Red Hat Linux 7.3

Guide de référence officiel Red Hat Linux

ISBN: N/A

Table des matières

Introduction
- Trouver la documentation appropriée
  - Documentation pour les débutants
  - Pour les utilisateurs expérimentés
  - Documentation pour les utilisateurs chevronnés
- Conventions de documentation
- Utilisation de la souris
- Copier et coller du texte avec X
- Prochainement
  - Vos réactions sont les bienvenues
- Enregistrez-vous pour bénéficier de l'assistance

I. Références liées au système
1. Structure d'un système de fichiers
   - Pourquoi partager une structure commune ?
   - Aperçu du FHS (Filesystem Hierarchy Standard)
   - Emplacement de fichiers Red Hat Linux spéciaux
2. Le système de fichiers `/proc`
   - Un système de fichiers virtuels
   - Les fichiers du niveau supérieur dans `/proc`
   - Répertoires dans `/proc`
   - Utilisation de `sysctl`
   - Autres ressources
3. Processus de démarrage, Init et arrêt
   - Introduction
   - Dans les coulisses du processus de démarrage
   - Information Sysconfig
   - Niveaux d'exécution d'Init

- Exécution de programmes au démarrage
- Arrêt
- Différences du processus de démarrage d'autres architectures

4. GRUB
   - Définition de GRUB
   - Terminologie
   - Interfaces
   - Commandes
   - Fichier de configuration du menu
   - Autres ressources
5. Le système de fichiers ext3
   - Fonctions d'ext3
   - Création d'un système de fichiers ext3
   - Passer à un système de fichiers ext3
   - Revenir à un système de fichiers ext2
6. Utilisateurs et groupes
   - Outils pour l'administration des utilisateurs et des groupes
   - Utilisateurs standard
   - Groupes standard
   - Groupes propres à l'utilisateur
   - Utilitaires masqués
7. Serveurs et clients X
   - La puissance de X
   - Le serveur XFree86
   - Environnements de bureau et gestionnaires de fenêtres
   - Niveaux d'exécution
   - Polices
   - Autres ressources

II. Références liées à la sécurité

8. Modules d'authentification enfichables (PAM)
   - Avantages des PAM
   - Fichiers de configuration PAM
   - Modules PAM
   - Indicateurs de contrôle PAM
   - Chemins d'accès aux modules PAM
   - Arguments PAM
   - Exemples de fichiers de configuration PAM
   - Propriété de PAM et des périphériques

Autres ressources

9. TCP Wrappers et `xinetd`
   - But de TCP Wrappers
   - Listes de contrôle d'accès basé sur l'hôte
   - Contrôle d'accès à l'aide de `xinetd`
   - Autres ressources
10. Protocole SSH
   - Introduction
   - Séquence des événements d'une connexion SSH
   - Couches de sécurité SSH
   - Fichiers de configuration d'OpenSSH
   - Beaucoup plus qu'un shell sécurisé
   - Exiger SSH pour les connexions à distance
11. Kerberos
   - Avantages de Kerberos
   - Désavantages de Kerberos
   - Terminologie Kerberos
   - Fonctionnement de Kerberos
   - Kerberos et PAM (modules d'authentification enfichables)
   - Configurer un serveur Kerberos 5
   - Configurer un client Kerberos 5
   - Autres ressources
12. Installation et configuration de Tripwire
   - Comment utiliserTripwire
   - Instructions d'installation
   - Emplacements des fichiers
   - Composants de Tripwire
   - Modification du fichier de politiques
   - Sélection des phrases d'accès
   - Initialisation de la base de données
   - Exécution d'une vérification d'intégrité
   - Impression des rapports
   - Mise à jour de la base de données après une vérification d'intégrité
   - Mise à jour du fichier de politiques
   - Tripwire et courrier électronique
   - Autres ressources

III. Références liées aux services réseau

13. Scripts réseau

- Fichiers de configuration d'interface
- Scripts de contrôle d'interface
- Fonctions réseau

14. Techniques de mise en oeuvre de pare-feu avec `iptables`
    - Filtrage de paquetages
    - Différences entre `iptables` et `ipchains`
    - Options utilisées avec les commandes `iptables`
    - Stockage de l'information `iptables`
    - Sources d'informations additionnelles
15. Apache
    - Modules par défaut
    - Démarrage et arrêt de `httpd`
    - Directives de configuration dans `httpd.conf`
    - Ajout de modules au serveur
    - Utilisation d'hôtes virtuels
    - Autres ressources
16. Courrier électronique
    - Protocoles
    - Les différents types de programme de messagerie électronique
    - Sendmail
    - Fetchmail
    - Procmail
    - Sécurité
    - Autres ressources
17. Berkeley Internet Name Domain (BIND)
    - Introduction au DNS et à BIND
    - Fichiers de configuration BIND
    - Utiliser `rndc`
    - Propriétés avancées de BIND
    - Erreurs fréquentes à éviter
    - Autres ressources
18. NFS (Network File System)
    - Méthodologie
    - Fichiers de configuration du serveur NFS
    - Fichiers de configuration d'un client NFS
    - Sécuriser NFS
    - Autres ressources
19. Protocole LDAP (Lightweight Directory Access Protocol)

Qu'est-ce que le protocole LDAP ?
Avantages et inconvénients de LDAP
Utilisations du protocole LDAP
Terminologie LDAP
Mises à jour de OpenLDAP 2.0
Fichiers OpenLDAP
Démons et utilitaires OpenLDAP
Modules pour l'ajout de fonctionnalités à LDAP
Configuration de OpenLDAP : présentation rapide
Configuration de votre système pour l'authentification à l'aide de OpenLDAP
Autres ressources
IV. Annexes
A. Paramètres généraux et modules
Spécification des paramètres d'un module
Paramètres des modules pour CD-ROM
Paramètres SCSI
Paramètres Ethernet
Index

Suivant
Introduction

Red Hat Linux 7.3: Guide de référence officiel Red Hat Linux

Red Hat, Inc.

1801 Varsity Drive
Raleigh NC 27606-2072 USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park NC 27709 USA

rhl-rg(FR)-7.3-HTML-RHI (2002-04-05T17:09-0400)

AMD, AMD Athlon, AMD Duron et AMD K6 sont des marques déposées d'Advanced Micro Devices, Inc.

Netscape est une marque déposée de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays.

Windows est une marque déposée de Microsoft Corporation.

SSH et Secure Shell sont des marques déposées de SSH Communications Security, Inc.

FireWire est une marque déposée de Apple Computer Corporation.

Tous les autres copyrights et marques cités sont la propriété de leurs détenteurs respectifs.

L'équipe de documentation de Red Hat Linux est composée par :

Sandra A. Moore, Product Documentation Manager — Principal rédacteur et réviseur du *Guide d'installation officiel Red Hat Linux pour x86* ; Sandra a contribué également à la rédaction du *Guide de démarrage officiel Red Hat Linux*.

Tammy Fox, Product Documentation Technical Lead — Principal rédacteur et réviseur du *Guide de personnalisation officiel Red Hat Linux* ; Tam a contribué également à la rédaction du *Guide de démarrage officiel Red Hat Linux* ainsi que des scripts et des feuilles de modèle DocBook.

Edward C. Bailey, Technical Writer — Edward a contribué à la rédaction du *Guide d'installation officiel Red Hat Linux pour x86*.

Johnray Fuller, Technical Writer — Principal rédacteur et réviseur du *Guide de référence officiel Red Hat Linux*.

John Ha, Technical Writer — John a contribué à la rédaction du *Guide de démarrage officiel Red Hat Linux*.

Sommaire

Introduction

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

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

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

- *Démarrage de Red Hat Linux* — Des informations sur les niveaux d'exécution, les répertoires `rc.d` et le mode de démarrage de vos applications préférées à l'amorçage du système.
- *Le système de fichiers `/proc`* — Ce système de fichiers fournit un aperçu du noyau du système.
- *Le chargeur de démarrage GRUB* — Un regard sur le chargeur de démarrage GRUB et sur la façon dont il démarre votre système.
- *Le système de fichiers ext3* — Apprenez comment ajouter ou retirer le système de fichiers ext3 des périphériques de stockage.
- *Guides de sécurité système et réseau* — Apprenez les méthodes les plus courantes utilisées par les pirates pour corrompre votre système, et les façons de prévenir les problèmes de sécurité.
- *Directives Apache* — Un regard sur la configuration par défaut d'Apache et les options disponibles.

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

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

Note **Note**

Bien que le présent manuel contienne l'information la plus actuelle possible, il est préférable que vous lisiez les Notes de mise à jour Red Hat Linux au cas où des informations seraient devenues obsolètes depuis leur publication. Ces "Notes de mise à jour" se trouvent sur le CD #1 Red Hat Linux et en ligne sur :

```
http://www.redhat.com/docs/manuals/linux
```

Trouver la documentation appropriée

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

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

Débutant

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

Moyennement expérimenté

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

Chevronné

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

Documentation pour les débutants

Pour un nouveau dans le monde 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 impressionante. Ces

informations vous donnent un aperçu du fonctionnement de Linux, indispensable pour approfondir ensuite ces sujets.

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

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

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

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

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

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

Introduction aux sites Web de Linux

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

Introduction aux groupes de discussion Linux

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

- linux.help — Un excellent site où vous obtiendrez de l'aide de la part d'autres utilisateurs Linux.
- linux.redhat — Ce groupe de discussion aborde des thèmes spécifiques à Red Hat Linux.
- linux.redhat.install — Posez vos questions concernant l'installation ou voyez comment d'autres personnes résolvent des problèmes similaires aux vôtres.
- linux.redhat.misc — Pour des questions ou des demandes d'aide particulières.
- linux.redhat.rpm — Une bonne adresse si vous n'arrivez pas à atteindre des objectifs particuliers avec **RPM**.

Livres sur Linux pour les utilisateurs débutants

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

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

Pour les utilisateurs expérimentés

Si vous avez utilisé d'autres distributions Linux, vous connaissez probablement déjà les commandes les plus utilisées. Vous avez peut être installé votre système Linux et téléchargé des logiciels que vous avez

trouvés sur Internet. Une fois Linux installé, les procédures de configuration peuvent toutefois poser problème.

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

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

Documentation pour les utilisateurs chevronnés

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

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

Conventions de documentation

En lisant ce manuel vous verrez que certains mots sont présentés en différents caractères, types, tailles et graisses. Cette présentation est systématique ; différents mots sont représentés dans le même style pour indiquer leur appartenance à une certaine catégorie. Les types de mots représentés de la façon suivante comprennent :

`command`

Les commandes de Linux (et d'autres commandes de systèmes d'exploitation, lorsqu'elles sont utilisées) sont représentées de la façon suivante. Ce style devrait vous indiquer que vous pouvez taper 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, tous seuls, seraient présentés différemment (comme les noms de fichiers). Ils sont alors considérés comme une partie de la commande ; toute la phrase est alors affichée comme une commande. Par exemple :

Utilisez la commande `cat fichier test` pour visualiser le contenu d'un fichier, appelé `fichiertest`, dans le répertoire actuellement en cours d'exécution.

`nom de fichier`

Les noms de fichiers, de répertoires, les chemins d'accès et noms des paquetages RPM sont représentés de la façon suivante. Ce style devrait indiquer qu'un fichier ou un répertoire portant ce nom existe dans votre système Red Hat Linux. Exemples :

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

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

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

application

Ce style vous indique que le programme appelé est une application d'utilisateur final (par opposition au logiciel de système). Par exemple :

Utilisez Netscape **Navigator** pour parcourir le Web.

[touche]

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

Pour utiliser le complètement [Tab], tapez un caractère puis appuyez sur la touche [Tab]. Votre terminal affichera la liste des fichiers du répertoire qui commencent avec cette lettre.

[touche]-[combinaison]

Une combinaison de touches se présente de cette façon. Par exemple :

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

texte d'une interface graphique

Un titre, un mot ou une expression apparaissant sur l'écran d'une interface graphique se présente de la façon suivante. Ce style vous indique qu'il s'agit d'un écran d'une interface graphique ou un élément d'un écran d'interface graphique (par exemple un texte associé à une case à cocher ou un champ). Exemples :

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

haut de menu d'un éran d'interface graphique ou d'une fenêtre

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

Sous **Paramètres** d'un terminal GNOME, vous trouverez les articles suivants : **Préférences**, **R.à Z. terminal**, **Réinitialiser et effacer** et **Sélection de la couleur**.

Si vous devez entrer une séquence de commandes depuis un menu d'interface graphique, ils apparaîtront de la façon suivante :

Pour lancer l'éditeur de texte Emacs, cliquez sur **Programmes**=>**Applications**=>**Emacs**.

bouton d'un écran ou d'une fenêtre d'interface graphique

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

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

`sortie de l'ordinateur`

Un texte de ce style vous indique qu'il est affiché par l'ordinateur à la ligne de commande. Vous verrez les réponses à vos commandes, messages d'erreur et invites interactives de votre saisie dans les scripts ou programmes affichés de cette manière. Par exemple :

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

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

La sortie qui répond à cette commande (dans de cas le contenu du répertoire) est affichée de la façon suivante.

`invite`

L'invite est la façon qu'a l'ordinateur de vous signifier qu'il est prêt à recevoir votre saisie. Elle est représentée de la façon suivante :

```
$

#

[stephen@maturin stephen]$

leopard login:
```

`saisie de l'utilisateur`

Le texte que l'utilisateur doit entrer, que ce soit à la ligne de commande ou dans une boîte de texte d'une interface graphique, est affiché de cette façon. Dans l'exemple suivant, **`text`** est affiché de cette façon:

Pour lancer votre système dans le progamme d'installation basé sur du texte, il vous faudra entrer la commande **`text`** à l'invite `boot:`.

De plus, nous utilisons différentes stratégies pour attirer votre attention sur certaines informations. Suivant l'importance de l'information pour votre système, ces remarques seront présentées sous forme de :

Note **Remarque**

N'oubliez pas que Linux différencie les majuscules et les minuscules. Autrement dit, rose n'est ni ROSE ni rOsE.

Tuyau **Astuce**

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

Important **Important**

Si vous modifiez le fichier de configuration DHCP, les changements ne prendront pas effet tant que vous ne redémarrerez pas le démon DHCP.

Attention **Attention**

N'effectuez pas de tâches standards en tant qu'utilisateur root. Nous vous conseillons d'utiliser toujours un compte utilisateur normal, à moins que vous ne deviez administrer votre système.

Avertissement **Avertissement**

Si vous choisissez de ne pas partitionner manuellement, une installation de classe serveur effacera toutes les partitions existantes sur tous les disques durs installés. N'utilisez cette classe d'installation que si vous êtes certain de ne pas avoir de données à sauvegarder.

Précédent Introduction | Sommaire | Niveau supérieur | Suivant Utilisation de la souris

Utilisation de la souris

Red Hat Linux utilise habituellement une souris à trois boutons. Si vous avez une souris à deux boutons, vous devriez avoir sélectionné l'émulation 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).

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" 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 appuyé. Glissez ensuite l'élément, tout en maintenant la touche appuyée, vers sont nouvel emplacement. Lâchez alors le bouton et posez l'élément.

Copier et coller du texte 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, cliquez avec le bouton central de la souris à l'endroit où vous voulez le placer.

Prochainement

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

Voici comment vous pouvez nous aider !

Vos réactions sont les bienvenues

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

N'oubliez pas de mentionner la référence du manuel :

```
rhl-rg(FR)-7.3-HTML-RHI (2002-04-05T17:09-0400)
```

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

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

Enregistrez-vous pour bénéficier de l'assistance

Si vous avez une édition officielle de Red Hat Linux 7.3, n'oubliez pas de vous inscrire pour bénéficier des avantages auxquels vous avez droit en tant que client Red Hat.

Vous aurez droit aux avantages suivants ou à certains d'entre eux, selon le produit officiel Red Hat Linux que vous avez acheté:

- Official Red Hat support — L'équipe d'assistance de Red Hat, Inc. répondra à vos questions concernant l'intallation.
- Red Hat Network — Mettez facilement à jour vos paquetages et recevez les nouvelles concernant la sécurité adaptées à votre système. Pour de plus amples informations, rendez-vous à l'adresse http://rhn.redhat.com for more details.
- *Under the Brim: The Official Red Hat E-Newsletter* — Recevez chaque mois les nouvelles et informations concernant les produits directement depuis Red Hat.

Pour vous inscrire, rendez-vous à l'adresse http://www.redhat.com/apps/activate/. Vous trouverez votre numéro d'identification de produit sur la carte noire, blanche et rouge de votre emballage officiel Red Hat Linux.

Pour en savoir plus sur l'assistance technique de Red Hat Linux, consultez l'annexe sur l'*Aassistance technique* du *Guide d'installation officiel Red Hat Linux*.

Merci d'avoir choisi Red Hat Linux et bonne chance !

L'équipe de documentation Red Hat

I. Références liées au système

Table des matières

1. Structure d'un système de fichiers
2. Le système de fichiers `/proc`
3. Processus de démarrage, Init et arrêt
4. GRUB
5. Le système de fichiers ext3
6. Utilisateurs et groupes
7. Serveurs et clients X

Chapitre 1. Structure d'un système de fichiers

Pourquoi partager une structure commune ?

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

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

- Fichiers partageables/fichiers non partageables
- Fichiers variables/fichiers statiques

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

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

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

Précédent | Sommaire | Suivant
Références liées au système | Niveau supérieur | Aperçu du FHS (Filesystem Hierarchy Standard)

Aperçu du FHS (Filesystem Hierarchy Standard)

Red Hat adhère au *FHS* (*Filesystem Hierarchy Standard* / standard en matière de hiérarchie du système de fichiers), document de collaboration définissant les noms et les emplacements de nombreux fichiers et répertoires. Nous continuerons à respecter cette norme pour garantir la conformité de Red Hat Linux.

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

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

http://www.pathname.com/fhs

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

Organisation de FHS

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

Le répertoire `/dev`

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

Le répertoire `/etc`

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

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

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

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

Le répertoire `/lib`

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

Le répertoire `/mnt`

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

Le répertoire `/opt`

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

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

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

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

Le répertoire `/proc`

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

Etant donné l'immense variété de données disponibles dans `/proc` et les différentes façons dont ce répertoire peut être utilisé pour communiquer avec le noyau, un chapitre entier a été consacré à ce sujet. Pour plus d'informations, consultez le Chapitre 2.

Le répertoire `/sbin`

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

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

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

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

Le répertoire /usr

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

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

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

Le répertoire /usr/local

FHS indique ce qui suit :

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

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

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

Le répertoire `/var`

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

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

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

```
/var
  |- arpwatrch
  |- cache
  |- db
  |- ftp
  |- gdm
  |- kerberos
  |- lib
  |- local
  |- lock
  |- log
  |- named
```

```
  |- mail -> spool/mail
  |- nis
  |- opt
  |- preserve
  |- run
  +- spool
       |- anacron
       |- at
       |- cron
       |- fax
       |- lpd
       |- mail
       |- mqueue
       |- news
       |- rwho
       |- samba
       |- slrnpull
       |- squid
       |- up2date
       |- uucp
       |- uucppublic
       |- vbox
       |- voice
  |- tmp
  |- tux
  |- www
  |- yp
```

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

`/usr/local` dans Red Hat Linux

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

d'utiliser `/usr/local` pour y placer les logiciels locaux de votre ordinateur.

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

Précédent
Structure d'un système de fichiers

Sommaire
Niveau supérieur

Suivant
Emplacement de fichiers Red Hat Linux spéciaux

Emplacement de fichiers Red Hat Linux spéciaux

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

Le répertoire `/var/spool/up2date/` contient des fichiers utilisés par le **Red Hat Update Agent**, y compris des informations de titres RPM. Cet emplacement peut aussi être utilisé pour stocker temporairement des RPM téléchargés lorsque vous mettez à jour votre système. Pour plus d'informations sur le Réseau Red Hat, voyez le site web à l'adresse suivante: https://rhn.redhat.com/.

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

Un autre emplacement spécial (`/etc/sysconfig`) stocke des informations de configuration. De nombreux scripts lancés au démarrage utilisent les fichiers de ce répertoire. Voyez la section intitulée *Information Sysconfig* dans Chapitre 3.

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

Avertissement

Ne supprimez le répertoire `/initrd/` sous aucun prétexte. L'enlever empêcherait votre système de démarrer, avec un message d'erreur panique noyau.

Chapitre 2. Le système de fichiers /proc

Le répertoire `/proc` contient des fichiers virtuels qui offrent des informations sur l'état courant du noyau Linux en cours d'exécution. Cela permet aux utilisateurs de scruter une vaste gamme d'informations, fournies de manière efficace du point de vue du noyau au sein du système. En outre, les utilisateurs peuvent utiliser le répertoire `/proc` pour communiquer des changements de configuration particuliers au noyau.

Un système de fichiers virtuels

Sous Linux, tout est stocké dans des fichiers. La plupart des utilisateurs sont d'ailleurs familiers avec les deux types de fichier principaux, soit texte et binaire. Cependant, le répertoire `/proc` contient des fichiers qui ne font partie d'aucun système de fichiers associé à vos disques durs, CD-ROM ou tout autre périphérique physique de stockage branché à votre système (sauf, pourrait-on dire, votre mémoire vive). Ces fichiers font plutôt partie d'un *système de fichiers virtuels*, activé ou désactivé dans le noyau Linux lorsqu'il est compilé.

