiques, comme par exemple, `-adobe-helvetica-medium-r-normal--*-120-*-*-*-*-*-*`. Il est possible d'obtenir une liste

complète des polices de base en exécutant `xlsfonts` ou d'en créer une de manière interactive en utilisant `xfontsel`.

7.4.1.1. Ajout de polices à Fontconfig

L'ajout de nouvelles polices au sous-système Fontconfig est un processus relativement simple.

1. Pour ajouter des polices à l'ensemble du système, copiez les nouvelles polices dans le répertoire `/usr/share/fonts/`. Il est judicieux de créer un nouveau sous-répertoire, tel que `local/` ou quelque chose de semblable, afin de pouvoir distinguer facilement entre les polices installées par l'utilisateur et celles installées par défaut.

   Pour ajouter de nouvelles polices pour un utilisateur spécifique, copiez les nouvelles polices dans le répertoire `.fonts/` du répertoire personnel (ou home) de l'utilisateur.

2. Pour mettre à jour le cache des informations de polices, utilisez la commande `fc-cache` comme dans l'exemple suivant :
   `fc-cache <path-to-font-directory>`

   Dans cette commande, remplacez `<path-to-font-directory>` par le répertoire contenant les nouvelles polices (soit `/usr/share/fonts/local/`, soit `/home/<user>/.fonts/`).

Astuce

Des utilisateurs individuels peuvent aussi installer des polices graphiquement en tapant `fonts:///` dans la barre d'adresse de **Nautilus** et en y faisant glisser les nouveaux fichiers de polices.

Important

Si le nom du fichier de polices se termine par une extension `.gz`, il s'agit d'un fichier compressé qui ne pourra pas être utilisé à moins d'être préalablement décompressé. Pour ce faire, utilisez la commande `gunzip` ou cliquez deux fois sur le fichier et faites glisser la police vers un répertoire dans **Nautilus**.

7.4.2. Système de polices Core X Font System

Pour des raisons de compatibilité, Red Hat Enterprise Linux inclut toujours le sous-système de polices core X font subsystem qui utilise le serveur de polices X (`xfs`) pour fournir les polices aux applications clients X.

Le serveur X recherche un serveur de polices spécifié dans la directive `FontPath` dans la section `Files` du fichier de configuration `/etc/X11/xorg.conf`. Pour obtenir de plus amples informations sur l'entrée `FontPath`, reportez-vous à la Section 7.3.1.4.

Le serveur X se connecte au serveur `xfs` sur un port déterminé afin d'obtenir des informations sur les polices. Dans de telles circonstances, le service `xfs` doit être en cours d'exécution pour que X puisse démarrer. Pour obtenir de plus amples informations sur la configuration de services à un niveau d'exécution particulier, reportez-vous au chapitre intitulé *Contrôle de l'accès aux services* du *Guide d'administration système de Red Hat Enterprise Linux*.

7.4.2.1. Configuration de `xfs`

Le script `/etc/rc.d/init.d/xfs` lance le serveur `xfs`. Il est possible de configurer plusieurs options dans son fichier de configuration `/etc/X11/fs/config`.

Ci-dessous figure une liste des options courantes :

- `alternate-servers` — Spécifie une liste d'autres serveurs de polices à utiliser si ce serveur de polices n'est pas disponible. Chaque serveur dans cette liste doit être séparé par une virgule.
- `catalogue` — Spécifie une liste classée de chemins de polices à utiliser. Chaque chemin de polices doit être séparé par une virgule.

  Utilisez la chaîne `:unscaled` immédiatement après le chemin de polices pour faire charger en premier les polices non-proportionnées dans cette liste. Spécifiez ensuite à nouveau le chemin de polices complet, pour que les autres polices proportionnées soient également chargées.
- `client-limit` — Spécifie le nombre maximum de clients que ce serveur de polices va approvisionner. La valeur par défaut est `10`.
- `clone-self` — Autorise le serveur de polices à reproduire une autre version de lui-même lorsque la limite de clients (`client-limit`) est atteinte. La valeur par défaut pour cette option est `on`.
- `default-point-size` — Spécifie la taille de point par défaut pour toute police qui ne spécifie pas cette valeur. La valeur par défaut est exprimée en décipoints. La valeur par défaut de `120` correspond à une police de 12 points.
- `default-resolutions` — Spécifie une liste de résolutions prises en charge par le serveur X. Chaque résolution figurant dans la liste doit être séparée par une virgule.
- `deferglyphs` — Spécifie si le chargement de *glyphs* (le graphique utilisé pour la représentation visuelle d'une police) doit être différé. Pour désactiver cette fonction, utilisez `none`, pour l'activer pour toutes ces polices, utilisez `all` ou pour ne l'activer que pour les polices 16-bit, utilisez `16`.
- `error-file` — Spécifie le chemin et le nom du fichier de l'endroit où les erreurs `xfs` doivent être enregistrées.
- `no-listen` — Empêche `xfs` d'être attentif à des protocoles spécifiques. Cette option a par défaut la valeur `tcp` afin d'empêcher `xfs` de recevoir des connexions sur les ports TCP, surtout pour des raisons de sécurité.

Astuce

Si vous utilisez `xfs` pour servir des polices à travers le réseau, supprimez cette ligne.

- `port` — Spécifie le port TCP sur lequel `xfs` recevra des connexions si l'option `no-listen` n'existe pas ou est désactivée par un commentaire.
- `use-syslog` — Spécifie si le journal d'erreurs système doit être utilisé.

7.4.2.2. Ajout de polices à `xfs`

Pour ajouter des polices au sous-système de polices core X font subsystem (`xfs`), suivez les étapes suivantes :

1. À moins qu'il n'existe déjà, créez un répertoire nommé `/usr/share/fonts/local/` à l'aide de la commande suivante, en étant connecté en tant que super-utilisateur (aussi appelé root) :
   ```
   mkdir /usr/share/fonts/local/
   ```

Si la création du répertoire `/usr/share/fonts/local/` est nécessaire, il faut ajouter ce dernier au chemin `xfs` à l'aide de la commande suivante, en étant connecté en tant que super-utilisateur :

```
chkfontpath --add /usr/share/fonts/local/
```

2. Copiez le nouveau fichier de polices dans le répertoire `/usr/share/fonts/local/`
3. Mettez à jour les informations de polices à l'aide de la commande suivante, en étant connecté en tant que super-utilisateur :

```
ttmkfdir -d /usr/share/fonts/local/ -o /usr/share/fonts/local/fonts.scale
```

4. Redémarrez le fichier de configuration du serveur de polices `xfs` à l'aide de la commande suivante, en étant connecté en tant que super-utilisateur :

```
service xfs reload
```

7.5. Niveaux d'exécution et X

Dans la plupart des cas, l'installation par défaut de Red Hat Enterprise Linux configure l'ordinateur pour qu'il démarre dans un environnement de connexion graphique, connu en tant que niveau d'exécution 5. Il est toutefois possible de démarrer en mode multi-utilisateur texte-seul, connu en tant que niveau d'exécution 3 et de démarrer ainsi une session X.

Pour obtenir de plus amples informations sur les niveaux d'exécution, reportez-vous à la Section 1.4.

Les sous-sections suivantes examinent la manière selon laquelle X démarre aussi bien au niveau d'exécution 3 qu'au niveau d'exécution 5.

7.5.1. Niveau d'exécution 3

Au niveau d'exécution 3, la meilleure façon de lancer une session X consiste à se connecter et à taper la commande `startx`. Cette commande `startx` est une commande frontale (ou front-end) à la commande `xinit`, qui lance le serveur X et y connecte les applications client X. Étant donné que l'utilisateur est déjà connecté au système au niveau d'exécution 3, `startx` ne lance pas un gestionnaire d'affichage et n'authentifie pas les utilisateurs. Pour obtenir de plus amples informations sur les gestionnaires d'affichage, reportez-vous à la Section 7.5.2.

Lorsque la commande `startx` est exécutée, elle recherche un fichier `.xinitrc` dans le répertoire personnel de l'utilisateur pour définir l'environnement de bureau et, le cas échéant, d'autres applications client X à lancer. Si aucun fichier `.xinitrc` n'existe, elle utilisera à sa place le fichier `/etc/X11/xinit/xinitrc` par défaut du système.

Le script `xinitrc` par défaut recherche alors les fichiers définis par l'utilisateur et les fichiers système par défaut, y compris `.Xresources`, `.Xmodmap` et `.Xkbmap` dans le répertoire personnel de l'utilisateur d'une part, et `Xresources`, `Xmodmap` et `Xkbmap` dans le répertoire `/etc/X11/` d'autre part. Les fichiers `Xmodmap` et `Xkbmap`, s'ils existent, sont utilisés par l'utilitaire `xmodmap` pour configurer le clavier. Les fichiers `Xresources` sont lus afin d'assigner des valeurs préférentielles spécifiques aux applications.

Après avoir paramétré ces options, le script `xinitrc` exécute tous les scripts situés dans le répertoire `/etc/X11/xinit/xinitrc.d/`. Parmi les scripts importants faisant partie de ce répertoire figure `xinput`, permettant de configurer des paramètres comme la langue par défaut.

Ensuite, le script `xinitrc` essaie d'exécuter `.Xclients` dans le répertoire personnel (home) de l'utilisateur et recourt à `/etc/X11/xinit/Xclients` s'il ne peut pas le trouver. Le rôle du fichier `Xclients` est de démarrer l'environnement de bureau ou, le cas échéant, un simple gestionnaire de fenêtres élémentaire. Le script `.Xclients` dans le répertoire personnel de l'utilisateur lance l'environnement de bureau spécifié par l'utilisateur dans le fichier `.Xclients-default`. Si le fichier `.Xclients` n'existe pas dans le répertoire personnel de l'utilisateur, le script standard

`/etc/X11/init/Xclients` tente de lancer un autre environnement de bureau, en premier GNOME et en second KDE, suivi de `twm`.

L'utilisateur revient à une session utilisateur en mode texte après s'être déconnecté de X au niveau d'exécution 3.

7.5.2. Niveau d'exécution 5

Lorsque le système démarre au niveau d'exécution 5, une application client X spéciale appelée gestionnaire d'affichage, est lancée. Un utilisateur doit s'authentifier en utilisant le gestionnaire d'affichage avant que tout environnement de bureau ou gestionnaire de fenêtres ne puisse être lancé.

Selon les environnements de bureau installés sur le système, trois gestionnaires d'affichage différents sont disponibles pour assurer l'authentification de l'utilisateur.

- `GNOME` — Le gestionnaire d'affichage par défaut pour Red Hat Enterprise Linux, `GNOME` permet à l'utilisateur de configurer des paramètres de langue, l'arrêt, le redémarrage et la connexion au système.
- `KDE` — Le gestionnaire d'affichage de KDE qui permet à l'utilisateur de démarrer, arrêter et se connecter au système.
- `xdm` — Un gestionnaire d'affichage rudimentaire ne permettant que la connexion de l'utilisateur au système.

Lors du démarrage au niveau d'exécution 5, le script `prefdm` détermine le gestionnaire d'affichage de préférence en consultant le fichier `/etc/sysconfig/desktop`. Pour obtenir une liste des options disponibles pour ce fichier, reportez-vous au fichier `/usr/share/doc/initscripts-<version-number>/sysconfig.txt` (où *<version-number>* correspond au numéro de version du paquetage `initscripts`).

Chacun des gestionnaires d'affichage référence le fichier `/etc/X11/xdm/Xsetup_0` pour paramétrer l'écran de connexion. Une fois que l'utilisateur s'est connecté au système, le script `/etc/X11/xdm/GiveConsole` s'exécute pour assigner à l'utilisateur la propriété de la console. Ensuite, le script `/etc/X11/xdm/Xsession` se lance pour effectuer de nombreuses tâches habituellement exécutées par le script `xinitrc` lorsque X est démarré au niveau d'exécution 3, y compris le paramétrage du système et des ressources de l'utilisateur ainsi que le lancement des scripts contenus dans le répertoire `/etc/X11/xinit/xinitrc.d/`.

Les utilisateurs peuvent spécifier l'environnement de bureau qu'ils souhaitent utiliser quand ils s'authentifient avec des gestionnaires d'affichage `GNOME` ou `KDE` en faisant leur choix dans le menu **Sessions** (accessible en choisissant le bouton **Menu principal** [sur le panneau] => **Préférences** => **Préférences supplémentaires** => **Sessions**). Si l'environnement de bureau n'est pas spécifié dans le gestionnaire de fenêtres, le script `/etc/X11/xdm/Xsession` vérifie les fichiers `.xsession` et `.Xclients` dans le répertoire personnel de l'utilisateur pour décider quel environnement de bureau charger. En dernier ressort, le fichier `/etc/X11/xinit/Xclients` est utilisé pour sélectionner un environnement de bureau ou gestionnaire de fenêtres à utiliser, de la même façon que pour le niveau d'exécution 3.

Lorsque l'utilisateur termine une session X sur l'affichage par défaut (`:0`) et se déconnecte, le script `/etc/X11/xdm/TakeConsole` s'exécute et réassigne la propriété de la console au super-utilisateur (ou root). Le gestionnaire d'affichage original, qui ne s'est pas arrêté depuis la connexion de l'utilisateur, prend le contrôle en lançant un nouveau gestionnaire d'affichage. Ce faisant, le serveur X est redémarré, un nouvel écran d'authentification est affiché et tout le processus recommence à nouveau.

L'utilisateur revient au gestionnaire d'affichage après s'être déconnecté de X au niveau d'exécution 5.

Pour obtenir de plus amples informations sur le contrôle de l'authentification des utilisateurs par les gestionnaires d'affichage, reportez-vous d'une part au fichier

`/usr/share/doc/gdm-<version-number>/README` (où `<version-number>` correspond au numéro de version du paquetage `gdm` installé) et d'autre part à la page de manuel de `xdm`.

7.6. Ressources supplémentaires

Il existe de nombreuses informations détaillées concernant le serveur X, les clients qui s'y connectent et les environnements de bureau et gestionnaires de fenêtres variés.

7.6.1. Documentation installée

- `/usr/X11R6/lib/X11/doc/README` — Document offrant une brève description de l'architecture XFree86 et de la façon d'obtenir des informations supplémentaires sur le projet XFree86 en tant que nouvel utilisateur.
- `/usr/X11R6/lib/X11/doc/RELNOTES` — Document destiné aux utilisateurs avancés qui désirent connaître les dernières fonctions offertes par XFree86.
- `man xorg.conf` — Page de manuel contenant des informations sur les fichiers de configuration `xorg.conf`, y compris la signification et la syntaxe des différentes sections figurant dans les fichiers.
- `man X.Org` — Page de manuel principale pour obtenir des informations sur la Fondation X.Org.
- `man Xorg` — Page de manuel décrivant le serveur d'affichage X11R6.8.

7.6.2. Sites Web utiles

- http://www.X.org/ — Page d'accueil du projet de la fondation X.Org, qui produit la version X11R6.8 du système X Window. La version X11R6.8 est offerte avec Red Hat Enterprise Linux pour contrôler le matériel nécessaire et fournir un environnement d'interface graphique (ou GUI).
- http://xorg.freedesktop.org/ — Page d'accueil de la version XR116.8, qui fournit des binaires et de la documentation pour le système X Window.
- http://dri.sourceforge.net/ — Page d'accueil du projet DRI (Direct Rendering Infrastructure). La DRI est le composant central de l'accélération matérielle 3D pour X.
- http://www.gnome.org/ — Page d'accueil du projet GNOME.
- http://www.kde.org/ — Page d'accueil de l'environnement de bureau KDE.
- http://nexp.cs.pdx.edu/fontconfig/ — Page d'accueil du sous-système de polices Fontconfig pour X.

7.6.3. Livres sur le sujet

- *The Concise Guide to XFree86 for Linux* de Aron Hsiao ; Que — Fournit l'avis d'un expert sur le fonctionnement de XFree86 sur les systèmes Linux.
- *The New XFree86* de Bill Ball ; Prima Publishing — Examine XFree86 et sa relation avec les environnements de bureau couramment utilisés, comme GNOME et KDE.
- *Beginning GTK+ and GNOME* de Peter Wright ; Wrox Press, Inc. — Présente aux programmeurs l'architecture GNOME, leur montrant comment débuter dans GTK+.

- *GTK+/GNOME Application Development* de Havoc Pennington ; New Riders Publishing — Fournit un examen avancé au coeur de la programmation GTK+, concentré sur un échantillon de code et une étude exhaustive des API disponibles.
- *KDE 2.0 Development* de David Sweet et Matthias Ettrich ; Sams Publishing — Explique aux développeurs débutants et avancés comment exploiter au maximum les nombreuses directives d'environnement nécessaires à l'élaboration d'applications QT pour KDE.

II. Références pour les services réseau

Il est possible de déployer une grande variété de services réseau sous Red Hat Enterprise Linux. Cette section décrit la configuration des interfaces réseau et fournit des informations détaillées sur les services réseau critiques tels que NFS, NFS, Serveur HTTP Apache, Sendmail, Postfix, Fetchmail, Procmail, BIND et LDAP et Samba.

Table des matières

Chapitre 8.

Interfaces réseau

Sous Red Hat Enterprise Linux, toutes les communications réseau se font entre des *interfaces* logicielles configurées et des *périphériques réseau physiques* connectés au système.

Les fichiers de configuration pour les interfaces réseau et les scripts permettant de les activer et désactiver sont placés dans le répertoire `/etc/sysconfig/network-scripts/`. Bien que le nombre et le type de fichiers d'interfaces puissent différer d'un système à l'autre, ce répertoire contient trois types de fichiers :

- *fichiers de configuration d'interfaces*
- *scripts de contrôle d'interfaces*
- *fichiers des fonctions réseau*

Les fichiers faisant partie de chacune de ces catégories fonctionnent en coopération afin de permettre l'activation de divers périphériques réseau.

Ce chapitre explore la relation entre ces fichiers et leur utilisation.

8.1. Fichiers de configuration réseau

Avant d'examiner les fichiers de configuration d'interfaces, dressons la liste des fichiers de configuration primaires utilisés pour configurer le réseau. Le fait de comprendre le rôle joué par ces fichiers dans la mise en place de la pile réseau peut s'avérer utile lors de la personnalisation de votre système Red Hat Enterprise Linux.

Les fichiers de configuration de réseau primaire sont les suivants :

- `/etc/hosts` — L'objectif principal de ce fichier est de résoudre les noms d'hôtes n'ayant pu être résolus d'une autre façon. Il peut également être utilisé pour résoudre des noms d'hôtes sur de petits réseaux ne disposant pas de serveur DNS. Quel que soit le type de réseau utilisé par l'ordinateur, ce fichier doit contenir une ligne spécifiant l'adresse IP du périphérique de bouclage (loopback) (`127.0.0.1`) en tant que `localhost.localdomain`. Pour obtenir davantage d'informations, consultez la page de manuel de `hosts`.
- `/etc/resolv.conf` — Ce fichier précise les adresses IP des serveurs DNS et le domaine de recherche. À moins d'être configuré autrement, les scripts d'initialisation du réseau sont contenus dans ce fichier. Pour obtenir davantage d'informations sur ce fichier, consultez la page de manuel de `resolv.conf`.
- `/etc/sysconfig/network` — Ce fichier précise les informations de routage et d'hébergement (hôte) pour toutes les interfaces réseau. Pour obtenir davantage d'informations sur ce fichier et sur les directives qu'il accepte, reportez-vous à la Section 4.1.25.
- `/etc/sysconfig/network-scripts/ifcfg-<interface-name>` — Pour chaque interface réseau, il existe un script de configuration d'interfaces correspondant. Chacun de ces fichiers fournit des informations spécifiques à une interface réseau particulière. Consultez la Section 8.2 pour obtenir davantage d'informations sur ce type de fichier et les directives qu'il accepte.


Attention

Le répertoire `/etc/sysconfig/networking/` est utilisé par l'**Outil d'administration réseau** (`system-config-network`) et son contenu ne doit pas être modifié manuellement. De plus, toute utilisation de l'**Outil d'administration réseau**, même le simple lancement de l'application, écrasera toutes les directives précédemment configurées dans `/etc/sysconfig/network-scripts`. Vu le risque de suppression de configuration, il est fortement recommandé de n'utiliser qu'une seule méthode pour la configuration réseau.

Pour obtenir davantage d'informations sur la configuration des interfaces réseau à la'ide de l'**Outil d'administration réseau**, consultez le chapitre intitulé *Configuration réseau* du *Guide d'administration système de Red Hat Enterprise Linux*.

8.2. Fichiers de configuration des interfaces

Les fichiers de configuration d'interfaces contrôlent le fonctionnement des interfaces logicielles associées aux périphériques réseau individuels. Lorsque votre système Red Hat Linux démarre, il utilise ces fichiers pour savoir quelles interfaces il doit afficher automatiquement et comment les configurer. Ces fichiers sont en général nommés `ifcfg-<name>`, où *<name>* fait référence au nom du périphérique contrôlé par le fichier de configuration.

8.2.1. Interfaces Ethernet

Le fichier `ifcfg-eth0` représente l'un des fichiers d'interfaces les plus courants ; il contrôle la première *carte d'interface réseau* Ethernet ou *NIC* (de l'anglais Network Interface Card) du système. Dans un système comportant plusieurs cartes, il y a plusieurs fichiers `ifcfg-eth`*<X>* (où *<X>* correspond à un numéro unique associé à une interface spécifique). Étant donné que chaque périphérique a son propre fichier de configuration, un administrateur peut contrôler le fonctionnement individuel de chaque interface.

Ci-dessous figure un exemple de fichier `ifcfg-eth0` pour un système utilisant une adresse IP fixe :

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
NETWORK=10.0.1.0
NETMASK=255.255.255.0
IPADDR=10.0.1.27
USERCTL=no
```

Les valeurs requises dans un fichier de configuration d'interfaces peuvent changer en fonction d'autres valeurs. Par exemple, le fichier `ifcfg-eth0` pour une interface utilisant DHCP est légèrement différent, car les informations IP sont fournies par le serveur DHCP :

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

L'**Outil d'administration réseau** (`system-config-network`) permet de modifier facilement les différents fichiers de configuration des interfaces réseau (reportez-vous au chapitre intitulé *Configuration réseau* du *Guide d'administration système de Red Hat Enterprise Linux* pour obtenir des instructions détaillées sur l'utilisation de cet outil).

Cependant, vous pouvez également modifier manuellement les fichiers de configuration pour une interface réseau donnée.

Vous trouverez ci-dessous une liste de paramètres pouvant être configurés dans un fichier de configuration d'interface Ethernet :

- `BOOTPROTO=<protocol>`, où `<protocol>` correspond à l'une des valeurs suivantes :
  - `none` — Indique qu'aucun protocole de démarrage ne devrait être utilisé.
  - `bootp` — Indique que le protocole BOOTP devrait être utilisé.
  - `dhcp` — Indique que le protocole DHCP devrait être utilisé.

- `BROADCAST=<address>`, où `<address>` correspond à l'adresse de diffusion. Cette directive a été abandonnée car la valeur est calculée automatiquement avec `ifcalc`.
- `DEVICE=<name>`, où `<name>` correspond au nom du périphérique physique (à l'exception des périphériques PPP à affectation dynamique où il s'agit du *nom logique*).
- `DHCP_HOSTNAME` — N'utilisez cette option que si le serveur DHCP a besoin du client pour spécifier un nom d'hôte avant de recevoir une adresse IP. (Avec Red Hat Enterprise Linux, le démon serveur DHCP ne prend pas en charge cette fonctionnalité.)
- `DNS{1,2}=<address>`, où `<address>` correspond à l'adresse d'un serveur devant être placée dans `/etc/resolv.conf` si la directive `PEERDNS` est réglée sur la valeur `yes`.
- `ETHTOOL_OPTS=<options>`, où `<options>` correspond à toutes les options spécifiques au périphériques qui sont prises en charge par `ethtool`. Par exemple, si vous souhaitiez forcer 100 Mo en transmission bidirectionnelle simultanée(ou full-duplex), vous choisiriez les paramètres suivants :

  ```
  ETHTOOL_OPTS="autoneg off speed 100 duplex full"
  ```

  Notez bien que la modification des paramètres de vitesse ou duplex nécessite presque toujours la désactivation de l'auto-négotiation à l'aide de l'option `autoneg off`. Ce point doit être mentionné en premier car les entrées d'options sont tributaires de l'ordre dans lequel elles apparaissent.
- `GATEWAY=<address>`, où `<address>` correspond à l'adresse IP du routeur réseau ou du périphérique de passerelle (s'il existe).
- `HWADDR=<MAC-address>`, où `<MAC-address>` correspond à l'adresse matérielle du périphérique Ethernet sous la forme `AA:BB:CC:DD:EE:FF`. Cette directive est utile pour les machines possédant de multiples NIC pour s'assurer que les interfaces sont assignées aux bons noms de périphériques indépendamment de l'ordre de chargement configuré pour chaque module de NIC. Cette directive ne devrait *pas* être utilisée avec `MACADDR`.
- `IPADDR=<address>`, où `<address>` correspond à l'adresse IP.
- `MACADDR=<MAC-address>`, où `<MAC-address>` correspond à l'adresse matérielle du périphérique Ethernet sous la forme `AA:BB:CC:DD:EE:FF`. Cette directive est utilisée pour assigner une adresse MAC à une interface, écrasant celle assignée par le NIC physique. Cette directive ne devrait *pas* être utilisée avec `HWADDR`.
- `MASTER=<bond-interface>`, où `<bond-interface>` correspond à l'interface de liaison de canaux à laquelle l'interface Ethernet est liée.

  Cette directive est utilisée en conjonction avec la directive `SLAVE`.

  Reportez-vous à la Section 8.2.3 pour obtenir davantage d'informations sur les interfaces de liaison de canaux.
- `NETMASK=<mask>`, où `<mask>` correspond à la valeur du masque réseau.
- `NETWORK=<address>`, où `<address>` correspond à l'adresse du réseau. Cette directive a été abandonnée car la valeur est calculée automatiquement avec `ifcalc`.
- `ONBOOT=<answer>`, où `<answer>` correspond à l'une des valeurs suivantes :

- `yes` — Indique que ce périphérique devrait être activé au démarrage.
- `no` — Indique que ce périphérique ne devrait pas être activé au démarrage.

- `PEERDNS=<answer>`, où `<answer>` correspond à l'une des valeurs suivantes :
  - `yes` — Modifier `/etc/resolv.conf` si la directive DNS est paramétrée. Si DHCP est utilisé, `yes` est alors la valeur par défaut.
  - `no` — Ne pas modifier `/etc/resolv.conf`.

- `SLAVE=<bond-interface>`,où `<bond-interface>` correspond à l'une des valeurs suivantes :
  - `yes` — Ce périphérique est contrôlé par l'interface de liaison de canaux spécifiée dans la directive `MASTER`.
  - `no` — Ce périphérique n'est *pas* contrôlé par l'interface de liaison de canaux spécifiée dans la directive `MASTER`.

  Cette directive est utilisée en conjonction avec la directive `MASTER`.

  Reportez-vous à la Section 8.2.3 pour obtenir de plus amples informations sur les interfaces de liaison de canaux.
- `SRCADDR=<address>`, où `<address>` correspond à l'adresse IP source spécifiée pour les paquets sortants.
- `USERCTL=<answer>`, où `<answer>` correspondant à l'une des valeurs suivantes :
  - `yes` — Les utilisateurs autres que le super-utilisateur sont autorisés à contrôler ce périphérique.
  - `no` — Les utilisateurs autres que le super-utilisateur ne sont pas autorisés à contrôler ce périphérique.

8.2.2. Interfaces IPsec

Avec Red Hat Enterprise Linux il est possible de se connecter à d'autres hôtes ou réseaux à l'aide d'une connexion IP sécurisée appelée IPsec. Pour obtenir des instructions sur la configuration d'IPsec à l'aide de l'**Outil d'administration réseau** (`system-config-network`) reportez-vous au chapitre intitulé *Configuration réseau* du *Guide d'administration système de Red Hat Enterprise Linux*. Pour obtenir des informations sur la configuration manuelle d'IPsec, consultez le chapitre intitulé *Réseaux virtuels privés* du *Guide de sécurité de Red Hat Enterprise Linux*.

L'extrait suivant correspond au fichier `ifcfg` d'une connexion IPsec de réseau à réseau pour le LAN A. Le nom unique permettant d'identifier la connexion de notre exemple est `ipsec1`, d'où le nom `/etc/sysconfig/network-scripts/ifcfg-ipsec1` donné au fichier qui lui correspond.

```
TYPE=IPsec
ONBOOT=yes
IKE_METHOD=PSK
SRCNET=192.168.1.0/24
DSTNET=192.168.2.0/24
DST=X.X.X.X
```

Dans cet exemple, la valeur `X.X.X.X` correspond à l'adresse IP routable sur un réseau public du routeur IPsec de destination.

Ci-dessous figure une liste des paramètres configurables peuvant s'appliquer à une interface IPsec :

- `DST=<address>`, où `<address>` représente l'adresse IP de l'hôte ou du routeur IPsec de destination. Ce paramètre est utilisé aussi bien pour des connexions IPsec d'hôte à hôte que pour des connexions IPsec de réseau à réseau.
- `DSTNET=<network>`, où `<network>` représente l'adresse réseau du réseau IPsec de destination. Ce paramètre est seulement utilisé pour des configurations IPsec de réseau à réseau.
- `SRC=<address>`, où `<address>` représente l'adresse IP de l'hôte ou du routeur IPsec source. Ce paramètre, disponible en tant qu'option, est seulement utilisé pour des connexions IPsec d'hôte à hôte.
- `SRCNET=<network>`, où `<network>` représente l'adresse réseau du réseau Ipsec source. Ce paramètre est seulement utilisé pour des configurations Ipsec de réseau à réseau.
- `TYPE=<interface-type>`, où `<interface-type>` a la valeur `IPSEC`. Les deux applications font partie du paquetage `ipsec-tools`.

Reportez-vous au fichier `/usr/share/doc/initscripts-<version-number>/sysconfig.txt` (remplacez `<version-number>` par le numéro de version du paquetage `initscripts` installé) pour obtenir des informations sur les paramètres de configuration, si vous utilisez des clés manuelles de cryptage avec Ipsec.

Le démon de gestion des clés IKEv1 baptisé `racoon` négocie et configure un ensemble de paramètres pour IPSec. Il peut utiliser des clés pré-partagées, des signatures RSA ou GSS-API. Si `racoon` est utilisé pour gérer automatiquement le cryptage des clés, les options suivantes sont alors requises :

- `IKE_METHOD=<encryption-method>`, où `<encryption-method>` représente `PSK`, `X509` ou `GSSAPI`. Si la valeur `PSK` est spécifiée, le paramètre `IKE_PSK` doit lui aussi être défini. Si la valeur `X509` est mentionnée, le paramètre `IKE_CERTFILE` doit lui aussi être défini.
- `IKE_PSK=<shared-key>`, où `<shared-key>` correspond à la valeur secrète et partagée de la méthode PSK (de l'anglais preshared keys).
- `IKE_CERTFILE=<cert-file>` où `<cert-file>` correspond à un fichier de certificats X.509 valide pour l'hôte.
- `IKE_PEER_CERTFILE=<cert-file>` où `<cert-file>` correspond à un fichier de certificats X.509 valide pour l'hôte *distant*.
- `IKE_DNSSEC=<answer>` où `<answer>` correspond à `yes`. Le démon `racoon` extrait le certificat X.509 de l'hôte distant via DNS. Si un paramètre `IKE_PEER_CERTFILE` est défini, *n'incluez pas* le paramètre ci-dessus.

Pour obtenir de plus amples informations sur les algorithmes de cryptage disponibles pour IPsec, consultez la page de manuel de `setkey`. Pour davantage d'informations sur `racoon`, reportez-vous aux pages de manuel de `racoon` et `racoon.conf`.

8.2.3. Interfaces de liaison de canaux

Red Hat Enterprise Linux permet aux administrateurs de lier ensemble plusieurs interfaces réseau pour ne former qu'un seul canal à l'aide du module de noyau `bonding` et d'une interface de réseau spéciale appelée interface de liaison de canaux. La liaison de canaux permet à plusieurs interfaces réseau d'agir comme une seule interface, augmentant simultanément la largeur de bande et offrant alors une certaine redondance.

Pour créer une interface de liaison de canaux, créez un fichier dans le répertoire `/etc/sysconfig/network-scripts/` nommé `ifcfg-bond<N>`, en remplaçant `<N>` par le numéro de l'interface, comme par exemple `0`.

Le contenu du fichier peut être identique à tout type d'interface qui sera lié, comme par exemple une interface Ethernet. La seule différence repose sur le fait que la directive `DEVICE=` doit correspondre à `bond<N>`, où `<N>` représente le numéro de l'interface.

Ci-dessous figure un exemple de fichier de configuration de liaison de canaux :

```
DEVICE=bond0
BOOTPROTO=none
ONBOOT=yes
NETWORK=10.0.1.0
NETMASK=255.255.255.0
IPADDR=10.0.1.27
USERCTL=no
```

Une fois l'interface de liaison de canaux créée, les interfaces réseau à lier ensemble doivent être configurées en ajoutant les directives `MASTER=` et `SLAVE=` dans leurs fichiers de configuration. Les fichiers de configuration pour chaque interface de liaison de canaux peuvent être pratiquement identiques.

Par exemple, dans le cas de deux interfaces Ethernet de liaison de canaux, `eth0` et `eth1` peuvent ressembler à l'extrait suivant :

```
DEVICE=eth<N>
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
SLAVE=yes
USERCTL=no
```

Dans cet exemple, remplacez *<N>* par la valeur numérique de l'interface.

Pour qu'une interface de liaison de canaux soit valide, le module de noyau doit être chargé. Pour s'assurer que le module est bien chargé lorsque l'interface de liaison de canaux est activée, ajoutez la ligne suivante dans `/etc/modules.conf` :

```
alias bond<N> bonding
```

Remplacez *<N>* par le numéro de l'interface, comme par exemple `0`. Pour chaque interface de liaison de canaux, une entrée correspondante doit se trouver dans `/etc/modules.conf`.

Une fois que `/etc/modules.conf` est configuré et que l'interface de liaison de canaux et les interfaces réseau sont elles aussi configurées, la commande `ifup` peut être utilisée pour activer l'interface de liaison de canaux.

Important

Les aspects importants de l'interface de liaison de canaux sont contrôlés par le module de noyau. Pour davantage d'informations sur le contrôle des modules `bonding`, reportez-vous à la Section A.3.2.

8.2.4. Fichiers alias et clone

Il existe deux types de fichiers de configuration d'interfaces d'une utilisation moins courante : les fichiers *alias* et *clone*.

Les fichiers de configuration d'interface alias qui sont utilisés principalement pour lier plusieurs adresses à une seule interface, suivent le principe de nommage `ifcfg-<if-name>:<alias-value>`.

Par exemple, un fichier `ifcfg-eth0:0` peut être configuré pour spécifier `DEVICE=eth0:0` et une adresse IP statique de 10.0.0.2, servant donc d'alias pour une interface Ethernet déjà configurée pour

recevoir ses informations IP via DHCP dans `ifcfg-eth0`. Avec une telle configuration, le périphérique `eth0` est lié à une adresse IP dynamique, mais la même carte réseau physique peut recevoir des requêtes via l'adresse IP fixe 10.0.0.2.

Attention

Les interfaces alias ne prennent pas en charge DHCP.

Le nom d'un fichier de configuration d'interface clone doit suivre le format suivant : `ifcfg-<if-name>-<clone-name>`. Alors qu'un fichier alias autorise plusieurs adresses pour une interface existante, un fichier clone lui permet de spécifier des options complémentaires pour une interface. Par exemple, le fichier d'une interface Ethernet DHCP standard appelée `eth0`, pourrait ressembler à l'extrait ci-dessous :

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
```

Puisque la valeur par défaut de la directive `USERCTL` est `no` si aucune valeur n'est spécifiée, les utilisateurs ne peuvent pas activer ou désactiver cette interface. Pour permettre aux utilisateurs de le faire, créez un clone en copiant `ifcfg-eth0` dans `ifcfg-eth0-user`, puis ajoutez la ligne suivante dans `ifcfg-eth0-user` :

```
USERCTL=yes
```

De cette manière, un utilisateur peut activer l'interface `eth0` avec la commande `/sbin/ifup eth0-user` puique les options de configuration de `ifcfg-eth0` sont combinées à celles de `ifcfg-eth0-user`. Bien qu'il s'agisse ici d'un exemple élémentaire, cette méthode peut être utilisée avec des options et interfaces diverses.

La méthode la plus simple pour créer des fichiers de configuration d'interface alias et clone consiste à utiliser l'**Outil d'administration réseau** graphique. Pour en savoir plus sur l'utilisation de cet outil, reportez-vous au chapitre intitulé *Configuration réseau* du *Guide d'administration système de Red Hat Enterprise Linux*.

8.2.5. Interfaces de connexion par modem

Si vous vous connectez à un réseau comme l'Internet par l'intermédiaire d'une connexion commutée PPP, il vous faut un fichier de configuration pour cette interface.

Le nom des fichiers d'interface PPP est attribué selon le format suivant : `ifcfg-ppp<X>` (où `<X>` représente un numéro unique correspondant à une interface spécifique).

Le fichier de configuration d'interface PPP est créé automatiquement lorsque vous utilisez `wvdial`, l'**Outil d'administration réseau** ou alors, **Kppp** est utilisé pour créer un compte de connexion par modem. Vous pouvez également créer et éditer ce fichier manuellement.

Un fichier `ifcfg-ppp0` typique ressemble à l'extrait ci-dessous :

```
DEVICE=ppp0
NAME=test
WVDIALSECT=test
MODEMPORT=/dev/modem
LINESPEED=115200
PAPNAME=test
USERCTL=true
```

```
ONBOOT=no
PERSIST=no
DEFROUTE=yes
PEERDNS=yes
DEMAND=no
IDLETIMEOUT=600
```

Le *protocole Internet ligne série (SLIP)* (de l'anglais Serial Line Internet Protocol) constitue une autre interface de connexion commutée, même s'il est moins fréquemment utilisé. Les fichiers SLIP ont des noms de fichiers de configuration d'interface de type `ifcfg-sl0`.

Parmi les options dont nous n'avons pas encore parlé, et qui peuvent être utilisées dans ces fichiers, figurent :

- `DEFROUTE=<answer>`, où `<answer>` correspond à l'une des valeurs suivantes :
  - `yes` — Indique que cette interface doit être configurée comme itinéraire par défaut.
  - `no` — Indique que cette interface ne doit pas être configurée comme itinéraire par défaut.

- `DEMAND=<answer>`, où `<answer>` correspond à l'une des valeurs suivantes :
  - `yes` — Indique que cette interface permettra à `pppd` d'initialiser une connexion lorsque quelqu'un essaiera de l'utiliser.
  - `no` — Indique qu'une connexion doit être établie manuellement pour cette interface.

- `IDLETIMEOUT=<value>`, où `<value>` correspond au nombre de secondes d'inactivité engendrant la déconnexion automatique de l'interface.
- `INITSTRING=<string>`, où `<string>` correspond à la chaîne d'initialisation transférée au modem. Cette option est principalement utilisée avec les interfaces SLIP.
- `LINESPEED=<value>`, où `<value>` correspond à la vitesse de transmission (en bauds) du périphérique. Parmi les valeurs standard possibles figurent `57600`, `38400`, `19200` et `9600`.
- `MODEMPORT=<device>`, où `<device>` correspond au nom du périphérique série utilisé pour établir la connexion pour l'interface.
- `MTU=<value>`, où `<value>` correspond au paramètre *unité de transfert maximum (MTU)* (de l'anglais Maximum Transfer Unit) pour l'interface. La valeur de MTU correspond au nombre maximal d'octets de données qu'un cadre peut comporter, sans compter les informations d'en-tête. Dans certaines situations de connexion par modem, le réglage de ce paramètre sur la valeur `576` entraîne une réduction du nombre de paquets éliminés abandonnés et une légère augmentation du débit de connexion.
- `NAME=<nom>`, où `<nom>` correspond à la référence au nom donné à un ensemble de configurations de connexions commutées.
- `PAPNAME=<name>`, où `<name>` correspond au nom d'utilisateur donné lors de l'échange d'informations avec le *protocole d'authentification du mot de passe (PAP)* (de l'anglais, Password Authentication Protocol) afin de permettre la connexion à un système distant.
- `PERSIST=<answer>`, où `<answer>` correspond à l'une des valeurs suivantes :
  - `yes` — Spécifie que cette interface doit rester active en permanence, même si elle est désactivée lorsqu'un modem raccroche.
  - `no` — Spécifie que cette interface ne doit pas rester active en permanence.

- `REMIP=<address>`, où `<address>` correspond à l'adresse IP du système distant. Cette valeur n'est généralement pas spécifiée.
- `WVDIALSECT=<name>`, où `<name>` associe cette interface à une configuration de composeur dans `/etc/wvdial.conf`. Ce fichier contient le numéro de téléphone à composer et d'autres informations importantes pour l'interface.

8.2.6. Autres interfaces

Parmi d'autres fichiers de configuration d'interfaces courants figurent :

- `ifcfg-lo` — Une *interface de bouclage* locale (loopback) est souvent utilisée pour effectuer des tests et pour une utilisation dans un certain nombre d'applications qui nécessitent une adresse IP référant au même système. Toutes les données envoyées au périphérique de bouclage sont immédiatement renvoyées vers la couche réseau de l'hôte.

  
  Avertissement

  Ne modifier jamais manuellement le script de l'interface de bouclage, `/etc/sysconfig/network-scripts/ifcfg-lo`. Des modifications pourraient provoquer un mauvais fonctionnement du système.
- `ifcfg-irlan0` — Une *interface infrarouge* permet à des informations de circuler entre des périphériques tels qu'un ordinateur portable et une imprimante, par l'intermédiaire d'un lien infrarouge fonctionnant de la même façon qu'un périphérique Ethernet, sauf qu'il est généralement utilisé dans une connexion de poste à poste.
- `ifcfg-plip0` — Une connexion *PLIP (Parallel Line Interface Protocol)* fonctionne de la même façon qu'un périphérique Ethernet, sauf qu'elle utilise un port parallèle.
- `ifcfg-tr0` — Les topologies en anneau à jeton (ou *Token Ring*) ne sont pas aussi courantes sur les *Réseaux locaux* (ou *LAN* de l'anglais Local Area Networks) qu'elles ne l'étaient autrefois ; elles ont été supplantées par Ethernet.

8.3. Scripts de contrôle d'interfaces

Les scripts de contrôle d'interfaces activent et désactivent des connexions d'interfaces. Il existe deux scripts de contrôle principaux, à savoir `/sbin/ifdown` et `/sbin/ifup` qui utilisent des scripts de contrôle situés dans le répertoire `/etc/sysconfig/network-scripts`.

Les scripts d'interfaces `ifup` et `ifdown` constituent des liens symboliques vers des scripts du répertoire `/sbin/`. Lorsque l'un ou l'autre de ces scripts est appelé, la valeur de l'interface doit être spécifiée, comme par exemple :

```
ifup eth0
```


Attention

Les scripts d'interfaces `ifup` et `ifdown` sont les seuls scripts que l'utilisateur devrait employer pour activer et désactiver les interfaces réseau.

Les scripts ci-dessous ne sont décrits qu'à titre de références.

Deux fichiers utilisés pour effectuer diverses tâches d'initialisation de réseau durant le processus d'activation d'une interface réseau, à savoir les fichiers `/etc/rc.d/init.d/functions` et `/etc/sysconfig/network-scripts/network-functions`. Reportez-vous à la Section 8.4 pour de plus amples informations.

Après avoir vérifié qu'une interface a été spécifiée et que l'utilisateur effectuant la requête est autorisé à contrôler l'interface, le script aproprié active ou désactive l'interface. La liste ci-dessous énumère les scripts de contrôle d'interfaces les plus courants qui se trouvent dans le répertoire `/etc/sysconfig/network-scripts/` :

- `ifup-aliases` — Configure des alias IP à partir des fichiers de configuration d'interfaces quand plusieurs adresses IP sont associées à une interface.
- `ifup-ippp` et `ifdown-ippp` — Permettent d'activer ou de désactiver les interfaces ISDN.
- `ifup-ipsec` et `ifdown-ipsec` — Permettent d'activer ou de désactiver les interfaces IPsec.
- `ifup-ipv6` et `ifdown-ipv6` — Permettent d'activer ou de désactiver les interfaces IPv6.
- `ifup-ipx` — Permet d'activer une interface IPX.
- `ifup-plip` — Permet d'activer une interface PLIP.
- `ifup-plusb` — Permet d'activer une interface USB pour les connexions réseau.
- `ifup-post` et `ifdown-post` — Contiennent des commandes à exécuter après l'activation ou la désactivation d'une interface.
- `ifup-ppp` et `ifdown-ppp` — Permettent d'activer ou de désactiver une interface PPP .
- `ifup-routes` — Ajoute des itinéraires statiques pour un périphérique particulier lorsque son interface est activée.
- `ifdown-sit` et `ifup-sit` — Contiennent des fonctions associées à l'activation et la désactivation d'un tunnel IPv6 au sein d'une connexion IPv4.
- `ifup-sl` et `ifdown-sl` — Permettent d'activer ou de désactiver une interface SLIP.
- `ifup-wireless` — Permet d'activer une interface sans fil.

Avertissement

La suppression ou la modification de scripts dans le répertoire `/etc/sysconfig/network-scripts/` peut provoquer le mauvais fonctionnement ou l'échec de diverses connexions. Seuls les utilisateurs chevronnés devraient modifier les scripts en relation avec une interface réseau.

Pour simplifier la manipulation simultanée de tous les scripts réseau, utilisez la commande `/sbin/service` sur le service réseau (`/etc/rc.d/init.d/network`), comme ci-dessous :

```
/sbin/service network <action>
```

Dans cet exemple, <*action*> peut correspondre à `start`, `stop` ou `restart`.

Pour afficher une liste des périphériques configurés et des interfaces réseau actuellement actives, utilisez la commande suivante :

```
/sbin/service network status
```

8.4. Fichiers de fonctions réseau

Red Hat Enterprise Linux utilise plusieurs fichiers contenant des fonctions importantes utilisées pour activer et désactiver les interfaces. Plutôt que de forcer chaque fichier de contrôle d'interfaces à contenir ces fonctions, elles sont regroupées dans un petit nombre de fichiers qui sont utilisés en fonction des besoins.

Le fichier `/etc/sysconfig/network-scripts/network-functions` contient les fonctions IPv4 les plus couramment utilisées par bon nombre de scripts de contrôle d'interfaces. Ces fonctions permettent entre autres de contacter des programmes en cours d'exécution ayant demandé des informations sur les modifications du statut d'une interface, de configurer des noms d'hôte, de trouver un périphérique passerelle, de vérifier le statut d'un périphérique particulier et finalement d'ajouter un itinéraire par défaut.

Les fonctions requises pour les interfaces IPv6 étant différentes de celles requises pour les interfaces IPv4, un fichier `/etc/sysconfig/network-scripts/network-functions-ipv6` est spécifiquement conçu pour contenir ces informations. Les fonctions spécifiées dans ce fichier permettent de configurer et de supprimer des routes IPv6 statiques, de créer et de supprimer des tunnels, d'ajouter des adresses IPv6 à des interfaces ou d'en supprimer et finalement de rechercher l'existence d'une adresse IPv6 sur une interface.

8.5. Ressources supplémentaires

Les ressources suivantes traitent des interfaces réseau de manière plus détaillée.

8.5.1. Documentation installée

- `/usr/share/doc/initscripts-<version>/sysconfig.txt` — Un guide des options disponibles pour les fichiers de configuration réseau, y compris les options IPv6 n'ayant pas été abordées dans ce chapitre.
- `/usr/share/doc/iproute-<version>/ip-cref.ps` — Ce fichier contient un grand nombre d'informations sur la commande `ip` pouvant être utilisée entre autres pour manipuler des tables de routage. Utilisez l'application **ggv** ou **kghostview** pour accéder à ce fichier.

Chapitre 9.

Système de fichiers réseau (NFS, Network File System)

Un système de fichiers réseau (ou *NFS* de l'anglais Network File System), permet aux hôtes distants de monter des systèmes de fichiers sur un réseau et de les utiliser exactement comme des systèmes de fichiers locaux. Ceci permet aux administrateurs système de stocker des ressources sur des serveurs centralisés sur le réseau.

Ce chapitre se concentre sur les concepts fondamentaux de NFS et des références supplémentaires. Pour obtenir des instructions spécifiques sur la configuration et l'exploitation de logiciels clients et serveurs NFS, consultez le chapitre intitulé *Système de fichiers réseau (NFS)* du *Guide d'administration système de Red Hat Enterprise Linux*.

9.1. Comment ça marche

À l'heure actuelle, il existe trois versions de NFS. La version 2 de NFS (NFSv2), une version plus ancienne qui est largement prise en charge. La version 3 de NFS (NFSv3) qui a davantage de fonctionnalités, y compris le traitement de fichiers de tailles variables et un meilleur rapportage d'erreurs, mais qui n'est pas entièrement compatible avec les clients NFSv2. La version 4 de NFS (NFSv4) qui inclut la sécurité Kerberos, fonctionne à travers des pare-feu et qui sur Internet, n'a plus besoin de portmapper, prend en charge les ACL et utilise des opérations avec état (ou qualifiées de stateful). Red Hat Enterprise Linux supporte les clients NFSv2, NFSv3 et NFSv4 et lors du montage d'un système de fichiers via NFS, Red Hat Enterprise Linux utilise NFSv4 par défaut, si le serveur le prend en charge.

Toutes les versions de NFS peuvent utiliser le protocole *TCP* (de l'anglais *Transmission Control Protocol*) exécuté sur un réseau IP, sachant qu'il est nécessaire pour NFSv4. NFSv2 et NFSv3 peuvent utiliser le protocole *UDP* (de l'anglais *User Datagram Protocol*) exécuté sur un réseau IP pour fournir une connexion réseau sans état (aussi qualifiée de stateless) entre le client et le serveur.

Lors de l'utilisation de NFSv2 ou NFSv3 avec UDP, la connexion UDP stateless dans des conditions normales minimise le trafic réseau, car le serveur NFS envoie un cookie au client une fois que ce dernier est autorisé à accéder au volume partagé. Ce cookie, qui représente une valeur aléatoire stockée côté serveur, est transmis en même temps que les requêtes RPC en provenance du client. Le serveur NFS peut être redémarré sans affecter le client et le cookie reste intact. Ceci étant, le protocole UDP étant sans état (ou stateless), si le serveur s'arrête inopinément, les clients UDP continuent à saturer le réseau de requêtes pour le serveur. Telle est la raison pour laquelle TCP est le protocole préféré lors de la connexion à un serveur NFS.

Lors de l'utilisation de NFSv4, une connexion dite stateful est effectuée et l'authentification Kerberos des utilisateurs et groupes avec des niveaux de sécurité variés est disponible de manière optionnelle. NFSv4 n'a pas d'interaction avec portmapper, `rpc.mountd`, `rpc.lockd` et `rpc.statd` étant donné qu'ils ont été incorporés au noyau. NFSv4 est en écoute sur le port bien connu 2049.

Remarque

TCP est le protocole de transport par défaut pour NFS sous Red Hat Enterprise Linux. Reportez-vous au chapitre intitulé *Système de fichiers réseau (NFS)* du *Guide d'administration système de Red Hat Enterprise Linux* afin d'obtenir de plus amples informations sur la connexion aux serveurs NFS à l'aide de TCP. Il est possible d'utiliser le protocole UDP si nécessaire pour des raisons de compatibilité mais il n'est pas recommandé pour une utilisation générale.

NFS n'effectue d'authentification que lorsqu'un système client tente de monter une ressource NFS partagée. Pour limiter l'accès au service NFS, des enveloppeurs TCP sont employés. Ceux-ci lisent les fichiers `/etc/hosts.allow` et `/etc/hosts.deny` pour déterminer si un client particulier doit se voir refuser ou accorder l'accès au service NFS. Pour plus d'informations sur la configuration des contrôles d'accès avec les enveloppeurs TCP, consultez le Chapitre 17.

Une fois que l'accès du client a été autorisé par les enveloppeurs TCP, le serveur NFS se réfère à son fichier de configuration, `/etc/exports` pour déterminer si le client peut monter l'un des systèmes de fichiers exportés. Dès que l'accès est autorisé, toutes opérations sur les fichiers ou répertoires sont possibles par l'utilisateur.

Avertissement

Lors de l'utilisation de NFSv2 ou NFSv3, qui ne prennent pas en charge l'authentification Kerberos, les privilèges de montage NFS sont accordés à l'hôte client et non pas à l'utilisateur. Ainsi, tout utilisateur sur un hôte client ayant des permissions d'accès peut accéder aux systèmes de fichiers exportés. Lors de la configuration de partages NFS, prêtez une attention particulière aux hôtes qui obtiennent les permissions de lecture/écriture (`rw`).

Important

Afin que NFS puisse fonctionner avec une installation par défaut de Red Hat Enterprise Linux dotée d'un pare-feu activé, il est nécessaire que IPTables soit configurée avec le port 2049 en TCP par défaut. Sans une configuration de IPTables, NFS ne peut fonctionner correctement.

Le script d'initialisation de NFS et le processus `rpc.nfsd` permettent désormais la liaison à un port spécifique lors du démarrage du système. Toutefois, cette opération est susceptible de créer des erreurs si le port n'est pas disponible ou entre en conflit avec un autre démon.

9.1.1. Services requis

Red Hat Enterprise Linux utilise une combinaison de prise en charge de niveau noyau avec des processus démons pour fournir le partage de fichiers NFS. NFSv2 et NFSv3 utilisent les *appels de procédure distante* (ou *RPC* de l'anglais Remote Procedure Calls) pour coder et décoder des requêtes entre les clients et les serveurs. Les services RPC sous Linux sont contrôlés par le service `portmap`. Pour partager ou monter les systèmes de fichiers NFS, les services suivants fonctionnent de concert, selon la version de NFS qui est implémentée :

- `nfs` — Un service qui lance les processus RPC appropriés pour répondre aux requêtes pour les systèmes de fichiers NFS partagés.
- `nfslock` — Un service facultatif qui lance les processus RPC appropriés pour permettre aux clients NFS de verrouiller des fichiers sur le serveur.
- `portmap` — Le service RPC pour Linux ; il répond aux requêtes pour des services RPC et définit des connexions vers le service RPC. Il n'est pas utilisé avec NFSv4.

Les processus RPC suivants facilitent les services NFS :

- `rpc.mountd` — Ce processus reçoit la requête de montage en provenance d'un client NFS et vérifie que le système de fichiers demandé est bien exporté. Ce processus est démarré automatiquement

par le service `nfs` et ne nécessite pas de configuration au niveau de l'utilisateur. Ce processus n'est pas utilisé avec NFSv4.

- `rpc.nfsd` — Ce processus est le serveur NFS. Il fonctionne avec le noyau Linux pour satisfaire les requêtes dynamiques des clients NFS, comme par exemple pour fournir des fils de serveur (ou threads) chaque fois qu'un client NFS se connecte. Ce processus correspond au service `nfs`.
- `rpc.lockd` — Un processus facultatif qui permet aux clients NFS de verrouiller des fichiers sur le serveur. Il correspond au service `nfslock`. Ce processus n'est pas utilisé avec NFSv4.
- `rpc.statd` — Ce processus implémente le protocole RPC de *Moniteur de statut de réseau (NSM)* (de l'anglais Network Status Monitor) qui avertit les clients NFS lorsqu'un serveur est redémarré sans avoir été préalablement arrêté correctement. Ce processus est lancé automatiquement par le service `nfslock` et ne nécessite pas de configuration au niveau de l'utilisateur. Ce processus n'est pas utilisé avec NFSv4.
- `rpc.rquotad` — Ce processus fournit des informations sur les quotas utilisateur s'appliquant aux utilisateurs distants. Il est lancé automatiquement par le service `nfs` et ne nécessite pas de configuration au niveau de l'utilisateur.
- `rpc.idmapd` — Ce processus fournit au client et serveur NFSv4 des appels ascendants (aussi appelés upcalls) qui établissent la correspondance entre les noms NFSv4 (qui sont des chaînes se présentant sous la forme utilisateur@domaine) et les UID et GID locaux. Pour que `idmapd` puisse fonctionner avec NFSv4, `/etc/idmapd.conf` doit être configuré. Ce service est nécessaire pour une utilisation avec NFSv4.
- `rpc.svcgssd` — Ce processus fournit le mécanisme de transport serveur pour le processus d'authentification (Kerberos Version 5) avec NFSv4. Ce service est nécessaire pour une utilisation avec NFSv4.
- `rpc.gssd` — Ce processus fournit le mécanisme de transport client pour le processus d'authentification (Kerberos Version 5) avec NFSv4. Ce service est nécessaire pour une utilisation avec NFSv4.

9.1.2. NFS et `portmap`

Remarque

La section suivante s'applique seulement aux implémentations de NFSv2 ou NFSv3 nécessitant le service de `portmap` pour la compatibilité ascendante.

Le service `portmap` sous Linux est nécessaire pour orienter les requêtes RPC vers les services appropriés. Les processus RPC s'annoncent à `portmap` lorsqu'ils démarrent, révélant le numéro de port qu'ils contrôlent et les numéros de programmes RPC qu'ils entendent servir. Le système client contacte alors `portmap` sur le serveur avec un numéro de programme RPC particulier. Le service `portmap` redirige ensuite le client vers le numéro de port correct afin de communiquer avec le service souhaité.

Parce que les services utilisant RPC se basent sur `portmap` pour assurer toutes les connexions avec les requêtes client entrantes, `portmap` doit être disponible avant le démarrage de chacun de ces services.

Le service `portmap` utilise des enveloppeurs TCP pour le contrôle d'accès et les règles de contrôle d'accès pour `portmap` affectent *tous* les services basés sur RPC. Il est également possible de spécifier chacun des démons RPC NFS devant être affectés par une règle de contrôle d'accès. Les pages de manuel relatives à `rpc.mountd` et `rpc.statd` contiennent des informations sur la syntaxe précise de ces règles.

9.1.2.1. Résolution de problèmes liés à NFS et `portmap`

Parce que `portmap` fournit la coordination entre les services RPC et les numéros des ports utilisés pour communiquer avec eux, il est utile d'afficher le statut des services RPC actuels à l'aide de `portmap` lors de la résolution de problèmes. La commande `rpcinfo` affiche chaque service basé sur RPC avec des numéros de port, un numéro de programme RPC, un numéro de version et un type de protocole IP (TCP ou UDP).

Pour s'assurer que les bons services NFS basés sur RPC sont activés pour `portmap`, utilisez la commande suivante en tant que super-utilisateur :

```
rpcinfo -p
```

Ci-dessous figure un exemple de sortie de cette commande :

```
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100021    1   udp  32774  nlockmgr
    100021    3   udp  32774  nlockmgr
    100021    4   udp  32774  nlockmgr
    100021    1   tcp  34437  nlockmgr
    100021    3   tcp  34437  nlockmgr
    100021    4   tcp  34437  nlockmgr
    100011    1   udp    819  rquotad
    100011    2   udp    819  rquotad
    100011    1   tcp    822  rquotad
    100011    2   tcp    822  rquotad
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100005    1   udp    836  mountd
    100005    1   tcp    839  mountd
    100005    2   udp    836  mountd
    100005    2   tcp    839  mountd
    100005    3   udp    836  mountd
    100005    3   tcp    839  mountd
```

La sortie ci-dessus montre que les bons services NFS sont en cours d'exécution. Si l'un des services NFS ne démarre pas correctement, `portmap` sera incapable d'établir la correspondance entre les requêtes RPC provenant du clients pour ce service et le port adéquat. Souvent, i NFS n'est pas présent dans la sortie de `rpcinfo`, le redémarrage de NFS permet à ces services de s'enregistrer correctement auprès de `portmap` et de commencer à fonctionner. Pour obtenir de plus amples informations sur le lancement de NFS, reportez-vous à la Section 9.2.

D'autres options utiles sont disponibles pour la commande `rpcinfo`. Reportez-vous à la page de manuel de `rpcinfo` afin d'obtenir de plus amples informations.

9.2. Lancement et arrêt de NFS

Afin d'exécuter un serveur NFS, le service `portmap` doit être en cours d'exécution. Pour vérifier que `portmap` est activé, tapez la commande suivante en tant que super-utilisateur :

```
/sbin/service portmap status
```

Si le service `portmap` est en cours d'exécution, le service `fs` peut alors être lancé. Pour démarrer un serveur NFS, tapez la commande suivante en tant que super-utilisateur :

```
/sbin/service nfs start
```

Pour arrêter le serveur, tapez la commande suivante en étant connecté comme super-utilisateur :

```
/sbin/service nfs stop
```

L'option `restart` est un raccourci pour arrêter, puis redémarrer NFS. Cette option est la manière la plus efficace pour que les changements de configuration prennent effet après la modification du fichier de configuration pour NFS.

Pour redémarrer le serveur, tapez la commande suivante en tant que super-utilisateur :

```
/sbin/service nfs restart
```

L'option `condrestart` (*conditional restart*) ne lance `nfs` que s'il est actuellement en cours d'exécution. Cette option est utile pour les scripts, vu qu'elle ne lance pas le démon s'il n'est pas en cours d'exécution.

Pour redémarrer le serveur sous certaines conditions, tapez la commande suivante en tant que super-utilisateur :

```
/sbin/service nfs condrestart
```

Pour recharger le fichier de configuration du serveur NFS sans redémarrer le service, tapez la commande suivante en tant que super-utilisateur :

```
/sbin/service nfs reload
```

Par défaut, le service `nfs` ne se lance *pas* automatiquement au démarrage. Pour configurer NFS pour une exécution au démarrage, utilisez un utilitaire initscript tel que `/sbin/chkconfig`, **/sbin/ntsysv** ou l'**Outil de configuration des services**. Reportez-vous au chapitre intitulé *Contrôle de l'accès aux services* du *Guide d'administration système de Red Hat Enterprise Linux* afin d'obtenir de plus amples informations sur ces outils.

9.3. Configuration du serveur NFS

Il existe trois manières de configurer un serveur NFS sous Red Hat Enterprise Linux : en utilisant l'**Outil de configuration du serveur NFS** (`system-config-nfs`), en modifiant manuellement son fichier de configuration (`/etc/exports`) ou en exécutant la commande `/usr/sbin/exportfs`.

Pour obtenir des instructions sur l'utilisation de l'**Outil de configuration du serveur NFS**, reportez-vous au chapitre intitulé *Système de fichiers réseau (NFS)* du *Guide d'administration système de Red Hat Enterprise Linux*. Le reste de cette section examine la modification manuelle de `/etc/exports` et l'utilisation de la commande `/usr/sbin/exportfs` pour exporter les systèmes de fichiers NFS.

9.3.1. Fichier de configuration de `/etc/exports`

Le fichier `/etc/exports` permet non seulement de contrôler les systèmes de fichiers spécifiques qui sont exportés vers des hôtes distants, mais il permet également de spécifier des options. Les lignes blanches ne sont pas prises en compte, des commentaires peuvent être mentionnés en ajoutant un symbole dièse (`#`) en début de ligne et un retour à la ligne peut être introduit grâce à une barre oblique inverse (`\`). Chaque système de fichiers exporté doit avoir sa propre ligne et toutes les listes d'hôtes autorisés placées après un système de fichiers exporté doivent être séparées par des espaces. Les

options pour chacun des hôtes doivent être placées entre parenthèses directement après l'identifieur d'hôte, sans espace entre l'hôte et la première parenthèse.

La ligne pour un système de fichiers exporté a la structure suivante :

```
<export> <host1>(<options>) <hostN>(<options>)...
```

Dans cette structure, remplacez *<export>* par le répertoire devant être exporté, remplacez *<host1>* par l'hôte ou le réseau vers lequel l'export est partagé et remplacez *<options>* par les options pour cet hôte ou ce réseau. Des hôtes supplémentaires peuvent être spécifiés dans une liste délimitée par des espaces.

Les méthodes suivantes peuvent être utilisées pour spécifier des noms d'hôtes :

- *hôte simple* — Où un hôte particulier est spécifié avec un nom de domaine pleinement qualifiée, un nom d'hôte ou une adresse IP.
- *caractères génériques* — Où les caractères `*` ou `?` sont utilisés pour prendre en compte un groupement de noms de domaines pleinement qualifiés qui correspondent à une chaîne de lettres donnée. Les caractères génériques (aussi appelés wildcards) ne devraient pas être utilisés avec les adresses IP ; il est toutefois possible qu'ils fonctionnent par accident, si les recherches inverses de DNS échouent.

  Soyez toutefois prudent lors de l'utilisation de caractères génériques avec des noms de domaines pleinement qualifiés, car ils sont souvent plus exacts que ce que vous escomptez. Par exemple, si vous utilisez `*.example.com` comme caractère générique, sales.example.com sera autorisé à accéder au système de fichiers exporté, mais pas bob.sales.example.com. Pour une correspondance incluant les deux noms de domaine, vous devrez spécifier `*.example.com` et `*.*.example.com`.
- *réseaux IP* — Autorisent la mise en correspondance d'hôtes en fonction de leur adresse IP dans un réseau plus grand. Par exemple, `192.168.0.0/28` autorisera les 16 premières adresses IP, de 192.168.0.0 à 192.168.0.15, à accéder au système de fichiers exporté, mais pas 192.168.0.16 ou une adresse IP supérieure.
- *groupes réseau* — Attribuent un nom de groupe réseau NIS, écrit ainsi : `@<group-name>`. Cette option attribue au serveur NIS la charge du contrôle d'accès pour ce système de fichier exporté, où les utilisateurs peuvent être ajoutés et supprimés dans un groupe NIS sans affecter `/etc/exports`.

Dans sa forme la plus simple, le fichier `/etc/exports` précise seulement le répertoire exporté et les hôtes autorisés à y accéder, comme dans l'exemple suivant :

```
/exported/directory bob.example.com
```

Dans cet exemple, `bob.example.com` peut monter `/exported/directory/`. Étant donné qu'aucune option n'est spécifiée dans cet exemple, les options NFS par défaut prennent effet :

- `ro` — Les montages du système de fichiers exporté sont en lecture-seule. Les hôtes distants ne peuvent pas modifier les données partagées sur le système de fichiers. Pour autoriser les hôtes à apporter des modifications au système de fichiers, l'option `rw` (lecture-écriture) doit être spécifiée.
- `wdelay` — Cette option entraîne un retard des opérations d'écriture sur le disque par NFS, s'il suspecte qu'une autre requête d'écriture est imminente. Ce faisant, les performances peuvent être améliorées grâce à une réduction du nombre d'accès au disque par des commandes d'écriture séparées, réduisant ainsi le temps d'écriture. L'option `no_wdelay` quant à elle, désactive cette fonction mais n'est disponible que lors de l'utilisation de l'option `sync`.
- `root_squash` — Cette option retire au super-utilisateur en connexion distante tous les privilèges de son statut en lui assignant l'ID d'utilisateur `nfsnobody` (personne). Ce faisant, le pouvoir du super-utilisateur distant est réduit au niveau d'utilisateur le plus bas, l'empêchant d'apporter des modifications non autorisées dans des fichiers sur le serveur distant. Sinon, l'option `no_root_squash` annule cette fonction de réduction des privilèges du super-utilisateur. Afin

de limiter le champ d'action de chaque utilisateur distant, y compris le super-utilisateur, utilisez l'option `all_squash`. Pour spécifier les ID d'utilisateur et de groupe à utiliser avec des utilisateurs distants d'un hôte particulier, utilisez respectivement les options `anonuid` et `anongid`. Dans ce cas, un compte utilisateur spécial peut être créé pour que les utilisateurs NFS distants le partagent et spécifient `(anonuid=<uid-value>,anongid=<gid-value>)`, où `<uid-value>` correspond au numéro de l'ID d'utilisateur et `<gid-value>` représente le numéro de l'ID de groupe.

Important

Par défaut, les *listes de contrôle d'accès* (*LCA* aussi appelées ACL de l'anglais Access Control Lists) sont prises en charge par NFS sous Red Hat Enterprise Linux. Pour désactiver cette fonction, spécifiez l'option `no_acl` lors de l'export du système de fichiers. Pour obtenir davantage d'informations sur cette fonction, reportez-vous au chapitre intitulé *Système de fichiers réseau (NFS)* du *Guide d'administration système de Red Hat Enterprise Linux*.

Toutes les valeurs par défaut de chaque système de fichiers exporté doivent être explicitement écrasées. Par exemple, si l'option `rw` n'est pas spécifiée, le système de fichiers exporté est partagé en lecture-seule. L'exemple suivant est une ligne de `/etc/exports` qui écrase les deux options par défaut :

```
/another/exported/directory 192.168.0.3(rw,sync)
```

Dans cet exemple, `192.168.0.3` peut monter `/another/exported/directory/` en lecture/écriture et tous les transferts vers le disque sont validés avant que la requête d'écriture par le client ne soit achevée.

De plus, d'autres options sont disponibles là où il n'existe pas de valeur par défaut. Elles permettent d'annuler la vérification de la sous-arborescence, l'accès à des ports non-sûrs et les verrouillages non-sûrs de fichiers (nécessaires pour certaines implémentations anciennes de client NFS). Consultez la page de manuel de `exports` pour obtenir deplus amples informations sur ces options moins souvent utilisées.

Avertissement

Le format du fichier `/etc/exports` est très précis, particulièrement en ce qui concerne l'utilisation des caractères d'espacement. Rappelez-vous bien de toujours séparer les systèmes de fichiers exportés des hôtes, et les hôtes entre eux à l'aide d'un caractère d'espacement. Toutefois, aucun autre caractère d'espacement ne doit figurer dans le fichier, sauf sur des lignes de commentaire.

Par exemple, les deux lignes suivantes n'ont pas la même signification :

```
/home bob.example.com(rw)
/home bob.example.com (rw)
```

La première ligne autorise seulement les utilisateurs de `bob.example.com` à avoir un accès en lecture/écriture au répertoire `/home/`. La deuxième ligne elle autorise les utilisateurs de `bob.example.com` à monter le répertoire en lecture-seule (la valeur par défaut), alors que tout autre utilisateur peut le monter en lecture/écriture.

Pour obtenir de plus amples informations sur la configuration d'un serveur NFS par le biais du fichier `/etc/exports`, reportez-vous au chapitre intitulé *Système de fichiers réseau (NFS)* du *Guide d'administration système de Red Hat Enterprise Linux*.

9.3.2. La commande `exportfs`

Chaque fichier exporté vers les utilisateurs distants via NFS ainsi que les droits d'accès liés à ces systèmes de fichiers sont énumérés dans le fichier `/etc/exports`. Lorsque le service `nfs` démarre, la commande `/usr/sbin/exportfs` se lance et lit ce fichier, passe le contrôle à `rpc.mountd` (si NFSv2 ou NFSv3 sont utilisés) pour le processus de montage proprement dit et ensuite à `rpc.nfsd` où les systèmes de fichiers sont alors disponibles pour les utilisateurs distants.

Lorsqu'elle est exécutée manuellement, la commande `/usr/sbin/exportfs` permet au super-utilisateur d'exporter ou de désexporter sélectivement des répertoires sans redémarrer le service NFS. Avec les options appropriées, la commande `/usr/sbin/exportfs` écrit les systèmes de fichiers exportés dans `/var/lib/nfs/xtab`. Puisque `rpc.mountd` se réfère au fichier `xtab` lorsqu'il décide des privilèges d'accès à un système de fichiers, les changements apportés à la liste des systèmes de fichiers exportés prennent effet immédiatement.

Ci-dessous figure une liste des options couramment utilisées pour `/usr/sbin/exportfs` :

- `-r` — Provoque l'export de tous les répertoires listés dans `/etc/exports` en dressant une nouvelle liste d'exports dans `/etc/lib/nfs/xtab`. Cette option rafraîchit effectivement la liste des exports avec les changements quelconques apportés à `/etc/exports`.
- `-a` — Provoque l'export ou le désexport de tous les répertoires, selon les autres options de la commande `/usr/sbin/exportfs`. Si aucune autre option n'est spécifiée, `/usr/sbin/exportfs` exporte tous les systèmes de fichiers spécifiés dans `/etc/exports`.
- `-o` *`file-systems`* — Spécifie les répertoires à exporter qui ne sont pas énumérés dans `/etc/exports`. Remplacez *`file-systems`* par les systèmes de fichiers supplémentaires à exporter. Ces derniers doivent être formatés selon le type spécifié dans `/etc/exports`. Reportez-vous à la Section 9.3.1 afin d'obtenir davantage d'informations sur la syntaxe de `/etc/exports`. Cette option est souvent utilisée pour tester un système de fichiers exporté avant de l'ajouter de façon permanente à la liste des systèmes de fichiers à exporter.
- `-i` — Ne prend pas en compte `/etc/exports` ; seules les options données par la ligne de commande sont utilisées pour définir les systèmes de fichiers exportés.
- `-u` — Désexporte tous les répertoires partagés. La commande `/usr/sbin/exportfs -ua` suspend le partage de fichiers NFS alors que tous les démons NFS restent actifs. Pour activer à nouveau le partage NFS, tapez `exportfs -r`.
- `-v` — Représente une opération prolixe où les systèmes de fichiers à exporter ou à désexporter sont affichés avec beaucoup de détails lorsque la commande `exportfs` est exécutée.

Si aucune option n'est transmise à la commande `/usr/sbin/exportfs`, elle affiche une liste des systèmes de fichiers actuellement exportés.

Pour obtenir davantage d'informations sur la commande `/usr/sbin/exportfs`, reportez-vous à la page de manuel d'`exportfs`.

9.3.2.1. Utilisation de la commande `exportfs` avec NFSv4

Étant donné que NFSv4 n'utilise plus le protocole `rpc.mountd` comme dans NFSv2 et NFSv3, le montage de systèmes de fichiers a changé.

Un client NFSv4 a désormais la possibilité de voir l'ensemble des exports effectués par le serveur NFSv4 en tant qu'un seul système de fichiers qui porte le nom de pseudo-système de fichiers NFSv4. Sous Red Hat Enterprise Linux, le pseudo-système de fichiers est identifié comme un seul système de fichiers réel, identifié à l'export avec l'option `fsid=0`.

Par exemple, les commandes suivantes pourraient être exécutées sur un serveur NFSv4 :

```
mkdir /exports
mkdir /exports/opt
```

```
mkdir /exports/etc
mount --bind /usr/local/opt /exports/opt
mount --bind /usr/local/etc /exports/etc
exportfs -o fsid=0,insecure,no_subtree_check gss/krb5p:/exports
exportfs -o rw,nohide,insecure,no_subtree_check gss/krb5p:/exports/opt
exportfs -o rw,nohide,insecure,no_subtree_check gss/krb5p:/exports/etc
```

Dans cet exemple, on fournit aux clients de multiples systèmes de fichiers à monter, en utilisant l'option `--bind`.

9.4. Fichiers de configuration de clients NFS

Les partages NFS sont montés côté client à l'aide de la commande `mount`. Le format de la commande est le suivant :

```
mount -t <nfs-type> -o <options> <host>:</remote/export> </local/directory>
```

Remplacez *<nfs-type>* par `nfs` pour les serveurs NFSv2 ou NFSv3 ou par `nfs4` pour les serveurs NFSv4. Remplacez *<options>* par une liste d'options séparées par des virgules pour le système de fichiers NFS (voir la Section 9.4.3 pour davantage d'informations). Remplacez *<host>* par l'hôte distant, *</remote/export>* par le répertoire distant à monter et remplacez *</local/directory>* par le répertoire local où le système de fichiers distant devra être monté.

Consultez la page de manuel de `mount` pour obtenir davantage d'informations.

Si vous accédez à un partage NFS en exécutant manuellement la commande `mount`, le système de fichiers doit être remonté manuellement une fois le système redémarré. Red Hat Enterprise Linux offre deux méthodes pour monter les systèmes de fichiers distants automatiquement au démarrage : le fichier `/etc/fstab` ou le service `autofs`.

9.4.1. `/etc/fstab`

Le fichier `/etc/fstab` est référencé par le service `netfs` au démarrage donc les lignes faisant référence aux partages NFS jouent le même rôle que la saisie manuelle de la commande `mount` durant le processus de démarrage.

Un exemple de ligne présente dans `/etc/fstab` permettant le montage d'un export NFS ressemble à l'exemple suivant :

```
<server>:</remote/export> </local/directory> <nfs-type> <options> 0 0
```

Remplacez *<server>* par le nom d'hôte, l'adresse IP ou le nom de domaine pleinement qualifié du serveur exportant le système de fichiers.

Remplacez *</remote/export>* par le chemin vers le répertoire exporté.

Remplacez *</local/directory>* par le système de fichiers local sur lequel le répertoire exporté est monté. Ce point de montage doit exister avant que `/etc/fstab` ne soit lu, sinon le montage échouera.

Remplacez *<nfs-type>* par `nfs` pour des serveurs NFSv2 ou NFSv3 ou par `nfs4` pour des serveurs NFSv4.

Remplacez *<options>* par une liste d'options séparées par des virgules pour le système de fichiers NFS (voir la Section 9.4.3 pour davantage d'informations). Reportez-vous à la page de manuel de `fstab` pour obtenir de plus amples informations.

9.4.2. autofs

Un inconvénient lors de l'utilisation de /etc/fstab est que, indépendamment de la fréquence d'utilisation de ce système de fichiers monté via NFS, le système doit allouer des ressources pour que ce montage demeure. Ceci n'est pas un problème pour un ou deux montages, mais si votre système maintient le montage de douzaines de systèmes à un moment donné, les performances générales du système peuvent en pâtir. Une alternative à /etc/fstab consiste à utiliser l'utilitaire basé sur le noyau nommé automount qui montera et démontera automatiquement les systèmes de fichiers NFS, économisant ainsi des ressources.

Le service autofs sert à contrôler la commande automount par le biais du fichier de configuration primaire /etc/auto.master. Alors que la commande automount peut être spécifiée dans une ligne de commande, il est plus commode de spécifier les points de montage, nom d'hôte, répertoire exporté et autres options dans un ensemble de fichiers, plutôt que de tous les taper manuellement.

Les fichiers de configuration autofs sont organisés selon une relation parent-enfant. Le fichier de configuration principal (/etc/auto.master) énumère des points de montage sur le système qui sont liés à un *type de correspondance* (map type) particulier, prenant la forme d'autres fichiers de configuration, programmes, chemins NIS et autres méthodes de montage moins courantes. Le fichier auto.master contient des lignes se référant à chacun de ces points de montage, organisées de la manière suivante :

```
<mount-point> <map-type>
```

L'élément <*mount-point*> de cette ligne indique l'emplacement du montage sur le système de fichiers local. L'option <*map-type*> fait référence à la manière dont le point de montage sera monté. La méthode la plus courante pour monter automatiquement des exports NFS consiste à utiliser un fichier en tant que type de chemin d'accès pour un point de montage particulier. Le fichier de chemin d'accès est généralement nommé auto.<*mount-point*>, où <*mount-point*> est le point de montage désigné dans auto.master. Les fichiers de chemin d'accès contiennent une ligne similaire à celle reproduite ci-dessous pour monter un export NFS :

```
</local/directory>  -<options>  <server>:</remote/export>
```

Remplacez </*local/directory;*> par le système de fichiers local où le répertoire exporté doit être monté. Ce point de montage doit exister avant que le fichier de chemin d'accès ne soit lu, sinon le montage échouera.

Remplacez <*options*> par une liste d'options séparées par des virgules pour le système de fichiers NFS (voir la Section 9.4.3 pour obtenir davantage d'informations). Assurez-vous de bien inclure un tiret (–) immédiatement avant la liste d'options.

Remplacez <*server*> par le nom d'hôte, l'adresse IP ou le nom de domaine pleinement qualifié du serveur exportant le système de fichiers.

Remplacez </*remote/export*> par le chemin vers le répertoire exporté.

Remplacez <*options*> par une liste d'options séparées par des virgules pour le système de fichiers NFS (voir la Section 9.4.3 pour obtenir davantage d'informations).