Les fichiers virtuels `/proc` ont des qualités intéressantes. D'abord, la plupart d'entre eux ont une taille de 0 octet. Toutefois, lorsqu'ils sont visualisés, ils contiennent pas mal d'informations. De plus, la plupart d'entre eux ont une date et une heure qui reflètent le moment présent, ce qui signifie qu'ils changent continuellement.

De nombreux programmes utilisent le système de fichiers `/proc` pour obtenir les paramètres du système de façon à pouvoir offrir de meilleures performances et plus de fonctions.

Puis, l'administrateur système peut utiliser `/proc` comme méthode simple d'accès aux informations sur l'état du noyau, les attributs de l'ordinateur, l'état des processus individuels, etc. La plupart des fichiers dans ce répertoire, tels que `interrupts`, `meminfo`, `mounts` et `partitions`, fournissent un aperçu actuel de l'environnement d'un système. D'autres, comme les répertoires `file systems` et `/proc/sys/` fournissent des informations sur la configuration des logiciels.

Enfin, pour faciliter le tout, les fichiers qui contiennent des informations sur un sujet similaire sont groupés dans des répertoires et sous-répertoires virtuels, comme `/proc/ide/` pour tous les périphériques physiques IDE.

Visualisation de fichiers virtuels

En utilisant les commandes `cat`, `more` ou `less` combinées aux fichiers dans `/proc`, vous avez immédiatement accès à une énorme source d'informations sur le système. Par exemple, pour savoir quel genre d'Unité centrale possède votre ordinateur, tapez `cat cpuinfo` et vous verrez quelquechose ressemblant à ceci:

```
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
```

Comme vous pouvez le constater, certaines de ces informations parlent d'elles-mêmes, alors que d'autres semblent écrites en un code étrange. C'est pourquoi des utilitaires existent pour collecter des données dans des fichiers `/proc` et les afficher d'une manière exploitable humainement. `apm`, `free` et `top` sont des exemples de ce genre d'applications.

Note **Remarque**

Quelques-uns des fichiers dans `/proc` sont paramétrés pour n'être lus que par le super-utilisateur, vous devrez donc vous connectez en tant que super-utilisateur avant de pouvoir essayer de les lire.

Changement des fichiers virtuels

En général, la plupart des fichiers virtuels dans le répertoire `/proc` ne peuvent être que lus. Toutefois, quelques uns peuvent être utilisés pour ajuster les réglages dans le noyau. Cela vaut particulièrement pour les fichiers du sous-répertoire `/proc/sys/`.

Pour changer la valeur d'un fichier virtuel, utilisez la commande `echo` et un symbole **>** pour rediriger la nouvelle valeur vers le fichier. Par exemple, pour changer votre nom d'hôte à la volée, vous pouvez taper:

```
echo bob.subgenious.com > /proc/sys/kernel/hostname
```

D'autres fichiers servent de commutation binaire. Par exemple, si vous tapez `cat /proc/sys/net/ipv4/ip_forward`, vous obtiendrez soit un `0`, soit un `1`. Le `0` indique que le noyau ne redirige pas les paquetages réseau. En utilisant la commande `echo` pour changer la valeur du fichier `ip_forward` en `1`, vous pouvez déclencher immédiatement la redirection de fichiers.

Pour une liste de quelques-uns des fichiers de configuration du noyau disponibles dans `/proc/sys/`, consultez la [la section intitulée *`/proc/sys`*](#).

[Précédent](#) Emplacement de fichiers Red Hat Linux spéciaux

[Sommaire](#)

[Niveau supérieur](#)

[Suivant](#) Les fichiers du niveau supérieur dans `/proc`

Les fichiers du niveau supérieur dans /proc

Ci-dessous se trouve une liste de quelques-uns des fichiers virtuels les plus utiles dans le niveau supérieur du répertoire /proc.

/proc/apm

Ce fichier fournit des informations sur l'état de la *gestion de la consommation d'énergie* (APM) et les options sur le système. Ces informations sont utilisées par le noyau pour fournir des informations à la commande apm.

La sortie de ce fichier sur un système sans batterie et, par conséquent, branché constamment sur un réseau d'alimentation AC ressemble à ceci :

```
1.16 1.2 0x03 0x01 0xff 0x80 -1% -1 ?
```

L'exécution de la commande apm -v sur un tel système donne un résultat semblable à ce qui suit :

```
APM BIOS 1.2 (kernel driver 1.14)
AC on-line, no system battery
```

Pour ces systèmes, apm ne peut pas faire grand chose d'autre que de mettre l'ordinateur en mode standby. La commande apm est beaucoup plus utile sur des portables et autres systèmes Linux portables. Cela se reflète également dans leurs fichiers /proc/apm. Voici un exemple de sortie de ce fichier sur un portable qui exécute Linux, lorsqu'il est branché à une prise de courant :

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

Si l'on débranche cet ordinateur de la prise de courant et le fait fonctionner à l'aide de sa propre batterie pendant quelques minutes, vous remarquerez que le contenu du fichier apm change :

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

Dans cet état, la commande apm fournit des informations lisibles à partir des données :

```
APM BIOS 1.2 (kernel driver 1.14)
AC off-line, battery status high: 99% (1 day, 5:52)
```

Cela montre bien la relation entre les données situées dans des fichiers `/proc` bruts et les utilitaires conçus pour se servir de ces informations dans un but spécifique.

/proc/cmdline

Ce fichier montre principalement les paramètres passés au noyau Linux lorsqu'il est démarré. Voici un exemple de ce à quoi un fichier `/proc/cmdline` peut ressembler :

```
ro root=/dev/hda2
```

Les données importantes contenues dans ce fichier peuvent être divisées de la façon suivante :

- `ro`, qui signifie que le noyau est chargé en lecture seule ;
- `root=/dev/hda2` — qui est la partition dans laquelle réside le système de fichiers racine.

/proc/cpuinfo

Ce fichier change selon le type d'unité centrale installée sur votre système. La sortie est assez simple à comprendre. Voici un exemple de ce à quoi peut ressembler ce fichier :

```
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
```

- `processor` — Fournit à chaque unité centrale un numéro d'identification. Si vous n'avez qu'une seule unité

centrale, ce numéro sera `0`.

- `cpu family` — Indique le type d'unité centrale que vous avez sur le système. Vous n'avez qu'à placer le numéro devant le « 86 » pour calculer la valeur. Cela est particulièrement pratique si vous vous interrogez sur l'architecture d'un système plus ancien (686, 586, 486 ou 386). Comme des paquetages RPM sont compilés à l'occasion pour des architectures particulières, cette valeur vous indique quels paquetages installer sur le système.
- `model name` — Donne le nom communément utilisé de l'unité centrale, de même que son nom de projet.
- `cpu MHz` — Indique la vitesse précise en MHz de cette unité centrale (en millièmes).
- `cache size` — Indique la quantité de mémoire cache de niveau 2 disponible pour l'unité centrale.
- `flags` — Définit un certain nombre de caractéristiques de l'unité centrale, telles que la présence d'une unité de calcul en virgule flottante (FPU) et la capacité de traiter des instructions MMX.

/proc/devices

Ce fichier affiche les divers périphériques d'entrée-sortie de caractères et par blocs actuellement configurés pour être utilisés avec le noyau. Il ne contient pas les modules qui sont disponibles, mais non chargés dans le noyau. Voici un exemple de ce fichier :

```
Character devices:
  1 mem
  2 pty
  3 ttyp
  4 ttyS
  5 cua
  7 vcs
 10 misc
 14 sound
 29 fb
 36 netlink
128 ptm
129 ptm
136 pts
137 pts
162 raw
254 iscsictl

Block devices:
  1 ramdisk
  2 fd
  3 ide0
  9 md
 22 ide1
```

La sortie de `/proc/devices` inclut le nombre majeur et le nom du périphérique.

Les *périphériques d'entrée-sortie de caractères* sont semblables aux *périphériques d'entrée-sortie par blocs*, à l'exception de deux différences de base.

Premièrement, les périphériques d'entrée-sortie par blocs ont un tampon disponible pour des demandes qui leur sont

envoyées, ce qui leur permet de mettre les demandes en ordre avant de les traiter. Cela est très utile avec des périphériques conçus pour stocker des informations, tels que les disques durs, parce que la possibilité de mettre les demandes en ordre avant de les écrire sur le périphérique permet de les placer plus efficacement. Les périphériques d'entrée-sortie de caractères ne nécessitent pas ce genre de mise en tampon.

Deuxièmement, les périphériques d'entrée-sortie par blocs peuvent envoyer et recevoir les informations par blocs d'une taille spécifique, pouvant être configurée de façon à répondre aux exigences d'un périphérique donné. Les périphériques d'entrée-sortie de caractères quant à eux envoient des données tant qu'il y a de l'espace, sans taille préconfigurée.

Vous trouverez plus d'informations sur les périphériques dans `/usr/src/linux-2.4/Documentation/devices.txt`.

/proc/dma

Ce fichier contient une liste des canaux d'accès direct en mémoire (DMA) ISA enregistrés utilisés. Voici un exemple de fichier `/proc/dma` :

```
 4: cascade
```

/proc/execdomains

Ce fichier donne la liste des domaines d'exécution actuellement pris en charge par le noyau Linux, ainsi que l'éventail de personnalités qu'ils prennent en charge.

```
0-255   Linux           [kernel]
```

Imaginez-vous les *domaines d'exécution* comme étant une sorte de personnalité d'un système d'exploitation donné. D'autres formats binaires, tels que Solaris, UnixWare et FreeBSD peuvent être utilisés avec Linux. En changeant la personnalité d'une tâche qui s'exécute sous Linux, un programmeur peut changer la façon dont le système d'exploitation traite certains appels système d'un binaire donné. A l'exception du domaine d'exécution `PER_LINUX`, ils peuvent être mis en oeuvre en tant que modules chargeables dynamiquement.

/proc/fb

Ce fichier contient une liste de mémoires vidéo, avec le numéro de chaque mémoire vidéo et le pilote qui la contrôle. La sortie de `/proc/fb` pour les systèmes qui contiennent des mémoires vidéo ressemble généralement à ceci :

```
0 VESA VGA
```

/proc/filesystems

Ce fichier affiche une liste des types de système de fichiers actuellement pris en charge par le noyau. Voici un exemple de

fichier `/proc/filesystems` d'un noyau générique :

```
nodev   rootfs
nodev   bdev
nodev   proc
nodev   sockfs
nodev   tmpfs
nodev   shm
nodev   pipefs
        ext2
nodev   ramfs
        iso9660
nodev   devpts
        ext3
nodev   autofs
nodev   binfmt_misc
```

La première colonne indique si le système de fichiers est monté sur un périphérique d'entrée-sortie par blocs ; s'il est écrit `nodev` dans cette colonne, le système de fichiers n'est pas monté sur un périphérique d'entrée-sortie par blocs. La seconde colonne établit la liste des noms de système de fichiers pris en charge.

Ces informations sont utilisées par la commande `mount` pour chercher les divers systèmes de fichiers lorsque aucun d'eux n'est spécifié comme argument.

`/proc/interrupts`

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

```
           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 unités centrales, le fichier peut être quelque peu 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 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 cet IRQ.

Chaque type d'interruption visualisé dans ce fichier, spécifique à l'architecture, a une signification différente. Pour les ordinateurs x86, les valeurs suivantes sont communes :

- `XT-PIC` — Anciennes interruptions d'ordinateurs AT qui ont longtemps été en circulation.
- `IO-APIC-edge` — Signal de voltage sur des transitions d'interruption de bas à élevé, créant une *dénivellation* là où l'interruption a lieu et n'étant signalé qu'une seule fois. Ce genre d'interruption, de même que l'interruption `IO-APIC-level`, ne se rencontrent que sur des systèmes ayant des unités centrales de la famille 586 ou plus.
- `IO-APIC-level` — Génère des interruptions lorsque le signal de voltage devient élevé, jusqu'à ce que le signal redevienne bas.

/proc/iomem

Ce fichier montre la topographie mémoire actuelle du système pour ses différents périphériques :

```
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 types différents de mémoire. La deuxième colonne indique la sorte de mémoire située dans ces registres. Plus particulièrement, cette colonne vous indique quels registres sont utilisés par le noyau dans la mémoire vive du système ou, si vous avez plusieurs ports Ethernet sur votre carte interface de réseau, les registres de mémoire assignés à chaque port.

/proc/ioports

Semblable à `/proc/iomem`, `/proc/ioports` fournit une liste des ports actuellement enregistrés utilisés pour l'entrée ou la sortie de communications avec un périphérique. Ce fichier peut être assez long ; le début ressemble à ceci :

```
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 l'éventail d'adresses de port E/S réservées au périphérique spécifié dans la seconde colonne.

/proc/isapnp

Ce fichier donne une liste des cartes *Plug & Play* (PnP) dans les fentes ISA du système. Cela se voit surtout avec des cartes son, mais peut aussi inclure d'autres périphériques. Un fichier `/proc/isapnp` ayant une entrée Soundblaster ressemble à ce qui suit :

```
Card 1 'CTL0070:Creative ViBRA16C PnP' PnP version 1.0 Product version 1.0
  Logical device 0 'CTL0001:Audio'
    Device is not active
    Active port 0x220,0x330,0x388
    Active IRQ 5 [0x2]
    Active DMA 1,5
    Resources 0
      Priority preferred
      Port 0x220-0x220, align 0x0, size 0x10, 16-bit address decoding
      Port 0x330-0x330, align 0x0, size 0x2, 16-bit address decoding
      Port 0x388-0x3f8, align 0x0, size 0x4, 16-bit address decoding
      IRQ 5 High-Edge
      DMA 1 8-bit byte-count compatible
      DMA 5 16-bit word-count compatible
      Alternate resources 0:1
        Priority acceptable
        Port 0x220-0x280, align 0x1f, size 0x10, 16-bit address decoding
        Port 0x300-0x330, align 0x2f, size 0x2, 16-bit address decoding
        Port 0x388-0x3f8, align 0x0, size 0x4, 16-bit address decoding
        IRQ 5,7,2/9,10 High-Edge
        DMA 1,3 8-bit byte-count compatible
        DMA 5,7 16-bit word-count compatible
```

Ce fichier peut être assez long, selon le nombre de périphériques affichés et leurs exigences ou demandes en termes de ressources.

Chaque carte affiche son nom, le numéro de version PnP et le numéro de version du produit. Si le périphérique est activé et configuré, ce fichier montre également le port et les numéros IRQ pour le périphérique. De plus, afin d'assurer une meilleure compatibilité, la carte spécifie les valeurs `preferred` et `acceptable` pour un certain nombre de paramètres. L'objectif est de permettre aux cartes PnP de travailler les unes aux côtés des autres et d'éviter tout IRQ ou conflit de port.

/proc/kcore

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

Avertissement **Avertissement**

N'essayez pas de visualiser le fichier `kcore` dans `/proc`. Le contenu de ce fichier va submerger votre terminal de texte. Si vous l'avez ouvert accidentellement, pressez [Ctrl]-[C] pour arrêter le processus, puis tapez `reset` pour faire revenir l'invite de commande.

Le contenu de ce fichier sont conçus pour l'examen par un débogueur, comm`gdb`, et ne sont pas humainement lisibles.

/proc/kmsg

Ce fichier est utilisé pour contenir des messages générés par le noyau. Ces messages sont ensuite pris par d'autres programmes, tels que `klogd`.

/proc/ksyms

Ce fichier contient les définitions de symbole exporté utilisées par les outils de module pour lier et associer dynamiquement des modules chargeables.

```
e003def4 speedo_debug   [eepro100]
e003b04c eepro100_init  [eepro100]
e00390c0 st_template    [st]
e002104c RDINDOOR       [megaraid]
e00210a4 callDone       [megaraid]
e00226cc megaraid_detect        [megaraid]
```

La deuxième colonne indique le nom d'une fonction du noyau, alors que la première donne la liste d'adresses de mémoire de cette fonction dans le noyau. La dernière colonne indique le nom du module chargé pour fournir cette fonction.

/proc/loadavg

Ce fichier fournit un aperçu de la moyenne de charge ou de l'utilisation de l'unité centrale, dans le temps, et donne aussi des données supplémentaires utilisées par la commande `uptime` et d'autres commandes. Voici un exemple de fichier `loadavg` :

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

Les trois premières colonnes mesurent l'utilisation de l'unité centrale en fonction des dernières périodes de 1, 5 et 10 minutes. La quatrième colonne indique le nombre de processus en cours d'exécution et le nombre total de processus. La dernière colonne affiche le dernier ID de processus utilisé.

/proc/locks

Ce fichier affiche les fichiers actuellement verrouillés par le noyau. Le contenu de ce fichier comprend des données de débogage interne du noyau et peut varier énormément selon l'utilisation du système. Voici un exemple de fichier `locks` d'un système très peu chargé :

```
1: FLOCK  ADVISORY  WRITE 807 03:05:308731 0 EOF c2a260c0 c025aa48 c2a26120
2: POSIX  ADVISORY  WRITE 708 03:05:308720 0 EOF c2a2611c c2a260c4 c025aa48
```

Chaque verrouillage se voit assigner un numéro unique au début de chaque ligne. La deuxième colonne indique la classe de verrouillage utilisée ; `FLOCK` représente les verrouillages de fichier UNIX de style plus ancien de l'appel de système `flock` et `POSIX` représente les verrouillages POSIX, plus récents, de l'appel de système `lockf`.

La troisième colonne peut avoir 2 valeurs. ADVISORY signifie que le verrouillage n'empêche pas les autres d'avoir accès aux données ; il ne fait qu'empêcher les autres d'essayer de les verrouiller. MANDATORY signifie que personne n'est autorisé à accéder aux données tant que le verrouillage est en place. La quatrième colonne indique si le verrouillage autorise le détenteur à l'accès READ (lecture) ou WRITE (écriture) au fichier et la cinquième colonne montre l'identifiant du processus qui détient le verrouillage.

La sixième colonne montre l'identifiant du fichier verrouillé, sous la forme *PERIPHERIQUE-MAJEUR*:*PERIPHERIQUE-MINEUR*:*NO.-INODE*. La septième colonne indique le début et la fin de la région verrouillée du fichier. Les autres colonnes pointent vers des structures de données internes du noyau utilisées aux fins de débogage spécialisé et peuvent être ignorées.

/proc/mdstat

Ce fichier contient des informations sur les configurations RAID à disques multiples. Si votre système n'a pas ce genre de configuration, votre fichier mdstat ressemblera à ceci :

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

Il y a peu d'intérêt, à moins que vous n'ayez des périphériques md créés et en cours d'utilisation. Dans ce cas, vous pouvez utiliser mdstat pour avoir le cadre général de ce qu'il se passe avec vos périphériques md*X*.

Le fichier /proc/mdstat suivant montre un système sur lequel md0 est configuré en tant que périphérique RAID 1. La resynchronisation des disques est en cours :

```
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>
```

/proc/meminfo

Voici l'un des fichiers /proc les plus communément utilisés car il donne de nombreuses informations importantes sur l'utilisation actuelle de mémoire vive du système. Un système ayant 256 Mo de mémoire vive et 384 Mo d'espace swap pourrait avoir un fichier /proc/meminfo semblable à ceci :

```
        total:    used:    free:  shared: buffers:  cached:
Mem:  261709824 253407232  8302592        0 120745984 48689152
Swap: 402997248     8192 402989056
MemTotal:       255576 kB
MemFree:          8108 kB
MemShared:           0 kB
Buffers:        117916 kB
Cached:          47548 kB
Active:         135300 kB
Inact_dirty:     29276 kB
Inact_clean:       888 kB
Inact_target:        0 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:       255576 kB
LowFree:          8108 kB
SwapTotal:      393552 kB
SwapFree:       393544 kB
```

La plupart des informations dans cet exemple sont utilisées par la commande `top`. En fait, la sortie de la commande `free` est même similaire en apparence au contenu et à la structure de `meminfo`. En examinant directement `meminfo`, plus de détails sont révélés :

- `Mem` — Etat courant de la mémoire vive du système, ainsi qu'une division de l'utilisation en octets des mémoires totale, utilisée, libre, partagée, tampon et cache.
- `Swap` — Quantité totale, utilisée et libre d'espace swap, en octets.
- `MemTotal` — Quantité totale de mémoire vive, en Ko.
- `MemFree` — Quantité de mémoire vive, en Ko, non utilisée par le système.
- `MemShared` — Non utilisé avec les noyaux 2.4 ou supérieurs, mais gardé pour des raisons de compatibilité avec les versions de noyau précédentes.
- `Buffers` — Quantité de mémoire vive, en Ko, utilisée pour les tampons de fichier.
- `Cached` — Quantité de mémoire vive, en Ko, utilisée comme mémoire cache.
- `Active` — Quantité totale de tampon ou de mémoire cache de pages, en Ko, en utilisation active.
- `Inact_dirty` — Quantité totale de tampon ou de mémoire cache de pages, en Ko, qui peut être libérée.
- `Inact_clean` — Quantité totale de tampon ou de mémoire cache de pages, en Ko, qui est réellement libre et disponible.
- `Inact_target` — La quantité nette d'attributions par seconde, en Ko, sous forme de moyenne par minute.
- `HighTotal` et `HighFree` — Quantité totale et libre de mémoire, respectivement, 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, respectivement, 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, en Ko.
- `SwapFree` — Quantité totale de mémoire swap libre, en Ko.

/proc/misc

Ce fichier affiche la liste des pilotes divers enregistrés sur le périphérique majeur divers, qui est le numéro 10 :