Bien que les fichiers de configuration autofs puissent être utilisés pour une variété de montages applicables à de nombreux types de périphériques et de systèmes de fichiers, ils sont particulièrement utiles lors de la création de montages NFS. Par exemple, des organisations stockent le répertoire /home/ d'un utilisateur sur un serveur central via le partage NFS. Ensuite, elles configurent le fichier auto.master sur chacun des postes de travail pour qu'il renvoie à un fichier auto.home contenant les spécifications du montage du répertoire /home/ via NFS. Ce faisant, l'utilisateur peut alors accéder à ses données personnelles et aux fichiers de configuration dans son répertoire /home/ en se connectant sur un ordinateur quelconque du réseau. Le fichier auto.master correspondant à une telle situation ressemblerait à l'extrait reproduit ci-dessous :

```
/home   /etc/auto.home
```

Cette ligne instruit le système d'installer le point de montage `/home/` sur le système local qui doit être configuré selon le fichier `/etc/auto.home` ressemblant à l'extrait suivant :

```
*  -fstype=nfs4,soft,intr,rsize=32768,wsize=32768,nosuid  server.example.com:/home
```

Cette ligne stipule que tout répertoire auquel un utilisateur tente d'accéder dans le répertoire `/home/` local (en raison de l'astérisque) devrait entraîner un montage NFS sur le système `server.example.com` au point de montage `/home/`. Les options de montage spécifient que chaque montage NFS du répertoire `/home/` devrait utiliser une série particulière de paramètres. Pour obtenir de plus amples informations sur les options de montage, y compris celles utilisées dans cet exemple, consultez la Section 9.4.3.

Pour davantage d'informations sur les fichiers de configuration de `autofs`, reportez-vous à la page de manuel de `auto.master`.

9.4.3. Options courantes de montage NFS

Outre le montage d'un système de fichiers sur un hôte distant via NFS, d'autres options peuvent être spécifiées au moment du montage afin de le rendre plus commode à utiliser. Ces options peuvent être utilisées avec des commandes `mount` exécutées manuellement, à l'aide de paramètres spécifiés dans `/etc/fstab` et grâce à `autofs`.

Ci-dessous figurent les options couramment utilisées pour les montages NFS :

- `fsid=num` — Force les paramètres des descritpeurs de fichiers et des attributs de fichiers sur le réseau à prendre la valeur *num*, au lieu d'un nombre dérivé du nombre majeur et mineur du périphérique bloc présent sur le système de fichiers monté. La valeur `0` prend une signification particulière lorsqu'elle est utilisée avec NFSv4. NFSv4 a une notion de racine (aussi appelée root) pour l'ensemble du système de fichiers exporté. Le point d'export exporté avec `fsid=0` est utilisé comme cette racine (ou root).
- `hard` ou `soft` — Spécifie si le programme utilisant un fichier via une connexion NFS doit s'arrêter et attendre (`hard`) que le serveur revienne en ligne, si l'hôte fournissant le système de fichiers exporté n'est pas disponible ou s'il doit au contraire émettre un message d'erreur (`soft`).

  Si l'option `hard` est spécifiée, l'utilisateur ne peut pas mettre fin au processus attendant le rétablissement de la communication NFS à moins que l'option `intr` ne soit également spécifiée.

  Si l'option `soft` est spécifiée, l'utilisateur peut ajouter une option `timeo=`<*value*> supplémentaire, où <*value*> spécifie le nombre de secondes devant s'écouler avant que le message d'erreur ne soit émis.
- `intr` — Autorise l'interruption des requêtes NFS si le serveur est en panne ou ne peut pas être contacté.
- `nfsvers=2` ou `nfsvers=3` — Spécifie la version spécifique du protocole NFS devant être utilisée. Cette option est utile pour des hôtes qui exécutent de multiples serveurs NFS. Si aucune version n'est précisée, NFS utilise le numéro de version le plus élevé pris en charge par le noyau et la commande `mount`. Cette option n'est pas prise en charge avec NFSv4 et ne devrait donc pas être utilisée.
- `noacl` — Désactive le traitement de toutes les LCA (ou ACL selon l'acronyme anglais). Une telle option sera peut-être nécessaire lors de l'interfaçage avec des versions plus anciennes de Red Hat Enterprise Linux, Red Hat Linux, ou de Solaris, étant donné que la technologie la plus récente en matière de listes de contrôle d'accès n'est pas compatible avec des systèmes anciens.
- `nolock` — Désactive le verrouillage de fichiers. Cette option peut être nécessaire afin de pouvoir se connecter à d'anciens serveurs NFS.

- `noexec` — Interdit l'exécution de binaires sur les systèmes de fichiers montés. Cette option est utile si votre système est en train de monter un système de fichiers non-Linux via NFS, contenant des binaires incompatibles.
- `nosuid` — Désactive les bits setuid et setgid. Cette option empêche que les utilisateurs puissent obtenir des privilèges plus étendus en exécutant un programme setuid.
- `port=num` — Spécifie la valeur numérique du port du serveur NFS. Si *`num`* équivaut à `0` (la valeur par défaut), `mount` interroge le gestionnaire de ports (ou portmapper) de l'hôte distant pour connaître le numéro de port à utiliser. Si le démon NFS de l'hôte distant n'est pas répertorié dans le gestionnaire de port, le numéro de port NFS standard utilisé est alors TCP 2049.
- `rsize=num` et `wsize=num` — Ces paramètres accélèrent la communication NFS pour les opérations de lecture (`rsize`) et d'écriture (`wsize`) en déterminant une taille de bloc de données supérieure, exprimée en octets, devant être transférée à un moment donné. Une extrême prudence est recommandée lors de la modification de ces valeurs ; certaines cartes réseau et certains noyaux Linux relativement anciens ne fonctionnent pas très bien avec des blocs d'une taille plus grande. Pour NFSv2 ou NFSv3, la valeur par défaut pour les deux paramètres est 8192. Pour NFSv4, la valeur par défaut pour les deux paramètres est 32768.
- `sec=mode` — Spécifie le type de sécurité à utiliser lors de l'authentification d'une connexion NFS.

  `sec=sys` représente le paramétrage par défaut, qui utilise des UID et GID UNIX locaux au moyen de AUTH_SYS pour authentifier des opérations NFS.

  `sec=krb5` utilise Kerberos V5 au lieu des UID et GID UNIX locaux pour authentifier les utilisateurs.

  `sec=krb5i` utilise Kerberos V5 pour l'authentification des utilisateurs et effectue la vérification de l'intégrité des opérations NFS à l'aide des contrôles de sommes sécurisés pour éviter la falsification de données.

  `sec=krb5p` utilise Kerberos V5 pour l'authentification des utilisateurs, le contrôle de l'intégrité et le cryptage du trafic NFS afin d'empêcher le reniflage de paquets.Ce paramétrage est certes le plus sûr mais il a également le temps de gestion système le plus élevé au niveau de la performance.
- `tcp` — Indique au montage NFS d'utiliser le protocole TCP.
- `udp` — Indique au montage NFS d'utiliser le protocole UDP.

Davantage d'options sont énumérées dans les pages de manuel de `mount` et `nfs`.

9.5. Sécurisation de NFS

NFS est tout à fait approprié pour le partage de systèmes de fichiers entiers avec un grand nombre d'hôtes connus et d'une manière transparente. Toutefois, étant donné la facilité d'utilisation, divers problèmes potentiels de sécurité peuvent surgir.

Il est important de prendre en considération les points suivants lorsque des systèmes de fichiers NFS sont exportés sur un serveur ou lorsqu'ils sont montés sur un client. Ce faisant, les risques de sécurité NFS seront minimisés et les données stockées sur le serveur seront mieux protégées.

Pour obtenir une liste complète des étapes que les administrateurs doivent suivre afin de sécuriser les serveurs NFS, reportez-vous au chapitre intitulé *Sécurité du serveur* du *Guide de sécurité de Red Hat Enterprise Linux*.

9.5.1. Accès des hôtes

La version de NFS que vous devriez implémenter dépend de votre réseau actuel et de vos craintes en matière de sécurité. Les sections suivantes expliquent les différences qui existent entre

l'implémentation de mesures de sécurité avec NFSv2, NFSv3 et NFSv4. Il est recommandé autant que possible, d'utiliser NFSv4 plutôt que d'autres versions de NFS.

9.5.1.1. Utilisation de NFSv2 ou NFSv3

NFS contrôle qui peut monter un système de fichiers exporté en se basant sur l'hôte qui effectue la requête de montage et non pas sur l'utilisateur qui exploitera effectivement le système de fichiers. Les hôtes doivent se voir accorder des droits explicites pour pouvoir monter le système de fichiers exporté. Les utilisateurs ne peuvent contrôler l'accès que par l'intermédiaire des permissions accordées aux fichier et répertoires. En d'autres termes, une fois qu'un système de fichiers est exporté via NFS, tout hôte distant connecté au serveur NFS peut avoir accès aux données partagées. Afin de limiter les risques potentiels, les administrateurs système peuvent restreindre l'accès à une lecture-seule ou peuvent réduire les permissions des utilisateurs à un ID d'utilisateur et de groupe commun. Ceci étant, de telles solutions peuvent empêcher l'utilisation du partage NFS selon l'intention d'origine.

De plus, si un agresseur prend le contrôle du serveur DNS utilisé par le système effectuant l'export du système de fichiers NFS, le système associé avec un nom d'hôte particulier ou un nom de domaine pleinement qualifié peut renvoyer vers un ordinateur non-légitime. À ce stade, l'ordinateur non-autorisé *devient* le système ayant l'autorisation de monter le partage NFS, puisqu'aucun nom d'utilisateur ou mot de passe n'est échangé pour fournir une sécurité supplémentaire au montage NFS.

Les caractères génériques doivent être utilisés avec parcimonie lors de l'export de répertoires via NFS car il est possible que le champ d'action de ces caractères génériques englobe à un plus grand nombre de systèmes que prévu.

Il est également possible de restreindre l'accès au service `portmap` grâce aux enveloppeurs TCP. L'accès aux ports utilisés par `portmap`, `rpc.mountd` et `rpc.nfsd` peut également être limité en créant des règles de pare-feu avec `iptables`.

Pour obtenir de plus amples informations sur la sécurisation de NFS et `portmap`, reportez-vous au chapitre intitulé *Sécurité du serveur* du *Guide de sécurité de Red Hat Enterprise Linux*. Le Chapitre 18 fournit également des informations supplémentaire sur les pare-feu.

9.5.1.2. Utilisation de NFSv4

La publication de NFSv4 a entraîné une révolution en matière d'authentification et de sécurité pour les exports NFS. NFSv4 rend obligatoire l'implémentation du module noyau RPCSEC_GSS, le mécanisme GSS-API de la version 5 de Kerberos, SPKM-3 et LIPKEY. Avec NFSv4, les mécanismes de sécurité obligatoires sont orientés vers l'authentification individuelle des utilisateurs et non pas vers celle des machines clientes comme c'était le cas sous NFSv2 et NFSv3.

Remarque

On suppose qu'un serveur d'émission de tickets Kerberos (ou KDC de l'anglais Key-Distribution Center) est correctement installé et configuré avant la configuration d'un serveur NFSv4.

NFSv4 inclut la prise en charge d'ACL basée sur le modèle Microsoft Windows NT, et non pas sur le modèle POSIX, en raison de ses fonctionnalités et parce qu'il est d'un déploiement plus répandu. NFSv2 et NFSv3 n'ont pas de prise en charge pour les attributs natifs d'ACL.

La suppression du démon `rpc.mountd` est une autre fonctionnalité de sécurité importante de NFSv4. Le démon `rpc.mountd` était à l'origine de brèches de sécurité potentielles en raison de la manière selon laquelle il traitait les gestionnaires de fichiers.

Pour obtenir de plus amples informations sur le cadre RPCSEC_GSS, y compris comment `rpc.svcgssd` et `rpc.gssd` opèrent entre eux, rendez-vous à l'adresse suivante : http://www.citi.umich.edu/projects/nfsv4/gssd/.

9.5.2. Permissions de fichiers

Une fois que le système de fichiers NFS est monté en lecture-écriture par un hôte distant, la seule protection dont dispose chacun des fichiers partagés se situe au niveau de ses permissions. Si deux utilisateurs partageant la même valeur d'ID d'utilisateur montent le même système de fichiers NFS, ils pourront modifier les fichiers mutuellement. De plus, toute personne connectée en tant que super-utilisateur sur le système client peut utiliser la commande `su –` pour devenir un utilisateur ayant accès à des fichiers particuliers via le partage NFS. Pour obtenir de plus amples informations sur les conflits entre NFS et les ID d'utilisateur, reportez-vous au chapitre intitulé *Gestion des comptes utilisateur et de l'accès aux ressources* du manuel *Introduction à l'administration système de Red Hat Enterprise Linux*.

Par défaut, les listes de contrôle d'accès (LCA) sont prises en charge par NFS sous Red Hat Enterprise Linux. Il est déconseillé de désactiver cette fonction. Pour obtenir de plus amples informations sur cette fonction, reportez-vous au chapitre intitulé *Système de fichiers réseau (NFS)* du *Guide d'administration système de Red Hat Enterprise Linux*.

Le comportement par défaut lors de l'export d'un système de fichiers via NFS consiste à utiliser la fonction de *réduction du super-utilisateur* (ou root squashing). Cette dernière permet de définir l'ID d'utilisateur d'une personne quelconque accédant au partage NFS en tant que super-utilisateur sur son ordinateur local, une valeur du compte personne (nobody) du serveur. Il est vivement conseillé de ne jamais désactiver cette fonction.

Si vous exportez un partage NFS en lecture-seule, songez à utiliser l'option `all_squash` qui donne à tout utilisateur accédant au système de fichiers exporté, l'ID d'utilisateur de `nfsnobody` (personne).

9.6. Ressources supplémentaires

L'administration d'un serveur NFS peut se transformer en un véritable défi. Maintes options, y compris un certain nombre qui ne sont pas mentionnées dans ce chapitre, sont disponibles pour l'export ou le montage de partages NFS. Pour obtenir de plus amples informations, consultez les sources d'information mentionnées ci-dessous.

9.6.1. Documentation installée

- `/usr/share/doc/nfs-utils-<version-number>/` — Remplacez <*version-number*> par le numéro de version du paquetage NFS installé. Ce répertoire contient de nombreuses informations sur l'implémentation de NFS sous Linux, y compris diverses configurations NFS et leur impact sur les performances au niveau du transfert de fichiers.
- `man mount` — Contient une vue complète des options de montage aussi bien pour les configurations de serveur que celles de client NFS.
- `man fstab` — Donne des informations détaillées sur le format du fichier `/etc/fstab` utilisé pour monter les systèmes de fichiers au démarrage.
- `man nfs` — Fournit des informations détaillées sur l'export de systèmes de fichiers spécifiques à NFS et sur les options de montage.
- `man exports` — Montre les options couramment utilisées dans le fichier `/etc/exports` lors de l'export de systèmes de fichiers NFS.

9.6.2. Sites Web utiles

- http://nfs.sourceforge.net/ — La page d'accueil du projet NFS Linux et un bon endroit pour les mises à jour du statut du projet.
- http://www.citi.umich.edu/projects/nfsv4/linux/ — Une ressource pour NFSv4avec le noyau Linux 2.6.
- http://www.nfsv4.org — La page d'accueil du projet NFS version 4 et tous les standards associés.
- http://www.vanemery.com/Linux/NFSv4/NFSv4-no-rpcsec.html — Cette page décrit en détail NFSv4 utilisé avec Fedora Core 2 et le noyau 2.6 qu'il contient.
- http://www.nluug.nl/events/sane2000/papers/pawlowski.pdf — Un excellent document technique sur les fonctionnalités et améliorations du protocole NFS Version 4.

9.6.3. Livres sur le sujet

- *Managing NFS and NIS* de Hal Stern, Mike Eisler, et Ricardo Labiaga ; O'Reilly & Associates — Ce livre constitue un excellent guide de référence pour les nombreux exports NFS et options de montage disponibles.
- *NFS Illustrated* de Brent Callaghan ; Addison-Wesley Publishing Company — Ce livre fournit des comparaisons de NFS avec d'autres systèmes de fichiers réseau et montre, en détail, comment se déroule une communication NFS.
- *Guide d'administration système de Red Hat Enterprise Linux* ; Red Hat, Inc. — Le chapitre *Système de fichiers réseau (NFS)* explique de manière concise comment configurer les clients et serveurs NFS.
- *Guide de sécurité de Red Hat Enterprise Linux*; Red Hat, Inc. — Le chapitre *Sécurité serveur* explique les différentes manières de sécuriser NFS et autres services.

Chapitre 10.

Serveur HTTP Apache

Le Serveur HTTP Apache est un serveur Web Open Source robuste de niveau commercial qui a été développé par l'organisation Apache Software Foundation (http://www.apache.org/). Red Hat Enterprise Linux comprend le Serveur HTTP Apache version 2.0 ainsi que de nombreux modules serveur conçus pour améliorer sa fonctionnalité.

Le fichier de configuration par défaut installé avec le Serveur HTTP Apache fonctionne dans la plupart des situations sans devoir être modifié. Ce chapitre décrit brièvement de nombreuses directives présentes dans son fichier de configuration (à savoir `/etc/httpd/conf/httpd.conf`) pour aider les utilisateurs nécessitant une configuration personnalisée ou devant convertir un fichier de configuration dans l'ancien format 1.3 du Serveur HTTP Apache.

Avertissement

Si vous utilisez l'outil graphique **Outil de configuration HTTP** (`system-config-httpd`), *n'éditez pas* manuellement le fichier de configuration du Serveur HTTP Apache car l'**Outil de configuration HTTP** crée une nouvelle version de ce fichier chaque fois qu'il est utilisé.

Pour obtenir davantage d'informations concernant l'**Outil de configuration HTTP**, consultez le chapitre intitulé *Configuration du Serveur HTTP Apache* du *Guide d'administration système de Red Hat Enterprise Linux*.

10.1. Serveur HTTP Apache 2.0

Il existe des différences importantes entre la version 2.0 et la version 1.3 du Serveur HTTP Apache (la version 1.3 faisait partie de la version 2.1 de Red Hat Enterprise Linux et les versions précédentes). Cette section passe en revue certaines des nouvelles fonctionnalités du Serveur HTTP Apache 2.0 et souligne des changements importants. Pour obtenir des informations sur la migration d'un fichier de configuration version 1.3 vers le format 2.0, reportez-vous à la Section 10.2.

10.1.1. Fonctions du Serveur HTTP Apache 2.0

La version 2.0 du Serveur HTTP Apache inclut les fonctionnalités suivantes :

- *API Apache* — Les modules utilisent un nouvel ensemble plus performant d'interfaces de programmation d'applications (ou API de l'anglais Application Programming Interfaces).

Important

Les modules élaborés pour le Serveur HTTP Apache 1.3 ne fonctionneront pas s'ils ne sont pas portés vers la nouvelle API. En cas de doute quant au portage d'un module particulier, consultez le développeur *avant* d'effctuer toute mise à niveau.

- *Filtrage* — Les modules peuvent jouer le rôle de filtres de contenu. Reportez-vous à la Section 10.2.4 pour en savoir plus sur le fonctionnement du filtrage.
- *Prise en charge IPv6* — Le format d'adressage IP nouvelle génération est pris en charge.

- *Directives simplifiées* — Bon nombre de directives complexes ont été supprimées alors que d'autres ont été simplifiées. Reportez-vous à la Section 10.5 pour obtenir davantage d'informations sur des directives spécifiques.
- *Réponses multilingues aux erreurs* — Lors de l'utilisation de documents *Server Side Include* (ou *SSI*), des pages de réponse personnalisées en cas d'erreur peuvent être proposées dans plusieurs langues.

Une liste plus complète des changements est disponible en ligne à l'adresse suivante : http://httpd.apache.org/docs-2.0/.

10.1.2. Changements au niveau des paquetages dans le Serveur HTTP Apache 2.0

Depuis la version 3 de Red Hat Enterprise Linux, les paquetages du Serveur HTTP Apache ont été renommés. De plus, certains paquetages connexes ont également été renommés, retirés ou incorporés dans d'autres paquetages.

Ci-dessous figure une liste des changements apportés aux paquetages :

- Les paquetages `apache`, `apache-devel` et `apache-manual` ont été renommés respectivement `httpd`, `httpd-devel` et `httpd-manual`.
- Le paquetage `mod_dav` a été incorporé au paquetage `httpd`.
- Les paquetages `mod_put` et `mod_roaming` ont été supprimés car leur fonctionnalité fait partie d'un sous-ensemble de celle fournie par `mod_dav` (qui est maintenant incorporé dans le paquetage `httpd`).
- Les paquetages `mod_auth_any` et `mod_bandwidth` ont été supprimés.
- Le numéro de version du paquetage `mod_ssl` est désormais synchronisé avec le paquetage `httpd`. Cela signifie que le paquetage `mod_ssl` du Serveur HTTP Apache 2.0 a un numéro de version *inférieur* à celui du paquetage `mod_ssl` pour le Serveur HTTP Apache 1.3.

10.1.3. Changements apportés au système de fichiers de la version 2.0 du Serveur HTTP Apache

Lors d'une mise à niveau vers la version 2.0 du Serveur HTTP Apache, les changements suivants sont apportés au système de fichiers :

- *Le répertoire de configuration, `/etc/httpd/conf.d/`, a été ajouté* — Ce nouveau répertoire sert à stocker les fichiers de configuration des modules en paquetages individuels, tels que `mod_ssl`, `mod_perl` et `php`. La directive `Include conf.d/*.conf` demande au serveur de charger les fichiers de configuration à partir de cet emplacement au sein du fichier de configuration du Serveur HTTP Apache, `/etc/httpd/conf/httpd.conf`.

Important

Lors de la migration d'une configuration existante, il est impératif d'insérer la ligne spécifiant le nouveau répertoire de configuration.

- *Les programmes `ab` et `logresolve` ont été déplacés* — Ces utilitaires sont passés du répertoire `/usr/sbin/` au répertoire `/usr/bin/`. Par conséquent, les scripts disposant de chemins d'accès absolus pour ces binaires ne fonctionneront pas.

- *Remplacement de la commande* `dbmmanage` — La commande `dbmmanage` a été remplacée par `htdbm`. Reportez-vous à la Section 10.2.4.5 pour obtenir de plus amples informations.
- *Le fichier de configuration* `logrotate` *a été renommé* — Le nom du fichier de configuration `logrotate` a été changé de `/etc/logrotate.d/apache` à `/etc/logrotate.d/httpd`.

La section suivante explique comment effectuer la migration d'une configuration du Serveur HTTP Apache version 1.3 vers le format 2.0.

10.2. Migration des fichiers de configuration du Serveur HTTP Apache version 1.3

Cette section présente la migration d'un fichier de configuration du Serveur HTTP Apache version 1.3 en vue d'une utilisation par le Serveur HTTP Apache 2.0.

Lors d'une mise à niveau de la version 2.1 de Red Hat Enterprise Linux à Red Hat Enterprise Linux 4 il est important de noter que le nouveau fichier de configuration pour le paquetage du Serveur HTTP Apache 2.0 sera installé sous `/etc/httpd/conf/httpd.conf.rpmnew` et que la version originale 1.3 `httpd.conf` ne sera pas modifiée. Bien sûr, il vous appartient entièrement de choisir entre l'utilisation du nouveau fichier de configuration vers lequels les anciens paramètres seront migrés et l'utilisation du fichier existant comme base et d'y apporter des modifications pour qu'il reflète vos besoins ; cependant, certaines parties du fichier ayant été plus modifiées que d'autres, une approche mixte est généralement préférable. Les fichiers de configuration pour les versions 1.3 et 2.0 sont divisés en trois sections.

Si le fichier `/etc/httpd/conf/httpd.conf` est une version modifiée de la version par défaut nouvellement installée et qu'une copie sauvegardée du fichier original est disponible, il sera peut-être plus simple d'invoquer la commande `diff` comme dans l'exemple suivant (en étant connecté en tant que super-utilisateur) :

```
diff -u httpd.conf.orig httpd.conf | less
```

Cette commande soulignera toutes les modifications apportées. Si une copie du fichier original n'est pas disponible, vous devrez l'extraire du paquetage RPM en utilisant les commandes `rpm2cpio` et `cpio`, comme dans l'exemple suivant :

```
rpm2cpio apache-<version-number>.i386.rpm | cpio -i --make
```

Dans la commande ci-dessous, remplacez *<version-number>* par le numéro de version du paquetage `apache`.

Enfin, il est utile de savoir que le Serveur HTTP Apache dispose d'un mode test qui permet de trouver les erreurs de configuration. Pour y accéder, saisissez la commande suivante :

```
apachectl configtest
```

10.2.1. Configuration de l'environnement global

La section intitulée Environnement global (Global Environment) du fichier de configuration contient des directives qui modifient tout le fonctionnement du Serveur HTTP Apache, comme par exemple, le nombre de requêtes simultanées qu'il peut traiter et les emplacements des divers fichiers. Cette section nécessite un grand nombre de changements et doit être basée sur le fichier de configuration du Serveur HTTP Apache version 2.0 vers lequel tous les anciens paramètres devront être migrés.

10.2.1.1. Liaison des interfaces et des ports

Les directives `BindAddress` et `Port` n'existent plus ; leur fonctionnalité est désormais fournie par une directive plus flexible nommée `Listen`.

Si `Port 80` figurant dans les paramtres du fichier de configuration version 1.3, il est nécessaire de le remplacer par `Listen 80` dans le fichier de configuration version 2.0. Si `Port` avait une valeur *autre que 80*, il est nécessaire d'ajouter le numéro du port au contenu de la directive `ServerName`.

L'extrait ci-dessous représente un exemple de directive du Serveur HTTP Apache version 1.3 :

```
Port 123
ServerName www.example.com
```

Pour transférer ce paramètre vers le Serveur HTTP Apache 2.0, utilisez la structure suivante :

```
Listen 123
ServerName www.example.com:123
```

Pour obtenir davantage d'informations sur le sujet, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible sur le site Web à :

- `http://httpd.apache.org/docs-2.0/mod/mpm_common.html#listen`
- `http://httpd.apache.org/docs-2.0/mod/core.html#servername`

10.2.1.2. Régulation de la taille de server-pool

Lorsque le Serveur HTTP Apache accepte les requêtes, il envoie des processus enfants ou des threads pour les traiter. Ce groupe de processus enfants ou de threads (aussi appelés fils) est appelé un *server-pool* (groupe de serveurs). Avec la version 2.0 du Serveur HTTP Apache, la responsabilité de la création et de la maintenance de ces groupes dépendait d'un groupe de modules appelés *Modules multitache* (ou *MPM*, de l'anglais Multi-Processing Modules). Contrairement à d'autres modules, seul un module du groupe MPM peut être chargé par le Serveur HTTP Apache. Trois modules MPM sont inclus dans la version 2.0, à savoir, `prefork`, `worker` et `perchild`. Seuls les MPM `prefork` et `worker` sont actuellement disponibles, mais il se peut que le MPM `perchild` soit disponible dans le futur.

Le comportement original du Serveur HTTP Apache 1.3 a été déplacé dans le MPM `prefork`. Ce dernier accepte les mêmes directives que le Serveur HTTP Apache version 1.3, il est donc possible de migrrer les directives suivantes :

- `StartServers`
- `MinSpareServers`
- `MaxSpareServers`
- `MaxClients`
- `MaxRequestsPerChild`

Le MPM `worker` implémente un serveur multitâche, multiprocessus offrant une modulabilité plus importante. Lors de l'utiliseation de ce MPM, les requêtes sont manipulées par des threads (ou fils) économisant donc les ressources système et permettant ainsi à un grand nombres de requêtes d'être servi de façon efficace. Bien que certaines directives acceptées par le MPM `worker` soient les mêmes que celles acceptées par le MPM `prefork`, les valeurs de ces directives ne devraient pas être transférées directement depuis une installation de Serveur HTTP Apache 1.3. Il vaut mieux utiliser les valeurs par défaut comme des recommandations générale et d'expérimenter ensuite afin de déterminer les valeurs qui fonctionnent le mieux dans votre situation particulière.

Important

Pour utiliser le MPM `worker`, créez le fichier `/etc/sysconfig/httpd` et ajoutez-y la directive suivante :

```
HTTPD=/usr/sbin/httpd.worker
```

Pour obtenir davantage d'informations sur le sujet, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible sur le site Web à :

- http://httpd.apache.org/docs-2.0/mpm.html

10.2.1.3. Prise en charge de DSO (Dynamic Shared Object)

Un grand nombre de changements étant nécessaire ici, il est vivement recommandé à toute personne essayant de modifier une configuration du Serveur HTTP Apache version 1.3 pour l'adapter à la version 2.0 (au lieu de migrer les changements vers la configuration version 2.0) de copier cette section du fichier de configuration Serveur HTTP Apache 2.0.

Les utilisateurs ne souhaitant pas copier la section de la configuration du Serveur HTTP Apache version 2.0 devraient prendre note des informations suivantes :

- Les directives `AddModule` et `ClearModuleList` n'existent plus. Elles étaient utilisées pour assurer l'activation des modules dans la bon ordre. L'API du Serveur HTTP Apache 2.0 API permet aux modules de préciser leur d'activation, éliminant ainsi la raison d'être de ces deux directives.
- L'ordre des lignes de `LoadModule` n'est désormais plus important dans la plupart des cas.
- De nombreux modules ont été ajoutés, supprimés, renommés, divisés ou incorporés les uns aux autres.
- Les lignes `LoadModule` des modules intégrés dans leurs propres RPM (`mod_ssl`, `php`, `mod_perl` et autres) ne sont plus nécessaires puisqu'elles se trouvent dans leur fichier propre inclus dans le répertoire `/etc/httpd/conf.d/`.
- Les diverses définitions `HAVE_XXX` ne sont plus définies.

Important

Lors de la modification du fichier original, notez que le fichier `httpd.conf` doit absolument contenir la directive suivante :

```
Include conf.d/*.conf
```

L'oubli de cette directive entraînerait l'échec de tous les modules contenus dans leurs propres RPM (tels que `mod_perl`, `php` et `mod_ssl`).

10.2.1.4. Autres changements liés à l'environnement global

Les directives suivantes ont été supprimées de la configuration du Serveur HTTP Apache 2.0 :

- *`ServerType`* — Le Serveur HTTP Apache ne peut être exécuté qu'en tant que `ServerType standalone`, rendant ainsi cette directive inutile.

- *AccessConfig* et *ResourceConfig* — Ces directives ont été supprimées puisqu'elles reflétaient la fonctionnalité de la directive Include. Si les directives AccessConfig et ResourceConfig sont définies, il est nécessaire de les remplacer par des directives Include.

  Pour obtenir l'assurance que les fichiers seront lus dans l'ordre désigné par les anciennes directives, il est nécessaire de placer les directives Include à la fin du fichier httpd.conf, en prenant bien soin de placer celle correspondant à ResourceConfig avant celle correspondant à AccessConfig. Si les valeurs par défaut sont utilisées, elles doivent être incluses explicitement dans les fichiers conf/srm.conf et conf/access.conf.

10.2.2. Configuration du serveur principal

La section relative à la configuration du serveur principal du fichier de configuration installe le serveur principal qui répond à toute les requêtes non-traitées par un hôte virtuel définit dans un conteneur <VirtualHost>. Des valeurs spécifiées ici offrent aussi des valeurs par défaut pour tous les fichiers conteneurs <VirtualHost> définis.

Les directives utilisées dans cette section ont été légèrement modifiées entre la version 1.3 du Serveur HTTP Apache et la version 2.0. Si la configuration du serveur principal a un niveau élevé personnalisation, il sera peut-être plus simple de modifier le fichier de configuration existant pour l'adapter au Serveur HTTP Apache 2.0. Les utilisateurs ayant une configuration peu personnalisée devraient migrer leurs changements vers la configuration 2.0 par défaut.

10.2.2.1. Mappage de UserDir

La directive UserDir est utilisée pour permettre à des URL telles que http://example.com/~bob/ de se mapper à un sous-répertoire au sein du répertoire personnel de l'utilisateur bob, comme par exemple /home/bob/public_html. Cette particularité permettant à un éventuel agresseur de déterminer si un nom d'utilisateur donné est présent sur le système, la configuration par défaut pour le Serveur HTTP Apache 2.0 désactive cette directive.

Pour activer le mappage de UserDir, changez la directive figurant dans le fichier httpd.conf de :

```
UserDir disable
```

à :

```
UserDir public_html
```

Pour obtenir davantage d'informations sur le sujet, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible sur le site Web à :

- http://httpd.apache.org/docs-2.0/mod/mod_userdir.html#userdir

10.2.2.2. Journalisation

Les directives de journalisation suivantes ont été supprimées :

- AgentLog
- RefererLog
- RefererIgnore

Cependant, les journaux Agent et Referrer sont encore disponibles en utilisant les directives CustomLog et LogFormat.

Pour obtenir davantage d'informations sur le sujet, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible sur le site Web à :

- http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#customlog
- http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#logformat

10.2.2.3. Indexation des répertoires

La directive `FancyIndexing` étant désormais obsolète a été supprimée. Cette même fonctionnalité est toutefois encore disponible par le biais de l'*option* `FancyIndexing` à l'intérieur de la directive `IndexOptions`.

La nouvelle option `VersionSort` appliquée à la directive `IndexOptions` permet de classer dans un ordre plus naturel les fichiers contenant des numéros de version. Par exemple, `httpd-2.0.6.tar` apparaît avant `httpd-2.0.36.tar` dans une page d'index de répertoires.

Les paramètres par défaut pour les directives `ReadmeName` et `HeaderName` ont été transférés des fichiers `README` et `HEADER` vers les fichiers `README.html` et `HEADER.html`.

Pour obtenir davantage d'informations sur le sujet, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible sur le site Web à :

- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#indexoptions
- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#readmename
- http://httpd.apache.org/docs-2.0/mod/mod_autoindex.html#headername

10.2.2.4. Négociation du contenu

La directive `CacheNegotiatedDocs` retient désormais les critères `on` ou `off`. Les cas existants de `CacheNegotiatedDocs` devront être remplacés par `CacheNegotiatedDocs on`.

Pour obtenir davantage d'informations sur le sujet, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible sur le site Web à :

- http://httpd.apache.org/docs-2.0/mod/mod_negotiation.html#cachenegotiateddocs

10.2.2.5. Documents d'erreur

Afin de pouvoir utiliser un message codé en dur avec la directive `ErrorDocument`, le message doit apparaître entre guillemets (["]), plutôt que d'être seulement précédé par des guillemets, comme c'était la cas avec le Serveur HTTP Apache 1.3.

L'extrait ci-dessous représente un exemple de directive du Serveur HTTP Apache version 1.3 :

```
ErrorDocument 404 "The document was not found
```

Pour transférer un paramètre `ErrorDocument` vers le Serveur HTTP Apache 2.0, utilisez la structure suivante :

```
ErrorDocument 404 "The document was not found"
```

Notez bien la présence des guillemets à la fin de l'exemple de directive `ErrorDocument` reproduit ci-dessus.

Pour obtenir davantage d'informations sur le sujet, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible sur le site Web à :

- http://httpd.apache.org/docs-2.0/mod/core.html#errordocument

10.2.3. Configuration des hôtes virtuels

Le contenu de tous les répertoires `<VirtualHost>` devrait être migré de la même manière que celle utilisée pour la section du serveur principal reportez-vous à la Section 10.2.2 pour obtenir des instructions sur le sujet..

Important

Notez que la configuration d'un hôte virtuel SSL/TLS a été supprimée du fichier de configuration du serveur principal pour être ajoutée dans le fichier `/etc/httpd/conf.d/ssl.conf`.

Pour obtenir de plus d'informations sur le sujet, reportez-vous au chapitre intitulé *Configuration du serveur sécurisé HTTP Apache* du *Guide d'administration système de Red Hat Enterprise Linux* et à la documentation en ligne disponible à l'adresse suivante :

- http://httpd.apache.org/docs-2.0/vhosts/

10.2.4. Modules et Serveur HTTP Apache 2.0

Dans la version 2.0 du Serveur HTTP Apache, le système de modules a été modifié afin de permettre aux modules d'être désormais liés ensemble ou combinés de plusieurs manières différentes. Les scripts *CGI*(de l'anglais *Common Gateway Interface*) par exemple, sont capables de générer des documents HTML analysés par le serveur qui peuvent ensuite être traités par `mod_include`. Grâce à ce développement, il existe désormais de nombreuses possibilités de combinaison des modules afin d'atteindre un objectif spécifique.

Cette situation est possible car chaque requête est servie par un seul module *handler*, suivi d'aucun ou de plusieurs modules *filter*.

Sous la version 1.3 du Serveur HTTP Apache par exemple, un script Perl serait traité dans son intégralité par le module Perl (`mod_perl`). Sous la version 2.0 du Serveur HTTP Apache, en revanche, la requête est initialement *traitée* par le module principal— qui sert des fichiers statiques — et est ensuite *filtrée* par `mod_perl`.

L'explication exacte de l'utilisation de cette fonction particulière et de toutes les autres nouvelles fonctions du Serveur HTTP Apache 2.0, va bien au-delà de la portée de ce document ; toutefois, la conversion a des ramifications non-négligeables si vous avez utilisé la directive `PATH_INFO` pour un document traité par un module qui est désormais traité comme un filtre étant donné que chaque directive contient des informations de chemin peu importantes après le vrai nom de fichier. Le module mémoire, qui traite initialement la requête, ne comprend pas par défaut `PATH_INFO` et renverra des erreurs de types `404 Not Found` pour les requêtes qui contiennent de telles informations. Vous pouvez également utiliser la directive `AcceptPathInfo` pour obliger le module mémoire à accepter les requêtes contenant `PATH_INFO`.

Ci-dessous figure un exemple de cette directive :

```
AcceptPathInfo on
```

Pour obtenir davantage d'informations sur le sujet, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible sur le site Web à :

- http://httpd.apache.org/docs-2.0/mod/core.html#acceptpathinfo
- http://httpd.apache.org/docs-2.0/handler.html
- http://httpd.apache.org/docs-2.0/filter.html

10.2.4.1. Module `suexec`

Dans la version du Serveur HTTP Apache 2.0, le module `mod_suexec` utilise la directive `SuexecUserGroup` (plutôt que les directives `User` et `Group`) pour la configuration des hôtes virtuels. Les directives `User` et `Group` peuvent toujours être utilisées d'une manière générale mais ne peuvent plus être utilisées pour la configuration des hôtes virtuels.

L'extrait ci-dessous représente un exemple de directive du Serveur HTTP Apache version 1.3 :

```
<VirtualHost vhost.example.com:80>
    User someone
    Group somegroup
</VirtualHost>
```

Pour transférer ce paramètre vers le Serveur HTTP Apache 2.0, utilisez la structure suivante :

```
<VirtualHost vhost.example.com:80>
    SuexecUserGroup someone somegroup
</VirtualHost>
```

10.2.4.2. Module `mod_ssl`

La configuration de `mod_ssl` a été transférée du fichier `httpd.conf` au fichier `/etc/httpd/conf.d/ssl.conf`. Pour que ce dernier soit chargé et que `mod_ssl` puisse fonctionner, la déclaration `Include conf.d/*.conf` doit figurer dans le fichier `httpd.conf`, comme l'explique la Section 10.2.1.3.

Les directives `ServerName` dans les hôtes virtuels avec SSLdoivent explicitement spécifier le numéro de port.

L'extrait ci-dessous représente un exemple de directive du Serveur HTTP Apache version 1.3 :

```
<VirtualHost _default_:443>
    # General setup for the virtual host
    ServerName ssl.example.name
    ...
</VirtualHost>
```

Pour transférer ce paramètre vers le Serveur HTTP Apache 2.0, utilisez la structure suivante :

```
<VirtualHost _default_:443>
    # General setup for the virtual host
    ServerName ssl.host.name:443
    ...
</VirtualHost>
```

Il est également important de noter que les deux directives `SSLLog` et `SSLLogLevel` ont été supprimées. Le module `mod_ssl` obéit désormais aux directives `ErrorLog` et `LogLevel`. Reportez-vous à la Section 10.5.35 et à la Section 10.5.36 pour obtenir de plus amples informations sur ces directives.

Pour obtenir davantage d'informations sur le sujet, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible sur le site Web à :

- http://httpd.apache.org/docs-2.0/mod/mod_ssl.html
- http://httpd.apache.org/docs-2.0/vhosts/

10.2.4.3. Module `mod_proxy`

Les instructions relatives au contrôle de l'accès proxy sont maintenant placées dans un bloc `<Proxy>` plutôt que dans un répertoire `<Directory proxy:>`.

La fonctionnalité de stockage temporaire de l'ancien `mod_proxy` a été divisée en trois modules, à savoir :

- `mod_cache`
- `mod_disk_cache`
- `mod_mem_cache`

Ceux-ci utilisent généralement des directives similaires aux versions plus anciennes du module `mod_proxy`. Il est cependant conseillé de vérifier chaque directive avant de migrer tout paramètre de cache.

Pour obtenir davantage d'informations sur le sujet, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible sur le site Web à :

- http://httpd.apache.org/docs-2.0/mod/mod_proxy.html

10.2.4.4. Module `mod_include`

Le module `mod_include` fonctionnant désormais comme un filtre, il est activé d'une façon différente. Reportez-vous à la Section 10.2.4 pour obtenir de plus amples informations sur les filtres.

L'extrait ci-dessous représente un exemple de directive du Serveur HTTP Apache version 1.3 :

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

Pour transférer ce paramètre vers le Serveur HTTP Apache 2.0, utilisez la structure suivante :

```
AddType text/html .shtml
AddOutputFilter INCLUDES .shtml
```

Notez que, comme auparavant, la directive `Options +Includes` est toujours nécessaire pour le conteneur `<Directory>` ou dans un fichier `.htaccess`.

Pour obtenir davantage d'informations sur le sujet, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible sur le site Web à :

- http://httpd.apache.org/docs-2.0/mod/mod_include.html

10.2.4.5. Modules `mod_auth_dbm` et `mod_auth_db`

Le Serveur HTTP Apache 1.3 prenait en charge deux modules d'authentification, à savoir, `mod_auth_db` et `mod_auth_dbm`, qui utilisaient respectivement les bases de données Berkeley et DBM. Ces modules ont été rassemblés dans un seul module nommé `mod_auth_dbm` dans la version 2.0 du Serveur HTTP Apache, pouvant accéder à plusieurs formats de base de données différents. Pour effectuer une migration depuis le fichier `mod_auth_db`, il est nécessaire de modifier les fichiers de configuration en remplaçant `AuthDBUserFile` et `AuthDBGroupFile` par les équivalents de `mod_auth_dbm` à savoir `AuthDBMUserFile` et `AuthDBMGroupFile`. Il est également nécessaire d'ajouter la directive `AuthDBMType DB`pour préciser le type de fichier de base de données utilisé.

Ci-dessous figure un exemple de configuration `mod_auth_db` pour le Serveur HTTP Apache 1.3 :

```
<Location /private/>
  AuthType Basic
  AuthName "My Private Files"
  AuthDBUserFile /var/www/authdb
  require valid-user
</Location>
```

Pour transférer ce paramètre vers la version 2.0 du Serveur HTTP Apache, utilisez la structure suivante :

```
<Location /private/>
  AuthType Basic
  AuthName "My Private Files"
  AuthDBMUserFile /var/www/authdb
  AuthDBMType DB
  require valid-user
</Location>
```

Notez que la directive `AuthDBMUserFile` peut également être utilisée dans des fichiers `.htaccess`.

Dans la version 2.0 du Serveur HTTP Apache, le script Perl `dbmmanage` utilisé pour manipuler les bases de données des noms d'utilisateur et mots de passe a été remplacé par `htdbm`. Le programme `htdbm` offre des fonctionnalités équivalentes et, tout comme le module `mod_auth_dbm`, peut exploiter une grande variété de formats de bases de données ; l'option `-T` peut être utilisée sur la ligne de commande pour spécifier le format à utiliser.

Le Tableau 10-1 montre comment migrer d'un format de base de données DBM vers `htdbm` en utilisant `dbmmanage`.

Action	Commande dbmmanage (1.3)	Équivalent de la commande htdbm (2.0)
Ajoute l'utilisateur à la base de données (en utilisant le mot de passe donné)	`dbmmanage authdb add username password`	`htdbm -b -TDB authdb username password`
Ajoute l'utilisateur à la base de données (invite à fournir le mot de passe)	`dbmmanage authdb adduser username`	`htdbm -TDB authdb username`
Retire l'utilisateur de la base de données	`dbmmanage authdb delete username`	`htdbm -x -TDB authdb username`
Répertorie les utilisateurs dans la base de données	`dbmmanage authdb view`	`htdbm -l -TDB authdb`

Action	Commande dbmmanage (1.3)	Équivalent de la commande htdbm (2.0)
Vérifie un mot de passe	`dbmmanage authdb check username`	`htdbm -v -TDB authdb username`

Tableau 10-1. Migration de `dbmmanage` vers `htdbm`

Les options `-m` et `-s` fonctionnant avec `dbmmanage` et `htdbm`, il est possible d'utiliser les algorithmes MD5 ou SHA1 respectivement, pour le hachage des mots de passe.

Lors de la création d'une nouvelle base de données avec `htdbm`, il est nécessaire d'utiliser l'option `-c`.

Pour obtenir davantage d'informations sur le sujet, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible sur le site Web à :

- http://httpd.apache.org/docs-2.0/mod/mod_auth_dbm.html

10.2.4.6. Module `mod_perl`

La configuration du module `mod_perl` a été transférée du fichier `httpd.conf` au fichier `/etc/httpd/conf.d/perl.conf`. Pour que ce fichier soit chargé et permette ainsi à `mod_perl` de fonctionner correctement, la déclaration `Include conf.d/*.conf` doit figurer dans le fichier `httpd.conf`, comme le décrit la Section 10.2.1.3.

Les occurrences de `Apache::` contenues dans votre fichier `httpd.conf` doivent être remplacées par `ModPerl::`. En outre, la façon dont les gestionnaires de signaux (ou handlers) sont enregistrés a été modifiée.

Ci-dessous figure un exemple de la configuration du Serveur HTTP Apache 1.3 pour le module `mod_perl` :

```
<Directory /var/www/perl>
    SetHandler perl-script
    PerlHandler Apache::Registry
    Options +ExecCGI
</Directory>
```

Ci-après se trouve le module `mod_perl` équivalent pour la version 2.0 du Serveur HTTP Apache :

```
<Directory /var/www/perl>
    SetHandler perl-script
    PerlResponseHandler ModPerl::Registry
    Options +ExecCGI
</Directory>
```

La plupart des modules pour `mod_perl` 1.x devraient fonctionner sans modification, avec `mod_perl` 2.x. Les modules XS nécessitent une recompilation et des modifications mineures de Makefile seront peut-être également nécessaires.

10.2.4.7. Module `mod_python`

La configuration du module `mod_python` a été transférée du fichier `httpd.conf` au fichier `/etc/httpd/conf.d/python.conf`. Pour que ce dernier soit chargé et permette ainsi à `mod_python` de fonctionner correctement, la déclaration `Include conf.d/*.conf` doit figurer dans le fichier `httpd.conf` comme le décrit la Section 10.2.1.3.

10.2.4.8. PHP

La configuration de PHP a été transférée du fichier `httpd.conf` au fichier `/etc/httpd/conf.d/php.conf`. Pour que celui-ci soit chargé, la déclaration `Include conf.d/*.conf` doit figurer dans le fichier `httpd.conf`, comme le décrit la Section 10.2.1.3.

Remarque

Toutes les directives de configuration de PHP utilisées avec le Serveur HTTP Apache 1.3 sont désormais entièrement compatibles, lors de la migration vers le Serveur HTTP Apache 2.0 sur Red Hat Enterprise Linux 4.

Dans PHP 4.2.0 et les versions postérieures, l'ensemble des variables par défaut qui sont prédéfinies et ont généralement une portée globale, a changé. Les variables d'entrée individuelle et les variables de serveur ne sont plus, par défaut, directement placées dans la portée globale. Ce changement risque d'interrompre les scripts. Revenez à l'ancien comportement en réglant `register_globals` sur `On` dans le fichier `/etc/php.ini`.

Pour obtenir davantage d'informations sur le sujet et pour obtenir des renseignements détaillés sur les changements au niveau de la portée globale, reportez-vous à l'URL suivante :

- http://www.php.net/release_4_1_0.php

10.2.4.9. Module `mod_authz_ldap`

Red Hat Enterprise Linux est fournit avec le module `mod_authz_ldap` pour le Serveur HTTP Apache. Ce module utilise le nom raccourci du nom distinct (ou distinguished name) d'un sujet et de l'émetteur du certificat SSL client afin de déterminer le nom distinct de l'utilisateur au sein d'un répertoire LDAP. Il est également à même d'effectuer les tâches suivantes : autoriser un utilisateur en fonction des attributs de l'entrée du répertoire LDAP de cet utilisateur, déterminer l'accès aux ressources en fonction des privilèges octroyés aux utilisateurs et aux groupes quant à ces ressources et peut également refuser l'accès aux utilisateurs dont le mot de passe a expiré. Le module `mod_ssl` est nécessaire lorsque le module `mod_authz_ldap` est utilisé.

Important

Le module `mod_authz_ldap` n'effectue pas l'authentification d'un utilisateur par rapport à un répertoire LDAP au moyen d'un hachage de mots de passe cryptés. Cette fonctionnalité est fournie par le module expérimental `mod_auth_ldap` qui ne fait pas partie de Red Hat Enterprise Linux. Pour obtenir de plus amples informations sur le statut de ce module, reportez-vous au site Web de l'organisation Apache Software Foundation qui se trouve à l'adresse suivante : http://www.apache.org/.

Le fichier `/etc/httpd/conf.d/authz_ldap.conf` configure le module `mod_authz_ldap`.

Pour obtenir de plus amples informations sur la configuration du module tiers `mod_authz_ldap`, reportez-vous au fichier `/usr/share/doc/mod_authz_ldap-<version>/index.html` (en prenant soin de remplacer *<version>* par le numéro de version du paquetage).

10.3. Après l'installation

Après l'installation du paquetage `httpd`, passez en revue la documentation du Serveur HTTP Apache disponible en ligne à l'adresse suivante : http://httpd.apache.org/docs-2.0/.

La documentation du Serveur HTTP Apache contient une liste exhaustive de toutes les options de configuration accompagnée d'une description complète. Ce chapitre fournit de brèves descriptions des directives de configuration utilisées par le Serveur HTTP Apache 2.0.

La version 2.0 du Serveur HTTP Apache offre la possibilité de définir des serveurs Web sécurisés au moyen du fort cryptage SSL offert par les paquetages `mod_ssl` et `openssl`. Notez que le fichier de configuration contient aussi bien un serveur Web non-sécurisé qu'un serveur Web sécurisé. Le serveur Web sécurisé fonctionne comme un hôte virtuel configuré dans le fichier `/etc/httpd/conf.d/ssl.conf`. Pour obtenir de plus amples informations sur les hôtes virtuels, reportez-vous à la Section 10.8. Pour vous informer sur la configuration d'un hôte virtuel sur un serveur sécurisé, reportez-vous à la Section 10.8.1. Pour vous informer sur l'installation d'un serveur sécurisé HTTP Apache, reportez-vous au chapitre intitulé *Configuration du serveur sécurisé HTTP Apache* du *Guide d'administration système de Red Hat Enterprise Linux*.

Remarque

Red Hat, Inc. ne contient pas les extensions FrontPage car la licence Microsoft™ interdit d'inclure ces extensions dans le produit d'un fournisseur tiers. Pour obtenir plus d'informations sur les extensions FrontPage et le Serveur HTTP Apache, rendez-vous à l'adresse suivante : http://www.rtr.com/fpsupport/.

10.4. Démarrage et arrêt de `httpd`

Le RPM `httpd` installe le script `/etc/init.d/httpd` qui est accessible à l'aide de la commande `/sbin/service`.

Pour démarrer le serveur, saisissez la commande suivante en étant connecté en tant que super-utilisateur :

```
/sbin/service httpd start
```

Pour arrêter le serveur, saisissez la commande suivante en étant connecté en tant que super-utilisateur :

```
/sbin/service httpd stop
```

L'option `restart` est une façon rapide d'arrêter et de redémarrer le Serveur HTTP Apache.

Pour redémarrer le serveur, saisissez la commande suivante en étant connecté en tant que super-utilisateur :

```
/sbin/service httpd restart
```

Remarque

Lors de l'exécution du Serveur HTTP Apache en tant que serveur sécurisé, il est nécessaire de saisir le mot de passe du serveur chaque fois que des options `start` ou `restart` sont utilisées.

Après avoir modifié le fichier `httpd.conf`, il n'est toutefois pas nécessaire d'arrêter et de redémarrer le serveur. Utilisez à la place l'option `reload` qui entraînera un rechargement du fichier.

Afin de recharger le fichier de configuration, saisissez la commande suivante en étant connecté en tant que super-utilisateur :

```
/sbin/service httpd reload
```

Remarque

Lors de l'exécution du Serveur HTTP Apache en tant que serveur sécurisé, vous *n'aurez pas* besoin de saisir votre mot de passe lors de utilisation de l'option `reload` (recharger).

Par défaut, le service `httpd` ne se lancera *pas* automatiquement au démarrage. Pour configurer le service `httpd` de manière à ce qu'il soit lancé au démarrage, utilisez un utilitaire de script d'initialisation (ou initscript) tel que `/sbin/chkconfig`, **/sbin/ntsysv** ou l'**Outil de configuration des services**. Reportez-vous au chapitre intitulé *Contrôle de l'accès aux services* du *Guide d'administration système de Red Hat Enterprise Linux* pour obtenir davantage d'informations sur ces outils.

Remarque

Lors de exécution du Serveur HTTP Apache en tant que serveur sécurisé, le mot de passe de ce dernier doit être saisi après le démarrage de l'ordinateur lorsqu'une clé SSL privée et cryptée est utilisée.

Pour toute information sur l'installation d'un serveur sécurisé HTTP Apache, reportez-vous au chapitre intitulé *Configuration du serveur sécurisé HTTP Apache* du *Guide d'administration système de Red Hat Enterprise Linux*.

10.5. Directives de configuration dans `httpd.conf`

Le fichier de configuration du Serveur HTTP Apache est `/etc/httpd/conf/httpd.conf`. Dans le fichier `httpd.conf` figurent de nombreux commentaires qui rendent sont contenu très explicite. La configuration par défaut fonctionne dans la plupart des situations ; cependant, il est important de bien connaître certaines des options de configuration les plus importantes.

Avertissement

Avec l'arrivée du Serveur HTTP Apache 2.0, de nombreuses options de configuration ont changé. Pour toute information sur la migration d'un fichier de configuration de la version 1.3 vers le nouveau format, reportez-vous à la Section 10.2.

10.5.1. Astuces générales de configuration

Lors de la configuration du Serveur HTTP Apache, modifiez `/etc/httpd/conf/httpd.conf` puis rechargez, redémarrez ou arrêtez le processus `httpd` comme l'explique la Section 10.4.

Avant de modifier `httpd.conf`, faites une copie de sauvegarde du fichier original. Ainsi, si vous commettez une erreur lors de la modification du fichier de configuration, vous pourrez toujours utiliser la copie de sauvegarde pour résoudre d'éventuels problèmes.

Si une erreur est commise et que le serveur Web ne fonctionne pas correctement, passez d'abord en revue les passages modifiés du fichier `httpd.conf` afin de corriger toute faute de frappe.

Consultez ensuite le journal d'erreurs du serveur Web, `/var/log/httpd/error_log`. Selon votre expérience, le journal d'erreurs peut paraître quelque peu difficile à interpréter. Ceci étant, les dernières entrées du journal d'erreurs devraient fournir des informations utiles.

Les sections suivantes contiennent de brèves descriptions des directives contenues dans le fichier `httpd.conf`. Ces descriptions ne sont pas exhaustives. Pour obtenir de plus amples informations, reportez-vous à la documentation de l'organisation Apache disponible en ligne à l'adresse suivante : http://httpd.apache.org/docs-2.0/.

Pour obtenir davantage d'informations sur les directives `mod_ssl`, reportez-vous à la documentation disponible en ligne à l'adresse suivante : http://httpd.apache.org/docs-2.0/mod/mod_ssl.html.

10.5.2. `ServerRoot`

Le répertoire `ServerRoot` est le répertoire de niveau supérieur contenant les fichiers du serveur. Par défaut, la directive `ServerRoot` est paramétrée sur `"/etc/httpd"` aussi bien pour le serveur sécurisé que pour le serveur non-sécurisé.

10.5.3. `PidFile`

`PidFile` est le nom du fichier dans lequel le serveur enregistre son identifiant de processus (PID). Le PID par défaut est `/var/run/httpd.pid`.

10.5.4. `Timeout`

`Timeout` définit la durée, exprimée en secondes, pendant laquelle le serveur attend des réceptions et des émissions pendant les communications. La valeur de `Timeout` est paramétrée sur `300` secondes par défaut, ce qui est approprié pour la plupart des situations.

10.5.5. `KeepAlive`

`KeepAlive` définit si votre serveur autorisera plus d'une requête par connexion ; cette directive peut servir à empêcher un client particulier d'utiliser une trop grande quantité des ressources dont le serveur est doté.

Par défaut, la valeur de `Keepalive` est réglée sur `off`. Si la valeur de `Keepalive` est `on` et que le serveur devient très occupé, il peut générer rapidement le nombre maximum de processus enfants. Dans ce cas, le serveur sera considérablement ralenti. Si la directive `Keepalive` est activée, il est recommandé de donner à `KeepAliveTimeout` une valeur basse (reportez-vous à la Section 10.5.7 pour obtenir de plus amples informations sur la directive `KeepAliveTimeout`) et de contrôler le fichier journal `/var/log/httpd/error_log` du serveur. Ce journal indique si le serveur est sur le point d'atteindre le maximum de processus enfants.

10.5.6. `MaxKeepAliveRequests`

Cette directive définit le nombre maximum de requêtes autorisées par connexion persistante. L'organisation Apache Project recommande l'utilisation d'un paramétrage élevé, ce qui entraîne une

amélioration des performances du serveur. Par défaut, la valeur de `MaxKeepAliveRequests` paramétrée sur `100` est approprié pour la plupart des situations.

10.5.7. `KeepAliveTimeout`

`KeepAliveTimeout` définit la durée exprimée en secondes pendant laquelle le serveur attend après avoir servi une requête, avant d'interrompre la connexion. Une fois que le serveur reçoit une requête, c'est la directive `Timeout` qui s'applique à sa place. Par défaut, la valeur donnée à la directive `KeepAliveTimeout` est de 15 secondes.

10.5.8. `IfModule`

Les balises `<IfModule>` et `</IfModule>` créent un conteneur conditionnel dont les directives ne sont activées que si le module spécifié est chargé. Les directives placées entre les 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 chargé. En revanche, si un point d'exclamation ([!]) figure devant le nom du module, les directives ne sont traitées que si le module contenu dans la balise `<IfModule>` n'est *pas* chargé.

Pour obtenir de plus amples informations sur les modules du Serveur HTTP Apache, reportez-vous à la Section 10.7.

10.5.9. Directives de server-pool spécifiques aux MPM

Comme l'explique la Section 10.2.1.2, sous le Serveur HTTP Apache 2.0, la responsabilité de gérer les caractéristiques de server-pool est octroyée à un groupe de modules appelé MPM. Les caractéristiques de server-pool sont différentes selon le MPM spécifique utilisé. C'est la raison pour laquelle un conteneur `IfModule` est nécessaire pour définir le server-pool du MPM qui est utilisé.

Par défaut, le Serveur HTTP Apache 2.0 définit le server-pool aussi bien pour le MPM `prefork` que le MPM `worker`.

Ci-dessous figure une liste des directives figurant dans les conteneurs de server-pool spécifiques aux MPM.

10.5.9.1. `StartServers`

La directive `StartServers` définit le nombre de processus serveur créés au démarrage. Étant donné que le serveur Web supprime et crée dynamiquement des processus serveur en fonction de la charge du trafic, il n'est pas nécessaire de modifier ce paramètre. Le serveur Web est configuré de manière à lancer `8` processus serveur au démarrage pour le MPM `prefork` et `2` pour le MPM `worker`.

10.5.9.2. `MaxRequestsPerChild`

`MaxRequestsPerChild` définit le nombre total de requêtes que chaque processus serveur enfant sert avant de s'arrêter. L'attribution d'une valeur à `MaxRequestsPerChild` est importante afin d'éviter des pertes de mémoire induites par des processus longs. La valeur par défaut de `MaxRequestsPerChild` pour le MPM `prefork` est `4000` et `0` pour le MPM `worker`.

10.5.9.3. `MaxClients`

`MaxClients` fixe une limite au nombre total de processus serveur ou de clients connectés simultanément qui peuvent s'exécuter en même temps. L'objectif principal de cette directive est d'éviter qu'un Serveur HTTP Apache surchargé n'entraîne le plantage de votre système d'exploitation. Pour

des serveurs très solicités, cette valeur devrait être élevée. La valeur par défaut du serveur est 150, indépendamment du MPM utilisé. Toutefois, il n'est pas recommandé d'attribuer à `MaxClients` une valeur supérieure à `256` lors de l'utilisation du MPM `prefork`.

10.5.9.4. `MinSpareServers` and `MaxSpareServers`

Ces valeurs ne sont pas seulement utilisées avec le MPM `prefork`. Elles ajustent la façon selon laquelle le Serveur HTTP Apache s'adapte dynamiquement à la charge reçue en maintenant un nombre approprié de processus serveur de secours déterminiés en fonction du nombre de requêtes entrantes. Le serveur vérifie le nombre de serveurs attendant une requête et en supprime certains s'ils sont plus nombreux que `MaxSpareServers` ou en crée d'autres s'ils sont moins nombreux que `MinSpareServers`.

La valeur par défaut donnée à `MinSpareServers` est `5` ; la valeur par défaut attribuée à `MaxSpareServers` est `20`. Ces paramètres par défaut devraient être adaptés à presque toutes les situations. Ne donnez pas à `MinSpareServers` une valeur très élevée car un tel choix se traduira en une charge de traitement importante sur le serveur, même si le trafic est faible.

10.5.9.5. `MinSpareThreads` et `MaxSpareThreads`

Ces valeurs ne sont pas seulement utilisées avec le MPM `worker`. Elles ajustent la façon selon laquelle le Serveur HTTP Apache s'adapte dynamiquement à la charge reçue en maintenant un nombre approprié de processus serveur de secour déterminés en fonction du nombre de requêtes entrantes. Le serveur vérifie le nombre de threads de serveurs attendant une requête et en supprime certains s'ils sont plus nombreux que `MaxSpareThreads` ou en crée d'autres s'ils sont moins nombreux que `MinSpareThreads`.

La valeur par défaut donnée à `MinSpareThreads` est `25` ; la valeur par défaut attribuée à `MaxSpareThreads` est `75`. Ces paramètres par défaut devraient être appropriés à la plupart des situations. La valeur de `MaxSpareThreads` doit être supérieure ou égale à la somme de `MinSpareThreads` et de `ThreadsPerChild`, dans le cas contraire, le Serveur HTTP Apache la corrigera automatiquement.

10.5.9.6. `ThreadsPerChild`

Cette valeur est utilisée uniquement avec le MPM `worker`. Il définit le nombre de threads (ou fils) au sein de chaque processus enfant. La valeur par défaut pour cette directive est `25`.

10.5.10. `Listen`

La commande `Listen` identifie les ports sur lesquels votre serveur Web acceptera les demandes entrantes. Par défaut, le Serveur HTTP Apache est paramétré pour écouter les communications Web non-sécurisées sur le port 80et (dans `/etc/httpd/conf.d/ssl.conf` définissant tout serveur sécurisé) les communications Web sécurisées sur le port 443.

Si le Serveur HTTP Apache est configuré pour écouter l'activité sur un port dont le numéro est inférieur à 1024, seul le super-utilisateur peut le lancer. En revanche, pour les ports dont le numéro est égal ou supérieur à 1024, `httpd` peut être lancée en tant que simple utilisateur.

La directive `Listen` peut également être utilisée pour spécifier des adresses IP particulières sur lesquelles le serveur acceptera des connexions.

10.5.11. `Include`

`Include` permet d'inclure d'autres fichiers de configuration au moment de l'exécution.

Le chemin d'accès vers ces fichiers de configuration peut être absolu ou relatif par rapport au `ServerRoot`.

Important

Pour que le serveur utilise individuellement des modules paquetés, tels que `mod_ssl`, `mod_perl` et `php`, la directive suivante doit être intégrée dans la `Section 1 : Global Environment` du `httpd.conf` :

```
Include conf.d/*.conf
```

10.5.12. `LoadModule`

`LoadModule` est utilisée pour charger des modules DSO (de l'anglais Dynamic Shared Object, objet partagé dynamiquement). Pour obtenir davantage d'informations sur la prise en charge DSO du Serveur HTTP Apache, y compris la manière précise d'utiliser la directive `LoadModule`, reportez-vous à la Section 10.7. Notez que l'ordre du chargement des modules *n'est plus important* avec le Serveur HTTP Apache 2.0. Reportez-vous à la Section 10.2.1.3 pour plus d'informations sur la prise en charge DSO du Serveur HTTP Apache 2.0.

10.5.13. `ExtendedStatus`

La directive `ExtendedStatus` spécifie si Apache doit produire des informations élémentaires (`off`) ou détaillées (`on`) sur l'état des serveurs, lorsque le gestionnaire de signal `server-status` est appelé. Ce dernier est appelé à l'aide des balises `Location`. Pour obtenir davantage d'informations sur l'appel de `server-status`, reportez-vous à la Section 10.5.60.

10.5.14. `IfDefine`

Les balises `IfDefine` entourent des directives de configuration. Elles s'appliquent si résultat du "test" spécifié dans la balise `IfDefine` est vrai. Les directives sont ignorées si le résultat du test est faux.

Le test dans les balises `IfDefine` est un nom de paramètre (comme 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, lorsque le serveur Web est démarré, le test est vrai et les directives contenues dans les balises `IfDefine` sont appliquées.

10.5.15. `SuexecUserGroup`

La directive `SuexecUserGroup` figurant dans le module `mod_suexec`, permet de spécifier les privilèges d'exécution des programmes CGI qui s'applique à l'utilisateur et au groupe. Des requêtes non-CGI continuent à être traitées en fonction de l'utilisateur et du groupe spécifié dans les directives `User` et `Group`.

Remarque

La directive `SuexecUserGroup` remplace la configuration du Serveur HTTP Apache 1.3 configuration qui utilisait les directives `User` (utilisateur) et `Group` (Groupe) au sein de la configuration des sections `VirtualHosts` (Hôtes virtuels).

10.5.16. `User`

La directive `User` définit le nom d'utilisateur du processus serveur et détermine les fichiers auxquels le serveur peut avoir accès. Tous les fichiers auxquels cet utilisateur n'aura pas accès seront également inaccessibles aux clients se connectant au Serveur HTTP Apache.

La valeur par défaut donnée à `User` est `apache`.

Cette directive a été supprimée pour la configuration des hôtes virtuels.

Remarque

Pour des raisons de sécurité, le Serveur HTTP Apache n'est pas exécuté en tant que super-utilisateur.

10.5.17. `Group`

Spécifie le nom de groupe des processus du Serveur HTTP Apache.

Cette directive a été supprimée pour la configuration des hôtes virtuels.

La valeur par défaut attribuée à `Group` est `apache`.

10.5.18. `ServerAdmin`

Donnez comme valeur à la directive `ServerAdmin` 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 donnée à `ServerAdmin` est `root@localhost`.

Généralement, la valeur donnée à `ServerAdmin` est `Webmaster@example.com`. Une fois cette valeur déterminée, créez un alias pour `Webmaster` établi au nom de la personne responsable du serveur Web dans `/etc/aliases` et exécutez `/usr/bin/newaliases`.

10.5.19. `ServerName`

`ServerName` permet de définir un nom d'hôte et un numéro de port (en accord avec la directive `Listen`) pour le serveur. La directive `ServerName` ne doit pas forcément correspondre au nom d'hôte de l'ordinateur. Par exemple, le serveur Web pourrait être `www.example.com` bien que le nom d'hôte du serveur soit `foo.example.com`. La valeur spécifiée dans `ServerName` doit être un nom de domaine (ou DNS, de l'anglais Domain Name Service) valide qui peut être résolu par le système — ne vous contentez surtout pas d'en inventer un.

Ci-dessous figure un exemple de directive `ServerName` :

```
ServerName www.example.com:80
```

Lors de la détermination d'un `ServerName`, assurez-vous que son adresse IP et son nom de serveur figurent bien dans le fichier `/etc/hosts`.

10.5.20. `UseCanonicalName`

Lorsque la valeur attribuée à cette directive est `on`, elle configure le Serveur HTTP Apache de manière à ce qu'il se référence en utilisant les valeurs précisées dans les directives `ServerName` et `Port`. En revanche, lorsque la valeur de `UseCanonicalName` est `off`, le serveur emploie à la place la valeur utilisée par le client envoyant la requête lorsqu'il fait référence à lui-même.

Par défaut, la valeur attribuée à `UseCanonicalName` est `off`.

10.5.21. `DocumentRoot`

`DocumentRoot` est le répertoire contenant la plupart des fichiers HTML qui seront servis en réponse aux requêtes. Le défaut de `DocumentRoot` aussi bien pour le serveur Web sécurisé que pour le serveur Web non-sécurisé est le répertoire `/var/www/html`. Par exemple, il se peut que le serveur reçoive une demande pour le document suivant :

```
http://example.com/foo.html
```

Le serveur recherche le fichier suivant dans le répertoire par défaut :

```
/var/www/html/foo.html
```

Pour modifier `DocumentRoot` afin qu'il ne soit pas partagé par le serveur Web sécurisé et par le serveur Web non-sécurisé, reportez-vous à la Section 10.8.

10.5.22. `Directory`

Les balises `<Directory /path/to/directory>` et `</Directory>` créent un conteneur utilisé pour entourer un groupe de directives de configuration devant uniquement s'appliquer à ce répertoire et à ses sous-répertoires. Toute directive applicable à un répertoire peut être utilisée à l'intérieur de balises `Directory`.

Par défaut, des paramètres très restrictifs sont appliqués au répertoire racine (`/`), à l'aide des directives `Options` (voir la Section 10.5.23) et `AllowOverride` (voir la Section 10.5.24). Sous une telle configuration, tout répertoire du système ayant besoin de paramètres plus permissifs doit contenir explicitement ces paramètres.

Dans la configuration par défaut, un autre conteneur `Directory` est également configuré pour `DocumentRoot` ; ce faisant, des paramètres moins rigides sont assignés à l'arborescence de répertoires, de manière à ce que le Serveur HTTP Apache puisse avoir accès à des fichiers placés dans ce dernier.

Le `répertoire` conteneur peut également être utilisé pour configurer des répertoires `cgi-bin` supplémentaires pour des applications côté-serveur en dehors du répertoire spécifié dans la directive `ScriptAlias` (reportez-vous à la Section 10.5.41 pour obtenir de plus amples informations sur la directive `ScriptAlias`).

Pour ce faire, le conteneur `Directory` doit déterminer l'option `ExecCGI` pour ce répertoire.

Par exemple, si les scripts CGI se trouvent dans `/home/my_cgi_directory`, ajoutez le conteneur `Directory` suivant au fichier `httpd.conf` :

```
<Directory /home/my_cgi_directory>
    Options +ExecCGI
</Directory>
```

Ensuite, il est nécessaire d'enlever le symbole de commanetaire présent dans la directive `AddHandler` afin de permettre l'identification des fichiers ayant une extension `.cgi` en tant que scripts CGI. Reportez-vous à la Section 10.5.56 pour obtenir des instructions sur le paramétrage de `AddHandler`.

Pour que cette opération se déroule parfaitement, il est nécessaire de définir les permissions pour les scripts CGI et pour le chemin d'accès complet vers les scripts en tant que 0755.

10.5.23. `Options`

La directive `Options` contrôle les fonctionnalités spécifiques du serveur qui sont disponibles dans un répertoire particulier. Par exemple, en vertu des paramètres restrictifs spécifiés pour le répertoire root, `Options` est réglée uniquement sur `FollowSymLinks`. Aucune fonctionnalité n'est activée, à l'exception du fait que le serveur est autorisé à suivre les liens symboliques dans le répertoire root.

Par défaut, dans le répertoire `DocumentRoot`, `Options` est paramétrée pour inclure `Indexes` et `FollowSymLinks`. `Indexes` permet au serveur de générer le contenu d'un répertoire si aucun `DirectoryIndex` (par exemple, `index.html`) n'est spécifié. `FollowSymLinks` permet au serveur de suivre des liens symboliques dans ce répertoire.

Remarque

Les déclarations `Options` de la section de configuration du serveur principal doivent être copiées individuellement dans chaque conteneur `VirtualHost`. Reportez-vous à la Section 10.5.65 pour obtenir de plus amples informations sur le sujet.

10.5.24. `AllowOverride`

La directive `AllowOverride` définit si des `Options` peuvent être annulées par les instructions présente dans un fichier `.htaccess`. Par défaut, aussi bien le répertoire racine que le répertoire `DocumentRoot` sont paramétrés pour ne permettre aucune annulation via `.htaccess`.

10.5.25. `Order`

La directive `Order` contrôle simplement l'ordre dans lequel les directives `allow` et `deny` sont analysées. Le serveur est configuré pour analyser les directives `Allow` avant d'analyser les directives `Deny` s'appliquant au répertoire `DocumentRoot`.

10.5.26. `Allow`

`Allow` spécifie le client pouvant accéder à un répertoire donné. Le client peut être `all`, un nom de domaine, une adresse IP, une adresse IP partielle, une paire réseau/masque réseau, etc. Le répertoire `DocumentRoot` est configuré afin d'autoriser les requêtes (`Allow`) de quiconque (`all`), de la sorte, tout le monde peut y accéder.

10.5.27. `Deny`

`Deny` fonctionne selon le même principe que `Allow`, sauf que cette fois-ci, l'accès est refusé à un client donné. Le `DocumentRoot` n'est pas configuré par défaut pour refuser (`Deny`) des requêtes provenant d'un client quelconque.

10.5.28. `UserDir`

`UserDir` est le nom du sous-répertoire, au sein du répertoire personnel de chaque utilisateur, où devraient être placés les fichiers HTML personnels devant être servis par le serveur Web. Par défaut, la valeur attribuée à cette directive est `disable` (désactiver).

Dans le fichier de configuration par défaut, le nom du sous-répertoire est `public_html`. Par exemple, il se peut que le serveur reçoive la requête suivante :

```
http://example.com/~username/foo.html
```

Le serveur rechercherait alorsle fichier :

```
/home/username/public_html/foo.html
```

Dans l'exemple ci-dessus, `/home/username/` est le répertoire personnel de l'utilisateur (notez que le chemin d'accès par défaut vers les répertoires personnels des utilisateurs peut être différent).

Assurez-vous que les autorisations relatives aux répertoires personnels des utilisateurs sont correctement définies. Les répertoires personnels des utilisateurs doivent avoir des permissions équivalentes à 0711. Les bits de lecture (r) et d'exécution (x) doivent être définis sur les répertoires `public_html` des utilisateurs (0755 fonctionnera également). Les fichiers qui seront servis dans les répertoires `public_html` des utilisateurs doivent au moins avoir un valeur équivalente à 0644.

10.5.29. `DirectoryIndex`

`DirectoryIndex` est la page servie par défaut lorsqu'un utilisateur demande un index de répertoire en insérant une barre oblique (/) à la fin d'un nom de répertoire.

Lorsqu'un utilisateur demande à accéder à la page http://*exemple*/*ce_répertoire*/, il obtient soit la page `DirectoryIndex` si elle existe, soit une liste de répertoires générée par le serveur. La valeur par défaut de `DirectoryIndex` est le type de topologie `index.html` et `index.html.var`. Le serveur essaie de trouver l'un de ces fichiers et renvoie le premier qu'il trouve. S'il ne trouve aucun des deux fichiers et que `Options Indexes` est paramétrée pour ce répertoire, le serveur génère et renvoie une liste au format HTML, des sous-répertoires et fichiers contenus dans le répertoire (à moins que la fonctionnalité de listage des répertoires ne soit desactivée).

10.5.30. `AccessFileName`

`AccessFileName` nomme le fichier que le serveur doit utiliser pour les informations de contrôle d'accès dans chaque répertoire. La valeur par défaut est `.htaccess`.

Juste après la directive `AccessFileName`, une série de balises `Files` établit un contrôle d'accès sur tout fichier commençant par `.ht`. Ces directives refusent l'accès par le Web à tous les fichiers `.htaccess` (ou d'autres commençant par `.ht`) pour des raisons de sécurité.

10.5.31. 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 une entrée saisie par le demandeur). Si la valeur de `CacheNegotiatedDocs` est paramétrée sur `on`, cette fonctionnalité est désactivée et les serveurs proxy seront alors autorisés à mettre en cache de tels documents.

10.5.32. 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 plutôt recommandé d'ajouter des types MIME à l'aide de la directive `AddType`.

Pour obtenir de plus amples informations sur `AddType`, reportez-vous à la Section 10.5.55.

10.5.33. DefaultType

`DefaultType` définit un type de contenu par défaut pour le serveur Web devant être utilisé pour des documents dont les types MIME ne peuvent pas être déterminés. La valeur par défaut est `text/plain`.

10.5.34. HostnameLookups

`HostnameLookups` peut être paramétrée sur `on`, `off` ou `double`. Si `HostnameLookups` est paramétrée sur `on`, le serveur résout automatiquement l'adresse IP pour chaque connexion. La résolution de l'adresse IP suppose que le serveur établisse une ou plusieurs connexions avec un serveur DNS, rallongeant ainsi la durée des opérations de traitement. Si `HostnameLookups` est paramétrée sur `double`, le serveur établira une recherche DNS double inversée, rallongeant par là-même encore plus la durée des opérations de traitement.

Afin de conserver des ressources sur le serveur, la valeur par défaut donnée à `HostnameLookups` est `off`.

Si des noms d'hôtes sont nécessaires dans les fichiers journaux de serveurs, songez à exécuter l'un des nombreux outils conçus pour analyser les fichiers journaux ; ces derniers effectuent des recherches DNS non seulement de manière plus efficace mais également en masse lors de la rotation des fichiers journaux de serveurs Web.

10.5.35. ErrorLog

`ErrorLog` spécifie le fichier dans lequel sont journalisées les erreurs concernant les serveurs. La valeur par défaut pour cette directive est `/var/log/httpd/error_log`.

10.5.36. LogLevel

`LogLevel` définit le niveau de détail avec lequel les messages d'erreur devraient être enregistrés dans les journaux d'erreurs. Les valeurs possibles de `LogLevel` sont (du niveau le moins détaillé au niveau le plus détaillé) `emerg`, `alert`, `crit`, `error`, `warn`, `notice`, `info` ou `debug`. La valeur par défaut donnée à `LogLevel` est `warn`.

10.5.37. `LogFormat`

La directive `LogFormat` configure le format des fichiers journaux des différents serveurs Web. Le `LogFormat` utilisé dépend en fait des paramètres attribués dans la directive `CustomLog` (voir la Section 10.5.38).

Ci-dessous figurent les options de format s'appliquant si la valeur de la directive `CustomLog` est `combined` :

`%h` (adresse IP de l'hôte distant ou nom d'hôte)

Répertorie l'adresse IP distante du client demandeur. Si la valeur de `HostnameLookups` est `on`, le nom d'hôte du client est enregistré à moins que le DNS ne puisse le fournir.

`%l` (rfc931)

Option non-utilisée. Un tiret ([-]) apparaît à sa place dans le fichier journal.

`%u` (utilisateur authentifié)

Affiche l'identifiant de l'utilisateur enregistré, si l'authentification était nécessaire. Cette option n'étant généralement pas utilisée, dans le fichier journal, un tiret ([-]) figure dans le champ en question.

`%t` (date)

Enregistre la date et l'heure de la requête.

`%r` (chaîne de demandes)

Enregistre la chaîne de demandes telle qu'elle a été envoyée depuis le navigateur ou le client.

`%s` (état)

Enregistre le code d'état HTTP renvoyé à l'hôte client.

`%b` (octets)

Enregistre la taille du document.

`%\"%{Referer}i\"` (referrer)

Enregistre l'URL de la page Web qui a renvoyé l'hôte client au serveur Web.