```
135 rtc
  1 psaux
134 apm_bios
```

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

/proc/modules

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

```
ide-cd                  27008   0 (autoclean)
cdrom                   28960   0 (autoclean) [ide-cd]
soundcore                4100   0 (autoclean)
agpgart                 31072   0 (unused)
binfmt_misc              5956   1
iscsi                   32672   0 (unused)
scsi_mod                94424   1 [iscsi]
autofs                  10628   0 (autoclean) (unused)
tulip                   48608   1
ext3                    60352   2
jbd                     39192   2 [ext3]
```

La première colonne contient le nom du module. La deuxième indique la taille de la mémoire du module, en octets. La troisième indique si le module est actuellement chargé (`1`) ou non chargé (`0`). La dernière colonne indique si le module peut se décharger automatiquement après une période d'inactivité (`autoclean`) ou s'il n'est pas utilisé (`unused`). Tout module ayant une ligne qui contient un nom entre parenthèses (`[` ou `]`) signifie que ce module dépend de la présence d'un autre module pour fonctionner.

/proc/mounts

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

```
rootfs / rootfs rw 0 0
/dev/hda2 / ext3 rw 0 0
/proc /proc proc rw 0 0
/dev/hda1 /boot ext3 rw 0 0
none /dev/pts devpts rw 0 0
none /dev/shm tmpfs rw 0 0
none /proc/sys/fs/binfmt_misc binfmt_misc rw 0 0
```

Cette sortie est semblable au contenu de `/etc/mtab`, sauf que `/proc/mount` peut être plus actuel.

La première colonne spécifie le périphérique monté et la deuxième colonne indique le point de montage. La troisième donne le type de système de fichiers et la quatrième vous 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`.

/proc/mtrr

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

```
reg00: base=0x00000000 (   0MB), size=  64MB: write-back, count=1
```

Les MTRR sont utilisés avec les unités centrales de la famille P6 d'Intel (Pentium Pro et supérieur) pour contrôler l'accès de l'unité centrale aux gammes de mémoire. En utilisant une carte vidéo sur un bus PCI ou ACP, un fichier `mtrr` correctement configuré peut augmenter les performances de plus de 150 %.

Dans la plupart des cas, cette valeur est correctement configurée pour vous. Pour avoir plus de renseignements sur les MTRR et la configuration manuelle de ce fichier, reportez-vous à http://web1.linuxhq.com/kernel/v2.3/doc/mtrr.txt.html.

/proc/partitions

- `major` — Nombre majeur du périphérique avec cette partition. Le nombre majeur dans cet exemple (`3`) correspond au périphérique `ide0` dans `/proc/devices`, ce qui nous permet de savoir le type de pilote de périphérique utilisé pour interagir avec cette partition.
- `minor` — Nombre mineur du périphérique avec cette partition. Cela permet de séparer les partitions en différents périphériques physiques et fait référence au nombre situé à la fin du nom de la partition.
- `#blocks` — Fournit la liste du nombre de blocs de disque physique contenus dans une partition donnée.
- `name` — Nom de la partition.

/proc/pci

Ce fichier contient une liste complète des périphériques PCI sur votre système. Evidemment, selon que vous ayez de nombreux périphériques PCI sur votre système ou non, `/proc/pci` peut être assez long. Voici 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. En plus de fournir le nom et la version du périphérique, ce qui est toujours bon à savoir lorsque vous oubliez la marque de votre carte d'interface réseau, cette liste vous donne des informations IRQ détaillées afin que vous puissiez détecter rapidement des conflits.

Tuyau

Astuce

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

```
lspci -vb
```

/proc/slabinfo

Ce fichier fournit des informations sur l'utilisation de la mémoire au niveau bloc (slab). Les noyaux Linux supérieurs à 2.2

utilisent des " *groupes d'emplacement mémoire de type bloc* " pour gérer la mémoire au-dessus du niveau page. Les objets couramment utilisés ont leurs propres groupes d'emplacement mémoire de type bloc.

Les valeurs dans ce fichier sont présentées selon l'ordre suivant : nom de cache, nombre d'objets actifs, nombre total d'objets, taille des objets, nombre de blocs (slabs) actifs des objets, nombre total de blocs des objets et nombre de pages par bloc.

Il est à noter qu'*actif* dans ce cas signifie " utilisé ". Un objet actif est un objet en cours d'utilisation et un bloc actif est un bloc qui contient des objets en cours d'utilisation.

/proc/stat

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

```
cpu  1139111 3689 234449 84378914
cpu0 1139111 3689 234449 84378914
page 2675248 8567956
swap 10022 19226
intr 93326523 85756163 174412 0 3 3 0 6 0 1 0 428620 0 60330 0 1368304 5538681
disk_io: (3,0):(1408049,445601,5349480,962448,17135856)
ctxt 27269477
btime 886490134
processes 206458
```

Voici certaines des statistiques les plus appréciées :

- `cpu` — Nombre de *jiffies* (1/100 de seconde) pendant lequel le système a été en mode utilisateur, mode utilisateur avec basse priorité (nice), mode système et au repos. Le total pour chacune des unités centrales est donné au sommet et chaque unité centrale individuelle est énumérée en dessous avec ses propres statistiques.
- `page` — Nombre de pages que le système a allouées vers et depuis le disque.
- `swap` — Nombre de pages échangées par le système.
- `intr` — Nombre d'interruptions qu'a subi le système.
- `btime` — Moment de démarrage, mesuré en nombre de secondes écoulées depuis le 1er janvier 1970, ce que l'on appelle aussi parfois l'*époque*.

/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 ceci :

```
Filename                        Type            Size    Used    Priority
/dev/hda6                       partition       136512  20024   -1
```

Bien que certaines de ces informations peuvent être obtenues à l'aide d'autres fichiers `/proc`, `swap` fournit un instantané

rapide de chaque nom de fichier swap, du type d'espace swap et des tailles totales et utilisées (en Ko). La colonne " Priority " est utile lorsque plusieurs fichiers swap sont utilisés et que certains d'entre eux sont préférés par rapport aux autres (s'ils sont sur des disques durs plus rapides par exemple). Plus la priorité est basse, plus il est possible que le fichier swap correspondant soit utilisé.

/proc/uptime

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

```
350735.47 234388.90
```

Le premier nombre vous indique le nombre total de secondes de fonctionnement depuis le démarrage. Le second vous indique, en secondes également, la période d'inactivité.

/proc/version

Ce fichier vous indique les versions du noyau Linux et de `gcc`, de même que la version de Red Hat Linux installée sur le système :

```
Linux version 2.4.18-0.4 (user@foo.redhat.com) (gcc version 2.96 20000731
(Red Hat Linux 7.2 2.96-106)) #1 Wed Mar 13 10:47:08 EST 2002
```

Ces informations ont diverses utilités, telles que de fournir des données sur la version à l'invite de connexion standard.

Précédent
Le système de fichiers `/proc`

Sommaire
Niveau supérieur

Suivant
Répertoires dans `/proc`

Répertoires dans /proc

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

Répertoires de processus

Chaque répertoire /proc contient un certain nombre de répertoires nommés à l'aide d'un chiffre. Voici comment se présente une liste de ces répertoires :

```
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 concernant ce processus. Le propriétaire et le groupe de chaque répertoire de processus est paramétré sur l'utilisateur qui exécute le processus. Lorsque le processus est terminé, son répertoire de processus /proc disparaît. Toutefois, pendant l'exécution du processus, de nombreuses informations spécifiques à ce processus sont contenues dans les différents fichiers du répertoire de processus.

Chaque répertoire de processus contient les fichiers suivants :

- cmdline — Arguments de la ligne de commande qui ont lancé le processus. La sortie du fichier cmdline pour le processus sshd ressemble à ceci :

  ```
  /usr/sbin/sshd
  ```

- cpu — Informations spécifiques sur l'utilisation de chaque unité centrale du système. Un processus exécuté sur un système à double unité centrale produit une sortie semblable à ce qui suit :

  ```
  cpu  11 3
  cpu0 0 0
  cpu1 11 3
  ```

- cwd — Lien vers le répertoire de travail courant pour ce processus.
- environ — Liste des variables d'environnement pour le processus. La variable d'environnement est fournie en majuscules et la valeur est en minuscules.

- `exe` — Lien vers le fichier exécutable de ce processus.
- `fd` — Répertoire qui contient tous les descripteurs de fichier pour un processus donné. Ils sont fournis en 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` — Topographies mémoire vers les divers fichiers exécutables et les bibliothèques associés à ce processus. Ce fichier peut être long, selon la complexité du processus. Voici comment le fichier débute pour `sshd` :

```
08048000-08080000 r-xp 00000000 03:05 226209     /usr/sbin/sshd
08080000-08082000 rw-p 00037000 03:05 226209     /usr/sbin/sshd
08082000-080c3000 rwxp 00000000 00:00 0
40000000-40016000 r-xp 00000000 03:05 304721     /lib/ld-2.2.2.so
40016000-40017000 rw-p 00015000 03:05 304721     /lib/ld-2.2.2.so
40017000-40018000 rw-p 00000000 00:00 0
40019000-4001b000 r-xp 00000000 03:05 144433     /lib/security/pam_stack.so
4001b000-4001c000 rw-p 00001000 03:05 144433     /lib/security/pam_stack.so
```

- `mem` — Mémoire retenue par le processus.
- `root` — Lien vers le répertoire root du processus.
- `stat` — Etat du processus.
- `statm` — Etat de la mémoire utilisée par le processus. Voici un exemple de fichier `statm` :

```
140 72 63 22 0 50 22
```

  Les sept colonnes font référence à différentes statistiques de mémoire pour le processus, soit, de droite à gauche, divers aspects de la mémoire utilisée :

  1. Taille totale du programme, en Ko ;
  2. Taille de portions de mémoire, 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 " sales ".

- `status` — Etat du processus sous une forme beaucoup plus lisible que celle qui est offerte par `stat` ou `statm`. Voici un exemple de ce à quoi peut ressembler ce fichier pour `sshd` :

```
Name:   sshd
State:  S (sleeping)
Pid:    14466
PPid:   723
TracerPid:      0
Uid:    0       0       0       0
Gid:    0       0       0       0
FDSize: 32
Groups:
VmSize:     3596 kB
VmLck:         0 kB
VmRSS:       288 kB
VmData:      552 kB
VmStk:        28 kB
VmExe:       224 kB
VmLib:      2596 kB
SigPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: 8000000000001000
SigCgt: 0000000000012000
CapInh: 0000000000000000
CapPrm: 00000000fffffeff
CapEff: 00000000fffffeff
```

Outre le nom et l'ID du processus, l'état (tel que `S (sleeping)` ou `R (running)`) et l'ID de l'utilisateur/groupe qui exécute le processus sont disponibles, de même qu'un grand nombre d'informations détaillées sur l'utilisation de la mémoire.

/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 devoir savoir son ID de processus.

Dans un environnement shell, la génération de la liste du répertoire `/proc/self` produit le même contenu que la génération de la liste du répertoire de processus pour ce processus.

/proc/bus

Ce répertoire contient des informations spécifiques aux nombreux bus disponibles sur le système. Ainsi, par exemple, sur un système standard ayant des bus ISA, PCI et USB, des informations actuelles sur chacun de ces bus disponibles se trouvent dans son répertoire sous `/proc/bus`.

Le contenu des sous-répertoires et fichiers disponibles diffère grandement selon la configuration de votre système. Cependant, chaque répertoire pour chacun des types de bus contient au moins un répertoire pour chaque bus de ce type. Ces répertoires individuels de bus, généralement spécifiés par des chiffres, tels que `00`, contiennent des fichiers binaires qui font référence aux divers périphériques disponibles sur les bus en question.

Exemple : un système ayant un bus USB auquel aucun périphérique n'est branché, a un répertoire `/proc/bus/usb` qui contient plusieurs fichiers :

```
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
[root@thoth /]# ls -l /proc/bus/usb/001
total 1
-rw-r--r--    1 root     root           18 May  3 16:25 001
```

Le répertoire `/proc/bus/usb` contient des fichiers qui détectent les différents périphériques sur les bus USB, ainsi que les pilotes nécessaires pour les utiliser. Le répertoire `001` contient tous les périphériques sur le premier (et le seul) bus USB. En examinant le contenu du fichier `devices`, nous constatons qu'il s'agit du concentrateur root USB sur la carte mère :

```
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
```

/proc/driver

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

Un fichier commun se trouvant à cet endroit est `rtc`, qui fournit une sortie provenant du pilote pour l'*horloge interne* du système, le dispositif qui maintient l'heure lorsque le système est éteint. Voici un exemple de ce à quoi peut ressembler `/proc/driver/rtc` :

```
rtc_time        : 01:38:43
rtc_date        : 1998-02-13
rtc_epoch       : 1900
alarm           : 00:00:00
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 plus d'informations sur l'horloge interne, consultez `/usr/src/linux-2.4/Documentation/rtc.txt`.

/proc/ide

Ce répertoire contient une gamme variée d'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 aussi disponible ; il fournit le numéro de version des divers pilotes utilisés sur les canaux IDE :

```
ide-cdrom version 4.59
ide-floppy version 0.97
ide-disk version 1.10
```

Plusieurs jeux de circuits fournissent également un fichier d'informations dans ce répertoire, donnant ainsi d'autres renseignements sur les lecteurs branchés via les différents canaux. Exemple : un jeu de circuits générique Ultra 33 PIIX4 d'Intel produit un fichier `/proc/ide/piix` qui vous indique si DMA et UDMA sont activés pour les périphériques 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
```

Si vous examinez le répertoire d'un canal IDE, tel que `ide0` pour le premier canal, vous obtenez des informations additionnelles. Le fichier `channel` indique le numéro de canal, alors que `model` vous indique le type de bus pour le canal (tel que `pci`).

Répertoires de périphérique

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

Note **Remarque**

Il existe un symlink pour chacun de ces répertoires de périphériques dans le répertoire `/proc/ide/`.

Chaque répertoire de périphérique contient un recueil d'informations et de statistiques. Le contenu de ces répertoires varient selon le type de périphérique connecté. Parmi les fichiers les plus utiles communs à beaucoup de périphériques se trouvent :

- `cache` — Cache du périphérique.
- `capacity` — Capacité du périphérique, en blocs de 512 octets.
- `driver` — Pilote et version utilisés pour contrôler le périphérique.
- `geometry` — Géométrie physique et logique du périphérique.
- `media` — Type de périphérique, tel que `disk`.
- `model` — Nom ou numéro de modèle du périphérique.
- `settings` — Ensemble de paramètres courants du périphérique. Ce fichier contient normalement pas mal d'informations techniques utiles. Voici un exemple de fichier `settings` pour un disque dur IDE standard :

```
name                 value          min          max          mode
----                 -----          ---          ---          ----
bios_cyl             784            0            65535        rw
bios_head            255            0            255          rw
bios_sect            63             0            63           rw
breada_readahead     4              0            127          rw
bswap                0              0            1            r
current_speed        66             0            69           rw
file_readahead       0              0            2097151      rw
ide_scsi             0              0            1            rw
init_speed           66             0            69           rw
io_32bit             0              0            3            rw
keepsettings         0              0            1            rw
lun                  0              0            7            rw
max_kb_per_request   64             1            127          rw
multcount            8              0            8            rw
nice1                1              0            1            rw
nowerr               0              0            1            rw
number               0              0            3            rw
pio_mode             write-only     0            255          w
slow                 0              0            1            rw
unmaskirq            0              0            1            rw
using_dma            1              0            1            rw
```

/proc/irq

Ce répertoire est utilisé pour régler l'affinité IRQ-CPU, qui permet de connecter un IRQ particulier à une seule unité centrale. Ou bien, vous pouvez empêcher qu'une unité centrale traite les IRQ.

Chaque IRQ a son propre répertoire, ce qui permet à chaque IRQ d'être configuré différemment par rapport aux autres. 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 d'IRQ. Les valeurs dans `smp_affinity` spécifient quelles unités centrales traitent cet IRQ spécifique.

Vous trouverez plus de renseignements dans le fichier `/usr/src/linux-2.4/Documentation/filesystems/proc.txt`.

/proc/net

Ce répertoire fournit une vision exhaustive de nombreux paramètres réseau et des statistiques. Chaque fichier couvre une gamme spécifique d'informations relatives au réseau sur le système :

- `arp` — Contient la table ARP du noyau. Ce fichier est particulièrement utile pour connecter une adresse de matériel à une adresse IP sur un système.
- `atm` — Répertoire qui contient des fichiers avec divers réglages et statistiques sur les *modes de transfert asynchrone* (ATM). Ce répertoire est surtout utilisé avec le réseautage ATM et les cartes ADSL.
- `dev` — Fournit la liste des divers périphériques réseau configurés sur le système. Ce fichier vous indique rapidement le nombre d'octets envoyés et reçus par chaque interface, le nombre de paquets entrants et sortants, le nombre d'erreurs trouvées, le nombre de paquets perdus, etc.
- `dev_mcast` — Affiche les différents groupes de multidiffusion Layer2 qu'écoute chaque périphérique.
- `igmp` — Fournit la liste des adresses IP de multidiffusion auxquelles s'est joint le système.
- `ip_fwchains` — Indique toute chaîne de pare-feu actuelle.
- `ip_fwnames` — Si toutes les `ipchains` sont en fonction, ce fichier virtuel liste tous les noms de chaîne de pare-feux.
- `ip_masquerade` — Table d'informations de masquerading.
- `ip_mr_cache` — Liste de la cache du routeur de diffusion.
- `ip_mr_vif` — Liste des interfaces virtuelles de diffusion.
- `netstat` — Contient un ensemble vaste, mais détaillé, de statistiques réseau, telles que les temps morts TCP, les cookies SYN envoyés et reçus, etc.
- `psched` — Liste des paramètres du programme d'ordonnancement global des paquets.
- `raw` — Liste de statistiques brutes sur les périphériques.
- `route` — Table de routage du noyau.
- `rt_cache` — Cache de routage actuelle.
- `snmp` — Liste de données du protocole SNMP pour différents protocoles réseau utilisés.
- `sockstat` — Statistiques sur les prises (sockets).
- `tcp` — Informations détaillées sur les prises TCP.
- `tr_rif` — Table de routage RIF en anneau à jeton.
- `udp` — Informations détaillées sur les prises UDP.
- `unix` — Liste des prises de domaine UNIX actuellement utilisées.
- `wireless` — Liste des données d'interface sans fil.

/proc/scsi

Tout comme le répertoire `/proc/ide` n'existe que si un contrôleur IDE est connecté au système, le répertoire `/proc/scsi` n'est disponible que si vous avez une carte hôte d'interface pour petits systèmes informatiques (SCSI).

Le fichier principal est `/proc/scsi/scsi`, qui contient une liste de tous les périphériques SCSI reconnus. Exemple : si un système a un lecteur de CD-ROM SCSI, une unité de bande, des disques durs et un contrôleur RAID SCSI, ce fichier ressemblera à ceci :

```
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
```

Cette liste fournit également le type de périphérique, de même que le nom de modèle, le fabricant et le canal/ID SCSI.

En outre, 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. Donc, dans le cas de l'exemple ci-dessus, les répertoires `aic7xxx` et `megaraid` sont présents car ces deux pilotes sont utilisés. Les fichiers dans chacun des répertoires contient l'éventail d'adresses E/S, les IRQ et des statistiques sur le contrôleur SCSI qui utilise le pilote. Bien que chaque contrôleur rapporte différents types (et quantités) d'information, la sortie de la plupart de ces fichiers vous sera très utile et facile à lire. Le fichier de la carte hôte SCSI Adaptec AIC-7880 Ultra, dans l'exemple, produit 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}

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       1     131       0       0       0
```

Cet écran vous permet de visualiser la vitesse de transfert des différents périphériques SCSI branchés 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 les périphériques. En examinant le fichier `/proc/scsi/scsi`, nous pouvons voir que ce contrôleur communique avec le lecteur de CD-ROM à une vitesse de 20 Mo par seconde, alors que la vitesse n'est que de 10 Mo par seconde dans le cas de l'unité de bande.

/proc/sys

Le répertoire `/proc/sys/` est spécial et différent des autres répertoires de `/proc` ; non seulement est-il rempli d'informations sur le système, il vous permet aussi d'effectuer des modifications à la configuration d'un noyau en cours d'exécution.

Avertissement **Attention**

N'essayez pas d'améliorer les paramètres de votre noyau sur un système de production à l'aide des différents fichiers du répertoire `/proc/sys`. Il arrive parfois que la modification d'un paramètre rende le noyau instable et nécessite le redémarrage du système.

Pour cette raison, avant de changer une valeur dans `/proc/sys`, assurez-vous de bien connaître les options valides de ce fichier et les résultats attendus.

Une bonne façon pour savoir si un fichier donné peut servir à configurer le noyau ou est conçu uniquement pour fournir de l'information consiste à en faire la liste. Si le fichier peut être écrit, vous pouvez alors l'utiliser pour configurer le noyau d'une certaine manière. Voici par exemple une liste partielle 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 cette liste, les fichiers `dir-notify-enable` et `file-max` peuvent être écrits et, par conséquent, peuvent être utilisés pour configurer le noyau. Les autres fichiers ne fournissent que des informations sur les paramètres actuels du noyau.

Pour changer une valeur dans un fichier `/proc/sys` il faut écrire la nouvelle valeur dans le fichier à l'aide de la commande echo. Par exemple, si vous souhaitez activer la touche d'appel système (System Request Key) sur un noyau en cours d'exécution, entrez la commande suivante :

```
[root@bleach /]# echo "1" > /proc/sys/kernel/sysrq
```

Cela aura pour effet de changer la valeur `sysrq` du fichier, qui passera de `0` (off) à `1` (on).

La touche d'appel système est conçue pour vous permettre d'indiquer au noyau d'exécuter certaines opérations importantes au moyen d'une simple combinaison de touches, telles que d'arrêter ou redémarrer le système, synchroniser tous les systèmes de fichiers montés ou mettre des informations importantes sur votre console. Cette fonction est utile lorsque vous utilisez un noyau de développement ou si vous avez des blocages de système. Pour en savoir plus sur la touche d'appel système, reportez-vous à `/usr/src/linux-2.4/Documentation/sysrq.txt`.

Quelques fichiers de configuration `/proc/sys` contiennent plus d'une valeur. Placez un caractère d'espacement entre chaque valeur passée à l'aide de la commande `echo`, afin d'envoyer correctement les nouvelles valeurs. Exemple :

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

Note **Remarque**

Toute modification de configuration effectuée à l'aide de la commande `echo` disparaît lorsque le système est redémarré. Pour faire en sorte que vos modifications soient appliquées au démarrage, reportez-vous à la la section intitulée *Utilisation de* `sysctl`.

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

/proc/sys/dev

Ce répertoire fournit des paramètres pour des périphériques particuliers sur le système. La plupart des systèmes ont au moins deux répertoires, soit `cdrom` et `raid`, mais les noyaux personnalisés peuvent en avoir d'autres, tels que `parport`, qui indique la capacité de partager un port parallèle entre plusieurs pilotes de périphérique.

Le répertoire `cdrom` contient un fichier appelé `info`, qui indique de nombreux paramètres de lecteur de CD-ROM importants :

```
CD-ROM information, Id: cdrom.c 3.12 2000/10/18

drive name:             hdc
drive speed:            32
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
```

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

De nombreux fichiers dans `/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 indiquer un `1` au bon fichier afin d'activer la fonction ou un `0` pour la désactiver.

Si la prise en charge RAID est compilée dans le noyau, un répertoire `/proc/sys/dev/raid` est disponible, qui contient au moins deux fichiers : `speed_limit_min` et `speed_limit_max`. Ces paramètres entrent en jeu de façon à ralentir ou accélérer la vitesse à laquelle le périphérique RAID est utilisé pour des tâches E/S particulièrement intensives, telles que la resynchronisation des disques.

/proc/sys/fs

Ce répertoire contient une gamme d'options et des informations concernant divers aspects des systèmes de fichiers : parts, indicateurs de fichier, dentry.

Le répertoire `binfmt_misc` est utilisé pour fournir au noyau la prise en charge pour des formats binaires variés.

Les fichiers importants dans `/proc/sys/fs` sont, notamment :

- `dentry-state` — Etat de la cache du répertoire. Le fichier ressemble à ceci :

```
57411   52939   45      0       0       0
```

Le premier nombre indique le nombre total d'entrées dans la 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 redemandé et le quatrième mesure les pages actuellement demandées par le système. Les deux derniers chiffres ne sont pas utilisés et affichent uniquement un zéro.

- `dquot-nr` — Nombre maximum d'entrées de parts de disque en cache.
- `file-max` — Vous permet de changer le nombre maximum d'indicateurs de fichier alloués par le noyau. Si vous augmentez la valeur dans ce fichier, vous pourrez résoudre des erreurs causées par le manque d'indicateurs de fichier disponibles.
- `file-nr` — Affiche, dans l'ordre, le nombre d'indicateurs de fichier alloués, utilisés et maximum.
- `overflowgid` et `overflowuid` — Définit l'ID groupe et l'ID utilisateur fixés, respectivement, pour l'utilisation 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 courant de superblocs utilisés.

/proc/sys/kernel

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

- `acct` — Contrôle la suspension de la comptabilisation de processus sur la base du pourcentage d'espace libre disponible sur le système de fichiers contenant le journal. Par défaut, ce fichier ressemble à ceci :

  ```
  4       2       30
  ```

  La deuxième valeur définit le seuil de pourcentage d'espace libre pour suspendre la journalisation, alors que la première valeur indique le pourcentage nécessaire pour reprendre la journalisation. La troisième valeur indique l'intervalle de temps en secondes entre les vérifications du système de fichier de la part du noyau pour savoir si la journalisation doit être suspendue ou reprise.
- `cap-bound` — Contrôle les réglages de *capability bounding*, qui fournit la liste des capacités que tout processus du système peut exécuter. Si une capacité n'est pas incluse dans cette liste, aucun processus, peu importe ses privilèges, ne peut l'exécuter. L'objectif de base est d'augmenter la sécurité du système en s'assurant que certaines choses ne peuvent se produire, du moins jusqu'à un certain point lors du processus de démarrage.

  Les nombreuses valeurs possibles dans ce cas vont au-delà des objectifs de ce manuel, veuillez alors consulter la documentation sur le noyau pour en savoir davantage.
- `ctrl-alt-del` — Contrôle si [Ctrl]-[Alt]-[Suppr] redémarre correctement l'ordinateur à l'aide d' `init` (valeur `0`) ou force un redémarrage immédiat sans synchroniser les tampons " sales " du disque (valeur `1`).
- `domainname` — Vous permet de configurer le nom de domaine du système, tel que `domain.com`.
- `hostname` — Vous permet de configurer le nom d'hôte du système, tel que `host.domain.com`.
- `hotplug` — Configure l'utilitaire à utiliser lorsqu'un changement de configuration est détecté par le système. Surtout utilisé avec USB et Cardbus PCI. La valeur par défaut de `/sbin/hotplug` ne devrait pas être modifiée, à moins que vous ne testiez un nouveau programme pour jouer ce rôle.
- `modprobe` — Définit l'emplacement du programme à utiliser pour charger des modules du noyau lorsque nécessaire. La valeur par défaut de `/sbin/modprobe` signifie que `kmod` l'appelle pour charger un module

lorsqu'un processus élémentaire du noyau appelle `kmod`.

- `msgmax` — Définit la taille maximum de tout message envoyé d'un processus à un autre ; la valeur par défaut est `8192` octets. Soyez prudent lorsque vous décidez d'augmenter cette valeur car les messages en file d'attente entre les processus sont stockés dans la mémoire non échangeable du noyau ; toute augmentation de `msgmax` augmente également la demande de mémoire vive pour le système.
- `msgmnb` — Définit le nombre maximum d'octets dans une file d'attente de messages. Par défaut, la valeur est `16384`.
- `msgmni` — Définit le nombre maximum d'identificateurs de file d'attente de messages. Par défaut, la valeur est `16`.
- `osrelease` — Numéro de version du noyau Linux. Ce fichier ne peut être modifié qu'en changeant la source du noyau et en recompilant.
- `ostype` — Type de système d'exploitation. Par défaut, ce fichier est paramétré sur `Linux` et cette valeur ne peut être modifiée qu'en changeant la source du noyau et en recompilant.
- `overflowgid` et `overflowuid` — Définit les ID groupe et utilisateur fixés, respectivement, pour l'utilisation avec des appels de système sur des architectures qui ne prennent en charge que des ID groupe et utilisateur 16 bits.
- `panic` — Définit le retardement en secondes effectué par le noyau pour le redémarrage du système lors d'une panique de noyau. Par défaut, la valeur est réglée sur `0`, ce qui désactive le redémarrage automatique après une panique.
- `printk` — Ce fichier contrôle toute une série de paramètres relatifs à l'affichage ou 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 de niveau journal se subdivisent dans l'ordre suivant :

  - `0` — Urgence noyau. Le système est inutilisable.
  - `1` — Alerte noyau. Il faut agir immédiatement.
  - `2` — Les conditions du noyaux sont considérées comme critiques.
  - `3` — Condition d'erreur du noyau générale.
  - `4` — Condition d'avertissement du noyau générale.
  - `5` — Avis du noyau d'une condition normale, mais importante.
  - `6` — Message d'information du noyau.
  - `7` — Messages de niveau débogage du noyau.

  Quatre valeurs se trouvent dans le fichier `printk` :

```
6       4       1       7
```

  Chacune de ces valeurs définit une règle différente pour traiter les messages d'erreur. La première valeur, appelée *niveau journal de la console*, spécifie la plus basse priorité de message qui sera affichée sur la console (notez que plus la priorité est basse, plus le numéro de 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.
- `rtsig-max` — Configure le nombre maximum de signaux POSIX en temps réel que le système peut avoir en file d'attente simultanément. La valeur par défaut est `1024`.
- `rtsig-nr` — Le nombre courant de signaux POSIX en temps réel mis en file d'attente par le noyau.
- `sem` — Ce fichier configure les paramètres de sémaphores dans le noyau. Un *sémaphore* est un objet IPC System V utilisé pour contrôler l'utilisation d'un processus spécifique.
- `shmall` — Définit la quantité totale de mémoire partagée qui peut être utilisée à un moment précis sur le système, en octets. Par défaut, cette valeur est `2097152`.
- `shmmax` — Définit la plus grande taille d'un segment de mémoire partagée autorisée par le noyau, en octets. Par

défaut, cette valeur est `33554432`. Toutefois, le noyau prend 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 `4096`.
- `sysrq` — Active la touche d'appel système si cette valeur est réglée sur autre chose que la valeur par défaut, qui est `0`.
- `threads-max` — Définit le nombre maximum de processus élémentaires (threads) devant être utilisés par le le noyau. La valeur par défaut est `4095`.
- `version` — Affiche la date et l'heure de la dernière compilation du noyau. Le premier champ dans ce fichier, tel que `#3`, fait référence au nombre de fois que le noyau a été construit à partir de la source.

Le répertoire `random` stocke un certain nombre de valeurs relatives à la génération de numéros aléatoires pour le noyau.

/proc/sys/net

Ce répertoire contient des répertoires variés relatifs à des éléments réseau, tels que des protocoles et des centres d'accentuation. Diverses configurations lors de la compilation du noyau déterminent la présence ou non de différents répertoires à cet endroit, tels que `appletalk`, `ethernet`, `ipv4`, `ipx` et `ipv6`. Dans ces répertoires, vous pouvez ajuster les diverses valeurs réseau pour la configuration en question sur un système en cours d'exécution.

Vu la grande variété d'options réseau possibles et disponibles sous Linux et la grande quantité d'espace nécessaire pour en parler, nous ne couvrirons que les répertoires `/proc/sys/net` les plus communs.

Le répertoire `core` contient une série de paramètres qui contrôlent l'interaction entre le noyau et les couches réseau. Ses fichiers les plus importants sont :

- `message_burst` — Dixièmes de seconde nécessaires pour écrire un nouveau message d'avertissement. Cela est utilisé pour prévenir les attaques de refus de service (DoS). La valeur par défaut est `50`.
- `message_cost` — Aussi utilisé pour prévenir les attaques de refus de service, en plaçant un " coût " sur chaque message d'avertissement. Plus la valeur de ce fichier est élevée (`5` par défaut), plus il est probable que le message d'avertissement soit ignoré.

  L'idée de base est qu'une personne puisse faire une attaque en bombardant votre système de requêtes qui génèrent des erreurs et remplissent vos journaux ou nécessitent toutes les ressources de votre système pour gérer la journalisation des erreurs. Les paramètres dans `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 autorisés à 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 `300`.
- `optmem_max` — Configure la taille maximum des tampons auxiliaires autorisée par prise (socket).
- `rmem_default` — Définit la taille par défaut en octets du tampon 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.

Vu la grande utilisation de réseaux IP avec Linux, un coup d'oeil aux fichiers les plus importants dans `ipv4` permet de découvrir des paramètres réseau additionnels puissants. Nombre de ces paramètres, utilisés de concert avec d'autres, sont très utiles pour prévenir des attaques contre votre système.

Attention **Avertissement**

Une modification erronée pourrait avoir un effet néfaste sur la connectivité à distance de votre système.

Voici quelques-uns des fichiers les plus importants du répertoire `ipv4` :

- `icmp_destunreach_rate`, `icmp_echoreply_rate`, `icmp_paramprob_rate` et `icmp_timeexeed_rate` — Pour définir le délai maximum d'envoi de paquets ICMP, en centièmes de seconde sur les systèmes Intel, aux hôtes sous différentes conditions. La valeur `0` élimine tout délai, ce qui n'est pas une bonne idée.
- `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 des adresses de diffusion ou de multidiffusion, respectivement. Une valeur de `0` permet au noyau de répondre, alors qu'une valeur de `1` lui fait ignorer les paquets.
- `ip_default_ttl` — Définit la *durée de vie* (TTL), 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 aux autres interfaces. Par défaut, ce fichier est paramétré sur `0` pour désactiver le réacheminement, mais si vous paramétrez ce fichier sur `1`, le réacheminement sera activé.
- `ip_local_port_range` — Spécifie l'éventail de ports à utiliser par TCP ou UDP lorsqu'un port local est requis. Le premier nombre est le port le plus bas à utiliser et le second est le port le plus élevé. Pour tout système pour lequel on prévoit avoir besoin de plus de ports que ceux de l'éventail paramétré par défaut (1024 à 4999), il est conseillé d'utiliser un éventail de 32768 à 61000 dans ce fichier.
- `tcp_syn_retries` — Fournit une limite du nombre de fois que votre système retransmet un paquet SYN lorsqu'il essaie d'effectuer une connexion.
- `tcp_retries1` — Définit le nombre de retransmissions permises, essayant de répondre à une connexion entrante. La valeur par défaut est `3`.
- `tcp_retries2` — Définit le nombre de retransmissions permises de paquets TCP. La valeur par défaut est `15`.

Si vous désirez obtenir une liste complète des fichiers et options disponibles, consultez `/usr/src/linux-2.4/Documentation/networking/ip-sysctl.txt`.

De nombreux autres répertoires existent dans le répertoire `/proc/sys/net/ipv4` et couvrent des sujets spécifiques. Le répertoire `conf` permet de configurer chaque interface du système de façon différente, ainsi que d'utiliser des paramètres par défaut pour des périphériques non configurés (dans le sous-répertoire `default`) et des paramètres qui écrasent toutes les configurations spéciales (dans le sous-répertoire `all`).

De façon à contrôler les connexions entre voisins directs, soit d'autres systèmes connectés directement à votre système, le répertoire `neigh` permet des configurations spéciales pour chaque interface. Cela vous permet de traiter différemment les systèmes auxquels vous vous fiez davantage en raison de leur proximité relative à votre système tout en vous laissant établir des règles strictes pour les systèmes qui se trouvent à plusieurs sauts de distance.

Le routage via IPV4 a aussi son propre répertoire, soit `route`. Contrairement à `conf` et `neigh`, le répertoire `route` contient des spécifications qui s'applique au routage avec toutes les interfaces du système. Nombre de ces paramètres, tels que `max_size`, `max_delay` et `min_delay`, font référence au contrôle de la taille de la cache de routage. Pour libérer la cache de routage, spécifiez simplement une valeur quelconque dans le fichier `flush`.

Vous trouverez plus d'informations sur ces répertoires et les valeurs possibles pour leur configuration dans `/usr/src/linux-2.4/Documentation/filesystems/proc.txt`.

/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` :

- `bdflush` — Définit différentes valeurs relatives au démon noyau `bdflush`.
- `buffermem` — Vous permet de contrôler la quantité en pourcentage de la mémoire totale du système devant être utilisée comme mémoire tampon. Voici à quoi ressemble la sortie de ce fichier :

```
2       10       60
```

  La première et la dernière valeurs définissent le pourcentage minimum et maximum de mémoire à utiliser comme mémoire tampon. La valeur au milieu indique le pourcentage de mémoire du système dédiée à la mémoire tampon à partir duquel le sous-système de gestion de la mémoire commencera à libérer la cache tampon plus que les autres types de mémoire pour compenser le manque général de mémoire libre.
- `freepages` — Indique différentes valeurs relatives aux pages libres de la mémoire du système. Ce fichier ressemble à ceci :

```
512     768     1024
```

  La première valeur indique le nombre minimum de pages libres permises avant que le noyau ne prenne le contrôle de l'attribution de mémoire supplémentaire. La deuxième valeur indique le nombre de pages libres avant que le noyau ne commence à effectuer agressivement des échanges (swap) pour préserver les performances. La troisième valeur est le nombre de pages libres que le système essaie de maintenir en tout temps.
- `kswapd` — Définit différentes valeurs concernant le démon noyau de swap-out, `kswapd`. Ce fichier contient trois valeurs :

```
512     32      8
```

  La première valeur indique le nombre maximum de pages que `kswapd` essaie de libérer en une seule tentative. Plus cette valeur est élevé, plus le noyau peut agir rapidement pour libérer des pages. La deuxième valeur définit le nombre de fois minimum que `kswapd` essaie de libérer une page. La troisième valeur indique le nombre de pages que `kswapd` essaie d'écrire en une tentative. Le bon réglage de la valeur finale permet d'améliorer les performances de systèmes qui utilisent beaucoup d'espace swap en leur indiquant d'écrire les pages en gros blocs, ce qui minimise le nombre de recherches de disque.
- `max_map_count` — Configure le nombre maximum de régions de topographie mémoire qu'un processus peut avoir. Dans la plupart des cas, la valeur par défaut, `65536`, est adéquate.
- `overcommit_memory` — Contient une valeur qui, lorsqu'elle est paramétré sur autre chose que la valeur par défaut `0`, permet au noyau de sauter une vérification standard pour s'assurer qu'il y a suffisamment de mémoire avant d'en attribuer.
- `pagecache` — Contrôle la quantité de mémoire utilisée par la cache de pages. Les valeurs dans `pagecache` sont exprimées en pourcentage et fonctionnent de façon semblable à `buffermem` pour appliquer des valeurs minimum et maximum de mémoire de cache de pages disponible.

- `page-cluster` — Définit le nombre de pages lues en une tentative. La valeur par défaut est 4, ce qui signifie en fait 16 pages ; cette valeur est adéquate pour la plupart des systèmes.
- `pagetable_cache` — Contrôle le nombre de tables de pages mises en cache par processeur. La première et la deuxième valeurs font référence aux nombres minimum et maximum de tables de pages à mettre de côté.

Des informations supplémentaires sur ces fichiers se trouvent dans `/usr/src/linux-2.4/Documentation/sysctl/vm.txt`.

/proc/sysvipc

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

/proc/tty

Ce répertoire contient des informations sur les périphériques tty disponibles et 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 périphérique tty. Les *périphériques série* sont utilisés avec les connexions série, telles que via modem ou câble série. Les *terminaux virtuels* créent la connexion console commune, telle que les consoles virtuelles disponibles lorsque vous appuyez sur [Alt]-[<F>] à la console système. Les *pseudo-terminaux* créent une communication à double sens utilisée par les applications de niveau supérieur, telles que **X11**.

Le fichier `drivers` est une liste des périphériques tty actuellement utilisés :

```
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` donne la liste des statistiques d'utilisation et le statut de chaque ligne tty série.

Pour que les périphériques tty puissent être utilisés de façon semblable aux périphériques réseau, le noyau Linux applique une *discipline de ligne* sur les périphériques. Cela permet au pilote de placer un type spécifique d'en-tête avec 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 une chaîne de blocs de données. SLIP et PPP sont des disciplines de ligne courantes et sont communément utilisées pour connecter des systèmes via un lien série.

Les disciplines de ligne enregistrées sont stockées dans le fichier `ldiscs` et des informations détaillées sont disponibles

dans le répertoire `ldisc`.

Précédent
Les fichiers du niveau supérieur dans `/proc`

Sommaire
Niveau supérieur

Suivant
Utilisation de `sysctl`

Utilisation de sysctl

La commande sysctl peut faciliter radicalement la visualisation, le réglage et l'automatisation spéciale de paramètres du noyau.

Pour avoir un aperçu rapide de tous les paramètres configurables dans le répertoire /proc/sys, entrez la commande sysctl -a en tant que super-utilisateur. Vous obtiendrez ainsi une longue liste exhaustive ; en voici un court extrait :

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

Il s'agit des mêmes informations de base que vous verriez si vous visualisiez chaque fichier individuellement. La seule différence est l'emplacement du fichier. /proc/sys/net/ipv4/route/min_delay est signifié par net.ipv4.route.min_delay, où les barres obliques de répertoire sont remplacées par des points et la portion proc.sys est supposée.