`%\"%{User-Agent}i\"` (utilisateur-agent)

Enregistre le type de navigateur Web effectuant la requête.

10.5.38. `CustomLog`

`CustomLog` identifie le fichier journal et le format du fichier journal. Par défaut, l'enregistrement se fait dans le fichier `/var/log/httpd/access_log`.

Le format par défaut de `CustomLog` est le format du fichier journal `combined` illustré ci-dessous :

```
remotehost rfc931 user date "request" status bytes referrer user-agent
```

10.5.39. `ServerSignature`

La directive `ServerSignature` ajoute une ligne contenant la version du Serveur HTTP Apache et le nom du serveur (`ServerName`) pour tout document créé par un serveur, comme par exemple, les messages d'erreurs renvoyés aux clients. La valeur par défaut donnée à `ServerSignature` est `on`.

La valeur de cette directive peut également être `off` ou `EMail`. La valeur `EMail` ajoute une balise HTML `mailto:ServerAdmin` à la ligne de signature des réponses produites automatiquement par le système.

10.5.40. `Alias`

Le paramètre `Alias` permet d'accéder aux répertoires se trouvant en dehors du répertoire `DocumentRoot`. Toute URL se terminant par l'alias sera automatiquement convertie en chemin d'accès vers l'alias. Par défaut, un alias pour un répertoire `icons` est déjà configuré. Un répertoire `icons` est accessible par le serveur Web, mais le répertoire ne figure pas dans `DocumentRoot`.

10.5.41. `ScriptAlias`

La directive `ScriptAlias` définit l'endroit où se trouvent les scripts CGI. D'une manière générale, il est préférable de ne pas laisser de scripts CGI dans `DocumentRoot`, où ils peuvent être consultés comme des documents texte. C'est pour cette raison qu'il existe un répertoire spécial en dehors du répertoire `DocumentRoot`, contenant des exécutables et scripts côté-serveur, qui est désigné par la directive `ScriptAlias`. Ce répertoire, connu sous le nom `cgi-bin`, a `/var/www/cgi-bin/` comme valeur par défaut.

Il est possible de créer des répertoires pour stocker des exécutables en dehors du répertoire `cgi-bin`. Pour de plus amples informations sur la manière de procéder, reportez-vous à la Section 10.5.56 et à la Section 10.5.22.

10.5.42. `Redirect`

Lorsqu'une page Web est déplacée, `Redirect` peut être utilisée pour mapper l'ancienne URL vers une autre URL. Le format est le suivant :

`Redirect /<`*`old-path`*`>/<`*`file-name`*`> http://<`*`current-domain`*`>/<`*`current-path`*`>/<`*`file-name`*`>`

Dans cet exemple, remplacez d'une part <*`old-path`*> par les informations de l'ancien-chemin vers <*`file-name`*> et d'autre part <*`current-domain`*> et <*`current-path`*> par les informations relatives au domaine et au chemin actuels pour <*`file-name`*>.

Dans cet exemple, toute requête pour <*`file-name`*> à l'ancien emplacement est automatiquement redirigée vers le nouvel emplacement.

Pour obtenir des informations sur les techniques de redirection, utilisez le module `mod_rewrite` inclus dans le Serveur HTTP Apache. Pour de plus amples informations sur la configuration du module `mod_rewrite`, reportez-vous à la documentation de l'organisation Apache Software Foundation disponible en ligne à l'adresse suivante : http://httpd.apache.org/docs-2.0/mod/mod_rewrite.html.

10.5.43. `IndexOptions`

`IndexOptions` contrôle l'apparence des listes de répertoires générées par le serveur, en ajoutant entre autres, des icônes et des descriptions de fichier. Si `Options Indexes` est définie (voir la Section 10.5.23), le serveur Web génère une liste des répertoires lorsqu'il reçoit une requête HTTP pour un répertoire sans index.

Le serveur Web recherche tout d'abord, dans le répertoire demandé un fichier correspondant aux noms spécifiés dans la directive `DirectoryIndex` (généralement, `index.html`). Si le serveur Web ne trouve aucun fichier `index.html`, le Serveur HTTP Apache génère une liste HTML des répertoires correspondant au répertoire demandé. L'apparence de cette liste de répertoires est contrôlée, en partie, par la directive `IndexOptions`.

La valeur de la configuration par défaut est `FancyIndexing`. Ainsi, un utilisateur peut réorganiser une liste de répertoires en cliquant sur les en-têtes des colonnes. En cliquant deux fois sur la même en-tête, le classement passera d'un ordre ascendant à un ordre descendant. La valeur `FancyIndexing` affiche également différentes icônes selon les types de fichiers, et ce, en fonction de leur extension.

Si l'option `AddDescription` est utilisée avec `FancyIndexing`, une brève description du fichier sera incluse dans les listes de répertoires générées par le serveur.

`IndexOptions` comprend un certain nombre de paramètres supplémentaires pouvant être utilisés pour contrôler l'apparence des répertoires créés par le serveur. Les paramètres `IconHeight` et `IconWidth` nécessitent que le serveur des balises HTML `HEIGHT` et `WIDTH` pour les icônes contenues dans les pages Web générées par le serveur. Le paramètre `IconsAreLinks` associe l'icône graphique à l'ancre du lien HTML, qui contient la cible du lien URL.

10.5.44. `AddIconByEncoding`

Cette directive nomme des icônes qui s'affichent par fichier avec codage MIME, dans des listes de répertoires générées par le serveur. Par exemple, le serveur Web est paramétré par défaut pour afficher l'icône `compressed.gif` à côté des fichiers codés MIME x-compress et x-gzip dans des listes de répertoires générées par le serveur.

10.5.45. `AddIconByType`

Cette directive nomme des icônes qui s'affichent à côté des fichiers avec des types MIME dans des listes de répertoires générées par serveur. Par exemple, le serveur est paramétré pour afficher l'icône `text.gif` à côté de fichiers avec un type MIME `text`, dans des listes de répertoires générées par le serveur.

10.5.46. `AddIcon`

`AddIcon` spécifie l'icône à afficher dans les listes de répertoires générées par le serveur pour des fichiers avec certaines extensions. Par exemple, le serveur Web est paramétré pour afficher l'icône `binary.gif` pour les fichiers portant les extensions `.bin` ou `.exe`.

10.5.47. `DefaultIcon`

`DefaultIcon` spécifie l'icône à afficher dans les listes de répertoires générées par le serveur pour les fichiers pour lesquels aucune autre icône n'est spécifiée. Le fichier image `unknown.gif` est la valeur par défaut.

10.5.48. `AddDescription`

Lors de l'utilisation de `FancyIndexing` comme paramètre de `IndexOptions`, la directive `AddDescription` peut être utilisée pour afficher des descriptions spécifiées par l'utilisateur pour certains fichiers ou pour certains types de fichiers dans des listes de répertoires générées par le serveur. La directive `AddDescription` prend en charge les fichiers de listes spécifiques, les expressions à caractères génériques ou les extensions de fichiers.

10.5.49. ReadmeName

`ReadmeName` nomme le fichier qui, s'il existe dans le répertoire, est ajouté à la fin des listes de répertoires générées par serveur. Le serveur Web commence par essayer d'inclure le fichier comme un document HTML, puis essaie de l'inclure comme un simple document texte. Par défaut, `ReadmeName` est paramétré sur `README.html`.

10.5.50. HeaderName

`HeaderName` nomme le fichier qui, s'il existe dans le répertoire, est ajouté au début des listes de répertoires générées par serveur. Comme `ReadmeName`, le serveur essaie, si possible, de l'inclure sous la forme d'un document HTML ou sinon, comme simple texte.

10.5.51. IndexIgnore

`IndexIgnore` affiche une liste d'extensions de fichiers, de noms de fichiers partiels, d'expressions contenant des caractères génériques ou de noms de fichiers complets. Le serveur Web n'inclura dans les listes de répertoires générées par le serveur, aucun fichier correspondant à l'un de ces paramètres.

10.5.52. AddEncoding

`AddEncoding` nomme des extensions de noms de fichiers qui devraient spécifier un type de codage particulier. Il est également possible d'utiliser `AddEncoding` pour donner l'instruction à certains navigateurs de décompresser certains fichiers lors de leur téléchargement.

10.5.53. AddLanguage

`AddLanguage` associe des extensions de noms de fichiers à des langues spécifiques. Cette directive est très utilisée pour le Serveur HTTP Apache (ou plusieurs) qui sert des contenus dans une multitude de langues et ce, en fonction de la préférence linguistique définie sur le navigateur client.

10.5.54. LanguagePriority

`LanguagePriority` permet de déterminer l'ordre de préférence des langues, au cas où aucune préférence linguistique ne serait paramétrée sur le navigateur client.

10.5.55. AddType

Utilisez la directive `AddType` pour définir ou annuler un type de MIME par défaut et des paires d'extensions de fichiers. L'exemple de directive suivant indique à Serveur HTTP Apache de reconnaître l'extension de fichier `.tgz` :

```
AddType application/x-tar .tgz
```

10.5.56. AddHandler

`AddHandler` mappe des extensions de fichiers sur des gestionnaires de signaux 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. L'exemple suivant est un exemple de directive `AddHandler` pour l'extension `.cgi`.

```
AddHandler cgi-script .cgi
```

Cette directive active les scripts CGI en dehors du répertoire `cgi-bin` afin qu'ils puissent fonctionner dans tout répertoire se trouvant sur le serveur dont l'option `ExecCGI` figure au sein du conteneur de répertoires. Reportez-vous à la Section 10.5.22 pour obtenir davantage d'informations sur la définition de l'option `ExecCGI` pour un répertoire.

Outre son utilisation avec les scripts CGI, la directive `AddHandler` sert aussi au traitement de fichiers HTML et imagemap analysés par le serveur.

10.5.57. `Action`

`Action` spécifie l'association d'un type de contenu MIME à un script CGI de sorte que lorsqu' un fichier de ce type de support est demandé, un script CGI particulier est exécuté.

10.5.58. `ErrorDocument`

La directive `ErrorDocument` associe un code de réponse HTTP à un message ou à une URL qui sera renvoyé au client. Par défaut, le serveur Web renvoie un simple message d'erreur, habituellement obscur, lorsqu'une erreur se produit. La directive `ErrorDocument` force le serveur Web à renvoyer à la place une page ou un message personnalisés.

Important

Pour que le message soit valide, il *doit* se trouver entre guillemets ["].

10.5.59. `BrowserMatch`

La directive `BrowserMatch` permet au serveur de définir des variables d'environnement ou de prendre des mesures appropriées en fonction du champ d'en-tête Utilisateur-Agent HTTP (User-Agent HTTP) — qui identifie le type de navigateur du client. Par défaut, le serveur Web utilise `BrowserMatch` pour refuser des connexions à certains navigateurs présentant des problèmes connus de même que pour désactiver les les activités keepalive et vidages d'en-têtes HTTP pour les navigateurs ayant des problèmes avec ces actions.

10.5.60. `Location`

Les balises `<Location>` et `</Location>` permettent de créer un conteneur dans lequel un contrôle d'accès basé sur l'URL peut être spécifié.

Par exemple, pour permettre aux personnes se connectant depuis le domaine du serveur de consulter des rapports sur l'état du serveur, utilisez les directives suivantes :

```
<Location /server-status>
    SetHandler server-status
    Order deny,allow
    Deny from all
    Allow from <.example.com>
</Location>
```

Remplacez `<.example.com>` par le nom de domaine de second niveau du serveur Web.

Pour fournir des rapports de configuration des serveurs (y compris des modules installés et des directives de configuration) en réponse à des requêtes en provenance de votre domaine, utilisez les directives suivantes :

```
<Location /server-info>
    SetHandler server-info
    Order deny,allow
    Deny from all
    Allow from <.example.com>
</Location>
```

Ici encore, remplacez <.example.com> par le nom de domaine de second niveau du serveur Web.

10.5.61. ProxyRequests

Pour configurer le Serveur HTTP Apache de manière à ce qu'il fonctionne comme un serveur Proxy, supprimez le symbole dièse (#) placé au début de la ligne <IfModule mod_proxy.c>, de la directive ProxyRequests et de chaque ligne figurant dans la section <Proxy>. Paramétrez la directive ProxyRequests sur On et définissez les domaines devant avoir accès au serveur dans la directive Allow from figurant dans la section <Proxy>.

10.5.62. Proxy

Les balises <Proxy *> et </Proxy> permettent de créer un conteneur qui renferme un groupe de directives de configuration devant s'appliquer seulement au serveur proxy. À l'intérieur des balises <Proxy>, il est possible d'utiliser de nombreuses directives s'appliquant à un répertoire.

10.5.63. Directives cache

Un certain nombre de directives cache commentées sont fournies dans le fichier de configuration par défaut du Serveur HTTP Apache. Dans la plupart des situations, il suffit de supprimer le commentaire en retirant le symbole dièse (#) placé au début de la ligne. Ci-après figure une liste de certaines des directives associées au cache ayant une grande importance :

- CacheEnable — Spécifie si le cache est un disque, une mémoire ou un cache de description de fichiers. Par défaut, CacheEnable configure un cache de disque pour les URL au niveau de ou au-dessous de /.
- CacheRoot — Définit le nom du répertoire qui contiendra les fichiers mis en cache. La valeur par défaut donnée à CacheRoot est le répertoire /var/httpd/proxy/.
- CacheSize — Définit la quantité d'espace en kilo-octets (Ko) que le cache peut utiliser. La valeur par défaut pour CacheSize est 5 Ko.

Ci-dessous figure une liste des autres directives courantes associées au cache.

- CacheMaxExpire — Définit la durée pendant laquelle les documents HTML mis en cache seront conservés (sans rechargement à partir du serveur Web duquel ils proviennent). La valeur par défaut est de 24 heures (86400 secondes).
- CacheLastModifiedFactor — Paramètre la création d'une date d'expiration pour un document qui a été reçu depuis le serveur d'origine sans date d'expiration définie. La valeur par défaut pour CacheLastModifiedFactor est réglée sur 0.1, ce qui signifie que la date d'expiration de tout document de ce type est égale à un dixième de la durée écoulée depuis la dernière modification du document.

- `CacheDefaultExpire` — Détermine la durée exprimée en heures, de l'expiration d'un document qui a été reçu à l'aide d'un protocole ne prenant pas en charge les délais d'expiration. La valeur par défaut est réglée sur `1` heure (`3600` secondes).
- `NoProxy` — Établit une liste de sous-réseaux, d'adresses IP, de domaines ou d'hôtes séparés par des espaces dont le contenu n'est pas mis en cache. Ce paramètre est le plus utile sur les sites Intranet.

10.5.64. `NameVirtualHost`

La directive `NameVirtualHost` associe une adresse IP à un numéro de port, si nécessaire, pour tout hôte virtuel portant un nom. La configuration d'hôtes virtuels nommés permet à un Serveur HTTP Apache de servir différents domaines sans devoir pour ce faire utiliser de multiples adresses IP.

Remarque

L'utilisation de tout hôte virtuel nommé fonctionne *seulement* avec des connexions HTTP non-sécurisées. Si vous devez employer des hôtes virtuels avec un serveur sécurisé, utilisez plutôt des hôtes virtuels basés sur l'adresse IP.

Afin d'activer l'hébergement d'hôtes virtuels basés sur le nom, supprimez le symbole de commentaire figurant dans la directive de configuration `NameVirtualHost` et ajoutez la bonne adresse IP. Ajoutez ensuite des conteneurs `VirtualHost` supplémentaires pour chaque hôte virtuel, en fonction des besoins de votre configuration.

10.5.65. `VirtualHost`

Des balises `<VirtualHost>` et `</VirtualHost>` permettent de créer un conteneur soulignant les caractéristiques d'un hôte virtuel. Le conteneur `VirtualHost` accepte la plupart des directives de configuration.

Un conteneur `VirtualHost` commenté est fourni dans `httpd.conf` et illustre le groupe minimum de directives de configuration nécessaires pour chaque hôte virtuel. Reportez-vous à la Section 10.8 pour obtenir de plus amples informations sur les hôtes virtuels.

Remarque

Le conteneur d'hôtes virtuels SSL par défaut se trouve désormais dans le fichier `/etc/httpd/conf.d/ssl.conf`.

10.5.66. Directives de configuration SSL

Les directives figurant dans le fichier `/etc/httpd/conf.d/ssl.conf` peuvent être configurées pour permettre des communications Web sécurisées à l'aide de SSL et TLS.

10.5.66.1. `SetEnvIf`

La directive `SetEnvIf` permet de régler des variables d'environnement en fonction des en-têtes des connexions entrantes. Il ne s'agit *pas* seulement d'une directive SSL, bien qu'elle soit présente dans le fichier `/etc/httpd/conf.d/ssl.conf` fourni. Dans le présent contexte, elle sert à désactiver la fonction keep-alive HTTP et à autoriser SSL à fermer la connexion sans générer de notification de fermeture de la part du navigateur client. Ce paramètre est nécessaire pour certains navigateurs qui n'interrompent pas la connexion SSL avec une grande fiabilité.

Pour obtenir de plus amples informations sur d'autres directives présentes dans le fichier de configuration SSL, consultez les documents disponibles aux adresses suivantes :

- http://localhost/manual/mod/mod_ssl.html
- http://httpd.apache.org/docs-2.0/mod/mod_ssl.html

Pour vous informer sur l'installation d'un serveur sécurisé HTTP Apache, reportez-vous au chapitre intitulé *Configuration du serveur sécurisé HTTP Apache* du *Guide d'administration système de Red Hat Enterprise Linux*.

Remarque

Dans la plupart des cas, les directives SSL sont configurées de manière appropriée lors de l'installation de Red Hat Enterprise Linux. Faites très attention lors de la modification des directives du serveur sécurisé HTTP Apache car une mauvaise configuration peut être à l'origine de brèches de sécurité, rendant tout système vulnérable.

10.6. Modules par défaut

Le Serveur HTTP Apache est distribué avec un certain nombre de modules. Par défaut, les modules suivants sont installés et activés avec le paquetage `httpd` dans Red Hat Enterprise Linux 4 :

```
mod_access
mod_actions
mod_alias
mod_asis
mod_auth
mod_auth_anon
mod_auth_dbm
mod_auth_digest
mod_auth_ldap
mod_autoindex
mod_cache
mod_cern_meta
mod_cgi
mod_dav
mod_dav_fs
mod_deflate
mod_dir
mod_disk_cache
mod_env
mod_expires
mod_ext_filter
mod_file_cache
```

```
mod_headers
mod_imap
mod_include
mod_info
mod_ldap
mod_log_config
mod_logio
mod_mem_cache
mod_mime
mod_mime_magic
mod_negotiation
mod_proxy
mod_proxy_connect
mod_proxy_ftp
mod_proxy_http
mod_rewrite
mod_setenvif
mod_speling
mod_status
mod_suexec
mod_unique_id
mod_userdir
mod_usertrack
mod_vhost_alias
```

En outre, les modules suivants sont disponibles en installant des paquetages complémentaires :

```
mod_auth_kerb
mod_auth_mysql
mod_auth_pgsql
mod_authz_ldap
mod_dav_svn
mod_jkz
mod_perl
mod_python
mod_ssl
php
```

10.7. Ajout de modules

Le Serveur HTTP Apache prend en charge des objets partagés dynamiquement (ou *DSO* de l'anglais *Dynamically Shared Objects*) ou des modules qui peuvent facilement être chargés selon les besoins.

Ã l'adresse suivante : http://httpd.apache.org/docs-2.0/dso.html, l'organisation Apache Project fournit une documentation complète en ligne sur les objets partagés dynamiquement (DSO). Sinon, si le paquetage `http-manual` est installé, de la documentation relative aux DSO est disponible en ligne à l'adresse suivante : http://localhost/manual/mod/.

Pour que le Serveur HTTP Apache puisse utiliser un DSO, il doit être spécifié dans une directive `LoadModule` du répertoire `/etc/httpd/conf/httpd.conf` ; si le module est fourni par un paquetage séparé, la ligne doit apparaître au sein du fichier de configuration des modules dans le répertoire `/etc/httpd/conf.d/`. Reportez-vous à la Section 10.5.12 pour obtenir de plus amples informations sur le sujet.

Lors de l'ajout ou de la suppression de modules du fichier `http.conf`, le Serveur HTTP Apache doit être rechargé ou relancé, comme l'explique la Section 10.4.

Lors de la création d'un nouveau module, installez tout d'abord le paquetage `httpd-devel` qui contient les fichiers à inclure (include files), les fichiers d'en-têtes ainsi que l'application *Apache eXtenSion* (`/usr/sbin/apxs`), qui utilise les fichiers à inclure et les fichiers d'en-têtes pour compiler les DSO.

Après l'écriture d'un module, utilisez `/usr/sbin/apxs` pour compiler les sources de votre module en dehors de l'arborescence source d'Apache. Pour obtenir de plus amples informations sur l'utilisation de la commande `/usr/sbin/apxs`, reportez-vous à la documentation Apache fournie en ligne à l'adresse suivante : http://httpd.apache.org/docs-2.0/dso.html et à la page de manuel de `apxs`.

Une fois le module compilé, placez-le dans le répertoire `/usr/lib/httpd/`. Ajoutez ensuite une ligne `LoadModule` dans le fichier `httpd.conf` en suivant la structure ci-dessous :

```
LoadModule <module-name> <path/to/module.so>
```

Où *<module-name>* correspond au nom du module et *<path/to/module.so>* au chemin d'accès vers le DSO.

10.8. Hôtes virtuels

L'hébergement intégré des hôtes virtuels du Serveur HTTP Apache permet au serveur de fournir différentes informations en fonction de l'adresse IP, du nom d'hôte ou du port faisant l'objet de la requête. Un guide complet sur l'utilisation des hôtes virtuels est disponible en ligne à l'adresse suivante : http://httpd.apache.org/docs-2.0/vhosts/.

10.8.1. Configuration d'hôtes virtuels

La meilleure façon de créer un hôte virtuel basé sur le nom consiste à utiliser le conteneur d'hôte virtuel fourni à titre d'exemple dans `httpd.conf`.

L'exemple de l'hôte virtuel offert se présente de la manière suivante :

```
#NameVirtualHost *:80
#
#<VirtualHost  *:80>
#    ServerAdmin webmaster@dummy-host.example.com
#    DocumentRoot /www/docs/dummy-host.example.com
#    ServerName dummy-host.example.com
#    ErrorLog logs/dummy-host.example.com-error_log
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
```

Pour activer la fonction d'hôte virtuel nommé, décommentez la ligne `NameVirtualHost` en retirant le symbole dièse (`#`) et en le remplaçant par le symbole de l'astérisque (`*`) accompagné de l'adresse IP attribuée à l'ordinateur.

Configurez ensuite un hôte virtuel, en décommentant et personnalisant le conteneur `<VirtualHost>`.

Sur la ligne `<VirtualHost>`, remplacez l'astérisque (`*`) par l'adresse IP du serveur. Remplacez aussi `ServerName` par le nom d'un DNS *valide* assigné à l'ordinateur et configurez les autres directives selon les besoins.

Étant donné que le conteneur `<VirtualHost>` accepte presque toutes les directives disponibles dans le cadre de la configuration du serveur principal, sa capacité à être personnalisé est très élevée.

Astuce

Si vous configurez un hôte virtuel pour qu'il écoute un port autre que le défaut, ce port doit être ajouté à la directive `Listen` dans la partie relative aux paramètres globaux du fichier `/etc/httpd/conf/http.conf`.

Afin de pouvoir activer l'hôte virtuel qui vient d'être créé, le Serveur HTTP Apache doit être rechargé ou redémarré. Reportez-vous à la Section 10.4 pour obtenir des instructions sur le sujet.

Des informations complètes sur la création et la configuration d'hôtes virtuels sur la base du nom ou de l'adresse IP sont fournies en ligne à l'adresse suivante : http://httpd.apache.org/docs-2.0/vhosts/.

10.8.2. Hôte virtuel du serveur Web sécurisé

Par défaut, le Serveur HTTP Apache est configuré aussi bien comme un serveur Web non-sécurisé que comme un serveur sécurisé. Aussi bien le serveur non-sécurisé que le serveur sécurisé utilisent la même adresse IP et le même nom d'hôte, mais écoutent des ports différents, à savoir 80 et 443 respectivement. Ce faisant, des communications aussi bien non-sécurisées que sécurisées peuvent être établies simultanément.

Il est important de savoir que les transmissions HTTP améliorées grâce à SSL monopolisent cependant plus de ressources que le protocole HTTP standard et que par conséquent, un serveur sécurisé sert moins de pages par seconde. Dans de telles conditions, il est souvent recommandé de minimiser les informations disponibles à partir du serveur sécurisé, tout particulièrement sur un site Web très solicité.

Important

N'utilisez pas d'hôtes virtuels nommés de concert avec un serveur Web sécurisé car le protocole de transfert SSL intervient avant que la requête HTTP n'identifie l'hôte virtuel nommé approprié. Les hôtes virtuels nommés ne fonctionnent qu'avec un serveur Web non-sécurisé.

Les directives de configuration pour du serveur sécurisé se trouvent entre des balises d'hôte virtuel dans le fichier `/etc/httpd/conf.d/ssl.conf`.

Par défaut, aussi bien le serveur Web, sécurisé que le serveur non-sécurisé partagent le même `DocumentRoot`. Il est cependant recommandé qu'un `DocumentRoot` différent soit disponible pour le serveur Web sécurisé.

Afin que le serveur Web non-sécurisé n'accepte plus de connexions, annulez la ligne `Listen 80` du fichier `httpd.conf` en ajoutant un symbole dièse (`#`) au début de cette ligne. Une fois cette opération terminée, la ligne ressemblera à l'extrait ci-dessous :

```
#Listen 80
```

Pour plus d'informations sur la configuration d'un serveur Web utilisant SSL, reportez-vous au chapitre intitulé *Configuration du serveur HTTP Apache sécurisé* du *Guide d'administration système de Red Hat Enterprise Linux*. Pour obtenir des astuces de configuration avancées, consultez la documentation de l'organisation Apache Software Foundation qui est disponible en ligne aux adresses suivantes :

- http://httpd.apache.org/docs-2.0/ssl/
- http://httpd.apache.org/docs-2.0/vhosts/

10.9. Ressources supplémentaires

Pour en savoir plus sur le Serveur HTTP Apache, consultez les ressources mentionnées ci-dessous.

10.9.1. Sites Web utiles

- http://httpd.apache.org — Le site Web officiel du Serveur HTTP Apache contenant de la documentation non seulement sur toutes les directives mais également sur tous les modules par défaut.
- http://www.modssl.org — Le site Web officiel de `mod_ssl`.
- http://www.apacheweek.com — Une newsletter hebdomadaire complète en ligne concernant Apache.

10.9.2. Livres sur le sujet

- *Apache Desktop Reference* de Ralf S. Engelschall ; Addison Wesley — Ce livre écrit par Ralf Engelschall, un membre de l'organisation 'Apache Software Foundation (ASF) et auteur de `mod_ssl`, *Apache Desktop Reference* constitue un guide de référence concis et exhaustif pour l'utilisation du Serveur HTTP Apache et plus particulièrement pour sa compilation, sa configuration et son exécution. Ce livre est également disponible en ligne à l'adresse suivante : http://www.apacheref.com/.
- *Professional Apache* de Peter Wainwright ; Wrox Press Ltd — Ce manuel, *Professional Apache*, fait partie des nombreux livres de la collection "Programmer to Programmer" de la maison d'édition Wrox Press Ltd, destiné aux administrateurs de serveurs Web aussi bien expérimentés que débutants.
- *Administering Apache* de Mark Allan Arnold ; Osborne Media Group — Ce livre est destiné aux fournisseurs d'accès Internet désireux d'offrir des services plus sécurisés.
- *Apache Server Unleashed* de Richard Bowen, et al ; SAMS BOOKS — Une source encyclopédique pour le Serveur HTTP Apache.
- *Apache Pocket Reference* d'Andrew Ford, Gigi Estabrook ; O'Reilly — La dernière nouveauté de la collection O'Reilly Pocket Reference.
- *Guide d'administration système de Red Hat Enterprise Linux* ; Red Hat, Inc. — Ce manuel contient un chapitre sur la configuration du Serveur HTTP Apache à l'aide de l'**Outil de configuration HTTP** ainsi qu'un chapitre sur la configuration du serveur sécurisé Serveur HTTP Apache.
- *Guide de sécurité de Red Hat Enterprise Linux*; Red Hat, Inc. — Ce manuel contient un chapitre intitulé *Sécurité serveur* qui examine différentes manières de sécuriser le Serveur HTTP Apache et d'autres services.

Chapitre 11.

Courrier électronique

L'apparition du courrier électronique (ou *email*) remonte au début des années 1960. La boîte aux lettres se présentait sous la forme d'un fichier dans le répertoire personnel d'un utilisateur que seul ce dernier pouvait lire. Les applications de messagerie primitives ajoutaient des nouveaux messages de texte au bas du fichier et l'utilisateur devait parcourir tout le fichier qui ne cessait de grandir, afin de retrouver tout message spécifique. Ce système ne pouvait envoyer de messages qu'aux utilisateurs d'un même système.

Le premier transfert réseau d'un courrier électronique a eu lieu en 1971 lorsqu'un ingénieur informatique nommé Ray Tomlinson a envoyé un message test entre deux ordinateurs via ARPANET — le précurseur de l'Internet. De là, la popularité de la communication par email s'est rapidement développée et en moins de deux ans, elle représentait 75 pour cent du trafic d'ARPANET.

Au fil du temps, les systèmes de messagerie électronique basés sur des protocoles réseau standardisés ont évolué de telle manière qu'ils font désormais partie des services les plus couramment utilisés sur l'Internet. Red Hat Enterprise Linux offre de nombreuses applications avancées permettant de servir et accéder aux emails.

Ce chapitre examine d'une part les protocoles de courrier électronique utilisés à l'heure actuelle et d'autre part, certains des programmes de messagerie électronique conçus pour envoyer et recevoir des emails.

11.1. Protocoles de courrier électronique

De nos jours, le courrier électronique est délivré à l'aide d'une architecture client/serveur. Un message électronique est créé au moyen d'un programme client de messagerie électronique. Ce programme envoie ensuite le message à un serveur. Ce dernier transmet à son tour le message au serveur de messagerie du destinataire où il est transmis au client de messagerie du destinataire final.

Afin de rendre ce processus possible, une vaste gamme de protocoles réseau standard permettent à différents ordinateurs exécutant souvent différents systèmes d'exploitation et utilisant des programmes de messagerie électroniques différents, d'envoyer et de recevoir des emails.

Les protocoles suivants qui sont abordés dans ce chapitre sont ceux le plus fréquemment utilisés pour le transfert de courrier électronique entre systèmes.

11.1.1. Protocoles de transfert de courrier électronique

La livraison de courrier d'une application cliente au serveur et d'un serveur d'origine à un serveur de destination est traitée par le protocole nommé *Simple Mail Transfer Protocol* (ou *SMTP*).

11.1.1.1. SMTP

L'objectif primaire de SMTP consiste à transférer le courrier électronique entre les serveurs de messagerie. Toutefois, il a également une importance critique pour les clients de messagerie. Afin d'envoyer un email, le client envoie le message électronique à un serveur de messagerie sortant, qui à son tour contacte le serveur de messagerie de destination pour la livraison du message. Dans de telles circonstances, il est nécessaire de spécifier un serveur SMTP lors de la configuraton d'un client de messagerie.

Sous Red Hat Enterprise Linux, un utilisateur peut configurer un serveur SMTP sur l'ordinateur local afin qu'il traite la livraison du courrier. Toutefois, il est également possible de configurer des serveurs SMTP distants pour le courrier sortant.

Il est important de noter ici que le protocole SMTP n'a pas besoin d'authentification pour fonctionner. Ainsi, quiconque utilisant l'Internet peut envoyer des emails à toute autre personne ou même à de grands groupes de personnes. C'est cette caractéristique de SMTP qui permet l'envoi de pourriel (aussi appelé junk email) ou de *spam*. Les serveurs SMTP modernes essaient néanmoins de minimiser ce comportement en n'autorisant que les hôtes connus à accéder au serveur SMTP. Les serveurs n'imposant pas ce genre de restriction sont appelés serveurs *open relay*.

Par défaut, Sendmail (`/usr/sbin/sendmail`) est le programme SMTP par défaut sous Red Hat Enterprise Linux. Néanmoins, une application serveur de messagerie plus simple appelée Postfix (`/usr/sbin/postfix`) est également disponible.

11.1.2. Protocoles d'accès au courrier

Pour récupérer le courrier électronique stocké sur les serveurs de messagerie, les applications client de messagerie utilisent deux protocoles primaires : *Post Office Protocol* (ou *POP*) et *Internet Message Access Protocol* (ou *IMAP*).

Contrairement à SMTP, ces deux protocoles exigent des clients qui se connectent de s'authentifier au moyen d'un nom d'utilisateur (aussi appelé identifiant) et d'un mot de passe. Par défaut, les mots de passe pour les deux protocoles sont transmis à travers le réseau de manière non-cryptée.

11.1.2.1. POP

Sous Red Hat Enterprise Linux, le serveur POP par défaut est `/usr/sbin/ipop3d` qui est inclus dans le paquetage `imap`. Lors de l'utilisation d'un serveur POP, les messages électroniques sont téléchargés par des applications client de messagerie. Par défaut, la plupart des clients de messagerie POP sont configurés automatiquement pour supprimer les messages sur le serveur une fois le transfert effectué ; toutefois, cette configuration peut souvent être modifiée.

Le protocole POP est compatible à 100 % avec des normes de messagerie Internet importantes, telles que *Multipurpose Internet Mail Extensions* (ou *MIME*), qui permet l'envoi de pièces jointes.

Le protocole POP est le plus approprié pour les utilisateurs disposant d'un système sur lequel ils peuvent lire leurs courrier électronique. Il fonctionne également bien pour des utilisateurs n'ayant pas de connexion continue à l'Internet ou à un réseau sur lequel le serveur de messagerie se trouve. Malheureusement, pour les utilisateurs ayant des connexions réseau lentes, POP requiert que les programmes client, après authentification, téléchargent la totalité du contenu de chaque message. Cette opération peut être longue si certains messages contiennent des pièces jointes.

La version la plus courante du protocole POP standard est POP3.

Il existe néanmoins de nombreuses variantes moins utilisées du protocole POP :

- *APOP* — POP3 avec authentification MDS. Un hachage codé du mot de passe de l'utilisateur est envoyé du client de messagerie au serveur plutôt qu'une version de ce dernier sous forme non-cryptée.
- *KPOP* — POP3 avec authentification Kerberos. Reportez-vous au Chapitre 19 pour obtenir de plus amples informations.
- *RPOP* — POP3 avec authentification RPOP. Cette variante utilise un identificateur (ID) publié pour chaque utilisateur, semblable à un mot de passe, pour authentifier les requêtes POP. Cependant, étant donné que cet ID n'est pas crypté, RPOP n'est pas plus sécurisé que le POP standard.

Pour une sécurité accrue, il est possible d'utiliser le cryptage *Secure Socket Layer* (*SSL*) pour l'authentification des clients et pour les sessions de transfert de données. Cette fonctionnalité peut être activée en utilisant le service `ipop3s` ou le programme `/usr/sbin/stunnel`. Reportez-vous à la Section 11.5.1 pour obtenir de plus amples informations.

11.1.2.2. IMAP

Sous Red Hat Enterprise Linux, `/usr/sbin/imapd` est le serveur IMAP par défaut, fourni par le paquetage `imap`. Lors de l'utilisation d'un serveur de messagerie IMAP, le courrier électronique est conservé sur le serveur où les utilisateurs peuvent lire et supprimer les emails. IMAP permet également aux applications client de créer, renommer ou supprimer des répertoires de messagerie sur le serveur afin d'organiser ou de stocker le courrier électronique.

Le protocole IMAP est utile tout particulièrement pour les utilisateurs accédant à leur courrier électronique au moyen d'ordinateurs multiples. Ce protocole est également pratique pour les utilisateurs se connectant au serveur de messagerie par le biais d'une connexion lente, car seule l'information d'entête du message est téléchargée jusqu'à ce qu'il soit ouvert, économisant ainsi de la largeur de bande. En outre, l'utilisateur peut également supprimer des messages sans devoir les lire ou les télécharger.

Par commodité, les applications IMAP client peuvent mettre en cache localement des copies des messages afin que l'utilisateur puissent naviguer parmi des messages déjà lus même lorsqu'il n'est pas directement connecté au serveur IMAP.

IMAP, tout comme POP, est compatible à 100 % avec des normes de messagerie Internet importantes, telles que MIME (Multipurpose Internet Mail Extensions) pour permettre l'envoi de pièces jointes.

Pour une sécurité accrue, il est possible d'utiliser le cryptage *SSL* pour l'authentification des clients et pour les sessions de transfert de données. Cette fonctionnalité peut être activée en utilisant le service `imaps` ou le programme `/usr/sbin/stunnel` Reportez-vous à la Section 11.5.1 pour obtenir de plus amples informations.

D'autres clients et serveurs IMAP libres et commerciaux sont disponibles ; un certain nombre d'entre eux poussent encore plus les possibilités du protocole IMAP et fournissent des fonctionnalités supplémentaires. Une liste compréhensive de ces derniers est disponible en ligne à l'adresses suivante : http://www.imap.org/products/longlist.htm.

11.2. Classifications des programmes de messagerie électronique

D'une manière générale, toutes les applications de messagerie électronique font partie d'au moins un des trois types d'applications. Chaque type joue un rôle bien précis dans le processus de déplacement et de gestion des messages électroniques. Bien que la plupart des utilisateurs ne connaissent que le programme de courrier électronique qu'ils utilisent pour recevoir et envoyer des messages, chacun de ces trois types d'applications est important pour assurer que les messages arrivent à la bonne destination.

11.2.1. Agent de transfert de courrier (ATC)

L'*Agent de Transfert de Courrier* (*ATC*, ou MTA de l'anglais Mail Transfer Agent) sert à transférer des messages électroniques entre des hôtes utilisant SMTP. Un message peut requérir l'utilisation de plusieurs ATC lors de sa progression vers sa destination finale.

Alors que la livraison de messages entre ordinateurs puisse apparaître comme étant une opération assez simple et directe, l'ensemble du processus permettant de décider si un ATC (aussi appelé MTA selon l'acronyme anglais) donné peut ou devrait accepter la livraison d'un message, est en fait assez complexe. De plus, en raison des problèmes créés par les spams, l'utilisation d'un ATC spécifique est généralement limitée par la configuration même de l'ATC ou par celle de l'accès au réseau sur lequel il se trouve.

De nombreux programmes clients de messagerie peuvent également être utilisés comme des ATC pour envoyer des messages électroniques. Toutefois, il ne faut pas confondre cette opération avec le rôle primaire d'un ATC. La seule raison pour laquelle les programmes clients de messagerie peuvent envoyer des messages comme le fait un ATC réside dans le fait que l'hôte exécutant l'application

ne dispose pas de son propre ATC. Cette situation s'applique tout particulièrement aux programmes clients de messagerie faisant partie de systèmes d'exploitations qui ne sont pas basés sur Unix. Cependant, ces programmes clients de messagerie n'envoient que des messages de sortie à un ATC qu'ils sont autorisés à utiliser et n'acheminent pas directement le message au serveur de messagerie du destinataire souhaité.

Étant donné que Red Hat Enterprise Linux installe deux ATC, à savoir Sendmail et Postfix, les programmes clients de messagerie ne sont généralement pas sollicités pour agir en tant qu'ATC. Red Hat Enterprise Linux inclut également Fetchmail, un ATC doté d'un objectif bien spécifique.

Pour obtenir de plus amples informations sur Sendmail, Postfix et Fetchmail, reportez-vous à la Section 11.3.

11.2.2. Agent de distribution du courrier (ADC)

Un *Agent de Distribution de Courrier* (*ADC* ou MDA de l'anglais Mail Delivery Agent) est utilisé par l'ATC pour distribuer le courrier arrivant dans la boîte aux lettres de l'utilisateur approprié. Dans de nombreuses situations, l'ADC est en fait un *Agent de Distribution Local* (*ADL*ou LDA de l'anglais Local Delivery Agent), comme `mail` ou Procmail.

En fait, tout programme traitant un message à des fins de distribution jusqu'au point où il peut être lu par une application client de messagerie peut être considéré comme un ADC. Telle est la raison pour laquelle certains ATC (comme Sendmail et Postfix) peuvent aussi jouer le rôle d'un ADC lorsqu'ils ajoutent de nouveaux messages électroniques au fichier spoule (aussi écrit spool) de courrier électronique d'un utilisateur local. En général, les ADC n'acheminent pas de messages entre les deux systèmes et ne fournissent pas d'interface utilisateur ; les ADC distribuent et classent les messages sur un ordinateur local pour qu'une application client de messagerie puissent y accéder.

11.2.3. Agent de gestion de courrier (AGC)

Un *Agent de Gestion de Courrier* (*AGC*, ou MUA de l'anglais Mail User Agent) est en fait une application client de messagerie. Un AGC est un programme qui, au minimum, permet à un utilisateur de lire et écrire des messages électroniques. De nombreux AGC peuvent récupérer des messages au moyen de protocoles POP ou IMAP, établissant des boîtes aux lettres pour stocker les messages et envoyant des messages de sortie à un ATC.

Les AGC (aussi appelés MUA selon l'acronyme anglais) peuvent être graphiques, comme **Mozilla Mail**, ou peuvent avoir une interface très simple à base de texte comme `mutt`.

11.3. Agent de transfert de courrier (ATC)

Red Hat Enterprise Linux comprend deux agents ATC principaux (ou MTA selon l'acronyme anglais), à savoir Sendmail et Postfix. Sendmail est configuré comme l'agent de transfert par défaut, bien que Postfix puisse facilement devenir l'ATC par défaut.

Astuce

Pour obtenir des informations sur la manière de changer l'ATC par défaut en remplaçant Sendmail par Postfix, reportez-vous au chapitre intitulé *Configuration de l'Agent de transfert de courrier (ATC)* du *Guide d'administration système de Red Hat Enterprise Linux*.

11.3.1. Sendmail

La tâche principale de Sendmail est de déplacer de façon sécurisée des messages électroniques entre des hôtes, utilisant généralement le protocole SMTP. Toutefois, Sendmail étant hautement configurable, il est possible de contrôler presque tous les aspects du traitement des messages, y compris le protocole à utiliser. De nombreux administrateurs système choisissent d'utiliser Sendmail comme ATC en raison de sa puissance et de sa modulabilité.

11.3.1.1. Objectif et limites

Il est important de bien comprendre ce qu'est Sendmail et ce qu'il peut faire, de même que ce qu'il n'est pas. À l'heure où des applications monolithiques jouent des rôles multiples, on pourrait penser que Sendmail est la seule application nécessaire pour exécuter un serveur de messagerie au sein d'une organisation. Techniquement parlant, c'est la cas puisque Sendmail peut non seulement spouler du courrier sur les répertoires de chaque utilisateur maisl il peut également livrer des messages sortantspour les utilisateurs. Cependant, la plupart des utilisateurs demandent bien plus que le simple acheminement du courrier. Ils veulent en général interagir avec le courrier électronique à l'aide d'un AGC qui utilise POP ou IMAP pour télécharger leurs messages sur leur ordinateur local. Ou il se peut qu'ils préférent avoir une interface Web pour avoir accès à leur boîte aux lettres. Ces autres applications peuvent fonctionner de concert avec Sendmail, mais elles existent en réalité pour des raisons différentes et peuvent fonctionner indépendamment les unes des autres.

L'explication de tout ce que Sendmail devrait et pourrait faire en fonction de sa configuration va bien au-delà de la portée de cette section. Étant donné la gammes d'options différentes et le nombre de réglages possibles, des volumes entiers ont été écrits pour expliquer toutes les possibilités de Sendmail et les façons de résoudre d'éventuels problèmes. Reportez-vous à la Section 11.6 pour obtenir une liste des ressources dédiées à Sendmail.

Cette section passe en revue les fichiers installés par défaut avec Sendmail et examine certaines modifications de configuration élémentaires, y compris comment éviter de recevoir du pourriel (ou spam) et comment augmenter les capacités de Sendmail avec le protocole *Lightweight Directory Access Protocol (LDAP)*.

11.3.1.2. Installation de Sendmail par défaut

Le fichier exécutable de Sendmail est `/usr/sbin/sendmail`.

Le fichier de configuration de Sendmail qui est long et détaillé se nomme `/etc/mail/sendmail.cf`. Évitez d'éditer le fichier `sendmail.cf` directement. Pour apporter des modifications à la configuration, éditez plutôt le fichier `/etc/mail/sendmail.mc`, sauvegardez le fichier original `/etc/mail/sendmail.cf` et utilisez ensuite le macroprocesseur `m4` qui est inclus pour créer un nouveau fichier `/etc/mail/sendmail.cf`. De plus amples informations sur la configuration de Sendmail sont disponibles dans la Section 11.3.1.3.

Divers fichiers de configuration Sendmail sont installés dans `/etc/mail/`, notamment :

- `access` — Spécifie les systèmes qui peuvent utiliser Sendmail pour le courrier électronique sortant.
- `domaintable` — Spécifie le mappage de noms de domaine.
- `local-host-names` — Spécifie les alias de l'hôte.
- `mailertable` — Spécifie des instructions qui annulent le routage de domaines particuliers.
- `virtusertable` — Spécifie une forme de dénomination par alias spécifique au domaine, ce qui permet à des domaines virtuels multiples d'être hébergés sur un seul ordinateur.

Plusieurs fichiers de configuration placés dans `/etc/mail/`, tels que `access`, `domaintable`, `mailertable` et `virtusertable`, doivent en fait stocker leurs informations dans des fichiers de base de données avant que Sendmail ne puisse appliquer les modifications apportées à la

configuration. Pour inclure les changements apportés à ces fichiers de configuration dans leurs fichiers de base de données, exécutez la commande suivante :

```
makemap hash /etc/mail/<name> < /etc/mail/<name>
```

où <*name*> doit être remplacé par le nom du fichier de configuration à convertir.

Par exemple, pour que tous les messages électroniques destinés au domaine `example.com` soient envoyés à <`bob@other-example.com`>, ajoutez la ligne reproduite ci-dessous au fichier `virtusertable` :

```
@example.com      bob@other-example.com
```

Pour finaliser cette modification, le fichier `virtusertable.db` doit être mis à jour à l'aide de la commande suivante, en étant connecté en tant que super-utilisateur :

```
makemap hash /etc/mail/virtusertable < /etc/mail/virtusertable
```

Ce faisant, un nouveau fichier `virtusertable.db` est créé, contenant la nouvelle configuration.

11.3.1.3. Modifications courantes de la configuration de Sendmail

Lors de la modification du fichier de configuration Sendmail, il est recommandé de générer un tout nouveau fichier `/etc/mail/sendmail.cf` plutôt que de modifier un fichier existant.

Avertissement

Avant de modifier le fichier `sendmail.cf`, il est toujours conseillé d'effectuer une copie de sauvegarde de la version courante du fichier.

Pour ajouter la fonctionnalité désirée à Sendmail, éditez le fichier `/etc/mail/sendmail.mc` en étant connecté en tant que super-utilisateur. Une fois cette opération terminée, utilisez le macroprocesseur `m4` pour générer un nouveau fichier `sendmail.cf` en exécutant la commande suivante :

```
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

Par défaut, le macroprocesseur `m4` est installé avec Sendmail mais fait partie du paquetage `m4`.

Après avoir créé un nouveau fichier `/etc/mail/sendmail.cf`, redémarrez Sendmail afin que les modifications soient appliquées. Pour ce faire, la meilleure façon de procéder consiste à taper la commande suivante :

```
/sbin/service sendmail restart
```

Important

Le fichier `sendmail.cf` par défaut n'autorise pas Sendmail à accepter des connexions réseau venant de tout hôte autre que l'ordinateur local. Afin de configurer Sendmail en tant que serveur pour d'autres clients, éditez `/etc/mail/sendmail.mc` et changez l'adresse spécifiée dans l'option `Addr=` de la directive `DAEMON_OPTIONS` de `127.0.0.1` à l'adresse IP d'un périphérique réseau actif ou supprimez tout simplement les commentaires de la directive `DAEMON_OPTIONS` en ajoutant `dnl` au début de la ligne. Une fois ces modifications apportées, régénérez le fichier `/etc/mail/sendmail.cf` en exécutant la commande suivante :

```
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

La configuration par défaut incluse dans Red Hat Enterprise Linux pour être utilisée pour la plupart des sites exclusivement SMTP. Toutefois, elle ne fonctionne pas avec des sites utilisant UUCP (de l'anglais UNIX to UNIX Copy). Si l'utilitaire de connexion UUCP UUCP est utilisé pour les transferts, le fichier `/etc/mail/sendmail.mc` doit être reconfiguré et un nouveau fichier `/etc/mail/sendmail.cf` doit être généré.

Consultez le fichier `/usr/share/sendmail-cf/README` avant de modifier tout fichier contenu dans les répertoires présents sous le répertoire `/usr/share/sendmail-cf`, car ils peuvent affecter la configuration future de fichiers `/etc/mail/sendmail.cf`.

11.3.1.4. Masquage

L'une des configurations courantes de Sendmail consiste à avoir un seul ordinateur qui agit comme passerelle de messagerie pour tous les ordinateurs sur le réseau. Par exemple, une société pourrait souhaiter qu'un ordinateur appelé `mail.bigcorp.com` gère tout son courrier électronique et attribue à tous les messages sortants la même adresse de retour.

Dans ce cas de figure, le serveur Sendmail est obligé de masquer le nom des ordinateurs du réseau de la société de façon à ce que leur adresse de retour soit `user@example.com` plutôt que `user@host.example.com`.

Pour ce faire, ajoutez les lignes suivantes à `/etc/mail/sendmail.mc` :

```
FEATURE(always_add_domain)dnl
FEATURE('masquerade_entire_domain')
FEATURE('masquerade_envelope')
FEATURE('allmasquerade')
MASQUERADE_AS('bigcorp.com.')
MASQUERADE_DOMAIN('bigcorp.com.')
MASQUERADE_AS(bigcorp.com)
```

Une fois qu'un nouveau fichier `sendmail.cf` aura été généré à l'aide de `m4`, cette configuration donnera l'impression que tous les messages envoyés à partir du réseau ont été été envoyés depuis `bigcorp.com`.

11.3.1.5. Blocage de pourriel

Les pourriels (aussi appelés spams) peuvent être définis comme étant des messages électroniques inutiles et indésirables reçus par un utilisateur qui n'a jamais demandé ce genre de communication. Il s'agit d'un abus très perturbateur, coûteux et répandu des normes de communication Internet.

Sendmail rend relativement aisé le blocage des nouvelles techniques utilisées pour envoyer des pourriels. Il bloque même par défaut, un grand nombre des méthodes d'envoi de spams les plus courantes.

Par exemple, le réacheminement de messages SMTP, également appelé retransmission (ou relaying), a été désactivé par défaut depuis la version 8.9 de Sendmail. Avant que ce changement n'ait lieu, Sendmail dirigeait l'hôte de messagerie (`x.edu`) de façon à ce qu'il accepte des messages d'un individu (`y.com`) et les envoie à un autre individu (`z.net`). Désormais, Sendmail doit être configuré de façon à autoriser un domaine à retransmettre du courrier par le biais du serveur. Pour configurer les domaines de retransmission, éditez le fichier `/etc/mail/relay-domains` et relancez Sendmail.

Ceci étant, les utilisateurs sont très souvent bombardés de pourriel provenant d'autres serveurs via l'Internet. Dans ce cas, les fonctions de contrôle d'accès de Sendmail, disponibles par l'entremise du fichier `/etc/mail/access` peuvent servir à empêcher les connexions en provenance d'hôtes

indésirables. L'exemple suivant illustre comment utiliser ce fichier pour non seulement bloquer mais également autoriser l'accès au serveur Sendmail :

```
badspammer.com        ERROR:550 "Go away and do not spam us anymore"
tux.badspammer.com    OK
10.0                  RELAY
```

Cet exemple stipule que tout message électronique envoyé par `badspammer.com` doit être bloqué à l'aide d'un code d'erreur 550 conforme à la norme RFC-821 et qu'un message doit être renvoyé à l'expéditeur de pourriel. Le courrier envoyé par le sous-domaine `tux.badspammer.com` est en revanche accepté. La dernière ligne montre que tout message envoyé depuis le réseau 10.0.*.* peut être retransmis au moyen du serveur de messagerie.

Étant donné que `/etc/mail/access.db` est une base de données, utilisez `makemap` pour activer toute modification. Pour ce faire, tapez la commande suivante en étant connecté en tant que super-utilisateur :

```
makemap hash /etc/mail/access < /etc/mail/access
```

Cet exemple n'illustre qu'une toute petite partie du potentiel de Sendmail en termes d'autorisation ou d'interdiction d'accès. Reportez-vous au document `/usr/share/sendmail-cf/README` pour obtenir de plus amples renseignements et d'autres exemples sur le sujet.

Étant donné que Sendmail fait appel à l'ADC Procmail pour la livraison de courrier, il est également possible d'utiliser un programme de filtrage de pourriel comme SpamAssassin, pour identifier et classer ce type de courrier à la place de l'utilisateur. Reportez-vous à la Section 11.4.2.6 pour obtenir de plus amples informations sur l'utilisation du programme SpamAssassin.

11.3.1.6. Utilisation de Sendmail avec LDAP

L'utilisation de *Lightweight Directory Access Protocol (LDAP)* est une façon très rapide et puissante de trouver des informations spécifiques sur un utilisateur particulier appartenant à un grand groupe. Par exemple, un serveur LDAP peut servir à chercher une adresse électronique spécifique dans un répertoire d'entreprises courant à partir du nom de famille de l'utilisateur. Au niveau de ce genre d'implémentation, LDAP est très différent de Sendmail ; en effet, LDAP stocke les informations hiérarchiques des utilisateurs alors que Sendmail ne s'occupe que de recevoir le résultat de la recherche LDAP par le biais de messages électroniques pré-adressés.

Toutefois, Sendmail prend en charge une intégration beaucoup plus grande avec LDAP, là où il utilise LDAP pour remplacer des fichiers maintenus séparément, tels que `aliases` et `virtusertables`, sur divers serveurs de messagerie qui fonctionnent ensemble pour prendre en charge une organisation de taille moyenne ou supérieure. En bref, LDAP extraie le niveau de routage du courrier depuis Sendmail et ses fichiers de configuration séparés pour en faire un cluster LDAP puissant qui peut être influencé par de nombreuses applications différentes.

La version actuelle de Sendmail inclut la prise en charge pour LDAP. Pour étendre les possibilités de votre serveur Sendmail à l'aide de LDAP, prenez d'abord un serveur LDAP, tel que **OpenLDAP**, opérationnel et correctement configuré. Ensuite, modifiez votre fichier `/etc/mail/sendmail.mc` pour y inclure les éléments suivants :

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

Remarque

Ces instructions ne s'appliquent qu'à une configuration très élémentaire de Sendmail avec LDAP. La configuration peut être très différente de celle-ci selon votre implémentation de LDAP, en particulier lors de la configuration de plusieurs ordinateurs Sendmail destinés à utiliser un serveur LDAP commun.

Consultez `/usr/share/doc/sendmail/README.cf` pour obtenir aussi bien des instructions détaillées sur la configuration de routage LDAP que des exemples.

Ensuite, recréez le fichier `/etc/mail/sendmail.cf` en exécutant `m4` et en redémarrant Sendmail. Reportez-vous à la Section 11.3.1.3 pour obtenir des instructions sur la manière de procéder.

Pour obtenir davantage d'informations sur LDAP, reportez-vous au Chapitre 13.

11.3.2. Postfix

Mis au point à l'origine chez IBM par Wietse Venema, un programmeur et expert en sécurité, Postfix est un ATC compatible avec Sendmail qui est conçu pour être sécurisé, rapide et facile à configurer.

Afin d'accroître la sécurité, Postfix utilise une conception modulaire dans laquelle de petits processus dotés de privilèges limités sont lancés par un démon *maître* (ou master). Les petits processus dotés de privilèges limités effectuent des tâches très spécifiques en relation avec les différentes étapes de livraison du courrier et sont exécutés dans un environnement dit chrooté afin de restreindre l'impact des attaques.

Pour configurer Postfix de sorte qu'il accepte des connexions réseau venant d'hôtes autres que l'ordinateur local, il suffit d'apporter quelques modifications mineures dans son fichier de configuration. Pour ceux ayant des besoins plus complexes, Postfix fournit un certain nombre d'options de configuration ainsi que des possibilités d'ajout de tiers, qui font de ce dernier un ATC non seulement riche en fonctionnalités mais également très versatile.

Les fichiers de configuration de Postfix are lisibles par tout un chacun et prennent en charge plus de 250 directives. Contrairement à Sendmail, aucun macro-traitement n'est nécessaire pour que les modifications prennent effet et la majorité des options les plus courremment utilisées sont décrites dans le fichier contenant de nombreux commentaires.

Important

Avant d'utiliser Postfix, il est nécessaire de changer l'ATC par défaut de Sendmail à Postfix. Reportez-vous au chapitre intitulé *Configuration de l'agent de transfert de courrier (ATC)* du *Guide d'administration système de Red Hat Enterprise Linux* pour obtenir de plus amples informations.

11.3.2.1. Installation de Postfix par défaut

L'exécutable de Postfix est `/usr/sbin/postfix`. Ce démon lance tous les processus connexes nécessaires pour traiter la livraison de courrier.

Postfix stocke ses fichiers de configuration dans le répertoire `/etc/postfix/`. Ci-après figure une liste des fichiers les plus courremment utilisés :

- `access` — Utilisé pour le contrôle d'accès, ce fichier spécifie les hôtes qui sont autorisés à se connecter à Postfix.
- `aliases` — Fournit une liste configurable requise par le protocole de messagerie.

- `main.cf` — Représente le fichier de configuration global de Postfix. La majorité des options de configuration sont spécifiées dans ce fichier.
- `master.cf` — Spécifie la manière selon laquelle Postfix interagit avec différents processus pour effectuer la livraison de courrier.
- `>transport` — Mappe les adresses de courrier électronique pour qu'elles prennent le relais des hôtes.

Important

Le fichier `/etc/postfix/main.cf` par défaut ne permet pas à Postfix d'accepter des connexions réseau venant d'un hôte autre que l'ordinateur local. Pour obtenir des informations sur la configuration de Postfix en tant que serveur pour d'autres clients, reportez-vous à la Section 11.3.2.2.

Lors de la modification de certaines options dans le répertoire `/etc/postfix/`, il sera peut-être nécessaire de redémarrer le service `postfix` afin que les modifications apportées prennent effet. Pour ce faire, la meilleure façon consiste à taper la commande suivante :

```
/sbin/service postfix restart
```

11.3.2.2. Configuration élémentaire de Postfix

Par défaut, Postfix n'accepte pas de connexions réseau venant d'un hôte autre que l'ordinateur local. Efeectuez les étapes suivantes en étant connecté en tant que super-utilisateur afin d'activer la livraison de courrier pour d'autres hôtes du réseau :

- Éditez le fichier `/etc/postfix/main.cf` à l'aide d'un éditeur de texte tel que `vi`.
- Décommentez la ligne `mydomain` en supprimant la symbole dièse (`#`) et remplacez *`domain.tld`* par le nom de domaine que le serveur de messagerie sert, tel que `example.com`.
- Décommentez la ligne `myorigin = $mydomain`.
- Décommentez la ligne `myhostname` et remplacez *`host.domain.tld`* par le nom d'hôte de l'ordinateur.
- Décommentez la ligne `mydestination = $myhostname, localhost.$mydomain`.
- Décommentez la ligne `mynetworks` et remplacez *`168.100.189.0/28`* par un paramètre de réseau valide pour les hôtes pouvant se connecter au serveur.
- Décommentez la ligne `inet_interfaces = all`.
- Redémarrez le service `postfix`.

Une fois ces étapes effectuées, l'hôte est en mesure d'accepter la livraison d'emails venant de l'extérieur

Postfix dispose d'une grande gamme d'options de configuration. Une des meilleures façons d'apprendre comment configurer Postfix consiste à lire les commentaires dans `/etc/postfix/main.cf`. Des ressources supplémentaires incluant des informations sur LDAP et l'intégration de SpamAssassin sont disponibles en ligne à l'adresse suivante : http://www.postfix.org/.

11.3.3. Fetchmail

Fetchmail est un ATC qui récupère du courrier électronique depuis des serveurs distants et le transfère à l'ATC local. De nombreux utilisateurs apprécient la possibilité de pouvoir séparer le processus de téléchargement de leurs messages stockés sur un serveur distant, du processus de lecture et d'organisation de leur courrier dans un AGC. Conçu tout spécialement pour les utilisateurs à accès par ligne commutée, Fetchmail se connecte et télécharge rapidement tous les messages électroniques dans le fichier spoule de messagerie à l'aide de nombreux protocoles différents parmi lesquels figurent POP3 et IMAP. Il permet même de réacheminer vos messages vers un serveur SMTP, si nécessaire.

Fetchmail est configuré pour chaque utilisateur grâce à un fichier `.fetchmailrc` du répertoire personnel de l'utilisateur.

Sur la base des préférences spécifiées dans le fichier `.fetchmailrc`, Fetchmail recherche les messages électroniques sur un serveur distant et les télécharge. Il les achemine ensuite sur le port 25 de l'ordinateur local, au moyen de l'ATC local, pour les placer dans le fichier spoule de l'utilisateur approprié. Si Procmail est disponible, il peut être utilisé pour filtrer les messages et les placer dans une boîte à lettres de sorte qu'ils puissent être lus avec par un AGC.

11.3.3.1. Options de configuration de Fetchmail

Bien qu'il soit possible de passer toutes les options nécessaires pour vérifier le courrier sur un serveur distant depuis la ligne de commande lors de l'exécution de Fetchmail, il est beaucoup plus simple d'utiliser un fichier `.fetchmailrc`. Insérez toutes les options de configuration souhaitées dans le fichier `.fetchmailrc` et ces options seront alors utilisées lors de chaque exécution de la commande `fetchmail`. Il est possible d'annuler toute option lors du lancement de Fetchmail en spécifiant l'option en question sur la ligne de commande.

Le fichier `.fetchmailrc` d'un utilisateur contient trois types d'options de configuration :

- *options globales* — Ce type d'options donne à Fetchmail des instructions qui contrôlent le fonctionnement du programme ou fournit des réglages pour toute connexion de vérification du courrier.
- *options serveur* — Ce type d'options spécifie les informations nécessaires concernant le serveur sondé, telles que le nom d'hôte ainsi que les préférences relatives aux serveurs de messagerie spécifiques, comme le port à vérifier ou le nombre de secondes devant s'écouler avant l'interruption de la connexion. Ces options affectent tout utilisateur employant ce serveur.
- *options utilisateur* — Ce type d'options contient des informations, telles que le nom d'utilisateur et le mot de passe, nécessaires pour l'authentification et la vérification du courrier à l'aide d'un serveur de messagerie donné.

Les options globales apparaissent en haut du fichier de configuration `.fetchmailrc`, suivies d'une ou plusieurs options serveur, précisant chacune un serveur de messagerie différent sur lequel Fetchmail devrait vérifier le courrier. Les options utilisateur suivent les options serveur pour chaque compte utilisateur devant être vérifié sur ce serveur de messagerie. Tout comme pour les options serveur, il est possible de spécifier non seulement de multiples options utilisateur à employer avec un serveur donné mais il est également possible de vérifier plusieurs comptes de messagerie sur un même serveur.

Les options serveur à utiliser sont appelées dans le fichier `.fetchmailrc` grâce à l'emploi d'un verbe d'option spécial, `poll` ou `skip`, qui précède toute information concernant le serveur. L'action `poll` indique à Fetchmail d'utiliser cette option serveur lorsqu'il est exécuté ; il vérifie en fait le courrier à l'aide des différentes options utilisateur. Toute option serveur placée après une action `skip` contourne les opérations de vérification, à moins que le nom d'hôte de ce serveur ne soit spécifié lorsque Fetchmail est invoqué. L'option `skip` est utile lors du test de configurations dans `.fetchmailrc` car elle vérifie les serveurs avec cette option uniquement lorsqu'ils sont invoqués spécifiquement et n'affecte pas les configurations actuelles.

Un exemple de fichier `.fetchmailrc` ressemble à l'extrait suivant :

```
set postmaster "user1"
```

```
set bouncemail

poll pop.domain.com proto pop3
     user 'user1' there with password 'secret' is user1 here

poll mail.domain2.com
     user 'user5' there with password 'secret2' is user1 here
     user 'user7' there with password 'secret3' is user1 here
```

Dans cet exemple, les options globales sont configurées de façon à ce que l'utilisateur reçoive le courrier seulement en dernier ressort (option `postmaster`) et que toutes les erreurs soient envoyées au maître de poste (ou postmaster) plutôt qu'à l'expéditeur (option `bouncemail`). L'action `set` indique à Fetchmail que cette ligne contient une option globale. Ensuite, deux serveurs de messagerie sont spécifiés ; le premier est configuré pour vérifier POP3 et le second pour essayer divers protocoles afin d'en trouver un qui fonctionne. Deux utilisateurs sont vérifiés dans le cas de la seconde option de serveur, mais tout message électronique trouvé pour l'un ou l'autre des utilisateurs est envoyé dans le fichier spoule de messagerie de l'utilisateur No. 1 (ou `user1`). Ainsi, il est possible de vérifier de multiples boîtes aux lettres sur plusieurs serveurs, tout en utilisant une une seule corbeille d'arrivée pour l'AGC. Toute information spécifique à chacun des utilisateurs commence par l'action `user`.

Remarque

Les utilisateurs ne doivent pas placer leur mot de passe dans le fichier `.fetchmailrc`. Si la section `with password '`*`<password>`*`'` est omise, Fetchmail demandera la saisie d'un mot de passe lors de son lancement.

Fetchmail offre de nombreuses options aussi bien globales que locales ou serveur. Beaucoup d'entre elles sont rarement utilisées ou ne s'appliquent qu'à des situations très particulières. La page de manuel de `fetchmail` explique chacune de ces options de façon détaillée, mais les options les plus courantes sont énumérées ci-dessous.

11.3.3.2. Options globales

Chaque option globale devrait être placée sur une seule ligne et précédée de l'action `set`.

- `daemon` *<seconds>* — Spécifie le mode démon où Fetchmail demeure en tâche de fond. Remplacez *<seconds>* par la durée en secondes pendant laquelle Fetchmail doit attendre avant de sonder le serveur.
- `postmaster` — Spécifie un utilisateur local auquel envoyer le courrier en cas de problèmes de distribution.
- `syslog` — Spécifie le fichier journal pour l'enregistrement des messages d'erreurs et d'état. La valeur `/var/log/maillog` est retenue par défaut.

11.3.3.3. Options serveur

Les options serveur doivent figurer sur leur propre ligne dans `.fetchmailrc`, après une action `poll` ou `skip`.

- `auth` *<auth-type>* — Remplacez *<auth-type>* par le type d'authentification à utiliser. Par défaut, l'authentification `password` est utilisée, mais certains protocoles prennent en charge d'autres types d'authentification, notamment `kerberos_v5`, `kerberos_v4` et `ssh`. Si le type

d'authentification `any` est retenu, Fetchmail essaiera d'abord des méthodes qui ne nécessitent aucun mot de passe, puis des méthodes qui masquent le mot de passe et, en dernier ressort, il essaiera d'envoyer le mot de passe en texte en clair pour effectuer l'authentification auprès du serveur.

- `interval <number>` — Indique à Fetchmail de sonder seulement le serveur spécifié après avoir vérifié le courrier sur tous les serveurs configurés un certain nombre de fois (où *<number>* représente ce nombre de fois). Cette option est généralement utilisée pour les serveurs de messagerie sur lesquels un utilisateur ne reçoit que rarement des messages.
- `port <port-number>` — Remplacez *<port-number>* par le numéro du port. Cette valeur annule le numéro du port par défaut pour un protocole spécifié.
- `proto <protocol>` — Remplacez *<protocol>* par le protocole, tel que `pop3` ou `imap`, devant être utilisé pour vérifier le courrier sur le serveur.
- `timeout <seconds>` — Remplacez *<seconds>* par la durée d'inactivité du serveur (exprimée en secondes) après laquelle Fetchmail abandonne une tentative de connexion. Si cette valeur n'est pas configurée, le système retient une valeur par défaut de `300` secondes.

11.3.3.4. Options utilisateur

Les options utilisateur peuvent être placées sur leurs propres lignes sous une option serveur ou alors sur la même ligne que l'option de serveur. Dans les deux cas, les options définies doivent suivre l'option `user` (définie ci-dessous).

- `fetchall` — Donne l'ordre à Fetchmail de télécharger tous les messages de la file d'attente, y compris les messages qui ont déjà été visualisés. Par défaut, Fetchmail ne récupère que les nouveaux messages.
- `fetchlimit <number>` — Remplacez *<number>* par le nombre de messages à extraire avant de s'arrêter.
- `flush` — Donne l'instruction à Fetchmail de supprimer tous les messages de la file d'attente qui ont été lus précédemment avant d'extraire les nouveaux messages.
- `limit <max-number-bytes>` — Remplacez *<max-number-bytes>* par la taille maximales en octets autorisée pour des messages lors de leur extraction. Cette option est pratique lors de connexions réseau lentes, particulièrement lorsqu'un gros message prend trop de temps à être télécharger.
- `password '<password>'` — Remplacez *<password>* par le mot de passe de l'utilisateur.
- `preconnect "<command>"` — Remplacez *<command>* par une commande à exécuter avant de récupérer les messages pour cet utilisateur.
- `postconnect "<command>"` — Remplacez *<command>* par une commande à exécuter après avoir récupéré les messages pour cet utilisateur.
- `ssl` — Active le cryptage SSL.
- `user "<username>"` — Remplacez *<username>* par le nom d'utilisateur employé par Fetchmail pour récupérer les messages électroniques. *Cette option doit être placée avant toute autre option utilisateur.*

11.3.3.5. Options de commande pour Fetchmail

La plupart des options utilisées en ligne de commande lors de l'exécution de la commande `fetchmail`, répliquent les options de configuration de `.fetchmailrc`. Ainsi, Fetchmail peut être utilisé avec ou sans fichier de configuration. Ces options ne sont pas utilisées en ligne de commande par la plupart des utilisateurs car il est plus simple de les laisser dans le fichier `.fetchmailrc`.

Toutefois, il se peut que dans certaines situations la commande `fetchmail` doive être exécutée avec d'autres options dans un but bien précis. Il est possible d'exécuter des options de commande afin d'annuler temporairement un paramètre de `.fetchmailrc` qui crée une erreur étant donné que toute option spécifiée à la ligne de commande annule les options contenues dans le fichiers de configuration.

11.3.3.6. Options d'information ou de débogage

Certaines options utilisées après la commande `fetchmail` permettent d'obtenir des informations importantes.

- `--configdump` — Affiche toutes les options possibles sur la base des informations fournies pas `.fetchmailrc` et les valeurs par défaut de Fetchmail. Lors de l'utilisation de cette option, aucun message électronique n'est téléchargé pour quelque utulisateur que ce soit.
- `-s` — Exécute Fetchmail en mode silencieux, empêchant tout message, autre que des messages d'erreurs, d'apparaître après la commande `fetchmail`.
- `-v` — Exécute Fetchmail en mode prolixe, affichant toute communication entre Fetchmail et les serveurs de messagerie distants.
- `-V` — Affiche des informations détaillées sur la version utilisée, dresse la liste de ses options globales et fournit les paramètres à employer pour chaque utilisateur, y compris le protocole de messagerie et la méthode d'authentification. Lors de l'utilisation de cette option, aucun courrier électronique n'est récupéré pour quelque utilisateur que ce soit.

11.3.3.7. Options spéciales

Ces options peuvent parfois être pratiques pour annuler les valeurs par défaut qui se trouvent souvent dans le fichier `.fetchmailrc`.

- `-a`— Indique à Fetchmail de télécharger tous les messages depuis le serveur de messagerie distant, qu'ils soient nouveaux ou qu'ils aient déjà été consultés. Par défaut, Fetchmail ne télécharge que les nouveaux messages.
- `-k` — Fetchmail laisse les messages sur le serveur de messagerie distant après les avoir téléchargés. Cette option annule le comportement par défaut consistant à supprimer les messages après les avoir téléchargés.
- `-l` <*`max-number-bytes`*> — Fetchmail ne télécharge pas les messages dont la taille est supérieure à la taille spécifiée et les laisse sur le serveur de messagerie distant.
- `--quit` — Quitte le processus du démon Fetchmail.

D'autres commandes et options `.fetchmailrc` sont offertes dans la page de manuel de `fetchmail`.

11.4. Agent de distribution de courrier (ADC)

Red Hat Enterprise Linux inclut deux ADC principaux, à savoir Procmail et `mail`. Ces deux applications sont considérées comme des agents de distribution locaux (ou ADL) et elles acheminent toutes les deux le courrier électronique du fichier spoule d'un ADC vers la boîte aux lettres de l'utilisateur. Toutefois, Procmail fournit un système de filtrage robuste.

Cette section examine seulement Procmail de façon détaillée. Pour toute information sur la commande `mail`, consultez la page de manuel qui lui est dédié.

Procmail distribue et filtre le courrier électronique dès qu'il est placé dans le fichier spoule de messagerie de l'hôte local. Il est puissant, peu exigeant en matière de ressources système et d'une utilisation courante. Procmail peut jouer un rôle critique dans la distribution du courrier qui sera lu par les applications client de messagerie.

Il existe différentes façons d'invoquer Procmail. Dès qu'un ATC dépose un message dans le fichier spoule de messagerie, Procmail est lancé. Ce dernier filtre et classe alors le message de manière à ce que l'AGC puisse le trouver puis quitte le processus. L'AGC peut également être configuré de sorte qu'il exécute Procmail chaque fois qu'un message est reçu afin que le courrier soit acheminé vers les boîtes aux lettres appropriées. Par défaut, la présence d'un fichier `/etc/procmailrc` ou d'un fichier `.procmailrc` (aussi appelé un fichier *rc*) dans le répertoire personnel d'un utilisateur invoquera Procmail dès qu'un ATC reçoit un nouveau message.

Toute action effectuée par Procmail sur un message électronique dépend de la capacité du message à satisfaire un ensemble de conditions ou *recettes* (aussi appelées recipes selon le terme anglais) particulières contenues dans le fichier `rc`. Si un message satisfait une recette, il peut alors être placé dans un fichier donné, être supprimé ou être traité d'une autre façon.

Lors du démarrage de Procmail, ce dernier lit les messages électroniques et sépare les informations relatives au corps du message de celles concernant l'en-tête. Ensuite, Procmail cherche les fichiers `/etc/procmailrc` et `rc` dans le répertoire `/etc/procmailrcs` pour trouver les variables d'environnement et recettes de Procmail s'appliquant par défaut à l'ensemble du système. Procmail cherche ensuite un fichier `.procmailrc` dans le répertoire personnel de l'utilisateur. De nombreux utilisateurs créent des fichiers `rc` supplémentaires pour Procmail, qui sont référencés dans leur fichier `.procmailrc` présent dans leur répertoire personnel.

Par défaut, aucun fichier `rc` s'appliquant à l'ensemble du système n'existe dans le répertoire `/etc` et aucun fichier `.procmailrc` n'existe dans le répertoire personnel de quelque utilisateur que ce soit. Par conséquent, pour utiliser Procmail, chaque utilisateur doit créer un fichier `.procmailrc` contenant des variables d'environnement et des règles spécifiques.

11.4.1. Configuration de Procmail

Les fichiers de configuration de Procmail contiennent des variables d'environnement importantes. Ces dernières précisent à Procmail les messages spécifiques devant être triés et le sort des messages qui ne satisfont aucune recette.

Ces variables d'environnement qui se trouvent généralement au début du fichier `.procmailrc` ont le format suivant :

```
<env-variable>="<value>"
```

Dans cet exemple, *<env-variable>* correspond au nom de la variable alors que l'élément *<value>* définit la variable elle-même.

La plupart des utilisateurs de Procmail De nombreuses n'utilisent pas de nombreuses variables d'environnement mais les plus importantes sont déjà définies par une valeur par défaut. La plupart du temps, les variables suivantes sont utilisées :

- `DEFAULT` — Définit la boîte aux lettres où seront placés les messages qui ne satisfont aucune recette.

  La valeur par défaut de `DEFAULT` est la même que `$ORGMAIL`.

- `INCLUDERC` — Spécifie des fichiers `rc` supplémentaires qui contiennent d'autres recettes que les messages doivent satisfaire. Ceci permet de diviser les listes de recettes Procmail en fichiers individuels qui jouent différents rôles, tels que le blocage de spams et la gestion de listes d'adresses électroniques, qui peuvent ensuite être activés ou désactivés à l'aide de caractères de commentaire dans le fichier `.procmailrc` de l'utilisateur.

Par exemple, des lignes présentes dans un fichier `.procmailrc` de l'utilisateur peuvent ressembler à l'extrait suivant :

```
MAILDIR=$HOME/Msgs
INCLUDERC=$MAILDIR/lists.rc
INCLUDERC=$MAILDIR/spam.rc
```

Si l'utilisateur souhaite désactiver le filtrage par Procmail de ses listes d'adresses, mais désire garder le contrôle du pourriel, il n'a qu'à commenter la première ligne `INCLUDERC` avec le symbole dièse (#).

- `LOCKSLEEP` — Définit la durée, en secondes, s'écoulant entre les tentatives de Procmail d'utiliser un fichier de verrouillage spécifique. La valeur par défaut est de huit secondes.
- `LOCKTIMEOUT` — Définit la durée, en secondes, qui doit s'écouler après la dernière modification d'un fichier de verrouillage avant que Procmail ne considère le fichier de verrouillage comme étant vieux et pouvant par conséquent être supprimé. La valeur par défaut est de 1024 secondes.
- `LOGFILE` — Représente le fichier dans lequel toutes les informations de Procmail ou tous les messages d'erreurs sont enregistrés.
- `MAILDIR` — Définit le répertoire de travail courant pour Procmail. Si cete variable est déterminée, tous les autres chemins d'accès vers Procmail sont relatifs à ce répertoire.
- `ORGMAIL` — Spécifie la boîte aux lettres originale ou un autre endroit où placer les messages s'ils ne peuvent être placés à l'emplacement par défaut ou à celui exigé par les recettes.

  Par défaut, une valeur de `/var/spool/mail/$LOGNAME` est utilisée.
- `SUSPEND` — Définit la durée, en secondes, pendant laquelle Procmail s'arrête si une ressource nécessaire, telle que l'espace swap, n'est pas disponible.
- `SWITCHRC` — Permet à un utilisateur de spécifier un fichier externe contenant des recettes Procmail supplémentaires, plus ou moins comme le fait l'option `INCLUDERC`, sauf que la vérification des recettes est arrêtée sur le fichier de configuration traitant et que seules les recettes du fichier spécifié avec `SWITCHRC` sont utilisées.
- `VERBOSE` — Fait en sorte que Procmail journalise davantage d'informations. Cette option est pratique pour le débogage.

D'autres variables d'environnement importantes sont obtenues depuis le shell, comme `LOGNAME`, qui est le nom de connexion ; `HOME`, qui est l'emplacement du répertoire personnel ; et `SHELL`, qui est le shell par défaut.

Consultez la page de manuel de `procmailrc` pour obtenir des explications exhaustives sur les variables d'environnement ainsi que sur leurs valeurs par défaut.

11.4.2. Recettes Procmail

Les nouveaux utilisateurs trouvent généralement que les recettes constituent l'élément le plus difficile de l'apprentissage de l'utilisation de Procmail. Ce sentiment est compréhensible jusqu'à un certain point, étant donné que les recettes effectuent la comparaison avec les messages à l'aide d'*expressions régulières*, qui est un format spécifique utilisé pour spécifier des qualifications de concordance de chaînes. Ceci étant, les expressions régulières ne sont pas très difficiles à créer et sont encore moins difficiles à comprendre en les lisant. De plus, la cohérence avec laquelle les recettes Procmail sont écrites, sans tenir compte des expressions régulières, permet d'acquérir de bonnes connaissances facilement, simplement en examinant les exemples. Pour consulter des exemples de recette Procmail, reportez-vous à la Section 11.4.2.5.