On peut utiliser la commande sysctl au lieu d'echo pour assigner des valeurs à des fichiers modifiables dans le répertoire /proc/sys/. Par exemple, au lieu d'utiliser cette commande :

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

Vous pouvez utiliser la commande sysctl :

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

Le réglage rapide de valeurs individuelles comme celle-ci dans /proc/sys est pratique durant des essais, mais ne fonctionne pas aussi bien sur un système de production car tous les réglages spéciaux /proc/sys sont perdus lorsque le système est redémarré. Pour préserver les réglages qui vous plaisent et faire en sorte qu'ils soient permanents pour le noyau, ajoutez-les au fichier /etc/sysctl.conf.

Chaque fois que le système démarre, le script `/etc/rc.d/rc.sysinit` est exécuté par `init`. Ce script contient une commande pour exécuter `sysctl` utilisant `/etc/sysctl.conf` en tant que valeur à utiliser. Par conséquent, toute valeur ajoutée à `/etc/sysctl.conf` sera appliquée dès que le système aura terminé de démarrer.

Précédent | Sommaire | Suivant
Répertoires dans `/proc` | Niveau supérieur | Autres ressources

Autres ressources

Ci-dessous sont présentées des sources d'informations supplémentaires sur `/proc`.

Documentation installée

Vous trouverez probablement l'essentiel de la documentation sur `/proc` dans votre système.

- `/usr/src/linux-2.4/Documentation/filesystems/proc.txt` — Informations variées, mais limitées, sur tous les aspects de `/proc`.
- `/usr/src/linux-2.4/Documentation/sysrq.txt` — Aperçu des options pour la touche d'appel système.
- `/usr/src/linux-2.4/Documentation/sysctl` — Répertoire contenant de nombreux conseils `sysctl`, notamment sur la modification de valeurs relatives au noyau (`kernel.txt`), l'accès aux systèmes de fichiers (`fs.txt`) et l'utilisation de la mémoire virtuelle (`vm.txt`).
- `/usr/src/linux-2.4/Documentation/networking/ip-sysctl.txt` — Aperçu de nombreuses options de réseau IP et leur signification pour le noyau.
- L'information qui fait le plus autorité sur `/proc` est probablement celle que vous trouverez en lisant le code source du noyau. Assurez-vous que le paquetage RPM `kernel-source` est installé sur votre système et jetez un coup d'oeil dans le répertoire `/usr/src/linux-2.4` pour trouver la source.

Sites Web utiles

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

Chapitre 3. Processus de démarrage, Init et arrêt

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

Note **Remarque**

Ce chapitre se concentre sur LILO, le chargeur de démarrage par défaut de Red Hat Linux 7.1 et versions précédentes. Toutefois, Red Hat Linux 7.3 contient un autre chargeur de démarrage, GRUB, qui est expliqué plus en détail dans le Chapitre 4. Pour plus d'informations sur GRUB, consultez le Chapitre 4.

Introduction

Une des caractéristiques les plus importantes de Red Hat Linux concerne sa méthode ouverte de démarrer et d'arrêter le système d'exploitation ; il charge des programmes spécifiques et utilise leur configuration particulière, permet de changer ces configurations afin de contrôler le processus de démarrage et arrête le tout de façon gracieuse et organisée.

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

Dans les coulisses du processus de démarrage

Note **Remarque**

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

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

Le BIOS teste le système, recherche et vérifie les périphériques et recherche ensuite une unité qui sera utilisée pour amorcer le système. Normalement, il vérifie le lecteur de disquette (ou le lecteur de CD-ROM sur de nombreux ordinateurs plus récents) afin de trouver un support amorçable, s'il y en a un, puis se tourne vers le disque dur. L'ordre des unités utilisées pour le démarrage est généralement contrôlé par une configuration particulière du BIOS sur le système. Après avoir installé Red Hat Linux sur le disque dur de l'ordinateur, le BIOS cherche un *bloc de démarrage maître* (MBR) en commençant par le premier secteur du premier disque dur, charge son contenu dans la mémoire et lui donne le contrôle.

Ce chargeur de démarrage maître contient les instructions sur la façon de charger *GRUB* ou *LILO* (*LI*nux *LO*ader), en fonction du chargeur de démarrage installé. Le MBR charge le chargeur de démarrage, qui prend alors la relève (si le chargeur de démarrage est installé dans le MBR). Dans la configuration par défaut de Red Hat Linux, GRUB ou LILO utilise les paramètres dans le MBR pour afficher les options de démarrage et permet à l'utilisateur de spécifier quel système d'exploitation doit être lancé.

Cela entraîne la question suivante : "Comment le chargeur de démarrage fait-il dans le MBR pour savoir ce qu'il faut faire lorsque le MBR est lu ?". Les instructions pour LILO sont en fait déjà écrites à cet endroit par l'entremise de `lilo` et du fichier de configuration `/etc/lilo.conf`. Même les instructions pour GRUB sont écrites dans le fichier de configuration `/boot/grub/grub.conf`. Pour plus d'informations sur GRUB, consultez le Chapitre 4.

Options dans `/etc/lilo.conf`

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

Avertissement

Avertissement

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

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

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
prompt
timeout=50
message=/boot/message
lba32
default=linux

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

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

Cet exemple montre un système qui est configuré pour amorcer deux systèmes d'exploitation : Red Hat

Linux et DOS. Voici plus de détails sur certaines des lignes de ce fichier (votre fichier `/etc/lilo.conf` pourrait être légèrement différent) :

- `boot=/dev/hda` indique à LILO de regarder sur le premier disque dur du premier contrôleur IDE.
- `map=/boot/map` localise le fichier map. Pour une utilisation normale, ce nom ne devrait pas être modifié.
- `install=/boot/boot.b` indique à LILO d'installer le fichier spécifié en tant que nouveau secteur de démarrage. Pour une utilisation normale, cela ne devrait pas être modifié. Si la ligne `install` manque, LILO prendra par défaut `/boot/boot.b` en tant que fichier à utiliser.
- L'existence de `prompt` indique à LILO de vous afficher tout ce qui est défini dans la ligne `message`. Bien qu'il ne soit pas recommandé d'éliminer la ligne `prompt`, si vous le faites, vous pourrez tout de même obtenir une invite en appuyant sur la touche [Maj] pendant que votre ordinateur commence l'amorçage.
- `timeout=50` définit combien de temps LILO doit attendre que l'utilisateur entre une commande avant d'amorcer la ligne d'entrée `default`. Cette période de temps est mesurée en dixièmes de seconde et est réglée sur 50 par défaut.
- `message=/boot/message` se réfère à l'écran que LILO affiche pour vous laisser sélectionner le système d'exploitation ou le noyau à amorcer.
- `lba32` décrit la géométrie du disque dur à LILO. Une autre ligne commune que l'on retrouve à cet endroit est `linear`. Vous ne devriez pas changer cette ligne à moins d'être sûr de ce que vous faites. Autrement, vous pourriez mettre votre ordinateur dans un état où il lui est impossible d'être redémarré.
- `default=linux` se réfère au système d'exploitation par défaut que LILO doit amorcer au moyen des options énumérées sous cette ligne. Le nom `linux` fait référence à la ligne `label` située sous chacune des options de démarrage.
- `image=/boot/vmlinuz-2.4.0-0.43.6` spécifie le noyau Linux à amorcer au moyen de cette option.
- `label=linux` donne le nom de l'option du système d'exploitation sur l'écran LILO. Dans ce cas, il s'agit également du nom auquel fait référence la ligne `default`.
- `initrd=/boot/initrd-2.4.0-0.43.6.img` se réfère à l'image *disque RAM initial* qui est utilisée lors du démarrage pour initialiser et lancer les périphériques qui font en sorte qu'il est possible d'amorcer le noyau. Le disque RAM initial est un ensemble de pilotes nécessaires au fonctionnement de l'unité de disque dur et tout ce qui sert à charger le noyau. Vous ne devriez jamais essayer de partager des disques RAM initiaux entre différents ordinateurs à moins que la configuration de leur matériel ne soit identique (et même dans ce cas, c'est une bien mauvaise idée).
- `read-only` spécifie que la partition racine (voir la ligne `root` en-dessous) ne peut être modifiée ; elle ne peut qu'être lue.
- `root=/dev/hda5` indique à LILO quelle partition de disque utiliser en tant que partition root.

LILO affiche ensuite l'écran Red Hat Linux initial sur lequel apparaissent les systèmes d'exploitation ou les noyaux qui, selon la configuration choisie, doivent être amorcés. Si vous n'avez installé que Red Hat

Linux et n'avez rien changé dans `/etc/lilo.conf`, vous ne verrez que l'option **linux**. Si vous installez le support du noyau SMP, vous verrez l'option **linux-up**. Si vous avez configuré LILO de façon à ce qu'il amorce également d'autres systèmes d'exploitation, cet écran vous donnera la possibilité de choisir quel système amorcer. Utilisez les flèches de direction pour choisir le système d'exploitation désiré et appuyez sur [Entrée]

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

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

Avertissement **Avertissement**

Ne supprimez le répertoire `/initrd/` sous aucun prétexte. Le retirer empêcherait votre système de démarrer, avec un message d'erreur panique noyau.

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

Init

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

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

Ensuite, `init` exécute le script `/etc/inittab`, qui décrit comment le système doit être configuré dans chaque *niveau d'exécution* et définit le niveau d'exécution par défaut. (Voir la [la section intitulée]

Niveaux d'exécution d'Init pour avoir plus de détails sur les niveaux d'exécution d'init.) Ce fichier établit notamment que `/sbin/update` doit être exécuté chaque fois qu'un niveau d'exécution commence. Le programme `update` sert à recopier périodiquement les tampons mémoire vers les disques.

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

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

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

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

```
K01pppoe -> ../init.d/pppoe
K05innd -> ../init.d/innd
K10ntpd -> ../init.d/ntpd
K15httpd -> ../init.d/httpd
K15mysqld -> ../init.d/mysqld
K15pvmd -> ../init.d/pvmd
K16rarpd -> ../init.d/rarpd
K20bootparamd -> ../init.d/bootparamd
K20nfs -> ../init.d/nfs
K20rstatd -> ../init.d/rstatd
K20rusersd -> ../init.d/rusersd
K20rwalld -> ../init.d/rwalld
K20rwhod -> ../init.d/rwhod
K25squid -> ../init.d/squid
K28amd -> ../init.d/amd
K30mcserv -> ../init.d/mcserv
K34yppasswdd -> ../init.d/yppasswdd
K35dhcpd -> ../init.d/dhcpd
K35smb -> ../init.d/smb
K35vncserver -> ../init.d/vncserver
K45arpwatch -> ../init.d/arpwatch
K45named -> ../init.d/named
K50snmpd -> ../init.d/snmpd
K54pxe -> ../init.d/pxe
K55routed -> ../init.d/routed
K60mars-nwe -> ../init.d/mars-nwe
K61ldap -> ../init.d/ldap
K65kadmin -> ../init.d/kadmin
K65kprop -> ../init.d/kprop
K65krb524 -> ../init.d/krb524
K65krb5kdc -> ../init.d/krb5kdc
K75gated -> ../init.d/gated
K80nscd -> ../init.d/nscd
K84ypserv -> ../init.d/ypserv
K90ups -> ../init.d/ups
K96irda -> ../init.d/irda
S05kudzu -> ../init.d/kudzu
S06reconfig -> ../init.d/reconfig
S08ipchains -> ../init.d/ipchains
S10network -> ../init.d/network
S12syslog -> ../init.d/syslog
S13portmap -> ../init.d/portmap
S14nfslock -> ../init.d/nfslock
```

```
S18autofs -> ../init.d/autofs
S20random -> ../init.d/random
S25netfs -> ../init.d/netfs
S26apmd -> ../init.d/apmd
S35identd -> ../init.d/identd
S40atd -> ../init.d/atd
S45pcmcia -> ../init.d/pcmcia
S55sshd -> ../init.d/sshd
S56rawdevices -> ../init.d/rawdevices
S56xinetd -> ../init.d/xinetd
S60lpd -> ../init.d/lpd
S75keytable -> ../init.d/keytable
S80isdn -> ../init.d/isdn
S80sendmail -> ../init.d/sendmail
S85gpm -> ../init.d/gpm
S90canna -> ../init.d/canna
S90crond -> ../init.d/crond
S90FreeWnn -> ../init.d/FreeWnn
S90xfs -> ../init.d/xfs
S95anacron -> ../init.d/anacron
S97rhnsd -> ../init.d/rhnsd
S99local -> ../rc.local
```

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

Lorsqu'`init` a parcouru tous les niveaux d'exécution, le script `/etc/inittab` lance un processus `getty` pour chaque console virtuelle (invites de connexion) et pour chaque niveau d'exécution (les niveaux d'exécution 2 à 5 obtiennent les six consoles, alors que le niveau d'exécution 1, qui est un mode mono-utilisateur, n'en obtient qu'une ; les niveaux 0 et 6 n'obtiennent aucune console virtuelle). Fondamentalement, `getty` ouvre des lignes pour terminaux *tty* [1], règle leurs modes, imprime l'invite de login, prend le nom d'utilisateur, puis commence un processus de login pour l'utilisateur concerné. Cela permet aux utilisateurs de s'authentifier dans le système et de commencer à l'utiliser.

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

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

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

SysV Init

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

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

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

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

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

- Le noyau recherche `init` dans le répertoire `/sbin`.

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

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

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

Dans cet exemple, le niveau d'exécution par défaut est 3, soit le chiffre qui suit le premier deux-points. Si vous désirez le changer, vous pouvez modifier manuellement `/etc/inittab`. Soyez très prudent lorsque vous apportez des changements au fichier `inittab`.

Si vous utilisez LILO comme chargeur de démarrage, vous pouvez réparer le fichier `inittab`. Pour ce faire, redémarrez le système, accédez à l'invite `boot:` à l'aide de [Ctrl]-[X] et tapez :

```
boot:  linux single
```

Si vous utilisez le chargeur de démarrage GRUB, vous pouvez réparer le fichier `inittab` en suivant la procédure ci-dessous

- Dans l'écran graphique de GRUB, sélectionnez l'étiquette de démarrage **Red Hat Linux** et appuyez sur [e] pour la modifier.
- Descendez jusqu'à la ligne du noyau et appuyez sur [e] pour la modifier.
- A l'invite, entrez `single` et appuyez sur [Entrée].
- Vous retournerez à l'écran de GRUB contenant les informations sur le noyau. Appuyez sur la touche [b] pour démarrer le système en mode mono-utilisateur.

Tuyau **Astuce**

Il est aussi possible de changer le niveau d'exécution au démarrage avec GRUB en utilisant la même méthode que ci-dessus, sauf en remplaçant `single` avec, par exemple, `3` ou `5`. Le reste des étapes reste intégralement comme ci-dessus.

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

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

Notes

[1] Consultez la section intitulée *`/proc/tty`* dans Chapitre 2 pour des informations supplémentaires sur les périphériques `tty`.

Précédent
Processus de démarrage, Init et arrêt

Sommaire
Niveau supérieur

Suivant
Information Sysconfig

Information Sysconfig

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

Fichiers dans `/etc/sysconfig`

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

- `amd`
- `apmd`
- `arpwatch`
- `authconfig`
- `cipe`
- `clock`
- `desktop`
- `firewall`
- `harddisks`
- `hwconf`
- `i18n`
- `init`
- `ipchains`
- `iptables`
- `irda`
- `keyboard`
- `kudzu`
- `mouse`
- `network`
- `pcmcia`
- `rawdevices`
- `sendmail`
- `soundcard`
- `ups`
- `vncservers`
- `xinetd`

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

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

/etc/sysconfig/amd

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

/etc/sysconfig/apmd

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

/etc/sysconfig/arpwatch

Le fichier `/etc/sysconfig/arpwatch` est utilisé pour transmettre des arguments au démon `arpwatch` au démarrage. Le démon `arpwatch` daemon entretient une table d'adresses Ethernet MAC et leurs parités d'adresses IP. Pour plus d' informations sur les paramètres que vous pouvez utiliser dans ce fichier, taper `man arpwatch`. Par défaut, ce fichier règle le propriétaire du processus `arpwatch` sur l'utilisateur `pcap`.

/etc/sysconfig/authconfig

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

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

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

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

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

/etc/sysconfig/clock

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

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

  - `GMT` — indique que l'horloge est réglée sur l'heure universelle (l'heure de Greenwich).
  - `ARC` — indique que le décalage de 42 ans de la console ARC est activé (pour les systèmes fondés sur Alpha seulement).

Actuellement, les valeurs correctes sont :

- `UTC=<valeur>`, où `<valeur>` est une des valeurs booléennes suivantes :

  - `true` — indique que l'horloge est réglée sur l'heure universelle. Toute autre valeur signifie qu'elle est réglée sur l'heure locale.
- `ARC=<valeur>`, où `<valeur>` est l'un des éléments suivants :

  - `true` — indique que le décalage de 42 ans de la console ARC est activé. Toute autre valeur indique que l'époque UNIX normale est supposée (uniquement pour les systèmes de type Alpha).

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

```
ZONE="Amerique/New York"
```

/etc/sysconfig/desktop

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

```
DESKTOP="GNOME"
```

/etc/sysconfig/dhcpd

Le fichier `/etc/sysconfig/dhcpd` est utilisé pour transmettre des arguments au démon `dhcpd` au démarrage. Le démon `dhcpd` met en oeuvre le "Dynamic Host Configuration Protocol" (DHCP) et le "Internet Bootstrap Protocol" (BOOTP). DHCP et BOOTP assignent des noms d'hôtes aux ordinateurs sur le réseau. Pour plus d'informations sur les paramètres que vous pouvez utiliser dans ce fichier, tapez `man dhcpd`.

/etc/sysconfig/firewall

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

/etc/sysconfig/gpm

Le fichier `/etc/sysconfig/gpm` est utilisé pour transmettre des arguments au démon `gpm` au démarrage. Le démon `gpm` est le serveur qui permet l'accélération de la souris et le collage par clic au milieu. Pour plus d'informations sur les paramètres que vous pouvez utiliser dans ce fichier, tapez `man gpm`. Par défaut, il règle le périphérique souris sur `/dev/mouse`.

/etc/sysconfig/harddisks

Le fichier `/etc/sysconfig/harddisks` vous permet de régler le(s) disque(s) dur(s). Vous pouvez également utiliser `/etc/sysconfig/hardiskhd[a-h]` pour configurer des disques spécifiques.

Avertissement **Avertissement**

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

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

- `USE_DMA=1`, où la valeur 1 active DMA. Toutefois, avec certaines combinaisons circuits/disque

dur, cette DMA pourrait entraîner une corruption de données. *Vérifiez la documentation concernant votre disque dur ou auprès du fabricant avant de l'activer.*

- `Multiple_IO=16`, où la valeur 16 autorise plusieurs secteurs par interruption d'entrée/sortie. Lorsqu'elle est activée, cette fonction réduit le temps de gestion du système d'exploitation de 30 à 50 %. *Utilisez-la avec prudence.*
- `EIDE_32BIT=3` active le support E/S (E)IDE 32-bits pour une carte d'interface.
- `LOOKAHEAD=1` active l'anticipation en lecture du lecteur.
- `EXTRA_PARAMS=` spécifie l'endroit où peuvent être ajoutés des paramètres supplémentaires.

/etc/sysconfig/hwconf

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

/etc/sysconfig/i18n

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

```
LANG="fr_FR"
```

/etc/sysconfig/identd

Le fichier `/etc/sysconfig/identd` est utilisé pour transmettre des arguments au démon `identd` au démarrage. Le démon `identd` le nom d'utilisateur des processus avec connexions TCP/IP ouvertes. Quelques-un des services sur le réseau, comme les serveurs FTP et IRC, causent des réponses lentes et de plaintes si `identd` n'est pas en fonction. Mais, en général, `identd` n'est pas un service indispensable, donc si la sécurité est critique, il ne faut pas le lancer. Pour plus d'informations sur les paramètres que vous pouvez utiliser dans ce fichier, tapez `man identd`. Par défaut, le fichier ne contient aucun paramètre.

/etc/sysconfig/init

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

Les valeurs suivantes peuvent être utilisées :

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

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

- RES_COL=<*valeur*>, où <*valeur*> est le numéro de la colonne de l'écran à laquelle commencer les étiquettes d'état. La valeur par défaut est 60.
- MOVE_TO_COL=<*valeur*>, où <*valeur*> déplace le curseur sur la valeur dans la ligne RES_COL. Indique, par défaut, une sortie de séquences ANSI par echo -e.
- SETCOLOR_SUCCESS=<*valeur*>, où <*valeur*> configure la couleur indiquant la réussite. Indique, par défaut, une sortie de séquences ANSI par echo -e, définissant la couleur sur vert.
- SETCOLOR_FAILURE=<*valeur*>, où <*valeur*> configure la couleur indiquant l'échec. Indique, par défaut, une sortie de séquences ANSI par echo -e, définissant la couleur sur rouge.
- SETCOLOR_WARNING=<*valeur*>, où <*valeur*> configure la couleur indiquant un avertissement. Indique, par défaut, une sortie de séquences ANSI par echo -e, définissant la couleur sur jaune.
- SETCOLOR_NORMAL=<*valeur*>, où <*valeur*> configure la couleur sur 'normal'. Indique, par défaut, une sortie de séquences ANSI par écho -e.
- LOGLEVEL=<*valeur*>, où <*valeur*> définit le niveau de connexion initial de la console pour le noyau. La valeur par défaut est 7 : 8 signifie tout (y compris le débogage) ; 1 ne signifie rien d'autre que les panics du noyau. syslogd écrasera ceci au démarrage.
- PROMPT=<*valeur*>, où <*valeur*> est une des valeurs booléennes suivantes :

    - yes — active le contrôle du mode interactif au clavier.
    - no — désactive le contrôle du mode interactif au clavier.