Les recettes Procmail se présentent sous la forme suivante :

```
:0<flags>: <lockfile-name>
```

```
* <special-condition-character> <condition-1>
* <special-condition-character> <condition-2>
* <special-condition-character> <condition-N>

<special-action-character><action-to-perform>
```

Les deux premiers caractères d'une recette Procmail sont le symbole des deux-points et un zéro. Divers indicateurs (ou flags) peuvent être placés après le zéro pour contrôler la manière selon laquelle Procmail traite la recette. Le symbole des deux-points placé après la section *<flags>* spécifie qu'un fichier de verrouillage (lockfile) sera créé pour ce message. Si un fichier de verrouillage est créé, le nom peut être spécifié dans l'espace *<lockfile-name>*.

Une recette peut contenir plusieurs conditions servant à vérifier la concordance d'un message. S'il aucune condition n'est spécifiée, tous les messages auront une concordance positive avec la recette. Les expressions régulières sont placées dans certaines conditions de façon à faciliter la concordance avec les messages. Si des conditions multiples sont utilisées, elles doivent toutes obtenir la concordance pour que l'action soit exécutée. Les conditions sont vérifiées sur la base des indicateurs spécifiés dans la première ligne de la recette. Des caractères spéciaux facultatifs placés après le caractère `*` permettent de contrôler ultérieurement la condition.

L'option *<action-to-perform>* spécifie l'action exécutée lorsque le message correspond à l'une des conditions. Il ne peut y avoir qu'une action par recette. Dans de nombreux cas, le nom d'une boîte aux lettres est utilisé ici pour envoyer dans ce fichier les messages satisfaisant les conditions, permettant ainsi de trier le courrier. Des caractères d'action spéciaux peuvent également être utilisés avant que l'action ne soit spécifiée. Reportez-vous à la Section 11.4.2.4 pour obtenir de plus amples informations.

11.4.2.1. Recettes de distribution et de non-distribution

L'action utilisée si la recette correspond à un message donné détermine si cette dernière est considérée comme étant une recette de *distribution* ou de *non-distribution*. Une recette de distribution contient une action qui écrit le message dans un fichier, envoie le message à un autre programme ou réachemine le message vers une autre adresse électronique. Une recette de non-distribution couvre toutes les autres actions, telles que l'utilisation d'un *bloc d'imbrication* (également appelé nesting block). Un bloc d'imbrication est un ensemble d'actions contenues entre deux accolades, `{ }`, qui sont exécutées sur des messages satisfaisant les conditions de la recette. Les blocs d'imbrication peuvent être emboîtés les uns dans les autres, offrant ainsi plus de contrôle pour l'identification et l'exécution d'actions sur des messages.

Lorsque des messages satisfont une recette de distribution, Procmail effectue l'action spécifiée et arrête de comparer le message à toute autre recette. Les messages qui satisfont les recettes de non-distribution continuent eux à être comparés aux autres recettes.

11.4.2.2. Indicateurs

Les indicateurs (ou flags) sont très importants pour déterminer la façon dont les conditions d'une recette sont comparées à un message. Les indicateurs suivants sont couramment utilisés :

- `A` — Spécifie que cette recette n'est utilisée que si la recette précédente sans indicateur `A` ou `a` a également obtenu la concordance avec ce message.
- `a` — Spécifie que cette recette n'est utilisée que si la recette précédente sans indicateur `A` ou `a` a également obtenu la concordance avec ce message *et* a été exécutée avec succès.
- `B` — Analyse le corps du message et recherche des conditions de concordance.
- `b` — Utilise le corps du message dans toute action découlant de cet indicateur, comme l'écriture du message dans un fichier ou son réacheminement. Il s'agit du comportement par défaut.

- `c` — Génère une copie conforme du message électronique. Cette option peut être utile avec les recettes de distribution, étant donné que l'action requise peut être exécutée sur le message et que la copie du message peut continuer à être traitée dans les fichiers `rc`.
- `D` — Rend la comparaison `egrep` sensible à la casse. Par défaut, le processus de comparaison n'est pas sensible à la casse.
- `E` — Semblable à l'indicateur `A` sauf que les conditions dans cette recette sont comparées à un message seulement si la recette précédant immédiatement la recentte sans indicateur `E` n'a pas obtenu la concordance. Cette action ressemble à une action *else*.
- `e` — Établit la comparaison de la recette au message seulement si l'action spécifiée dans la recette présente juste avant échoue.
- `f` — Utilise le tube (aussi appelé pipe) comme filtre.
- `H` — Analyse l'en-tête du message et recherche des conditions de concordance. Cette situation se produit par défaut.
- `h` — Utilise l'en-tête dans une action découlant de cet indicateur. Ce dernier représente le comportement par défaut.
- `w` — Indique à Procmail d'attendre que le filtre ou le programme spécifiés aient terminé leurs opérations et rapporte si l'opération précédente a réussi ou échoué, avant de considérer le message comme étant filtré.
- `W` — Identique à `w` sauf que les messages de type "Échec du programme" (ou Program failure) sont supprimés.

Pour obtenir une liste détaillée d'indicateurs supplémentaires, reportez-vous à la page de manuel de `procmailrc`.

11.4.2.3. Spécification d'un fichier de verrouillage local

Les fichiers de verrouillage sont très utiles avec Procmail pour garantir que seul un processus essaie de modifier un certain message à un moment donné. Il est possible de spécifier un fichier de verrouillage local en plaçant le symbole des deux points (`:`) après tout indicateur dans la première ligne d'une recette. Ce faisant, un fichier de verrouillage local est créé en fonction du nom de fichier de destination et de toute valeur contenue dans la variable d'environnement globale `LOCKEXT`.

Vous pouvez aussi spécifier le nom du fichier de verrouillage local à utiliser avec cette recette après le symbole des deux points (:).

11.4.2.4. Conditions et actions spéciales

Des caractères spéciaux utilisés avant les conditions de recettes et et avant les actions de Procmail modifient la façon selon aquelle elles sont interprétées.

Les caractères suivants peuvent être utilisés après le symbole `*` au début de la ligne de condition d'une recette :

- `!` — Placé dans la ligne de condition, ce caractère inverse la condition, de sorte que la concordance sera désormais établie seulement si la condition ne satisfait pas le message.
- `<` — Vérifie si la taille du message est inférieure à un nombre d'octets spécifié.
- `>` — Vérifie si la taille du message est supérieure à un nombre d'octets spécifié.

Les caractères suivants sont utilisés pour exécuter des actions spéciales :

- `!` — Placé dans la ligne d'action, ce caractère indique à Procmail de réacheminer le message vers les adresses électroniques spécifiées.
- `$` — Renvoie à une variable définie précédemment dans le fichier `rc`. Cette option est généralement utilisée pour définir une boîte aux lettres commune à laquelle diverses recettes feront référence.
- `|` — Démarre un programme spécifié afin qu'il traite le message.
- `{` and `}` — Construit un bloc d'imbrication, utilisé pour contenir des recettes supplémentaires devant être appliquer aux messages satisfaisant les conditions.

Si aucun caractère spécial n'est utilisé au début de la ligne d'action, Procmail considère que la ligne d'action spécifie la boîte aux lettres où les messages doivent être déposés.

11.4.2.5. Exemples de recettes

Procmail est certes un programme extrêmement flexible, mais en raison de cette flexibilité, la création d'une recette Procmail de toutes pièces peut être une tâche difficile pour de nouveaux utilisateurs.

Le meilleure façon de développer les capacités nécessaires pour créer les conditions des recettes Procmail consiste à bien comprendre la notion d'expressions régulières et à examiner de nombreux exemples élaborés par d'autres. Une explication exhaustive des expressions régulières va au-delà de la portée de cette section. La structure des recettes Procmail ainsi que des exemples de recettes Procmail sont disponibles à différents endroits sur Internet (notamment à l'adresse suivante : http://www.iki.fi/era/procmail/links.html). En examinant ces exemples de recettes, il est possible d'acquérir des connaissances solides sur la bonne utilisation et sur l'adaptation des expressions régulières. En outre, des informations élémentaires sur des règles d'expressions régulières de base se trouvent dans la page de manuel de `grep`.

Les simples exemples reproduits ci-dessous illustrent la structure 'élémentaire de recettes Procmail et peuvent servir de base pour des conceptions plus élaborées.

Une recette élémentaire ne contient pas forcément de conditions, comme le montre l'exemple ci-dessous :

```
:0:
new-mail.spool
```

La première ligne spécifie qu'un fichier de verrouillage local doit être créé, mais n'indique aucun nom. Procmail utilise donc le nom du fichier de destination et y ajoute la valeur spécifiée dans la variable d'environnement `LOCKEXT`. Étant donné qu'aucune condition n'est spécifiée, tous les messages satisfont cette recette et sont par conséquent placés dans le fichier spoule unique appelé `new-mail.spool` qui se trouve dans le répertoire spécifié par la variable d'environnement `MAILDIR`. Un AGC peut ensuite visualiser les messages dans ce fichier.

Une recette de base, telle que celle-ci, peut être placée à la fin de tous les fichiers `rc` afin que les messages soient acheminés vers un emplacement par défaut.

L'exemple ci-dessous illustre l'etablissement de la concordance avec des messages d'une adresse électronique spécifique et le dépôt de ces derniers dans la corbeille.

```
:0
* ^From: spammer@domain.com
/dev/null
```

Dans cet exemple, tout message envoyé par `spammer@domain.com` est acheminé vers le périphérique`/dev/null` où il est supprimé.

Avertissement

Assurez-vous que les règles fonctionnent bien comme vous le désirez avant d'acheminer les messages concernés vers `/dev/null` afin qu'ils soient supprimés de façon permanente. Si les conditions de votre recette retiennent accidentellement des messages qui ne devraient pas l'être et qu'ils disparaissent sans laisser de trace, il est alors difficile de résoudre tout problème lié à la règle.

Une solution plus appropriée consiste à pointer l'action de la recette vers une boîte aux lettres spéciale qui peut être vérifiée de temps en temps, afin de voir si elle contient de fausses concordances. Une fois convaincu qu'aucun message ne fait l'objet d'une concordance accidentelle, supprimez la boîte aux lettres et établissez l'action de façon à ce qu'elle envoie les messages vers `/dev/null`.

La recette ci-dessous retient les messages envoyés depuis une liste de diffusion spécifique et les place dans un dossier déterminé.

```
:0:
* ^(From|CC|To).*tux-lug
tuxlug
```

Tout message envoyé depuis la liste de diffusion `tux-lug@domain.com` est automatiquement placé dans la boîte aux lettres `tuxlug` pour le AGC. Notez que la condition dans cet exemple a une concordance avec le message si l'adresse électronique de la liste de diffusion se trouve sur l'une des lignes suivantes : `From` (De), `CC` ou `To` (À).

Pour obtenir des informations sur des recettes plus détaillées et plus puissantes, consultez l'une des nombreuses ressources disponibles dans la Section 11.6.

11.4.2.6. Filtres de spam

Puisque Procmail est appelé par Sendmail, Postfix et Fetchmail lors de la réception de nouveaux messages, il peut être utilisé comme un outil puissant pour combattre le pourriel.

Le combat contre le pourriel est encore plus efficace lorsque Procmail est utilisé de concert avec SpamAssassin. En effet, grâce à une double action ces deux applications peuvent rapidement identifier des messages-pourriel, les trier et les détruire.

SpamAssassin recours à une analyse de l'en-tête et du texte, à des listes noires et à des bases de données de localisation de spam ainsi qu'à une analyse bayesienne auto-organisatrice de pourriel pour identifier et étiqueter rapidement et précisément tout pourriel (aussi appelé spam).

Pour un utilisateur local, la meilleure façon d'utiliser SpamAssassin consiste à insérer la ligne suivante vers le haut du fichier `~/.procmailrc` :

```
INCLUDERC=/etc/mail/spamassassin/spamassassin-default.rc
```

Le programme `/etc/mail/spamassassin/spamassassin-default.rc` contient une simple règle Procmail permettant d'activer SpamAssassin pour tout courrier électronique reçu. Si un message est reconnu comme étant un pourriel, il est étiqueté en tant que tel dans l'en-tête et la mention suivante est ajoutée au sujet :

```
*****SPAM*****
```

Le corps du message de l'email est précédé d'un compte-rendu des éléments ayant justifié le diagnostic de spam.

Pour classer les emails étiquetés en tant que pourriel, il est possible d'utiliser une règle semblable à celle reproduite ci-dessous :

```
:0 Hw
```

```
* ^X-Spam-Status: Yes
spam
```

Selon cette règle, tous les messages étiquetés en tant que spam dans l'en-tête sont rangés dans une boîte aux lettres nommée `spam`.

Étant donné que SpamAssassin est un script Perl, il sera peut-être nécessaire d'utiliser le démon binaire SpamAssassin (`spamd`) et l'application client (`spamc`) sur des serveurs très sollicités. Pour configurer SpamAssassin de la sorte, il est nécessaire d'avoir un accès super-utilisateur à l'hôte.

Pour lancer le démon `spamd`, tapez la commande suivante en étant connecté en tant que super-utilisateur (ou root) :

```
/sbin/service spamassassin start
```

Pour lancer le démon SpamAssassin lors du démarrage du système, utilisez un utilitaire initscript, comme l'**Outil de configuration des services** (`system-config-services`), pour activer le service `spamassassin`. Reportez-vous à la Section 1.4.2 pour obtenir de plus amples informations sur les utilitaires initscript.

Pour configurer Procmail afin qu'il utilise l'application client SpamAssassin au lieu du script Perl, placez le ligne suivante vers le haut du fichier `~/.procmailrc`. Pour une configuration s'appliquant à tout le système, placez cette dernière dans `/etc/procmailrc` :

```
INCLUDERC=/etc/mail/spamassassin/spamassassin-spamc.rc
```

11.5. Agent de gestion de courrier (AGC)

De nombreux progammes de messagerie sont disponibles sous Red Hat Enterprise Linux. Ce sont des programmes clients de messagerie graphiques et riches en fonctionnalités, tels que **Mozilla Mail** ou **Ximian Evolution**, ainsi que des programmes de messagerie basés sur du texte tel que **mutt**.

Pour obtenir des informations sur l'utilisation de ces applications, reportez-vous au chapitre intitulé *Applications de messagerie* du *Guide étape par étape de Red Hat Enterprise Linux*.

Le reste de cette section se concentre sur l'établissement d'une communication sécurisée entre le client et le serveur.

11.5.1. Établissement d'une communication sécurisée

Parmi les AGC très utilisés fournis avec Red Hat Enterprise Linux figurent **Mozilla Mail**, **Ximian Evolution** et `mutt` qui offrent des sessions de messagerie cryptées avec SSL.

Comme pour tout autre service voyageant sur un réseau non-crypté, des informations de messagerie importantes comme les noms d'utilisateur, mots de passe voire des messages entiers, peuvent être interceptées et lues par des utilisateurs du réseau. En outre, étant donné que les protocoles POP et IMAP standard transfèrent les informations d'authentification en texte clair, un pirate peut obtenir l'accès aux comptes utilisateur en recueillant les noms d'utilisateur et mots de passe lors de leur transfert sur le réseau.

11.5.1.1. Clients de messagerie sécurisés

La plupart des AGC Linux conçus pour vérifier le courrier sur des serveurs distants prennent en charge le cryptage SSL. Afin d'utiliser SSL lors de la récupération de courrier, son activation est nécessaire aussi bien sur le client de messagerie que sur le serveur de messagerie.

L'activation de SSL du côté client est une opération simple, il suffit même parfois de cliquer sur un bouton dans la fenêtre de configuration de l'AGC ou de l'activer au moyen d'une option dans le fichier de configuration de l'AGC. IMAP et POP sécurisés ont des numéros de port connus (respectivement 993 et 995) que l'AGC utilise pour authentifier et télécharger les messages.

11.5.1.2. Établissement de communications sécurisées pour les clients de messagerie

L'utilisation du système de cryptage SSL pour les utilisateur d'IMAP et POP sur le serveur de messagerie est une opération relativement simple.

Créez tout d'abord un certificat SSL. Pour ce faire, il existe deux possibilités : vous pouvez faire la demande d'un certificat SSL auprès d'une *Autorité de certification* (*AC*) ou vous pouvez créer vous-même un certificat auto-signé.

Avertissement

Les certificats auto-signés ne devraient être utilisés qu'a des fins de test. Tout serveur utilisé dans un environnement de production devrait avoir recours à un certificat obtenu auprès d'une AC.

Pour créer un certificat SSL auto-signé pour IMAP, allez dans le répertoire `/usr/share/ssl/certs/` et saisissez les commandes suivantes en étant connecté en tant que super-utilisateur :

```
rm -f imapd.pem
make imapd.pem
```

Pour achever le processus de création du certificat, répondez à toutes les questions.

Afin de créer un certificat SSL auto-signé pour for POP, allez dans le répertoire `/usr/share/ssl/certs/` et saisissez les commandes suivantes en étant connecté en tant que super-utilisateur :

```
rm -f ipop3d.pem
make ipop3d.pem
```

Ici encore, répondez à toutes les questions afin d'achever le processus de création du certificat.

Important

Assurez-vous de bien supprimer les fichiers `imapd.pem` et `ipop3d.pem` par défaut avant d'exécuter chaque commande `make`.

Une fois terminé, exécutez la commande `/sbin/service xinetd restart` pour redémarrer le démon `xinetd` qui contrôle `imapd` et `ipop3d`.

Il est également possible d'utiliser la commande `stunnel` en tant qu'enveloppeur de cryptage SSL placé autour des démons non-sécurisés standard `imapd` ou `pop3d`.

Le programme `stunnel` utilise des bibliothèques OpenSSL externes fournies avec Red Hat Enterprise Linux pour offrir un cryptage fort et pour protéger les connexions. Il est recommandé de faire une demande de certificat SSL auprès d'une autorité de certification (AC), mails il est également possible de créer un certificat auto-signé.

Pour créer un certificat SSL auto-signé, allez dans le répertoire `/usr/share/ssl/certs/` et tapez la commande suivante :

```
make stunnel.pem
```

Ici encore, répondez à toutes les questions afin d'achever le processus de création du certificat.

Une fois le certificat créé, il est possible d'utiliser la commande `stunnel` pour démarrer le démon `imapd` à l'aide de la commande suivante :

```
/usr/sbin/stunnel -d 993 -l /usr/sbin/imapd imapd
```

Après l'exécution de cette commande, il est possible d'ouvrir un client de messagerie IMAP et d'établir une connexion au serveur de messagerie utilisant le système de cryptage SSL.

Pour lancer `pop3d` à l'aide de la commande `stunnel`, tapez la commande suivante :

```
/usr/sbin/stunnel -d 995 -l /usr/sbin/pop3d pop3d
```

Pour obtenir de plus amples informations sur la façon d'utiliser `stunnel`, lisez la page de manuel de `stunnel` ou consultez les documents présents dans le répertoire `/usr/share/doc/stunnel-<numéro- version>/`, où *<version-number>* correspond au numéro de version de `stunnel`.

11.6. Ressources supplémentaires

Ci-dessous figure une liste de la documentation supplémentaire relative aux applications de messagerie.

11.6.1. Documentation installée

- Les paquetages `sendmail` and `sendmail-cf` contiennent des informations sur la manière de configurer Sendmail.
  - `/usr/share/doc/sendmail/README.cf` — Contient entre autres des informations sur `m4`, sur les emplacements des fichiers pour Sendmail, sur les boîtes de messagerie prises en charge et sur les façons d'accéder à des fonctionnalités avancées.

  En outre, les pages de manuel de `sendmail` et `aliases` contiennent des informations utiles sur les différentes options de Sendmail et sur la configuration adéquate du fichier Sendmail, `/etc/mail/aliases`.
- `/usr/share/doc/postfix-<version-number>` — Contient de nombreuses informations sur la manière de configurer Postfix. Remplacez *<version-number>* par le numéro de version de Postfix.
- `/usr/share/doc/fetchmail-<version-number>` — Contient une liste complète des fonctions Fetchmail dans le fichier `FEATURES` et un document `FAQ` d'introduction. Remplacez *<version-number>* par le numéro de version de Fetchmail.
- `/usr/share/doc/procmail-<version-number>` — Contient un fichier `README` qui offre un aperçu de Procmail, un fichier `FEATURES` qui explore toutes les fonctions du programme et un fichier `FAQ` qui offre les réponses à de nombreuses questions de configuration courantes. Remplacez *<version-number>* par le numéro de version de Procmail.

  Lors de l'apprentissage de la manière selon laquelle Procmail fonctionne et de la façon de créer de nouvelles recettes, les pages de manuel suivantes sont d'une aide très précieuses :

- `procmail` — Offre un aperçu du fonctionnement de Procmail et des étapes de filtrage du courrier.
- `procmailrc` — Explique le format de fichier `rc` utilisé pour créer des recettes.
- `procmailex` — Donne des exemples pratiques utiles de recettes Procmail.
- `procmailsc` — Explique la technique de weighted scoring utilisée par Procmail pour vérifier s'il y a concordance entre une recette donnée et un message.
- `/usr/share/doc/spamassassin-<version-number>/` — Contient de nombreuses informations sur SpamAssassin. Remplacez *<version-number>* par le numéro de version du paquetage `spamassassin`.

11.6.2. Sites Web utiles

- http://www.redhat.com/mirrors/LDP/HOWTO/Mail-Administrator-HOWTO.html — Fournit un aperçu du fonctionnement du courrier électronique et examine les solutions et configurations possibles de messagerie électronique, tant du côté serveur que client.
- http://www.redhat.com/mirrors/LDP/HOWTO/Mail-User-HOWTO/ — Examine le courrier électronique du point de vue de l'utilisateur, analyse diverses applications client de messagerie très utilisées et offre une introduction sur des sujets variés, tels que les alias, le réacheminement, la réponse automatique, les listes d'adresses, les filtres de courrier et le pourriel.
- http://www.redhat.com/mirrors/LDP/HOWTO/mini/Secure-POP+SSH.html — Explique une façon de télécharger du courrier POP en utilisant SSH avec le réacheminement de port, afin que les mots de passe et les messages soient transférés de manière sécurisée.
- http://www.sendmail.net/ — Contient des informations récentes, entrevues et articles relatifs à Sendmail, notamment un aperçu détaillé des nombreuses options disponibles.
- http://www.sendmail.org/ — Offre une explication technique très détaillée des fonctions de Sendmail et des exemples de configuration.
- http://www.postfix.org/ — Représente la page d'accueil du projet Postfix contenant de nombreuses informations sur Postfix. La liste de diffusion représente une excellente source d'informations.
- http://catb.org/~esr/fetchmail/ — Représente la page d'accueil de Fetchmail, comprenant un manuel en ligne et un forum aux questions (FAQ) complet.
- http://www.procmail.org/ — Représente la page d'accueil de Procmail, avec des liens menant à diverses listes d'adresses de participants dédiées à Procmail, de même que de nombreux documents FAQ.
- http://www.ling.helsinki.fi/users/reriksso/procmail/mini-faq.html — Constitue un excellent FAQ sur Procmail, offrant des conseils en matière de résolution de problèmes, des informations sur le verrouillage de fichiers et l'utilisation de caractères génériques (aussi appelés wildcards).
- http://www.uwasa.fi/~ts/info/proctips.html — Contient de nombreux conseils rendant l'utilisation de Procmail plus aisée. Ce site inclut des instructions sur la manière de tester les fichiers `.procmailrc` et d'utiliser le marquage de Procmail pour décider si une action donnée doit être exécutée ou non.
- http://www.spamassassin.org/ — Représente le site officiel du projet SpamAssassin.

11.6.3. Livres sur le sujet

- *Sendmail* de Bryan Costales avec Eric Allman et al ; O'Reilly & Associates — Une bonne référence pour Sendmail, écrite avec l'aide du créateur original de Delivermail et Sendmail.
- *Removing the Spam : Email Processing and Filtering* de Geoff Mulligan ; Addison-Wesley Publishing Company — Un livre examinant les diverses méthodes utilisées par les administrateurs de messagerie ayant recours à des outils établis, tels que Sendmail et Procmail, pour gérer les problèmes causés par le pourriel.
- *Internet Email Protocols : A Developer's Guide* de Kevin Johnson ; Addison-Wesley Publishing Company — Un recueil d'informations détaillées sur les principaux protocoles de messagerie et la sécurité offerte par ceux-ci.
- *Managing IMAP* de Dianna Mullet et Kevin Mullet ; O'Reilly & Associates — Une explication des étapes nécessaires à la configuration d'un serveur IMAP.
- *Guide de sécurité de Red Hat Enterprise Linux* ; Red Hat, Inc. — Le chapitre intitulé *Sécurité de serveur* explique différentes manières de sécuriser Sendmail et d'autres services.

Chapitre 12.

Berkeley Internet Name Domain (BIND)

Sur la plupart des réseaux modernes, y compris l'Internet, les utilisateurs localisent les autres ordinateurs au moyen du nom. Ainsi les utilisateurs n'ont pas à se souvenir de l'adresse réseau numérique des ressources réseau. La manière la plus efficace de configurer un réseau afin de permettre des connexions à base de nom consiste à établir un *Service de Nom de Domaine* (ou *DNS*, de l'anglais Domain Name Service) ou un *serveur de noms* qui permet d'associer des noms d'hôte d'un réseau à des adresses numériques et vice-versa.

Ce chapitre examine le serveur de noms inclus dans Red Hat Enterprise Linux, le serveur DNS *Berkeley Internet Name Domain* (*BIND*), et met l'accent tout particulièrement sur la structure de ses fichiers de configuration et sur la manière de l'administrer aussi bien localement qu'à distance.

Pour obtenir des instructions sur la configuration de BIND à l'aide de l'application graphique **Outil de configuration du service de noms de domaines** (`redhat-config-bind`), reportez-vous au chapitre intitulé *Configuration de BIND* du *Guide d'administration système de Red Hat Enterprise Linux*.

Avertissement

Si vous utilisez l'**Outil de configuration du service de noms de domaines**, ne modifiez manuellement aucun des fichiers de configuration de BIND car tous les changements seront annulés lors d'une utilisation postérieure de l'**Outil de configuration du service de noms de domaines**.

12.1. Introduction au DNS

Lorsque les hôtes d'un réseau se connectent entre eux au moyen d'un nom d'hôte, auquel on fait réfèrence également sous le terme *nom de domaine pleinement qualifié ou FQDN* de l'anglais fully qualified domain name, le DNS est utilisé pour associer les noms des différents ordinateurs à l'adresse IP de l'hôte.

L'utilisation du DNS et du FQDN offre aux administrateurs système de nombreux avantages et leur permet, en outre, de changer facilement l'adresse IP d'un hôte sans avoir d'impact sur les requêtes basées sur le nom qui sont envoyées à cet ordinateur. Inversement, les administrateurs peuvent décider des machines qui traiteront une requête basée sur le nom.

Le service DNS est normalement mis en oeuvre grâce à des serveurs centralisés qui font autorité pour certains domaines et se réfèrent à d'autres serveurs DNS pour d'autres domaines.

Lorsqu'un hôte client demande des informations au serveur de noms, il se connecte généralement sur le port 53. Le serveur de noms tente alors de résoudre le FQDN d'après sa bibliothèque de solutions qui peut contenir des informations importantes sur l'hôte demandé ou des données mise en cache suite à une requête antérieure. Si le serveur de noms ne possède pas déjà la réponse dans sa bibliothèque de solutions, il se tourne vers d'autres serveurs de noms, appelés *serveurs de noms root* (ou serveurs de noms racines), afin de déterminer les serveurs de noms faisant autorité pour le FQDN en question. Grâce à ces informations, il effectuera ensuite une requête auprès des serveurs de noms faisant autorité pour déterminer l'adresse IP de l'hôte en question. S'il effectue une opération dans le sens inverse (reverse lookup), la même procédure qui est utilisée, si ce n'est que la requête est présentée avec une adresse IP inconnue au lieu d'un nom.

12.1.1. Zones de serveurs de noms

Sur Internet, le FQDN d'un hôte peut être structuré en sections. Celles-ci sont ensuite organisées hiérarchiquement, comme un arbre, avec un tronc principal, des branches primaires, des branches secondaires, et ainsi de suite. Prenons, par exemple, le FQDN suivant :

```
bob.sales.example.com
```

Lors de l'analyse de la manière selon laquelle un FQDN trouve l'adresse IP qui renvoie à un système particulier, lisez le nom de droite à gauche, chaque niveau de la hiérarchie étant séparé par des points (`.`). Dans notre exemple, l'élément `com` définit le *domaine de niveau supérieur* pour ce FQDN. Le nom `example` est un sous-domaine de `com` alors que `sales` est un sous-domaine de `example`. Le nom le plus à gauche `bob` identifie le nom d'hôte d'une machine particulière.

À l'exception du nom de domaine, chaque section s'appelle une *zone* et définit un *espace de nom* particulier. Un espace de nom contrôle l'attribution des noms des sous-domaines à sa gauche. Alors que cet exemple ne contient que deux sous-domaines, un FQDN doit contenir au moins un sous-domaine mais peut en inclure beaucoup plus, selon l'organisation choisie pour l'espace de nom.

Les zones sont définies sur des serveurs de noms qui font autorité par l'intermédiaire de *fichiers de zone*, décrivant entre autres, l'espace de nom de cette zone, les serveurs de courrier qui doivent être utilisés pour un domaine ou sous-domaine particulier. Les fichiers de zone sont stockés sur des *serveurs de noms primaires* (aussi appelés *serveurs de noms maîtres*), qui font vraiment autorité et constituent l'endroit où des changements peuvent être apportés aux fichiers ; les *serveurs de noms secondaires* (aussi appelés *serveurs de noms esclaves*) quant à eux reçoivent leurs fichiers de zone des serveurs de noms primaires. Tout serveur de noms peut être simultanément maître ou esclave pour différentes zones et peut aussi être considéré comme faisant autorité pour de multiples zones. Tout cela dépend de la configuration du serveur de noms.

12.1.2. Types de serveurs de noms

Il existe quatre types de configuration possibles pour les serveurs de noms primaires :

- *maître* — (master) Stocke les enregistrements de zone originaux faisant autorité pour un espace de nom particulier et répond aux questions d'autres serveurs de noms qui cherchent des réponses quant à cet espace de nom.
- *esclave* — (slave) Répond aux requêtes d'autres serveurs de noms concernant les espaces de nom pour lesquels il est considéré comme faisant autorité. Les serveurs de noms esclaves reçoivent leurs informations d'espace de nom des serveurs de noms maîtres.
- *cache-seulement* — (cacing-only) Offre des services de résolution de nom vers IP mais ne fait pas autorité pour quelque zone que ce soit. Les réponses pour toutes les résolutions sont placées en cache dans une base de données stockée en mémoire pour une période établie qui est spécifiée par l'enregistrement de zone importé.
- *retransmission* — (forwarding) Fait suivre des requêtes de résolution à une liste spécifique de serveurs de noms. Si aucun des serveurs de noms spécifiés ne peut effectuer la résolution, le processus s'arrête et la résolution a échoué.

Un serveur de noms appartenir à un ou plusieurs de ces types. Par exemple, un serveur de noms peut être non seulement maître pour certaines zones, esclave pour d'autres mais il peut également offrir seulement la transmission d'une résolution pour d'autres zones.

12.1.3. BIND en tant que serveur de noms

Le serveur de noms BIND fournit ses services de résolution de noms à l'aide du démon `/usr/sbin/named`. BIND contient également un utilitaire d'administration appelé `/usr/sbin/rndc`. De plus amples informations sur `rndc` sont disponibles dans la Section 12.4.

BIND stocke ses fichiers de configuration aux emplacements suivants :

- le fichier `/etc/named.conf` — Le fichier de configuration du démon `named`.
- le répertoire `/var/named/` — Le répertoire de travail de `named` qui stocke les fichiers de zone, de statistiques et les fichiers de cache.

Les sections suivantes examinent les fichiers de configuration de manière plus détaillée.

12.2. `/etc/named.conf`

Le fichier `named.conf` est une suite de déclarations utilisant des options imbriquées qui sont placées entre accolades, `{ }`. Lorsqu'ils modifient le fichier `named.conf`, les administrateurs doivent veillez tout particulièrement à ne pas faire de fautes de syntaxe car des erreurs mineures en apparence empêcheront le démarrage du service `named`.

Avertissement

Ne modifiez pas manuellement le fichier `/etc/named.conf` ou tout autre fichier du répertoire `/var/named/` si vous utilisez l'**Outil de configuration du service de noms de domaines**. Tous les changements apportés manuellement à ces fichiers seront annulés lors d'une l'utilisation ultérieure de l'**Outil de configuration du service de noms de domaines**.

Un fichier `named.conf` typique est organisé de manière semblable à l'extrait ci-dessous :

```
<statement-1> ["<statement-1-name>"] [<statement-1-class>] {
   <option-1>;
   <option-2>;
   <option-N>;
};

<statement-2> ["<statement-2-name>"] [<statement-2-class>] {
   <option-1>;
   <option-2>;
   <option-N>;
};

<statement-N> ["<statement-N-name>"] [<statement-N-class>] {
   <option-1>;
   <option-2>;
   <option-N>;
};
```

12.2.1. Types courants de déclarations

Les types de déclarations suivants sont couramment utilisés dans `/etc/named.conf` :

12.2.1.1. Déclaration `acl`

La déclaration `acl` (de l'anglais access control list, ou déclaration de liste de contrôle d'accès) définit des groupes d'hôtes qui peuvent ensuite être autorisés ou non à accéder au serveur de noms.

Une déclaration `acl` se présente sous le format suivant :

```
acl <acl-name> {
    <match-element>;
    [<match-element>; ...]
};
```

Dans cette déclaration, remplacez *<acl-name>* par le nom de la liste du contrôle d'accès et remplacez *<match-element>* par une liste d'adresses IP séparées entre elles par un point virgule. La plupart du temps, une adresse IP individuelle ou la notation réseau de l'IP (telle que `10.0.1.0/24`) est utilisée pour identifier les adresses IP dans la déclaration `acl`.

Les listes de contrôle d'accès suivantes sont déjà définies en tant que mots-clés afin de simplifier la configuration :

- `any` — Correspond à toutes les adresses IP.
- `localhost` — Correspond à toute adresse IP utilisée par le système local.
- `localnets` — Correspond à toute adresse IP sur tout réseau auquel le système local est connecté.
- `none` — Ne correspond à aucune adresse IP.

Lorsqu'elles sont utilisées avec d'autres déclarations (telles que la déclaration `options`), les déclarations `acl` peuvent être très utiles pour éviter la mauvaise utilisation d'un serveur de noms BIND.

L'exemple ci-dessous établit deux listes de contrôle d'accès et utilise une déclaration `options` pour définir la manière dont elles seront traitées par le serveur de noms :

```
 acl black-hats {
    10.0.2.0/24;
    192.168.0.0/24;
 };

acl red-hats {
    10.0.1.0/24;
 };

options {
    blackhole { black-hats; };
    allow-query { red-hats; };
    allow-recursion { red-hats; };
 }
```

Cet exemple comporte deux listes de contôle d'accès, `black-hats` et `red-hats`. Les hôtes de la liste `black-hats` se voient dénier l'accès au serveur de noms, alors que ceux de la liste `red-hats` se voient eux donner un accès normal.

12.2.1.2. Déclaration `include`

La déclaration `include` permet à des fichiers d'être inclus dans un fichier `named.conf`. Ce faisant, des données de configurations critiques (telles que les clés, `keys`) peuvent être placées dans un fichier séparé doté de permissions restrictives.

Une déclaration `include` se présente sous le format suivant :

```
include  "<file-name>"
```

Dans cette déclaration, *<file-name>* est remplacé par le chemin d'accès absolu vers un fichier.

12.2.1.3. Déclaration `options`

La déclaration `options` définit les options globales de configuration serveur et établit des valeurs par défaut pour les autres déclarations. Cette déclaration peut être utilisée entre autres pour spécifier l'emplacement du répertoire de travail `named` ou pour déterminer les types de requêtes autorisés.

La déclaration `options` se présente sous le format suivant :

```
options {
        <option>;
 [<option>; ...]
};
```

Dans cette déclaration, les directives *<option>* sont remplacées par une option valide.

Ci-dessous figure une liste des options couramment utilisées :

- `allow-query` — Spécifie les hôtes autorisés à interroger ce serveur de noms. Par défaut, tous les hôtes sont autorisés à interroger le serveur de noms. Il est possible d'utiliser ici une liste de contrôle d'accès ou un ensemble d'adresses IP ou de réseaux afin de n'autoriser que des hôtes particuliers à interroger le serveur de noms.
- `allow-recursion` — Semblable à `allow-query`, cette option s'applique à des demandes récursives. Par défaut, tous les hôtes sont autorisés à effectuer des demandes récursives sur le serveur de noms.
- `blackhole` — Spécifie les hôtes qui ne sont pas autorisés à interroger le serveur de noms.
- `directory` — Change le répertoire de travail `named` pour une valeur autre que la valeur par défaut, `/var/named/`.
- `forward` — Contrôle le comportement de retransmission d'une directive `forwarders`.

  Les options suivantes sont acceptées :

  - `first` — Établit que les serveurs de noms spécifiés dans la directive `forwarders` soient interrogés avant que `named` ne tente de résoudre le nom lui-même.
  - `only` — Spécifie que `named` ne doit pas tenter d'effectuer lui-même une résolution de nom dans le cas où des demandes vers les serveurs de noms spécifiés dans la directive `forwarders` échouent.

- `forwarders` — Spécifie une liste d'adresses IP valides correspondant aux serveurs de noms vers lesquels les requêtes devraient être envoyées pour la résolution.
- `listen-on` — Spécifie l'interface réseau sur laquelle `named` prend note des requêtes. Par défaut, toutes les interfaces sont utilisées.

  De cette manière, si le serveur DNS sert également de passerelle, BIND peut être configuré de telle sorte qu'il réponde seulement aux requêtes en provenance de l'un des réseaux.

  Une directive `listen-on` peut ressembler à l'extrait ci-dessous :

  ```
  options {
     listen-on { 10.0.1.1; };
  };
  ```

  Dans cet exemple, seules les requêtes qui proviennent de l'interface réseau servant le réseau privé (`10.0.1.1`) sont acceptées.

- `notify` — Établit si `named` notifie les serveurs esclaves lorsqu'une zone est mise à jour. Les options suivantes sont acceptées :
  - `yes` — Notifie les serveurs esclaves.
  - `no` — Ne notifie pas les serveurs esclaves.
  - `explicit` — Notifie seulement les serveurs esclaves spécifiés dans une liste `also-notify` à l'intérieur d'une déclaration de zone.

- `pid-file` — Spécifie l'emplacement du fichier de processus ID créé par `named`.
- `root-delegation-only` — Active l'application des propriétés de délégation dans les TLD (de l'anglais top-level domains ou domaines de premier niveau) et les zones root avec une liste d'exclusion facultative. Le procédé dit de *Délégation* consiste à diviser une zone unique en multiples sous-zones. Afin de créer une zone déléguée, des éléments connus sous le nom *NS records* sont utilisés. Ces informations NameServer (ou delegation records) précise les serveurs de noms d'autorité pour une zone particulière.

  L'exemple suivant de `root-delegation-only` spécifie une liste d'exclusion de TLD desquels des réponses non-déléguées sont attendues en toute confiance :

```
options {
   root-delegation-only exclude { "ad"; "ar"; "biz"; "cr"; "cu"; "de"; "dm"; "id";
      "lu"; "lv"; "md"; "ms"; "museum"; "name"; "no"; "pa";
      "pf"; "se"; "sr"; "to"; "tw"; "us"; "uy"; };
};
```

- `statistics-file` — Spécifie un autre emplacement des fichiers de statistiques. Par défaut, les statistiques `named` sont enregistrées dans le fichier `/var/named/named.stats`.

De nombreuses autres options sont également disponibles, dont beaucoup dépendent les unes des autres pour fonctionner correctement. Consultez le document *BIND 9 Administrator Reference Manual* dans la Section 12.7.1 et la page de manuel de `bind.conf` pour obtenir de plus amples informations.

12.2.1.4. Déclaration `zone`

Une déclaration `zone` définit les caractéristiques d'une zone tels que l'emplacement de ses fichiers de configuration et les options spécifiques à la zone. Cette déclaration peut être utilisée pour remplacer les déclarations globales d'`options`.

Une déclaration `zone` se présente sous le format suivant :

```
zone <zone-name> <zone-class> {
     <zone-options>;
     [<zone-options>; ...]
};
```

Dans la déclaration, *<zone-name>* correspond au nom de la zone, *<zone-class>* à la classe optionnelle de la zone et *<zone-options>* représente une liste des options caractérisant la zone.

L'attribut *<zone-name>* de la déclaration de zone est particulièrement important. Il représente la valeur par défaut assignée à la directive `$ORIGIN` utilisée au sein du fichier de zone correspondant qui se trouve dans le répertoire `/var/named/`. Le démon `named` ajoute le nom de la zone à tout nom de domaine qui n'est pas pleinement qualifié, énuméré dans le fichier de zone.

Par exemple, si une déclaration `zone` définit l'espace de nom pour `example.com`, utilisez `example.com` comme *<zone-name>* afin qu'il soit placé à la fin des noms d'hôtes au sein du fichier de zone `example.com`.

Pour obtenir de plus amples informations sur les fichiers de zone, reportez-vous à la Section 12.3.

Parmi les options les plus courantes de la déclaration de `zone` figurent :

- `allow-query` — Spécifie les clients qui sont autorisés à demander des informations à propos de cette zone. Par défaut toutes les requêtes d'informations sont autorisées.
- `allow-transfer` — Spécifie les serveurs esclaves qui sont autorisés à demander un transfert des informations relatvies à la zone. Par défaut toutes les requêtes de transfert sont autorisées.
- `allow-update` — Spécifie les hôtes qui sont autorisés à mettre à jour dynamiquement les informations dans leur zone. Par défaut aucune requête de mise à jour dynamique n'est autorisée.

  Soyez très prudent lorsque vous autorisez des hôtes à mettre à jour des informations concernant leur zone. N'activez cette option que si l'hôte est sans aucun doute digne de confiance. De manière générale, il est préférable de laisser un administrateur mettre à jour manuellement les enregistrements de la zone et recharger le service `named`.
- `file` — Spécifie le nom du fichier qui figure dans le répertoire de travail `named` et qui contient les données de configuration de la zone.
- `masters` — Spécifie les adresses IP à partir desquelles demander des informations sur la zone faisant autorité. Cette option ne doit être utilisée que si la zone est définie en tant que `type slave`.
- `notify` — Détermine si `named` notifie les serveurs esclaves lorsqu'une zone est mise à jour. Cette directive accepte les options suivantes :
  - `yes` — Notifie les serveurs esclaves.
  - `no` — Ne notifie pas les serveurs esclaves.
  - `explicit` — Notifie seulement les serveurs esclaves spécifiés dans une liste `also-notify` à l'intérieur d'une déclaration de zone.

- `type` — Définit le type de zone. Les types énumérés ci-dessous peuvent être utilisés.

  Ci-après figure une liste des options valides :
  - `delegation-only` — Applique l'état de délégation des zones d'infrastructure comme COM, NET ou ORG. Toute réponse reçue sans délégation explicite ou implicite est traitée en tant que `NXDOMAIN`. Cette option est seulement applicable dans des fichiers de zone TLD ou root en implémentation récursive ou de mise en cache.
  - `forward` — Retransmet toutes les requêtes d'informations concerant cette zone vers d'autres serveurs de noms
  - `hint` — Représente un type spécial de zone utilisé pour diriger des transactions vers les serveurs de noms racines qui résolvent des requêtes lorsqu'une zone n'est pas connue autrement. Aucune configuration autre que la valeur par défaut n'est nécessaire avec une zone `hint`.
  - `master` — Désigne le serveur de noms faisant autorité pour cette zone. Une zone devrait être configurée comme maître (`master`) si les fichiers de configuration de la zone se trouvent sur le système.
  - `slave` — Désigne le serveur de noms comme serveur esclave (slave) pour cette zone. Cette option spécifie également l'adresse IP du serveur de noms maître pour cette zone.

- `zone-statistics` — Configure `named` pour qu'il conserve des statistiques concernant cette zone en les écrivant soit dans l'emplacement par défaut (`/var/named/named.stats`), soit dans le fichier spécifié dans l'option `statistics-file` de la déclaration `server`. Reportez-vous à la Section 12.2.2 pour obtenir de plus amples informations sur la déclaration `server`.

12.2.1.5. Exemples de déclarations `zone`

La plupart des changements apportés au fichier `/etc/named.conf` d'un serveur de noms maître ou esclave implique l'ajout, la modification ou la suppression de déclarations de `zone`. Alors que ces déclarations de `zone` peuvent contenir de nombreuses options, la plupart des serveurs de noms nécessitent seulement quelques options pour fonctionner de manière efficace. Les déclarations de `zone` figurant ci-dessous représentent des exemples très élémentaires pour illustrer une relation de serveurs de noms maître/esclave.

Ci-dessous se trouve un exemple de déclaration `zone` pour le serveur de noms primaire hébergeant `example.com` (`192.168.0.1`) :

```
zone "example.com" IN {
  type master;
  file "example.com.zone";
  allow-update { none; };
};
```

Dans cette déclaration, la zone est identifiée en tant que `example.com`, le type est défini comme `master` et le service `named` a comme instruction de lire le fichier `/var/named/example.com.zone`. Elle indique à `named` de refuser la mise à jour à tout autre hôte.

La déclaration `zone` d'un serveur esclave pour `example.com` est légèrement différente de l'exemple précédent. Pour un serveur esclave, le type est `slave` et une directive indiquant à `named` l'adresse IP du serveur maître remplace la ligne `allow-update`.

Ci-dessous se trouve un exemple de déclaration `zone` de serveur de noms pour la zone `example.com` :

```
zone "example.com" {
  type slave;
  file "example.com.zone";
  masters { 192.168.0.1; };
};
```

Cette déclaration `zone` configure `named` sur le serveur esclave de manière à ce qu'il cherche le serveur maître à l'adresse IP `192.168.0.1` pour y trouver les informations concernant la zone appelée `example.com`. Les informations que le serveur esclave reçoit du serveur maître sont enregistrées dans le fichier `/var/named/example.com.zone`.

12.2.2. Autres types de déclarations

Ci-dessous se trouve une liste de types de déclarations moins fréquemment utilisés mais nénamoins disponibles au sein de `named.conf` :

- `controls` — Configure diverses contraintes de sécurité nécessaires â l'utilisation de la commande `rndc` pour administrer le service `named`.

  Consultez la Section 12.4.1 pour acquérir davantage de connaissances sur la structure de la déclaration `controls` et sur les options disponibles.

- `key "<key-name>"` — Définit une clé spécifique par nom. Les clés servent à valider diverses actions, comme les mises à jour sécurisées ou l'utilisation de la commande `rndc`. Deux options sont utilisées avec `key` :

  - `algorithm <algorithm-name>` — Représente le type d'algorithme utilisé, tel que `dsa` ou `hmac-md5`.
  - `secret "<key-value>"` — Représente la clé cryptée.

  Reportez-vous à la Section 12.4.2 pour obtenir des instructions sur l'écriture d'une déclaration `key`.

- `logging` — Permet d'utiliser de multiples types de journaux (ou logs) appelés canaux (ou *channels*). En utilisant l'option `channel` dans la déclaration `logging`, il est possible de construire un type de journal personnalisé, avec des caractèristique propres à savoir nom de fichier (`file`), sa limite de taille (`size`), version (`version`) et son propre niveau d'importance (`severity`). Une fois qu'un canal personnalisé a été défini, une option `category` est utilisée pour catégoriser le canal et commencer la journalisation quand `named` est redémarrée.

  Par défaut, `named` journalise des messages standards grâce au démon `syslog` qui les place dans `/var/log/messages`. Ce processus de journalisation a lieu car plusieurs canaux standards sont intégrés dans BIND, avec plusieurs niveaux d'importance (severity levels), comme celui qui traite les messages de journalisation informationnels (`default_syslog`) et celui qui traite spécifiquement les messages de débogage (`default_debug`). Une catégorie par défaut, appelée `default`, utilise les canaux compris dans BIND pour accomplir la journalisation normale, sans configuration spéciale.

  La personnalisation de la journalisation peut être un processus très détaillé qui dépasse le cadre du présent chapitre. Pour obtenir davantage d'informations sur la création de journaux personnalisés avec BIND, consultez le document intitulé *BIND 9 Administrator Reference Manual* dans la Section 12.7.1.

- `server` — Définit des options particulières qui affectent la façon selon laquelle `named` doit répondreaux serveurs de noms distants, particulièrement pour ce qui est des notifications et des transferts de zone.

  L'option `transfer-format` détermine si un enregistrement de ressources est envoyé avec chaque message (`one-answer`) ou si des enregistrements de ressources multiples sont envoyés avec chaque message (`many-answers`). Alors que l'option `many-answers` est plus efficace, seuls les serveurs de noms BIND les plus récents peuvent la comprendre.

- `trusted-keys` — Contient des clés publiques variées qui sont utilisées pour des DNS sécurisés (DNSSEC). Consultez la Section 12.5.3 pour obtenir de plus amples informations sur la sécurité avec BIND.

- `view "<view-name>"` — Crée des vues spéciales en fonction du réseau sur lequel l'hôte interroge le serveur de noms. Ce type de déclaration permet à certains hôtes de recevoir une réponse quant à une zone particulière alors que d'autres hôtes reçoivent des informations totalement différentes. Certains hôtes dignes de confiance peuvent également se voir accorder l'accès à certaines zones alors que d'autres hôtes qui ne sont pas dignes de confiance doivent limiter leurs requêtes à d'autres zones.

  Il est possible d'obtenir de multiples vues mais leurs leurs noms doivent être uniques. L'option `match-clients` spécifie les adresses IP qui s'appliquent à une vue particulière. Toute déclaration `options` peut aussi être utilisée dans une vue, avec priorité sur les options globales déjà configurées pour `named`. La plupart des déclarations `view` contiennent de multiples déclarations `zone` qui s'appliquent à la liste `match-clients`. L'ordre dans lequel les déclarations `view` sont énumérées est important, puisque c'est la première déclaration `view` qui correspond à l'adresse IP d'un client, qui est utilisée.

  Consultez la Section 12.5.2 pour obtenir davantage d'informations sur la déclaration `view`.

12.2.3. Balises de commentaire

La liste suivante regroupe les balises (ou tags) de commentaire valides qui sont utilisés dans `named.conf` :

- `//` — Lorsque ce symbole est placé en début de ligne, cette dernière n'est pas prise en compte par `named`.
- `#` — Lorsque ce symbole est placé en début de ligne, cette dernière n'est pas prise en compte par `named`.

- `/*` et `*/` — Lorsque du texte est placé entre ces symboles, le bloc de texte en question n'est pas pris en compte par `named`.

12.3. Fichiers de zone

Les *Fichiers de zone* contiennent des informations sur un espace de nom particulier et sont stockés dans le répertoire de travail `named` qui est par défaut `/var/named/`. Chaque fichier de zone est nommé selon les données d'options de `file` dans la déclaration `zone`, et ce, généralement d'une manière qui se réfère au domaine en question et identifie le fichier comme contenant des données de zone, telles que `example.com.zone`.

Chaque fichier de zone peut contenir des *directives* et des *enregistrements de ressources*. Les directives donnent au serveur de noms l'instruction d'effectuer une certaine tâche ou d'appliquer des paramètres spéciaux à la zone. Les enregistrements de ressources définissent les paramètres de la zone, assignant des identités aux hôtes individuels. Les directives sont facultatives, mais les enregistrements de ressources sont requis pour fournir un service de nom à une zone.

Toutes les directives et enregistrements de ressources doivent être spécifiées sur des lignes individuelles.

Des commentaires peuvent être placés dans les fichiers de zone après les caractères points-virgules (`;`).

12.3.1. Directives des fichiers de zone

Les directives sont identifiées par le symbole dollar (`$`) suivit du nom de la directive. Elles apparaissent généralement en haut du fichier de zone.

Les directives les plus couramment utilisées sont les suivantes :

- `$INCLUDE` — Configure `named` de façon à ce qu'il inclue un autre fichier de zone dans ce fichier de zone à l'endroit où la directive apparaît. Ce faisant, il est possible de stocker des configurations de zone supplémentaires à l'écart du fichier de zone principal.
- `$ORIGIN` — Attache le nom de domaine à des enregistrements non-qualifiés, comme ceux qui spécifient seulement l'hôte et rien de plus.

  Par exemple, un fichier de zone peut contenir la ligne suivante :
  `$ORIGIN example.com.`

  Tous les noms utilisés dans les enregistrement de ressources qui ne se terminent pas par un point (`.`) se verront ajouter `example.com.`

  

  Remarque

  L'utilisation de la directive `$ORIGIN` n'est pas nécessaire si l'on nomme la zone dans `/etc/named.conf` parce que le nom de la zone est utilisé par défaut, comme la valeur de la directive `$ORIGIN`

- `$TTL` — Règle la valeur par défaut de *Time to Live (TTL)* (ou temps de vie) pour la zone. Cette valeur exprimée en secondes, correspond à la durée pendant laquelle un enregistrement de ressources de zone est valide. Chaque enregistrement de ressources peut contenir sa propre valeur TTL, qui remplace alors cette directive.

  L'aumentation de cette valeur permet aux serveurs de noms distants de mettre en cache ces informations de zone pendant plus longtemps, réduisant ainsi nombre de requêtes effectuées au sujet de

cette zone et rallongeant le temps nécessaire pour la prolifération des changements apportés aux enregistrements de ressources.

12.3.2. Enregistrements de ressources des fichiers de zone

Les enregistrements de ressources représentent le premier composant d'un fichier de zone.

Il existe de nombreux types d'enregistrements de ressources des fichiers de zone. Ceux énumérés ci-dessous sont néanmoins les plus fréquemment utilisés :

- `A` — Enregistrement d'adresse qui spécifie une adresse IP à assigner à un nom, comme dans l'exemple ci-dessous :

  ```
  <host>      IN      A      <IP-address>
  ```

  Si la valeur *<host>* est omise, alors un enregistrement `A` renvoie à une adresse IP par défaut pour la partie supérieure de l'espace de nom. Ce système est la cible de toutes les requêtes non-FQDN.

  Examinons les exemples d'enregistrements `A` suivants pour le fichier de zone `example.com` :

  ```
                IN      A       10.0.1.3
  server1       IN      A       10.0.1.5
  ```

  Les requêtes pour `example.com` sont dirigées vers 10.0.1.3, alors que les requêtes pour `server1.example.com` sont orientées vers 10.0.1.5.

- `CNAME` — Enregistrement de nom canonique mappant un nom à un autre. Ce type d'enregistrement est plus connu sous le nom d'enregistrement d'alias.

  L'exemple suivant indique à `named` que toute requête envoyée à *<alias-name>* devrait être dirigée vers l'hôte, *<real-name>*. Les enregistrements `CNAME` sont généralement utilisés pour pointer vers les services qui utilisent un procédé commun de nommage, comme par exemple, `www` pour les serveurs Web.

  ```
  <alias-name>      IN      CNAME       <real-name>
  ```

  Dans l'exemple suivant, un enregistrement `A` lie un nom d'hôte à une adresse IP alors qu'un enregistrement `CNAME` pointe le nom d'hôte `www` le fréquemment utilisé vers l'adresse.

  ```
  server1       IN      A       10.0.1.5
  www           IN      CNAME   server1
  ```

- `MX` — Enregistrement Mail eXchange, qui indique où devrait aller le courrier envoyé à un nom d'espace particulier contrôlé par cette zone.

  ```
        IN      MX      <preference-value>   <email-server-name>
  ```

  Dans cet exemple, *<preference-value>* permet de classer numériquement les serveurs de messagerie pour un espace de nom, en donnant une préférence à certains systèmes de messagerie par rapport à d'autres. L'enregistrement de ressources `MX` doté de la valeur *<preference-value>* la plus basse est préféré aux autres. Toutefois, de multiples serveurs de messagerie peuvent avoir la même valeur pour distribuer uniformément le trafic d'emails entre eux.

  L'option *<email-server-name>* peut être un nom d'hôte ou un FQDN.

  ```
        IN      MX      10      mail.example.com.
        IN      MX      20      mail2.example.com.
  ```

  Dans cet exemple, le premier serveur de messagerie `mail.example.com` est préféré au serveur de messagerie `mail2.example.com` lors de la réception des courriers électroniques destinés au domaine `example.com`.

- `NS` — Enregistrement de serveur de noms (NameServer) annonçant les serveurs de noms faisant autorité pour une zone particulière.

  Ci-dessous figure un exemple d'enregistrement `NS` :

  ```
        IN      NS      <nameserver-name>
  ```

L'élément <*nameserver-name*> devrait correspondre à un FQDN.

Ensuite, deux serveurs de noms sont répertoriés comme faisant autorité pour le domaine. Le fait que ces serveurs de noms soient esclaves ou que l'un d'eux soit maître n'a pas d'importance ; ils sont tous les deux considérés comme faisant autorisé.

```
        IN      NS      dns1.example.com.
        IN      NS      dns2.example.com.
```

- `PTR` — Enregistrement PoinTeR, conçu pour pointer vers une autre partie de l'espace de nom.

  Les enregistrements `PTR` servent essentiellement à la résolution inverse des noms, puisqu'ils renvoient les adresses IP vers un nom particulier. Consultez la Section 12.3.4 pour obtenir des exemples supplémentaires d'utilisation des enregistrements `PTR`.

- `SOA` — Enregistrement de ressources Start Of Authority, proclame des informations importantes faisant autorité sur un espace de nom pour le serveur de noms.

  Situé après les directives, un enregistrement de ressources `SOA` est le premier enregistrement de ressources dans un fichier de zone.

  L'exemple qui suit montre la structure de base d'un enregistrement de ressources `SOA` :

```
@       IN      SOA     <primary-name-server>       <hostmaster-email> (
                        <serial-number>
                        <time-to-refresh>
                        <time-to-retry>
                        <time-to-expire>
                        <minimum-TTL> )
```

  Le symbole `@` place la directive `$ORIGIN` (ou le nom de zone, si la directive `$ORIGIN` n'est pas déterminée) en tant qu'espace de nom défini par le présent enregistrement de ressources `SOA`. Le nom d'hôte du serveur de noms primaire faisant autorité pour ce domaine est utilisé pour le <*primary-name-server*> et l'adresse électronique de la personne à contacter à propos de cet espace de nom est remplacée par <*hostmaster-email*>.

  La directive <*serial-number*> est incrémentée lors de chaque modification du fichier de zone afin que `named` sache qu'il doit recharger cette zone. La valeur <*time-to-refresh*> indique à tout serveur esclave combien de temps il doit attendre avant de demander au serveur de noms maître si des changements ont été effectués dans la zone. La valeur <*serial-number*> est utilisée par le serveur esclave pour déterminer s'il est en train d'utiliser des données de zone périmées et doit par conséquent les rafraîchir.

  La valeur <*time-to-retry*> précise au serveur de noms esclave l'intervalle pendant lequel il doit attendre avant d'émettre une autre requête de rafraîchissement, au cas où le serveur de noms maître ne répondrait pas. Si le serveur maître n'a pas répondu à une requête de rafraîchissement avant que la durée indiquée dans <*time-to-expire*> ne se soit écoulée, le serveur esclave cesse de répondre en tant qu'autorité pour les requêtes au sujet de cet espace de nom.

  La valeur <*minimum-TTL*> demande que d'autres serveurs de noms mettent en cache les informations pour cette zone pendant au moins cette durée définie.

  Lors de la configuration de BIND, toutes les durées sont exprimées en secondes. Toutefois, il est égalemnt possible d'utiliser des abréviations pour des unités de temps autres que des secondes, comme les minutes (`M`), les heures (`H`), les jours (`D`) et les semaines (`W`). Le Tableau 12-1 montre une durée exprimée en secondes et la période équivalente dans un autre format.

Secondes	Autres unités de temps
60	1M
1800	30M
3600	1H
10800	3H

Secondes	Autres unités de temps
21600	6H
43200	12H
86400	1D
259200	3D
604800	1W
31536000	365D

Tableau 12-1. Les secondes comparées à d'autres unités de temps

L'exemple suivant montre ce à quoi l'enregistrement d'une ressources `SOA` peut ressembler lorsqu'il est configuré avec des valeurs réelles.

```
@     IN     SOA    dns1.example.com.     hostmaster.example.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
                    3600       ; retry after 1 hour
                    604800     ; expire after 1 week
                    86400 )    ; minimum TTL of 1 day
```

12.3.3. Exemples de fichiers de zone

Si on les observe individuellement, les directives et enregistrements de ressources peuvent être difficiles à comprendre. Cependant, tout devient beaucoup plus simple lorsqu'on peut les observer ensemble dans un seul fichier commun.

L'exemple suivant illustre un fichier de zone très élémentaire.

```
$ORIGIN example.com.
$TTL 86400
@     IN     SOA    dns1.example.com.     hostmaster.example.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
                    3600       ; retry after 1 hour
                    604800     ; expire after 1 week
                    86400 )    ; minimum TTL of 1 day

      IN     NS     dns1.example.com.
      IN     NS     dns2.example.com.

      IN     MX     10     mail.example.com.
      IN     MX     20     mail2.example.com.

             IN     A       10.0.1.5

server1      IN     A       10.0.1.5
server2      IN     A       10.0.1.7
dns1         IN     A       10.0.1.2
dns2         IN     A       10.0.1.3

ftp          IN     CNAME   server1
mail         IN     CNAME   server1
mail2        IN     CNAME   server2
www          IN     CNAME   server2
```

Dans cet exemple sont utilisées des directives et des valeurs `SOA` standard. Les serveurs de noms faisant autorité seront `dns1.example.com` et `dns2.example.com`, qui ont des enregistrements `A` les liant respectivement à `10.0.1.2` et à `10.0.1.3`.

Les serveurs de messagerie configurés par les enregistrements `MX` pointent vers les serveurs `server1` et `server2` au moyen des enregistrements `CNAME`. Puisque les noms des serveurs `server1` et `server2` ne finissent pas par un point (`.`), le domaine `$ORIGIN` est attaché, rallongeant le nom en `server1.example.com` et `server2.example.com`. Grâce aux enregistrements de ressources `A` associés, leurs adresses IP peuvent être déterminées.

Les services FTP et Web services, disponibles aux noms `ftp.example.com` et `www.example.com` standard, sont pointés vers les serveurs appropriés en utilisant les enregistrements `CNAME`.

12.3.4. Fichiers de résolution de noms inverse

Un fichier de zone de résolution de nom inverse est utilisé pour traduire une adresse IP dans un espace de nom particulier en un FQDN. Il ressemble beaucoup à un fichier de zone standard, sauf que les enregistrements de ressources `PTR` servent à lier les adresses IP au nom d'un domaine pleinement qualifié.

Un enregistrement `PTR` ressemble à l'extrait ci-dessous :

```
<last-IP-digit>       IN      PTR     <FQDN-of-system>
```

L'élément *<last-IP-digit>* fait référence au dernier chiffre d'une adresse IP qui pointe vers le FQDN d'un système particulier.

Dans l'exemple suivant, les adresses IP allant de `10.0.1.20` à `10.0.1.25` pointent vers les FQDN correspondants.

```
$ORIGIN 1.0.10.in-addr.arpa.
$TTL 86400
@     IN      SOA     dns1.example.com.      hostmaster.example.com. (
                      2001062501 ; serial
                      21600      ; refresh after 6 hours
                      3600       ; retry after 1 hour
                      604800     ; expire after 1 week
                      86400 )    ; minimum TTL of 1 day

      IN      NS      dns1.example.com.
      IN      NS      dns2.example.com.

20    IN      PTR     alice.example.com.
21    IN      PTR     betty.example.com.
22    IN      PTR     charlie.example.com.
23    IN      PTR     doug.example.com.
24    IN      PTR     ernest.example.com.
25    IN      PTR     fanny.example.com.
```

Ce fichier de zone serait mis en service avec une déclaration `zone` dans le fichier `named.conf` similaire à l'extrait suivant :

```
zone "1.0.10.in-addr.arpa" IN {
  type master;
  file "example.com.rr.zone";
  allow-update { none; };
};
```

Il existe peu de différences entre cet exemple et une déclaration `zone` standard, sauf pour ce qui est de la manière de nommer l'hôte. Notez qu'une zone de résolution de noms inverse nécessite que les trois

premiers blocs de l'adresse IP soient inversés, puis suivis de l'entité `.in-addr.arpa`. Ce faisant, il est possible d'associer correctement à cette zone le bloc unique de nombres IP utilisé dans le fichier de zone de résolution de nom inverse.

12.4. Utilisation de `rndc`

BIND contient un utilitaire appelé `rndc` qui permet d'utiliser des lignes de commande pour administrer le démon `named` à partir de l'hôte local ou d'un hôte distant.

Afin d'empêcher l'accès non-autorisé au démon `named`, BIND utilise une méthode d'authentification à clé secrète partagée pour accorder des privilèges aux hôtes. Ainsi, une clé identique doit être présente aussi bien dans `/etc/named.conf` que dans le fichier de configuration de `rndc`, à savoir `/etc/rndc.conf`

12.4.1. Configuration de `/etc/named.conf`

Pour que `rndc` puisse se connecter à un service `named`, une déclaration `controls` doit être présente dans le fichier `/etc/named.conf` du serveur BIND.

La déclaration `controls`, décrite dans l'exemple qui suit, permet à `rndc` de se connecter à partir d'un hôte local.

```
controls {
  inet 127.0.0.1 allow { localhost; } keys { <key-name>; };
};
```

Cette déclaration indique à `named` qu'il doit écouterle port TCP 953 par défaut de l'adresse inversée et doit 'autoriser les commandes `rndc` provenant de l'hôte local, si la clé adéquate est donnée. Le *<key-name>* fait référence à la déclaration `key`, qui se trouve dans le fichier `/etc/named.conf`. L'exemple suivant illustre une déclaration `key`.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
};
```

Dans ce cas, la déclaration *<key-value>* utilise l'algorithme HMAC-MD5. Afin de créer des clés à l'aide de l'algorithme HMAC-MD5, utilisez la commande suivante :

```
dnssec-keygen -a hmac-md5 -b <bit-length> -n HOST <key-file-name>
```

Une clé d'au moins 256 bits de long est un bon choix. La clé qui doit être placée dans la zone *<key-value>* se trouve dans le fichier *<key-file-name>* généré par cette commande.

Avertissement

Étant donné que `/etc/named.conf` est lisible par tout un chacun, il est judicieux de placer la déclaration `key` dans un fichier séparé que seul le super-utilisateur (ou root) peut lire et d'utiliser ensuite une déclaration `include` pour le référencer. Par exemple :

```
include "/etc/rndc.key";
```

12.4.2. Configuration de `/etc/rndc.conf`

La déclaration `key` représente la déclaration la plus importante du fichier `/etc/rndc.conf`.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
};
```

Les éléments <*key-name*> et <*key-value*> doivent être absolument identiques aux paramètres les concernant qui figurent dans `/etc/named.conf`.

Pour établir la correspondance entre les clés spécifiées dans le fichier `/etc/named.conf` du serveur cible, ajoutez les lignes reproduites ci-dessous au fichier `/etc/rndc.conf`.

```
options {
  default-server  localhost;
  default-key     "<key-name>";
};
```

Cette directive détermine une clé globale par défaut. Toutefois, le fichier de configuration `rndc` peut également spécifier différentes clés pour différents serveurs, comme le montre l'exemple suivant :

```
server localhost {
  key  "<key-name>";
};
```

Attention

Assurez-vous que seul le super-utilisateur (ou root) puisse effectuer des opérations de lexture et d'écriture dans le fichier `/etc/rndc.conf`.

Pour obtenir davantage d'informations sur le fichier `/etc/rndc.conf`, consultez la page de manuel de `rndc.conf`.

12.4.3. Options de ligne de commande

Une commande `rndc` se présente sous le format suivant :

```
rndc <options> <command> <command-options>
```

Lors de l'exécution de `rndc` sur un hôte local configuré de façon appropriée, les commandes suivantes sont disponibles :

- `halt` — Arrête immédiatement le service `named`.
- `querylog` — Journalise toutes les requêtes effectuées auprès de ce serveur de noms.
- `refresh` — Rafraîchit la base de données du serveur de noms.
- `reload` — Recharge les fichiers de zone mais conserve toutes les réponses précédemment mises en cache. Cette commande permet également d'apporter des changements aux fichiers de zone sans perdre toutes les résolutions de nom stockées.

  Si les changements n'affectent qu'une zone particulière, rechargez seulement cette zone en ajoutant le nom de la zone après la commande `reload`.

- `stats` — Vide les statistiques courante de `named` vers le fichier `/var/named/named.stats`.
- `stop` — Arrête correctement le serveur, en enregistrant préalablement toute mise à jour dynamique et toute donnée *Incremental Zone Transfers* (*IXFR*).

Dans certaines situations, il sera peut-être nécessaire d'annuler les paramètres par défaut contenus dans le fichier `/etc/rndc.conf`. Les options suivantes sont disponibles :

- `-c <configuration-file>` — Spécifie l'autre emplacement d'un fichier de configuration.
- `-p <port-number>` — Spécifie le numéro de port à utiliser pour la connexion de `rndc`, autre que le port par défaut 953.
- `-s <server>` — Spécifie un serveur autre que le `default-server` (serveur pardéfaut) précisé dans `/etc/rndc.conf`.
- `-y <key-name>` — Spécifie une clé autre que l'option `default-key` (clé par défaut) présente dans le fichier `/etc/rndc.conf`.

Des informations supplémentaires sur ces options sont disponibles dans la page de manuel de `rndc`.

12.5. Fonctionnalités avancées de BIND

La plupart des implémentations de BIND utilisent `named` pour fournir un service de résolution de noms ou pour faire autorité pour un domaine ou sous-domaine particuliers. Toutefois, la version 9 de BIND possède aussi un certain nombre de fonctionnalités avancées qui permettent d'offrir un service DNS plus efficace et plus sécurisé.

Attention

Certaines de ces fonctionnalités avancées, comme DNSSEC, TSIG et IXFR (qui sont définies dans la section suivante), ne doivent être utilisées que dans les environnements réseau ayant des serveurs de noms qui prennent en charge ces fonctionnalités. Si votre environnement réseau inclut des serveurs de noms autres que BIND ou des versions de BIND plus anciennes, vérifiez que chaque fonctionnalité avancée est bien prise en charge avant d'essayer de l'utiliser.

Toutes les fonctionnalités mentionnées ici sont décrites en détail dans le document intitulé *BIND 9 Administrator Reference Manual* auquel la Section 12.7.1 fait référence.

12.5.1. Améliorations du protocole DNS

BIND prend en charge les transferts de zone incrémentaux (ou IXFR de l'anglais Incremental Zone Transfers) dans lesquels le serveur de noms esclave ne télécharge que les portions mises à jour d'une zone modifiée sur un serveur de noms maître. Le processus de transfert standard nécessite que la zone entière soit transférée vers chaque serveur de noms esclave même pour des changements mineurs. Pour des domaines très populaires avec des fichiers de zones très longs et pour de nombreux serveurs de noms esclaves, IXFR rend la notification et les processus de mise à jour bien moins exigeants en ressources.

Notez que IXFR n'est disponible que si vous utilisez une *mise à jour dynamique* pour apporter des modifications aux informations de zone maître. Si vous éditez manuellement des fichiers de zone pour effectuer des changements, le processus de transfert AXFR (Automatic Zone Transfer) est utilisé. Davantage d'informations sur les mises à jour dynamiques sont disponibles dans le document intitulé *BIND 9 Administrator Reference Manual*. Reportez-vous à la Section 12.7.1 pour obtenir davantage d'informations.

12.5.2. Vues multiples

En fonction de l'utilisation de la déclaration `view` dans `named.conf`, BIND peut fournir différentes informations en fonction du réseau puis lequel la requête provient.

Cette option est utilisée essentiellement pour refuser des entrées DNS confidentielles depuis des clients externes au réseau local, tout en permettant des requêtes provenant de clients internes au réseau local.

La déclaration `view` utilise l'option `match-clients` pour établir la correspondance entre des adresses IP ou des réseaux entiers et pour leur attribuer des options et des données de zones spéciales.

12.5.3. Sécurité

BIND supporte plusieurs méthodes différentes pour protéger la mise à jour et le transfert de zones, aussi bien sur les serveurs de noms maîtres qu'esclaves :

- *DNSSEC* — Abréviation de *DNS SECurity*, cette fonctionnalité permet de signer cryptographiquement des zones avec une *clé de zone*.

  De cette façon, on peut vérifier que les informations relatives à une zone spécifique proviennent d'un serveur de noms qui les a signées avec une clé privée particulière, du moment que le receveur possède la clé publique de ce serveur de noms.

  La version 9 de BIND prend aussi en charge la méthode d'authentification de messages SIG(0) utilisant un système de clé publique/privée.
- *TSIG* — Abréviation de *Transaction SIGnatures* ; cette fonctionnalité permet d'effectuer un transfert de maître à esclave, mais seulement après vérification qu'une clé secrète partagée existe sur le serveur maître et sur le serveur esclave.

  Cette fonctionnalité renforce la méthode d'autorisation de transfert basée sur l'adresse IP standard. Un agresseur devra non seulement accéder à l'adresse IP pour transférer la zone, mais il devra aussi connaître la clé secrète.

  La version 9 de BIND prend aussi en charge *TKEY*, qui est une autre méthode de clé secrète partagée pour autoriser les transferts de zone.

12.5.4. IP version 6

La version 9 de BIND prend en charge un service de noms dans des environnements IP version 6 (IPv6) grâce aux enregistrements de zone `A6`.

Si votre environnement réseau inclut aussi bien des hôtes IPv4 que des hôtes IPv6, utilisez le démon de résolution léger `lwresd` sur tous les clients du réseau. Ce démon est un serveur de noms très efficace, de type caching-only, qui prend en charge les nouveaux enregistrements d'informations `A6` et `DNAME` utilisés sous IPv6. Consultez la page de manuel de `lwresd` pour obtenir davantage d'informations.

12.6. Erreurs courantes à éviter

De manière générale, les débutants font fréquemment des erreurs en éditant des fichiers de configuration BIND. Évitez les problèmes suivants :

- *Assurez-vous de bien incrémenter le numéro de série lors de toute modification d'un fichier de zone.*

Si le numéro de série n'est pas incrémenté, le serveur de noms maître possède certes les nouvelles informations correctes, mais les serveurs de noms esclaves ne sont jamais notifiés du changement ou ne tentent pas de rafraîchir leurs données concernant cette zone.

- *Assurez-vous de bien utiliser ellipses et points-virgules correctement dans le fichier* `/etc/named.conf`.

  Un point-virgule omis ou une ellipse non-fermée empêcheront `named` de démarrer.

- *Rappelez-vous bien de placer des points (`.`) dans les fichiers de zone après tous les FQDN mais de les omettre pour les noms d'hôtes.*

  Un point à la fin d'un nom de domaine indique un nom de domaine pleinement qualifié (en d'autres termes, complet). Si le point est omis, `named` ajoutera le nom de la zone ou la valeur `$ORIGIN` après le nom pour le compléter.

- *Si votre pare-feu crée des problèmes en bloquant les connexions du programme* `named` *vers d'autres serveurs de noms, éditez son fichier de configuration.*

  La version 9 de BIND utilise par défaut des ports aléatoires supérieurs à 1024 pour envoyer des requêtes à d'autres serveurs de noms. Toutefois certains pare-feu s'attendent à ce que tous les serveurs de noms communiquent uniquement en utilisant le port 53. Pour forcer `named` à utiliser le port 53, ajoutez la ligne reproduite ci-dessous dans la déclaration `options` de `/etc/named.conf` :

  ```
  query-source address * port 53;
  ```

12.7. Ressources supplémentaires

Les sources d'information mentionnées ci-dessous fournissent de la documentation supplémentaire sur l'utilisation de BIND.

12.7.1. Documentation installée

- BIND propose une gamme complète de documentation installée couvrant de nombreux sujets, chacun d'eux étant placé dans son propre répertoire thématique :
  - `/usr/share/doc/bind-<version-number>/` — Ce répertoire dresse une liste des fonctionnalités les plus récentes. Remplacez `<version-number>` par la version de `bind` qui est installée sur le système.
  - `/usr/share/doc/bind-<version-number>/arm/` — Ce répertoire contient les versions HTML et SGML du document intitulé *BIND 9 Administrator Reference Manual*, qui décrit de manière détaillée les ressources nécessaires pour BIND, la façon de configurer différents types de serveurs de noms, d'effectuer la répartition de charges ainsi que d'autres sujets avancés. Pour la plupart des nouveaux utilisateurs de BIND, ces ressources constituent le meilleur point de départ. Remplacez `<version-number>` par la version de `bind` qui est installée sur le système.
  - `/usr/share/doc/bind-<version-number>/draft/` — Ce répertoire contient des documents techniques variés quui abordent les problèmes liés au service DNS et propose certaines solutions pour les résoudre. Remplacez `<version-number>` par la version de `bind` qui est installée sur le système.
  - `/usr/share/doc/bind-<version-number>/misc/` — Ce répertoire contient des documents conçus pour traiter de problèmes spécifiques avancés. Les utilisateurs de la version 8 de BIND devraient consulter le document `migration` pour s'informer des modifications importantes à effectuer pour passer à la version 9 de BIND. Le fichier `options` dresse une liste de toutes les options implémentées dans BIND 9 qui sont utilisées dans `/etc/named.conf`. Remplacez `<version-number>` par la version de `bind` qui est installée sur le système.

  - `/usr/share/doc/bind-<version-number>/rfc/` — Ce répertoire fournit tout document RFC en relation avec BIND. Remplacez `<version-number>` par la version de `bind` qui est installée sur le système.

- Les pages de manuel de BIND — Il existe un certain nombre de pages de manuel pour les diverses applications et les fichiers de configuration intervenant avec BIND. La liste suivante mentionne certaines des pages de manuel les plus importantes.

  Applications administratives

  - `man rndc` — Explique les différentes options disponibles lors de l'utilisation de la commande `rndc` pour contrôler un serveur de noms BIND.

  Applications serveur

  - `man named` — Examine les arguments assortis qui peuvent être utilisés pour contrôler le démon du serveur de noms BIND.
  - `man lwresd` — Décrit le but et les options disponibles pour le démon de résolution très léger.

  Fichiers de configuration

  - `man named.conf` — Une liste exhaustive des options disponibles au sein du fichier de configuration `named`.
  - `man rndc.conf` — Une liste exhaustive des options disponibles au sein du fichier de configuration `rndc`.

12.7.2. Sites Web utiles

- http://www.isc.org/products/BIND — La page d'accueil du projet BIND où vous pourrez trouver des informations sur les versions actuelles ainsi qu'une version PDF du document intitulé *BIND 9 Administrator Reference Manual*.
- http://www.redhat.com/mirrors/LDP/HOWTO/DNS-HOWTO.html — Un document couvrant l'utilisation de BIND en tant que serveur de noms de résolution mettant en cache et la configuration de divers fichiers de zone nécessaires pour qu'il soit utilisé comme serveur de noms primaire pour un domaine.

12.7.3. Livres sur le sujet

- *Guide d'administration système de Red Hat Enterprise Linux* — Le chapitre *Configuration de BIND* explique comment configurer un serveur DNS à l'aide de l'**Outil de configuration du service de noms de domaines**.
- *DNS and BIND* de Paul Albitz et Cricket Liu ; publié par O'Reilly & Associates — Un livre de référence populaire qui explique les options de configuration de BIND des plus simples aux plus ésotériques et fournit aussi des stratégies pour sécuriser votre serveur DNS.
- *The Concise Guide to DNS and BIND* de Nicolai Langfeldt ; publié par Que — Un livre qui examine la connexion entre les services de réseaux multiples et BIND, en mettant l'accent sur les sujets techniques et orientés vers des applications pratiques.

Chapitre 13.

Protocole LDAP (Lightweight Directory Access Protocol)

Le protocole *Lightweight Directory Access Protocol* (ou *LDAP*) est en fait un ensemble de protocoles ouverts utilisés pour accéder à des informations stockées localement sur un réseau. Il est basé sur le standard *X.500* pour le partage de répertoires, mais est moins complexe et moins gourmand en ressources, d'où la référence à LDAP sous le terme "*X.500 Lite*." Le standard X.500 est un répertoire qui contient des informations hiérarchisées et organisées pouvant inclure des renseignements tels que des noms, des adresses et des numéros de téléphone.

Comme X.500, LDAP organise des informations d'une manière hiérarchique en utilisant des répertoires. Ces répertoires peuvent stocker diverses informations et peuvent même être utilisés d'une manière semblable au service d'informations réseau (ou NIS de l'anglais Network Information Service), permettant à tout un chacun d'accéder à son compte depuis une machine quelconque présente sur un réseau sous LDAP.

Dans la plupart des cas, LDAP sert d'annuaire téléphonique virtuel, permettant aux utilisateurs d'accéder facilement aux coordonnées d'autres utilisateurs. Mais le protocole LDAP est beaucoup plus flexible qu'un annuaire téléphonique traditionnel car il peut renvoyer un demandeur vers d'autres serveurs LDAP de par le monde, fournissant ainsi un référentiel d'informations global et improvisé. À l'heure actuelle cependant, le protocole LDAP est plus généralement utilisé au sein de grandes organisations comme des universités, des services gouvernementaux et des entreprises du secteur privé.

Le protocole LDAP est un système client/serveur. Le serveur peut utiliser diverses bases de données pour stocker un répertoire, chacune d'elles étant optimisée de façon à permettre des opérations de consultation rapides et en grande quantité. Lorsqu'un client LDAP se connecte à un serveur LDAP, il peut soit consulter un répertoire, soit y apporter des modifications. Lors de l'arrivée d'une requête, le serveur y répond localement ou la renvoie à un serveur LDAP de niveau supérieur qui aura lui la réponse. Si l'application cliente tente de changer des informations dans un répertoire LDAP, le serveur vérifie d'abord que l'utilisateur est bien autorisé à effectuer des changements et ensuite ajoute ou met à jour les informations.

Ce chapitre décrit la configuration et l'utilisation de OpenLDAP 2.0, une implémentation Open Source des protocoles LDAPv2 et LDAPv3.

13.1. Pourquoi utiliser LDAP ?

Le principal avantage du protocole LDAP réside dans la possibilité de réunir les informations concernant toute une organisation dans un lieu central. Par exemple, plutôt que de gérer des listes d'utilisateurs pour chaque groupe au sein d'une organisation, LDAP peut être utilisé comme un répertoire central accessible sur tout le réseau. De plus, puisque LDAP prend en charge les fonctions Secure Sockets Layer (SSL) et Transport Layer Security (TLS), des données confidentielles peuvent être protégées contre toute intrusion.

LDAP prend aussi en charge diverses bases de données parallèles pour y enregistrer des répertoires. Ainsi, les administrateurs dispose de la flexibilité nécessaire pour déployer la base de données la plus adaptée au type d'informations que le serveur doit disséminer. De plus, comme LDAP comporte une interface de programmation d'application (ou API de l'anglais Application Programming Interfaces) bien définie, le nombre d'applications compatibles avec LDAP est vaste et croissant aussi bien en quantité qu'en qualité.

13.1.1. Caractéristiques d'OpenLDAP

OpenLDAP comprend un certain nombre de caractéristiques importantes parmi lesquelles figurent :

- *Prise en charge de LDAPv3* — OpenLDAP prend en charge SASL (de l'anglais Simple Authentication and Security Layer), TLS (Transport Layer Security) et SSL (Secure Sockets Layer) entre autres améliorations. De nombreux changements apportés au protocole depuis LDAPv2 visent à augmenter la sécurité de LDAP.
- *Prise en charge de IPv6* — OpenLDAP prend en charge le protocole de la prochaine génération, Internet Protocol version 6.
- *LDAP sur IPC* — OpenLDAP peut communiquer au sein d'un système en utilisant IPC (de l'anglais interprocess communication). Il en résulte une sécurité améliorée car il n'est plus nécessaire de communiquer à travers un réseau.
- *Mise à jour de C API* — Améliore la manière dont les programmeurs se connectent aux serveurs de répertoires LDAP et les utilisent.
- *Prise en charge de LDIFv1* — Grâce à cette prise en charge, OpenLDAP 2.0 est pleinement compatible avec la version 1 du format LDIF (ou LDAP Data Interchange Format).
- *Amélioration du serveur autonome LDAP* — À présent le serveur inclut entre autres un système de contrôle d'accès mis à jour, un pool de conversation et des outils plus performants.

13.2. Terminologie de LDAP

Toute discussion concernant LDAP nécessite une compréhension élémentaire d'un certain nombre de termes spécifiques à LDAP :

- *entrée* — Correspond à une seule unité dans un répertoire LDAP. Chaque entrée (ou entry) est identifiée par son *Nom distinctif ou DN* (de l'anglais Distinguished Name) unique.
- *attributs* — Des attributs (ou attributes en anglais) sont des éléments d'information directement associés à une entrée. Par exemple, une organisation pourrait être représentée en tant qu'une entrée LDAP. Parmi les attributs associés à l'organisation, on pourrait avoir son numéro de fax, son adresse, etc. Des personnes peuvent également être représentées par des entrées dans un répertoire LDAP, avec par exemple des attributs courants tels que le numéros de téléphone de la personne en question et son adresse électronique.

  Certains attributs sont obligatoires, tandis que d'autres sont facultatifs. Une définition de classe d'objets (*objectclass*) détermine les attributs spécifiques qui sont obligatoires pour chaque entrée. Des définitions de classes d'objets figurent dans différents fichiers schéma contenus dans le répertoire `/etc/openldap/schema/`. Pour obtenir de plus amples informations sur le sujet, consultez la Section 13.5.
- *LDIF* — Le format d'échange de données *LDAP Data Interchange Format* (LDIF) est un format de texte ASCII pour les entrées LDAP. Les fichiers qui échangent des données avec des serveurs LDAP doivent avoir le format LDIF. Une entrée LDIF ressemble à l'extrait ci-dessous :

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

  Toute entrée peut contenir autant de paires `<attrtype>: <attrvalue>` quil n'est nécessaire. Une ligne blanche indique que l'entrée est terminée.

Attention

Toutes les paires <*attrtype*> et <*attrvalue*> *doivent* être définies dans un fichier de schéma correspondant pour pouvoir utiliser ces informations.

Toute valeur figurant entre un < et un > représente une variable que vous pouvez paramétrer lorsqu'une nouvelle entrée LDAP est créée. Toutefois, cette règle ne s'applique pas à <*id*>. Cet élément <*id*> représente un nombre paramétré par l'application utilisée pour modifier l'entrée.

13.3. Démons et utilitaires d'OpenLDAP

La suite de bibliothèques et d'outils OpenLDAP est incluse dans les paquetages suivants :

- `openldap` — Contient les bibliothèques nécessaires pour faire fonctionner le serveur OpenLDAP et les applications clientes.
- `openldap-clients` — Contient les outils de ligne de commande pour visualiser et modifier les répertoires d'un serveur LDAP.
- `openldap-servers` — Contient les serveurs et autres utilitaires nécessaires pour configurer et faire fonctionner un serveur LDAP.

Deux serveurs sont contenus dans le paquetage `openldap-servers` : le *démon autonome LDAP* (`/usr/sbin/slapd`) et le *démon autonome LDAP de réplication de mise à jour* (`/usr/sbin/slurpd`).

Le démon `slapd` est un serveur LDAP autonome, tandis que le démon `slurpd` sert à synchroniser les changements d'un serveur LDAP vers les autres serveurs LDAP du réseau. Le démon `slurpd` n'est utilisé que pour des opérations avec de multiples serveurs LDAP.

Pour effectuer des tâches administratives, le paquetage `openldap-servers` installe les utilitaires suivants dans le répertoire `/usr/sbin/` :

- `slapadd` — Ajoute des entrées d'un fichier LDIF dans un répertoire LDAP. Par exemple, la commande `/usr/sbin/slapadd -l ldif-input` lit le fichier LDIF *`ldif-input`* contenant les nouvelles entrées.

Important

Seul le super-utilisateur peut utiliser `/usr/sbin/slapadd`. Toutefois, le serveur de répertoires tourne en tant que l'utilisateur `ldap`. Par conséquent, le serveur de répertoires n'est pas en mesure de modifier un fichier quelconque créé par `slapadd`. Pour résoudre ce problème, après avoir utilisé `slapadd`, tapez la commande suivante :

```
chown -R ldap /var/lib/ldap
```

- `slapcat` — Extrait des données d'un répertoire LDAP dans le format par défaut, à savoir le système *Berkeley DB de Sleepycat Software*, et les enregistre dans un fichier LDIF. Par exemple, la commande `/usr/sbin/slapcat -l ldif-output` renvoie un fichier LDIF nommé *`ldif-output`* qui contient les entrées du répertoire LDAP.
- `slapindex` — Indexe à nouveau le répertoire `slapd` sur la base du contenu actuel. Cet outil devrait être exécuté chaque fois que les options d'indexation de `/etc/openldap/slapd.conf` sont modifiées.
- `slappasswd` — Crée une valeur pour le mot de passe utilisateur crypté devant être utiliser avec `ldapmodify` ou la valeur `rootpw` dans le fichier de configuration de `slapd`, `/etc/openldap/slapd.conf`. Exécutez la commande `/usr/sbin/slappasswd` pour créer le mot de passe.

Avertissement

Vous devez arrêter `slapd` en exécutant la commande `/sbin/service lapd stop` avant d'utiliser `slapadd`, `slapcat` ou `slapindex`. Dans le cas contraire, l'intégrité du répertoire LDAP risque d'être compromise.

Pour obtenir de plus amples informations sur l'utilisation de ces utilitaires, consultez leurs pages de manuel respectives.

Le paquetage `openldap-clients` installe dans `/usr/bin/` des outils permettant d'ajouter, de modifier et de supprimer des entrées dans un répertoire LDAP. Parmi ces outils figurent :

- `ldapadd` — Ajoute des entrées dans un répertoire LDAP en acceptant la saisie d'entrées par le biais d'un fichier ou par une saisie standard ; `ldapadd` est en fait un lien dur vers la commande `ldapmodify -a`.
- `ldapdelete` — Supprime des entrées dans un répertoire LDAP en acceptant la saisie de l'utilisateur à une invite du shell ou par le biais d'un fichier.
- `ldapmodify` — Modifie les entrées dans un répertoire LDAP, acceptant leur saisie par un fichier ou par une saisie standard.
- `ldappasswd` — Définit le mot de passe pour un utilisateur LDAP.
- `ldapsearch` — Recherche des entrées dans un répertoire LDAP en utilisant une invite du shell.

À l'exception de la commande `ldapsearch`, chacun de ces utilitaires est plus facilement utilisé en référencant un fichier contenant les changements à effectuer plutôt qu'en tapant une commande pour chaque entrée devant être modifiée dans le répertoire LDAP. Le format d'un tel fichier est expliqué dans les pages de manuel de chaque utilitaire.

13.3.1. NSS, PAM et LDAP

Outre les paquetages OpenLDAP, Red Hat Enterprise Linux comprend un paquetage nommé `nss_ldap` qui améliore la capacité de LDAP à s'intégrer aussi bien dans un environnement Linux que dans tout autre environnement UNIX.

Le paquetage `nss_ldap` fournit les modules suivants :

- `/lib/libnss_ldap-<`*`glibc-version`*`>.so`
- `/lib/security/pam_ldap.so`

Le paquetage `nss_ldap` fournit les modules suivants pour les architectures Itanium ou AMD64 :

- `/lib64/libnss_ldap-<`*`glibc-version`*`>.so`
- `/lib64/security/pam_ldap.so`

Le module `libnss_ldap-<`*`glibc-version`*`>.so` permet aux applications de rechercher des utilisateurs, des groupes, des hôtes et d'autres informations en utilisant un répertoire LDAP via l'interface *Nameservice Switch* (ou NSS) de glibc (remplacez `<`*`glibc-version`*`>` par la version de `libnss_ldap` utilisée). NSS permet aux applications de s'authentifier en utilisant LDAP de concert avec le service de noms NIS et les fichiers plats d'authentification.

Le module `pam_ldap` permet aux applications fonctionnant avec PAM d'authentifier les utilisateurs en utilisant les informations stockées dans un répertoire LDAP. Les applications fonctionnant avec PAM comprennent la connexion console, les serveurs de messagerie POP et IMAP ainsi que Samba. En déployant un serveur LDAP sur votre réseau, toutes ces applications peuvent, pour leur au-

thentification, utiliser la même combinaison identifiant d'utilisateur/mot de passe, ce qui simplifie considérablement l'administration.

Pour obtenir de plus amples informations sur la configuration des PAM, reportez-vous au Chapitre 16 et aux pages de manuel de PAM.

13.3.2. PHP4, LDAP et le Serveur HTTP Apache

Red Hat Enterprise Linux comprend un paquetage avec un module LDAP pour le langage de scripts PHP côté serveur.

Le paquetage `php-ldap` ajoute la prise en charge LDAP au langage de script PHP4 avec intégration HTML grâce au module `/usr/lib/php4/ldap.so`. Ce module permet aux scripts PHP4 d'accéder aux informations stockées dans un répertoire LDAP.

Red Hat Enterprise Linux est vendu avec le module `mod_authz_ldap` pour le Serveur HTTP Apache. Ce module utilise la forme courte du nom distinct d'un sujet et le fournisseur du certificat SSL client afin de déterminer le nom distinct de l'utilisateur au sein d'un répertoire LDAP. Il est également capable d'autoriser des utilisateurs selon les attributs de l'entrée du répertoire LDAP de cet utilisateur, en déterminant l'accès aux ressources sur la base des privilèges dont disposent l'utilisateur et du groupe sur ces dernières et en refusant l'accès aux utilisateurs dont les mots de passe ont expiré. Le module `mod_ssl` est nécessaire lorsque le module `mod_authz_ldap` est utilisé.

Important

Le module `mod_authz_ldap` n'authentifie pas un utilisateur auprès d'un répertoire LDAP à l'aide d'un mot de passe crypté. Cette fonctionnalité est fournie par le module expérimental nommée `mod_auth_ldap` qui n'est pas inclus dans Red Hat Enterprise Linux. Pour obtenir de plus amples informations sur le statut de ce module, reportez-vous au site Web de l'organisation Apache Software Foundation à l'adresse suivante : http://www.apache.org/.

13.3.3. Applications client LDAP

Il existe des clients LDAP graphiques prennant en charge la création et la modification de répertoires, mais ces applications ne sont *pas* incluses dans Red Hat Enterprise Linux. C'est le cas de l'application **LDAP Browser/Editor** (Navigateur/éditeur LDAP) — Cet outil basé sur Java est disponible en ligne à l'adresse suivante : http://www.iit.edu/~gawojar/ldap/.

La plupart des autres clients LDAP accèdent aux répertoires en lecture-seule et les utilisent pour référencer, et non pas modifier, les informations relatives à toute l'entreprise. Parmi ces applications figurent Sendmail, **Mozilla**, **Gnome Meeting** et **Evolution**.

13.4. Fichiers de configuration d'OpenLDAP

Les fichiers de configuration d'OpenLDAP sont installés dans le répertoire `/etc/openldap/`. Ci-dessous figure une brève liste des répertoires et fichiers les plus importants :

- `/etc/openldap/ldap.conf` — Ce fichier est le fichier de configuration pour toutes les applications *clientes* qui utilisent les bibliothèques OpenLDAP telles que `ldapsearch`, `ldapadd`, Sendmail, **Evolution** et **Gnome Meeting**.

- `/etc/openldap/slapd.conf` — Ce fichier est le fichier de configuration du démon `slapd`. Pour obtenir davantage d'informations sur ce fichier, reportez-vous à la Section 13.6.1.
- Le répertoire `/etc/openldap/schema/` — Ce sous-répertoire contient le schéma utilisé par le démon `slapd`. Pour obtenir davantage d'informations sur ce répertoire, reportez-vous à la Section 13.5.

Remarque

Si le paquetage `nss_ldap` est installé, il crée un fichier nommé `/etc/ldap.conf`. Ce fichier est utilisé par les modules PAM et NSS fournis par le paquetage `nss_ldap`. Pour obtenir davantage d'informations, consultez la Section 13.7.

13.5. Répertoire `/etc/openldap/schema/`

Le répertoire `/etc/openldap/schema/` contient des définitions LDAP précédemment placées dans les fichiers `slapd.at.conf` et `slapd.oc.conf`. Le fichier `/etc/openldap/schema/redhat/` contient des schémas personnalisés distribués par Red Hat pour Red Hat Enterprise Linux.

Toutes les *définitions de syntaxe d'attribut* et *définitions de la classe d'objet* sont maintenant placées dans des fichiers schéma différents. Ces derniers sont référencés dans `/etc/openldap/slapd.conf` en utilisant les lignes `include`, comme dans l'exemple ci-dessous :

```
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/redhat/autofs.schema
```

Attention

Ne modifiez aucun élément schéma défini dans les fichiers schéma installés par OpenLDAP.

Ceci étant, vous pouvez étendre le schéma utilisé par OpenLDAP afin de prendre en charge d'autres types d'attributs et classes d'objets en utilisant comme guide les fichiers schéma par 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 en dessous de vos lignes schéma `include` par défaut :

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

Ensuite, définissez vos nouveaux types d'attributs et classes d'objets dans le fichier `local.schema`. Beaucoup d'organisations utilisent les types d'attributs et classes d'objet existants dans les fichiers schéma installés par défaut et ajoutent de nouvelles classes d'objets dans le fichier `local.schema`.

L'extension d'un schéma pour qu'il corresponde à des besoins spécialisés est une tâche complexe qui dépasse la portée du présent chapitre. Pour obtenir de plus amples d'informations sur le sujet, consultez l'adresse suivante : http://www.openldap.org/doc/admin/schema.html.

13.6. Aperçu de la configuration d'OpenLDAP

Cette section fournit une présentation rapide des opérations à accomplir pour installer et configurer un annuaire OpenLDAP (aussi appelé répertoire). Pour obtenir de plus amples informations sur le sujet, reportez-vous aux URL suivantes :

- http://www.openldap.org/doc/admin/quickstart.html — Le guide rapide pour commencer (*Quick-Start Guide*) sur le site Web d'OpenLDAP.
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — Le document *LDAP Linux HOWTO* du Projet de documentation Linux (Linux Documentation Project) en miroir sur le site de Red Hat.

Ci-dessous figurent les étapes de base pour créer un serveur LDAP :

1. Installez les RPM d'`openldap`, `openldap-servers` et `openldap-clients`.
2. Éditez le fichier `/etc/openldap/slapd.conf` afin de spécifier le domaine et le serveur LDAP. Reportez-vous à la Section 13.6.1 afin d'obtenir davantage d'informations.
3. Lancez `slapd` à l'aide de la commande :
   ```
   /sbin/service ldap start
   ```
   Après avoir configuré LDAP, utilisez `chkconfig`, `ntsysv` ou l'**Outil de configuration des services** pour configurer LDAP de façon à le lancer au démarrage. Pour de plus amples informations sur la configuration des services, consultez le chapitre intitulé *Contrôle de l'accès aux services* du *Guide d'administration système de Red Hat Enterprise Linux*.
4. Ajoutez des entrées à un répertoire LDAP à l'aide de `ldapadd`.
5. Utilisez `ldapsearch` afin de vérifier si `slapd` accède correctement aux informations.
6. À ce stade, le répertoire LDAP devrait fonctionner correctement et peut donc être configuré avec des applications compatibles avec LDAP.

13.6.1. Édition de `/etc/openldap/slapd.conf`

Afin d'utiliser le serveur LDAP `slapd`, modifiez son fichier de configuration, `/etc/openldap/slapd.conf` de façon à spécifier le domaine et le serveur corrects.

La ligne de `suffix` nomme le domaine pour lequel le serveur LDAP fournira les informations et devrait être changée comme suit :

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

de façon à refléter votre nom de domaine. Par exemple :

```
suffix          "dc=example,dc=com"
```

L'entrée `rootdn` est le *Nom distinct* (ou *DN* selon l'acronyme anglais) pour un utilisateur dont l'activité n'est pas limitée par les paramètres de contrôle d'accès ou de limites administratives définis pour toute opération sur le répertoire LDAP. L'utilisateur `rootdn` peut être considéré comme le super-utilisateur pour le répertoire LDAP. Dans le fichier de configuration, modifiez la ligne `rootdn` pour changer la valeur par défaut comme dans l'exemple suivant :

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

Si vous avez l'intention de peupler le répertoire LDAP sur le réseau, modifiez la ligne `rootpw` — en remplaçant la valeur par défaut par une chaîne de mot de passe cryptée. Afin de créer une chaîne de mots de passe cryptée, tapez la commande suivante :

```
slappasswd
```

Lorsque le système vous le emandera, saisissez et confirmez un mot de passe. Le programme affiche alors à l'invite du shell, le mot de passe crypté résulant de la commande.

Ensuite, copiez le mot de passe crypté que vous venez de créer dans `/etc/openldap/slapd.conf` sur une des lignes `rootpw` et supprimez le signe dièse (`#`).

Une fois cette modification apportée, la ligne devrait ressembler à l'exemple reproduit ci-dessous :

```
rootpw {SSHA}vv2y+i6V6esazrIv70xSSnNAJE18bb2u
```

Avertissement

Les mots de passe LDAP, y compris la directive `rootpw` spécifiée dans `/etc/openldap/slapd.conf`, sont envoyés sur le réseau en *texte clair*, à moins que le cryptage TLS ne soit activé.

Pour permettre le cryptage TLS, passez en revue les commentaires figurant dans `/etc/openldap/slapd.conf` et consultez la page de manuel de `slapd.conf`.

Pour une sécurité accrue, la directive `rootpw` devrait être désactivée après avoir peuplé le répertoire LDAP. Pour ce faire, ajoutez un signe dièse devant cette directive (`#`).

Si vous utilisez l'outil de ligne de commande `/usr/sbin/slapadd` localement pour peupler le répertoire, il n'est pas nécessaire d'utiliser la directive `rootpw`.

Important

Seul le super-utilisateur peut utiliser `/usr/sbin/slapadd`. Toutefois, le serveur de répertoires tourne en tant que l'utilisateur `ldap`. Par conséquent, le serveur de répertoires ne peut modifier aucun fichier créé par `slapadd`. Pour résoudre ce problème, après avoir utilisé `slapadd` tapez la commande ci-dessous :

```
chown -R ldap /var/lib/ldap
```

13.7. Configuration d'un système pour l'authentification avec OpenLDAP

Cette section donne un bref aperçu de la manière de configurer l'authentification des utilisateurs à l'aide d'OpenLDAP. À moins d'être un expert d'OpenLDAP, vous aurez probablement besoin de plus de documentation que vous n'en trouverez ici. Reportez-vous aux références fournies dans la Section 13.9 pour obtenir davantage d'informations.

Installez les paquetages LDAP nécessaires

Commencez par vérifier que les paquetages appropriés sont installés aussi biensur le serveur LDAP et que sur les machines LDAP clientes. Le serveur LDAP nécessite le paquetage `openldap-servers`.

Les paquetages `openldap`, `openldap-clients` et `nss_ldap` doivent être installés sur tous les ordinateurs clients LDAP.

Éditez des fichiers de configuration

- Sur le serveur LDAP, éditez le fichier `/etc/openldap/slapd.conf` pour vous assurer qu'il correspond bien aux éléments spécifiques de votre organisation. Pour obtenir des instructions sur la manière d'éditer `slapd.conf`, reportez-vous à la Section 13.6.1.
- Sur les ordinateurs clients, `/etc/ldap.conf` et `/etc/openldap/ldap.conf` doivent contenir le bon serveur et les bonnes informations de la base de recherche pour l'organisation.

  Pour ce faire, lancez l'**Outil de configuration d'authentification** graphique (`system-config-authentication`) et sélectionnez **Activer le support LDAP** sous l'onglet **Informations utilisateur**.

  Vous pouvez également modifier ces fichiers manuellement.
- Sur les ordinateurs clients, le fichier `/etc/nsswitch.conf` doit être édité afin de pouvoir utiliser LDAP.

  Pour ce faire, lancez l'**Outil de configuration d'authentification** (`system-config-authentication`) et sélectionnez **Activer le support LDAP** sous l'onglet **Informations utilisateur**.

  Si vous éditez `/etc/nsswitch.conf` manuellement, ajoutez `ldap` aux lignes appropriées.

  Comme par exemple :

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

13.7.1. PAM et LDAP

Pour faire en sorte que des applications compatibles avec PAM standards utilisent LDAP pour l'authentification, exécutez l'**Outil de configuration d'authentification** (`system-config-authentication`) et sélectionnez **Activer le support LDAP** sous l'onglet **Authentification**. Pour obtenir davantage d'informations sur la configuration de PAM, consultez le Chapitre 16 et les pages de manuel de PAM.

13.7.2. Migration de 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 des informations d'authentification vers un format LDAP.

Remarque

Perl doit 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 le domaine approprié. La valeur par défaut du domaine DNS par défaut devrait être modifiée de manière semblable à l'extrait suivant :

```
$DEFAULT_MAIL_DOMAIN = "example";
```

La base par défaut devrait également être changée, pour ressembler à ceci :

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

Le travail de migration d'une base de données d'utilisateurs vers un format lisible par LDAP incombe à un groupe de scripts de migration installés dans le même répertoire. À l'aide du Tableau 13-1, déterminez le script à utiliser pour la migration de base de données d'utilisateurs.

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

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

Service de noms existant	LDAP fonctionne-t-il ?	Script à utiliser
Fichiers `/etc`	oui	`migrate_all_online.sh`
Fichiers `/etc`	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`

Tableau 13-1. Scripts de migration LDAP

13.8. Migration de répertoires de versions précédentes

Depuis Red Hat Enterprise Linux, OpenLDAP utilise le système Berkeley DB de Sleepycat Software comme format de stockage sur disque pour les répertoires. Des versions précédentes d'OpenLDAP utilisaient le gestionnaire de bases de données GNU (*GNU Database Manager*, *gdbm*). Dans de telles circonstances, et avant de mettre à niveau une implémentation LDAP de Red Hat Enterprise Linux 4, les données LDAP d'origine devraient être préalablement exportéesavant la mise à niveau pour être ensuite importées de nouveau. Cette opération peut être effectuée en suivant les étapes suivantes :

1. Exécutez la commande `/usr/sbin/slapcat -l ldif-output` qui produira un fichier LDIF nommé *`ldif-output`* contenant les entrées du répertoire LDAP, *avant* de mettre à niveau le système d'exploitation.
2. Mettez à niveau le système d'exploitation, en faisant bien attention de ne pas reformater la partition contenant le fichier LDIF.
3. Importez de nouveau le répertoire LDAP sur le format Berkeley DB mis à niveau en exécutant la commande `/usr/sbin/slapadd -l ldif-output`.

13.9. Ressources supplémentaires

Les ressources suivantes fournissent des informations supplémentaires sur LDAP. Il est fortement recommandé de les consulter, en particulier le site Web d'OpenLDAP et le HOWTO LDAP, avant de configurer LDAP sur un ou plusieurs systèmes.

13.9.1. Documentation installée

- `/usr/share/docs/openldap-<numéro-version>` — Contient un document `README` général ainsi que des informations diverses.
- Pages de manuel de LDAP — Il existe un nombre de pages de manuel pour les diverses applications et fichiers de configuration utilisés avec LDAP. La liste suivante contient certaines des pages de manuel les plus importantes.

  Applications client

  - `man ldapadd` — Décrit comment ajouter des entrées à un répertoire LDAP.
  - `man ldapdelete` — Décrit comment supprimer des entrées dans un répertoire LDAP.
  - `man ldapmodify` — Décrit comment modifier des entrées dans un répertoire LDAP.
  - `man ldapsearch` — Décrit comment rechercher des entrées dans un répertoire LDAP.
  - `man ldappasswd` — Décrit comment définir ou modifier le mot de passe d'un utilisateur de LDAP.

  Applications serveur

  - `man slapd` — Décrit les options de ligne de commande pour le serveur LDAP.
  - `man slurpd` — Décrit les options de ligne de commande pour le serveur de réplication LDAP.

  Applications administratives

  - `man slapadd` — Décrit les options de ligne de commande utilisées pour ajouter des entrées dans une base de données `slapd`.
  - `man slapcat` — Décrit les options de ligne de commande utilisées pour générer un fichier LDIF à partir d'une base de données `slapd`.
  - `man slapindex` — Décrit les options de ligne de commande utilisées pour régénérer un index selon le contenu d'une base de données `slapd`.
  - `man slappasswd` — Décrit les options de ligne de commande utilisées pour générer des mots de passe d'utilisateur pour les répertoires LDAP.

  Fichiers de configuration

  - `man ldap.conf` — Décrit le format et les options disponibles au sein du fichier de configuration pour les clients LDAP.
  - `man slapd.conf` — Décrit le format et les options disponibles au sein du fichier de configuration référencé aussi bien par les applications serveur de LDAP (`slapd` et `slurpd`) que par les outils administratifs de LDAP (`slapadd`, `slapcat` et `slapindex`).

13.9.2. Sites Web utiles

- http://www.openldap.org/ — Page d'accueil du projet de l'organisation OpenLDAP. Ce site Web contient de nombreuses informations sur la configuration d'OpenLDAP ainsi que sur la feuille de route future et sur les changements apportés à la version.
- http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html — Document HOWTO complet, pertinent et mis à jour sur LDAP.
- http://www.padl.com/ — Développeurs de `nss_ldap` et `pam_ldap` entre autres outils LDAP utiles.
- http://www.kingsmountain.com/ldapRoadmap.shtml — Feuille de route LDAP de Jeff Hodges contenant des liens vers différents Forums aux questions (FAQ) et des informations importantes concernant le protocole LDAP.
- http://www.newarchitectmag.com/archives/2000/05/wilcox/ — Examen utile de la gestion des groupes sous LDAP.
- http://www.ldapman.org/articles/ — Articles offrant une bonne introduction à LDAP, y compris des méthodes pour concevoir une arborescence de répertoires et personnaliser des structures de répertoire.

13.9.3. Livres sur le sujet

- *OpenLDAP by Example* de John Terpstra et Benjamin Coles ; Prentice Hall.
- *Implementing LDAP* de Mark Wilcox ; Wrox Press, Inc.
- *Understanding and Deploying LDAP Directory Services* de Tim Howes et al. ; Macmillan Technical Publishing

Chapitre 14.

Samba

Samba est une implémentation Open Source du protocole Server Message Block (SMB). Il permet l'interaction sur un réseau de Microsoft Windows®, Linux, UNIX et d'autres systèmes d'exploitation, permettant ainsi l'accès à des fichiers basés sur Windows et à des partages d'imprimantes. L'utilisation de SMB par Samba lui permet d'apparaître comme un serveur Windows aux clients Windows.

14.1. Présentation de Samba

La troisième version principale de Samba, la version 3.0.0, a incorporé de nombreuses améliorations par rapport aux versions précédentes, y compris :

- La possibilité de faire partie d'un domaine Active Directory au moyen de LDAP et Kerberos
- La prise en charge intégrée de Unicode pour l'internationalisation
- La prise en charge de connexions client Microsoft Windows XP Professional aux serveurs Samba sans devoir toucher à la base de registre local
- L'ajout de deux nouveaux documents développés par l'équipe de Samba.org, qui inclut un manuel de référence de plus de 400 pages et un manuel dl'implémentation et d'intégration de plus de 300 pages. Pour obtenir de plus amples informations sur ces titres publiés, reportez-vous à la Section 14.9.3.

14.1.1. Fonctionnalités de Samba

Samba est une application serveur performante et versatile. Même les administrateurs système expérimentés doivent connaître les capacités et limitations de Samba avant de tenter d'effectuer son installation et sa configuration.

Ce que Samba peut accomplir :

- Mettre des arborescences de répertoires et des imprimantes à la disposition de clients Linux, UNIX et Windows
- Aider lors de la navigation du réseau (avec ou sans NetBIOS)
- Authentifier les connexions de domaines Windows
- Fournir la résolution du serveur de noms Windows Internet Name Service (WINS)
- Agir en tant que contrôleur principal de domaine (ou PDC, de l'anglais Primary Domain Controller) de type Windows NT®
- Agir en tant que Contrôleur de Domaine Secondaire (ou BDC, de l'anglais Backup Domain Controller) pour un contrôleur principal (PDC) basé sur Samba
- Agir comme un serveur membre du domaine Active Directory
- Joindre un PDC Windows NT/2000/2003

Ce que Samba ne peut pas effectuer :

- Agir comme un BDC pour un PDC Windows (et vice versa)
- Agir comme le contrôleur d'un domaine Active Directory

14.2. Démons de Samba et services apparentés

La section suivante offre une brève présentation des démons et services de Samba traités de manière individuelle ainsi que des informations sur la manière de les démarrer et de les arrêter.

14.2.1. Présentation des démons

Samba est composé de trois démons (`smbd`, `nmbd` et `winbindd`). Deux services (`smb` et `windbind`) contrôlent la manière selon laquelle les démons sont démarrés et arrêtés et ainsi que d'autres fonctionnalités en relation avec les services. Chaque démon est traité en détail, de même que le service spécifique qui le contrôle.

14.2.1.1. Le démon `smbd`

Le démon serveur `smbd` fournit des services de partage de fichiers et d'impression aux clients Windows. En outre, il est responsable de l'authentification des utilisateurs, du verrouillage des ressources et du partage des données par le biais du protocole SMB. Les ports par défaut sur lesquels le serveur est à l'écoute de tout trafic SMB sont les ports TCP 139 et 445.

Le démon `smbd` est contrôlé par le service `smb`.

14.2.1.2. Le démon `nmbd`

Le démon serveur `nmbd` comprend et répond à toutes les requêtes de service de nom NetBIOS telles que celles produites par SMB/CIFS dans des systèmes basés sur Windows. Parmi ces derniers figurent les clients Windows 95/98/ME, Windows NT, Windows 2000, Windows XP et LanManager. Ce démon joue également un rôle au niveau des protocoles de navigation qui constituent l'affichage du **voisinnage réseau** (Network Neighborhood) de Windows. Le port par défaut sur lequel le serveur attend du trafic NMB est le port UDP 137.

Le démon `nmbd` est contrôlé par le service `smb`.

14.2.1.3. Le démon `winbindd`

Le service `winbind` effectue la résolution entre les informations relatives aux utilisateurs et aux groupes sur un serveur Windows NT et les rend utilisables par des plates-formes UNIX. Cette opération est possible grâce à l'utilisation d'appels RPC de Microsoft, du système PAM (Pluggable AuthenticationModule, ou module d'authentification enfichable) et du NSS (Name Service Switch). Ceci permet aux utilisateurs de domaines Windows NT d'apparaître comme des utilisateurs UNIX sur une machine UNIX. Bien qu'intégré à la distribution Samba, le service `winbind` est contrôlé séparément du service `smb`.

Le démon `winbindd` est contrôlé par le service `winbind` et il n'est pas nécessaire que le service `smb` soit lancé pour que le démon tourne. Étant donné que `winbind` est un service côté client utilisé pour la connexion aux serveurs basés sur Windows NT, une discussion plus approfondie de `winbind` dépasse la portée de ce manuel.

14.2.2. Démarrage et arrêt de Samba

Pour démarrer un serveur Samba, tapez la commande suivante à une invite du shell en étant connecté en tant que super-utilisateur :

```
/sbin/service smb start
```

Important

Pour configurer un serveur membre du domaine, il est nécessaire de faire d'abord partie du domaine ou de l'Active Directory en utilisant la commande `net join` *avant* de démarrer le service `smb`.

Pour arrêter le serveur, tapez la commande suivante à une invite du shell en étant connecté en tant que super-utilisateur :

```
/sbin/service smb stop
```

L'option `restart` est une manière rapide d'arrêter et de redémarrer Samba. Cette option constitue la manière la plus fiable d'appliquer des modifications au niveau de la configuration après avoir édité le fichier de configuration de Samba. Notez bien que l'option de redémarrage (restart) lance le démon même s'il ne tournait pas à l'origine.

Pour redémarrer le serveur, en étant connecté en tant que super-utilisateur, tapez la commande suivante à une invite du shell :

```
/sbin/service smb restart
```

L'option `condrestart` (*redémarrage sous certaines conditions*) ne lance `smb` que s'il est déjà en cours d'exécution. Cette option est utile pour les scripts car elle ne démarre pas le démon s'il n'est pas déjà en cours d'exécution.

Remarque

Lorsque le fichier `smb.conf` est modifié, Samba le recharge automatiquement après quelques minutes. L'exécution manuelle de la commande `restart` ou `reload` est tout aussi efficace.

Pour redémarrer le serveur sous certaines conditions, en tant que super-utilisateur, typez la commande suivante :

```
/sbin/service smb condrestart
```

Un rechargement manuel du fichier `smb.conf` peut être utile en cas d'échec du rechargement automatique par le service `smb`. Pour être certain que le fichier de configuration du serveur Samba est rechargé sans devoir redémarrer le service, en tant que super-utilisateur, typez la commande suivante :

```
/sbin/service smb reload
```

Par défaut, le service `smb` ne démarre *pas* automatiquement à l'amorçage. Pour configurer Samba de sorte qu'il se lance au démarrage, employez un utilitaire initscript, tel que `/sbin/chkconfig`, `/sbin/ntsysv` ou le programme **Outil de configuration des services**. Reportez-vous au chapitre intitulé *Contrôle de l'accès aux services* du *Guide d'administration système de Red Hat Enterprise Linux* pour obtenir de plus amples informations sur ces outils.

14.3. Types de serveurs Samba et fichier `smb.conf`

La configuration de Samba est une opération assez simple. Toutes les modifications apportées à Samba ont lieu dans le fichier de configuration `/etc/samba/smb.conf`. Bien que le fichier par défaut `smb.conf` soit bien documenté, il n'aborde pas des sujets complexes tels que LDAP, Active Directory et les nombreuses implémentations de contrôleurs de domaines.

Les sections suivantes décrivent les différentes manières selon lesquelles un serveur Samba peut être configuré. Gardez bien à l'esprit vos besoins et les modifications devant être apportées au fichier `smb.conf` pour effectuer une configuration réussie.

14.3.1. Serveur autonome

Un serveur autonome peut être le serveur d'un groupe de travail ou un membre de l'environnement d'un groupe de travail. Un serveur autonome n'est pas un contrôleur de domaine et ne joue aucun rôle dans un domaine. Les exemples suivants illustrent plusieurs configurations de sécurité anonyme au niveau du partage et un exemple de configuration de sécurité au niveau de l'utilisateur. Pour obtenir de plus amples informations sur les modes de sécurité au niveau du partage ou au niveau de l'utilisateur, reportez-vous à la Section 14.4.

14.3.1.1. Anonyme en lecture-seule

Le fichier `smb.conf` suivant montre un extrait du fichier de configuration nécessaire pour permettre l'implémentation d'un partage de fichiers anonyme en lecture-seule. Le paramètre `security = share` rend un partage anonyme. Notez bien que les niveaux de sécurité pour un seul serveur Samba ne peuvent pas être mélangé. La directive de sécurité (`security`) est un paramètre global pour Samba qui se trouve dans la section de configuration `[global]` du fichier `smb.conf`.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
security = share

[data]
comment = Documentation Samba Server
path = /export
read only = Yes
guest only = Yes
```

14.3.1.2. Anonyme en lecture/écriture

Le fichier `smb.conf` suivant montre un extrait du fichier de configuration nécessaire pour permettre l'implémentation d'un partage de fichiers anonyme en lecture/écriture. Pour permettre le partage anonyme de fichiers en lecture/écriture, donnez à la directive `read only` (lecture-seule) la valeur `no`. Les directives `force user` et `force group` sont également ajoutées pour appliquer les règles de propriété à tout fichier ajouté et spécifié comme appartenant au partage.

Remarque

Bien qu'il soit possible d'avoir un serveur anonyme en lecture/écriture, un tel choix n'est pas recommandé. Tous fichiers placés dans l'espace de partage, indépendemment de l'utilisateur, sont assignés à la combinaison utilisateur/groupe telle qu'elle est spécifiée dans le fichier `smb.conf` par un utilisateur (`force user`) et un groupe (`force group`) génériques.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
security = share

[data]
```

```
comment = Data
path = /export
force user = docsbot
force group = users
read only = No
guest ok = Yes
```

14.3.1.3. Serveur d'impression anonyme

Le fichier `smb.conf` suivant montre un extrait du fichier de configuration nécessaire pour implémenter un serveur d'impression anonyme. Comme nous l'avons montré, le fait de donner à `browsable` la valeur `no`, n'inclut pas l'imprimante dans la liste **Voisinnage réseau** de Windows. Bien que n'apparaissant pas lors de la navigation, la configuration explicite de l'imprimante est possible. Grâce à la connexion à `DOCS_SRV` en utilisant NetBIOS, le client peut avoir accès à l'imprimante s'il fait également partie du groupe de travail `DOCS`. On suppose également que le client a installé le pilote d'impression local approprié puisque la directive `use client driver` a la valeur `Yes`. Dans ce cas, le serveur Samba n'a aucune responsabilité quant au partage de pilotes d'impression avec le client.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
security = share
printcap name = cups
disable spools= Yes
show add printer wizard = No
printing = cups

[printers]
comment = All Printers
path = /var/spool/samba
guest ok = Yes
printable = Yes
use client driver = Yes
browseable = Yes
```

14.3.1.4. Fichier en lecture/écriture et serveur d'impression sécurisés

Le fichier `smb.conf` suivant montre un extrait du fichier de configuration nécessaire pour implémenter un serveur d'impression sécurisé en lecture/écriture. Le fait de donner à la directive `security` la valeur `user` force Samba à authentifier les connexions client. Remarquez bien que le partage `[homes]` n'a pas de directive `force user` ou `force group`, contrairement au partage `[public]`. Le partage `[homes]` utilise les informations relatives à l'utilisateur authentifié pour la création de tout fichier, contrairement aux directives `force user` et `force group` dans `[public]`.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
security = user
printcap name = cups
disable spools = Yes
show add printer wizard = No
printing = cups

[homes]
```

```
comment = Home Directories
valid users = %S
read only = No
browseable = No

[public]
comment = Data
path = /export
force user = docsbot
force group = users
guest ok = Yes

[printers]
comment = All Printers
path = /var/spool/samba
printer admin = john, ed, @admins
create mask = 0600
guest ok = Yes
printable = Yes
use client driver = Yes
browseable = Yes
```

14.3.2. Serveur membre d'un domaine

Un membre d'un domaine, bien qu'étant semblable à un serveur autonome, est connecté à un contrôleur de domaine (soit Windows, soit Samba) et soumis aux règles de sécurité de ce domaine. Le serveur du département d'une entreprise exécutant Samba et ayant un compte machine sur contrôleur de domaine principal (ou PDC, Primary Domain Controller) est un exemple de serveur membre d'un domaine. Tous les clients du département continuent à s'authentifier auprès du PDC et les profiles du bureau ainsi que les fichiers des politiques réseau sont inclus. La différence est que le serveur du département a la capacité de contrôler les partages au niveau de l'impression et du réseau.

14.3.2.1. Serveur membre du domaine Active Directory

Le fichier `smb.conf` suivant montre un extrait du fichier de configuration nécessaire pour implémenter un serveur membre du domaine Active Directory. Dans notre exemple, Samba non seulement authentifie les utilisateurs pour les services exécutés localement, mais il est également un client de Active Directory. Assurez-vous que le paramètre de votre zone (`realm`) kerberos apparaît bien tout en lettres majuscules (par exemple, `realm = EXAMPLE.COM`). Étant donné que Windows 2000/2003 a besoin de Kerberos pour l'authentification de Active Directory, la directive `realm` est nécessaire. Si Active Directory et Kerberos sont exécutés sur des serveurs différents, il se peut que la directive `password server` soit nécessaire pour permettre la distinction entre les deux.

```
[global]
realm = EXAMPLE.COM
security = ADS
encrypt passwords = yes
# Optional. Use only if Samba cannot determine the Kerberos server automatically.
password server = kerberos.example.com
```

Pour qu'un serveur membre fasse partie d'un domaine Active Directory, il est nécessaire d'effectuer les étapes suivantes :

- Configuration du fichier `smb.conf` sur le serveur membre

- Configuration de Kerberos, y compris le fichier `/etc/krb5.conf`, sur le serveur membre
- Création du compte machine sur le serveur du domaine Active Directory
- Association du serveur membre au domaine Active Directory

Pour créer le compte machine et faire partie de Active Directory de Windows 2000/2003, Kerberos doit tout d'abord être initialisé pour le serveur membre souhaitant faire partie du domaine Active Directory. Pour créer un ticket administratif pour Kerberos, tapez la commande suivante en étant connecté en tant que super-utilisateur (ou root) sur le serveur membre :

```
root# kinit administrator@EXAMPLE.COM
```

La commande `kinit` est un script d'initialisation de Kerberos qui référence le compte administrateur de Active Directory et la zone Kerberos (realm). Étant donné que Active Directory a besoin de tickets Kerberos, `kinit` obtient et met en cache un ticket d'émission de tickets (ou TGT, ticket-granting ticket) Kerberos pour l'authentification client/serveur. Pour obtenir de plus amples informations sur Kerberos, le fichier `/etc/krb5.conf` et la commande `kinit`, reportez-vous au Chapitre 19.

Pour faire partie d'un serveur Active Directory (windows1.example.com), tapez la commande suivante en étant connecté en tant que super-utilisateur (ou root) sur le serveur membre :

```
root# net ads join -S windows1.example.com -U administrator%password
```

Étant donné que la machine `windows1` a été trouvée automatiquement dans la zone Kerberos appropriée (la commande `kinit` a abouti), la commande `net` établit la connexion avec le serveur Active Directory utilisant le compte administrateur et le mot de passe requis. Ainsi, le compte machine est créé sur le serveur Active Directory et les permissions sont accordées pour que le membre du domaine Samba puisse faire partie du domaine.

Remarque

Étant donné que `security = ads` est utilisé, et non pas `security = user`, il n'est pas nécessaire d'utiliser un mot de passe secondaire (backend) tel que `smbpasswd`. Des clients plus anciens ne prenant pas en charge `security = ads` sont authentifiés comme si `security = domain` avait été configuré. Ce changement ne touche pas les fonctionnalités et autorise des utilisateurs locaux qui n'étaient pas inclus auparavant dans le domaine.

14.3.2.2. Serveur membre d'un domaine basé sur Windows NT4

Le fichier `smb.conf` suivant montre un extrait du fichier de configuration nécessaire pour implémenter un serveur membre d'un domaine basé sur Windows NT4. Devenir un serveur membre d'un domaine basé sur Windows NT4 revient en fait comme à se connecter à un Active Directory. La différence essentielle réside dans le fait que les domaines basés sur NT4 n'utilisent pas Kerberos dans leur méthode d'authentification, ce qui simplifie le fichier `smb.conf`. Dans ce cas, le serveur membre de Samba joue le rôle d'une machine intermédiare vers le serveur de domaine basé sur NT4.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
security = domain

[homes]
comment = Home Directories
valid users = %S
```

```
read only = No
browseable = No

[public]
comment = Data
path = /export
force user = docsbot
force group = users
guest ok = Yes
```

Le fait d'avoir Samba comme un serveur membre d'un domaine peut être utile dans de nombreuses situations. Dans certains cas le serveur Samba peut être utilisé à d'autres fins que le partage de fichiers et d'impression. Il peut s'avérer utile de transformer Samba en serveur membre d'un domaine, dans des situations où des applications exclusivement Linux doivent être utilisées dans l'environnement du domaine. Il est utile pour les administrateurs d'effectuer un suivi de toutes les machines faisant partie du domaine, même s'il n'est pas basé sur Windows. Dans le cas où le matériel du serveur basé sur Windows deviendrait obsolète, il est relativement facile de modifier le fichier `smb.conf` pour convertir le serveur en PDC basé sur Samba. Si les serveurs basés sur Windows NT sont mis à niveau vers Windows 2000/2003, le fichier `smb.conf` est facilement modifiable pour inclure les changements d'infrastructure.dans Active Directory, si nécessaire.

Important

Après avoir configuré le fichier `smb.conf`, intégrez le domaine *avant* de démarrer Samba en tapant la commande suivante en étant connecté en tant que super-utilisateur :

```
root# net rpc join -U administrator%password
```

Notez bien que l'option `-S`, qui précise le nom d'hôte du serveur de domaine, ne doit pas obligatoirement être spécifiée dans la commande `net rpc join`. Samba utilise le nom d'hôte spécifié par la directive `workgroup` dans le fichier `smb.conf` plutôt que de demander à ce qu'il soit spécifié explicitement.

14.3.3. Contrôleur de domaine

Un contrôleur de domaine dans Windows NT joue essentiellement le même rôle qu'un service d'information réseau (ou NIS, Network Information Service) dans un environnement Linux. Les contrôleurs de domaine et les serveurs NIS hébergent tous les deux des bases de données d'informations utilisateurs/groupes sur les hôtes, ainsi que sur les services apparentés. Les contrôleurs de domaine sont principalement utilisés pour la sécurité, y compris l'authentification des utilisateurs accédant aux ressources du domaine. Le service qui maintient l'intégrité de la base de données relative aux utilisateurs/groupes s'appelle *gestionnaire des comptes de sécurité* (ou SAM, Security Account Manager). La base de données de SAM est stockée de manière différente dans des systèmes Windows et Linux basés sur Samba, si bien que la réplication de SAM ne peut se faire et que les plates-formes ne peuvent pas être mélangées dans un environnement PDC/BDC.

Dans un environnement Samba, il ne peut y avoir qu'un seul PDC et aucun ou plusieurs BDC.

Important

Samba ne peut pas exister dans l'environnement d'un contrôleur de domaine mélangé Samba/Windows (Samba ne peut pas être un BDC d'un PDC Windows ou vice versa). Autrement, les PDC et BDC de Samba *peuvent* coexister.

14.3.3.1. Contrôleur de domaine principal (PDC, Primary Domain Controller) utilisant `tdbsam`

L'implémentation la plus simple et la plus courante d'un PDC Samba utilise le backend de la base de données de mot de passe nommé `tdbsam`. Conçu dans l'intention de remplacer le backend `smbpasswd` désormais un peu passé, `tdbsam` est doté de nombreuses améliorations qui sont examinées en revue de manière détaillée dans la Section 14.5. La directive `passdb backend` contrôle le backend spécifique devant être utilisé pour le PDC.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
passdb backend = tdbsam
security = user
add user script = /usr/sbin/useradd -m %u
delete user script = /usr/sbin/userdel -r %u
add group script = /usr/sbin/groupadd %g
delete group script = /usr/sbin/groupdel %g
add user to group script = /usr/sbin/usermod -G %g %u
add machine script = \
 /usr/sbin/useradd -s /bin/false -d /dev/null \
 -g machines %u
# The following specifies the default logon script
# Per user logon scripts can be specified in the user
# account using pdbedit
logon script = logon.bat
# This sets the default profile path.
# Set per user paths with pdbedit
logon path = \\%L\Profiles\%U
logon drive = H:
logon home = \\%L\%U
domain logons = Yes
os level = 35
preferred master = Yes
domain master = Yes
idmap uid = 15000-20000
idmap gid = 15000-20000

[homes]
comment = Home Directories
valid users = %S
read only = No
browseable = No
writable = Yes

[public]
comment = Data
path = /export
force user = docsbot
force group = users
```

```
guest ok = Yes

[netlogon]
comment = Network Logon Service
path = /var/lib/samba/netlogon/scripts
admin users = ed, john, sam
guest ok = No
browseable = No
writable = No

# For profiles to work, create a user directory under the
# path shown. mkdir -p /var/lib/samba/profiles/john
[Profiles]
comment = Roaming Profile Share
path = /var/lib/samba/profiles
read only = No
browseable = No
guest ok = Yes
profile acls = Yes

# Other resource shares
...
...
```

Remarque

Si vous avez besoin de plus d'un contrôleur de domaine ou avez plus de 250 utilisateurs, n'utilisez *pas* un backend d'authentification `tdbsam`. Dans ces cas particuliers, il est plutôt recommandé d'utiliser LDAP.

14.3.3.2. Contrôleur de domaine principal (PDC, Primary Domain Controller) utilisant LDAP

L'implémentation la plus performante et la plus flexible d'un PDC Samba se manifeste par sa capacité à avoir un backend pour les mots de passe avec LDAP, qui est est très modulable. Les serveurs de base de donnés LDAP peuvent être utilisés à des fins de redondance et de fail-over en raison de leur réplication sur le BDC Samba. Les groupes de PDC et BDC de LDAP dotés d'une capacité de répartition de charge (load balancing) sont parfaits pour un environnement d'entreprise. D'autre part, les configurations LDAP sont par essence complexes à configurer et à maintenir. Si SSL doit être incorporé à LDAP, le degré de complexité est aussitôt multiplié. Malgré tout, avec une planification précise et prudente, LDAP représente une solution idéale pour des environnements d'entreprise.

Prêtez attention à la directive `passdb backend` ainsi qu'aux spécifications de suffixe avec LDAP. Bien que la configuration de Samba pour LDAP soit relativement simple, l'installation de OpenLDAP elle n'est pas si simple. LDAP devrait être installé et configuré avant que toute configuration de Samba n'ait lieu. Remarquez également que Samba et LDAP ne doivent pas forcément être sur le même serveur pour pouvoir fonctionner. Il est d'ailleurs fortement recommandé de les séparer dans un environnement d'entreprise.

```
[global]
workgroup = DOCS
netbios name = DOCS_SRV
passdb backend = ldapsam:ldap://ldap.example.com
```

```
username map = /etc/samba/smbusers
security = user
add user script = /usr/sbin/useradd -m %u
delete user script = /usr/sbin/userdel -r %u
add group script = /usr/sbin/groupadd %g
delete group script = /usr/sbin/groupdel %g
add user to group script = /usr/sbin/usermod -G %g %u
add machine script = \
 /usr/sbin/useradd -s /bin/false -d /dev/null \
 -g machines %u
# The following specifies the default logon script
# Per user logon scripts can be specified in the
# user account using pdbedit
logon script = scripts\logon.bat
# This sets the default profile path.
# Set per user paths with pdbedit
logon path = \\%L\Profiles\%U
logon drive = H:
logon home = \\%L\%U
domain logons = Yes
os level = 35
preferred master = Yes
domain master = Yes
ldap suffix = dc=example,dc=com
ldap machine suffix = ou=People
ldap user suffix = ou=People
ldap group suffix = ou=Group
ldap idmap suffix = ou=People
ldap admin dn = cn=Manager
ldap ssl = no
ldap passwd sync = yes
idmap uid = 15000-20000
idmap gid = 15000-20000
...

# Other resource shares
...
...
```

Remarque

L'implémentation de LDAP dans ce fichier `smb.conf` suppose qu'un serveur LDAP opérationnel a été installé avec succès sur `ldap.example.com`.

14.3.3.3. Contrôleur de domaine secondaire (BDC, Backup Domain Controller) utilisant LDAP

Un BDC est une partie intégrale de toute solution Samba/LDAP en entreprise. Les fichiers `smb.conf` existant entre le PDC et le BDC sont quasiment identiques, à l'exception de la directive `domain master`. Assurez-vous que la valeur du PDC est bien `Yes` et que celle du BDC est `No`. Si vous avez plusieurs BDC pour un PDC, la directive `os level` est utile pour définir la priorité d'élection du BDC. Plus la valeur est élevée, plus la priorité du serveur est élevée pour les connexions clients.

Remarque

Un BDC peut soit utiliser la base de données LDAP du PDC, soit avoir sa propre base de données LDAP. Cette exemple utilise la base de données LDAP du PDC comme on le voit dans la directive `passdb backend`.

```
[global] workgroup = DOCS
netbios name = DOCS_SRV2
passdb backend = ldapsam:ldap://ldap.example.com
username map = /etc/samba/smbusers
security = user
add user script = /usr/sbin/useradd -m %u
delete user script = /usr/sbin/userdel -r %u
add group script = /usr/sbin/groupadd %g
delete group script = /usr/sbin/groupdel %g
add user to group script = /usr/sbin/usermod -G %g %u
add machine script = \
 /usr/sbin/useradd -s /bin/false -d /dev/null \
 -g machines %u
# The following specifies the default logon script
# Per user logon scripts can be specified in the
# user account using pdbedit
logon script = scripts\logon.bat
# This sets the default profile path.
# Set per user paths with pdbedit
logon path = \\%L\Profiles\%U
logon drive = H:
logon home = \\%L\%U
domain logons = Yes
os level = 35
preferred master = Yes
domain master = No
ldap suffix = dc=example,dc=com
ldap machine suffix = ou=People
ldap user suffix = ou=People
ldap group suffix = ou=Group
ldap idmap suffix = ou=People
ldap admin dn = cn=Manager
ldap ssl = no
ldap passwd sync = yes
idmap uid = 15000-20000
idmap gid = 15000-20000
...

# Other resource shares
...
...
```

14.3.3.4. Contrôleur de domaine principal (PDC, Primary Domain Controller) avec Active Directory

Bien que Samba puisse être membre d'un Active Directory, il ne peut pas fonctionner en tant que contrôleur de domaine Active Directory.

14.4. Modes de sécurité pour Samba

Il existe seulement deux types de modes de sécurité pour Samba, à savoir *share-level* (niveau du partage) et *user-level* (niveau de l'utilisateur) ; collectivement, on fait référence à ces deux modes sous le terme *niveaux de sécurité*. La sécurité au niveau du partage peut être implémentée d'une seule manière alors que la sécurité au niveau de l'utilisateur peut elle être mise en oeuvre de quatre manières différentes. On appelle *modes de sécurité* les différentes manières d'implémenter un niveau de sécurité.

14.4.1. Sécurité au niveau de l'utilisateur

La sécurité au niveau de l'utilisateur est le choix par défaut pour Samba. Même si la directive `security = user` n'est pas présente dans le fichier `smb.conf`, elle est utilisée par Samba. Si le serveur accepte le nom d'utilisateur/mot de passe du client, ce dernier peut alors monter des partages multiples sans devoir saisir un mot de passe à chaque fois. Samba peut aussi accepter des requêtes nom d'utilisateur/mot de passe basées sur les sessions. Le client maintient des contextes d'authentification multiples grâce à l'utilisation d'un identifiant utilisateur unique (ou UID) pour chaque connexion.

Dans `smb.conf`, la directive `security = user` définissant la sécurité au niveau de l'utilisateur est :

```
[GLOBAL]
...
security = user
...
```

14.4.2. Sécurité au niveau du partage

Dans la cas de la sécurité au niveau du partage, le serveur accepte seulement un mot de passe sans demander un nom d'utilisateur explicite de la part du client. Le serveur attend la saisie d'un mot de passe pour chaque partage, indépendemment du nom d'utilisateur. Un certain nombre de rapports indiquent que les clients Microsoft Windows rencontrent des problèmes de compatibilité avec les serveurs implémentant la sécurité au niveau du partage. Les développeurs de Samba découragent fortement l'utilisation de la sécurité au niveau du partage.

Dans `smb.conf`, la directive `security = share` définissant la sécurité au niveau du partage est :

```
[GLOBAL]
...
security = share
...
```

14.4.3. Mode de sécurité domaine (Sécurité au niveau de l'utilisateur)

En mode de sécurité domaine, le serveur Samba dispose d'un compte machine (un compte de confiance pour la sécurité du domaine) qui force toutes les requêtes d'authentification à passer par les contrôleurs de domaine. Le serveur Samba se voit devenir un serveur membre du domaine en utilisant la directive suivante dans `smb.conf` :

```
[GLOBAL]
...
security = domain
workgroup = MARKETING
...
```

14.4.4. Mode de sécurité Active Directory (Sécurité au niveau de l'utilisateur)

Si vous avez un environnement Active Directory, il est possible de faire partie du domaine en tant que membre natif d'Active Directory. Même si une politique de sécurité limite l'utilisation de protocoles d'authentification compatibles avec NT, le serveur Samba peut faire partie d'un ADS à l'aide de Kerberos. Samba en mode membre d'Active Directory peut accepter des tickets Kerberos.

Dans `smb.conf`, les directives suivantes font de Samba un serveur membre d'Active Directory :

```
[GLOBAL]
...
security = ADS
realm = EXAMPLE.COM
password server = kerberos.example.com
...
```

14.4.5. Mode de sécurité serveur (Sécurité au niveau utilisateur)

Le mode de sécurité serveur était auparavant utilisé lorsque Samba n'était pas à même d'agir comme un serveur membre d'un domaine.

Remarque

Il est fortement recommandé de ne *pas* utiliser ce mode étant donné qu'il existe de nombreux inconvénients au niveau de la sécurité.

Dans `smb.conf`, les directives suivantes permettent à Samba de fonctionner en mode sécurité serveur :

```
[GLOBAL]
...
encrypt passwords = Yes
security = server
password server = "NetBIOS_of_Domain_Controller"
...
```

14.5. Bases de données d'informations sur les comptes Samba

La dernière version de Samba offre un certain nombre de nouvelles fonctionnalités parmi lesquelles figurent de nouveaux backends pour les bases de données de mots de passe qui n'étaient pas disponibles auparavant. La version 3.0.0 de Samba prend pleinement en charge toutes les bases de données utilisées dans les versions précédentes de Samba. Toutefois, bien que de nombreux backends soient pris en charge, il se peut que certains ne soient pas appropriés pour une utilisation dans un environnement de production.

14.5.1. Backends à compatibilité ascendante

Texte clair

Les backends en texte clair ne sont rien d'autre que des backends de type `/etc/passwd`. Avec des backends en texte clair, tous les noms d'utilisateur et mots de passe sont transmis de manière non cryptée entre le client et le serveur Samba. Cette méthode n'est pas sûre du tout et son utilisation est par conséquent fortement déconseillée. Il est possible que différents clients Windows se connectant au serveur Samba à l'aide de mots de passe en texte clair ne soient pas en mesure de prendre en charge une telle méthode d'authentification.

`smbpasswd`

`smbpasswd`, un backend populaire employé dans des paquetages précédents de Samba utilise une simple structure de texte ASCII qui inclut le compte LanMan et NT de MS Windows LanMan ainsi que des informations cryptées sur les mots de passe. Il manque au backend `smbpasswd` le stockage des contrôles étendus du Storage Area Manager (SAM) de Windows NT/2000/2003. Le backend `smbpasswd` n'est pas recommandé car il n'est pas facilement modulable et ne comporte aucune information sur Windows, comme les RID (Relative Identifier) pour des groupes basés sur NT. Le backend `tdbsam` résout certes ces problèmes pour une utilisation dans une base de données relativement petite (250 utilisateurs), mais il n'en fait toujours pas une solution de niveau entreprise.

Avertissement

Il est possible que ce type de backend soit abandonné dans les prochaines versions et remplacé par le backend `tdbsam`, qui inclut le contrôle étendu de SAM.

`ldapsam_compat`

Le backend `ldapsam_compat` permet la prise en charge continue de OpenLDAP pour une utilisation avec les versions mises à niveau de Samba. Cette option est idéale pour une migration, mais n'est pas requise. Cet outil sera dans le futur abandonné.

14.5.2. Nouveaux backends

`tdbsam`

Le backend `tdbsam` fournit un backend de base de données idéal pour les serveurs locaux, les serveurs ne nécessitant pas de réplication intégrée de base de données et des serveurs ne nécessitant pas modulabilité ou la complexité de LDAP. Le backend `tdbsam` inclut toutes les informations de la base de données `smbpasswd`, ainsi que les informations de SAM qui n'étaient pas précédemment incluses. L'inclusion des données détaillées de SAM permet à Samba d'implémenter les mêmes contrôles d'accès aux comptes et aux systèmes que ceux en place avec les systèmes basés sur Windows NT/2000/2003.

Le backend `tdbsam` est recommandé pour un maximum de 250 utilisateurs. Des organisations plus grandes nécessitent l'intégration d'Active Directory ou de LDAP en raison des problèmes potentiels qu'il pose au niveau de la modulabilité et de l'infrastructure réseau.

`ldapsam`

Le backend `ldapsam` fournit une excellente méthode d'installation distribuée des comptes pour Samba. LDAP est parfait en raison de sa capacité à répliquer sa base de données sur un nombre quelconque de serveurs grâce au démon `slurpd` d'OpenLDAP. Les bases de données de LDAP sont légères et modulables et sont donc parfaites pour la plupart des organisations, particulièrement les grandes entreprises. LDAP montre certainement la "tendance future" quant à Samba. Les améliorations apportées à LDAP sont ajoutées en permanence à Samba, comme par exemple des manières de réduire les problèmes d'installation et de configuration.

`mysqlsam`

Le backend `mysqlsam` utilise un backend de base de données basé sur MySQL. Cette caractéristique est utile pour les sites qui implémentent déjà MySQL.

`xmlsam`

Le backend `xmlsam` utilise des données sur les comptes et mots de passe qui sont stockées dans un fichier au format XML. Cette méthode peut se révéler utile lors de la migration de différentes bases de données de backends ou de sauvegardes.

14.6. Navigation réseau avec Samba

La *navigation réseau* (Network browsing) est un concept permettant aux serveurs Windows et Samba d'apparaître dans le **Voisinnage réseau** de Windows. Au sein du **Voisinnage réseau** apparaissent des icones qui représentent des serveurs et, lorsque ces icones sont ouvertes, les partages et imprimantes du serveur qui sont disponibles sont affichés.

Les capacités de navigation réseau nécessitent NetBIOS sur TCP/IP. La mise en réseau basée sur NetBIOS utilise la messagerie de diffusion générale (UDP) pour effectuer la gestion de listes de navigation. Sans NetBIOS et WINS comme méthode primaire pour la résolution de noms d'hôtes sur TCP/IP, d'autres méthodes telles que des fichiers statiques (`/etc/hosts`) ou DNS doivent être utilisées.

Un navigateur maître de domaine dresse les listes de navigation à partir des navigateurs maîtres locaux sur tous les sous-réseaux afin que la navigation puisse s'effectuer entre les groupes de travail et les sous-réseaux. De plus, le navigateur maître de domaine devrait de préférence être le navigateur maître local de son propre sous-réseau.

14.6.1. Navigation des groupes de travail

Pour chaque groupe de travail, il ne doit exister qu'un seul navigateur maître de domaine. Il est possible d'avoir un navigateur maître local par sous-réseau sans navigateur maître de domaine, mais cette situation entraîne l'isolement de groupes de travail qui ne peuvent pas se voir. Pour la résolution de noms NetBIOS dans des groupes de travail à travers des sous-réseaux, WINS est nécessaire.

Remarque

Le navigateur maître de domaine peut être la même machine que le serveur WINS.

Il ne peut y avoir qu'un seul navigateur maître de domaine par nom de groupe de travail. Ci-dessous figure un extrait du fichier `smb.conf` dans lequel le serveur Samba est un navigateur maître de domaine.

```
[global]
domain master = Yes
local master = Yes
preferred master = Yes
os level = 35
```

Ci-après figure un extrait du fichier `smb.conf` dans lequel le serveur Samba est un navigateur maître local :

```
[global]
domain master = no
local master = Yes
preferred master = Yes
os level = 35
```

La directive `os level` fonctionne comme un système prioritaire pour les navigateurs maîtres d'un sous-réseau. L'attribution de différentes valeurs garantit que les navigateurs maîtres n'entrent pas en conflit entre eux quant à l'autorité.

Astuce

L'abaissement de la valeur de la directive `os level` entraîne un conflit entre Samba et les autres navigateurs maîtres du même sous-réseau. Plus la valeur est élevée, plus la priorité est élevée. La valeur la plus élevée à laquelle un serveur Windows peut fonctionner est 32. Ceci est une bonne manière de régler les multiples navigateurs maîtres locaux.

Dans certaines situations une machine Windows NT du sous-réseau pourrait être le navigateur maître local. Ci-dessous figure un exemple de configuration de `smb.conf` dans laquelle le serveur Samba n'est pas du tout utilisé pour sa capacité en matière de navigation.

```
[global]
domain master = no
local master = no
preferred master = no
os level = 0
```

Avertissement

Le fait d'avoir de multiples navigateurs maîtres locaux entraîne une compétition entre les serveurs au niveau des requêtes d'élection de navigation. Assurez-vous de ne bien avoir qu'un seul navigateur maître local par sous-réseau.

14.6.2. Navigation de domaine

Par défaut, un PDC Windows NT pour un domaine est également le navigateur maître de domaine pour ce domaine. Un serveur Samba doit être configuré en tant que serveur maître de domaine dans ce type de situation. La navigation réseau échouera peut-être si le serveur Samba exécute WINS en même temps que les autres contrôleurs de domaine en fonctionnement.

Pour les sous-réseaux qui n'incluent pas le PDC de Windows NT, il est possible d'implémenter un serveur Samba en tant que navigateur maître local. La configuration de `smb.conf` pour un navigateur

maître local (ou aucune navigation du tout) dans un environnement de contrôleur de domaine est l'équivalent de la configuration d'un groupe de travail.

14.6.3. WINS (Windows Internetworking Name Server)

Un serveur Samba ou un serveur Windows NT peut fonctionner comme un serveur WINS. Lorsqu'un serveur WINS est utilisé avec NetBIOS activé, les paquets UDP unicast peuvent être routés permettant ainsi la résolution de noms à travers les réseaux. Sans serveur WINS, la diffusion UDP est limitée au sous-réseau local et par conséquent, ne peut pas être routée vers les autres sous-réseaux, groupes de travail ou domaines. Si la reproduction est nécessaire, n'utilisez pas Samba comme votre serveur WINS principal car Samba ne prend pas actuellement en charge la réplication WINS.

Dans un environnement mélangé composé de serveurs NT/2000/2003 et Samba, il est recommandé d'utiliser les capacités WINS de Microsoft. Dans un environnement exclusivement Samba, il est recommandé d'utiliser *un seul* serveur Samba pour WINS.

Ci-dessous figure un extrait du fichier `smb.conf` dans lequel le serveur Samba est utilisé comme un serveur WINS :

```
[global]
wins support = Yes
```

Astuce

Tous les serveurs (y compris Samba) devraient se connecter à un serveur WINS pour la résolution de noms NetBIO. Sans WINS, la navigation n'a lieu que sur le sous-réseau local. En outre, même si une liste pour tout le domaine est obtenue d'une manière ou d'une autre, sans WINS, la résolution des hôtes pour le client n'est pas possible.

14.7. Samba avec la prise en charge du système d'impression CUPS

Samba permet aux machines clientes non seulement de partager les imprimantes reliées au serveur Samba mais il permet également d'envoyer des documents Linux à des partages d'imprimantes Windows. Bien que d'autres systèmes d'impression fonctionnent avec Red Hat Enterprise Linux, CUPS (de l'anglais Common UNIX Print System) est le systèmes d'impression recommandé en raison de son étroite intégration à Samba.

14.7.1. Paramètres simples pour `smb.conf`

L'exemple ci-dessous illustre une configuration très élémentaire de `smb.conf` pour la prise en charge de CUPS :

```
[global]
load printers = Yes
printing = cups
printcap name = cups

[printers]
comment = All Printers
path = /var/spool/samba/print
printer = IBMInfoP
```

```
browseable = No
public = Yes
guest ok = Yes
writable = No
printable = Yes
printer admin = @ntadmins

[print$]
comment = Printer Drivers Share
path = /var/lib/samba/drivers
write list = ed, john
printer admin = ed, john
```

D'autres configurations d'impression plus compliquées sont possibles. Pour une sécurité et confidentialité accrue lors de l'impression de documents importants, les utilisateurs peuvent avoir leur propre spouleur d'impression ne se trouvant pas sur un chemin d'accès public. De la sorte, si un travail d'impression n'aboutit pas, d'autres utilisateurs n'auront pas accès au fichier.

Le partage `print$` contient les pilotes d'impression auxquels les clients peuvent avoir accès s'ils ne sont pas disponibles localement. Le partage `print$` est facultatif et n'est pas forcément nécessaire selon le type d'organisation.

En donnant au paramètre `browseable` la valeur `Yes`, l'imprimante pourra être affichée dans le voisinnage réseau de Windows, à supposé que le serveur Samba soit configuré correctement dans le domaine/groupe de travail.

14.8. Programmes de la distribution Samba

14.8.1. `findsmb`

`findsmb <`*`subnet_broadcast_address`*`>`

Le programme `findsmb` est un script Perl qui permet de recueillir des informations sur les systèmes compatibles avec SMB sur un sous-réseau particulier. Si aucun sous-réseau n'est spécifié, le sous-réseau local est utilisé. Parmi les éléments spécifiés figurent l'adresse IP, le nom, groupe de travail ou nom de domaine NetBIOS, le système d'exploitation et la version.

L'exemple suivant montre la sortie de la commande `findsmb` exécutée en tant qu'un utilisateur valide du système :

`findsmb`

```
IP ADDR       NETBIOS NAME  WORKGROUP/OS/VERSION
------------------------------------------------------------------------
10.1.59.25    VERVE          [MYGROUP] [Unix] [Samba 3.0.0-15]
10.1.59.26    STATION22      [MYGROUP] [Unix] [Samba 3.0.2-7.FC1]
10.1.56.45    TREK          +[WORKGROUP] [Windows 5.0] [Windows 2000 LAN Manager]
10.1.57.94    PIXEL          [MYGROUP] [Unix] [Samba 3.0.0-15]
10.1.57.137   MOBILE001      [WORKGROUP] [Windows 5.0] [Windows 2000 LAN Manager]
10.1.57.141   JAWS          +[KWIKIMART] [Unix] [Samba 2.2.7a-security-rollup-fix]
10.1.56.159   FRED          +[MYGROUP] [Unix] [Samba 3.0.0-14.3E]
10.1.59.192   LEGION        *[MYGROUP] [Unix] [Samba 2.2.7-security-rollup-fix]
10.1.56.205   NANCYN        +[MYGROUP] [Unix] [Samba 2.2.7a-security-rollup-fix]
```

14.8.2. make_smbcodepage

`make_smbcodepage <c|d> <codepage_number> <inputfile> <outputfile>`

Le programme `make_smbcodepage` compile le fichier d'une page de code binaire à partir d'une définition en format texte. L'opération inverse est également permise par la décompilation du fichier d'une page de code binaire en une définition en format texte. Ce programme obsolète fait partie des caractéristiques d'internationalisation appartenant aux versions précédentes de Samba qui sont incluses par défaut dans la version courante de samba.

14.8.3. make_unicodemap

`make_unicodemap <codepage_number> <inputfile> <outputfile>`

Le programme `make_unicodemap` compile des fichiers binaires Unicode à partir de fichiers texte afin que Samba puisse afficher des jeux de caractères qui ne sont pas de type ASCII. Ce programme obsolète faisait partie des caractéristiques d'internationalisation de versions précédentes de Samba qui sont désormais incluses dans la version courante de Samba.

14.8.4. net

`net <protocol> <function> <misc_options> <target_options>`

L'utilitaire `net` est semblable à l'utilitaire `net` utilisé pour Windows et MS-DOS. Le premier argument est utilisé pour spécifier le protocole à utiliser lors de l'exécution d'une commande. L'option *<protocol>* peut être `ads`, `rap` ou `rpc` pour la spécification du type de connexion serveur. Active Directory utilise `ads`, Win9x/NT3 utilise `rap` et Windows NT4/2000/2003 utilise `rpc`. Si le protocole n'est pas précisé, `net` essaie automatiquement de le déterminer.

L'exemple suivant affiche une liste des partages disponibles pour un hôte portant le nom `wakko` :

```
net -l share -S wakko
Password:

Enumerating shared resources (exports) on remote server:


Share name   Type     Description
----------   ----     -----------
data         Disk     Wakko data share
tmp          Disk     Wakko tmp share
IPC$         IPC      IPC Service (Samba Server)
ADMIN$       IPC      IPC Service (Samba Server)
```

L'exemple suivant affiche une liste des utilisateurs Samba pour un hôte portant le nom `wakko` :

```
net -l user -S wakko
root password:

User name             Comment
-----------------------------
andriusb              Documentation
joe                   Marketing
lisa                  Sales
```

14.8.5. `nmblookup`

`nmblookup <options> <netbios_name>`

Le programme `nmblookup` effectue la résolution des noms NetBIOS en adresse IP. Le programme diffuse sa demande sur le sous-réseau local jusqu'à ce que la machine cible réponde.

Ci-après figure un exemple :

```
nmblookup trek
querying trek on 10.1.59.255
10.1.56.45 trek<00>
```

14.8.6. `pdbedit`

`pdbedit <options>`

Le programme `pdbedit` gère les comptes présents dans la base de données de SAM. Tous les backends sont pris en charge, y compris `smbpasswd`, LDAP, NIS+ et la bibliothèque de base de données `tdb`.

Ci-dessous figurent des exemples d'ajout, de suppression et de listage d'utilisateurs :

```
pdbedit -a kristin
new password:
retype new password:
Unix username:        kristin
NT username:
Account Flags:        [U          ]
User SID:             S-1-5-21-1210235352-3804200048-1474496110-2012
Primary Group SID:    S-1-5-21-1210235352-3804200048-1474496110-2077
Full Name:
Home Directory:       \\wakko\kristin
HomeDir Drive:
Logon Script:
Profile Path:         \\wakko\kristin\profile
Domain:               WAKKO
Account desc:
Workstations:
Munged dial:
Logon time:           0
Logoff time:          Mon, 18 Jan 2038 22:14:07 GMT
Kickoff time:         Mon, 18 Jan 2038 22:14:07 GMT
Password last set:    Thu, 29 Jan 2004 08:29:28 GMT
Password can change:  Thu, 29 Jan 2004 08:29:28 GMT
Password must change: Mon, 18 Jan 2038 22:14:07 GMT

pdbedit -v -L kristin
Unix username:        kristin
NT username:
Account Flags:        [U          ]
User SID:             S-1-5-21-1210235352-3804200048-1474496110-2012
Primary Group SID:    S-1-5-21-1210235352-3804200048-1474496110-2077
Full Name:
Home Directory:       \\wakko\kristin
HomeDir Drive:
Logon Script:
Profile Path:         \\wakko\kristin\profile
Domain:               WAKKO
```

```
Account desc:
Workstations:
Munged dial:
Logon time:           0
Logoff time:          Mon, 18 Jan 2038 22:14:07 GMT
Kickoff time:         Mon, 18 Jan 2038 22:14:07 GMT
Password last set:    Thu, 29 Jan 2004 08:29:28 GMT
Password can change:  Thu, 29 Jan 2004 08:29:28 GMT
Password must change: Mon, 18 Jan 2038 22:14:07 GMT

pdbedit -L
andriusb:505:
joe:503:
lisa:504:
kristin:506:

pdbedit -x joe

pdbedit -L
andriusb:505:
lisa:504:
kristin:506:
```

14.8.7. `rpcclient`

`rpcclient <server> <options>`

Le programme `rpcclient` exécute des commandes administratives utilisant les RPC de Microsoft, qui fournissent l'accès aux l'interfaces d'administration graphiques (ou GUI) pour la gestion des systèmes. Ce dernier est le plus souvent utilisé par les utilisateurs expérimentés qui comprennent bien la complexité des RPC de Microsoft.

14.8.8. `smbcacls`

`smbcacls <//server/share> <filename> <options>`

Le programme `smbcacls` modifie les ACL de Windows dans les fichiers et répertoires partagés par le serveur Samba.

14.8.9. `smbclient`

`smbclient <//server/share> <password> <options>`

Le programme `smbclient` est un client UNIX souple qui fournit des fonctionnalités semblables à `ftp`.

14.8.10. `smbcontrol`

`smbcontrol -i <options>`

`smbcontrol <options> <destination> <messagetype> <parameters>`

Le programme `smbcontrol` envoie des messages de contrôle aux démons `smbd` ou `nmbd` en cours d'exécution. L'exécution de `smbcontrol -i` lance la commande de manière interactive jusqu'à ce qu'une ligne blanche ou que la lettre 'q' soit saisie.

14.8.11. `smbgroupedit`

`smbgroupedit <options>`

Le programme `smbgroupedit` établit la correspondance entre les groupes Linux et les groupes Windows. Il permet également à un groupe Linux d'être un groupe de domaine.

14.8.12. `smbmount`

`smbmount <//server/share> <mount_point> <-o options>`

Le programme `smbmount` utilise le programme de bas niveau `smbmnt` pour monter un système de fichiers smbfs (partage Samba). La commande `mount -t smbfs <//server/share> <mount_point> <-o options>` fonctionne également.