/etc/sysconfig/ipchains

Le fichier /etc/sysconfig/ipchains contient des informations utilisées par le noyau pour établir des règles ipchains concernant le filtrage des paquetages.

Pour modifier ce fichier, exécutez la commande service ipchains save lorsques des règles ipchains valides sont en place. Normalement vous ne devriez pas modifier ce fichier. Utilisez plutôt la commande ipchains pour configurer les règles de filtrage des paquets et ensuite enregistrez les règles dans ce fichier.

/etc/sysconfig/iptables

Comme `/etc/sysconfig/ipchains`, le fichier `/etc/sysconfig/iptables` stocke des informations utilisées par le noyau pour fournir des services spécialisés de filtrage des paquets. Toutefois, ce fichier est utilisé par `iptables` plutôt que par `ipchains`.

Vous ne devriez pas modifier ce fichier manuellement, à moins que vous ne connaissiez les méthodes utilisées pour construire les règles `iptables`. Ces règles sont écrites dans `/etc/sysconfig/iptables` par la commande `service iptables save`, qui stocke les règles `iptables` courantes en exécutant le programme `/sbin/iptables-save`. Ensuite, une fois que `iptables` a été redémarré, par exemple lorsque le système est démarré et que le programme `/sbin/iptables-restore` lit le fichier et rétablit les règles de filtrage des paquets.

`/etc/sysconfig/irda`

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

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

- `DEVICE=<`*`valeur`*`>`, où `<`*`valeur`*`>` est le périphérique (généralement le port série) qui gère les connexions à infrarouge.
- `DONGLE=<`*`valeur`*`>`, où `<`*`valeur`*`>` spécifie le type de clé électronique utilisée pour les communications par infrarouges. Ce paramètre existe pour les gens qui utilisent des clés électroniques série plutôt que de vrais ports infrarouges. Une clé électronique est un dispositif qui est branché à un port série traditionnel pour la communication par infrarouges. Cette ligne est, par défaut, réglée sur l'inactivité car les ordinateurs bloc-notes ayant de vrais ports infrarouges sont beaucoup plus fréquents que ceux qui ont des clés électroniques ajoutées.
- `DISCOVERY=<`*`valeur`*`>`, où `<`*`valeur`*`>` est une des valeurs booléennes suivantes :
  - `yes` — lance `irattach` en mode découverte, ce qui signifie qu'il cherche activement d'autres périphériques à infrarouge. Cette fonction doit être activée pour que l'ordinateur puisse chercher de façon active une connexion infrarouge (c'est-à-dire un élément qui ne prend pas l'initiative de connexion).
  - `no` — ne s'exécute pas en mode découverte.

/etc/sysconfig/keyboard

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

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

/etc/sysconfig/kudzu

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

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

/etc/sysconfig/mouse

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

- FULLNAME=<*valeur*>, où <*valeur*> se réfère au nom complet de la souris utilisée.
- MOUSETYPE=<*valeur*>, où <*valeur*> est l'un des éléments suivants :
  - microsoft — une souris Microsoft™.
  - mouseman — une souris MouseMan™.
  - mousesystems — une souris Systems™.
  - ps/2 — une souris PS/2.
  - msbm — une souris bus Microsoft™.
  - logibm — une souris bus Logitech™.
  - atibm — une souris bus ATI™.
  - logitech — une souris Logitech™.

  - `mmseries` — un ancien modèle de souris MouseMan™.
  - `mmhittab` — une souris mmhittab.

- `XEMU3=<valeur>`, où `<valeur>` est une des valeurs booléennes suivantes :

  - `yes` — la souris n'a que deux boutons, mais trois boutons de souris devraient être simulés.
  - `no` — la souris a déjà trois boutons.

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

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

/etc/sysconfig/named

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

Actuellement, seules les valeurs suivantes peuvent être utilisées:

- `ROOTDIR="</some/where>"`, où `</some/where>` se réfère au chemin complet du répertoire d'un environnement chroot configuré sous lequel `named` va fonctionner. Cet environnement chroot doit être au préalable configuré. Tapez `info chroot` pour plus d'informations sur la façon de faire.
- `OPTIONS="<value>"`, où `<value>` est toute option listée dans la page de manuel de `named`, excepté **`-t`**. Au lieu de **`-t`**, utilisez la ligne de commande `ROOTDIR` ci-dessus à la place.

Pour plus d'informations sur les paramètres que vous pouvez utiliser dans ce fichier, tapez `man named`. Pour des informations détaillées sur la façon de configurer un serveur BIND DNS, lisez le Chapitre 17. Par défaut, le fichier ne contient aucun paramètre.

/etc/sysconfig/netdump

`/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 envoie des surplus de mémoire sur le réseau. En général, `netdump` n'est pas un service indispensable, donc il ne faut le lancer que si vous en avez absolument besoin. Pour plus d'informations sur les paramètres que vous pouvez utiliser dans ce fichier,

tapez `man netdump`.

/etc/sysconfig/network

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

- `NETWORKING=<valeur>`, où `<valeur>` est une des valeurs booléennes suivantes :
  - `yes` — la connexion au réseau devrait être configurée.
  - `no` — la connexion au réseau ne devrait pas être configurée.
- `HOSTNAME=<valeur>`, où `<valeur>` devrait être un *nom de domaine complet*, tel que `hôte.domaine.com`, mais vous pouvez choisir le nom d'hôte que vous voulez.

  Note **Remarque**

  Pour assurer la compatibilité avec des logiciels plus anciens que certaines personnes risqueraient d'installer (tels que `trn`), le fichier `/etc/HOSTNAME` devrait contenir la même valeur qu'ici.
- `GATEWAY=<value>`, où `<value>` est l'adresse IP du périphérique de réseau.
- `GATEWAYDEV=<valeur>`, où `<valeur>` est le périphérique de passerelle, tel que `eth0`.
- `NISDOMAIN=<valeur>`, où `<valeur>` est le nom de domaine NIS.

/etc/sysconfig/ntpd

Le fichier `/etc/sysconfig/ntpd` est utilisé pour transmettre des arguments au démon `ntpd` au démarrage. Le démon `ntpd` régule et entretient l'horloge du système pour la synchroniser avec un serveur d'heure standard Internet. Il met en oeuvre la version 4 du "Network Time Protoco (NTP). Pour plus d'informations sur les paramètres que vous pouvez utiliser dans ce fichier, consultez la page suivante avec votre navigateur: `/usr/share/doc/ntp-<version>/ntpd.htm` (où <version> est le numéro de la version de `ntpd`). Par défaut, ce fichier règle le propriétaire du processus `ntpd` sur l'utilisateur `ntp`.

/etc/sysconfig/pcmcia

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

- `PCMCIA=<valeur>`, où `<valeur>` est un des éléments suivants :

  - `yes` — le support PCMCIA doit être activé.
  - `no` — le support PCMCIA ne doit pas être activé.

- `PCIC=<valeur>`, où `<valeur>` est un des éléments suivants :

  - `i82365` — l'ordinateur a un circuit de socket PCMCIA de type i82365.
  - `tcic` — l'ordinateur a un circuit de socket PCMCIA de type tcic.

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

/etc/sysconfig/radvd

Le fichier `/etc/sysconfig/radvd` est utilisé pour transmettre des arguments au démon `radvd` au démarrage. Le démon `radvd` écoute les requête de routeur et envoie des annonces de routeur pour le protocole IP version 6. Ce service permet aux hôtes d'un réseau de modifier dynamiquement leur routeur par défaut, sur la base de ces annonces de routeur. Pour plus d'informations sur les paramètres que vous pouvez utiliser dans ce fichier, tapez `man radvd`. Par défaut, ce fichier règle le propriétaire du processus `radvd` sur l'utilisateur `radvd`.

/etc/sysconfig/rawdevices

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

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

/etc/sysconfig/redhat-config-users

`/etc/sysconfig/redhat-config-users` est le fichier de configuration pour l'application graphique, **redhat-config-users**. Dans Red Hat Linux 7.3 ce fichier n'est utilisé que pour filtrer les utilisateurs du système. Pour plus d'informations sur l'emploi de cette application, voyez le chapitre *Utilisateur et Configuration de groupe (User and Group Configuration)* dans le *Guide de personnalisation officiel Red Hat Linux*.

/etc/sysconfig/samba

Le fichier /etc/sysconfig/samba est utilisé pour transmettre des arguments au démons smbd et nmbd au 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 plus d'informations sur les paramètres que vous pouvez utiliser dans ce fichier, tapez man smbd. Par défaut, ce fichier règle le fonctionnement desmbd et nmbd en mode démon.

/etc/sysconfig/sendmail

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

Les valeurs suivantes peuvent être utilisées :

- DAEMON=<*valeur*>, où <*valeur*> est une des valeurs booléennes suivantes :
  - yes — **Sendmail** doit être configuré pour contrôler le port 25 afin de détecter le courrier entrant. yes implique l'utilisation des options -bd de **Sendmail**.
  - no — **Sendmail** ne devrait pas être configuré pour contrôler le port 25 afin de détecter le courrier entrant.
- QUEUE=1h qui est donné à **Sendmail** en tant que -q$QUEUE. L'option -q n'est pas donnée à **Sendmail** si le fichier /etc/sysconfig/sendmail existe et que QUEUE est vide ou non défini.

/etc/sysconfig/soundcard

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

Il peut contenir ce qui suit :

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

/etc/sysconfig/squid

Le fichier /etc/sysconfig/squid est utilisé pour transmettre des arguments au démon squid au démarrage. Le démon squid est un serveur proxy de cache pour les applications clientes par le Web. Pour plus d'informations sur la configuration d'un serveur proxy squid ouvrez avec votre navigateur /usr/share/doc/squid-<*version*>/ directory (remplacez <*version*> avec le numéro de version squid installée sur votre système). Par défaut, ce fichier règle le démarrage premier de squid en mode démon et règle le délai avant auto-interruption.

/etc/sysconfig/tux

/etc/sysconfig/tux est le fichier de configuration de TUX, le serveur Web basé sur le noyau. Pour plus d'informations sur la configuration du serveur TUX server, ouvrez avec votre navigateur /usr/share/doc/tux-<*version*>/tux/index.html (remplacez <*version*> par le numéro de la version de TUX installée sur votre système). Les paramètres disponibles pour ce fichier sont listés dans /usr/share/doc/tux-<*version*>/tux/parameters.html.

/etc/sysconfig/ups

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

- SERVER=<*valeur*>, où <*valeur*> est un des éléments suivants :
  - yes — un dispositif UPS est branché à votre système.
  - no — aucun dispositif UPS n'est branché à votre système.
- MODEL=<*valeur*>, où <*valeur*> doit être un des éléments suivants ou doit être réglé sur NONE si aucun dispositif UPS n'est branché à votre système :
  - apcsmart — pour un périphérique SmartUPS™ APC ou semblable.
  - fentonups — pour un UPS Fenton™.
  - optiups — pour un dispositif UPS OPTI™.
  - bestups — pour un UPS Best Power™.
  - genericups — pour un UPS générique.
  - ups-trust425+625 — pour un UPS Trust™.
- DEVICE=<*valeur*>, où <*valeur*> spécifie où le dispositif UPS est branché, tel que

`/dev/ttyS0`.

- `OPTIONS=<valeur>`, où `<valeur>` est une commande spéciale qui doit être passée au dispositif UPS.

`/etc/sysconfig/vncservers`

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

Il peut contenir ce qui suit :

- `VNCSERVERS=<valeur>`, où `<valeur>` est réglé sur quelque chose qui ressemble à `"1:fred"`, pour indiquer qu'un serveur VNC devrait être démarré pour l'utilisateur fred sur l'écran :1. Avant de pourvoir se connecter au serveur VNC distant, l'utilisateur fred doit avoir configuré un mot de passe VNC utilisant `vncpasswd`.

Notez que lorsque vous utilisez un serveur VNC, la communication que vous établissez avec le serveur est chiffrée. Pour cela son utilisation sur un réseau peu sûr est déconseillée. Pour des instruction spécifiques concernant l'utilisation de SSH pour sécuriser la communication VNC, lisez les informations contenues dans le site http://www.uk.research.att.com/vnc/sshvnc.html. Pour plus d'informations concernant SSH, consultez le Chapitre 10 ou le *Guide de personnalisation officiel Red Hat Linux*.

`/etc/sysconfig/xinetd`

Le fichier `/etc/sysconfig/xinetd` est utilisé pour transmettre des arguments au démon `xinetd` au démarrage. Le démon `xinetd` lance des programmes qui fournissent des services Internet lorsqu'une requête est reçue pour le port de ce service. Pour plus d'informations sur les paramètres que vous pouvez utiliser dans ce fichier, tapez `man xinetd`. Pour plus d'informations sur le service `xinetd`, consultez la la section intitulée *Contrôle d'accès à l'aide de `xinetd`* dans Chapitre 9.

Les répertoires dans le répertoire `/etc/sysconfig/`

Les répertoires suivants se trouvent normalement dans `/etc/sysconfig/` avec une description basique de ce qu'ils contiennent :

- `apm-scripts` — Parmi ceux-ci se trouve le script Red Hat APM suspendre/reprendre. Il n'est

pas conseillé d'éditer directement ce fichier. Si vous devez l'adapter, il suffit de créer un fichier nommé `/etc/sysconfig/apm-scripts/apmcontinue` et il sera invoqué 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.
- `networking` — Ce répertoire est utilisé par l'utilitaire d'administration **Red Hat Network Administration Tool** et il n'est pas conseillé de l'éditer manuellement. Pour plus d'informations sur la configuration des interfaces grâce à **Red Hat Network Administration Tool**, consultez le chapitre *Configuration réseau (Network Configuration)* du *Guide de personnalisation officiel Red Hat Linux*.
- `network-scripts` — Ce répertoire contient les fichiers de configuration relatifs au réseau suivants:

  - Les fichiers de configuration réseau pour chaque interface réseau configurée, tels que `ifcfg-eth0` for pour l'interface Ethernet `eth0`.
  - Les scripts utilisés pour avancer et rabaisser les interfaces réseau, tels que `ifup` and `ifdown`.
  - Les scripts utilisés pour avancer et rabaisser les interfaces ISDN, tels que as `ifup-isdn` et `ifdown-isdn`
  - Divers scripts de fonctions réseau partagées, qu'il n'est pas conseillé d'éditer directement.

  Pour plus d'informations sur le répertoire `network-scripts` , lisez le Chapitre 13
- `rhn` — Ce répertoire contient des fichiers de configuration pour les utilitaires **Red Hat Network Registration Client**, **Red Hat Update Agent Configuration Tool**, **Red Hat Update Agent** et l'apliquette de panneau **Red Hat Update Agent**, ainsi que les clés `systemid` GPG. Il ne faut éditer manuellement aucun fichier de ce répertoire. Pour plus d'informations sur le Red Hat Network, consultez le site Red Hat Network à l'adresse suivante: https://rhn.redhat.com/.

Précédent — Dans les coulisses du processus de démarrage
Sommaire — Niveau supérieur
Suivant — Niveaux d'exécution d'Init

Niveaux d'exécution d'Init

L'idée derrière l'utilisation de différents services à des niveaux d'exécution différents se résume principalement au principe que divers systèmes peuvent être utilisés de différentes façons. Certains services ne peuvent être utilisés tant que le système n'a pas un état ou un *mode* bien précis, tel que de permettre l'utilisation à plus d'un utilisateur ou d'avoir une connexion réseau disponible.

Vous pourriez parfois désirer utiliser le système à un mode plus bas, pour tester des problèmes relatifs au réseau au niveau 2 ou laisser le système au niveau d'exécution 3 sans exécuter de session X Window par exemple. Dans ces cas, l'exécution de services qui dépendent d'un mode du système plus élevé pour fonctionner n'a pas de sens car ils ne fonctionneront pas correctement de toute manière. En ayant défini chaque service pour qu'il s'exécute lorsque son niveau d'exécution particulier est atteint, vous vous assurez d'obtenir un processus de démarrage ordonné et vous pouvez changer rapidement le mode de l'ordinateur sans vous préoccuper des services devant être lancés ou arrêtés manuellement.

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

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

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

Vous pouvez à loisir configurer les niveaux d'exécution 2 et 4. De nombreux utilisateurs configurent ces niveaux d'exécution comme ils préfèrent et laissent les niveaux d'exécutions 3 et 5 seuls. Ceci leur permet d'entrer et de sortir rapidement de leur configuration personnalisée sans déranger les caractéristiques des niveaux d'exécution standard.

Si votre ordinateur ne démarre pas en raison d'un `/etc/inittab` incorrect ou ne vous laisse pas vous connecter parce que votre `/etc/passwd` est corrompu ou parce que vous avez oublié votre mot de

passe, démarrez en mode mono-utilisateur.

Si vous utilisez LILO, vous pouvez accéder au mode mono-utilisateur en entrant **`linux single`** à l'invite `boot:`.

Si vous utilisez GRUB, vous pouvez accéder au mode mono-utilisateur en suivant la procédure ci-dessous :

- Dans l'écran graphique de GRUB, sélectionnez l'étiquette de démarrage **Red Hat Linux** et appuyez sur [e] pour la modifier.
- Descendez à la ligne du noyau et appuyez sur [e] pour la modifier.
- A l'invite, entrez `single` et appuyez sur [Entrée].
- Vous retournerez à l'écran de GRUB contenant les informations sur le noyau. Appuyez sur la touche [b] pour démarrer le système en mode mono-utilisateur.

Un système trés simple démarrera et vous pourrez le configurer à l'aide du shell qu'il contient.

Si cela ne fonctionne pas, tapez **`linux init=/bin/bash`** à l'invite de LILO `boot:`. Ainsi faisant, vous vous retrouverez à: une invite de shell. Notez que seul le système de fichiers root est monté et qu'il n'est monté qu'en lecture seule. Pour le monter en mode d'écriture, (pour pouvoir par exemple modifier un fichier `/etc/inittab` corrompu), faites ce qui suit :

```
mount -n /proc
mount -o rw,remount /
```

Utilitaires de gestion des scripts Init

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

De plus, l'utilitaire `ntsysv` offre une interface orientée écran que vous trouverez peut-être plus facile à utiliser que l'interface de ligne de commande de `chkconfig`.

Si vous préférez une interface graphique, utilisez le programe **serviceconf**.

Ces deux utilitaires doivent être exécutés en tant que root.

Pour plus d'informations sur ces outils, consultez le *Guide de personnalisation officiel Red Hat Linux*.

Exécution de programmes au démarrage

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

En outre, si vous avez besoin d'une configuration de port série, vous pouvez créer et modifier `/etc/rc.serial` qui sera exécuté automatiquement au démarrage. Ce script peut exécuter toute une série de commandes `setserial` afin de configurer spécialement les ports série du système. Lisez les pages de manuel `setserial` pour plus de détails.

Arrêt

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

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

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

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

Avertissement **Avertissement**

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

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

Différences du processus de démarrage d'autres architectures

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

Par exemple, l'architecture Alpha utilise le chargeur de démarrage `aboot`, tandis que l'architecture Itanium utilise le chargeur de démarrage `ELILO`.

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

Chapitre 4. GRUB

Afin de pouvoir démarrer Red Hat Linux sur votre système, il est nécessaire de spécifier à ce dernier les modalités de démarrage à l'aide d'une série d'instructions spéciales, placées dans un *chargeur de démarrage*, soit un code résidant dans votre disque dur principal ou tout autre périphérique conçu pour le lancement du noyau Linux.

Si vous utilisez un système basé sur x86 qui ne fait démarrer que Red Hat Linux et n'avez qu'une seule version de noyau Linux, le processus exact utilisé par le chargeur de démarrage n'est pas très important. Le programme d'installation de Red Hat Linux vous donne la possibilité de configurer facilement et rapidement le chargeur de démarrage installé dans le *bloc de démarrage maître* de votre disque dur, afin de charger le système d'exploitation.

En revanche, si vous souhaitez avoir la possibilité de faire démarrer différents types de noyau Linux ou d'autres systèmes d'exploitation, il vous est essentiel de savoir la méthode employée par Red Hat Linux pour vous proposer les options nécessaires et de comprendre le processus de démarrage, ainsi que les changements à apporter.

Ce chapitre est consacré à GRUB, la méthode employée par Red Hat Linux pour démarrer les systèmes d'exploitation sur des ordinateurs x86 et aborde les différentes commandes et options de configuration qui vous permettront de contrôler le processus de démarrage.