Exemple :

```
smbmount //wakko/html /mnt/html -o username=kristin
Password: <password>
[root@yakko /]# ls -l /mnt/html
total 0
-rwxr-xr-x    1 root     root            0 Jan 29 08:09 index.html
```

14.8.13. `smbpasswd`

`smbpasswd <options> <username> <password>`

Le programme `smbpasswd` gère les mots de passe cryptés. Ce programme peut être exécuté aussi bien par un super-utilisateur pour changer le mot de passe d'un utilisateur quelconque que par un utilisateur ordinaire pour changer son propre mot de passe Samba.

14.8.14. `smbspool`

`smbspool <job> <user> <title> <copies> <options> <filename>`

Le programme `smbspool` est une interface compatible avec le système d'impression CUPS pour Samba. Bien qu'il soit conçu pour une utilisation avec des imprimantes CUPS, `smbspool` peut également fonctionner avec des imprimantes non-CUPS.

14.8.15. `smbstatus`

`smbstatus <options>`

Le programme `smbstatus` affiche le statut des connexions actuelles à un serveur Samba.

14.8.16. `smbtar`

`smbtar <options>`

Le programme `smbtar` effectue la sauvegarde et la restauration de fichiers et de répertoires en partage sous Windows sur une bande d'archive locale. Bien que ce programme soit semblable à la commande `tar`, les deux ne sont pas compatibles.

14.8.17. testparm

```
testparm <options> <filename> <hostname IP_address>
```

Le programme `testparm` vérifie la syntaxe du fichier `smb.conf`. Si votre fichier `smb.conf` se trouve dans l'emplacement par défaut (`/etc/samba/smb.conf`), il n'est pas nécessaire de préciser l'emplacement. La spécification du nom d'hôte et de l'adresse IP pour le programme `testparm` permet de vérifier que les fichiers `hosts.allow` et `host.deny` sont bien configurés correctement. Le programme `testparm` affiche également un résumé de vos fichiers `smb.conf` et le rôle du serveur (autonome, domaine, etc.) après avoir effectué les tests. Ce programme est utile lors du débogage étant donné qu'il exclut les commentaires et fournit les informations de manière concise pour des administrateurs expérimentés.

Exemple :

```
testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[tmp]"
Processing section "[html]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
<enter>
# Global parameters
[global]
        workgroup = MYGROUP
        server string = Samba Server
        security = SHARE
        log file = /var/log/samba/%m.log
        max log size = 50
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        dns proxy = No

[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /var/spool/samba
        printable = Yes
        browseable = No

[tmp]
        comment = Wakko tmp
        path = /tmp
        guest only = Yes

[html]
        comment = Wakko www
        path = /var/www/html
        force user = andriusb
        force group = users
        read only = No
        guest only = Yes
```

14.8.18. `testprns`

`testprns <printername> <printcapname>`

Le programme `testprns` vérifie si `printername` est une option valide et qu'elle existe dans le fichier `printcap`. Si `printcapname` n'est pas spécifiée, la valeur par défaut précisée dans les fichiers de configuration de Samba ou de `printcap` est la valeur utilisée.

14.8.19. `wbinfo`

`wbinfo <options>`

Le programme `wbinfo` affiche des informations du démon `winbindd`. Logiquement, le démon `winbindd` doit être en cours d'exécution pour que `wbinfo` fonctionne.

14.9. Ressources supplémentaires

Les sections suivantes offrent la possibilité d'explorer Samba de manière plus détaillée.

14.9.1. Documentation installée

- `/usr/share/doc/samba-<version-number>/` — Tous les fichiers supplémentaires inclus dans la distribution de Samba. Parmi ces derniers figurent entre autres tous les scripts d'aide, des exemples de fichiers de configuration et de la documentation.

14.9.2. Documentation de Red Hat

- *Guide d'administration système de Red Hat Enterprise Linux* ; Red Hat, Inc. — Le chapitre *Samba* explique comment configurer un serveur Samba.

14.9.3. Livres sur le sujet

- *The Official Samba-3 HOWTO-Collection* de John H. Terpstra et Jelmer R. Vernooij ; Prentice Hall — La documentation officielle en anglais de Samba-3, telle qu'elle est publiée par l'équipe de développement de Samba. Il s'agit plus d'un guide de référence que d'un guide étape par étape.
- *Samba-3 by Example*de John H. Terpstra; Prentice Hall — Une autre version officielle en anglais publiée par l'équipe de développement de Samba qui fournit des exemples détaillées d'OpenLDAP, DNS, DHCP et des fichiers de configuration d'impression. Ce document contient des informations élémentaires en relation avec le sujet qui sont d'une grande aide lors d'une implémentation proprement dite.
- *Using Samba, 2nd Edition* de Jay T's, Robert Eckstein, et David Collier-Brown ; O'Reilly — Une bonne ressource aussi bien pour les débutants que pour les utilisateurs expérimentés, incluant des documents de référence détaillés.

14.9.4. Sites Web utiles

- http://www.samba.org/ — Page d'accueil de la distribution Samba où se trouve toute documentation officielle créée par l'équipe de développement de Samba. De nombreuses ressources sont disponibles en formats HTML et PDF, alors que d'autres ne sont disponibles qu'en les achetant. Bien qu'un certain nombre de ces liens ne soient pas spécifiques à Red Hat Enterprise Linux, certains concepts sont tout à fait applicables.
- http://samba.org/samba/archives.html — Listes des emails actifs en relation avec la communauté Samba. Il est recommandé d'activer le mode groupé (digest) car les listes sont très actives.
- Forums Samba — Divers forums Samba organisés en fils de discussion (ou thread), tels que gmane.org, utilisant le protocole NNTP sont également disponibles. Ces forums sont une alternative à la réception d'emails venant des listes de diffusion.
- http://samba.idealx.org/ — Idealx.org distribue des scripts d'installation et de configuration pour l'intégration de Samba et OpenLDAP. Ces derniers sont fortement recommandés pour aider à gérer les ressources associées à LDAP. Ces scripts se trouvent à l'emplacement suivant : `/usr/share/doc/samba-3.0.3/LDAP/smbldap-tools` mais peuvent également être téléchargés depuis le site Web de Idealx.

Chapitre 15.

FTP

FTP (de l'anglais File Transfer Protocol) est l'un des protocoles les plus anciens et les plus utilisés que l'on trouve sur Internet de nos jours. Son but est de transférer de manière sécurisée des fichiers entre les ordinateurs hôtes d'un réseau sans que l'utilisateur ne doive se connecter directement à l'hôte distant ou ne doive savoir comment utiliser le système distant. Ce protocole permet aux utilisateurs d'accéder à des fichiers sur des systèmes distants en utilisant un ensemble standard de commandes simples.

Ce chapitre présente les éléments de base du protocole FTP ainsi que les options de configuration pour le serveur FTP primaire inclus dans Red Hat Enterprise Linux, `vsftpd`.

15.1. Protocole FTP (File Transport Protocol)

FTP utilise une architecture de serveur client pour transférer des fichiers à l'aide du protocole réseau TCP. Étant donné que FTP est un protocole relativement ancien, il utilise une authentification basée sur un nom d'utilisateur et un mot de passe non-cryptés. Telle est la raison pour laquelle ce protocole est considéré comme vulnérable au niveau de la sécurité et que son utilisation est déconseillée à moins qu'elle ne soit essentielle. Une bonne alternative à FT existe avec `sftp`, de la suite d'outils OpenSSH. Pour obtenir des informations sur la configuration d'OpenSSH, reportez-vous au chapitre intitulé *OpenSSH* du *Guide d'administration système de Red Hat Enterprise Linux*. Pour de plus amples informations sur le protocole SSH, reportez-vous au Chapitre 20.

Toutefois, en raison de l'utilisation très répandue de FTP sur Internet, il est souvent nécessaire de partager des fichiers avec le public. Les administrateurs système devraient donc être conscients des caractéristiques uniques du protocole FTP.

15.1.1. Ports multiples, Modes multiples

Contrairement à la plupart des protocoles utilisés sur Internet, FTP a besoin de multiples ports réseau afin de pouvoir fonctionner correctement. Lorsqu'une application FTP client établit une connexion avec un serveur FTP, elle ouvre le port 21 sur le serveur — appelé *port de commande*. Ce port est utilisé pour exécuter toutes les commandes destinées au serveur. Toute donnée requise du serveur est renvoyée au client via un *port de données*. Le numéro de port pour les connexions aux données et la manière selon laquelle les connexions aux données sont effectuées varient selon que le client demande les données en mode *actif* ou en mode *passif*.

Ces modes sont définis de la manière suivante :

mode actif

Le mode actif représente la méthode utilisée à l'origine par le protocole FTP pour transférer des données à l'application cliente. Lorsqu'un transfert de données en mode actif est engendré par le client FTP, le serveur établit une connexion depuis le port 20 sur le serveur vers l'adresse IP et un port aléatoire, non-privilégié (supérieur à 1024) spécifié par le client. Dans une telle situation, l'ordinateur client doit être autorisé à accepter des connexions sur tout port supérieur à 1024. Avec le nombre croissant de réseaux non-sécurisés, tels que l'Internet, l'utilisation de pare-feu pour protéger les ordinateurs clients est désormais très répandue. Étant donné que ces pare-feu côté client refusent souvent les connexions entrantes originaires de serveurs FTP en mode actif, il est recommandé d'utiliser le mode passif.

mode passif

Le mode passif, tout comme le mode actif, est engendré par l'application client FTP. Lors d'une demande de données auprès du serveur, le client FTP indique qu'il souhaite accéder aux données en mode passif et le serveur fournit une adresse IP et un port aléatoire, non-privilégié (supérieur à 1024) sur le serveur. Le client se connecte alors à ce port sur le serveur afin de télécharger les informations demandées.

Alors que le mode passif résout les problèmes d'interférence du pare-feu côté client avec des connexions aux données, il peut rendre plus complexe l'administration du pare-feu côté serveur. En limitant dans le fichier de configuration du serveur FTP, l'éventail des ports non-privilégiés disponibles pour des connexions passives, il est possible de restreindre le nombre de ports ouverts sur un serveur, ce qui permet également de simplifier la création de règles de pare-feu pour le serveur. Reportez-vous à la Section 15.5.8 pour obtenir de plus amples informations sur la manière de limiter le nombre de ports passifs.

15.2. Serveurs FTP

Red Hat Enterprise Linux est fourni avec deux serveurs FTP différents :

- **Accélérateur de contenu Red Hat** — Un serveur Web basé sur le noyau qui fournit un serveur Web haute performance et des services FTP. Étant donné que le but de sa conception est à l'origine la vitesse, ses fonctionnalités sont limitées et son fonctionnement n'est possible que comme serveur FTP anonyme. Pour obtenir de plus amples informations sur la configuration et l'administration de l'**Accélérateur de contenu Red Hat**, consultez la documentation disponible en ligne à l'adresse suivante : http://www.redhat.com/docs/manuals/tux/.
- `vsftpd` — Un démon FTP sécurisé et rapide qui est le serveur FTP préféré pour Red Hat Enterprise Linux. Le reste de ce chapitre se concentre sur `vsftpd`.

15.2.1. `vsftpd`

Le démon `vsftpd` (acronyme de Very Secure FTP Daemon) est conçu pour être rapide, stable et surtout sécurisé du point de branchement à l'utilisateur final. Sa capacité à traiter un grand nombre de connexions de manière efficace et sécurisée explique la raison pour laquelle `vsftpd` est le seul FTP autonome distribué avec Red Hat Enterprise Linux.

Le modèle de sécurité utilisé par `vsftpd` possède trois caractéristiques essentielles, à savoir :

- *Séparation claire entre les processus privilégiés et les processus non-privilégiés* — Des processus différents traitent différentes tâches et chacun de ces derniers fonctionne avec le minimum de privilèges nécessaires pour la tâche à exécuter.
- *Les tâches demandant un degré élevé de privilèges sont traitées par des processus dotés du minimum de privilèges nécessaires* — En contrôlant les compatibilités, contenues dans la bibliothèque `libcap`, des tâches qui nécessitent généralement l'ensemble des privilèges root peuvent être exécutées de manière plus sûre depuis un processus doté de privilèges moins étendus.
- *La plupart des processus sont exécutés dans une prison `chroot`* — Autant que possible, le répertoire root des processus devient le répertoire partagé ; ce répertoire est alors considéré comme une prison `chroot`. Par exemple, si le répertoire `/var/ftp/` est le répertoire partagé primaire, `vsftpd` réassigne alors `/var/ftp/` au nouveau répertoire root, `/`. Cette situation empêche toute activité de la part de pirates malintentionnés sur les répertoires qui ne sont pas présents sous le nouveau répertoire root.

L'utilisation de ces pratiques de sécurité entraîne les conséquences suivantes sur la manière dont `vsftpd` traite les requêtes :

- *Le processus parent tourne avec le moins de privilèges requis.* — Le processus parent calcule dynamiquement le degré de privilèges dont il a besoin pour minimiser le degré de risque. Les processus enfants traitent l'interaction directe avec les clients FTP et tournent avec aussi peu de privilèges que possible.
- *Toutes les opérations nécessitant un degré élevé de privilèges sont traitées par un petit processus parent* — D'une manière semblable à Serveur HTTP Apache, `vsftpd` lance des processus enfants non-privilégiés pour le traitement des connexions entrantes. Ce faisant, le processus parent privilégié peut être aussi petit que possible et traiter relativement peu de tâches.
- *Le processus parent se méfie de toutes les requêtes provenant de processus enfants non-privilégiés* — Toute communication avec des processus enfants est reçue sur un socket et la validité de toute information provenant de processus enfants est vérifiée avant que toute opération ne soit exécutée.
- *La plupart de l'interaction avec les clients FTP est traitée par des processus enfants non-privilégiés dans une prison `chroot`* — Étant donné que ces processus enfants ne sont pas privilégiés et n'ont accès qu'au répertoire partagé, tout processus planté ne permet à un agresseur d'accéder qu'aux fichiers partagés.

15.3. Fichiers installés avec `vsftpd`

Le RPM `vsftpd` installe sur le système le démon (`/usr/sbin/vsftpd`), son fichier de configuration et tout fichier connexe, ainsi que les répertoires FTP. Ci-après figure une liste des fichiers et répertoires le plus souvent utilisés pour la configuration de `vsftpd` :

- `/etc/rc.d/init.d/vsftpd` — Le *script d'initialisation* (*initscript*) utilisé par la commande `/sbin/service` pour utiliser, arrêter ou recharger `vsftpd`. Reportez-vous à la Section 15.4 pour obtenir de plus amples informations sur l'utilisation de ce script.
- `/etc/pam.d/vsftpd` — Le fichier de configuration du module d'authentification enfichable ou PAM (de l'anglais Pluggable Authentication Modules) de `vsftpd`. Ce fichier définit les conditions qu'un utilisateur doit satisfaire pour pouvoir se connecter au serveur FTP. Pour obtenir de plus amples informations, reportez-vous au Chapitre 16.
- `/etc/vsftpd/vsftpd.conf` — Le fichier de configuration de `vsftpd`. Reportez-vous à la Section 15.5 pour obtenir une liste des options importantes présentes dans ce fichier.
- `/etc/vsftpd.ftpusers` — Une liste des utilisateurs qui ne sont pas autorisés à se connecter à `vsftpd`. Par défaut, cette liste inclut entre autres les utilisateurs `root`, `bin` et `daemon`.
- `/etc/vsftpd.user_list` — Ce fichier peut être configuré de manière à refuser ou permettre l'accès aux utilisateurs faisant partie de la liste, selon que la directive `userlist_deny` a pour valeur `YES` (par défaut) ou `NO` dans `/etc/vsftpd/vsftpd.conf`. Si `/etc/vsftpd.user_list` est utilisé pour accorder l'accès aux utilisateurs, les noms d'utilisateur *ne doivent pas* apparaître dans `/etc/vsftpd.ftpusers`.
- `/var/ftp/` — Le répertoire contenant les fichiers fournis par `vsftpd`. Il contient également le répertoire `/var/ftp/pub/` pour les utilisateurs anonymes. Les deux répertoires sont lisibles par tout un chacun, mais sont uniquement modifiables par l'utilisateur root.

15.4. Démarrage et arrêt de `vsftpd`

Le RPM `vsftpd` installe le script `/etc/rc.d/init.d/vsftpd` qui est accessible à l'aide de la commande `/sbin/service`.

Pour démarrer le serveur, connectez-vous en tant que super-utilisateur et tapez la commande suivante :

```
/sbin/service vsftpd start
```

Pour arrêter le serveur, connectez-vous en tant que super-utilisateur et tapez la commande suivante :

```
/sbin/service vsftpd stop
```

L'option `restart` représente une manière raccourcie d'arrêter et de démarrer ensuite `vsftpd`. Cette méthode représente la manière la plus efficace d'appliquer des changements apportés au niveau de la configuration, suite à la modification du fichier de configuration de `vsftpd`.

Pour redémarrer le serveur, connectez-vous en tant que super-utilisateur et tapez la commande suivante :

```
/sbin/service vsftpd restart
```

L'option `condrestart` (ou redémarrage conditionnel de l'anglais *conditional restart*) ne démarre `vsftpd` que s'il est actuellement en cours d'exécution. Cette option est utile pour les scripts car elle ne démarre pas le démon s'il n'est pas en cours d'exécution.

Pour redémarrer conditionnellement le serveur, connectez-vous en tant que super-utilisateur et tapez la commande suivante :

```
/sbin/service vsftpd condrestart
```

Par défaut, le service `vsftpd` *n'est pas lancé* automatiquement au démarrage. Pour configurer le service `vsftpd` de sorte qu'il soit amorcé lors du démarrage, utilisez un utilitaire initscript tel que `/sbin/chkconfig`, **/sbin/ntsysv** ou le programme de l'**Outil de configuration des services**. Reportez-vous au chapitre intitulé *Contrôle de l'accès aux services* du *Guide d'administration système de Red Hat Enterprise Linux* pour obtenir de plus amples informations sur ces outils.

15.4.1. Démarrage de multiples copies de `vsftpd`

Parfois, un ordinateur est utilisé pour fournir de multiples domaines FTP. Cette technique est appelée *multihoming* (aussi appeleé hébergement multidomaines). Une possibilité d'effectuer du multihoming à l'aide de `vsftpd` consiste à exécuter de multiples copies du démon, chacune disposant de son propre fichier de configuration.

Pour ce faire, assignez d'abord les adresses IP appropriées aux périphériques réseau ou aux alias des périphériques réseau du système. Reportez-vous au chapitre intitulé *Configuration réseau* du *Guide d'administration système de Red Hat Enterprise Linux* pour obtenir de plus amples informations sur la configurations des périphériques réseau et des alias de périphériques réseau. Des informations supplémentaires sur les scripts de configuration réseau sont également disponibles dans le Chapitre 8.

Ensuite, assurez-vous que le serveur DNS pour les domaines FTP est bien configuré pour référencer le bon ordinateur. Si le serveur DNS tourne sur Red Hat Enterprise Linux, reportez-vous au chapitre intitulé *Configuration de BIND* du *Guide d'administration système de Red Hat Enterprise Linux* afin d'obtenir des instructions sur l'utilisation de l'**Outil de configuration du service de noms de domaines** (`system-config-bind`). Pour obtenir de plus amples informations sur BIND et ses fichiers de configuration, consultez le Chapitre 12.

Pour que `vsftpd` réponde à des requêtes sur des adresses IP, il est nécessaire que de multiples copies du démon tournent. La première copie doit être exécutée à l'aide des initscripts de `vsftpd`, comme il l'est décrit dans la Section 15.4. Cette copie utilise le fichier de configuration standard, `/etc/vsftpd/vsftpd.conf`.

Chaque site FTP supplémentaire doit avoir un fichier de configuration portant un nom unique dans le répertoire `/etc/vsftpd/`, comme `/etc/vsftpd/vsftpd-site-2.conf`. Chaque fichier de configuration ne doit être lisible et modifiable que par le super-utilisateur. Au sein de chaque fichier de configuration relatif à chaque serveur FTP écoutant sur un réseau IPv4, la directive suivante doit être unique :

```
listen_address=N.N.N.N
```

Remplacez *N.N.N.N* par l'adresse IP *unique* du site FTP fourni. Si le site utilise IPv6, employez plutôt la directive `listen_address6`.

Une fois que chaque serveur supplémentaire est doté d'un fichier de configuration, le démon `vsftpd` doit être exécuté depuis une invite du shell root à l'aide de la commande suivante :

```
vsftpd /etc/vsftpd/<configuration-file> &
```

Dans la commande ci-dessus, remplacez *<configuration-file>* par le nom unique du fichier de configuration du serveur, tel que `/etc/vsftpd/vsftpd-site-2.conf`.

Parmi d'autres directives pouvant faire l'objet de modifications sur une base individuelle pour chaque serveur figurent :

- `anon_root`
- `local_root`
- `vsftpd_log_file`
- `xferlog_file`

Pour obtenir une liste détaillée des directives disponibles dans le fichier de configuration de `vsftpd`, reportez-vous à la Section 15.5.

Pour configurer tout serveur supplémentaire afin qu'il s'exécute automatiquement au démarrage, ajoutez la commande ci-dessus à la fin du fichier de configuration `/etc/rc.local`.

15.5. Options de configuration de `vsftpd`

Bien que `vsftpd` n'offre pas forcément le même degré de personnalisation que d'autres serveurs FTP courants, il fournit suffisamment d'options pour répondre aux besoins de la plupart des administrateurs. Étant donné que sa gamme de fonctionnalités n'est pas excessivement vaste, les erreurs pragmatiques et de configuration sont plus restreintes.

Toute configuration de `vsftpd` est traitée par son fichier de configuration, `/etc/vsftpd/vsftpd.conf`. Chaque directive apparaît sur sa propre ligne au sein du fichier et suit le format suivant :

```
<directive>=<value>
```

Pour chaque directive, remplacez d'une part *<directive>* par une directive valide et d'autre part *<value>* par une valeur valide.

Important

Dans une directive, aucun espace ne doit figurer entre la *<directive>*, le signe égal et l'élément *<value>*.

Les lignes de commentaire doivent être précédées par un signe dièse (`#`) et ne sont pas prises en compte par le démon.

Pour obtenir une liste complète de toutes les directives disponibles, reportez-vous à la page de manuel de `vsftpd.conf`.

Important

Pour obtenir un aperçu des différentes manières de sécuriser `vsftpd`, reportez-vous au chapitre intitulé *Sécurité de serveur* du *Guide de sécurité de Red Hat Enterprise Linux*.

Ci-dessous figure une liste des directives les plus importantes présentes dans `/etc/vsftpd/vsftpd.conf`. Toute directive ne se trouvant pas explicitement dans le fichier de configuration de `vsftpd` se voit attribuer la valeur par défaut.

15.5.1. Options pour le démon

Ci-dessous figure une liste des directives contrôlant le comportement général du démon `vsftpd`.

- `listen` — Lorsque cette option est activée, `vsftpd` est exécuté en mode autonome. Red Hat Enterprise Linux lui attribue la valeur `YES`. Cette directive ne peut pas être utilisée de concert avec la directive `listen_ipv6`.

  La valeur par défaut est `NO`.

- `listen_ipv6` — Lorsque cette option est activée, `vsftpd` est exécuté en mode autonome, mais n'écoute que l'interface de connexion (ou socket) IPv6. Cette directive ne peut pas être utilisée de concert avec la directive `listen`.

  La valeur par défaut est `NO`.

- `session_support` — Lorsque cette option est activée, `vsftpd` tente de maintenir les sessions de connexion pour chaque utilisateur par le biais de modules d'authentification enfichables (ou PAM). Reportez-vous au Chapitre 16 pour obtenir de plus amples informations. Si l'ouverture de sessions n'est pas nécessaire, la désactivation de cette option permet à `vsftpd` de tourner avec moins de processus et avec des privilèges moindres.

  La valeur par défaut est `YES`.

15.5.2. Options de connexion et contrôles d'accès

Ci-dessous figure une liste des directives contrôlant le comportement de connexion et les mécanismes de contrôle d'accès.

- `anonymous_enable` — Lorsque cette option est activée, des utilisateurs anonymes sont autorisés à se connecter. Les noms d'utilisateurs anonymes (dits `anonymous`) et `ftp` sont acceptés.

  La valeur par défaut est `YES`.

  Reportez-vous à la Section 15.5.3 pour obtenir une liste des directives ayant un impact sur les utilisateurs anonymes.

- `banned_email_file` — Si la directive `deny_email_enable` a pour valeur `YES`, elle spécifie le fichier contenant une liste de mots de passe de messagerie anonymes pour lesquels l'accès au serveur est refusé.

  La valeur par défaut est `/etc/vsftpd.banned_emails`.

- `banner_file` — Spécifie le fichier contenant le texte affiché lorsqu'une connexion est établie avec le serveur . Cette option écrase tout texte spécifié dans la directive `ftpd_banner`.

  Il n'existe pas de valeur par défaut pour cette directive.

- `cmds_allowed` — Spécifie une liste de commandes FTP, séparées les unes des autres par des virgules, qui permises par le serveur. Toutes les autres commandes sont refusées.

Il n'existe pas de valeur par défaut pour cette directive.

- `deny_email_enable` — Lorsque cette option est activée, tout utilisateur anonyme employant des mots de passe de messagerie spécifiés dans `/etc/vsftpd.banned_emails` se voit refuser l'accès au serveur. Le nom du fichier référencé par cette directive peut être spécifié à l'aide de la directive `banned_email_file`.

  La valeur par défaut est `NO`.

- `ftpd_banner` — Lorsque cette option est activée, la chaîne spécifiée dans cette directive est affichée lorsque qu'une connexion au serveur est établie. Cette option peut être annulé par la directive `banner_file`.

  Par défaut, `vsftpd` affiche sa bannière standard.

- `local_enable` — Lorsque cette option est activée, les utilisateurs locaux sont autorisés à se connecter au système.

  La valeur par défaut est `YES`.

  Reportez-vous à la Section 15.5.4 pour obtenir une liste des directives ayant un impact sur les utilisateurs locaux.

- `pam_service_name` — Spécifie le nom du service PAM pour `vsftpd`.

  La valeur par défaut est `ftp`. Notez que sous Red Hat Enterprise Linux, cette valeur est `vsftpd`.

- `tcp_wrappers` — Lorsque cette option est activée, les enveloppeurs TCP sont utilisés pour accorder l'accès au serveur. De plus, si le serveur FTP est configuré sur de multiples adresses IP, l'option `VSFTPD_LOAD_CONF` peut être utilisée pour charger des fichiers de configuration différents en fonction de l'adresse IP demandée par le client. Pour obtenir de plus amples informations sur les enveloppeurs TCP, reportez-vous au Chapitre 17.

  La valeur par défaut est `NO`. Notez que, sous Red Hat Enterprise Linux, la valeur est `YES`.

- `userlist_deny` — Lorsque cette option est utilisée de concert avec la directive `userlist_enable` et que sa valeur est `NO`, tous les utilisateurs locaux se voient refuser l'accès à moins que le nom d'utilisateur ne figure dans le fichier spécifié par la directive `userlist_file`. Étant donné que l'accès est refusé avant même que le client ne puisse saisir son mot de passe, le choix de la valeur `NO` pour cette directive empêche les utilisateurs de soumettre des mots de passe non-cryptés sur le réseau.

  La valeur par défaut est `YES`.

- `userlist_enable` — Lorsque cette option est activée, les utilisateurs mentionnés dans le fichier spécifiés par la directive `userlist_file` se voient refuser l'accès. Étant donné que l'accès est refusé avant même que le client ne puisse saisir son mot de passe, les utilisateurs n'ont pas la possibilité de soumettre des mots de passe non-cryptés sur le réseau.

  La valeur par défaut est `NO`, cependant, sous Red Hat Enterprise Linux la valeur donnée est `YES`.

- `userlist_file` — Spécifie le fichier référencé par `vsftpd` lorsque la directive `userlist_enable` est activée.

  La valeur par défaut est `/etc/vsftpd.user_list` ; cette dernière est créée durant l'installation.

- `cmds_allowed` — Spécifie une liste de commandes FTP, séparées les unes des autres par des virgules, que le serveur autorise. Toutes les autres commandes sont refusées.

  Il n'existe pas de valeur par défaut pour cette directive.

15.5.3. Options pour les utilisateurs anonymes

Ci-dessous figure une liste des directives qui contrôlent l'accès des utilisateurs anonymes au serveur. Pour utiliser ces options, la valeur de la directive `anonymous_enable` doit être `YES`.

- `anon_mkdir_write_enable` — Lorsque cette option est activée de concert avec la directive `write_enable`, des utilisateurs anonymes sont autorisés à créer de nouveaux répertoires au sein du répertoire parent qui a des permissions en écriture.

  La valeur par défaut est `NO`.

- `anon_root` — Spécifie le répertoire que `vsftpd` utilise après la connexion d'un utilisateur anonyme.

  Il n'existe pas de valeur par défaut pour cette directive.

- `anon_upload_enable` — Lorsque cette option est activée de concert avec la directive `write_enable`, des utilisateurs anonymes sont autorisés à télécharger vers le serveur des fichiers dans unrépertoire parent doté de permissions en écriture.

  La valeur par défaut est `NO`.

- `anon_world_readable_only` — Lorsque cette option est activée, des utilisateurs anonymes sont autorisés à télécharger des fichiers lisibles par tout un chacun.

  La valeur par défaut est `YES`.

- `ftp_username` — Spécifie le compte de l'utilisateur local (énoncé dans `/etc/passwd`) employé pour l'utilisateur FTP anonyme. Le répertoire personnel spécifié dans `/etc/passwd` pour l'utilisateur est le répertoire root de l'utilisateur FTP anonyme.

  La valeur par défaut est `ftp`.

- `no_anon_password` — Lorsque cette option est activée, l'utilisateur anonyme ne doit pas saisir de mot de passe.

  La valeur par défaut est `NO`.

- `secure_email_list_enable` — Lorsque cette option est activée, seule une liste de mots de passe électroniques spécifiée pour les connexions anonymes est acceptée. Ce faisant, il est d'offrir une certaine sécurité à un contenu public sans avoir besoin d'utilisateurs virtuels.

  Les connexions anonymes sont refusées à moins que le mot de passe fourni soit contenu dans `/etc/vsftpd.email_passwords`. Le format du fichier est un mot de passe par ligne, sans espace à la fin.

  La valeur par défaut est `NO`.

15.5.4. Options pour les utilisateurs locaux

Ci-dessous figure une liste des directives caractérisant la manière selon laquelle les utilisateurs locaux ont accès au serveur. Pour utiliser ces options, la directive `local_enable` doit avoir la valeur `YES`.

- `chmod_enable` — Lorsque cette option est activée, la commande FTP `SITE CHMOD` est autorisée pour les utilisateurs locaux. Cette commande permet aux utilisateurs de changer les permissions s'appliquant aux fichiers.

  La valeur par défaut est `YES`.

- `chroot_list_enable` — Lorsque cette option est activée, les utilisateurs locaux énumérés dans le fichier qui est spécifié dans la directive `chroot_list_file`, sont placés dans une prison `chroot` dès qu'ils se connectent.

  Si cette option est activée de concert avec la directive `chroot_local_user`, les utilisateurs locaux énumérés dans le fichier qui est spécifié dans la directive `chroot_list_file` *ne sont pas* placés dans une prison `chroot` lors de la connexion.

  La valeur par défaut est `NO`.

- `chroot_list_file` — Spécifie le fichier contenant une liste des utilisateurs locaux référencés lorsque la valeur de la directive `chroot_list_enable` est `YES`.

  La valeur par défaut est `/etc/vsftpd.chroot_list`.

- `chroot_local_user` — Lorsque cette option est activée, les utilisateurs locaux opèrent dans l'environnement chrooté de leur répertoire personnel après leur connexion.

  La valeur par défaut est `NO`.

  
  Avertissement

  L'activation de l'option `chroot_local_user` crée un certain nombre de problèmes de sécurité, particulièrement pour les utilisateurs possédant les privilèges nécessaire pour télécharger sur le serveur. Elle *n'est* par conséquent pas recommendée.

- `guest_enable` — Lorsque cette option est activée, tous les utilisateurs autres que les utilisateurs anonymes sont connectés en tant que l'utilisateur invité (`guest`) qui est l'utilisateur local spécifié dans la directive `guest_username`.

  La valeur par défaut est `NO`.

- `guest_username` — Spécifie le nom d'utilisateur vers lequel l'utilisateur invité (`guest`) est mappé.

  La valeur par défaut est `ftp`.

- `local_root` — Spécifie le répertoire que `vsftpd` utilise après la connexion d'un utilisateur local.

  Il n'existe pas de valeur par défaut pour cette directive.

- `local_umask` — Spécifie la valeur donnée à umask pour la création de fichiers. Notez que la valeur par défaut se présente sous la forme octale (un système numérique en base huit), qui inclut un préfixe "0". Sinon la valeur est traitée comme un entier à base 10.

  La valeur par défaut est `022`.

- `passwd_chroot_enable` — Lorsque cette option est activée de concert avec la directive `chroot_local_user`, `vsftpd` chroote les utilisateurs locaux si l'élément `/./` figure dans le champ du répertoire personnel au sein de `/etc/passwd`.

  La valeur par défaut est `NO`.

- `user_config_dir` — Spécifie le chemin vers un répertoire contenant les fichiers de configuration portant le nom des utilisateurs du système local qui renferment des paramètres spécifiques pour ces utilisateurs. Toute directive figurant dans le fichier de configuration d'un utilisateur annule celles figurant dans `/etc/vsftpd/vsftpd.conf`.

  Il n'existe pas de valeur par défaut pour cette directive.

15.5.5. Options pour les répertoires

Ci-dessous figure la liste des directives ayant un impact sur les répertoires.

- `dirlist_enable` — Lorsque cette option est activée, les utilisateurs sont autorisés à visionner les listes de répertoires.

  La valeur par défaut est `YES`.

- `dirmessage_enable` — Lorsque cette option est activée, un message apparaît chaque fois qu'un utilisateur ouvre un répertoire avec un fichier message. Ce message se trouve dans le répertoire qui est ouvert. Le nom de ce fichier est spécifié dans la directive `message_file` et part défaut prend la valeur `.message`.

  La valeur par défaut est `NO`. Notez que, sous Red Hat Enterprise Linux, la valeur est `YES`.

- `force_dot_files` — Lorsque cette option est activée, les fichiers commençant par un point (`.`) sont inclus dans les listes de répertoires, à l'exception des fichiers `.` et `..`

  La valeur par défaut est `NO`.

- `hide_ids` — Lorsque cette option est activée, toutes les listes de répertoires font apparaître `ftp` comme l'utilisateur et le groupe de chaque fichier.

  La valeur par défaut est `NO`.

- `message_file` — Spécifie le nom du fichier message lorsque la directive `dirmessage_enable` est utilisée.

  La valeur par défaut est `.message`.

- `text_userdb_names` — Lorsque cette option est activée, des noms d'utilisateurs et noms de groupes test sont utilisés au lieu des entrées UID et GID. L'activation de cette option peut entraîner un ralentissement des performances du serveur.

  La valeur par défaut est `NO`.

- `use_localtime` — Lorsque cette option est activée, les listes de répertoires révèlent l'heure locale de l'ordinateur au lieu de l'heure GMT.

  La valeur par défaut est `NO`.

15.5.6. Options pour le transfert de fichiers

Ci-dessous figure la liste des directives ayant un impact sur les répertoires.

- `download_enable` — Lorsque cette option est activée, le téléchargement de fichiers est autorisé.

  La valeur par défaut est `YES`.

- `chown_uploads` — Lorsque cette option est activée, tous les fichiers téléléchargés vers les serveur par des utilisateurs anonymes deviennent la propriété de l'utilisateur spécifié dans la directive `chown_username`.

  La valeur par défaut est `NO`.

- `chown_username` — Spécifie la propriété de fichiers téléchargés anonymement vers le serveur si la directive `chown_uploads` est activée.

  La valeur par défaut est `root`.

- `write_enable` — Lorsque cette option est activée, les commandes FTP permettant de modifier le système de fichiers sont permises, telles que `DELE`, `RNFR` et `STOR`.

  La valeur par défaut est `YES`.

15.5.7. Options de journalisation

Ci-dessous figure une liste des directives ayant un impact sur le comportement de journalisation de `vsftpd`.

- `dual_log_enable` — Lorsque cette option est activée de concert avec `xferlog_enable`, `vsftpd` enregistre deux fichiers simultanément : un journal compatible avec `wu-ftpd` dans le fichier spécifiée dans la directive `xferlog_file` (par défaut `/var/log/xferlog`) et un fichier journal `vsftpd` standard spécifié dans la directive `vsftpd_log_file` (par défaut `/var/log/vsftpd.log`).

  La valeur par défaut est `NO`.

- `log_ftp_protocol` — Lorsque cette option est activée de concert avec `xferlog_enable` et lorsque `xferlog_std_format` a pour valeur `NO`, toutes les commandes et réponses FTP sont journalisées. Cette directive est très utilise lors d'opérations de débogage.

  La valeur par défaut est `NO`.

- `syslog_enable` — Lorsque cette option est activée de concert avec `xferlog_enable`, toute journalisation normalement enregistrée dans le fichier journal standard `vsftpd` spécifié dans la directive `vsftpd_log_file` (par défaut `/var/log/vsftpd.log`) est envoyée à l'enregistreur du système sous le service FTPD.

  La valeur par défaut est `NO`.

- `vsftpd_log_file` — Spécifie le fichier journal `vsftpd`. Pour que ce fichier soit utilisé, `xferlog_enable` doit être activée et `xferlog_std_format` doit avoir pour valeur `NO` ou, si la valeur de `xferlog_std_format` est`YES`, l'activation de`dual_log_enable` est nécessaire. Il est important de noter ici que si `syslog_enable` a pour valeur `YES`, le journal du système est utilisé à la place du fichier spécifié dans cette directive.

  La valeur par défaut est `/var/log/vsftpd.log`.

- `xferlog_enable` — Lorsque cette commande est activée, `vsftpd` journalise les connexions (seulement au format `vsftpd`) et les informations de transfert de fichiers dans le fichier journal spécifié dans la directive `vsftpd_log_file` (par défaut `/var/log/vsftpd.log`). Si `xferlog_std_format` a pour valeur `YES`, les informations de transfert de fichiers sont journalisées mais les connexions elles ne le sont pas et le fichier spécifié dans `xferlog_file` (par défaut `/var/log/xferlog`) est utilisé à la place. Il est important de noter ici que les fichiers journaux aussi bien que les formats de journaux sont utilisés si la valeur de `dual_log_enable` est `YES`.

  La valeur par défaut est `NO`. Notez que, sous Red Hat Enterprise Linux, la valeur est `YES`.

- `xferlog_file` — Spécifie le fichier journal compatible avec `wu-ftpd`. Pour que ce fichier soit utilisé, `xferlog_enable` doit être activé et la valeur de `xferlog_std_format` doit être `YES`. Elle est également utilisée si la valeur de `dual_log_enable` est `YES`.

  La valeur par défaut est `/var/log/xferlog`.

- `xferlog_std_format` — Lorsque cette option est activée de concert avec `xferlog_enable`, seul un journal de transfert de fichiers compatible avec `wu-ftpd` est enregistré dans le fichier spécifié dans la directive `xferlog_file` (par défaut `/var/log/xferlog`). Il est important de noter ici que ce fichier journalise seulement les transferts de fichiers et n'enregistre pas les connexions au serveur.

  La valeur par défaut est `NO`. Notez que, sous Red Hat Enterprise Linux, la valeur est `YES`.

Important

Pour maintenir la compatibilité avec les fichiers journaux enregistrés par l'ancien serveur FTP `wu-ftpd`, la directive `xferlog_std_format` prend la valeur `YES` sous Red Hat Enterprise Linux. Toutefois, ce paramètre signifie que les connexions au serveur ne sont pas journalisées.

Pour journaliser les connexions au format `vsftpd` et maintenir un journal des transferts de fichiers qui est compatible avec `wu-ftpd`, donnez à `dual_log_enable` la valeur `YES`.

S'il n'est pas important de maintenir un journal des transferts de fichiers qui est compatible avec `wu-ftpd`, vous pouvez donner à `xferlog_std_format` la valeur `NO`, commenter la ligne à l'aide d'un signe dièse (`#`) ou supprimer la ligne complètement.

15.5.8. Options réseau

Ci-dessous figure une liste des directives ayant un impact sur la manière dont `vsftpd` interagit avec le réseau.

- `accept_timeout` — Spécifie la durée donnée à un client utilisant une connexion passive pour se connecter.

  La valeur par défaut est `60`.

- `anon_max_rate` — Spécifie le taux de transfert de données maximal, exprimé en octets par seconde, pour les utilisateurs anonymes.

  La valeur par défaut est `0`, ce qui ne limite pas le taux de transfert.

- `connect_from_port_20` Lorsque cette option est activée, `vsftpd` tourne avec suffisamment de privilèges pour ouvrir le port 20 sur le serveur lors des transferts de données en mode actif. La désactivation de cette option permet à `vsftpd` de tourner avec moins de privilèges, mais cette option peut-être incompatible avec certains clients FTP.

  La valeur par défaut est `NO`. Notez que, sous Red Hat Enterprise Linux, la valeur est `YES`.

- `connect_timeout` — Spécifie la durée maximale exprimée en secondes, donnée à un client utilisant un mode actif pour répondre à une connexion de données.

  La valeur par défaut est `60`.

- `data_connection_timeout` — Spécifie la durée maximale exprimée en secondes, pendant laquelle les transferts de données peuvent s'arrêter. Une fois cette durée écoulée, la connexion au client distant est fermée.

  La valeur par défaut est `300`.

- `ftp_data_port` — Spécifie le port utilisé pour les connexions actives aux données lorsque `connect_from_port_20` a pour valeur `YES`.

  La valeur par défaut est `20`.

- `idle_session_timeout` — Spécifie la durée maximale pouvant s'écouler entre des commandes depuis un client distant. Une fois cette durée écoulée, la connexion au client distant est fermée.

  La valeur par défaut est `300`.

- `listen_address` — Spécifie l'adresse IP sur laquelle `vsftpd` doit être à l'écoute de connexions réseau.

  Il n'existe pas de valeur par défaut pour cette directive.

  

  Astuce

  Si plusieurs copies de `vsftpd` tournent et servent différentes adresses IP, le fichier de configuration de chaque copie du démon `vsftpd` doit avoir une valeur différente pour cette directive. Reportez-vous à la Section 15.4.1 pour obtenir de plus amples informations sur les serveurs FTP en hébergement multidomaine (aussi appelé multihoming).

- `listen_address6` — Spécifie l'adresse IPv6 sur laquelle `vsftpd` doit être à l'écoute de connexions réseau lorsque `listen_ipv6` a pour valeur `YES`.

  Il n'existe pas de valeur par défaut pour cette directive.

Astuce

Si plusieurs copies de `vsftpd` tournent et servent différentes adresses IP, le fichier de configuration de chaque copie du démon `vsftpd` doit avoir une valeur différente pour cette directive. Reportez-vous à la Section 15.4.1 pour obtenir de plus amples informations sur les serveurs FTP en hébergement multidomaine (aussi appelé multihoming).

- `listen_port` — Spécifie le port sur lequel `vsftpd` doit être à l'écoute de connexions réseau.

  La valeur par défaut est `21`.

- `local_max_rate` — Spécifie le taux maximal (exprimé en octets par seconde) auquel les données sont transférées, pour les utilisateurs locaux connectés au serveur.

  La valeur par défaut est `0`, ce qui ne limite pas le taux de transfert.

- `max_clients` — Spécifie le nombre maximal de clients autorisés à se connecter simultanément au serveur lorsqu'il tourne en mode autonome. Toute connexion client supplémentaire provoquerait un message d'erreur.

  La valeur par défaut est `0`, ce qui ne limite pas les connexions.

- `max_per_ip` — Spécifie le nombre maximal de clients autorisés à se connecter depuis l'adresse IP source.

  La valeur par défaut est `0`, ce qui ne limite pas les connexions.

- `pasv_address` — Spécifie l'adresse IP utilisée pour l'adresse IP publique du serveur aux serveurs se trouvant derrière des pare-feu NAT (Network Address Translation). Cette option permet à `vsftpd` de fournir la bonne adresse de retour pour des connexions en mode passif.

  Il n'existe pas de valeur par défaut pour cette directive.

- `pasv_enable` — Lorsque cette option est activée, les connexions en mode passif ne sont pas permises.

  La valeur par défaut est `YES`.

- `pasv_max_port` — Spécifie le port le plus élevé possible qui est envoyé aux clients FTP pour des connexions en mode passif. Ce paramètre est utilisé pour limiter la plage de ports afin que les règles de pare-feu soient faciles à créer.

  La valeur par défaut est `0`, ce qui ne limite pas la plage des ports passifs les plus élevés. La valeur ne doit pas dépasser `65535`.

- `pasv_min_port` — Spécifie le port le plus bas possible qui est envoyé au client FTP pour des connexions en mode passif. Ce paramètre est utilisé pour limiter la plage de ports afin que les règles de pare-feu soient faciles à créer.

  La valeur par défaut est `0`, ce qui ne limite pas la plage des ports passifs les plus bas. La valeur ne doit pas être inférieure à `1024`.

- `pasv_promiscuous` — Lorsque cette option est activée, les connexions aux données ne sont pas analysées pour vérifier qu'elles proviennent bien de la même adresse IP. Ce paramètre est seulement utile pour certains types de tunnellisation.

  

  Attention

  N'activez pas cette option à moins qu'elle ne soit absolument nécessaire. En effet, elle désactive une fonctionnalité de sécurité importante permettant de vérifier que les connexions en mode passif proviennent bien de la même adresse IP que la connexion de contrôle qui lance le transfert de données.

  La valeur par défaut est `NO`.

- `port_enable` — Lorsque cette option est activée, les connexions en mode actif ne sont pas permises.

  La valeur par défaut est `YES`.

15.6. Ressources supplémentaires

Pour obtenir de plus amples informations sur `vsftpd`, reportez-vous aux ressources mentionnées ci-dessous.

15.6.1. Documentation installée

- Le répertoire `/usr/share/doc/vsftpd-<version-number>/` — Remplacez `<version-number>` par le numéro de la version du paquetage `vsftpd` installée sur le système. Ce répertoire contient un document `README` fournissant des informations élémentaires sur le logiciel. Le fichier `TUNING` contient des astuces de base pour régler la performance alors que le répertoire `SECURITY/` contient lui des informations sur le modèle de sécurité employé par `vsftpd`.
- Pages de manuels de `vsftpd` — Il existe un certain nombre de pages de manuel pour le démon et les fichiers de configuration. Ci-après figure une liste des pages de manuel les plus importantes.

  Application serveur

  - `man vsftpd` — Examine les options de ligne de commande disponibles pour `vsftpd`.

  Fichiers de configuration

  - `man vsftpd.conf` — Contient une liste détaillée des options disponibles au sein du fichier de configuration de `vsftpd`.
  - `man 5 hosts_access` — Examine le format et les options disponibles au sein des fichiers de configuration des enveloppeurs TCP : `hosts.allow` et `hosts.deny`.

15.6.2. Sites Web utiles

- http://vsftpd.beasts.org/ — La page du projet `vsftpd` est très utile pour trouver la documentation la plus récente et pour contacter l'auteur du logiciel.
- http://slacksite.com/other/ftp.html — Ce site Web fournit une explication concise des différences existant entre FTP en mode passif et en mode actif.
- http://war.jgaa.com/ftp/?cmd=rfc — Une liste complète de documents *RFC* (de l'anglais *Request for Comments*) en relation avec le protocole FTP.

15.6.3. Livre sur le sujet

- *Guide de sécurité de Red Hat Enterprise Linux* ; Red Hat, Inc. — Le chapitre intitulé *Sécurité serveur* explique différentes manières de sécuriser `vsftpd` et d'autres services.

III. Références pour la sécurité

L'utilisation de protocoles sécurisés représente un aspect très important dans la maintenance de l'intégrité de systèmes. Cette section décrit les outils critiques utilisés pour l'authentification des utilisateurs, le contrôle de l'accès au réseau, la communication réseau sécurisée. Pour obtenir davantage d'informations sur la sécurisation d'un système Red Hat Enterprise Linux, reportez-vous au *Guide de sécurité de Red Hat Enterprise Linux.*

Table des matières

Chapitre 16.

Modules d'authentification enfichables (PAM)

Des programmes qui autorisent des utilisateurs à accéder à un système vérifient préalablement l'identité de chaque utilisateur au moyen d'un processus appelé *authentification*. Dans le passé, chaque programme de ce genre effectuait les opérations d'authentification d'une manière qui lui était propre. Sous Red Hat Enterprise Linux, un grand nombre de ces programmes sont configurés de telle sorte qu'ils utilisent un processus d'authentification centralisé appelé *modules d'authentification enfichables* (ou *PAM* de l'anglais Pluggable Authentication Modules).

PAM utilise une architecture modulaire enfichable, offrant à l'administrateur système une grande flexibilité quant à l'établissement d'une politique d'authentification pour le système.

Dans la plupart des cas, les fichiers de configuration PAM par défaut sont tou à fait adéquats pour les applications utilisant PAM. Toutefois, dans certains cas il sera nécessaire de modifier le fichier un configuration PAM. Étant donné qu'une mauvaise configuration de PAM peut compromettre la sécurité du système, il est important de comprendre la structure de ces fichiers avant de leur apporter toute modification (reportez-vous à la Section 16.3 pour obtenir de plus amples informations).

16.1. Avantages de PAM

PAM offre entre autres les avantages suivants :

- Il fournit un procédé d'authentification commun qui peut être utilisé avec un grand éventail d'applications.
- Il offre aussi bien aux administrateur système qu'aux développeurs d'applications un niveau de souplesse et de contrôle considérable quant à l'authentification.
- Il permet aux développeurs d'applications de concevoir des programmes sans avoir à créer leur propre système d'authentification.

16.2. Fichiers de configuration PAM

Le répertoire `/etc/pam.d/` contient les fichiers de configuration PAM pour chaque application utilisant PAM. Les versions précédentes de PAM utilisaient le fichier `/etc/pam.conf`, mais ce dernier a été abandonné et `pam.conf` n'est désormais nécessaire que si le répertoire `/etc/pam.d/` n'existe pas.

16.2.1. Fichiers des services PAM

Chaque application ou *service* utilisant PAM a un fichier dans le répertoire `/etc/pam.d/`. Chacun de ces fichiers est nommé en fonction du service dont il contrôle l'accès.

Il appartient au programme utilisant PAM de définir le nom de sonservice et d'installer son fichier de configuration PAM dans le répertoire `/etc/pam.d/`. Par exemple, le programme `login` attribue le nom login à son service et installe le fichier de configuration PAM `/etc/pam.d/login`.

16.3. Format des fichiers de configuration PAM

Chaque fichier de configuration PAM comprend un ensemble de directives établies selon format suivant :

```
<module interface>  <control flag>  <module name>  <module arguments>
```

Les sections suivantes décrivent ces éléments un par un.

16.3.1. Interface du module

Il existe quatre types d'interfaces pour les modules PAM, chacune correspondant à un aspect différent du processus d'autorisation :

- `auth` — Cette interface de module sert à authentifier l'utilisateur. Elle demande par exemple la saisie d'un mot de passe pour lequel elle vérifie la validité. Les modules avec cette interface peuvent également établir des certificats d'identité, tels que l'appartenance à un groupe ou des tickets Kerberos.
- `account` — Cette interface de module sert à vérifier que l'accès est bien autorisé. Par exemple, elle peut vérifier si un compte utilisateur a expiré ou non, ou bien si l'utilisateur est autorisé à se connecter à un moment donné de la journée.
- `password` — Cette interface de module sert à définir et vérifier les mots de passe.
- `session` — Cette interface de module ser à configurer et gérer des sessions d'utilisateurs. Les modules ayant cette interface peuvent également effectuer des tâches supplémentaires requises pour autoriser l'accès, comme par exemple pour monter le répertoire personnel d'un utilisateur ou activer sa boîte aux lettres.

Remarque

Un module individuel peut fournir une interface de module quelconque ou toutes les interfaces de modules. Par exemple, `pam_unix.so` fournit les quatre interfaces de module.

Dans un fichier de configuration PAM, le champ relatif à l'interface de module est le premier à être défini. Par exemple, une ligne typique d'un fichier de configuration pourrait ressembler à l'extrait suivant :

```
auth      required  pam_unix.so
```

Cette ligne donne l'instruction à PAM d'utiliser l'interface `auth` du module `pam_unix.so`.

16.3.1.1. Empilage d'interfaces de module

Les directives relatives aux interfaces de modules peuvent être *empilées* ou placées les unes sur les autres, afin que de multiples modules soient utilisés ensemble dans un but particulier. Dans de telles circonstances, l'ordre dans lequel les modules sont répertoriés est très important au niveau du processus d'authentification.

Grâce à l'empilage, un administrateur peut facilement exiger la présence de différentes conditions avant d'autoriser un utilisateur à s'authentifier. Par exemple, `rlogin` utilise normalement cinq modules `auth` empilés, comme le montre son fichier de configuration PAM :

```
auth       required     pam_nologin.so
auth       required     pam_securetty.so
```

```
auth       required     pam_env.so
auth       sufficient   pam_rhosts_auth.so
auth       required     pam_stack.so service=system-auth
```

Avant qu'un utilisateur puisse utiliser `rlogin`, PAM s'assure que le fichier `/etc/nologin` n'existe pas, que l'utilisateur n'essaie pas de se connecter à distance en tant que super-utilisateur (ou root) au moyen d'une connexion réseau et que toutes les variables d'environnement peuvent être chargées. Ensuite, si une authentification `rhosts` est établie avec succès, la connexion est autorisée. En revanche, si l'authentification `rhosts` n'aboutit pas, une authentification de mot de passe standard est exécutée.

16.3.2. Indicateurs de contrôle

Lorsqu'ils sont appelés, tous les modules PAM donnent un résultat indiquant soit la réussite, soit l'échec. Les indicateurs de contrôle indiquent à PAM la manière de traiter ce résultat. Étant donné que les modules peuvent être empilés dans un ordre bien précis, les indicateurs de contrôle décident de l'importance de la réussite ou de l'échec d'un module spécifique par rapport au but général d'authentification d'un utilisateur pour un service donné.

Il existe quatre types d'indicateurs de contrôle prédéfinis, à savoir :

- `required` — Le module doit être vérifié avec succès pour que l'authentification puisse se poursuivre. Si la vérification d'un module de type `required` échoue, l'utilisateur n'en est pas averti tant que tous les modules associés à cette interface n'ont pas été vérifiés.
- `requisite` — Le module doit être vérifié avec succès pour que l'authentification puisse se poursuivre. Cependant, si la vérification d'un module de type `requisite` échoue, l'utilisateur en est averti immédiatement par le biais d'un message lui indiquant l'échec du premier module de types `required` *ou* `requisite`.
- `sufficient` — En cas d'échec, les vérifications de modules sont ignorées. Toutefois, si la vérification d'un module de type `sufficient` est réussie *et* qu'aucun module précédent de type `required` n'a échoué, aucun autre module de ce type n'est nécessaire et l'utilisateur sera authentifié auprès du service.
- `optional` — Les vérifications de modules sont ignorées. Un module de type `optional` ne devient nécessaire que pour la réussite d'une authentification lorsqu'aucun autre module ne référence l'interface.

Important

L'ordre dans lequel les modules de type `required` sont appelés n'est pas primordial. Les indicateurs de contrôles `sufficient` et `requisite` en revanche, donnent à l'ordre une importance vitale.

Pour PAM, il existe désormais une nouvelle syntaxe d'indicateurs de contrôle qui offre un contrôle encore plus précis. Veuillez lire la documentation relative à PAM disponible dans le répertoire `/usr/share/doc/pam-<version-number>/` (où `<version-number>` correspond au numéro de version de PAM) pour obtenir des informations sur cette nouvelle syntaxe.

16.3.3. Nom de module

Le nom de module donne à PAM le nom du module enfichable contenant l'interface module spécifiée. Sous les versions plus anciennes de Red Hat Enterprise Linux, le chemin entier du module était fourni dans le fichier de configuration PAM, tel que `/lib/security/pam_stack.so`. Toutefois, depuis l'arrivée de systèmes multilib qui stockent des modules PAM de 64-octets dans le répertoire

`/lib64/security/`, le nom du répertoire est omis car les applications sont liées à la version appropriée de `libpam`, qui peut trouver la version correcte du module.

16.3.4. Arguments des modules

PAM utilise des arguments pour transmettre des informations à un module enfichable lors du processus d'authentification de certains modules.

Par exemple, le module `pam_userdb.so` utilise des indications secrètes stockées dans un fichier de la base de données Berkeley pour authentifier les utilisateurs. La base de données Berkeley est une base de données Open Source intégrée dans de nombreuses applications. Le module nécessite un argument `db` pour spécifier à la base de données Berkeley la base de données précise devant être utilisée pour le service demandé.

Une ligne `pam_userdb.so` typique d'un fichier de configuration PAM ressemble à l'extrait suivant :

```
auth      required  pam_userdb.so db=<path-to-file>
```

Dans l'exemple précédent, remplacez *<path-to-file>* par le chemin d'accès complet au fichier de la base de données Berkeley DB.

Les arguments non valides ne sont pas pris en compte et n'ont aucune incidence sur la réussite ou l'échec du module PAM. Toutefois, la plupart des modules rapporteront des erreurs dans le fichier `/var/log/messages`.

16.4. Exemples de fichiers de configuration PAM

Ci-dessous figure un exemple de fichier de configuration PAM :

```
#%PAM-1.0
auth      required  pam_securetty.so
auth      required  pam_unix.so shadow nullok
auth      required  pam_nologin.so
account   required  pam_unix.so
password  required  pam_cracklib.so retry=3
password  required  pam_unix.so shadow nullok use_authtok
session   required  pam_unix.so
```

La première ligne est un commentaire, comme l'indique le caractère dièse (`#`) placé au début de la ligne.

Les lignes deux à quatre empilent trois modules pour l'authentification de la connexion (ou login).

```
auth      required  pam_securetty.so
```

Ce module permet de s'assurer que *si* l'utilisateur essaie de se connecter en tant que super-utilisateur (ou root), le terminal tty sur lequel il se connecte fait bien partie de la liste se trouvant dans le fichier `/etc/securetty`, *si* ce fichier existe.

```
auth      required  pam_unix.so shadow nullok
```

Ce module invite l'utilisateur à saisir un mot de passe, puis le vérifie à l'aide des informations stockées dans `/etc/passwd` et s'il existe, consulte `/etc/shadow`. Le module `pam_unix.so` détecte et utilise automatiquement les mots de passe masqués pour authentifier les utilisateurs. Reportez-vous à la Section 6.5 pour obtenir davantage d'informations.

L'argument `nullok` donne l'instruction au module `pam_unix.so` d'autoriser un mot de passe vide.

```
auth       required  pam_nologin.so
```

Il s'agit de la dernière phase du processus d'authentification. Cette dernière consiste à vérifier l'existence du fichier `/etc/nologin`. Si `nologin` existe et que l'utilisateur n'est pas le super-utilisateur (ou root), l'authentification échoue.

Remarque

Dans cet exemple, les trois modules `auth` font l'objet d'une vérification, même si le premier module `auth` échoue. De cette façon, l'utilisateur ne peut pas savoir à quel moment l'authentification a échoué. Si des agresseurs venaient à connaître ces informations, ils pourraient plus facilement déduire de manière la plus efficace de pénétrer dans le système.

```
account    required  pam_unix.so
```

Ce module effectue toute vérification de compte nécessaire. Par exemple, si des mots de passe masqués ont été activés, l'élément compte du module `pam_unix.so` vérifiera si le compte a expiré ou si l'utilisateur a changé son mot de passe pendant le délai de grâce alloué.

```
password  required  pam_cracklib.so retry=3
```

Si un mot de passe n'est plus valable, l'élément mot de passe du module `pam_cracklib.so` invite l'utilisateur à en fournir un nouveau. Il vérifie ensuite le mot de passe créé afin de déterminer s'il peut être facilement retrouvé par un programme de craquage de mots de passe basé sur des dictionnaires. Si le test du mot de passe échoue, le programme donne à l'utilisateur deux autres possibilités de créer un mot de passe sûr, comme il l'est précisé dans l'argument `retry=3`.

```
password  required  pam_unix.so shadow nullok use_authtok
```

Cette ligne spécifie que, si le programme change le mot de passe de l'utilisateur, il doit le faire en utilisant l'élément `password` du module `pam_unix.so`. Ceci se produit uniquement si la partie `auth` du module `pam_unix.so` détermine que le mot de passe doit être changé.

L'argument `shadow` donne l'instruction au module de créer des mots de passe masqués lors de la mise à jour du mot de passe d'un utilisateur.

L'argument `nullok` donne l'instruction au module d'autoriser l'utilisateur à changer son mot de passe *à partir d'un* mot de passe vide ; sinon, un mot de passe non valide est traité comme un verrouillage de compte.

Le dernier argument de cette ligne, `use_authtok`, est un bon exemple montrant l'importance de l'ordre lors de l'empilage de modules PAM. Cet argument indique au module de ne pas demander à l'utilisateur un nouveau mot de passe. À la place, il accepte tout mot de passe enregistré dans le module de mots de passe précédent. De cette façon, tous les nouveaux mots de passe doivent passer le test de sécurité `pam_cracklib.so` avant d'être acceptés.

```
session required pam_unix.so
```

La dernière ligne spécifie que l'élément session du module `pam_unix.so` gérera la session. Au début et à la fin de chaque session, ce module enregistre dans `/var/log/messages` le nom d'utilisateur ainsi que le type de service. Un empilage avec d'autres modules de session permet d'obtenir une fonctionnalité plus avancée.

L'exemple de fichier de configuration ci-dessous illustre l'empilage du module `auth` pour le programme `rlogin`.

```
#%PAM-1.0
```

```
auth       required    pam_nologin.so
auth       required    pam_securetty.so
auth       required    pam_env.so
auth       sufficient  pam_rhosts_auth.so
auth       required    pam_stack.so service=system-auth
```

Tout d'abord, `pam_nologin.so` vérifie l'existence de `/etc/nologin`. S'il existe, seul le super-utilisateur (ou root) se voit autoriser la connexion.

```
auth       required    pam_securetty.so
```

Le module `pam_securetty.so` empêche les connexions en tant que super-utilisateur sur des terminaux non sécurisés. Ce faisant, toute tentative d'accès au module `rlogin` est rejetée en raison des mesures de sécurité de l'application.

Astuce

Pour établir une connexion à distance en tant que super-utilisateur, utilisez OpenSSH à la place. Pour obtenir davantage d'nformations sur le sujet, consultez le Chapitre 20.

```
auth       required    pam_env.so
```

Cette ligne charge le module `pam_env.so`, qui définit les variables d'environnement spécifiées dans `/etc/security/pam_env.conf`.

```
auth       sufficient  pam_rhosts_auth.so
```

Le module `pam_rhosts_auth.so` authentifie ensuite l'utilisateur à l'aide de `.rhosts` dans le répertoire personnel de l'utilisateur. En cas de réussite, PAM authentifie immédiatement la session. En revanche, si `pam_rhosts_auth.so` échoue lors de l'authentification de l'utilisateur, cette tentative infructueuse n'est pas prise en compte.

```
auth       required    pam_stack.so service=system-auth
```

Si le module `pam_rhosts_auth.so` ne réussit pas à authentifier l'utilisateur, le module `pam_stack.so` exécute une authentification normale avec mot de passe.

L'argument `service=system-auth` indique que l'utilisateur doit passer à travers la configuration PAM pour l'authentification système telle qu'elle se trouve dans `/etc/pam.d/system-auth`.

Astuce

Pour éviter que PAM n'invite l'utilisateur à fournir un mot de passe lorsque la vérification `securetty` échoue, changez l'indicateur du module `pam_securetty.so` de `required` à `requisite`.

16.5. Création des modules PAM

Il est possible à tout moment, d'ajouter des modules d'authentification enfichables pouvant être ensuite utilisés par des applications prenant en charge les PAM. Par exemple, si un développeur élabore une méthode de création de mot de passe unique et écrit un module PAM pour la prendre en charge, les programmes utilisant PAM pourront immédiatement employer ce nouveau module ainsi que cette méthode de mot de passe sans nécessité de recompilation ou modification. Ainsi, des développeurs et

administrateurs système peuvent combiner et tester rapidement des méthodes d'authentification pour différents programmes sans devoir les recompiler.

De la documentation sur l'écriture de modules est fournie dans le répertoire `/usr/share/doc/pam-<version- number>/` (où *<version-number>* correspond au numéro de version de PAM).

16.6. PAM et mise en cache de certificats administratifs

Sous Red Hat Enterprise Linux, une panoplie d'outils administratifs graphiques offre aux utilisateurs des privilèges supérieurs pour une durée allant jusqu'à cinq minutes via le module `pam_timestamp.so`. Il est important de comprendre comment ce mécanisme fonctionne. En effet, si un utilisateur quitte un terminal pendant que `pam_timestamp.so` est actif, quiconque ayant un accès physique à la machine peut effectuer des manipulations de toute sorte.

Sous le système d'estampille de PAM, l'application administrative graphique demande à l'utilisateur de saisir le mot de passe root au démarrage. Une fois authentifié, le module `pam_timestamp.so` crée un fichier d'estampille dans le répertoire `/var/run/sudo/`, par défaut. Si le fichier d'estampille existe déjà, d'autres programmes administratifs graphiques ne demanderont pas la saisie d'un mot de passe. Au contraire, le module `pam_timestamp.so` rafraîchira le fichier d'estampille — réservant cinq minutes supplémentaires d'accès administratif inconditionnel à l'utilisateur.

L'existence du fichier d'estampille est dénotée par l'icône d'authentification dans la zone de notifications sur le panneau. Ci-dessous figure une illustration de l'icône d'authentification :

Figure 16-1. L'icône d'authentification

16.6.1. Suppression du fichier d'estampille

Avant de s'absenter d'une console sur laquelle une estampille PAM est activée, il est recommandé de supprimer le fichier d'estampille. Pour effectuer cette opération dans un environnement graphique, cliquez sur l'icône d'authentification sur le panneau. Lorsque la boîte de dialogue apparaît, cliquez sur le bouton **Abandonner l'autorisation**.

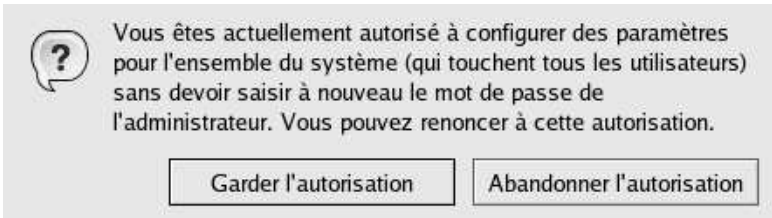

Figure 16-2. Dialogue de l'icône d'authentification

Si vous vous êtes connecté à distance à un système à l'aide de `ssh`, utilisez la commande `/sbin/pam_timestamp_check -k root` pour supprimer le fichier d'estampille.

Remarque

Vous devez être connecté en tant que l'utilisateur qui, à l'origine, a appelé le module `pam_timestamp.so` afin d'utiliser la commande `/sbin/pam_timestamp_check`. Ne vous connectez pas en tant que super-utilisateur pour exécuter cette commande.

Pour obtenir davantage d'informations sur la suppression du fichier d'estampille à l'aide de `pam_timestamp_check`, consultez la page de manuel de `pam_timestamp_check`.

16.6.2. Directives `pam_timestamp` courantes

Le module `pam_timestamp.so` accepte plusieurs directives. Ci-dessous figurent les deux options les plus couramment utilisées :

- `timestamp_timeout` — Spécifie le nombre de secondes pendant lequel le fichier d'estampille est valide. La valeur par défaut est de 300 secondes (soit cinq minutes).
- `timestampdir` — Spécifie le répertoire dans lequel le fichier d'estampille est stocké. La valeur par défaut est `/var/run/sudo`.

Pour obtenir davantage d'informations sur le contrôle du module `pam_timestamp.so`, reportez-vous à la Section 16.8.1.

16.7. Propriété de PAM et des périphériques

Red Hat Enterprise Linux donne au premier utilisateur s'étant connecté à la console de la machine la possibilité de manipuler les périphériques et d'exécuter des tâches qui sont normalement réservées au super-utilisateur. Cette situation est contrôlée par un module PAM appelé `pam_console.so`.

16.7.1. Propriété des périphériques

Lorsqu'un utilisateur se connecte à un système Red Hat Enterprise Linux, le module `pam_console.so` est appelé par `login` ou par les programmes de connexion graphiques **gdm** et **kdm**. Si l'utilisateur est le premier à se connecter à la console physique — que l'on appelle alors *utilisateur console* — le module lui attribue la propriété des périphériques qui appartiennent normalement au super-utilisateur. L'utilisateur console demeure propriétaire de ces périphériques jusqu'à la dernière session locale de cet utilisateur se termine. Une fois que l'utilisateur s'est déconnecté, la propriété de ces périphériques retourne au super-utilisateur.

Les périphériques affectés incluent notamment les cartes son ainsi que les lecteurs de disquettes et de CD-ROM.

Ainsi, un utilisateur local peut gérer ces périphériques sans être connecté en tant que super-utilisateur, ce qui simplifie les tâches courantes de l'utilisateur console.

En modifiant le fichier `/etc/security/console.perms`, l'administrateur peut changer la liste des périphériques contrôlés par `pam_console.so`.

Avertissement

Si le fichier de configuration du gestionnaire d'affichage de **gdm**, **kdm** ou **xdm** a été modifié pour permettre aux utilisateurs distants de se connecter *et* si l'hôte est configuré pour être exécuté en niveau

d'exécution 5, il est conseillé de remplacer les directives <console> et <xconsole> à l'intérieur de /etc/security/console.perms par les valeurs suivantes :

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]* :0\.[0-9] :0
<xconsole>=:0\.[0-9] :0
```

Ce faisant, les utilisateurs distants ne pourront pas accéder aux périphériques et aux applications à accès limité sur cette machine.

Si le fichier de configuration du gestionnaire d'affichage de **gdm**, **kdm** ou **xdm** a été modifié pour permettre aux utilisateurs distants de se connecter *et* si l'hôte est configuré pour être exécuté à tout niveau d'exécution autre que 5, il est conseillé de supprimer entièrement la directive <xconsole> et de remplacer la directive <console> par la valeur suivante :

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]*
```

16.7.2. Accès aux applications

L'utilisateur console peut également accéder à un certains programmes à l'aide d'un fichier portant le nom de la commande dans le répertoire /etc/security/console.apps/.

Un groupe d'applications auquel l'utilisateur console a accès contient trois programmes qui arrêtent ou redémarrent le système, à savoir :

- /sbin/halt
- /sbin/reboot
- /sbin/poweroff

Puisqu'il s'agit d'applications prenant en charge PAM, le fichier pam_console.so est indispensable pour qu'elles puissent fonctionner.

Pour obtenir de plus amples informations, reportez-vous à la Section 16.8.1.

16.8. Ressources supplémentaires

Ci-dessous figure une liste de sources d'informations se rapportant à l'utilisation et à la configuration de PAM. Outre ces ressources, consultez les fichiers de configuration PAM de votre système afin de mieux comprendre leur structure.

16.8.1. Documentation installée

- Les pages de manuel de PAM — Il existe un nombre de pages de manuel pour les diverses applications et fichiers de configuration associés à PAM. La liste suivante énumère certaines des pages de manuel les plus importantes.

  Fichiers de configuration

  - man pam — Fournit de bonnes informations d'introduction sur PAM, incluant la structure et les objectifs des fichiers de configuration PAM. Notez que bien que cette page de manuel parle du fichier /etc/pam.conf, les fichiers de configuration proprement dits de PAM sous Red Hat Enterprise Linux se trouvent dans le répertoire /etc/pam.d/.

- `man pam_console` — Décrit le but du module `pam_console.so`. Il décrit également la syntaxe appropriée pour une entrée à l'intérieur du fichier de configuration PAM.
- `man console.apps` — Décrit le format et les options disponibles de `/etc/security/console.apps`, le fichier de configuration qui définit les applications précises auxquelles à accès l'utilisateur console assigné par PAM.
- `man console.perms` — Décrit le format et les options disponibles de `/etc/security/console.perms`, le fichier de configuration pour les permissions de l'utilisateur console assigné par PAM.
- `man pam_timestamp` — Décrit le module `pam_timestamp.so`.

- `/usr/share/doc/pam-<version-number>` — Contient un *Guide pour les administrateurs système*, un *Manuel pour les concepteurs de modules* et le *Manuel pour les développeurs d'applications*. Il contient également une copie de DCE-RFC 86.0, la norme PAM (remplacez `<version-number>` par le numéro de version de PAM).
- `/usr/share/doc/pam-<version-number>/txts/README.pam_timestamp` — Contient des informations sur le module PAM `pam_timestamp.so` (remplacez `<version-number>` par le numéro de version de PAM).

16.8.2. Site Web utile

- http://www.kernel.org/pub/linux/libs/pam/ — Le site Web de distribution principal du projet Linux-PAM contenant des informations sur différents modules PAM, un Forum Aux Questions (FAQ) ainsi que de la documentation supplémentaire sur PAM.

Chapitre 17.

Enveloppeurs TCP et `xinetd`

Le contrôle de l'accès aux services réseau est l'une des tâches de sécurité les plus importantes à laquelle un administrateur de serveurs doit faire face. Heureusement, sous Red Hat Enterprise Linux il existe un certain nombre d'outils conçus pour effectuer cette tâche. Par exemple, le pare-feu basé sur `iptables` filtre les paquets réseau indésirables au sein de la pile réseau du noyau. Pour les services réseau qui utilisent ce pare-feu, des *enveloppeurs TCP* ajoutent une couche de protection supplémentaire en déterminant les hôtes autorisés ou non à se connecter à des services réseau "*enveloppés*". Parmi ces services réseau enveloppés figure le *super-serveur* `xinetd`. Ce service est baptisé super-serveur parce qu'il contrôle les connexions à un sous-ensemble de services réseau et raffine encore plus le contrôle de l'accès.

La Figure 17-1 représente une illustration élémentaire de la manière selon laquelle ces outils fonctionnent ensemble pour protéger des services réseau.

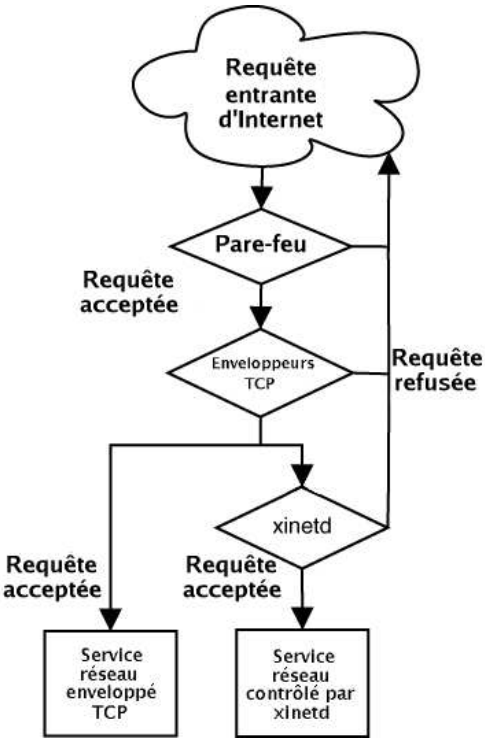

Figure 17-1. Contrôle de l'accès aux services réseau

Ce chapitre examine d'une part le rôle que jouent les enveloppeurs TCP et `xinetd` dans le processus de contrôle de l'accès aux services réseau et analyse d'autre part la manière selon laquelle ces outils

peuvent être utilisés afin d'améliorer aussi bien la gestion de la journalisation que celle de l'utilisation du système. Pour obtenir des informations sur l'utilisation de pare-feu avec `iptables`, reportez-vous au Chapitre 18.

17.1. Enveloppeurs TCP

Le paquetage des enveloppeurs TCP (`tcp_wrappers`) est installé par défaut et fournit un moyen de contrôler l'accès aux services réseau en fonction de l'hôte. La bibliothèque `/usr/lib/libwrap.a` représente l'élément le plus important du paquetage. D'une manière générale, un service enveloppé avec TCP est un service qui a été compilé avec la bibliothèque `libwrap.a`.

Lorsqu'une tentative de connexion à un service enveloppé avec TCP est effectuée, le service cherche d'abord les fichiers *d'accès des hôtes (hosts access)* (`/etc/hosts.allow` et `/etc/hosts.deny`) afin de déterminer si l'hôte client est autorisé ou non à se connecter. Dans la plupart des cas, il utilise ensuite le démon syslog (`syslogd`) pour écrire le nom de l'hôte envoyant la requête et le nom du service demandé dans `/var/log/secure` ou `/var/log/messages`.

Si un hôte client a la permission de se connecter, les enveloppeurs TCP cèdent le contrôle de la connexion au service demandé et n'interfèrent plus entre l'hôte client et le serveur dans le processus de communication.

Outre le contrôle d'accès et la connexion, les enveloppeurs TCP peuvent activer des commandes afin d'interagir avec le client avant de de refuser ou de céder le contrôle de la connexion au service réseau demandé.

Étant donné que les enveloppeurs TCP représentent un ajout précieux à la panoplie des outils de sécurité de tout administrateur de serveurs, la plupart des services réseau sous Red Hat Enterprise Linux sont étroitement liés à la bibliothèque `libwrap.a`. Parmi ces applications figurent `/usr/sbin/sshd`, `/usr/sbin/sendmail` et `/usr/sbin/xinetd`.

Remarque

Afin de déterminer si un binaire de service réseau est lié à `libwrap.a`, tapez la commande suivante en étant connecté en tant que super-utilisateur (ou root) :

```
strings -f <binary-name> | grep hosts_access
```

Remplacez <*binary-name*> par le nom du binaire du service réseau.

Si une invite apparaît, le service réseau n'est *pas* lié à `libwrap.a`.

17.1.1. Avantages des enveloppeurs TCP

Les enveloppeurs TCP offrent deux avantages par rapport à d'autres techniques de contrôle des services réseau :

- *La transparence des opérations aussi bien pour l'hôte client que pour le service réseau enveloppé* — Ni le client établissant la connexion, ni le service réseau enveloppé ne remarqueront que des enveloppeurs TCP sont utilisés. Les utilisateurs légitimes sont connectés et branchés au service demandé alors que les connexions provenant de clients non-autorisés sont refusées.
- *Une gestion centrale de protocoles multiples* — Étant donné que les enveloppeurs TCP fonctionnent indépendamment des services réseau qu'ils protègent, ils permettent à de nombreuses applications serveur de partager un jeu de fichiers de configuration commun, permettant ainsi de simplifier la gestion des services.

17.2. Fichiers de configuration des enveloppeurs TCP

Afin de déterminer si un ordinateur client est autorisé à se connecter à un service, les enveloppeurs TCP référencent les deux fichiers suivants, couramment appelés fichiers d'accès des hôtes :

- `/etc/hosts.allow`
- `/etc/hosts.deny`

Lorsqu'une requête client est reçue par un service enveloppé avec TCP, ce dernier suit les étapes élémentaires ci-dessous :

1. *Le service référence `/etc/hosts.allow`* — Le service enveloppé avec TCP analyse le fichier `/etc/hosts.allow` de manière séquentielle et applique la première règle spécifiée pour ce service. Si une règle correspond au service, il autorise la connexion. Sinon, il passe à l'étape suivante.
2. *Le service référence `/etc/hosts.deny`* — Le service enveloppé avec TCP analyse le fichier `/etc/hosts.deny` de manière séquentielle. Si une règle correspond au service, il refuse la connexion. Sinon, il autorise l'accès au service.

Ci-après figurent des points importants qu'il convient de prendre en compte lors de l'utilisation d'enveloppeurs TCP pour protéger des services réseau :

- Parce que les règles d'accès contenues dans le fichier `hosts.allow` sont appliquées en premier, elles ont priorité par rapport aux règles spécifiées dans le fichier `hosts.deny`. Par conséquent, si l'accès à un service est autorisé dans `hosts.allow` mais qu'une règle refusant l'accès à ce même service est contenue dans le fichier `hosts.deny`, cette dernière ne sera pas prise en compte.
- Étant donné que les règles dans chaque fichier sont lues de haut en bas et que la première règle appliquée à un service donné est la seule règle prise en compte, l'ordre de ces dernières est extrêmement important.
- Si aucune règle contenue dans l'un ou l'autre des fichiers ne s'appliquent au service ou si aucun de ces fichiers n'existe, l'accès au service est autorisé.
- Des services enveloppés avec TCP ne mettent pas en cache les règles des fichiers d'accès d'hôtes, ainsi, tout changement apporté à `hosts.allow` ou `hosts.deny` prend effet immédiatement sans devoir redémarrer les services réseau.

Avertissement

Si la dernière ligne du fichier d'accès d'hôtes ne correspond pas au caractère symbolisant une nouvelle ligne (créé en appuyant sur la touche [Entrée]), la dernière règle du fichier échouera et un message d'erreur sera journalisé soit dans `/var/log/messages`, soit dans `/var/log/secure`. Ce principe s'applique également à des règles s'étendant sur plusieurs lignes où le symbole de la barre oblique inverse est omis. L'exemple suivant illustre la partie pertinente d'un message de journal relatif à l'échec d'une règle en raison de l'une ou l'autre des circonstances mentionnées précédemment :

```
warning: /etc/hosts.allow, line 20: missing newline or line too long
```

17.2.1. Formatage des règles d'accès

Le format est le même pour le fichier `/etc/hosts.allow` et le fichier `/etc/hosts.deny`. Aucune ligne blanche ou commençant par un symbole dièse (`#`) n'est pas prise en compte ; de plus, chaque règle doit figurer sur sa propre ligne.

Chaque règle utilise le format élémentaire suivant pour contrôler l'accès aux services réseau :

```
<daemon list>: <client list> [: <option>: <option>: ...]
```

- *<daemon list>* — Correspond à une liste de noms de processus (*pas* de noms de services) séparés les uns des autres par une virgule ou au *caractère générique*ALL (aussi appelé wildcard), (voir la Section 17.2.1.1). La liste des démons accepte également des *opérateurs* (voir la Section 17.2.1.4 afin d'offrir une plus grande flexibilité.
- *<client list>* — Correspond à une liste de noms d'hôtes, d'adresses IP d'hôtes, de *filtres* spéciaux, (voir la Section 17.2.1.2) ou de jokers (aussi appelés wildcards) spéciaux (voir la Section 17.2.1.1), dont les éléments sont séparés les uns des autres par une virgule. Cette liste identifie les hôtes auxquels la règle s'applique. La liste de clients accepte également les opérateurs énumérés dans la Section 17.2.1.4 afin d'offrir une plus grande flexibilité.
- *<option>* — Correspond à une action facultative ou à une liste d'actions facultatives séparées les unes des autres par une virgule, devant être exécutée lorsque la règle est appliquée. Les champs d'options prennent en charge les *expansions* (voir la Section 17.2.2.4) et peuvent être utilisés pour lancer des commandes du shell, autoriser ou refuser l'accès et modifier le comportement de connexion (voir la Section 17.2.2).

Ci-après figure un exemple élémentaire de règle d'accès d'hôtes :

```
vsftpd : .example.com
```

Cette règle donne aux enveloppeurs TCP l'instruction de surveiller les connexions établies au démon FTP (`vsftpd`) à partir de tout hôte du domaine `example.com`. Si cette règle apparaît dans `hosts.allow`, la connexion sera acceptée. En revanche, si la règle est présente dans `hosts.deny`, la connexion sera refusée.

La règle d'accès d'hôtes figurant ci-dessous est plus complexe et inclus deux champs d'option :

```
sshd : .example.com  \
: spawn /bin/echo '/bin/date' access denied>>/var/log/sshd.log \
: deny
```

Notez que chaque champ d'option est précédé de la barre oblique inverse (`\`). L'utilisation de ce symbole empêche que la règle n'échoue en raison de sa longueur.

Cet exemple de règle stipule que si un hôte du domaine `example.com` essaie d'établir une connexion au démon SSH (`sshd`), la commande `echo` doit être exécutée (permettant de journaliser cette tentative de connexion dans un fichier spécial) et la connexion doit être refusée. Puisque la directive optionnelle `deny` est utilisée, cette ligne entraînera un refus de l'accès même si elle figure dans le fichier `hosts.allow`. Pour obtenir des informations plus détaillées sur les options disponibles, reportez-vous à la Section 17.2.2.

17.2.1.1. Jokers

Les jockers (aussi appelés wildcards) permettent aux enveloppeurs TCP d'autoriser plus facilement les groupes de démons et d'hôtes. Ils sont le plus souvent utilisés dans le champ relatif à la liste de clients des règles d'accès.

Les jokers (ou wildcards) suivants peuvent être utilisés :

- `ALL` — Accorde à tout client l'accès d'un service. Ce joker peut être utilisé aussi bien pour la liste des démons que celle des clients.
- `LOCAL` — Autorise tout hôte ne contenant pas de point (`.`), tel que locahost.
- `KNOWN` — Autorise tout hôte dont le nom ou l'adresse d'hôte sont connus ou lorsque l'utilisateur est connu.

- UNKNOWN — Autorise tout hôte dont le nom ou l'adresse d'hôte sont inconnus ou lorsque l'utilisateur est inconnu.
- PARANOID — Autorise tout hôte dont le nom d'hôte ne correspond pas à l'adresse d'hôte.

Attention

Les jokers KNOWN, UNKNOWN et PARANOID doivent être utilisés avec précaution car une rupture de la résolution de noms peut empêcher des utilisateurs légitimes de se voir accorder l'accès au service.

17.2.1.2. Filtres

Les filtres peuvent être utilisés dans le champ relatif à la liste de clients faisant partie des règles d'accès afin de spécifier de manière plus précise des groupes d'hôtes clients.

Ci-dessous figure une liste des filtres les plus couramment acceptés pour une entrée dans la liste de clients :

- *Nom d'hôte commençant par un point (.)* — En plaçant un point au début d'un nom d'hôte, tous les hôtes partageant les éléments listés du nom seront autorisés. L'exemple suivant s'applique à tout hôte du domaine example.com :
```
ALL : .example.com
```
- *Adresse IP finissant par un point (.)* — En plaçant un point à la fin d'une adresse IP, tous les hôtes partageant les premiers groupes numériques d'une adresse IP seront autorisés. L'exemple suivant s'applique à tout hôte du réseau 192.168.x.x :
```
ALL : 192.168.
```
- *Paire adresse IP / masque réseau* — Les expressions de masques réseau peuvent également être utilisées comme filtre pour contrôler l'accès à un groupe particulier d'adresses IP. L'exemple suivant s'applique à tout hôte doté d'une adresse IP comprise entre 192.168.0.0 et 192.168.1.255 :
```
ALL : 192.168.0.0/255.255.254.0
```

Important

Dans l'espace d'adressage IPv4, les déclarations de paires adresse / longueur de préfixe (*prefixlen*) ne sont pas prises en charge. Seules les règles IPv6 peuvent utiliser ce format.

- *Paire [adresse IPv6] / prefixlen* — Les paires [net] / prefixlen peuvent également être utilisées comme un filtre pour contrôler l'accès à un groupe particulier d'adresses IPv6. L'exemple suivant s'applique à tout hôte doté d'une adresse IP comprise entre 3ffe:505:2:1:: et 3ffe:505:2:1:ffff:ffff:ffff:ffff :
```
ALL : [3ffe:505:2:1::]/64
```
- *L'astérisque (*)* — Des astérisques peuvent être utilisés pour autoriser des groupes entiers de noms d'hôtes ou d'adresses IP, à condition qu'ils ne fassent pas aussi partie d'une liste de clients contenant d'autres types de filtres. L'exemple suivant s'appliquerait à tout hôte du domaine example.com :
```
ALL : *.example.com
```
- *La barre oblique (/)* — Si une liste de clients commence par une barre oblique, elle est considérée comme un nom de fichier. Ce symbole est utile lorsque des règles spécifiant de nombreux hôtes sont nécessaires. L'exemple suivant renvoie les enveloppeurs TCP au fichier /etc/telnet.hosts pour toutes les connexion à Telnet :

```
in.telnetd : /etc/telnet.hosts
```

D'autres filtres, moins utilisés, sont également acceptés par les enveloppeurs TCP. Consultez la section 5 de la page de manuel d'`hosts_access` pour obtenir de plus amples informations.

Avertissement

Soyez très prudent lorsque vous utilisez des noms d'hôtes et des noms de domaines. Des agresseurs peuvent recourir à une variété de tactiques pour contourner une résolution de nom précise. En outre, toute perturbation du service DNS empêcherait même des utilisateurs autorisés d'utiliser les services réseau.

Il est donc préférable, autant que possible, d'utiliser des adresses IP.

17.2.1.3. Portmap et les enveloppeurs TCP

Lors de la création de règles de contrôle d'accès pour `portmap`, n'utilisez pas de noms d'hôtes car l'implémentation des enveloppeurs TCP de `portmap` ne prend pas en charge la consultation des hôtes. Pour cette raison, utilisez seulement des adresses IP ou le mot-clé `ALL` lors de la spécification des hôtes dans `hosts.allow` ou `hosts.deny`.

De plus, les changements apportés aux règles de contrôle d'accès de `portmap` ne prennent pas toujours effet immédiatement sans devoir redémarrer le service `portmap`.

Étant donné que des services très populaires comme NIS et NFS dépendent de `portmap` pour fonctionner, assurez-vous de bien prendre ces limitations en compte.

17.2.1.4. Opérateurs

À l'heure actuelle, les règles de contrôle d'accès acceptent un seul opérateur, à savoir `EXCEPT`. Il peut être utilisé aussi bien dans la liste des démons d'une règle que dans celle des clients.

L'opérateur `EXCEPT` permet d'introduire des exceptions spécifiques à des correspondances plus générales au sein de la même règle.

Dans l'exemple ci-dessous tiré d'un fichier `hosts.allow`, tous les hôtes `example.com` sont autorisés à se connecter aux services sauf `cracker.example.com` :

```
ALL: .example.com EXCEPT cracker.example.com
```

Dans l'autre exemple ci-dessous tiré du fichier `hosts.allow`, les clients du réseau 192.168.0.*x* peuvent utiliser tous les services sauf FTP :

```
ALL EXCEPT vsftpd: 192.168.0.
```

Remarque

Au niveau de l'organisation, il est souvent plus facile d'éviter d'utiliser les opérateurs `EXCEPT`. Ce faisant, d'autres administrateurs peuvent examiner rapidement les fichiers appropriés pour voir les hôtes pour lesquels l'accès aux services doit être autorisé ou refusé, sans devoir examiner tous les opérateurs `EXCEPT`.

17.2.2. Champs d'options

Outres les règles élémentaires autorisant ou refusant l'accès, l'implémentation de Red Hat Enterprise Linux des enveloppeurs TCP prend en charge des extensions au langage du contrôle d'accès grâce à des champs d'options. En utilisant des champs d'options au sein des règles d'accès d'hôtes, les administrateurs peuvent accomplir un vaste éventail de tâches telles que la modification du comportement de journalisation, la consolidation du contrôle d'accès et le lancement de commandes du shell.

17.2.2.1. Journalisation

Les champs d'options permettent aux administrateurs de changer facilement la fonction de journalisation et le niveau de gravité d'une règle à l'aide de la directive `severity`.

Dans l'exemple suivant, les connexions au démon SSH à partir de tout hôte du domaine `example.com` sont journalisées avec la facility par défaut de `syslog` `authpriv` (car aucune valeur de facility n'est spécifiée) avec une priorité `emerg` :

```
sshd : .example.com : severity emerg
```

Il est également possible de spécifier un service à l'aide de l'option `severity`. L'exemple suivant journalise tous les hôtes du domaine `example.com` qui tentent de se connecter au service SSH avec une facility de `local0` et `alert` comme priorité :

```
sshd : .example.com : severity local0.alert
```

Remarque

Dans la pratique, cet exemple ne fonctionne pas tant que le démon syslog (`syslogd`) est configuré pour journaliser sur la fonction `local0`. Consultez la page de manuel de `syslog.conf` pour obtenir de plus amples informations sur la configuration personnalisée des fonctions de journalisation.

17.2.2.2. Contrôle d'accès

Les champs d'options permettent également aux administrateurs d'autoriser ou de refuser de manière explicite des hôtes dans une seule règle en ajoutant la directive `allow` ou `deny` en tant que dernière option.

Par exemple, les deux règles suivantes autorisent des connexions SSH à partir de `client-1.example.com`, mais les refusent à partir de `client-2.example.com` :

```
sshd : client-1.example.com : allow
sshd : client-2.example.com : deny
```

En permettant le contrôle d'accès sur la base de règles individuelles, le champ d'options parmet aux administrateurs de consolider toutes les règles d'accès dans un seul et même fichier : soit `hosts.allow`, soit `hosts.deny`. Pour certains, cette méthode est la manière la plus simple d'organiser des règles d'accès.

17.2.2.3. Commandes du shell

Les champs d'options permettent aux règles d'accès de lancer des commandes du shell au moyen des deux directives suivantes :

- spawn — Lance une commande du shell en tant que processus enfant. Cette directive permet d'effectuer des tâches comme l'utilisation de /usr/sbin/safe_finger pour obtenir des informations supplémentaires sur le client faisant une requête ou pour créer des fichiers de journalisation spéciaux en utilisant la commande echo.

  Dans l'exemple suivant, les clients essayant d'accéder aux services Telnet à partir du domaine example.com sont journalisés dans un fichier spécial :

```
in.telnetd : .example.com \
  : spawn /bin/echo '/bin/date' from %h>>/var/log/telnet.log \
  : allow
```

- twist — Remplace le service demandé par la commande spécifiée. Cette directive est souvent utilisée pour créer des pièges à l'intention des agresseurs (également appelés "pots de miel" ou "honey pots"). Elle peut également être utilisée pour envoyer des messages à des clients se connectant. La commande twist doit se trouver à la fin de la ligne de règles.

  Dans l'exemple suivant, les clients essayant d'accéder aux services FTP à partir du domaine example.com reçoivent un message envoyé au moyen de la commande echo :

```
vsftpd : .example.com \
: twist /bin/echo "421 Bad hacker, go away!"
```

Pour obtenir de plus amples informations sur les options des commandes du shell, consultez la page de manuel de hosts_options.

17.2.2.4. Expansions

Les expansions, lorsqu'elles sont utilisées de concert avec les directives spawn et twist permettent d'obtenir des informations sur le client, le serveur et les processus impliqués.

Ci-après figure une liste des expansions prises en charge :

- %a — Fournit l'adresse IP du client.
- %A — Fournit l'adresse IP du serveur.
- %c — Fournit diverses informations sur le client, comme les noms d'utilisateur et d'hôte, ou le nom d'utilisateur et l'adresse IP.
- %d — Fournit le nom du processus démon.
- %h — Fournit le nom d'hôte du client (ou l'adresse IP, si le nom d'hôte n'est pas disponible).
- %H — Fournit le nom d'hôte du serveur (ou l'adresse IP, si le nom d'hôte n'est pas disponible).
- %n — Fournit le nom d'hôte du client. S'il n'est pas disponible, unknown est affiché. S'il n'y a pas de correspondance entre le nom d'hôte et l'adresse du client, paranoid est alors affiché.
- %N — Fournit le nom d'hôte du serveur. Si celui-ci n'est pas disponible, unknown est affiché. S'il n'y a pas de correspondance entre le nom d'hôte et l'adresse du client, paranoid est affiché.
- %p — Fournit l'ID du processus démon.
- %s — Fournit divers types d'informations sur le serveur, tels que le processus démon et l'hôte ou l'adresse IP du serveur.
- %u — Fournit le nom d'utilisateur du client. Si celui-ci n'est pas disponible, unknown est affiché.

L'exemple de règle suivant utilise une expansion en même temps que la commande spawn pour identifier l'hôte client dans un fichier de journalisation personnalisé.

Lors de toute tentative de connexion au démon SSH (sshd) à partir d'un hôte du domaine example.com, exécutez la commande echo afin de journaliser non seulement la tentative, mais également le nom d'hôte du client (à l'aide de l'expansion %h), dans un fichier spécial :

```
sshd : .example.com  \
```

```
: spawn /bin/echo '/bin/date' access denied to %h>>/var/log/sshd.log \
: deny
```

De même, des expansions peuvent être utilisées pour personnaliser les messages renvoyés au client. Dans l'exemple suivant, les clients essayant de se connecter aux services FTP à partir du domaine `example.com` sont informés qu'ils ont été bannis du serveur :

```
vsftpd : .example.com \
: twist /bin/echo "421 %h has been banned from this server!"
```

Pour obtenir une explication complète des expansions disponibles et des options supplémentaires de contrôle d'accès, reportez-vous à la section 5 de la page de manuel d'`hosts_access` (`man 5 hosts_access`) et à la page de manuel d'`hosts_options`.

Pour obtenir des informations supplémentaires sur les enveloppeurs TCP, consultez la Section 17.5. Pour des informations sur la manière de sécuriser les enveloppeurs TCP, consultez le chapitre intitulé *Sécurité du serveur* du *Guide de sécurité de Red Hat Enterprise Linux*.

17.3. xinetd

Le démon `xinetd` est un *super-service* enveloppé par TCP permettant de contrôler l'accès à un sous-réseau de services réseau populaires parmi lesquels figurent FTP, IMAP et Telnet. Il permet également de spécifier des options de configuration spécifiques aux services en matière de contrôle d'accès, journalisation améliorée, liaison, redirection et de contrôle d'utilisation des ressources.

Lorsqu'un hôte client essaie de se connecter à un service réseau contrôlé par `xinetd`, le super-service reçoit la requête et vérifie l'existence de toute règle de contrôle d'accès des enveloppeurs TCP. Si l'accès est autorisé, `xinetd` vérifie non seulement que la connexion est bien autorisée selon ses propres règles d'accès pour ce service mais que le service n'utilise pas plus de ressources que la quantité qui lui est attribuée et qu'il ne commet aucune infraction aux règles définies. Il démarre alors une instance du service demandé et lui cède le contrôle de la connexion. Une fois la connexion établie, `xinetd` n'interfère plus dans le processus de communication entre l'hôte client et le serveur.

17.4. Fichiers de configuration de xinetd

Ci-dessous figurent les fichiers de configuration de `xinetd` :

- `/etc/xinetd.conf` — Le fichier de configuration global de `xinetd`.
- `/etc/xinetd.d/` — Le répertoire contenant tous les fichiers spécifiques aux services.

17.4.1. Fichier /etc/xinetd.conf

Le fichier `/etc/xinetd.conf` contient des paramètres de configuration généraux qui influencent tous les services placés sous le contrôle de `xinetd`. Ce fichier n'est lu que lors du lancement du service `xinetd`, par conséquent, afin que des changements apportés à la configuration puissent prendre effet, l'administrateur doit redémarrer le service `xinetd`. Ci-après figure un exemple de fichier `/etc/xinetd.conf` :

```
defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
```

```
        log_on_failure          = HOST
        cps                     = 25 30
}
includedir /etc/xinetd.d
```

Les lignes présentes dans l'extrait ci-dessus contrôlent les aspects suivants de `xinetd` :

- `instances` — Détermine le nombre maximal de requêtes qu'un service `xinetd` peut gérer à un moment donné.
- `log_type` — Configure `xinetd` de sorte qu'il utilise la facility de journalisation `authpriv` qui enregistre des entrées de journalisation dans le fichier `/var/log/secure`. L'ajout d'un directive telle que `FILE /var/log/xinetdlog` entraînerait la création d'un fichier de journalisation personnalisé portant le nom `xinetdlog` dans le répertoire `/var/log/`.
- `log_on_success` — Configure `xinetd` de façon à ce qu'il effectue la journalisation si la connexion est établie avec succès. Par défaut sont enregistrés aussi bien l'adresse IP de l'hôte distant que l'ID de processus serveur traitant la requête.
- `log_on_failure` — Configure `xinetd` de façon à ce qu'il effectue la journalisation si la connexion échoue ou si elle n'est pas autorisée.
- `cps` — Configure `xinetd` de manière à n'autoriser que 25 connexions par seconde à un service donné. Si cette limite est atteinte, le service est retiré pendant 30 secondes.
- `includedir /etc/xinetd.d/` — Inclut des options stipulées dans les fichiers de configuration spécifiques aux services qui se trouvent dans le répertoire `/etc/xinetd.d/`. Reportez-vous à la Section 17.4.2 pour obtenir de plus amples informations.

Remarque

Souvent, aussi bien les paramètres `log_on_success` que `log_on_failure` présents dans `/etc/xinetd.conf` font l'objet de modifications plus avancées dans les fichiers journaux spécifiques à chaque service. C'est la raison pour laquelle figurent parfois dans le journal d'un service donné plus d'informations que ne l'indique le fichier `/etc/xinetd.conf`. Reportez-vous à la Section 17.4.3.1 pour obtenir de plus amples informations.

17.4.2. Répertoire `/etc/xinetd.d/`

Le répertoire `/etc/xinetd.d/` contient les fichiers de configuration relatifs à chaque service géré par `xinetd` ; ces derniers portent un nom faisant référence au service. De même que pour `xinetd.conf`, ce fichier est lu seulement lorsque le service `xinetd` est lancé. Ainsi, afin que tout changement puisse prendre effet, l'administrateur doit relancer le service `xinetd`.

Le format des fichiers contenus dans le répertoire `/etc/xinetd.d/` se base sur les mêmes conventions que `/etc/xinetd.conf`. Chaque service est stocké dans un fichier de configuration séparé afin de faciliter la personnalisation et d'éviter qu'elle n'affecte d'autres services.

Pour comprendre comment ces fichiers sont structurés, examinons le fichier `/etc/xinetd.d/telnet` :

```
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
```

```
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = yes
}
```

Les lignes de l'extrait ci-dessous contrôlent différents aspects du service `telnet` :

- `service` — Définit le nom du service, généralement pour correspondre à un service mentionné dans le fichier `/etc/services`.
- `flags` — Définit une variété d'attributs pour la connexion. L'option `REUSE` donne l'instruction à `xinetd` de réutiliser le socket pour une connexion Telnet.
- `socket_type` — Spécifie le socket comme étant de type `stream`.
- `wait` — Détermine si le service est mono-fil (single-threaded, `yes`) ou multi-fils (multi-threaded, `no`).
- `user` — Détermine l'ID d'utilisateur sous lequel le processus est exécuté.
- `server` — Définit le fichier binaire exécutable devant être lancé.
- `log_on_failure` — Détermine les paramètres de journalisation de `log_on_failure` en plus de ceux déjà définis dans `xinetd.conf`.
- `disable` — Détermine si le service est actif.

17.4.3. Modification des fichiers de configuration de xinetd

Il existe une vaste gamme de directives pour les services protégés par `xinetd`. Cette section souligne certaines des options les plus couramment utilisées.

17.4.3.1. Options de journalisation

Les options de journalisation suivantes sont disponibles aussi bien pour `/etc/xinetd.conf` que pour les fichiers de configuration spécifiques à certains services stockés dans le répertoire `/etc/xinetd.d/`.

Ci-dessous figure une liste des options de journalisation les plus couramment utilisées :

- `ATTEMPT` — Enregistre une tentative qui a échoué (`log_on_failure`).
- `DURATION` — Enregistre la durée d'utilisation du service par un système distant (`log_on_success`).
- `EXIT` — Enregistre le statut de sortie ou le signal d'arrêt d'un service (`log_on_success`).
- `HOST` — Enregistre l'adresse IP de l'hôte distant (`log_on_failure` et `log_on_success`).
- `PID` — Enregistre l'ID du processus serveur recevant la requête (`log_on_success`).
- `USERID` — Enregistre l'utilisateur distant selon la méthode définie dans le document RFC 1413 pour tous les services en flux continu multi-fils (multi-threaded) (`log_on_failure` et `log_on_success`).

Pour obtenir une liste complète des options de journalisation, consultez la page de manuel de `xinetd.conf`.

17.4.3.2. Options de contrôle d'accès

Les utilisateurs de services xinetd peuvent choisir d'utiliser les règles de contrôle d'accès des enveloppeurs TCP, d'effectuer le contrôle d'accès par le biais des fichiers de configuration de xinetd ou de recourir à un mélange des deux. Des informations sur l'utilisation des fichiers de contrôle d'accès d'hôtes des enveloppeurs TCP se trouvent dans la Section 17.2.

Cette section examine l'utilisation de xinetd pour contrôler l'accès aux services.

Remarque

À la différence des enveloppeurs TCP, les modifications du contrôle d'accès ne prennent effet que si l'administrateur de xinetd redémarre le service xinetd.

De plus, contrairement aux enveloppeurs TCP, le contrôle d'accès par xinetd concerne uniquement les services contrôlés par xinetd.

Le contrôle de l'accès des hôtes avec xinetd est différent de la méthode utilisée par les enveloppeurs TCP. Alors que ces derniers placent toutes les configurations d'accès dans deux fichiers, à savoir /etc/hosts.allow et /etc/hosts.deny, le contrôle d'accès avec xinetd se trouve dans le fichier de configuration de chaque service au sein du répertoire /etc/xinetd.d.

Les options d'accès des hôtes figurant ci-après sont prises en charge par xinetd :

- only_from — Permet seulement aux hôtes spécifiés d'utiliser le service.
- no_access — Empêche les hôtes spécifiés d'utiliser le service.
- access_times — Spécifie la fourchette de temps pendant laquelle un service particulier peut être utilisé. Cette durée doit être stipulée dans un format de notation sur 24 heures de type HH :MM-HH:MM.

Les options only_from et no_access peuvent utiliser une liste d'adresses IP ou de noms d'hôtes ou peuvent également spécifier un réseau entier. Comme avec les enveloppeurs TCP, la combinaison du contrôle d'accès de xinetd avec une configuration de journalisation améliorée permet d'accroître la sécurité en empêchant les requêtes provenant d'hôtes bannis tout en enregistrant des informations détaillées sur chaque tentative de connexion.

Par exemple, le fichier suivant /etc/xinetd.d/telnet peut être utilisé non seulement pour bloquer l'accès à Telnet à partir d'un groupe de réseaux spécifiques mais également pour limiter la fourchette de temps globale pendant laquelle même les utilisateurs autorisés peuvent se connecter :

```
service telnet
{
        disable         = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        no_access       = 10.0.1.0/24
        log_on_success  += PID HOST EXIT
        access_times    = 09:45-16:15
}
```

Dans cet exemple, lorsque tout système client provenant du réseau 10.0.1.0/24, tel que 10.0.1.2, essaie d'accéder au service Telnet, il reçoit le message reproduit ci-dessous, indiquant que la connexion a été fermée par un hôte étranger :

```
Connection closed by foreign host.
```

De plus, leurs tentatives de connexion sont enregistrées dans `/var/log/secure` de la manière suivante :

```
May 15 17:38:49 boo xinetd[16252]: START: telnet pid=16256 from=10.0.1.2
May 15 17:38:49 boo xinetd[16256]: FAIL: telnet address from=10.0.1.2
May 15 17:38:49 boo xinetd[16252]: EXIT: telnet status=0 pid=16256
```

Lorsque des enveloppeurs TCP sont utilisés de concert avec les accès de contrôle de `xinetd`, il est important de bien comprendre la relation existant entre les deux mécanismes de contrôle d'accès.

Ci-dessous figure l'ordre des opérations que `xinetd` suit lorsqu'un client demande à établir une connexion :

1. Le démon `xinetd` accède aux règles d'accès d'hôtes des enveloppeurs TCP par le biais d'un appel à la bibliothèque `libwrap.a`. Si une règle de refus (deny) s'applique à l'hôte client, la connexion est abandonnée. Si une règle d'autorisation (allow) s'applique à l'hôte client, la connexion est passée à `xinetd`.
2. Le démon `xinetd` vérifie ses propres règles de contrôle d'accès aussi bien pour le service `xinetd` que pour le service demandé. Si une règle de refus (deny) s'applique à l'hôte client, la connexion est abandonnée. Sinon, `xinetd` démarre une instance du service demandé et lui cède le contrôle de la connexion.

Important

Il convient d'être très prudent lors de l'utilisation des contrôles d'accès des enveloppeurs TCP conjointement avec les contrôles d'accès de `xinetd`. En effet, une mauvaise configuration peut entraîner des effets indésirables.

17.4.3.3. Options de liaison et redirection

Les fichiers de configuration de services pour `xinetd` prennent en charge la liaison du service à une adresse IP et la redirection de requêtes entrantes pour ce service vers une autre adresse IP, un autre nom d'hôte ou un autre port.

La liaison est contrôlée par l'option `bind` dans les fichiers de configuration spécifiques à chaque service et lie le service à une adresse IP dans le système. Une fois configurée, l'option `bind` autorise seulement des requêtes pour l'adresse IP adéquate à se connecter au service. De cette manière, différents services peuvent se trouver liés à différentes interfaces réseau selon les besoins.

Cet aspect est particulièrement utile pour les systèmes à adaptateurs de réseaux multiples ou ayant de multiples adresses IP configurées. Sur un tel système, des services non-sécurisés, comme Telnet, peuvent être configurés de manière à recevoir des requêtes seulement sur l'interface connectée à un réseau privé et pas sur l'interface connectée à l'Internet.

L'option `redirect` accepte une adresse IP ou un nom d'hôte suivi par un numéro de port. Elle permet de configurer le service de manière à ce qu'il redirige toute requête pour ce service vers l'hôte et le numéro de port spécifiés. Cette fonction peut être employée pour pointer vers un autre numéro de port sur le même système, rediriger la requête vers une autre adresse IP sur la même machine, déplacer la requête vers un système et numéro de port totalement différents ou pour utiliser toute combinaison des options mentionnées. De cette façon, un utilisateur se connectant à un certain service sur un système peut être rerouté vers un autre système sans interruption.

Le démon xinetd peut accomplir cette redirection en créant un processus qui reste actif pour la durée de la connexion entre l'ordinateur du client effectuant la requête et l'hôte fournissant le service proprement dit, en transférant les données entre les deux systèmes.

Les avantages des options bind et redirect se remarquent le plus lorsque ces options sont utilisées ensemble. En liant un service à une adresse IP particulière sur un système puis en redirigeant les requêtes pour ce service vers une seconde machine que seule la première peut percevoir, il est possible d'utiliser un système interne pour fournir des services à un réseau totalement différent. Ces options peuvent également être utilisées pour non seulement limiter l'exposition d'un service particulier sur un ordinateur multi-site à une adresse IP connue mais aussi pour rediriger toute requête pour ce service vers une autre machine spécialement configurée à cet effet.

Examinons par exemple le cas d'un système utilisé comme pare-feu avec ce paramétrage pour son service Telnet :

```
service telnet
{
        socket_type  = stream
        wait   = no
        server   = /usr/sbin/in.telnetd
        log_on_success  += DURATION USERID
        log_on_failure  += USERID
        bind                    = 123.123.123.123
        redirect                = 10.0.1.13 23
}
```

Les options bind et redirect présentes dans ce fichier garantissent que le service Telnet sur cette machine soit lié à l'adresse IP externe (123.123.123.123), celle qui prend en charge l'Internet. De plus, toute requête de service Telnet envoyée vers 123.123.123.123 est redirigée via un second adaptateur réseau vers une adresse IP interne (10.0.1.13) à laquelle seuls le pare-feu et les systèmes internes peuvent accéder. Le pare-feu envoie alors la communication entre les deux systèmes et le système se connectant pense qu'il est connecté à 123.123.123.123 alors qu'il est en fait connecté à une machine différente.

Cette fonction est particulièrement utile pour les utilisateurs avec des connexion à large bande et avec seulement une adresse IP fixe. Lors de l'utilisation de la traduction d'adresses de réseau (ou NAT de l'anglais Network Address Translation), les systèmes situés derrière la machine passerelle, qui utilisent des adresses IP exclusivement internes, ne sont pas disponibles depuis l'extérieur du système passerelle. Toutefois, avec certains services contrôlés par xinetd et configurés avec les options bind et redirect, la machine passerelle peut servir de proxy entre les systèmes externes et une machine interne particulière qui est configurée pour fournir le service en question. De plus, les diverses options de contrôle d'accès et de journalisation de xinetd peuvent également servir comme protections supplémentaires.

17.4.3.4. Options de gestion des ressources

Le démon xinetd permet d'ajouter un niveau élémentaire de protection contre des attaques de Refus de service (ou DoS, de l'anglais Denial of Service). Ci-dessous figure une liste des directives pouvant aider à limiter l'efficacité de telles attaques :

- per_source — Détermine le nombre maximal d'instances d'un service spécifique en fonction de l'adresse IP d'origine. Elle n'accepte comme argument que des chiffres entiers et peut être utilisée aussi bien dans xinetd.conf que dans des fichiers de configuration spécifiques aux services stockés dans le répertoire xinetd.d/.
- cps — Détermine le nombre maximal de connexions par seconde. Cette directive accepte deux arguments sous forme de valeurs entières séparés par un espace blanc. Le premier représente le nombre maximal de connexions autorisées à un service par seconde. Le deuxième correspond au

nombre de secondes pendant lequel xinetd doit attendre avant de réactiver le service. Il n'accepte que des nombres entiers comme argument et peut être utilisé aussi bien dans xinetd.conf que dans les fichiers de configuration spécifiques au service contenus dans le répertoire xinetd.d/.

- max_load — Définit le seuil d'utilisation d'un processeur (CPU) pour un service. Cette directive accepte un argument avec une valeur flottante.

D'autres options peuvent être utilisées pour la gestion des ressources avec xinetd. Reportez-vous au chapitre intitulé *Sécurité du serveur* du *Guide de sécurité de Red Hat Enterprise Linux* pour obtenir de plus amples informations. Consultez également la page de manuel de xinetd.conf.

17.5. Ressources supplémentaires

Des informations supplémentaires sur les enveloppeurs TCP et xinetd sont disponibles sur la documentation du système et sur Internet.

17.5.1. Documentation installée

La documentation installée sur votre système est un bon endroit pour commencer des recherches sur les enveloppeurs TCP, sur xinetd et sur les options de configuration de contrôle d'accès.

- /usr/share/doc/tcp_wrappers-<*version*>/ — Ce répertoire contient un fichier README décrivant le fonctionnement des enveloppeurs TCP et les divers risques potentiels d'usurpation d'adresse et de nom d'hôte.
- /usr/share/doc/xinetd-<*version*>/ — Ce répertoire comprend un fichier README qui examine les différents aspects du contrôle d'accès ainsi qu'un fichier sample.conf offrant différentes idées quant à la modification des fichiers de configuration spécifiques à des services donnés qui figurent dans le répertoire /etc/xinetd.d/.
- Pages de manuel des enveloppeurs TCP et pages en relation avec xinetd — Il existe un certain nombre de pages de manuel correspondant aux diverses applications et fichiers de configuration en relation avec les enveloppeurs TCP et xinetd. Les listes suivantes représentent certaines des pages de manuel les plus importantes.

  Application serveur

  - man xinetd — La page de manuel relative au démon du super-service xinetd.

  Fichiers de configuration

  - man 5 hosts_access — La page de manuel relative aux fichiers de contrôle d'accès des hôtes des enveloppeurs TCP.
  - man hosts_options — La page de manuel relative aux champs d'options des enveloppeurs TCP.
  - man xinetd.conf — La page de manuel énumérant les options de configuration de xinetd.

17.5.2. Sites Web utiles

- http://www.xinetd.org — La page d'accueil de `xinetd`, contenant des exemples de fichiers de configuration, une liste complète des fonctions et un FAQ très riche.
- http://www.macsecurity.org/resources/xinetd/tutorial.shtml — Un tutoriel complet décrivant les nombreuses manières différentes de modifier les fichiers de configuration par défaut de `xinetd` afin qu'ils correspondent à des but de sécurité spécifiques.

17.5.3. Livres sur le sujet

- *Guide de sécurité de Red Hat Enterprise Linux* ; Red Hat, Inc. — Fournit un aperçu de la sécurité en matière de poste de travail, serveur et réseau et contient des suggestions spécifiques quant aux enveloppeurs TCP et au service `xinetd`.
- *Hacking Linux Exposed* de Brian Hatch, James Lee et George Kurtz ; Osbourne/McGraw-Hill — Représente une excellente ressource sur la sécurité et contient des informations sur les enveloppeurs TCP et le service `xinetd`.

Chapitre 18.

iptables

Avec Red Hat Enterprise Linux sont installés des outils avancés permettant le *filtrage de paquets* réseau — le processus consistant à contrôler les paquets réseau lorsqu'ils entrent, traversent et sortent de la pile réseau au sein du noyau. Les versions de noyaux antérieurs à 2.4 utilisaient `ipchains` pour le filtrage de paquets et faisaient appel à des listes de règles appliquées aux paquets à chaque étape du processus de filtrage. Avec l'arrivée du noyau 2.4 est apparu `iptables` (aussi appelé *netfilter*), qui est semblable à la commande `ipchains` mais multiplie les potentialités et le degré de contrôle disponible en matière de filtrage de paquets réseau.

Ce chapitre décrit en détail les principes de base en matière de filtrage de paquets, explique les différences entre `ipchains` et `iptables`, présente les différentes options disponibles avec `iptables` et finalement montre comment maintenir l'intégrité des règles de filtrage entre les démarrages du système.

Pour obtenir des instructions sur la construction de règles `iptables` ou sur la configuration d'un pare-feu basé sur ces règles, reportez-vous à la Section 18.7.

Avertissement

Le mécanisme de pare-feu par défaut avec le noyau 2.4 et des noyaux plus récents est `iptables`, mais `iptables` ne peut pas être utilisé si `ipchains` est déjà en cours d'exécution. Si `ipchains` est présent au démarrage, le noyau émet un message d'erreur et ne réussit pas à démarrer `iptables`.

Ces messages d'erreur n'affectent pas la fonctionnalité d'`ipchains`.

18.1. Filtrage de paquets

Dans le noyau Linux est intégrée la capacité de filtrer des paquets, permettant à certains d'entre eux d'être reçus par le système ou de le traverser alors que d'autres sont bloqués. Le netfilter du noyau contient trois *tables* ou *listes de règles* intégrées, à savoir :

- `filter` — Table par défaut pour le traitement des paquets réseau.
- `nat` — Table utilisée pour modifier les paquets qui créent une nouvelle connexion et utilisée pour la traduction d'adresses réseau (ou *NAT* de l'anglais *Network Address Translation*).
- `mangle` — Table utilisée pour la modification de types spécifiques de paquets.

Astuce

Outre ses tables intégrées, des tables spécifiques peuvent être créées et enregistrées dans le répertoire `/lib/modules/<kernel-version>/kernel/net/ipv4/netfilter/` où `<kernel-version>` correspond au numéro de version du noyau.

Chacune de ces tables comporte à son tour un groupe de *chaînes* intégrées qui correspondent aux actions effectuées par netfilter sur le paquet.

Les chaînes pour la table `filter` sont les suivantes :

- *INPUT* — Cette chaîne s'applique aux paquets ciblés pour l'hôte.
- *OUTPUT* — Cette chaîne s'applique aux paquets réseau générés localement.
- *FORWARD* — Cette chaîne s'applique aux paquets routés à travers l'hôte.

Les chaînes pour la table `nat` sont les suivantes :

- *PREROUTING* — Cette chaîne modifie les paquets lorsqu'ils arrivent.
- *OUTPUT* — Cette chaîne modifie des paquets réseau générés localement avant qu'ils ne soient envoyés.
- *POSTROUTING* — Cette chaîne modifie les paquets avant qu'ils ne soient envoyés.

Les chaînes intégrées pour la table `mangle` sont les suivantes :

- *INPUT* — Cette chaîne modifie des paquets réseau ciblés pour l'hôte.
- *OUTPUT* — Cette chaîne modifie des paquets réseau générés localement avant qu'ils ne soient envoyés.
- *FORWARD* — Cette chaîne modifie des paquets réseau routés à travers l'hôte.
- *PREROUTING* — Cette chaîne modifie les paquets réseau entrants avant qu'ils ne soient routés.
- *POSTROUTING* — Cette chaîne modifie les paquets avant qu'ils ne soient envoyés.

Chaque paquet réseau reçu ou envoyé par un système Linux est soumis à au moins une règle. Un paquet peut toutefois être soumis à plusieurs règles à l'intérieur de chaque table avant d'arriver à la fin de la chaîne. La structure et le rôle de ces règles peuvent changer, mais elles visent généralement à identifier un paquet en provenance ou à destination d'une adresse IP donnée ou d'un groupe d'adresses, lors de l'utilisation d'un protocole et d'un service réseau particuliers.

Remarque

N'utilisez pas de noms de domaines pleinement qualifiés dans les règles de pare-feu qui sont enregistrées dans les fichiers `/etc/sysconfig/iptables` ou `/etc/sysconfig/ip6tables`. Dans l'exemple ci-dessous, `iptables -A FORWARD -s example.com -i eth0 -j DROP example.com` n'est pas valide parce que le service `iptables` est lancé au démarrage avant tout DNS associé aux services, ce qui entraîne un message d'erreur. Seules des adresses IP sont valides dans la création de règles de pare-feu.

Indépendamment de leur destination, lorsque les paquets correspondent à une règle précise présente dans une des tables, ils se voient assigner une *cible* ou font l'objet d'une certaine action. Si la règle spécifie une cible de type `ACCEPT` pour un paquet vérifié, il évite les autres contrôles de règles et peut procéder vers sa destination. En revanche, si une règle spécifie une cible de type `DROP`, le paquet est abandonné et se voit refuser l'accès au système ; rien n'est envoyé en retour à l'hôte qui a expédié le paquet. Si une règle spécifie une cible de type `QUEUE`, le paquet est mis en attente dans l'espace-utilisateur (aussi appelé user-space). Finalement, si une règle spécifie une cible de type `REJECT` en option, le paquet est "abandonné" par rejet et dans ce cas, un "paquet d'erreur" est envoyé en retour à l'expéditeur.

Chaque chaîne dispose d'une politique par défaut pour accepter (`ACCEPT`), abandonner (`DROP`), rejeter (`REJECT`) ou mettre en attente (`QUEUE`). Si aucune des règles présentes dans la chaîne ne s'applique au paquetage, celui-ci est traité en fonction de la politique par défaut de la chaîne.

La commande `iptables` permet de configurer ces tables et d'en créer de nouvelles si nécessaire.

18.2. Différences entre iptables et ipchains

Au premier abord, ipchains et iptables semblent assez similaires. Les deux méthodes de filtrage de paquets font appel à des chaînes de règles actives à l'intérieur du noyau Linux pour décider du traitement des paquets qui répondent à certaines règles. Cependant, la commande iptables représente une manière plus flexible de filtrer les paquets en donnant à l'administrateur un degré de contrôle plus élevé, sans pour autant ajouter un degré plus élevé de complexité.

Ainsi, les utilisateurs à l'aise avec la commande ipchains devront tenir compte des différences importantes qui existent entre les commandes ipchains et iptables, avant d'essayer de se servir d'iptables :

- *Sous iptables, chaque paquet filtré est traité en utilisant les règles d'une seule chaîne, plutôt que celles de chaînes multiples.* Par exemple, un paquet identifié comme FORWARD pénétrant dans un système à l'aide de ipchains devrait passer à travers les chaînes INPUT, FORWARD et OUTPUT afin de pouvoir poursuivre sa progression vers sa destination. Toutefois, iptables envoie les paquets uniquement à la chaîne INPUT s'ils sont destinés au système local et les envoie seulement à la chaîne OUTPUT, s'ils ont été créés par le système local. Pour cette raison, il est très important de bien placer la règle destinée au contrôle d'un paquet spécifique dans la règle qui effectue le traitement proprement dit du paquet.
- *La cible DENY a été remplacée par la cible DROP.* Dans ipchains, les paquets qui répondaient aux critères d'une règle présente dans une chaîne pouvaient être dirigés vers la cible DENY. Cette cible doit être remplacée par une cible DROP iptables.
- *Lorsque des options sont placées dans une règle, l'ordre est important.* Avec ipchains, l'ordre des options s'appliquant aux règles n'est pas important. La commande iptables elle, utilise une syntaxe plus stricte. Ainsi, dans les commandes iptables le protocole spécifique (ICMP, TCP ou UDP) doit être précisé avant les ports d'origine ou de destination.
- *Lorsque le type d'interface réseau à utiliser dans une règle est précisé, seules des interfaces entrantes (option -i) peuvent être employées avec les chaînes INPUT ou FORWARD et des interfaces sortantes (option -o) avec les chaînes FORWARD ou OUTPUT*. Ceci est nécessaire d'une part parce que les chaînes OUTPUT ne sont plus utilisées par les interfaces entrantes et d'autre part, parce que les chaînes INPUT ne sont pas vues par les paquets traverant des interfaces sortantes.

Les informations fournies ci-dessus ne constituent en aucun cas une liste complète des changements apportés car iptables est en fait un filtre réseau qui a entièrement été réécrit. Pour obtenir des informations plus spécifiques, reportez-vous au document *Linux Packet Filtering HOWTO* référencé dans la Section 18.7 (HOWTO Filtrage de paquets réseau sous Linux).

18.3. Options utilisées avec les commandes iptables

Les règles permettant le filtrage de paquets sont mises en oeuvre en exécutant la commande iptables. Les aspects suivants du paquet sont le plus souvent utilisés comme critère :

- *Type de paquet* — Spécifie le type de paquets que la commande filtre.
- *Origine/Destination du paquet* — Spécifie les paquets que la commande filtre en fonction de l'origine ou de la destination du paquet.
- *Cible* — Spécifie l'action à appliquer sur les paquets répondant aux critères évoqués ci-dessus.

Pour obtenir de plus amples informations sur des options spécifiques qui traitent ces aspects des paquets, reportez-vous à la Section 18.3.4 et à la Section 18.3.5.

Les options utilisées avec des règles iptables données doivent être regroupées logiquement en fonction du but et des conditions de la règle globale, afin que la règle soit valide. Le reste de cette section examine des options couramment utilisées avec la commande iptables.

18.3.1. Structure des options d'iptables

Beaucoup de commandes iptables ont la structure suivante :

```
iptables [-t <table-name>] <command> <chain-name> <parameter-1> \
         <option-1> <parameter-n> <option-n>
```

L'option <*table-name*> permet à l'utilisateur de sélectionner une autre table que la table filter par défaut devant être utilisée avec cette commande. L'option <*command*> stipule une action spécifique à accomplir, telle que l'ajout ou l'élimination d'une règle spécifiée par <*chain-name*>. Après l'option <*chain-name*> figurent des paires de paramètres et d'options qui définissent comment traiter un paquet répondant aux critères de la règle.

En examinant la structure d'une commande iptables, il est important de se rappeler que contrairement à la plupart autres commandes, la longueur et la complexité d'une commande iptables varie en fonction de son but. Une commande destinées à éliminer une règle d'une chaîne peut être très courte, alors qu'une commande visant à filtrer les paquets d'un sous-réseau à l'aide d'un certain nombre de paramètres et d'options peut être plutôt longue. Lors de la création de commandes iptables, il est important de savoir que nombre de paramètres et d'options peuvent nécessiter des paramètres et d'options supplémentaires pour mieux rafiner la requête de l'option précédente. Pour élaborer une règle valide, cette chaîne d'actions doit continuer jusqu'à ce que chaque paramètre et option nécessitant un autre ensemble d'options ait été traité.

Saisissez la commande iptables -h pour obtenir une liste exhaustive de structures de la commande iptables.

18.3.2. Options de commande

Les options de commande donnent à iptables l'instruction d'exécuter une action spécifique. Une seule option de commande est autorisée pour chaque commande iptables. À l'exception de la commande d'aide, toutes les autres commandes doivent être écrites en majuscules.

Les options de commande disponibles avec iptables sont les suivantes :

- -A — Ajoute la règle iptables à la fin d'une chaîne donnée. On utilise cette option pour ajouter simplement une règle lorsque l'ordre des règles à l'intérieur de la chaîne n'est pas primordial.
- -C — Contrôle une règle donnée avant de l'ajouter à la chaîne spécifiée par l'utilisateur. Cette commande peut vous aider à écrire des règles iptables compliquées en vous indiquant les paramètres et options supplémentaires à établir.
- -D — Élimine une règle à l'intérieur d'une chaîne donnée de façon numérique (comme par exemple en utilisant 5 pour la cinquième règle d'une chaîne). Il est également possible de taper la règle complète et iptables efface la règle dans la chaîne correspondante.
- -E — Change le nom d'une chaîne spécifiée par un utilisateur. Cette option n'affecte en aucun cas la structure de la table.
- -F — Supprime la chaîne sélectionnée, entraînant par là-même l'élimination de toutes les règles de la chaîne. Si aucune chaîne n'est spécifiée, cette commande supprime chaque règle contenue dans chaque chaîne.
- -h — Fournit une liste des structures de scommande, ainsi qu'un bref résumé des paramètres et options des commandes.
- -I — Insère une règle à l'intérieur d'une chaîne, à un point précis, spécifié par une valeur entière définie par l'utilisateur. Si aucun numéro n'est spécifié, iptables place la commande au tout début de la chaîne.

Attention

Lors de l'utilisation de l'option `-A` ou de l'option `-I`, prêtez une attention toute particulière à l'ordre dans lequel les règles apparaissent dans une chaîne. En effet, ce dernier est très important car il permet de déterminer les règles précises devant s'appliquer à des paquets spécifiques.

- `-L` — Établit la liste complète des règles dans la chaîne indiquée après la commande. Pour dresser une liste de toutes les règles présentes dans toutes les chaînes contenues dans la table de`filter` par défaut, ne précisez ni chaîne, ni table. Sinon, la syntaxe à utiliser pour établir la liste des règles contenues dans une chaîne donnée d'une table précise, doit être la suivante :
  `iptables -L <chain-name> -t <table-name>`

  Pour toute information sur les options supplémentaires utilisées avec l'option de commande `-L` qui fournit le nombre de règles et permet une description plus détaillée de ces dernières, consultez la Section 18.3.6.
- `-N` — Crée une nouvelle chaîne avec un nom spécifié par l'utilisateur.
- `-P` — Définit la politique par défaut d'une chaîne donnée, de sorte que des paquets traversant une chaîne entière sans satisfaire les critères d'une règle soient envoyés vers la cible spécifiée, telle que ACCEPT ou DROP.
- `-R` — Remplace une règle dans une chaîne donnée. Il est impératif d'utiliser un numéro de règle après le nom de chaîne. La première règle dans une chaîne correspond à la règle numéro un.
- `-X` — Supprime une chaîne spécifiée par un utilisateur. L'élimination d'une chaîne intégrée appartenant à une table quelconque n'est pas permise.
- `-Z` — Remet à zéro les compteurs d'octets et de paquets dans toutes les chaînes pour une table spécifique.

18.3.3. Options de paramètre d'`iptables`

Une fois que certaines commandes `iptables` ont été spécifiées (y compris celles utilisées pour l'ajout, l'élimination, l'insertion ou le remplacement de règles à l'intérieur d'une chaîne donnée), il est nécessaire d'ajouter d'autres paramètres pour la construction d'une règle de filtrage de paquets.

- `-c` — Effectue une remise à zéro des compteurs pour une règle donnée. Ce paramètre accepte les options `PKTS` (paquets) et `BYTES` (octets) pour spécifier le compteur à remettre à zéro.
- `-d` — Définit le nom d'hôte du destinataire, l'adresse IP ou le réseau du paquetage qui correspond à la règle. Lorsqu'un réseau répond aux critères de la règle, les formats suivants sont pris en charge pour l'adresse IP/masque réseau :
  - *`N.N.N.N/M.M.M.M`* — où *`N.N.N.N`* correspond à la plage d'adresses IP et *`M.M.M.M`* au masque réseau.
  - *`N.N.N.N/M`* — où *`N.N.N.N`* correspond à la plage d'adresses IP et *`M`* au masque réseau.
- `-f` — Applique cette règle uniquement aux paquets fragmentés.

  En utilisant le point d'exclamation comme option (`!`) après ce paramètre, seuls les paquets non-fragmentés seront comparés aux critères des règles.
- `-i` — Règle l'interface réseau entrante, telle que `eth0` ou `ppp0`. Avec `iptables`, ce paramètre optionnel ne peut être utilisé qu'avec des chaînes INPUT et FORWARD lorsqu'elles sont utilisées avec la table `filter` et la chaîne PREROUTING lorsqu'elle est utilisée avec les tables `nat` et `mangle`.

  Ce paramètre prend également en charge les options spéciales ci-dessous :

- Point d'exclamation (!) — Inverse la directive, c'est-à-dire que toutes les interfaces spécifiées sont exclues de cette règle.
- Le symbole plus (+) — Représente un caractère générique utilisé pour comparer toutes les interfaces qui correspondent à la chaîne spécifiée. Par exemple, le paramètre -i eth+ appliquerait cette règle à toutes les interfaces Ethernet, mais ne prendrait pas en compte les autres interfaces, comme ppp0.

Si le paramètre -i est utilisé sans qu'aucune interface ne soit spécifiée, toutes les interfaces sont affectées par la règle.

- -j — Passe directement à la cible spécifiée lorsqu'un paquetage correspond à une règle particulière. Les cibles valides pouvant être utilisées après l'option -j incluent des options standard (à savoir ACCEPT, DROP, QUEUE et RETURN), ainsi que des options étendues qui sont disponibles grâce aux modules chargés par défaut avec le paquetage RPM iptables de Red Hat Enterprise Linux, comme par exemple LOG, MARK et REJECT. Consultez la page de manuel d'iptables pour obtenir plus d'informations sur les cibles mentionnées ici et sur d'autres cibles.

  Il est également possible de diriger un paquet correspondant à une règle vers une chaîne définie par l'utilisateur, située en dehors de la chaîne actuelle, afin que d'autres règles puissent être appliquées à ce paquet.

  Si aucune cible n'est spécifiée, le paquet continue sans qu'aucune autre action ne soit entreprise. Ceci étant, le compteur de cette règle avance tout de même d'une unité.
- -o — Paramètre l'interface sortante pour une règle donnée et ne peut être utilisée qu'avec des chaînes OUTPUT et FORWARD dans la table filter et la chaîne POSTROUTING dans les tables nat et mangle. Les options de ce paramètre sont les mêmes que pour les paramètres relatifs aux interfaces réseau entrantes (-i).
- -p — Paramètre le protocole IP pour la règle, qui peut être icmp, tcp, udp ou all, afin qu'il corresponde à tous les protocoles possibles. De plus, il est possible d'utiliser tout protocole inclus dans /etc/protocols. Si l'option est omise lors de la création de la règle, l'option all est considérée comme étant la valeur par défaut.
- -s — Définit l'origine d'un paquet particulier en utilisant la même syntaxe que pour le paramètre de destination (-d).

18.3.4. Options de concordance d'iptables

Différents protocoles réseau offrent des options de contrôle de concordance spécifiques qui peuvent être configurées de manière à comparer un paquet donné en utilisant ce protocole. Évidemment, il est nécessaire d'identifier préalablement le protocole en question dans la commande iptables. Par exemple, -p tcp <*protocol-name*> (où <*protocol-name*> correspond au protocole cible) fait en sorte que des options soient disponibles pour le protocole spécifié.

18.3.4.1. Protocole TCP

Les options de concordance disponibles pour le protocole TCP (-p tcp) sont les suivantes :

- --dport — Paramètre le port de destination pour le paquet. Vous pouvez utiliser le nom d'un service réseau (comme www ou smtp), un numéro de port ou une plage de numéros de port pour configurer cette option. Pour parcourir les noms et alias de services réseau et les numéros de port utilisés, affichez le fichier /etc/services. L'option de concordance --destination-port est identique à l'option --dport.

  Pour indiquer une plage de numéros de port, il suffit de séparer les numéros par le symbole des deux points (:), comme dans l'exemple suivant : -p tcp --dport 3000:3200. La plus grande plage valide est 0:65535.

Utilisez un point d'exclamation (!) après l'option --dport pour comparer tous les paquets qui *n'utilisent pas* ce service réseau ou port.

- --sport — Paramètre le port d'origine du paquet, en utilisant les mêmes options que --dport. L'option de concordance --source-port est identique à l'option --sport.
- --syn — S'applique à tous les paquets TCP, appelés communément *paquets SYN*, conçus pour initier la communication. Aucun paquet transportant des données de charge utile n'est touché. En plaçant un point d'exclamation (!) comme indicateur après l'option --syn, tous les paquets non-SYN seront comparés.
- --tcp-flags — Permet à des paquets TCP avec des bits ou des indicateurs définis, d'être comparés à une règle. L'option de concordance --tcp-flags accepte deux paramètres. Le premier est le masque, qui définit l'indicateur à examiner dans le paquet. Le second se rapporte à l'indicateur qui doit être défini pour la concordance.

  Les indicateurs disponibles sont les suivants :

  - ACK
  - FIN
  - PSH
  - RST
  - SYN
  - URG
  - ALL
  - NONE

  Par exemple, une règle iptables contenant -p tcp --tcp-flags ACK,FIN,SYN SYN ne comparera que les paquets TCP ayant l'indicateur SYN défini et les indicateurs ACK et FIN non-définis.

  L'utilisation d'un point d'exclamation (!) après --tcp-flags inverse l'effet de l'option de concordance.
- --tcp-option — Essaie de comparer des options spécifiques à TCP qui peuvent être définies dans un paquet donné. Cette option de concordance peut aussi être inversée en utilisant un point d'exclamation (!).

18.3.4.2. Protocole UDP

Les options de concordance suivantes s'appliquent au protocole UDP (-p udp) :

- --dport — Spécifie le port de destination du paquet UDP, utilisant le nom du service, le numéro de port ou une plage de numéros de ports. L'option de concordance --destination-port est identique à l'option --dport.
- --sport — Spécifie le port d'origine du paquet UDP, utilisant le nom du service, le numéro de port ou une plage de numéros de ports. L'option de concordance --source-port est identique à l'option --sport.

18.3.4.3. Protocole ICMP

Les options de concordance suivantes sont disponibles pour le protocole Internet Control Message Protocol (ICMP) (-p icmp) :

- `--icmp-type` — Détermine le nom ou le numéro du type d'ICMP à comparer avec cette règle. Une liste de noms ICMP valides est disponible en tapant la commande `iptables -p icmp -h`.

18.3.4.4. Modules avec options de concordance supplémentaires

Des options de concordance supplémentaires sont également disponibles par l'entremise des modules chargés par la commande `iptables`. Pour utiliser un module d'option de concordance, chargez le module en l'appelant par son nom à l'aide de l'option `-m`, comme par exemple : `-m <module-name>` (où `<module-name>` correspond au nom du module).

Un nombre important de modules est disponible par défaut. Il est même possible de créer des modules qui fournissent des fonctionnalités supplémentaires.

Ci-dessous figure une liste partielle des modules les plus couramment utilisés :

- Module `limit` — Permet de limiter le nombre de paquets qui sont comparés à une règle donnée. Cette option se révèle tout particulièrement utile lorsqu'elle est utilisée avec la cible `LOG` car elle permet d'éviter que les paquets concordants n'inondent le journal du système avec des messages répétitifs ou qu'ils ne consomment trop de ressources système. Reportez-vous à la Section 18.3.5 pour obtenir de plus amples informations sur la cible `LOG`.

  Le module `limit` active les options suivantes :

  - `--limit` — Détermine le nombre de concordances pour un espace-temps donné, grâce à un modificateur nombre (number) et temps (time) paramétré selon le fomrat suivant : `<number>/<time>`. Par exemple, en écrivant `--limit 5/hour`, une règle effectue son contrôle de concordance seulement cinq fois en une heure.

    Si aucun modificateur nombre ou temps n'est précisé, une valeur par défaut de `3/hour` (3 fois en une heure) sera retenue.

  - `--limit-burst` — Détermine le nombre de paquets pouvant être comparés à une règle, à un moment donné. Cette option qui devrait être utilisée conjointement avec l'option `--limit`, accepte un numéro pour définir le seuil maximal.

    Si aucun numéro n'est indiqué, cinq paquets seulement sont au départ comparés à la règle.

- module `state` — Active la concordance d'état.

  Le module `state` active les options suivantes :

  - `--state` — Établit la correspondance d'un paquet avec les états de connexion suivants :
    - `ESTABLISHED` — Le paquet concordant est associé à d'autres paquets dans une connexion établie.
    - `INVALID` — Ce paquet concordant ne peut être pas lié à une connexion connue.
    - `NEW` — Le paquet concordant crée une nouvelle connexion ou fait partie d'une connexion à double sens qui n'a pas été vue précédemment.
    - `RELATED` — Le paquet concordant établit une nouvelle connexion qui est d'une manière ou d'une autre apparentée à une connexion existante.

    Ces états de connexion peuvent être employés de concert avec d'autres à condition qu'ils soient séparés par des virgules, comme par exemple : `-m state --state INVALID,NEW`.

- `mac` module — Active la concordance d'une adresse MAC matérielle.

  Le module `mac` active l'option suivante :

- `--mac-source` — Établit la correspondance avec une adresse MAC de la carte d'interface réseau qui a envoyé le paquet. Pour exclure une adresse MAC d'une règle, placez un point d'exclamation (`!`) après l'option de concordance `--mac-source`.

Pour obtenir des informations sur les autres options de concordance disponibles à l'aide des modules, reportez-vous à la page de manuel de `iptables`.

18.3.5. Options de cible

Une fois qu'un paquet concorde avec une règle spécifique, cette dernière peut diriger le paquet vers un certain nombre de cibles qui décideront de son traitement et, si possible, effectueront des actions supplémentaires. Chaque chaîne possède une cible par défaut qui est utilisée si aucune des règles de cette chaîne ne correspond à un paquet ou si aucune des règles qui correspondent au paquet ne spécifie de cible particulière.

Ci-dessous figurent les cibles standard :

- *<user-defined-chain>* — Remplacez *<user-defined-chain>* par le nom d'une chaîne définie par l'utilisateur au sein de cette table. Cette cible transmet le paquet à la chaîne cible.
- `ACCEPT` — Autorise le paquet à continuer sa progression vers sa destination ou une autre chaîne.
- `DROP` — Abandonne le paquet sans répondre au demandeur. Le système ayant expédié ce paquet n'est pas informé de l'échec de l'opération.
- `QUEUE` — Met le paquet en attente pour un traitement par une application de l'espace-utilisateur (user-space).
- `RETURN` — Arrête le contrôle du paquet en fonction des règles en vigueur dans la chaîne actuelle. Si le paquet avec la cible `RETURN` correspond à une certaine règle appelée depuis une autre chaîne, le paquet est renvoyé à la première chaîne pour que le contrôle de la règle reprenne au point où il s'était arrêté. Dans le cas où la règle `RETURN` est utilisée dans une chaîne intégrée et que le paquet ne peut pas aller vers sa chaîne précédente, la cible par défaut pour la chaîne actuelle détermine l'action à entreprendre.

Outre ces cibles standard, d'autres cibles peuvent être utilisées avec des extensions appelées *modules cibles*. Pour obtenir de plus amples informations sur les modules d'options pour la concordance, reportez-vous à la Section 18.3.4.4.

Il existe de nombreux modules cibles étendus ; la plupart d'entre eux s'appliquent à des tables ou à des situations spécifiques. Ci-dessous figurent certains des modules cibles les plus répandus, inclus par défaut dans Red Hat Enterprise Linux :

- `LOG` — Journalise tous les paquets correspondant à cette règle. Étant donné que les paquets sont journalisés par le noyau, le fichier `/etc/syslog.conf` détermine l'emplacement où ces entrées de journal sont enregistrées. Par défaut, elles sont placées dans le fichier `/var/log/messages`.

  D'autres options peuvent être utilisées après la cible `LOG` pour spécifier le processus de journalisation, telles que :

  - `--log-level` — Détermine le niveau de priorité d'un événement de journalisation. Une liste des niveaux de priorité est disponible dans la page de manuel de `syslog.conf`.
  - `--log-ip-options` — Journalise toute option indiquée dans l'en-tête d'un paquet IP.
  - `--log-prefix` — Ajoute une chaîne d'un maximum de 29 caractères avant la ligne de journal, lorsqu'elle est écrite. Cette option est utile lors de l'écriture de filtres syslog utilisés conjointement avec la journalisation de paquets.

- `--log-tcp-options` — Journalise toute option précisée dans l'en-tête d'un paquet TCP.
- `--log-tcp-sequence` — Écrit le numéro de séquence TCP relatif au paquet dans le journal.

- `REJECT` — Renvoie un paquet d'erreur au système distant et abandonne le paquet.

  La cible `REJECT` accepte une option `--reject-with <type>` (où *<type>* correspond au type de rejet) qui permet d'inclure des informations plus détaillées avec le paquet d'erreur. Le message d'erreur `port-unreachable` (impossible d'atteindre le port) représente l'erreur *<type>* par défaut envoyée si aucune autre option n'est utilisée. Pour obtenir une liste complète des options disponibles pour *<type>*, consultez la page de manuel d'`iptables`.

D'autres extensions de cibles, dont bon nombre sont très utiles pour le masquage d'IP à l'aide de la table `nat` ou avec la modification de paquets à l'aide de la table `mangle`, figurent dans la page de manuel d'`iptables`.

18.3.6. Options de listage

La commande de listage par défaut, `iptables -L`, fournit un aperçu très élémentaire des chaînes actuelles contenues dans la table de filtres par défaut. L'utilisation d'options supplémentaires telles que celles énumérées ci-dessous, permettent d'obtenir davantage d'informations :

- `-v` — Affiche une sortie détaillée, incluuant le nombre de paquets et d'octets lus par chaque chaîne, le nombre de paquets et d'octets contrôlés par chaque règle et l'identité des interfaces liées à une règle particulière.
- `-x` — Présente les nombres selon leur valeur exacte. Sur un système très chargé, le nombre de paquets et d'octets vus par une chaîne donnée peut être abrégé en utilisant `K` (milliers), `M` (millions) et `G` (milliards) à la fin du nombre. Cette option force l'affichage du nombre complet.
- `-n` — Affiche les adresses IP et les numéros de port dand un format numérique, plutôt que d'utiliser le format par défaut constitué du nom d'hôte et du service réseau.
- `--line-numbers` — Énumère les règles dans chaque chaîne à côté de leur ordre numérique dans la chaîne. Cette option est utile lors de la tentative de suppression d'une règle donnée dans une chaîne ou lors dela localisation de l'emplacement d'une règle à insérer dans une chaîne.
- `-t` — Spécifie un nom de table.

18.4. Enregistrement des règles d'`iptables`

Les règles créées avec la commande `iptables` sont stockées en mémoire. Si le système est redémarré avant l'enregistrement de l'ensemble de règles `iptables`, toutes les règles sont perdues. Pour que des règles de filtrage réseau (netfilter) soient conservées lors d'un redémarrage, elles doivent être enregistrées. Pour ce faire, connectez-vous en tant que super-utilisateur et tapez les éléments suivants :

```
/sbin/service iptables save
```

Cette commande exécute l'init script d'`iptables`, qui lance le programme `/sbin/iptables-save` et enregistre la configuration actuelle d'`iptables` dans le fichier `/etc/sysconfig/iptables`. Le fichier `/etc/sysconfig/iptables` existant est enregistré en tant que `/etc/sysconfig/iptables.save`.

Lors du prochain démarrage, le script d'initialisation (ou init script) de `iptables` applique à nouveau les règles enregistrées dans `/etc/sysconfig/iptables` à l'aide de la commande `/sbin/iptables-restore`.

Alors qu'il est toujours préférable de tester une nouvelle règle iptables avant de l'enregistrer dans le fichier /etc/sysconfig/iptables, il est possible de copier des règles iptables dans ce fichier à partir d'une version de ce dernier provenant d'un autre ordinateur. Cette opération permet de de répandre facilement un ensemble de règles iptables à de multiples ordinateurs.

Important

Si le fichier /etc/sysconfig/iptables est distribué sur d'autres machines, il suffit de taper /sbin/service iptables restart pour que ces nouvelles règles soient appliquées.

18.5. Scripts de contrôle d'iptables

Il existe deux méthodes élémentaires pour contrôler iptables sous Red Hat Enterprise Linux, à savoir :

- **Outil de configuration du niveau de sécurité** (system-config-securitylevel) — Une interface graphique pour créer, activer et enregistrer les règles de base de pare-feu. Pour obtenir de plus amples informations sur l'utilisation de cet outil, reportez-vous au chapitre intitulé *Configuration de base d'un pare-feu* du *Guide d'administration système de Red Hat Enterprise Linux*.
- /sbin/service iptables <*option*> — Une commande exécutée par le super-utilisateur capable d'activer, de désactiver et d'effectuer d'autres fonctions de iptables par le biais de son script d'initialisation (initscript). Remplacez <*option*> dans la commande par l'une des directives suivantes :
  - start — Si un pare-feu est configuré (ce qui signifie que /etc/sysconfig/iptables existe), toutes les iptables en cours d'exécution seront complètement arrêtées, puis redémarrées à l'aide de la commande /sbin/iptables-restore. La directive start ne fonctionne que si le module de noyau ipchains n'est pas chargé.
  - stop — Si un pare-feu est en cours d'exécution, les règles de pare-feu en mémoire sont supprimées et tous les modules et les aides d'iptables sont déchargés.

    Si la directive IPTABLES_SAVE_ON_STOP au sein du fichier de configuration /etc/sysconfig/iptables-config passe de sa valeur par défaut à la valeur yes, les règles courantes sont enregistrées dans /etc/sysconfig/iptables et toutes les règles existantes sont déplacées vers le fichier /etc/sysconfig/iptables.save.

    Reportez-vous à la Section 18.5.1 pour obtenir davantage d'informations sur le fichier iptables-config.
  - restart — Si un pare-feu est en cours d'exécution, les règles de pare-feu en mémoire sont vidées et le pare-feu est redémarré s'il est configuré dans /etc/sysconfig/iptables. La directive restart ne fonctionne que si le module de noyau ipchains n'est pas chargé.

    Si la directive IPTABLES_SAVE_ON_RESTART au sein du fichier de configuration /etc/sysconfig/iptables-config passe de sa valeur par défaut à la valeur yes, les règles courantes sont enregistrées dans /etc/sysconfig/iptables et toutes les règles existantes sont déplacées vers le fichier /etc/sysconfig/iptables.save.

    Reportez-vous à la Section 18.5.1 pour obtenir davantage d'informations sur le fichier iptables-config.
  - status — Affiche à l'invite du shell le statut du pare-feu et la liste de toutes les règles activées. Si aucune règle de pare-feu n'est chargée ou configurée, cette commande l'indique.

Une liste des règles actives contenant des adresses IP au sein des listes de règles est donnée, à moins que la valeur par défaut de IPTABLES_STATUS_NUMERIC ne soit modifiée pour la valeur no dans le fichier de configuration /etc/sysconfig/iptables-config. Cette modification fait revenir la sortie de statut à des informations sur le domaine et sur l'hôte. Reportez-vous à la Section 18.5.1 pour davantage d'informations sur le fichier iptables-config.

- panic — Supprime toutes les règles de pare-feu. La politique de toutes les tables configurées est définie en tant que DROP.
- save — Enregistre les règles de pare-feu dans /etc/sysconfig/iptables à l'aide de iptables-save. Reportez-vous à la Section 18.4 pour obtenir davantage d'informations sur le sujet.

Astuce

Il est possible d'utiliser les mêmes commandes initscript pour contrôler netfilter pour IPv6 en remplaçant ip6tables par iptables dans les commandes /sbin/service présentes dans cette section. Pour obtenir davantage d'informations sur IPv6 et sur le filtrage réseau, consultez la Section 18.6.

18.5.1. Fichier de configuration des scripts de contrôle de iptables

Le comportement des scripts d'initialisation d'iptables est contrôlé par le fichier de configuration /etc/sysconfig/iptables-config. Ci-dessous figure une liste des directives contenues dans ce fichier :

- IPTABLES_MODULES — Spécifie une liste de modules iptables supplémentaires (séparés les uns des autres par des espaces) qui doivent être chargés lorsqu'un pare-feu est activé. Parmi ces derniers peuvent figurer les assistants du suivi des connexions et de NAT.
- IPTABLES_MODULES_UNLOAD — Décharge les modules à l'arrêt et au démarrage. Cette directive accepte les valeurs suivantes :
  - yes — Cette option doit être définie pour qu'un pare-feu puisse redémarrer ou s'arrêter correctement. Cette valeur est retenue comme défaut.
  - no — Cette option ne devrait être définie que s'il existe des problèmes lors du déchargement des modules netfilter.

- IPTABLES_SAVE_ON_STOP — Enregistre les règles courantes du pare-feu dans /etc/sysconfig/iptables lorsque le pare-feu est arrêté. Cette directive accepte les valeurs suivantes :
  - yes — Enregistre les règles existantes dans /etc/sysconfig/iptables lorsque le pare-feu est arrêté et déplace la version précédente vers /etc/sysconfig/iptables.save.
  - no — N'enregistre pas les règles existantes lorsque le pare-feu est arrêté. Cette valeur est retenue comme défaut.

- IPTABLES_SAVE_ON_RESTART — Enregistre les règles courantes de pare-feu lorsque le pare-feu est redémarré. Cette directive accepte les valeurs suivantes :
  - yes — Enregistre les règles existantes dans /etc/sysconfig/iptables lorsque le pare-feu est redémarré et déplace la version précédente vers /etc/sysconfig/iptables.save.

- no — N'enregistre pas les règles existantes lorsque le pare-feu est redémarré. Cette valeur est retenue comme défaut.

- IPTABLES_SAVE_COUNTER — Enregistre et restaure tous les paquets et les compteurs d'octets dans toutes les chaînes et règles. Cette directive accepte les valeurs suivantes :
  - yes — Enregistre les valeurs du compteur.
  - no — N'enregistre pas les valeurs du compteur. Cette valeur est retenue comme défaut.

- IPTABLES_STATUS_NUMERIC — Affiche une sortie de statut pour les adresses IP à la place du domaine et des noms d'hôtes. Cette directive accepte les valeurs suivantes :
  - yes — Renvoie uniquement les adresses IP avec une sortie de statut. Cette valeur est retenue comme défaut
  - no — Renvoie le domaine ou les noms d'hôtes dans une sortie de statut.

18.6. ip6tables et IPv6

Si le paquetage iptables-ipv6 est installé, netfilter sous Red Hat Enterprise Linux peut filtrer le protocole Internet IPv6 de la nouvelle génération. La commande utilisée pour manipuler le netfilter avec IPv6 est ip6tables. La plupart des directives de cette commande sont identiques à celles utilisées pour iptables, mise à part que la table nat n'est pas encore prise en charge. Cela signifie qu'il n'est pas encore possible d'effectuer des tâches de traduction d'adresses réseau pour IPv6, telles que le masquage et la redirection de ports.

Les règles enregistrées pour ip6tables sont stockées dans le fichier /etc/sysconfig/ip6tables. Les anciennes règles enregistrées par les scripts d'initialisation de ip6tables sont stockées dans le fichier /etc/sysconfig/ip6tables.save.

Le fichier de configuration pour le script d'initialisation de ip6tables est /etc/sysconfig/ip6tables-config ; les noms de chaque directive varie légèrement. Par exemple, la directive de iptables-config, IPTABLES_MODULES, est IP6TABLES_MODULES dans ip6tables-config.

18.7. Ressources supplémentaires

Veuillez consulter les informations ci-dessous pour obtenir des informations supplémentaires sur le filtrage de paquets avec iptables.

18.7.1. Documentation installée

- man iptables — Contient une description des commandes iptables ainsi qu'une liste complète des cibles, options et extensions de concordance.

18.7.2. Sites Web utiles

- http://www.netfilter.org/ — La page d'accueil du projet netfilter/iptables. Contient une série d'informations sur `iptables`, y compris un FAQ traitant de problèmes spécifiques et un certain nombre de guides rédigés par Rusty Russell, le responsable du pare-feu IP de Linux. Les documents HOWTO sur le site couvrent en anglais des sujets tels que les concepts élémentaires de mise en réseau, le filtrage de paquets et les configurations NAT.
- http://www.linuxnewbie.org/nhf/Security/IPtables_Basics.html — Une présentation simple concernant le déplacement de paquets dans le noyau Linux, ainsi qu'une introduction à la construction de commandes `iptables` simples.
- http://www.redhat.com/support/resources/networking/firewall.html — Cette page Web contient plusieurs liens vers de nombreuses mises à jour au sujet du filtrage de paquets.
- *Guide de sécurité de Red Hat Enterprise Linux* ; Red Hat, Inc. — Ce document contient un chapitre traitant du rôle des pare-feu au sein d'une stratégie de sécurité générale ainsi que des stratégies sur la construction de règles de pare-feu.
- *Guide d'administration système de Red Hat Enterprise Linux* ; Red Hat, Inc. — Ce document contient un chapitre sur la configuration de pare-feu à l'aide de l'**Outil de configuration du niveau de sécurité**.

Chapitre 19.

Kerberos

La sécurité et l'intégrité d'un système au sein d'un réseau peut être une lourde tâche. En effet, elle peut monopoliser le temps de plusieurs administrateurs rien que pour effectuer le suivi des services en cours d'exécution sur un réseau et surveiller la manière selon laquelle ils sont utilisés. De plus, l'authentification des utilisateurs auprès des services réseau peut s'avérer être une opération dangereuse lorsque la méthode utilisée par le protocole est par essence non-sécurisée, comme c'est la cas avec les protocoles FTP et telnet lors du transfert de mots de passe de manière non-cryptée sur le réseau. Kerberos représente un moyen d'éliminer le besoin de protocoles qui utilisent des méthodes d'authentification vulnérables, permettant ainsi de renforcer la sécurité réseau en général.

19.1. Qu'est-ce que Kerberos ?

Kerberos est un protocole d'authentification réseau créé par MIT qui utilise une cryptographie à clés symétriques[1] pour authentifier les utilisateurs auprès des services réseau — éliminant par là même la nécessité de transmettre des mots de passe sur le réseau. Lorsque les utilisateurs s'authentifient auprès des services réseau au moyen de Kerberos, les utilisateurs non-autorisés tentant d'intercepter des mots de passe en surveillant le trafic sur le réseau voient leurs desseins contrecarrés.

19.1.1. Avantages de Kerberos

La plupart des services réseau conventionnels utilisent des procédures d'authentification basées sur des mots de passe. Dans ce cadre, un utilisateur doit s'authentifier auprès d'un serveur réseau précis en fournissant son nom d'utilisateur et son mot de passe. Regrettablement, la transmission des informations d'authentification pour de nombreux services s'effectue de façon non-cryptée. Pour qu'une telle procédure soit sécurisée, il est essentiel que le réseau soit inaccessible aux utilisateurs externes d'une part et d'autre part, que tous les ordinateurs et utilisateurs du réseau soient dignes de confiance.

Même si c'est le cas, une fois qu'un réseau est connecté à l'Internet, on ne peut plus supposer que le réseau soit sécurisé. Il suffit à tout pirate obtenant l'accès au réseau d'utiliser un simple analyseur de paquets (aussi connu sous le nom de renifleur de paquets) pour intercepter des noms d'utilisateurs et des mots de passe envoyés en texte clair. Dans de telles circonstances, les comptes utilisateur et l'intégrité de toute l'infrastructure de sécurité sont remis en cause.

Le but essentiel de Korberos est d'éviter la transmission de mots de passe non-cryptés à travers le réseau. Lorsque Korberos est utilisé correctement, il élimine de façon efficace la menace que représentent les renifleurs de paquets pour un réseau.