Définition de GRUB

GRUB (GRand Unified Bootloader) de GNU est un programme qui installe un chargeur de démarrage dans le bloc de démarrage maître, présent au tout début des secteurs d'un disque dur. Il vous permet d'insérer des instructions spécifiques dans le bloc de démarrage maître pour charger un menu GRUB ou un environnement de commande qui vous permet de démarrer le système d'exploitation de votre choix, de passer des instructions spéciales au noyau lors du démarrage ou d'obtenir des paramètres système (tels que la mémoire vive disponible) avant le démarrage.

Processus de démarrage x86

Lorsqu'un ordinateur x86 démarre pour la première fois, le BIOS du système vérifie des paramètres spécifiques, tels que la mémoire vive disponible, la date et l'heure, les périphériques disque présents et

l'ordre dans lequel ils doivent être contrôlés pour permettre le démarrage. Généralement, le BIOS est configuré pour vérifier le lecteur de disquette ou de CD-ROM (ou les deux) avant d'essayer de démarrer depuis le disque dur. Si aucun support d'amorçage n'est détecté dans ces périphériques amovibles, le BIOS s'en remet alors aux premiers secteurs du premier disque dur disponible pour obtenir des instructions relatives à l'endroit où il est possible de trouver et de charger le système d'exploitation. Ces premiers secteurs, communément appelés MBR (de l'anglais Master Boot Record), soit bloc de démarrage maître en français, lancent le processus visant à amorcer un système d'exploitation présélectionné, un menu de type GRUB relatif aux options du système d'exploitation ou une interface de ligne de commande afin d'exécuter des options spéciales.

Le lancement de GRUB, et ensuite du système d'exploitation, implique plusieurs étapes :

1. *Chargement du chargeur de démarrage primaire, normalement appelé Etape No 1.* Le chargeur de démarrage primaire doit résider dans le petit espace alloué au bloc de démarrage maître, d'une dimension de moins de 512 octets. Par conséquent, l'unique action entreprise par le chargeur de démarrage primaire consiste à charger le chargeur de démarrage secondaire, à cause de l'absence d'espace qui empêche d'effectuer toute autre opération.
2. *Chargement du chargeur de démarrage secondaire, communément appelé Etape No 2.* Le chargeur de démarrage secondaire fournit les fonctions avancées qui permettent le chargement d'un système d'exploitation donné. Avec GRUB, cela correspond au code qui vous permet d'afficher un menu ou d'entrer des commandes.
3. *Chargement du système d'exploitation, tel que le noyau Linux, dans une partition définie.* Une fois que GRUB a obtenu les instructions nécessaires pour le démarrage du système d'exploitation, depuis ses propres lignes de commande ou son fichier de configuration, il trouve le fichier de démarrage nécessaire et passe le contrôle de l'ordinateur au système d'exploitation en question.

Note **Remarque**

Certains systèmes de fichiers, ainsi que certaines configurations de système de fichiers, peuvent nécessiter la création d'un fichier d'Etape 1.5 qui sert essentiellement de lien entre les deux chargeurs de démarrage (primaire et secondaire).

Par exemple, si le fichier de votre chargeur de démarrage secondaire (Etape 2) réside sur une partition qui utilise un système de fichiers auquel le chargeur de démarrage primaire (Etape 1) ne peut accéder, il est toutefois possible d'ordonner au chargeur de démarrage primaire de charger des instructions complémentaires indiquées dans le fichier d'Etape 1.5 qui lui permettront de lire le fichier du chargeur de démarrage secondaire. Pour plus d'informations, consultez les pages d'`info` de GRUB.

Cette méthode de démarrage est appelée *chargement direct*, n raison de l'utilisation d'instructions visant à charger directement le système d'exploitation, sans code intermédiaire entre les chargeurs de démarrage et les fichiers principaux du système d'exploitation (tel que le noyau). Cependant, en fonction des différents types de système d'exploitation, les processus de démarrage peuvent varier. Exemple : les

systèmes d'exploitation DOS et Windows de Microsoft, lorsqu'ils sont installés, ont l'habitude de tout écraser sans intégrer la configuration du MBR courant. Ceci a pour effet d'éliminer toute autre information mémorisée précédemment dans le bloc de démarrage maître par d'autres systèmes d'exploitation, tel que Red Hat Linux. Les systèmes d'exploitation de Microsoft, ainsi que divers autres systèmes d'exploitation propriétaires, utilisent une méthode de démarrage basée sur le *chargement de chaîne*. En procédant de la sorte, le bloc de démarrage maître pointe uniquement vers le premier secteur de la partition qui renferme le système d'exploitation où sont installés les fichiers spéciaux nécessaires au lancement de ce système d'exploitation.

GRUB prend en charge ces deux méthodes de démarrage et vous donne ainsi la possibilité de l'utiliser avec quasiment tous les systèmes d'exploitation, les systèmes de fichiers les plus répandus et les types de disques dur reconnus par votre BIOS.

Caractéristiques de GRUB

GRUB contient un certain nombre de caractéristiques qui le rendent plus intéressant que d'autres chargeurs de démarrage. Voici les plus importantes :

- *GRUB offre un véritable environnement avant système d'exploitation basé sur des commandes pour les ordinateurs x86, conférant une flexibilité maximale pour le chargement des systèmes d'exploitation avec certaines options ou pour la récolte d'informations concernant le système.* De nombreuses architectures non-x86 ont utilisé des environnements avant système d'exploitation pendant des années vous permettant de contrôler le mode de démarrage depuis une ligne de commande. Cependant, bien que *LILO* et d'autres chargeurs de démarrage x86 offrent certaines fonctionnalités de commande, GRUB en compte beaucoup plus.
- *GRUB prend en charge le mode LBA (Logical Block Addressing (LBA)).* Le mode LBA place les conversions d'adressage utilisées pour localiser des fichiers sur le disque dans le micrologiciel du disque et est utilisé sur de nombreux disques durs IDE et sur tous les disques durs SCSI. Avant l'arrivée du mode LBA, les disques durs risquaient la limite physique de 1024 cylindres, le BIOS se révélant souvent dans l'incapacité de trouver des fichiers, tels que les fichiers du chargeur de démarrage ou du noyau, au-delà de ce point. 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 des 1024 cylindres, à condition que votre BIOS accepte la prise en charge du mode LBA (ce qui est le cas pour la plupart des BIOS).
- *Le fichier de configuration de GRUB est lu sur le disque à chaque démarrage du système, ce qui vous évite d'avoir à effacer le bloc de démarrage maître à chaque changement des options de démarrage.* La plupart des chargeurs de démarrage ne sont pas suffisamment sophistiqués pour être en mesure de lire les fichiers de configuration et de les utiliser pour mettre en oeuvre des options de démarrage. Par exemple, pour effectuer une modification de la configuration de démarrage de LILO, telle que de changer le système d'exploitation à démarrer par défaut, vous devez modifier un fichier de configuration LILO et lancer une commande qui écrase le bloc de démarrage maître du système en le remplaçant par une nouvelle configuration. Cela est beaucoup

plus risqué que la méthode de GRUB car un bloc de démarrage maître mal configuré empêcherait tout simplement le démarrage du système. Par contre, si vous ne configurez pas le fichier de configuration correctement avec GRUB et redémarrez l'ordinateur, le système affichera simplement une ligne de commande que vous pourrez utiliser pour entrer manuellement les commandes nécessaires pour lancer le système d'exploitation. Le MBR n'est nullement affecté, sauf pour la mise à jour de l'Etape 1, l'Etape 2 ou les emplacements des menus de fichiers de configuration, ce qui est rarement nécessaire.

Note **Remarque**

Lorsque l'on effectue des changements au fichier de configuration de GRUB, il n'est pas nécessaire de relancer GRUB. Tous les changements effectués sont automatiquement détectés. Si vous relancez GRUB, vous vous retrouverez à la ligne de commande du shell GRUB.

Installation de GRUB

Si, durant l'installation de Red Hat Linux, GRUB n'était pas installé, voici comment procéder et en faire le chargeur de démarrage par défaut.

Note **Remarque**

Si vous utilisez déjà LILO comme chargeur de démarrage, il n'est pas nécessaire de le désinstaller pour pouvoir utiliser GRUB. Une fois installé, GRUB devient le chargeur de démarrage par défaut de votre système.

En tout premier lieu, vérifiez que vous êtes bien en possession de la dernière édition du paquetage GRUB. Vous trouverez également une copie du paquetage GRUB dans les CD-ROM d'installation de Red Hat Linux.

Ensuite, lancez la commande `/sbin/grub-install <emplacement>` depuis l'invite du shell, dans laquelle `<emplacement>` correspond à l'emplacement où GRUB doit être installé, par exemple

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

En redémarrant le système, vous verrez le chargeur de démarrage GRUB.

Différences du processus de démarrage d'autres architectures

Niveau supérieur

Terminologie

Terminologie

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. Cette information est très importante si vous voulez configurer GRUB pour lui permettre le démarrage de plusieurs systèmes d'exploitation.

Noms de périphérique

Le premier disque dur d'un système est appelé `(hd0)` par GRUB. La première partition de ce disque est appelée `(hd0,0)` par GRUB et la cinquième partition du second disque est appelée `(hd1,4)`. En général, les règles de nomination pour les systèmes de fichiers, lorsque l'on utilise GRUB, se présentent comme ceci :

```
(<type-de-périphérique><numéro-de-périphérique-bios>,<numéro-de-partition>)
```

Les parenthèses et les virgules sont très importantes dans un nom. *<type-de-périphérique>* se rapporte au fait qu'un disque dur (`hd`) ou un lecteur de disquette (`fd`) est spécifié.

<numéro-de-périphérique-bios> correspond au numéro du périphérique tel qu'indiqué par le BIOS de votre système, commençant par `0`. Le disque dur IDE primaire est numéroté `0`, alors que le disque dur IDE secondaire est numéroté `1`. La façon dont l'ordre est établi est très proche de la façon dont le noyau de Linux dispose les périphériques avec des lettres ; là où `a` dans `hda` se rapporte à `0`, le `b` dans `hdb` se rapporte à `1` et ainsi de suite.

Note **Remarque**

Rappelez-vous que le système de numérotation de GRUB pour les périphériques commence par `0` et non par `1`. C'est là une des erreurs les plus fréquentes commises par les nouveaux utilisateurs de GRUB.

<numéro-de-partition> se rapporte au numéro d'une partition spécifique sur ce périphérique. Comme pour *<numéro-de-périphérique-bios>*, la numérotation des partitions commence par `0`. Même si la plupart des partitions sont désignées par des numéros, si votre système utilise des partitions BSD, celles-ci seront désignées par des lettres, `a` ou `c`.

GRUB fait appel aux règles suivantes pour désigner des ériphés et partitions :

- Peu importe si votre disque dur est IDE ou SCSI, tous les noms de disque dur commencent par `hd` et les lecteurs de disquette 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. C'est important lorsque l'on souhaite que GRUB configure le bloc de démarrage maître pour un disque donné. Par exemple, `(hd0)` indique le premier périphérique et `(hd3)` le quatrième.
- Si vous possédez plusieurs disques durs, il est très important de connaître leur ordre selon le BIOS. Cela reste assez simple à faire si vous ne possédez que des disques durs IDE ou SCSI, mais à partir du moment où tous les deux sont installés, les choses deviennent un peu plus compliquées.

Noms de fichier

En saisissant des commandes pour GRUB qui impliquent un fichier, tel qu'une liste de menu qui permet le démarrage de plusieurs systèmes d'exploitation, il est impératif d'inclure le fichier immédiatement après avoir désigné le périphérique et la partition. Voici un exemple pour un nom de fichier absolu :

```
(<type-périphérique><numéro-périphérique-bios>,<numéro-partition>)/chemin-d'accès//fichier
```

La plupart du temps, vous indiquerez des fichiers en spécifiant le chemin d'accès sur cette partition plus le nom du fichier. C'est assez simple.

Vous pouvez également indiquer à GRUB des fichiers qui n'apparaissent pas dans le système de fichiers, tel qu'un chargeur de chaîne par exemple qui apparaît dans les tous premiers blocs d'une partition. Pour indiquer ces fichiers, vous devez fournir une *liste de blocs* qui explique à GRUB, bloc par bloc, l'emplacement du fichier sur la partition. Etant donné qu'un fichier peut se trouver positionné sur plusieurs blocs, il existe une manière particulière d'écrire une liste de blocs. Chaque emplacement de section de fichier est décrit par un numéro de bloc décalé, suivi d'un nombre de blocs après ce point de décalage ; les sections sont reliées entre elles, dans l'ordre, séparées par des virgules.

Prenons l'exemple de la liste de blocs suivante pour illustrer tout cela :

```
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.

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

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

Vous pouvez également utiliser la commande `chainloader` 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 en tant que root :

```
chainloader +1
```

Système de fichiers root de GRUB

Certains utilisateurs sont désorientés par l'emploi du terme "système de fichiers root" 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.

Par système de fichiers root de GRUB on désigne la partition racine d'un périphérique donné. GRUB exploite notamment ces informations pour monter le périphérique et procéder au chargement des fichiers.

Avec Red Hat Linux, une fois que GRUB a chargé sa propre partition root contenant le noyau Linux, la commande `kernel` peut être exécutée, l'emplacement du fichier de noyau étant optionnel. Dès le lancement du noyau Linux, il définit son propre système de fichiers root et c'est celui-ci que la plupart des utilisateurs associe à Linux. Oubliés le système de fichiers root de GRUB et ses montages ; ils n'ont servi qu'au démarrage du fichier du noyau.

Veuillez lire les notes concernant les commandes `root` et `kernel` repérables dans la la section intitulée *Commandes* pour des informations complémentaires.

Interfaces

GRUB présente trois puissantes interfaces qui ont pour rôle de fournir plusieurs niveaux de fonctions. Chacune de ces interfaces vous permet de démarrer des systèmes d'exploitation et il vous est même possible de passer d'une interface à l'autre à l'intérieur de l'environnement GRUB.

Interfaces menu

Si la configuration de GRUB a été réalisée par le programme d'installation de Red Hat Linux, vous connaissez déjà cette interface. Un menu avec les différents systèmes d'exploitation et noyaux pré configurés avec leurs propres commandes de démarrage est présenté sous la forme de liste, de façon nominale, une fois que le système a été mis en marche. La sélection s'effectue en utilisant les flèches du clavier pour mettre en évidence une option différente de celle qui est présentée par défaut et la touche [Entrée] pour valider la sélection. Si aucun choix n'est fait avant l'expiration d'un délai préétabli, GRUB procède au démarrage de l'option par défaut.

Depuis l'interface menu, il est également possible, grâce à la touche [e], d'éditer les commandes mises en évidence dans le menu ou encore, grâce à la touche [c] de charger une interface de ligne de commande.

Interface éditeur d'entrée de menu

Pour accéder à cette interface, appuyez sur la touche [e] depuis l'interface menu. Les commandes de GRUB concernant cette entrée sont présentées ci-après et vous pouvez y effectuer des changements avant le lancement du système d'exploitation en ajoutant ([o] après la ligne en usage ; [O] avant celle-ci), modifiant ([e]) ou supprimant ([d]).

Une fois que vos modifications sont effectuées et que les lignes ressemblent à ce que vous souhaitiez, appuyez sur la touche [b]pour les exécuter et démarrer le système d'exploitation. La touche d'échappement [Esc] permet d'annuler ces modifications et vous ramène à l'interface menu standard. La touche [c] , elle, vous amène à l'interface de ligne de commande.

Tuyau **Astuce**

Pour obtenir des informations concernant le changement de niveaux d'exécution avec GRUB à l'aide de l'éditeur d'entrée de menu, reportez-vous à la la section intitulée *SysV Init* dans Chapitre 3.

L'interface de ligne de commande

Cette interface GRUB est la plus élémentaire, mais c'est aussi celle qui vous offre le plus de contrôle. Vous pouvez y saisir n'importe quel type de commande GRUB valide et appuyer sur la touche [Entrée] pour en assurer l'exécution. Cette interface présente certaines fonctions avancées ressemblant aux fonctions du shell comme, par exemple, la touche d'achèvement automatique de ligne [Tab], selon le contexte et des combinaisons de touches avec [Ctrl] lors de la saisie de commandes, telles que [Ctrl]-[a] pour retourner au début de la ligne et [Ctrl]-[e] pour aller directement à la fin de la ligne. De plus, les touches de direction, [Début], [Fin] et [Suppr.] fonctionnent de la même façon que sous le shell `bash`.

Ordre d'utilisation de l'interface

Lorsque l'environnement GRUB commence à charger le chargeur de démarrage secondaire, il part à la recherche de son fichier de configuration. Une fois que celui-ci a été trouvé, il l'utilise pour la construction de la liste des systèmes d'exploitation à charger et vous présente l'interface menu.

Si le fichier de configuration est introuvable ou s'il s'avère impossible à lire, GRUB vous présente l'interface de ligne de commande qui vous permettra de saisir manuellement les commandes nécessaires au démarrage d'un système d'exploitation.

Si le fichier de configuration n'est pas valide, GRUB affiche l'erreur et attend une commande. Ceci vous est d'une grande aide parce que vous avez ainsi une information précise quant à la position même du problème et la possibilité de réparer le fichier. Appuyez sur une touche quelconque pour retourner à l'interface menu d'où vous pourrez éditer l'option du menu fautif et apporter les corrections nécessaires grâce à l'erreur rapportée par GRUB. Si vos corrections s'avèrent inefficaces, l'erreur est affichée et vous avez la possibilité de recommencer.

Commandes

GRUB possède une gamme de commandes qui peuvent être exécutées de façon interactive depuis l'interface de ligne de commande. Certaines de ces commandes acceptent une option après leur nom et ces options doivent être séparées de la commande et des autres options présentes par un espace.

Les commandes les plus utiles sont indiquées ci-après :

- `boot` — Démarre le système d'exploitation ou le chargeur de chaîne qui a été sélectionné et chargé précédemment.
- `chainloader <nom-de-fichier>` — Charge le fichier indiqué comme chargeur de chaîne. Pour s'assurer que ce fichier sera pris dès le premier secteur de la première partition, utilisez `+1` comme nom de fichier.
- `displaymem` — Affiche l'usage actuel de mémoire, sur la base des informations fournies par le BIOS. C'est pratique quand vous ignorez de combien de mémoire vive le système dispose et que celui-ci doit encore être démarré.
- `initrd <nom-de-fichier>` — Vous permet de spécifier un disque virtuel initial à utiliser pour l'amorçage, opération indispensable au noyau lorsque celui-ci a besoin de certains modules pour un démarrage correct.
- `install <Etape-1> <install-disque> <Etape-2>` p `<fichier-config>` — Installe GRUB dans votre bloc de démarrage maître. Ce qui permet aux interfaces GRUB de se présenter lors du redémarrage du système.

  Avertissement **Attention**

  La commande `install` effacera tout ce qui a été écrit précédemment dans le bloc de démarrage maître en le réécrivant. Si elle est exécutée, tout ce que vous avez mis en oeuvre pour démarrer votre système d'exploitation, à part GRUB, sera effacé irrémédiablement.

  Assurez-vous de bien savoir ce que vous faites avant d'exécuter cette commande.

  Il existe plusieurs façons de configurer cette commande. Cependant, vous devez spécifier `<étape-1>`, qui indique un périphérique, une partition et un fichier où l'image du premier chargeur de démarrage peut être trouvée, tel que `(hd0,0)/grub/stage1`. De plus, vous

devez indiquer le disque où le chargeur de démarrage de l'étape No 1 doit être installé, tel que `(hd0)`.

La section `<étape-2>` indique au chargeur de démarrage de l'étape No 1 l'emplacement du chargeur de démarrage de l'Etape No 2 comme, par exemple, `(hd0,0)/grub/stage2`. L'option `p` indique à la commande `install` qu'un fichier de configuration de menu est spécifié dans la section `<fichier-config>` comme, par exemple, `(hd0,0)/grub/grub.conf`.

- `kernel <nom-de-fichier-du-noyau> <option-1> <option-N>` — Indique quel fichier du noyau charger depuis le système de fichiers root de GRUB lorsque l'on charge directement le système d'exploitation. Des options peuvent accompagner la commande `kernel`, qui seront passées au noyau lors de son chargement.

  Pour Red Hat Linux, vous pouvez avoir une ligne `kernel` qui ressemble à ceci :

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

  Cette ligne indique que le fichier `vmlinuz` est chargé depuis le système de fichiers root de GRUB, tel que `(hd0,0)`. Une option est aussi passée au noyau indiquant que le système de fichiers root pour le noyau Linux doit se situer sur `hda5`, la cinquième partition du premier disque dur IDE lors de son démarrage. Plusieurs autres options peuvent être placées après cette option si nécessaire.
- `root <périphérique-et-partition>` — Configure la partition racine de GRUB pour en faire le périphérique et la partition spécifiques, comme `(hd0,0)`, et monte la partition afin de rendre les fichiers lisibles.
- `rootnoverify <périphérique-et-partition>` — Agit de la même façon que la commande `root`, mais ne monte pas la partition.

D'autres commandes sont aussi disponibles. Entrez `info grub` pour avoir une liste complète.

Fichier de configuration du menu

Le fichier de configuration, utilisé pour créer la liste des systèmes d'exploitation à démarrer dans l'interface menu, permet à l'utilisateur de sélectionner un groupe préétabli de commandes à exécuter. Les commandes de la la section intitulée *Commandes* peuvent être utilisées, ainsi que certaines commandes spéciales toutefois réservées au fichier de configuration.

Commandes spéciales du fichier de configuration

Les commandes suivantes ne peuvent être utilisées qu'avec le fichier de configuration du menu de GRUB :

- `color <couleur-normale> <couleur-sélectionnée>` — Vous permet de définir les couleurs à utiliser dans le menu, soit une couleur pour le premier plan et une pour l'arrière-plan. Il est possible de n'utiliser que les noms de ces couleurs, tel que `red/black`. Voici à quoi cela peut ressembler :