19.1.2. Désavantages de Kerberos

Bien que Kerberos permette d'éliminer une sérieurse menace de sécurité, son implémentation peut être difficile pour de multiples raisons :

- La migration de mots de passe utilisateur d'une base de données de mots de passe UNIX standard, comme `/etc/passwd` ou `/etc/shadow`, vers une base de données de mots de passe Kerberos peut être relativement longue car il n'existe aucun mécanisme automatique permettant d'effectuer cette

1. Un système au sein duquel le client et le serveur partagent une clé commune qui est utilisée pour crypter ou décrypter les communications réseau

tâche. Pour obtenir de plus amples informations sur le sujet, consultez la question numéro 2.23 du FAQ de Kerberos disponible à l'adresse suivante :

http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html

- Kerberos n'est que partiellement compatible avec le système d'authentification PAM (de l'anglais Pluggable Authentication Modules) utilisé par la plupart des serveurs exécutant Red Hat Enterprise Linux. Pour obtenir de plus amples informations sur le sujet, reportez-vous à la Section 19.4.
- Kerberos suppose certes que tout utilisateur soit digne de confiance mais utilise un hôte non-sécurisé sur un réseau non-sécurisé. Son but primaire est d'empêcher que des mots de passe en texte clair ne soient envoyés à travers ce réseau. Toutefois, si quelqu'un d'autre que l'utilisateur lui-même a physiquement accès à l'hôte qui émet les tickets utilisés pour l'authentification — appelé *centre de distribution de clés* (ou *KDC* de l'anglais Key Distribution Center) — l'ensemble du système d'authentification Kerberos est menacé d'être compromis.
- Pour qu'une application utilise Kerberos, ses sources doivent être modifiées afin d'effectuer les appels appropriés dans les bibliothèques Kerberos. Les applications modifiées de la sorte sont considérées comme étant *kerberisées*. Pour certaines applications, ceci peut poser de nombreux problèmes en raison de la taille et de la conception de l'application. Pour d'autres applications qui ne sont pas compatibles, des modifications doivent être apportées à la manière selon laquelle les serveurs et les clients communiquent entre eux. Là encore, il se peut que des modifications importantes soient nécessaires au niveau de la programmation. Les applications dont les sources ne sont pas accessibles et dont la prise en charge de Kerberos n'est pas disponible par défaut sont celles posant généralement le plus de problèmes.
- Avec une solution Kerberos, c'est tout ou rien. Une fois que Kerberos est utilisé sur le réseau, tout mot de passe non-crypté transmis à un service non-kerberisé risque d'être intercepté. Dans de telles circonstances, le système ne tirera aucun avantage de l'utilisation de Korberos. Afin de sécuriser votre réseau avec Kerberos, vous devez soit utiliser des versions kerberisées de *toutes* les applications client/serveur qui envoient des mots de passe en texte clair, soit n'utiliser absolument *aucune* application client/serveur.

19.2. Terminologie spécifique à Kerberos

Kerberos dispose de sa propre terminologie pour définir différents aspects du service. Avant d'évoquer la manière slon laquelle Kerberos fonctionne, il convient de se familiariser avec les termes suivants :

serveur d'authentification (ou AS, Authentication Server)

Un serveur émettant des tickets pour un service souhaité ces derniers sont à leur tour transmis aux utilisateurs pour l'accès au service. Le serveur d'authentification (ou AS de l'anglais Authentification Serveur) répond aux requêtes des clients qui ne disposent pas de certificats d'identité ou ne les ont pas envoyés avec leur demande. Il est généralement utilisé pour obtenir l'accès au service du Serveur d'Émission de Tickets (ou TGS de l'anglais Ticket-granting Server) qui est octroyé en créant un Ticket d'émission de Tickets (ou TGT de l'anglais Ticket-granting Ticket). L'AS tourne généralement sur le même hôte que le Centre de Distribution de Clés (ou KDC de l'anglais Key Distribution Center).

ciphertext

Des données cryptées.

client

Une entité sur le réseau (un utilisateur, un hôte ou une application) pouvant recevoir un ticket de Kerberos.

certificats d'identité

Un ensemble temporaire de certificats d'identité électroniques qui vérifient l'identité d'un client pour un service particulier. Cet ensemble de certificats d'identité est aussi appelé un ticket ou credentials selon le mot anglais.

cache de certificats d'identités ou fichier de tickets

Un fichier contenant les clés nécessaires au cryptage des communications entre un utilisateur et divers services réseau. Kerberos 5 fournit un cadre permettant d'utiliser d'autres types de caches tels qu'une mémoire partagée, mais les fichiers sont mieux pris en charge de cette façon.

hache crypté (ou crypt hash)

Un hache unidirectionnel utilisé pour l'authentification des utilisateurs. Bien qu'étant plus sûr que le texte clair, un pirate expérimenté peut assez facilement le décoder.

GSS-API

L'API d'authentification Generic Security Service Application Program Interface (définie dans le document RFC-2743 publié par The Internet Engineering Task Force) représente un ensemble de fonctions qui fournissent des services de sécurité. L'API est utilisée par les clients et les services pour leur authentification réciproque sans qu'aucun des deux programmes ne reconnaissent vraiment le mécanisme sous-jacent. Si un service réseau (comme le serveur cyrus-IMAP) utilise GSS-API, il peut se servir de Kerberos pour ses besoins d'authentification.

hache (ou hash)

Un nombre créé à partir de texte et utilisé pour garantir que des données transmises n'ont pas été manipulées de manière malveillante.

clé

Un 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.

centre de distribution de clés (ou KDC, Key Distribution Center)

Un service émettant des tickets Kerberos, généralement exécuté sur le même hôte que le serveur d'émission de tickets ou TGS (de l'anglais Ticket-granting Server).

keytab (ou table clé)

Un 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`. Le serveur d'administration de KDC, `/usr/kerberos/sbin/kadmind`, est le seul service utilisant tout autre fichier (il utilise `/var/kerberos/krb5kdc/kadm5.keytab`).

`kinit`

La commande `kinit` permet à un principal déjà connecté d'obtenir et de mettre en cache le ticket d'émission de tickets initial (ou TGT de l'anglais Ticket-granting Ticket). Pour obtenir de plus amples informations sur l'utilisation de la commande `kinit`, consultez sa page de manuel.

principal (ou nom principal)

Le principal est le nom unique d'un utilisateur ou d'un service autorisé à s'authentifier à l'aide de Kerberos. Un nom principal a le format suivant : `root[/instance]@REALM`. Pour un utilisateur ordinaire, l'élément root correspond à l'ID de connexion. L'`instance` est facultative. Si le principal a une instance, elle est séparée de l'élément root par une barre oblique en avant ("/").

Une chaîne vide ("") est considérée comme une instance valide (qui est différente de l'instance `NULL` par défaut), mais son utilisation peut être source de confusion. Tous les noms principaux d'une zone (aussi appelée realm selon le mot anglais) ont leur propre clé qui est dérivée de leur mot de passe ou est définie de façon aléatoire pour les services.

zone (ou realm)

Un réseau utilisant Kerberos, composé d'un ou plusieurs serveurs appelés KDC et d'un nombre clients potentiellement élevé.

service

Programme accessible sur le réseau.

ticket

Un ensemble temporaire de certificats d'identité électroniques qui vérifient l'identité d'un client pour un service particulier. Ce ticket est aussi appelé certificats d'identité ou credentials.

service d'émission de tickets (ou TGS, Ticket -granting Service)

Serveur émettant les tickets pour un service souhaité. L'utilisateur doit ensuite employer ces derniers pour accéder au service en question. Le TGS fonctionne en général sur le même hôte que le KDC.

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

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

mot de passe non-crypté

Un mot de passe en texte clair, lisible par tout un chacun.

19.3. Fonctionnement de Kerberos

Kerberos est différent des autres méthodes d'authentification basées sur la combinaison nom d'utilisateur/mot de passe car, au lieu d'authentifier chaque utilisateur auprès de chaque service réseau, il utilise un cryptage symétrique et un tiers digne de confiance connu sous le nom de Centre de distribution de tickets (ou KDC de l'anglais Key Distribution Center) afin d'authentifier les utilisateurs auprès d'un ensemble de services réseau. Une fois l'authentification auprès du KDC effectuée, il renvoie à l'ordinateur de l'utilisateur un ticket spécifique à cette session de sorte que tout service kerberisé puisse rechercher le ticket sur l'ordinateur de l'utilisateur plutôt que de demander à l'utilisateur de s'authentifier à l'aide d'un mot de passe.

Lorsqu'un utilisateur faisant partie d'un réseau kerberisé se connecte sur son poste de travail, son principal est envoyé au KDC dans une demande de ticket d'émission de ticket ou TGT (de l'anglais Ticket-granting Ticket) de la part du serveur d'authentification (ou AS de l'anglais Authentication Server). Cette demande peut être envoyée par le programme de connexion afin qu'elle soit transparente pour l'utilisateur ou elle peut être soumise par le programme `kinit` une fois l'utilisateur connecté.

Le KDC vérifie la présence du principal dans sa base de données. Si le principal y figure, 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 le progamme `kinit` présent sur l'ordinateur client décrypte ensuite le TGT à l'aide de la clé de l'utilisateur (qu'il obtient à partir du mot de passe). La clé de l'utilisateur est utilisée seulement sur l'ordinateur client et *n'est pas* envoyée sur le réseau.

Le TGT, qui est paramétré de sorte qu'il expire après un certain laps de temps (généralement dix heures), est stocké dans le cache de certificats d'identité de l'ordinateur client. Un délai d'expiration est défini de manière à ce qu'un TGT compromis puisse être utilisé par un pirate seulement pendant

une courte durée. Une fois que le TGT est émis, l'utilisateur n'a pas à redonner son mot de passe au KDC tant que le TGT n'a pas expiré ou tant qu'il ne se déconnecte pas et se connecte à nouveau plus tard.

Chaque fois que l'utilisateur doit accéder à un service réseau, le logiciel client utilise le TGT pour demander au serveur d'émission de tickets (TGS) de fournir un nouveau ticket pour ce service spécifique. Le ticket du service est alors émis et utilisé pour authentifier l'utilisateur auprès de ce service de façon transparente.

Avertissement

Le système Kerberos peut être compromis chaque fois qu'un utilisateur présent sur le réseau s'authentifie auprès d'un service non-kerberisé en envoyant un mot de passe en texte en clair. Telle est la raison pour laquelle l'utilisation d'un service non-kerberisé est fortement déconseillée. Parmi de ces services figurent Telnet et FTP. L'utilisation d'autres protocoles cryptés tels que les services sécurisés OpenSSH ou SSL est certes acceptable, mais n'est pas idéale.

Ces informations n'offrent qu'un aperçu général du fonctionnement typique de l'authentification avec Kerberos sur un réseau. Pour obtenir de plus amples informations sur ce sujet, reportez-vous à la Section 19.7.

Remarque

Le bon fonctionnement de Kerberos dépend de certains services réseau. Il a tout d'abord besoin d'une synchronisation approximative de l'horloge entre les différents ordinateurs du réseau. Par conséquent, un programme de synchronisation de l'horloge devrait être installé pour le réseau, comme par exemple, `ntpd`. Pour obtenir de plus amples informations sur la configuration de `ntpd`, consultez `/usr/share/doc/ntp-`<*`version-number`*>`/index.htm` et examinez les renseignements concernant la configuration des serveurs Network Time Protocol (remplacez <*`version-number`*> par le numéro de la version du paquetage `ntp` installée sur le système).

En outre, étant donné que certains aspects de Kerberos dépendent du service de noms de domaines (ou DNS, de l'anglais Domain Name Service), assurez-vous que les entrées DNS et les hôtes sur le réseau sont tous correctement configurés. Pour obtenir de plus amples informations, reportez-vous au guide de l'administrateur système Kerberos V5 (*Kerberos V5 System Administrator's Guide*) disponible en anglais aux formats PostScript et HTML dans `/usr/share/doc/krb5-server-`<*`version-number`*> (remplacez <*`version-number`*> par le numéro de la version du paquetage `krb5-server` installée sur le système).

19.4. Kerberos et PAM

Actuellement, les services kerberisés n'utilisent pas les modules d'authentification enfichagbles (ou PAM de l'anglais Pluggable Authentication Modules) — les serveurs kerberisés contournent complètement les PAM. Toutefois, les applications utilisant des PAM peuvent se servir de Kerberos pour l'authentification si le module `pam_krb5` (contenu dans le paquetage `pam_krb5`) est installé. Le paquetage `pam_krb5` contient des exemples de fichiers de configuration permettant à des services tels que `login` et `gdm` d'authentifier des utilisateurs et d'obtenir des certificats d'identité initiaux à l'aide de leur mot de passe. Pour autant que l'accès aux serveurs de réseau s'effectue toujours à l'aide de services kerberisés ou de services utilisant GSS-API, tels que IMAP, le réseau peut être considéré comme raisonnablement sécurisé.

Astuce

Les administrateurs s'assureront de ne pas permettre l'authentification des utilisateurs auprès de la plupart des réseaux au moyen de leurs mots de passe Kerberos. En effet, de nombreux protocoles utilisés par ces services ne cryptent pas le mot de passe avant de l'envoyer sur le réseau, annulant ainsi tous les avantages d'un système Korberos. Les utilisateurs ne devraient par exemple pas être autorisés à s'authentifier au moyen de leur mot de passe Kerberos sur un réseau Telnet.

19.5. Configuration d'un serveur Kerberos 5

Lors de la configuration de Kerberos, installez tout d'abord le serveur. S'il est nécessaire de configurer des serveurs esclaves, les informations détaillées relatives à la configuration de relations entre les serveurs maîtres et esclaves sont présentées fournies dans le guide d'installation de Kerberos V5 (*Kerberos 5 Installation Guide*) qui se trouve dans le répertoire `/usr/share/doc/krb5-server-<numéro-version>` (remplacez `<version-number>` par le numéro de la version du paquetage `krb5-server` installée sur votre système).

Pour installer un serveur Kerberos, suivez les étapes suivantes :

1. Avant d'installer Kerberos 5, assurez-vous que la synchronisation de l'horloge et que le DNS fonctionnent sur tous les ordinateurs clients et serveurs. Prêtez une attention toute particulière à la synchronisation du temps entre le serveur Kerberos et ses différents clients. Si le horloge du serveur et celle des client diffèrent de plus de cinq minutes (cette durée par défaut est configurable dans Kerberos 5), les clients Kerberos ne pourront pas s'authentifier auprès du serveur. Cette synchronisation de l'horloge est nécessaire pour empêcher un agresseur d'utiliser un ancien ticket afin de se faire passer pour un utilisateur valide.

   Il est recommandé de configurer un réseau client/serveur compatible avec NTP (Network Time Protocol) même si vous n'utilisez pas Kerberos. Red Hat Enterprise Linux inclut le paquetage `ntp` pour cette raison. Consultez `/usr/share/doc/ntp-<version-number>/index.htm` pour obtenir des informations détaillées sur la configuration des serveurs Network Time Protocol et rendez-vous à l'adresse suivante : http://www.eecis.udel.edu/~ntp pour obtenir des informations supplémentaires sur NTP.

2. Installez les paquetages `krb5-libs`, `krb5-server` et `krb5-workstation` sur la machine choisie pour l'exécution du KDC. Cette machine doit bénéficier d'une sécurité très élevée — dans la mesure du possible, elle ne devrait exécuter aucun service autre que le KDC.

   Si une interface utilisateur graphique (ou GUI) est nécessaire pour l'administration de Kerberos, installez le paquetage `gnome-kerberos`. Celui-ci contient `krb5`, un outil graphique permettant la gestion des tickets.

3. Éditez les fichiers de configuration `/etc/krb5.conf` et `/var/kerberos/krb5kdc/kdc.conf` afin qu'ils correspondent aux mappages nom de zone et domaine-à-zone. Une simple zone (aussi appelée realm) peut être construite en remplaçant des instances de *`EXAMPLE.COM`* et *`example.com`* par le nom de domaine correct — en vous assurant de bien respecter le format approprié des noms contenant des lettres majuscules et de ceux avec des minuscules — et en remplaçant le KDC *`kerberos.example.com`* par le nom de votre serveur Kerberos. Par convention, tous les noms de realm sont en lettres majuscules et tous les noms d'hôtes et de domaines DNS sont en lettres minuscules. Pour obtenir des informations plus détaillées sur les différents formats de ces fichiers, consultez leurs pages de manuel respectives.

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

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

La commande `create` crée la base de données qui stockera les clés pour votre realm Kerberos. L'option `-s` permet la création forcée d'un fichier *stash* dans lequel la clé du serveur maître est conservée. En l'absence d'un fichier stash à partir duquel la clé peut être lue, le serveur Korberos (`krb5kdc`) enverra une invite pour que l'utilisateur saisisse le mot de passe du serveur maître (qui permet de recréer la clé) chaque fois qu'il est lancé.

5. Éditez le fichier `/var/kerberos/krb5kdc/kadm5.acl`. Ce fichier est utilisé par `kadmind` d'une part afin de déterminer les éléments principaux devant avoir un accès administratif à la base de données de Kerberos et d'autre part, afin de définir leur niveau d'accès. Une seule ligne suffit à la plupart des sociétés, comme dans l'exemple ci-dessous :
```
*/admin@EXAMPLE.COM  *
```
La plupart des utilisateurs seront représentés dans la base de données par un seul principal (avec une instance *NULL* ou vide, tel que *joe@EXEMPLE.COM*). Avec cette configuration, les utilisateurs ayant un second principal avec une instance *admin* (par exemple, *joe/admin@EXEMPLE.COM*) peuvent exercer un pouvoir total sur la base de données Kerberos du realm.

Une fois que `kadmind` est lancé sur le serveur, tout utilisateur peut accéder à ses services en exécutant `kadmin` sur un client ou serveur quelconque du realm. Toutefois, seuls les utilisateurs spécifiés dans le fichier `kadm5.acl` peuvent modifier le contenu de la base de données, à l'exception du changement de leur propre mot de passe.

Remarque

L'utilitaire `kadmin` communique avec le serveur `kadmind` sur le réseau et utilise Kerberos pour effectuer l'authentification. Pour cette raison, il est nécessaire que le premier principal existe avant d'effectuer une connexion au serveur sur le réseau afin de l'administrer. Pour créer le premier principal, utilisez `kadmin.local`, une commande conçue spécifiquement pour être utilisée sur le même hôte que le KDC et qui ne nécessite pas Kerberos pour l'authentification.

Tapez la commande `kadmin.local` suivante sur terminal KDC afin de créer le premier élément principal :
```
/usr/kerberos/sbin/kadmin.local -q "addprinc username/admin"
```

6. Lancez 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 à l'aide de la commande `addprinc` avec `kadmin`. Les commandes `kadmin` et `kadmin.local` sont des interfaces de ligne de commande vers le KDC. En tant que telles, de nombreuses commandes sont disponibles après le lancement du programme `kadmin`. Reportez-vous à la page de manuel de `kadmin` pour obtenir de plus amples informations.

8. Vérifiez que le KDC émet bien des tickets. Tout d'abord, exécutez `kinit` pour obtenir un ticket et stockez-le dans un fichier de cache de certificats d'identité. Utilisez ensuite `klist` pour afficher la liste des certificats d'identité présents dans votre cache et utilisez `kdestroy` pour détruire le cache et les certificats qu'il contient.

Remarque

Par défaut, `kinit` tente une authentification en utilisant le même nom d'utilisateur que celui servant à la connexion au système (pas le serveur Kerberos). Si ce nom d'utilisateur ne correspond pas à un principal de la base de données Korberos, `kinit` émet un message d'erreur. Dans ce cas, donnez à `kinit` le nom du bon principal en l'insérant comme argument sur la ligne de commande (`kinit <principal>`).

Une fois les étapes ci-dessus accomplies, le serveur Kerberos devrait être opérationnel.

19.6. Configuration d'un client Kerberos 5

Il est moins complexe de configurer un client Kerberos 5 qu'un serveur. Vous devez au minimum installer les paquetages clients et fournir à vos clients un fichier de configuration `krb5.conf` valide. Les versions kerberisées de `rsh` et `rlogin` devront également être modifiées au niveau de la configuration.

1. Assurez-vous que la synchronisation de temps existe bien entre le client Kerberos et le KDC. Reportez-vous à la Section 19.5 pour obtenir de plus amples informations. En outre, vérifiez que le DNS fonctionne correctement sur le client Kerberos avant d'installer les programmes clients de Kerberos.
2. Installez les paquetages `krb5-libs` et `krb5-workstation` sur tous les ordinateurs clients. Vous devez fournir un fichier `/etc/krb5.conf` valide pour chaque client (il est généralement possible d'utiliser le même fichier `krb5.conf` que celui employé par le KDC).
3. Avant qu'un poste de travail appartenant au realm puisse permettre aux utilisateurs de se connecter à l'aide des commandes kerberisées `rsh` et `rlogin`, le paquetage `xinetd` doit être installé sur le poste de travail en question et le principal de l'hôte propre du poste doit également être présent dans la base de données Kerberos. Les programmes des serveurs `kshd` et `klogind` doivent également avoir accès aux clés du principal de leur service.

   À l'aide de `kadmin`, ajoutez un principal d'hôte pour le poste de travail sur le KDC. L'instance sera dans ce cas le nom d'hôte du poste de travail. Utilisez l'option `-randkey` de la commande `addprinc` de `kadmin` pour créer le principal et lui attribuer une clé aléatoire :

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

   Maintenant que vous avez créé le principal, vous pouvez extraire les clés du poste de travail en exécutant `kadmin` *sur le poste de travail lui-même* et en utilisant la commande `ktadd` dans `kadmin` :

   ```
   ktadd -k /etc/krb5.keytab host/blah.example.com
   ```
4. Pour pouvoir utiliser d'autres services réseau kerberisés, ils doivent d'abord être démarrés. Ci-dessous figure une liste des services kerberisés les plus courants ainsi que les instructions relatives à leur activation :
   - `rsh` et `rlogin` — Afin d'utiliser les versions kerberisées de `rsh` et `rlogin`, vous devez activer `klogin`, `eklogin` et `kshell`.
   - Telnet — Afin d'utiliser le service kerberisé Telnet, `krb5-telnet` doit être activé.
   - FTP — Afin de fournir un accès FTP, créez puis extrayez une clé pour un élément principal avec un root définit comme `ftp`. Pour cette opération, assurez-vous que l'instance est bien configurée sur le nom d'hôte pleinement qualifié du serveur FTP et activez ensuite `gssftp`.
   - IMAP — Afin d'utiliser un serveur IMAP kerberisé, le paquetage `cyrus-imap` utilise Kerberos 5 si le paquetage `cyrus-sasl-gssapi` est également installé. Le paquetage `cyrus-sasl-gssapi` contient les plugins Cyrus SASL qui prennent en charge l'authentification GSS-API. Cyrus IMAP devrait fonctionner correctement avec Kerberos tant que l'utilisateur `cyrus` est en mesure de trouver la bonne clé dans `/etc/krb5.keytab` et tant que l'élément root pour le principal est paramétré sur `imap` (créé avec `kadmin`).

     Le paquetage `dovecot` contient également une alternative à `cyrus-imap` qui est basée sur leserveur IMAP, également inclus dans Red Hat Enterprise Linux mais qui à l'heure actuelle ne prend pas en charge GSS-API et Kerberos.

- CVS — Afin d'utiliser un serveur CVS kerberisé, `gserver` recourt à un principal avec un root ayant la valeur `cvs` qui, autrement, est identique au serveur CVS `pserver`.

Reportez-vous au chapitre intitulé *Contrôle de l'accès aux services* du *Guide d'administration système de Red Hat Enterprise Linux* pour obtenir de plus amples informations sur l'activation des services.

19.7. Ressources supplémentaires

Pour obtenir davantage d'informations sur Kerberos, reportez-vous aux sources d'informations mentionnées ci-dessous.

19.7.1. Documentation installée

- `/usr/share/doc/krb5-server-<`*`numéro-de-version`*`>` — Le guide d'installation Kerberos V5 (*Kerberos V5 Installation Guide*) et le guide de l'administrateur système Kerberos V5 (*Kerberos V5 System Administrator's Guide* disponibles en anglais aux formats PostScript et HTML. Le paquetage `krb5-server` doit être installé.
- `/usr/share/doc/krb5-workstation-<`*`numéro de version`*`>` — Le guide de l'utilisateur Kerberos V5 UNIX (*Kerberos V5 UNIX User's Guide* disponible an anglais aux formats PostScript et HTML. Le paquetage `krb5-workstation` doit être installé.
- Pages de manuels de Kerberos — Il existe un certain nombre de pages de manuel relatives à la variété des applications et fichiers de configuration jouant un rôle dans l'implémentation de Kerberos. Ci-dessous figure une liste des pages de manuel les plus importantes.

  Applications client

  - `man kerberos` — Offre une présentation du système Kerberos qui d'une part décrit la manière slon laquelle les certificats d'identité fonctionnent et d'autre part, fournit des recommandations quant à l'obtention et la suppression de tickets Kerberos. Le bas de la page de manuel référence un certain nombre de pages de manuel connexes.
  - `man kinit` — Décrit comment utiliser cette commande afin d'obtenir et de mettre en cache un ticket d'émission de tickets (ou TGT de l'anglais Ticket-granting Ticket).
  - `man kdestroy` — Décrit comment utiliser cette commande afin de supprimer des certificats d'identité Kerberos.
  - `man klist` — Décrit comment utiliser cette commande afin d'afficher une liste des certificats d'identité Kerberos mis en cache.

  Applications administratives

  - `man kadmin` — Décrit comment utiliser cette commande pour administrer la base de données Kerberos V5.
  - `man kdb5_util` — Décrit comment utiliser cette commande afin de créer et effectuer des fonctions administratives de bas niveau dans la base de données Kerberos V5.

Applications serveur

- `man krb5kdc` — Décrit des options de ligne de commande disponibles pour le KDC Kerberos V5.
- `man kadmind` — Décrit des options de ligne de commande disponibles pour le serveur d'administration Kerberos V5.

Fichiers de configuration

- `man krb5.conf` — Décrit le format et les options disponibles au sein du fichier de configuration de la bibliothèque Kerberos V5.
- `man kdc.conf` — Décrit le format et les options disponibles au sein du fichier de configuration de la bibliothèque Kerberos V5 AS et du centre de distribution des clés (ou KDC de l'anglais Key Distribution Center).

19.7.2. Sites Web utiles

- http://web.mit.edu/kerberos/www/ — La page *Kerberos: The Network Authentication Protocol* (Kerberos : le protocole d'authentification réseau) 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 — La version PostScript de *Kerberos : An Authentication Service for Open Network Systems* (Kerberos : un service d'authentification pour des systèmes de réseau ouvert) de Jennifer G. Steiner, Clifford Neuman et Jeffrey I. Schiller. Il s'agit du document original rédigé en anglais décrivant Kerberos.
- http://web.mit.edu/kerberos/www/dialogue.html — Le document *Designing an Authentication System : a Dialogue in Four Scenes* (Conception d'un système d'authentification : un dialogue en quatre parties) écrit en anglais 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 en font un bon point de départ pour les néophytes.
- http://www.ornl.gov/~jar/HowToKerb.html — Le document *How to Kerberize your site* (Comment "kerberiser" votre site) rédigé en anglais est une excellente référence pour la "kerberisation" d'un réseau.
- http://www.networkcomputing.com/netdesign/kerb1.html — Le document *Kerberos Network Design Manual* (Manuel pour la conception d'un réseau Kerberos) rédigé en anglais, offre un aperçu complet du système Kerberos.

Chapitre 20.

Protocole SSH

SSH™ (ou *S*ecure *SH*ell) est un protocole qui facilite les connexions sécurisées entre deux systèmes à l'aide d'une architecture client/serveur et permet aux utilisateurs de se connecter à distance à des systèmes hôte de serveurs.Toutefois, contrairement à d'autres protocoles de communication à distance, tels que FTP ou Telnet, SSH crypte la session de connexion et empêche ainsi tout agresseur de recueillir des mots de passe non-cryptés.

SSH est conçu pour remplacer les applications de terminal plus anciennes et moins sécurisées qui sont utilisées pour se connecter à des hôtes distants, comme **telnet** ou **rsh**. Un programme similaire appelé **scp** remplace des programmes moins récents conçus pour copier des fichiers entre des hôtes, tels que **rcp**. Étant donné que ces applications plus anciennes ne cryptent pas les mots de passe entre le client et le serveur, il est recommandé d'éviter autant que possible de les utiliser. En effet, l'utilisation de méthodes sécurisées pour se connecter à des systèmes distants, réduit les risques aussi bien pour le système client que pour l'hôte distant.

20.1. Fonctionnalités de SSH

SSH offre les précautions suivantes au niveau de la sécurité :

- Après avoir effectué une connexion initiale, le client peut s'assurer que sa connexion est établie avec le même serveur que lors de sa session précédente.
- Le client transmet ses données d'authentification au serveur au moyen d'un cryptage solide 128 bits.
- Toutes les données envoyées et reçues lors d'une session sont transférées au moyen d'un cryptage 128 bits, rendant ainsi le décryptage et la lecture de toute transmission interceptée extrêmement difficile.
- Le client peut retransmettre des applications X11[1] depuis le serveur. Cette technique appelée *retransmission X11*, fournit un moyen d'utiliser en toute sécurité des applications graphiques sur un réseau.

Étant donné que le protocole SSH crypte tout ce qu'il envoie et reçoit, il peut être utilisé pour sécuriser des protocoles autrement vulnérables. Grâce à la technique de *retransmission de port*, un serveur SSH peut être employé pour sécuriser des protocoles non-sécurisés tels que POP, augmentant ainsi la sécurité globale du système et de ses données.

Red Hat Enterprise Linux inclut le paquetage général OpenSSH (`openssh`) ainsi que les paquetages serveur OpenSSH (`openssh-server`) et client OpenSSH (`openssh-clients`). Consultez le chapitre intitulé *OpenSSH* du *Guide d'administration système de Red Hat Enterprise Linux* pour obtenir des instructions sur l'installation et le déploiement d'OpenSSH. Notez également que les paquetages OpenSSH ont besoin du paquetage OpenSSL (`openssl`) qui installe de nombreuses bibliothèques cryptographiques importantes permettant à OpenSSH de fournir des communications cryptées.

20.1.1. Pourquoi utiliser SSH ?

Les utilisateurs d'ordinateurs malintentionnés disposent d'une variété d'outils pour interrompre, intercepter et réacheminer le trafic réseau afin de s'octroyer l'accès à un système. D'une manière générale, ces menaces peuvent être répertoriées de la manière suivante :

1. X11 fait référence au système d'affichage de fenêtres X11R6.7, généralement appelé X Window System ou X. Red Hat Enterprise Linux inclut XFree86, un système X Window System Open Source.

- *Interception d'une communication entre deux systèmes* — Dans ce scénario, le pirate peut se trouver quelque part sur le réseau entre les entités qui communiqueent, pouvant ainsi copier toute information qui est transmise entre elles. Le pirate peut intercepter et garder les informations ou peut les modifier avant de les envoyer au destinataire prévu.

  Cette attaque peut être orchestrée en utilisant un programme renifleur — un utilitaire réseau courant.

- *Usurpation de l'identité d'un hôte* — Grâce à cette technique, le système d'un agresseur est configuré de telle manière qu'il apparaît comme étant le destinataire souhaité d'une transmission. Si cette stratégie fonctionne, le système de l'utilisateur ne détecte pas qu'il communique en fait avec le mauvais hôte.

  Ce type d'attaque peut être organisé grâce à l'utilisation de techniques appelées empoisonnements DNS[2] ou usurpation d'adresse IP[3].

Ces deux techniques permettent d'intercepter des informations potentiellement confidentielles et si cette interception est effectuée pour des raisons hostiles, le résultat peut être catastrophique.

L'utilisation du protocole SSH pour effectuer une connexion au shell à distance ou pour copier des fichiers permet de réduire considérablement ces menaces au niveau de la sécurité. En effet, le client et serveur SSH utilisent des signatures numériques pour vérifier leur identité respectives. En outre, toute communication entre le système client et le système serveur est cryptée. Toute tentative d'usurpation d'identité à une extrémité ou à une autre de la communication est difficilement possible puisque chaque paquet est crypté à l'aide d'une clé connue seulement par le système local et le système distant.

20.2. Versions du protocole 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.

À l'heure actuelle, il existe deux versions différentes du protocole SSH (la version 1 et la version 2). La version 1 de SSH utilise plusieurs algorithmes de cryptage brevetés (toutefois, certains de ces brevets ont expiré) et expose une brèche de sécurité bien connue qui permet à un agresseur d'insérer des données dans le flux de communication. Sous Red Hat Enterprise Linux, la suite OpenSSH utilise la version SSH 2 dotée d'un algorithme d'échange de clés amélioré qui offre une protection contre le type d'agression possible avec la version 1. Ceci étant, la suite OpenSSH prend en charge les connexions effectuées avec la version 1.

Important

Il est conseillé d'utiliser autant que possible, des serveurs et clients compatibles avec la version 2.

20.3. Séquence d'événements d'une connexion SSH

Pour aider à protéger l'intégrité d'une communication SSH entre deux ordinateurs hôte, la série suivante d'événements doit être utilisée.

2. L'empoisonnement DNS a lieu lorsqu'un intrus pénètre dans un serveur DNS, dirigeant les systèmes client vers la copie d'un hôte avec une intention malveillante.
3. L'usurpation d'adresse IP se produit lorsqu'un intrus envoie des paquets réseau qui apparaissent faussement comme provenant d'un hôte de confiance du réseau.

- Une liaison cryptographique est établie afin de permettre au client de vérifier qu'il est bien en communication avec le serveur souhaité.
- La couche de transport de la connexion entre le client et tout hôte distant est cryptée au moyen d'un chiffre symétrique.
- Le client s'authentifie auprès du serveur.
- Le client distant peut interagir avec l'hôte distant au moyen d'une connexion cryptée.

20.3.1. Couche de transport

Le rôle principal de la couche de transport est de faciliter une communication sécurisée entre deux hôtes non seulement au moment de l'authentification, mais également lors de la communication ayant lieu. Pour ce faire, la couche de transport traite le cryptage et décryptage de données et offre une certaine protection quant à l'intégrité des paquets de données lors de leur envoi et de leur réception. De plus, la couche de transport effectue la compression des données permettant d'accélérer la vitesse de transfert des informations.

Lorsqu'un client communique avec un serveur au moyen d'un protocole SSH, de nombreux éléments importants sont échangés afin que les deux systèmes puissent créer correctement la couche de transport. Lors de cet échange, les opérations suivantes ont lieu :

- Des clés sont échangées.
- L'algorithme de cryptage de clés publiques est déterminé.
- L'algorithme de cryptage symétrique est déterminé.
- L'algorithme d'authentification de message est déterminé.
- L'algorithme de hachage est déterminé.

Lors de l'échange des clés, le serveur s'identifie au client au moyen d'une *clé d'hôte* unique. Si le client communique pour la première fois avec ce serveur, la clé du serveur n'est pas connue du client et la connexion ne peut pas être établie. OpenSSH contourne ce problème en acceptant la clé d'hôte du serveur après notification de l'utilisateur et vérifie l'acceptation de la nouvelle clé d'hôte. Lors des connexions suivantes, la clé d'hôte du serveur est vérifiée en la comparant avec une version enregistrée sur le client, permettant ainsi au client de s'assurer qu'il communique bien avec le serveur désiré. Si, à l'avenir, la clé d'hôte ne correspond plus à la version enregistrée sur le client, l'utilisateur doit supprimer cette dernière avant qu'une nouvelle connexion puisse avoir lieu.

Attention

Il est tout à fait possible pour un pirate de se faire passer pour le serveur SSH lors de la première connexion car le système local ne détecte aucune différence entre le serveur désiré et le faux serveur créé par le pirate. Afin d'éviter une telle situation, contrôlez l'intégrité d'un nouveau serveur SSH en contactant l'administrateur du serveur avant d'établir la première connexion ou dans le cas où une clé d'hôte ne correspond pas à celle stockée sur le serveur.

Le protocole SSH est conçu pour fonctionner avec presque tout d'algorithme de clé publique ou tout format de codage. Après que l'échange initial des clés crée une valeur de hachage 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 futures données envoyées via la connexion.

Après la transmission d'une certaine quantité de données au moyen d'une clé et d'un algorithme précis (la quantité exacte dépend de l'implémentation du protocole SSH), un nouvel échange de clés s'effectue ; cette opération engendre la création d'un autre ensemble de valeurs de hachage et d'une

autre valeur secrète partagée. De cette façon, même si un pirate réussit à déterminer les valeurs de hachage et la valeur secrète partagée, ces informations ne lui seront utiles que pour une durée limitée.

20.3.2. Authentification

Une fois que la couche de transport a créé un tunnel sécurisé pour envoyer les informations entre les deux systèmes, le serveur indique au client les différentes méthodes d'authentification prises en charge, telles que l'utilisation d'une signature dotée d'une clé codée ou la saisie d'un mot de passe. Le client doit ensuite essayer de s'authentifier auprès du serveur au moyen d'une des méthodes spécifiées.

Les serveurs et clients SSH pouvent être configurés de façon à permettre différents types d'authentification, donnant à chacune des deux parties un niveau de contrôle optimal. Le serveur peut décider des méthodes de cryptage qu'il prend en charge en fonction de son modèle de sécurité et le client lui peut choisir l'ordre des méthodes d'authentification à utiliser parmi les options disponibles. Grâce à la nature sécurisée de la couche de transport SSH, même les méthodes d'authentification qui au premier abord semblent non-sécurisées (telles que l'authentification basée sur l'hôte et le mot de passe) peuvent être utilisées en toute sécurité.

20.3.3. Canaux

Après avoir effectué avec succès l'authentification au moyen de la couche transport SSH, des *canaux* multiples sont ouverts au moyen d'une technique appelée multiplexage[4]. Chacun de ces canaux peut traiter la communication pour des sessions de terminal différentes et pour des sessions de retransmission X11.

Le client et le serveur peuvent créer un nouveau canal. Chaque canal reçoit ensuite un numéro différent à chaque extrémité de la connexion. Lorsque le client essaie d'ouvrir un nouveau canal, il envoie le numéro du canal accompagné de la requête. Ces informations sont stockées par le serveur et utilisées pour diriger la communication vers ce canal. Cette procédure est utilisée afin que des types différents de session ne créent pas de nuisances mutuelles et de sorte qu'à la fin d'une session donnée, son canal puisse être fermé sans que la connexion SSH primaire ne soit interrompue.

Les canaux prennent aussi en charge le *contrôle du flux de données*, ce qui leur permet d'envoyer et de recevoir des données de façon ordonnée. Ce faisant, aucune donnée n'est envoyée sur le canal tant que l'hôte n'a pas reçu un message lui indiquant que le canal est ouvert.

Le client et le serveur négocient automatiquement la configuration de chaque canal, en fonction du type de service demandé par le client et de la manière selon laquelle l'utilisateur est connecté au réseau. Ainsi, le traitement des différents types de connexions distantes est non seulement extrêmement flexible, mais il ne nécessite même pas d'apporter des modifications à la structure de base du protocole.

20.4. Fichiers de configuration d'OpenSSH

OpenSSH est constitué de deux ensembles de fichiers de configuration, un pour les programmes client (`ssh`, `scp` et `sftp`) et l'autre pour le service (`sshd`).

Les informations de configuration SSH qui s'appliquent à l'ensemble du système sont stockées dans le répertoire `/etc/ssh` où figurent :

- `moduli` — Fichier contenant les groupes Diffie-Hellman utilisés pour l'échange de clés Diffie-Hellman qui est crucial pour la création d'une couche de transport sécurisée. Lorsque les clés sont

4. Une connexion multiplexe se compose de plusieurs signaux envoyés sur un support partagé courant. Avec le protocole SSH, divers canaux sont envoyés sur une connexion courante sécurisée.

échangées au début d'une session SSH, une valeur secrète partagée ne pouvant être déterminée que conjointement par les deux parties est créée. Cette valeur est ensuite utilisée pour effectuer l'authentification de l'hôte.

- `ssh_config` — Fichier de configuration client SSH pour l'ensemble du système. Il est écrasé si un même fichier est présent dans le répertoire personnel de l'utilisateur (`~/.ssh/config`).
- `sshd_config` — Fichier de configuration pour le démon `sshd`.
- `ssh_host_dsa_key` — Clé DSA privée utilisée par le démon `sshd`.
- `ssh_host_dsa_key.pub` — Clé DSA publique utilisée par le démon `sshd`.
- `ssh_host_key` — Clé RSA privée utilisée par le démon `sshd` pour la version 1 du protocole SSH.
- `ssh_host_key.pub` — Clé RSA publique utilisée par le démon `sshd` pour la version 1 du protocole SSH.
- `ssh_host_rsa_key` — Clé RSA privée utilisée par le démon `sshd` pour la version 2 du protocole SSH.
- `ssh_host_rsa_key.pub` — Clé RSA publique utilisée par le démon `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 répertoire `~/.ssh/` où figurent :

- `authorized_keys` — Fichier contenant une liste de clés publiques autorisées pour les serveurs. Lorsque le client se connecte à un serveur, ce dernier authentifie le client en vérifiant sa clé publique signée qui est stockée dans ce fichier.
- `id_dsa` — Fichier contenant la clé DSA privée de l'utilisateur.
- `id_dsa.pub` — Clé DSA publique de l'utilisateur.
- `id_rsa` — Clé RSA privée utilisée par `ssh` pour la version 2 du protocole SSH.
- `id_rsa.pub` — Clé RSA publique utilisée par `ssh` pour la version 2 du protocole SSH.
- `identity` — Clé RSA privée utilisée par `ssh` pour la version 1 du protocole SSH.
- `identity.pub` — Clé RSA privée utilisée par `ssh` pour la version 1 du protocole SSH.
- `known_hosts` — Fichier contenant les clés d'hôtes DSA des serveurs SSH auxquels l'utilisateur a accédé. Ce fichier est très important car il permet de garantir que le client SSH se connecte au bon serveur SSH.

Important

Si la clé d'hôte d'un serveur SSH a changé, le client informe l'utilisateur que le processus de connexion ne peut pas se poursuivre tant que la clé d'hôte du serveur n'a pas été supprimée du fichier `known_hosts` à l'aide d'un éditeur de texte. Avant de procéder à cette opération, il est toutefois conseillé de contacter l'administrateur système du serveur SSH pour vous assurer que le serveur n'est pas compromis.

Consultez les pages de manuel de `ssh_config` et `sshd_config` pour obtenir plus d'informations sur les différentes directives disponibles dans les fichiers de configuration de SSH.

20.5. Beaucoup plus qu'un shell sécurisé

Une interface sécurisée en ligne de commande n'est qu'une utilisation parmi tant d'autres, de SSH. En ayant la quantité nécessaire de bande passante, les sessions X11 peuvent être dirigées sur un canal

SSH. Ou, en utilisant la retransmission TCP/IP, les connexions par port entre les systèmes, considérées auparavant comme étant non-sécurisés, peuvent être mappées à des canaux SSH spécifiques.

20.5.1. Retransmission X11

L'ouverture d'une session X11 par le biais d'une connexion SSH établie est aussi facile que l'exécution d'un programme X sur un ordinateur local. Lorsqu'un programme X est exécuté à partir d'une invite du shell sécurisée, le client et le serveur SSH créent un nouveau canal sécurisé et les données du programme X sont ensuite envoyées à l'ordinateur client via ce canal d'une manière transparente.

La retransmission X11 peut être très utile. Elle peut être utilisée par exemple, pour créer une session interactive sécurisée avec `up2date`. Pour ce faire, connectez-vous au serveur en utilisant **ssh** et en tapant :

```
up2date &
```

Après avoir fourni le mot de passe du super-utilisateur pour le serveur, l'**Agent de mise à jour Red Hat** apparaît et permet à l'utilisateur distant de mettre à jour en toute sécurité son système à distance.

20.5.2. Retransmission de port

Grâce à SSH, il est possible de sécuriser des protocoles TCP/IP non-sécurisés via la retransmission de port. En utilisant cette technique, le serveur SSH devient un conduit crypté vers le client SSH.

La retransmission de port consiste à mapper un port local du client vers un port distant du serveur. SSH permet de mapper un port quelconque du serveur vers un port quelconque du client ; pour que cette technique fonctionne, il n'est pas nécessaire qu'une correspondance existe entre ces numéros de port.

Pour créer un canal de retransmission de port TCP/IP qui écoute les connexions sur l'hôte local, utilisez la commande suivante :

```
ssh -L local-port:remote-hostname:remote-port username@hostname
```

Remarque

Pour configurer la retransmission de port de manière à ce qu'elle écoute sur les ports inférieurs à 1024, il est nécessaire d'avoir un accès de niveau super-utilisateur (ou root).

Pour vérifier le courrier électronique sur un serveur nommé `mail.example.com` en utilisant le protocole POP via une connexion cryptée, utilisez la commande ci-dessous :

```
ssh -L 1100:mail.example.com:110 mail.example.com
```

Une fois que le canal de retransmission de port est en place entre l'ordinateur client et le serveur messagerie, indiquez au client de messagerie POP3 d'utiliser le port 1100 sur l'hôte local afin de vérifier le nouveau courrier. Toutes les requêtes envoyées au port 1100 du système client seront transmises de façon sécurisée au serveur `mail.example.com`.

Si `mail.example.com` n'exécute pas un serveur SSH, mais qu'un autre ordinateur l'exécute, SSH peut toujours être utilisé pour sécuriser une partie de la connexion. Dans ce cas toutefois, une commande légèrement différente est nécessaire :

```
ssh -L 1100:mail.example.com:110 other.example.com
```

Dans cet exemple, des requêtes POP3 en provenance du port 1100 de l'ordinateur client sont retransmises vers le serveur SSH, `other.example.com` par le biais de la connexion SSH sur le port 22 . Ensuite, `other.example.com` se connecte au port 110 sur `mail.example.com` pour vérifier la réception de nouveau courrier. Notez qu'en utilisant cette technique, seule la connexion entre le système client et le serveur SSH `other.example.com` est sécurisée.

La retransmission de port peutégalement être utilisée 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 hôte utilisant des ports bloqués est tout de même possible en redirigeant leur communication sur une connexion SSH établie.

Remarque

L'utilisation de la retransmission de port pour transférer des connexions de cette façon permet à tout utilisateur du système client de se connecter à ce service. Si le système client est compromis, les pirates auront également accès aux services retransmis.

Les administrateurs système préoccupés quant à l'utilisation de la retransmission de port peuvent désactiver cette fonction sur le serveur en spécifiant le paramètre `No` pour la ligne AllowTcpForwarding dans `/etc/ssh/sshd_config` et en redémarrant ensuite le service `sshd`.

20.6. Utilisation nécessaire de SSH pour les connexions à distance

Pour que le protocole SSH soit vraiment efficace, il est essentiel de n'utiliser aucun protocole de connexion non-sécurisé, tel que Telnet et FTP. Sinon, il est possible de protéger le mot de passe d'un utilisateur en utilisant SSH pour une session, mais il pourra être ensuite être intercepté lors d'une connexion ultérieure avec Telnet.

Ci-dessous figurent un certain nombre de services devant être désactivés :

- `telnet`
- `rsh`
- `rlogin`
- `vsftpd`

Pour désactiver des méthodes de connexion au système qui ne sont pas sécurisées, utilisez le programme en ligne de commande nommé `chkconfig`, le programme basé sur ncurses appelé **ntsysv** ou l'application graphique baptisé **Outil de configuration des services** (`redhat-config-services`). Tous ces outils nécessitent un accès de niveau super-utilisateur (ou root).

Pour obtenir de plus amples informations sur les niveaux d'exécution et sur la configuration des services à l'aide de `chkconfig`, de `ntsysv` et de l'**Outil de configuration des services**, reportez-vous au chapitre intitulé *Contrôle de l'accès aux services* du *Guide d'administration système de Red Hat Enterprise Linux*.

20.7. Ressources supplémentaires

Pour obtenir de plus amples informations sur SSH, consultez les ressources mentionnées ci-dessous.

20.7.1. Documentation installée

- Le répertoire `/usr/share/doc/openssh-<version-number>/` — Remplacez `<version-number>` par le numéro de version du paquetage OpenSSH. Ce répertoire contient un README fournissant des informations élémentaires sur le projet OpenSSH et un fichier portant le mon `RFC.nroff` donnant des informations générales sur le protocole SSH.
- Pages de manuel en relation avec SSH — Il existe un certain nombre de pages de manuel pour une variété d'applications et de fichiers de configuration associés à SSH. Ci-dessous figurent certaines des pages de manuel les plus importantes.

  Applications client

  - `man ssh` — Décrit comment utiliser cette commande pour établir une connexion à un serveur SSH.
  - `man scp` — Décrit comment utiliser cette commande pour copier des fichiers depuis et sur un serveur SSH.
  - `man sftp` — Décrit comment utiliser cette commande pour copier de manière interactive, des fichiers depuis et sur un serveur SSH.

  Application serveur

  - `man sshd` — Décrit les options de la ligne de commande disponibles pour le serveur SSH.

  Fichiers de configuration

  - `man ssh_config` — Décrit le format et les options disponibles au sein le fichier de configuration pour les clients SSH.
  - `man sshd_config` — Décrit le format et les options disponibles au sein du fichier de configuration pour le serveur SSH.

20.7.2. Sites Web utiles

- http://www.openssh.com — La page FAQ de OpenSSH, les rapports de bogues, listes de diffusion, buts du projet ainsi que des explications plus techniques des fonctionnalités de sécurité.
- http://www.openssl.org — La page FAQ de OpenSSH, listes de diffusion et une description du but du projet.
- http://www.freessh.org — Le logiciel client SSH pour d'autres plates-formes.

20.7.3. Livre sur le sujet

- *Guide d'administration système de Red Hat Enterprise Linux* ; Red Hat, Inc. — Le chapitre *OpenSSH* explique comment configurer un serveur SSH et comment utiliser le logiciel client SSH qui fait partie de la suite d'outils OpenSSH. Il examine également comment créer une paire de clés RSA (ou DSA) permettant des connexions sans mot de passe.

Chapitre 21.

SELinux

Security-Enhanced Linux (ou *SELinux*) est une architecture de sécurité intégrée dans le noyau 2.6.*x* à l'aide des modules LSM (ou *linux security modules*). Il s'agit d'un projet de l'organisation United States National Security Agency (NSA) et de la communauté SELinux. L'intégration de SELinux dans Red Hat Enterprise Linux est le fruit d'un effort commun entre l'organisation NSA et Red Hat.

21.1. Introduction à SELinux

SELinux fournit un système de contrôle d'accès obligatoire (ou MAC, de l'anglais *mandatory access control*) intégré au noyau Linux. Sous un système standard de contrôle d'accès discrétionnaire Linux (ou DAC, de l'anglais *discretionary access control*), une application ou un processus exécuté en tant qu'utilisateur (UID ou SUID) reçoit la permission de l'utilisateur sur des objets tels que des fichiers, des sockets et d'autres processus. L'exécution d'un noyau MAC SELinux permet de protéger le système contre des applications malveillantes ou défectueuses qui peuvent endommager ou détruire le système. SELinux définit les droits d'accès et de transition de chaque utilisateur, application, processus et fichier du système. SELinux gouverne alors les interactions de ces *sujets* et *objets* à l'aide d'une *politique* de sécurité qui spécifie le degré de rigueur ou de souplesse d'une installation donnée de Red Hat Enterprise Linux.

Dans l'ensemble, SELinux est presque complètement invisible pour les utilisateurs du système. Seuls les administrateurs système doivent se préoccuper de la rigueur d'une politique devant être implémentée dans leur environnement serveur. La politique, qui peut être aussi rigoureuse ou souple que nécessaire, est définie de manière très détaillée. Ce niveau de détails donne au noyau SELinux un contrôle complet et granulaire sur l'ensemble du système.

Lorsqu'un sujet tel qu'une application tente d'accéder à un objet tel qu'un fichier, le serveur d'application des politiques dans le noyau cherche un AVC (ou *access vector cache*), dans lequel les permissions sur des sujets et des objets sont mises en cache. Si une décision ne peut pas être prise en fonction des données présentes dans l'AVC, la requête continue son chemin vers le serveur de sécurité qui recherche le *contexte de sécurité* de l'application et du fichier dans la matrice. La permission est alors accordée ou refusée et un message `avc: denied` apparaît dans `/var/log/messages` de manière détaillée. Les sujets et les objets obtiennent leur contexte de sécurité de la politique installée, qui fournit également les informations peuplant la matrice du serveur de sécurité.

Outre l'exécution en mode d'application (ou *enforcing* mode), SELinux peut tourner dans un mode permissif (ou *permissive* mode), où l'AVC est consulté et les refus sont journalisés, mais SELinux n'applique pas cette politique.

Pour obtenir davantage d'informations sur la manière selon laquelle SELinux fonctionne, consultez la Section 21.3.

21.2. Fichiers en relation avec SELinux

Les sections suivantes examinent les fichiers de configuration de SELinux et les systèmes de fichiers connexes.

21.2.1. Pseudo-système de fichiers `/selinux/`

Le pseudo-système de fichiers `/selinux/` contient des commandes qui sont utilisées le plus couramment par le sous-système du noyau. Ce type de système de fichiers est semblable au pseudo-système de fichiers `/proc/`.

Dans la plupart des cas, les administrateurs et les utilisateurs n'ont pas à manipuler ce composant, contrairement à d'autres fichiers et répertoires de SELinux.

L'extrait ci-dessous reproduit un échantillon du contenu du répertoire `/selinux/` :

```
-rw-rw-rw-  1 root root 0 Sep 22 13:14 access
dr-xr-xr-x  1 root root 0 Sep 22 13:14 booleans
--w-------  1 root root 0 Sep 22 13:14 commit_pending_bools
-rw-rw-rw-  1 root root 0 Sep 22 13:14 context
-rw-rw-rw-  1 root root 0 Sep 22 13:14 create
--w-------  1 root root 0 Sep 22 13:14 disable
-rw-r--r--  1 root root 0 Sep 22 13:14 enforce
-rw-------  1 root root 0 Sep 22 13:14 load
-r--r--r--  1 root root 0 Sep 22 13:14 mls
-r--r--r--  1 root root 0 Sep 22 13:14 policyvers
-rw-rw-rw-  1 root root 0 Sep 22 13:14 relabel
-rw-rw-rw-  1 root root 0 Sep 22 13:14 user
```

Par exemple, l'exécution de la commande `cat` sur le fichier `enforce` renvoie soit un `1` pour le mode d'application, soit un `0` pour le mode permissif.

21.2.2. Fichiers de configuration de SELinux

Les sections suivantes examinent les fichiers de configuration et de politiques de SELinux ainsi que les systèmes de fichiers connexes qui se trouvent dans le répertoire `/etc/`.

21.2.2.1. Fichier de configuration `/etc/sysconfig/selinux`

Il est possible de configurer SELinux Red Hat Enterprise Linux de deux manières : en utilisant l'**Outil de configuration du niveau de sécurité** (`system-config-securitylevel`) ou en éditant manuellement le fichier de configuration (`/etc/sysconfig/selinux`).

Le fichier `/etc/sysconfig/selinux` est le fichier de configuration principal permettant non seulement d'activer ou de désactiver SELinux, mais permettant également de déterminer la politique spécifique qui doit être appliquée sur le système ainsi que la manière selon laquelle elle doit être appliquée.

Remarque

Le fichier `/etc/sysconfig/selinux` contient un lien symbolique vers le fichier de configuration proprement dit, à savoir `/etc/selinux/config`.

La partie ci-dessous examine la totalité du sous-système d'options qui sont disponibles pour la configuration :

- `SELINUX=<enforcing|permissive|disabled>` — Définit l'état de niveau supérieur de SELinux sur un système.
  - `enforcing` — La politique de sécurité de SELinux est appliquée.
  - `permissive` — Le système SELinux émet des messages d'avertissements mais n'applique pas la politique. Cette option est utile pour le débogage ou la résolution de problèmes. En mode

permissif, davantage de refus seront journalisés étant donné que les sujets seront en mesure de poursuivre des actions qui, en mode d'application, seraient par contre refusées. Par exemple, un utilisateur traversant toute une arborescence de répertoires entraîne la création de multiples messages `avc: denied` pour chaque niveau de répertoire lu, une situation qui ne se produirait pas avec un noyau en mode d'application car il aurait empêché dès le départ l'utilisateur de traverser l'arborescence et aurait mis fin à la création d'autres messages de refus.

- `disabled` — SELinux est complètement désactivée. Les crochets de SELinux sont retirés du noyau et le pseudo-système de fichiers est abandonné.

Astuce

Les actions prises alors que SELinux est désactivée peuvent avoir un impact sur le système de fichiers dans le sens où il n'aura peut-être plus le bon contexte de sécurité, tel qu'il est défini par la politique. En exécutant `fixfiles relabel` avant d'activer SELinux le système de fichiers reprendra la bonne étiquette (ou label) afin que SELinux fonctionne correctement lors de son activation. Pour obtenir davantage d'informations, consultez la page de manuel de `fixfiles`(8).

Remarque

Des espaces blancs supplémentaires à la fin d'une ligne de configuration ou des lignes blanches superflues à la fin du fichier peuvent entraîner un comportement imprévu. Par mesure de sécurité, supprimez tout espace blanc qui n'est pas nécessaire.

- `SELINUXTYPE=<targeted|strict>` — Spécifie la politique spécifique qui est actuellement appliquée par SELinux.
  - `targeted` — Seuls les démons réseau ciblés sont protégés.

Important

Les démons suivants sont protégés dans la politique ciblée par défaut : `dhcpd`, `httpd (apache.te)`, `named`, `nscd`, `ntpd`, `portmap`, `snmpd`, `squid` et `syslogd`. Le reste du système est exécuté dans le domaine `unconfined_t`.

Les fichiers de politiques pour ces démons se trouvent dans `/etc/selinux/targeted/src/policy/domains/program` et sont susceptibles de modifications suite à la publication de nouvelles versions de Red Hat Enterprise Linux.

L'application des politiques pour ces démons peut être activée ou désactivée à l'aide de valeurs booléennes contrôlées par l'**Outil de configuration du niveau de sécurité** (`system-config-securitylevel`). La modification d'une valeur booléenne pour un démon ciblé désactive la transition de politique pour le démon, ce qui empêche par exemple `init` de faire transiter `dhcpd` du domaine `unconfined_t` au domaine spécifié dans `dhcpd.te`. Le domaine `unconfined_t` autorise les sujets et objets avec ce contexte de sécurité à être exécutés sous une sécurité Linux standard.

- `strict` — La protection SELinux est totale et ce, pour tous les démons. Les contextes de sécurité sont définis pour tous les sujets et objets et toute action est traitée par le serveur d'application des politiques.

21.2.2.2. Répertoire `/etc/selinux/`

Le répertoire `/etc/selinux/` représente l'emplacement primaire de tous les fichiers de politiques ainsi que celui du principal fichier de configuration.

L'extrait ci-dessous reproduit un échantillon du contenu du répertoire `/etc/selinux/` :

```
-rw-r--r--  1 root root  448 Sep 22 17:34 config
drwxr-xr-x  5 root root 4096 Sep 22 17:27 strict
drwxr-xr-x  5 root root 4096 Sep 22 17:28 targeted
```

Les deux sous-répertoires `strict/` et `targeted/` sont les répertoires spécifiques dans lesquels les fichiers de politiques portant le même nom (c'est à dire strict et targeted) sont stockés.

Pour obtenir davantage d'informations sur la politique de SELinux et sur la configuration des politiques, consultez le Guide de rédaction de politiques SELinux de Red Hat.

21.2.3. Utilitaires de SELinux

La liste suivante contient certains des utilitaires de SELinux les plus couramment utilisés :

- `/usr/bin/setenforce` — Modifie en temps réel le mode que SELinux exécute. En exécutant `setenforce 1`, SELinux est mis en mode d'application (ou enforcing mode). En exécutant `setenforce 0`, SELinux est mis en mode permissif (ou permissive mode). Pour vraiment désactiver SELinux, vous devez soit définir le paramètre dans `/etc/sysconfig/selinux`, soit passer le paramètre `selinux=0` au noyau, soit dans `/etc/grub.conf`, soit au démarrage.
- `/usr/bin/sestatus -v` — Obtient le status détaillé d'un système exécutant SELinux. L'exemple suivant reproduit un extrait de la sortie de `sestatus` :
  ```
  SELinux status:         enabled
  SELinuxfs mount:        /selinux
  Current mode:           enforcing
  Policy version:         18
  ```
- `/usr/bin/newrole` — Exécute un nouveau shell dans un nouveau contexte ou rôle. La politique doit autoriser la transition vers le nouveau rôle.
- `/sbin/restorecon` — Définit le contexte de sécurité d'un ou plusieurs fichiers en marquant les attributs étendus avec le fichier ou le contexte de sécurité approprié.
- `/sbin/fixfiles` — Vérifie ou corrige la base de données du contexte de sécurité sur le système de fichiers.

Pour obtenir davantage d'informations, consultez la page de manuel abordant ces utilitaires.

Pour obtenir davantage d'informations sur l'ensemble des utilitaires binaires disponibles, consultez le contenu des paquetages `setools` ou `policycoreutils` en exécutant `rpm -ql <package-name>` où `<package-name>` correspond au nom du paquetage spécifique.

21.3. Ressources supplémentaires

Les sections suivantes fournissent des ressources permettant d'explorer SELinux de manière plus approfondie.

21.3.1. Documentation installée

- `/usr/share/doc/setools-<version-number>/` — Toute la documentation concernant les utilitaires contenus dans le paquetage `setools`. Parmi celle-ci figurent tous les scripts d'aide, des exemples de fichiers de configuration et de la documentation en général.

21.3.2. Documentation de Red Hat

- *Guide de rédaction de politiques SELinux de Red Hat* ; — Explique comment créer et configurer la politique SELinux.
- *Guide de développement d'applications SELinux de Red Hat* ; — Examine le développement d'applications dans un système SELinux.

21.3.3. Sites Web utiles

- http://www.nsa.gov/selinux/ — Page d'accueil de l'équipe de développement de NSA SELinux. De nombreuses ressources sont disponibles aux formats HTML et PDF. Bien que bon nombre de ces liens ne soient pas spécifiques à Red Hat Enterprise Linux, certains concepts peuvent néanmoins être pertinents.
- http://fedora.redhat.com/docs/ — Page d'accueil du projet de documentation de Fedora contenant des documents spécifiques à Fedora Core qui seront peut-être plus opportuns en raison du cycle de développement plus court.
- http://selinux.sourceforge.net — Page d'accueil de la communauté SELinux.

IV. Annexes

Table des matières

Annexe A.

Paramètres généraux et modules

Cette annexe est fournie pour illustrer *certains* des paramètres possibles pour les *pilotes*[1] de périphériques matériels courants qui, sous Red Hat Enterprise Linux, sont appelés *modules* noyau. Dans la plupart des cas, les paramètres par défaut fonctionneront. Néanmoins, dans certaines situations, des paramètres de module supplémentaires sont nécessaires afin qu'un périphérique puisse fonctionner correctement ou pour annuler les paramètres par défaut du module pour ce périphérique.

Durant l'installation, Red Hat Enterprise Linux utilise un sous-ensemble limité de pilotes de périphériques afin de créer un environnement d'installation stable. Bien que le programme d'installation prenne en charge une installation sur des types de matériel très variés, certains pilotes (y compris ceux pour des adaptateurs SCSI et réseau) ne sont pas inclus dans le noyau d'installation. Ils doivent en fait être chargés par l'utilisateur en tant que modules lors du démarrage. Pour obtenir des informations sur les modules noyau supplémentaires lors du processus d'installation, reportez-vous à la section relative aux autres méthodes de démarrage présentes dans le chapitre intitulé *Étapes pour démarrer* du *Guide d'installation de Red Hat Enterprise Linux*.

Une fois l'installation terminée, la prise en charge de nombreux périphériques est assurée grâce à des modules noyau (ou kernel modules).

Important

De nombreux pilotes de périphériques qui ne sont pas pris en charge sont fournis par Red Hat dans un groupe de paquetages nommés `kernel-unsupported-<kernel-version>`, `kernel-smp-unsupported-<kernel-version>` et `kernel-hugemem-unsupported-<kernel-version>`. Remplacez `<kernel-version>` par la version du noyau installée sur le système. Ces paquetages ne sont pas installés par le programme d'installation de Red Hat Enterprise Linux et les modules fournis ne sont pas pris en charge par Red Hat, Inc..

A.1. Spécification des paramètres d'un module

Dans certaines situations, il peut s'avérer nécessaire de fournir certains paramètres à un module lors de son chargement, afin qu'il puisse fonctionner correctement.

Par exemple, afin de permettre un duplex total à une vitesse de connexion de 100Mbps pour une carte Intel Ether Express/100, chargez le pilote `e100` avec l'option `e100_speed_duplex=4`.

Avertissement

Lorsqu'un paramètre contient une virgule, assurez-vous de *ne pas* mettre d'espace après la virgule.

1. Un pilote est un type de logiciel qui permet à Linux d'utiliser un périphérique matériel donné. Sans pilote, le noyau ne peut pas communiquer avec les périphérique attachés.

Astuce

La commande `modinfo` est également utile pour obtenir une liste de différentes informations relatives au module noyau, telles que la version, les dépendances, les options de paramètres et les alias.

A.2. Paramètres SCSI

Matériel	Module	Paramètres
Contrôleur de mémoire 3ware	`3w-xxxx.o`	
NCR53c810/820/720, NCR53c700/710/700-66	`53c7,8xx.o`	
AACRAID Adaptec	`aacraid.o`	
Adaptec 28xx, R9xx, 39xx 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, AIC-3860	`aic7xxx.o`	
Contrôleur ICP RAID	`gdth.o`	
IBM ServeRAID	`ips.o`	
AMI MegaRAID 418, 428, 438, 466, 762	`megaraid.o`	
Qlogic 1280	`qla1280.o`	

Tableau A-1. Paramètres SCSI

A.3. Paramètres Ethernet

Important

De nos jours, la plupart des cartes d'interface réseau basées sur Ethernet (ou NIC) ne nécessitent pas de paramètres de module pour modifier les paramétrages. Ils peuvent par contre être configurés à l'aide de `ethtool` ou de `mii-tool`. Les paramètres de module ne devraient être ajustés que si ces

outils ne fonctionnent pas. Les paramètres de module peuvent être affichés à l'aide de la commande `modinfo`.

Remarque

Pour obtenir de plus amples informations sur l'utilisation de ces outils, reportez-vous aux pages de manuel de `ethtool`, `mii-tool` et `modinfo`.

Matériel	Module	Paramètres
3Com EtherLink PCI III/XL Vortex (3c590, 3c592, 3c595, 3c597) Boomerang (3c900, 3c905, 3c595)	`3c59x.o`	full_duplex= *0* est actif *1* est inactif
RTL8139, SMC EZ Card Fast Ethernet, cartes RealTek utilisant RTL8129 ou RTL8139 Fast Ethernet chipsets.	`8139too.o`	
Pilote Intel Ether Express/100	`e100.o`	e100_speed_duplex=*X* *If X* = 0 = autodetect speed and duplex 1 = 10Mbps, half duplex 2 = 10Mbps, full duplex 3 = 100Mbps, half duplex 4 = 100Mbps, full duplex
Intel EtherExpress/1000 Gigabit	`e1000.o`	
Pilote Intel i82557/i82558 PCI EtherExpressPro	`eepro100.o`	
NatSemi DP83815 Fast Ethernet	`natsemi.o`	
AMD PCnet32 et AMD PCnetPCI	`pcnet32.o`	
SIS 900/701G PCI Fast Ethernet	`sis900.o`	
ThunderLAN	`tlan.o`	

Matériel	Module	Paramètres
Cartes Ethernet PCI Digital 21x4x Tulip SMC EtherPower 10 PCI(8432T/8432BT) SMC EtherPower 10/100 PCI(9332DST) DEC EtherWorks 100/10 PCI(DE500-XA) DEC EtherWorks 10 PCI(DE450) DEC QSILVER's, Znyx 312 etherarray Allied Telesis LA100PCI-T Danpex EN-9400, Cogent EM110	`tulip.o`	io=*io_port*
Cartes PCI Fast Ethernet VIA Rhine PCI avec soit VIA VT86c100A Rhine-II PCI ou 3043 Rhine-I D-Link DFE-930-TX PCI 10/100	`via-rhine.o`	

Tableau A-2. Paramètres de modules Ethernet

A.3.1. Utilisation de plusieurs cartes Ethernet

Il est possible d'utiliser plusieurs cartes Ethernet sur un seul ordinateur. Pour chaque carte, il doit exister une ligne `alias`, et éventuellement une ligne `options`, pour chaque carte dans le fichier `/etc/modules.conf`. Reportez-vous au chapitre intitulé *Modules noyau* du *Guide d'administration système de Red Hat Enterprise Linux* pour obtenir de plus amples informations sur le sujet.

Pour obtenir davantage d'informations sur l'utilisation de multiples cartes Ethernet, consultez le document intitulé *Linux Ethernet-HOWTO* disponible en ligne et en anglais à l'adresse suivante : http://www.redhat.com/mirrors/LDP/HOWTO/Ethernet-HOWTO.html.

A.3.2. Module de liaison de canaux

Red Hat Enterprise Linux permet aux administrateurs de lier des NIC sur un seul canal en utilisant le module noyau de liaison (`bonding`) et une interface réseau spéciale appelée *interface de liaison de canaux*. La liaison de canaux permet à deux interfaces réseau ou plus, d'agir en tant qu'une seule, augmentant ainsi la largeur de bande et offrant de la redondance.

Afin de lier plusieurs interfaces réseau, l'administrateur doit effectuer les étapes suivantes :

1. Ajoutez la ligne suivante dans `/etc/modules.conf` :
   `alias bond<N> bonding`

   Remplacez <*N*> par le numéro de l'interface, comme `0`. Pour chaque interface de liaison de canaux configurée, une entrée correspondante doit exister dans `/etc/modules.conf`.
2. Configurez une interface de liaison de canaux comme l'explique la Section 8.2.3.
3. Afin d'accroître la performance, ajustez les options de module disponibles pour identifier les combinaisons qui fonctionnent le mieux. Faites particulièrement attention aux commandes `miimon` et `arp_interval` ainsi qu'aux paramètres de `arp_ip_target`. Reportez-vous à la Section A.3.2.1 afin d'obtenir une liste des options disponibles.

4. Après avoir testé le module, ajoutez vos options de modules préférées dans le fichier `/etc/modules.conf`.

A.3.2.1. Directives du module `bonding`

Avant d'en finir avec les paramètres du module `bonding`, il est bon de tester ceux qui fonctionnent le mieux. Pour ce faire, ouvrez une invite du shell en étant connecté en tant que super-utilisateur et saisissez la commande suivante :

```
tail -f /var/log/messages
```

Ouvrez une autre invite de shell et utilisez la commande `/sbin/insmod` pour charger le module `bonding` avec différents paramètres, tout surveillant les messages du noyau pour reprérer toute indication d'erreur.

La commande `/sbin/insmod` est exécutée selon le format suivant :

```
/sbin/insmod bond<N> <parameter=value>
```

Remplacez *<N>* par le numéro de l'interface de liaison. Remplacez *<parameter=value>* par une liste de paramètres pour l'interface dont les éléments sont séparés les uns des autres par un espace.

Une fois convaincu qu'il n'y a pas d'erreurs et après avoir vérifié la performance de l'interface de liaison, ajoutez les paramètres appropriés du module `bonding` dans `/etc/modules.conf`.

La liste ci-dessous répertorie les paramètres disponibles pour le module `bonding` :

- `mode=` — Spécifie l'une des quatre politiques autorisées pour le module `bonding`. Les valeurs acceptables pour ce paramètre sont les suivants :
  - `0` — Définit une politique round-robin pour la tolérance aux pannes et la répartition de charge. Les transmissions sont reçues et envoyées en séquence sur chaque interface esclave liée, en commençant par la première interface disponible.
  - `1` — Définit une politique active-backup pour la tolérance aux pannes. Les transmissions sont reçues et envoyées via la première interface esclave liée qui est disponible. Une autre interface esclave liée est seulement utilisée si l'interface esclave liée qui est active, échoue.
  - `2` — Définit une politique XOR (exclusive-or) pour la tolérance aux pannes et la répartition de charge. En utilisant cette méthode, l'interface établit la correspondance entre l'adresse MAC des requêtes entrantes et l'adresse MAC de l'une des NIC esclaves. Une fois ce lien établi, les transmissions sont envoyées séquentiellement en commençant par la première interface disponible.
  - `3` — Définit une politique de diffusion pour la tolérance aux pannes. Toutes les transmissions sont envoyées sur toutes les interfaces esclaves.
  - `4` — Définit une politique d'agrégats de liens dynamiques IEEE 802.3ad. Crée des groupes d'agrégats qui partagent les mêmes paramétrages de vitesse et de duplex. Transmet et reçoit sur tous les esclaves dans le groupe actif. Requiert un interrupteur conforme à la norme 802.3ad.
  - `5` — Définit une politique TLB (Transmit Load Balancing) pour la tolérance aux pannes et la répartition de charge. Le trafic sortant est distribué selon la charge actuelle sur chaque interface esclave. Le trafic entrant est reçu par l'esclave actuel. Si l'esclave de réception échoue, un autre esclave prend le relais de son adresse MAC.
  - `6` — Définit une politique ALB (Active Load Balancing) pour la tolérance aux pannes et la répartition de charge. Inclut la répartition de charge de transmission et de réception pour le trafic IPV4. La répartition de charge de réception est effectuée par négociation ARP.

- `miimon=` — Spécifie (en millisecondes) la fréquence de contrôle du lien MII. Cette option est utile si une haute disponibilité est requise vu que MII est utilisé pour vérifier que le NIC est bien activé.

Pour vérifier que le pilote de ce NIC particulier supporte l'outil MII, saisissez la commande suivante en étant connecté en tant que super-utilisateur :

```
ethtool <interface-name> | grep "Link detected:"
```

Dans cette commande, remplacez <*interface-name*> par le nom de l'interface du périphérique, tel que `eth0` et non pas par l'interface `bond`. Si MII est pris en charge, la commande renvoie l'extrait suivant :

```
Link detected: yes
```

Si une interface de liaison est utilisée à des fin de haute disponibilité, le module de chaque NIC doit prendre en charge MII.

Le réglage de la valeur sur `0` (la valeur par défaut) désactive cette fonction. Lors de la configuration de ce paramètre, un bon point de départ est la valeur `100`.

- `downdelay=` — Spécifie (en millisecondes) la durée d'attente après l'échec d'un lien, avant que ce dernier ne soit désactivé. La valeur doit être un multiple de la valeur spécifiée dans le paramètre `miimon`. Par défaut, la valeur étant réglée sur `0`, le paramètre est désactivé.
- `updelay=` — Spécifie (en millisecondes) la durée d'attente avant qu'un lien soit activé. La valeur doit être un multiple de la valeur spécifiée dans le paramètre `miimon`.Par défaut, la valeur étant réglée sur `0`, le paramètre est désactivé.
- `arp_interval=` — Spécifie (en millisecondes) la fréquence du contrôle ARP.

  Si ce paramétrage est utilisé tout en étant en mode `mode 0` ou `2` (les deux modes de répartition de charge), le commutateur réseau doit être configuré pour distribuer les paquets uniformément sur toutes les NIC. Afin d'obtenir de plus amples informations sur ce sujet, consultez le document `/usr/share/doc/kernel-doc-`<*kernel-version*>`/Documentation/networking/bonding.txt`.

  Par défaut, la valeur étant réglée sur `0`, ce paramètre est désactivé.
- `arp_ip_target=` — Spécifie l'adresse IP cible des requêtes ARP lorsque le paramètre `arp_interval` est activé. Jusqu'à 16 adresses IP peuvent être spécifiées dans une liste dont les éléments sont séparés les uns des autres par une virgule.
- `primary=` — Spécifie le nom de l'interface, telle que `eth0`, du périphérique primaire. Le périphérique primaire dit `primary` représente la première des interfaces de liaison devant être utilisées et n'est pas abandonnée à moins qu'elle n'échoue. Cette configuration est particulièrement utile lorsqu'un NIC de l'interface de liaison est plus rapide et donc, capable de traiter un charge plus importante.

  Ce paramétrage est seulement valide lorsque l'interface de liaison est en mode active-backup. Consultez le document `/usr/share/doc/kernel-doc-`<*kernel-version*>`/Documentation/networking/bonding.txt` pour obtenir davantage d'informations.
- `multicast=` — Spécifie une valeur entière pour le type de prise en charge de multi-diffusion désiré.

  Les valeurs acceptables pour ce paramètre sont les suivantes :

  - `0` — Désactive la prise en charge de la multi-diffusion.
  - `1` — Active la prise en charge de la multi-diffusion, mais seulement sur l'esclave activé.
  - `2` — Active la prise en charge de la multi-diffusion sur tous les esclaves (valeur par défaut).

Important

Il est essentiel que soit les paramètres de `arp_interval` et `arp_ip_target` soit ceux de `miimon` soient spécifiés. Dans le cas contraire, la performance réseau peut dégénérer lorsqu'un lien ne peut être établi avec succès.

Consultez le document suivant :

`/usr/share/doc/kernel-doc-<`*`kernel-version`*`>/Documentation/networking/bonding.txt`

pour obtenir des instructions détaillées sur la liaison d'interfaces.

Index

Symboles

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Y

Z

Colophon

Les guides sont écrits sous format DocBook SGML v4.1. Les formats HTML et PDF sont produits à l'aide de feuilles de style DSSSL personnalisées et de scripts de wrapper jade personnalisés. Les fichiers DocBook SGML sont écrits avec **Emacs** avec l'aide du mode PSGML.

Garrett LeSage a créé les graphiques d'admonition (remarque, astuce, important, attention et avertissement). Ils peuvent être librement redistribués avec la documentation Red Hat.

L'équipe de documentation de produits Red Hat est composée des personnes suivantes :

Sandra A. Moore — Rédaction/Conception du *Guide d'installation pour les architectures x86, Itanium™, AMD64 et Intel® Extended Memory 64 Technology (Intel® EM64T) Red Hat Enterprise Linux* ; Rédaction/Conception du *Guide d'installation pour les architectures POWER IBM® Red Hat Enterprise Linux* ; Rédaction/Conception du *Guide d'installation pour les architectures S/390® IBM® et zSeries® eServer™ IBM® Red Hat Enterprise Linux*

John Ha — Rédaction/Conception du manuel *Configuration et gestion d'un cluster de Suite de cluster de Red Hat* ; Contribution à la rédaction/conception du *Guide de sécurité de Red Hat Enterprise Linux* ; Conception des feuilles de style et des scripts DocBook personnalisés

Edward C. Bailey — Rédaction/Conception du manuel *Introduction à l'administration système de Red Hat Enterprise Linux* ; Rédaction/Conception des *Notes de mise à jour* ; Contribution à la rédaction du *Guide d'installation pour les architectures x86, Itanium™, AMD64 et Intel® Extended Memory 64 Technology (Intel® EM64T) Red Hat Enterprise Linux*

Karsten Wade — Rédaction/Conception du *Guide de développement d'applications SELinux de Red Hat* ; Rédaction/Conception du *Guide de rédaction de politiques SELinux de Red Hat*

Andrius Benokraitis — Rédaction/Conception du *Guide de référence de Red Hat Enterprise Linux* ; Contribution à la rédaction/conception du *Guide de sécurité de Red Hat Enterprise Linux* ; Contribution à la rédaction du manuel *Guide d'administration système de Red Hat Enterprise Linux*

Paul Kennedy — Rédaction/Conception du *Guide de l'administrateur de GFS de Red Hat* ; Contribution à la rédaction du manuel *Configuration et gestion d'un cluster de Suite de cluster de Red Hat*

Mark Johnson — Rédaction/Conception du *Guide d'administration et de configuration du bureau de Red Hat Enterprise Linux*

Melissa Goldin — Rédaction/Conception du *Guide étape par étape de Red Hat Enterprise Linux*

L'équipe de traduction de Red Hat est composée des personnes suivantes :

Amanpreet Singh Alam — Traductions en punjabi

Jean-Paul Aubry — Traductions françaises

David Barzilay — Traductions portugaises (brésiliennes)

Runa Bhattacharjee — Traductions en bengali

Chester Cheng — Traductions chinoises traditionnelles

Verena Fuehrer — Traductions allemandes

Kiyoto James Hashida — Traductions japonaises

N. Jayaradha — Traductions en tamil

Michelle Jiyeen Kim — Traductions coréennes

Yelitza Louze — Traductions espagnoles

Noriko Mizumoto — Traductions japonaises

Ankitkumar Rameshchandra Patel — Traductions en gujarati

Rajesh Ranjan — Traductions en hindi

Nadine Richter — Traductions allemandes
Audrey Simons — Traductions françaises
Francesco Valente — Traductions italiennes
Sarah Saiying Wang — Traductions chinoises simplifiées
Ben Hung-Pin Wu — Traductions chinoises traditionnelles