  ```
  color red/black green/blue
  ```

- `default <nom-titre>` — Le titre de l'entrée par défaut qui sera chargée si le délai imparti pour le choix d'une option du menu est dépassé.
- `fallback <nom-titre>` — Nom du titre de l'entrée à essayer dans le cas où la première tentative échoue.
- `hiddenmenu` — Son usage empêche l'affichage de l'interface menu de GRUB, chargeant l'entrée par défaut (`default`) lorsque le temps d'attente initial `timeout` est dépassé. L'utilisateur peut visualiser le menu standard de GRUB en appuyant sur la touche d'échappement [Esc].
- `password <mot-de-passe>` — Quand cette commande est utilisée, elle interdit à tout utilisateur ne connaissant pas le mot de passe d'éditer les entrées relatives aux options de ce menu.

  Eventuellement, vous pouvez indiquer un fichier de configuration de menu après `<mot-de-passe>`, de sorte que, si le mot de passe est connu, GRUB procède au redémarrage de la seconde étape du chargeur de démarrage et fasse appel à ce fichier de configuration alternatif pour construire le menu. Si ce fichier alternatif est laissé en dehors de la commande, tout utilisateur en possession du mot de passe sera à même d'éditer le fichier de configuration actuel.
- `timeout` — Permet de régler le temps, en secondes, qui s'écoule avant que GRUB ne charge

l'entrée indiquée dans la commande `default`.

- `splashimage` — Indique l'emplacement de l'image de fond utilisée lors du démarrage de GRUB.
- `title` — Définit le titre à utiliser avec un groupe donné de commandes utilisé lors du chargement d'un système d'exploitation.

Le symbole # sert à placer des commentaires dans le fichier de configuration du menu.

Structure des fichiers de configuration

Les commandes servant à la définition des préférences générales pour l'interface menu de GRUB sont placées dans le haut du fichier, suivies des différentes entrées relatives à chacun des systèmes d'exploitation à démarrer.

Un fichier de configuration du menu de GRUB simple servant au démarrage de Red Hat Linux ou de Microsoft Windows 2000 pourrait se présenter comme suit :

```
default=linux
timeout=10
color=green/black light-gray/blue

# section pour charger linux
title linux
root (hd0,1)
kernel /vmlinuz root=/dev/hda5
boot

# section pour charger Windows 2000
title windows
rootnoverify (hd0,0)
chainloader +1
```

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

Le paramétrage d'un fichier de menu de configuration GRUB pour le démarrage multiple de systèmes d'exploitation va au-delà de ce chapitre. Reportez-vous à la [la section intitulée *Autres ressources*] pour obtenir les informations nécessaires quant au démarrage de différents systèmes d'exploitation avec

GRUB.

Précédent Sommaire Suivant
Commandes Niveau supérieur Autres ressources

Autres ressources

Ce chapitre se limite à une introduction à GRUB et ses nombreuses options. En consultant les différentes autres sources d'informations disponibles, il est possible d'en apprendre davantage sur le mode de fonctionnement de GRUB et, notamment, sur la façon de le configurer pour démarrer des systèmes d'exploitation non-Linux.

Documentation installée

- `/usr/share/doc/grub-0.90` — `/usr/share/doc/grub-0.90` correspond au répertoire où est placée la documentation de GRUB dans le système de fichiers.
- La commande `man grub` permet d'avoir accès à la page de manuel de GRUB, qui contient la liste des options à utiliser pour charger le shell GRUB.
- La page d'info de GRUB, accessible en tapant la commande `info grub`, contient des leçons, ainsi qu'un manuel de référence pour les utilisateurs et les programmeurs et une foire aux questions (FAQ).

Sites Web utiles

- http://www.gnu.org/software/grub — La page d'accueil du projet GRUB de GNU : le site contient des informations concernant l'état du développement de GRUB ainsi qu'une FAQ.
- http://www.uruk.org/orig-grub — La documentation originale de GRUB, telle qu'elle existait avant que le projet ne soit passé à la Free Software Foundation pour un plus grand développement.
- http://www.redhat.com/mirrors/LDP/HOWTO/mini/Multiboot-with-GRUB.html — Etudie les différents usages possibles de GRUB, y compris le démarrage de systèmes d'exploitation différents de Linux.
- http://www.linuxgazette.com/issue64/kohli.html — Article de présentation sur la configuration de GRUB sur votre système en partant de zéro, avec un regard sur les options de ligne de commande de GRUB.

Chapitre 5. Le système de fichiers ext3

Avec la sortie de Red Hat Linux 7.2, Red Hat a changé de système de fichiers par défaut et est passé du format ext2 au système de fichiers *ext3* à journalisation.

Fonctions d'ext3

Le système de fichiers ext3 est, pour l'essentiel, une version améliorée du système ext2. Les améliorations en question offrent les avantages suivants :

Disponibilité

Après une panne de courant ou un blocage du système (également appelé *arrêt incorrect du système*), la cohérence de tous les systèmes de fichiers ext2 montés sur la machine doit être vérifiée par le programme `e2fsck`. Il s'agit là d'un processus très long qui peut retarder le démarrage du système, surtout pour les gros volumes contenant un nombre important de fichiers. Pendant la vérification, il est impossible d'accéder aux données contenues dans ces volumes.

La fonction de journalisation offerte par le système de fichiers ext3 permet d'éviter ce type de vérification du système de fichiers après un arrêt incorrect du système. Avec ext3, la vérification du système ne se produit que rarement, lors de problèmes matériels, comme par exemple un échec du disque dur. Le temps de récupération d'un système de fichiers ext3 après un arrêt incorrect du système ne dépend pas de la taille du système de fichiers ou du nombre de fichiers, mais de la taille du "journal" servant à maintenir la cohérence entre les fichiers. Pour la taille de journal par défaut, la récupération s'effectue en environ une seconde, selon la vitesse du matériel.

Intégrité des données

Le système de fichiers ext3 offre une meilleure intégrité des données en cas d'arrêt incorrect du système. Le système de fichiers ext3 vous permet de choisir le type et le niveau de protection reçus par vos données. Par défaut, Red Hat Linux 7.3 configure les volumes ext3 pour qu'ils maintiennent un niveau élevé de cohérence entre les données en ce qui concerne l'état du système de fichiers.

Vitesse

Même si ext3 écrit certaines données plusieurs fois, son débit est plus élevé que celui de ext2 dans la plupart des cas, la fonction de journalisation d'3 optimisant le mouvement de la tête de l'unité

de disques durs. Vous pouvez choisir parmi trois modes de journalisation pour optimiser la vitesse, mais cela signifie que vous perdrez un peu en intégrité des données.

Transition facile

Il est très facile de passer d'ext2 à ext3 ; pour profiter des avantages d'un système de fichiers à journalisation, vous n'avez pas à reformater votre disque. Voir la la section intitulée *Passer à un système de fichiers ext3* pour savoir comment réaliser cette tâche.

Si vous procédez à une installation complète de Red Hat Linux 7.3, le système de fichiers assigné par défaut aux partitions Linux du système est ext3. Si vous mettez à jour une version de Red Hat Linux utilisant des partitions ext2, le programme d'installation vous permet de convertir ces partitions en partitions ext3 sans perdre de données. Voir l'appendice intitulé *Mise à jour du système courant* dans le *Guide d'installation officiel Red Hat Linux* pour en savoir plus.

Les sections qui suivent vous guideront tout au long du processus de création et d'ajustement de partitions ext3. Si vous disposez de partitions ext2 et que vous exécutez Red Hat Linux 7.3, vous pouvez passer les sections ci-dessous concernant le partitionnement et le formatage et vous rendre directement à la la section intitulée *Passer à un système de fichiers ext3*.

Création d'un système de fichiers ext3

Si vous ajoutez un nouveau disque à un système Red Hat Linux et que vous souhaitez utiliser le système de fichiers ext3, vous devez commencer par partitionner le disque dur à l'aide d'un programme tel que `fdisk`, puis formater le système de fichiers.

Partitionnement à l'aide de `fdisk`

Pour utiliser `fdisk`, ouvrez une invite de shell et connectez-vous comme utilisateur root. La commande `fdisk` requiert que vous spécifiiez le périphérique que vous partitionnez comme argument à la commande. Dans les exemples qui suivent, le périphérique sera `/dev/hdb`, ce qui correspond au second périphérique sur le canal IDE primaire. Pour commencer, tapez :

```
/sbin/fdisk /dev/hdb
```

Le tableau suivant détaille les commandes `fdisk` les plus communes.

Tableau 5-1. commandes `fdisk`

Commande	Fonction
`m`	affiche l'aide
`p`	affiche la table de partitions en cours
`d`	efface une partition
`n`	crée une nouvelle partition
`w`	écrit la table de partitions sur le disque
`t`	règle le type de système de fichiers anticipé pour la partition
`l`	affiche la liste de types de systèmes de fichiers pour les partitions
`q`	quitte `fdisk` sans modifier le disque

Tuyau **Astuce**

A tout moment, si vous voulez quitter le programme *sans* modifier votre disque, vous pouvez taper **q**.

Maintenant que vous vous trouvez dans le programme `fdisk`, tapez **n** pour créer une nouvelle partition. Le programme vous demandera de choisir un type de partition ; sélectionnez **e** si vous souhaitez une partition étendue et **p** si vous voulez une partition primaire.

Avant de choisir le type de partition, n'oubliez pas que Red Hat Linux n'autorise pas plus de quatre partitions primaires par disque. Si vous souhaitez en créer davantage, l'une des quatre partitions primaires peut devenir une partition étendue, jouant le rôle de conteneur pour une ou plusieurs partitions logiques. Etant donné qu'elle joue ce rôle de conteneur, la taille de la partition étendue doit être au moins égale à la taille totale de toutes les partitions logiques qu'elle devra contenir. Pour en savoir plus sur les partitions de disque, reportez-vous à l'appendice *Introduction aux partitions de disque* du *Guide d'installation officiel Red Hat Linux*.

Après avoir choisi le type de partition et le numéro de la partition, choisissez la tête de cylindre sur laquelle vous voulez que la partition démarre. Vous pouvez appuyer sur [Entrée] pour accepter la valeur par défaut.

Ensuite, spécifiez la taille. Le plus simple est de taper **+*taille*M**, *taille* correspondant à la taille de la partition en mégaoctets. Si vous appuyez sur [Entrée] sans entrer de valeur, `fdisk` utilisera le reste du disque.

Répétez cette opération jusqu'à ce que vous ayez créé le schéma de partionnement souhaité.

Tuyau **Astuce**

Nous vous conseillons de noter la correspondance entre les partitions (par exemple, `/dev/hdb2`) et les systèmes de fichiers (par exemple, `/home/username`) à mesure que vous créez chaque partition.

Vous devez ensuite spécifier le type de système de fichiers que vous voulez mettre sur le disque, car `fdisk` crée des partitions de type `unknown` par défaut.

Pour ce faire, tapez **t**, suivi d'un numéro de partition. Entrez ensuite la valeur hexadécimale du type de système de fichiers que vous souhaitez installer sur la partition. Pour les partitions swap Linux, la valeur hexadécimale est **82**. Pour les partitions ext2 ou ext3 Linux, la valeur est **83**. Pour les autres types de partitions, utilisez la commande `l` pour voir la liste des types de systèmes de fichiers et les valeurs hexadécimales correspondantes. Répétez cette opération pour chaque partition créée.

Lorsque vous avez fini de créer les partitions, tapez **w** pour sauvegarder votre travail et quitter le programme.

Avertissement **Avertissement**

Lorsque vous tapez **w**, vous détruisez définitivement les données existant sur le périphérique. Si vous souhaitez les préserver, tapez **q** pour quitter le programme sans modifier le disque, puis créez une copie de sauvegarde de vos données.

Formatage de systèmes de fichiers ext3 avec `mkfs`

Une fois que vous avez créé des partitions sur le disque à l'aide d'un programme de partitionnement tel que `fdisk`, utilisez la commande `mkfs` pour créer un système de fichiers ext3 sur chaque partition.

Pour ce faire, connectez-vous en tant qu'utilisateur root et tapez :

```
/sbin/mkfs -t ext3 /dev/hdbX
```

Dans la commande ci-dessus, remplacez *hdb* par la lettre du lecteur et *X* par le numéro de la partition.

Avertissement **Avertissement**

Lorsque vous utilisez `mkfs` pour formater une partition, les données existant sur cette partition seront définitivement détruites. partition.

Allocation d'une étiquette avec `e2label`

Une fois que vous avez créé une partition et que vous l'avez formatée, allouez-lui une étiquette à l'aide de la commande `e2label`. Cela vous permet d'ajouter la partition à `/etc/fstab` en utilisant une étiquette au lieu d'un chemin d'accès au périphérique, ce qui rend le système plus robuste. [1] Pour ajouter une étiquette à une partition, tapez la commande suivante en tant que root :

```
/sbin/e2label /dev/hdbX /mount/point
```

hdb correspond à la lettre du lecteur, *X* au numéro de partition, et */mount/point* au point de montage que vous pensez utiliser pour la partition.

Une fois que vous avez alloué une étiquette à chaque partition, ajoutez les partitions à `/etc/fstab`.

Pour ce faire, connectez-vous en tant que root et tapez :

```
pico -w /etc/fstab
```

Ajoutez ensuite une ligne à `/etc/fstab` pour chaque partition étiquetée. Exemple :

```
LABEL=/mount/point   /mount/point   ext3   defaults   1 2
```

Dans l'entrée ci-dessus dans `/etc/fstab`, remplacez *chaque* `/mount/point` par le point de montage que vous pensez utiliser pour la partition.

Si vous souhaitez obtenir davantage d'informations sur les diverses options disponibles dans `/etc/fstab`, tapez `man fstab`.

S'il y a des partitions pour lesquelles vous ne connaissez pas l'étiquette, tapez la commande suivante :

```
/sbin/tune2fs -l /dev/hdbX |grep volume
```

Dans la commande ci-dessus, remplacez *hdb* par la lettre du lecteur et *X* par le numéro de la partition.

Vous obtiendrez alors quelque chose de similaire à ce qui suit :

```
Filesystem volume name: /mount/point
```

Dans cette entrée, `/mount/point` correspond à l'étiquette de volume.

Une fois que vous avez complété les étapes ci-dessus, un nouveau disque ext3 aura été ajouté à votre système. La section suivante vous expliquera comment convertir une partition ext2 en partition ext3.

Notes

[1] Si vous ajoutez une partition à `/etc/fstab`, la partition sera montée au démarrage ; en outre, l'utilisation de `mount` est ainsi simplifiée.

Précédent
Le système de fichiers ext3

Sommaire
Niveau supérieur

Suivant
Passer à un système de fichiers ext3

Passer à un système de fichiers ext3

Le programme `tune2fs` permet d'ajouter un journal à un système de fichiers ext2 existant sans altérer les données se trouvant sur la partition. Si le système de fichiers est déjà monté au moment de la transition, le journal sera visible (fichier `.journal`) dans le répertoire root du système de fichiers. Si le système de fichiers n'est pas monté, le journal sera caché et n'apparaîtra pas du tout dans le système de fichiers.

Pour convertir un système de fichiers ext2 en système ext3, connectez-vous en tant qu'utilisateur root et tapez :

```
/sbin/tune2fs -j /dev/hdbX
```

Dans la commande ci-dessus, remplacez *hdb* par la lettre du lecteur et *X* par le numéro de la partition.

Une fois que c'est fait, n'oubliez pas de changer le type de partition de ext2 à ext3 dans `/etc/fstab`.

Si vous êtes en train de convertir votre système de fichiers root, vous devrez utiliser une image `initrd` (ou disque RAM) pour démarrer. Pour créer une image de ce type, exécutez le programme `mkinitrd`. Pour obtenir de plus amples informations sur l'utilisation de la commande `mkinitrd`, tapez `man mkinitrd`. Vérifiez également que votre configuration LILO ou GRUB charge `initrd`.

Si vous n'effectuez pas cette modification, le système démarrera, mais le système de fichiers root sera monté en tant qu'ext2 au lieu d'ext3.

Revenir à un système de fichiers ext2

Le système ext3 étant relativement nouveau, certains utilitaires ne le prennent pas encore en charge. Par exemple, vous aurez peut-être besoin de réduire une partition à l'aide de `resize2fs`, qui ne prend pas encore en charge ext3. Dans ce cas, vous serez peut-être obligé de revenir de façon temporaire à un système de fichiers ext2.

Pour reconvertir une partition, vous devez commencer par démonter la partition ; connectez-vous en tant qu'utilisateur root et tapez :

```
umount /dev/hdbX
```

Dans la commande ci-dessus, remplacez *hdb* par la lettre du lecteur et *X* par le numéro de partition. Dans tout le reste de cette section, les commandes utiliseront *hdb1* pour ces valeurs.

Ensuite, changez le type de système de fichiers en ext2 ; pour ce faire, tapez :

```
/sbin/tune2fs -O ^has_journal /dev/hdb1
```

Vérifiez que la partition ne comporte pas d'erreurs ; pour cela, tapez :

```
/sbin/e2fsck -y /dev/hdb1
```

Ensuite, montez de nouveau la partition en tant que système de fichiers ext2 ; pour ce faire, tapez :

```
mount -t ext2 /dev/hdb1 /mount/point
```

Dans la commande ci-dessus, remplacez */mount/point* par le point de montage de la partition.

Ensuite, supprimez le fichier `.journal` au niveau root de la partition en choisissant le répertoire où il

est monté et en tapant :

```
rm -f .journal
```

Vous disposez alors d'une partition ext2.

Précédent | Sommaire | Suivant
Passer à un système de fichiers ext3 | Niveau supérieur | Utilisateurs et groupes

Chapitre 6. Utilisateurs et groupes

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

Les *utilisateurs* peuvent autant être des personnes (comptes réservés à un utilisateur physique défini) que des personnes logiques (les comptes existent pour des applications de façon à pouvoir exécuter des tâches particulières). Ces deux types d'utilisateurs ont un *Identificateur Utilisateur* (qui généralement est unique) et un *Identificateur Groupe*.

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

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

La bonne gestion des utilisateurs et groupes, ainsi que l'assignation et la révocation des permissions, est l'une des tâches les plus importantes de tout gestionnaire de système.

Outils pour l'administration des utilisateurs et des groupes

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

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

Utilisateurs standard

Dans le Tableau 6-1, vous trouverez les utilisateurs standard configurés par le processus d'installation (comme montré dans `/etc/passwd` file). L'ID groupe (GID) figurant dans ce tableau correspond au *groupe principal* pour l'utilisateur. Reportez-vous à la la section intitulée *Groupes propres à l'utilisateur* pour plus de détails sur l'utilisation des groupes.

Tableau 6-1. Utilisateurs standard

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

apache	48	48	/var/www	
named	25	25	/var/named	
piranha	60	60	/etc/sysconfig/ha	
amanda	33	6	var/lib/amanda/	
ident	98	98	/	/sbin/nologin
rpc	32	32	/	
wnn	49	49	/var/lib/wnn	
xfs	43	43	/etc/X11/fs	
mailnull	47	47	/var/spool/mqueue	
pvm	24	24	/usr/share/pvm3	/bin/bash
ldap	55	55	/var/lib/ldap	
mysql	27	27	/var/lib/mysql	
rpcuser	29	29	/var/lib/nfs	/sbin/nologin
nsfnobody	65534	65534	/var/lib/nfs	/sbin/nologin
junkbust	73	73	/etc/junkbuster	
gdm	42	42	/var/gdm	
squid	23	23	/var/spool/squid	/dev/null
nscd	28	28	/	
rpm	37	37	/var/lib/rpm	
mailman	41	41	/var/mailman	
radvd	75	75	/	
postgres	26	26	/var/lib/pgsql	

Précédent
Utilisateurs et groupes

Sommaire
Niveau supérieur

Suivant
Groupes standard

Groupes standard

Dans le Tableau 6-2, vous trouverez les groupes standard tels que définis par le processus d'installation (comme montré dans le fichier `/etc/group`).

Tableau 6-2. Groupes standard

Groupe	GID	Membres
root	0	root
bin	1	root, bin, daemon
daemon	2	root, bin, daemon
sys	3	root, bin, adm
adm	4	root, adm, daemon
tty	5	
disk	6	root
lp	7	daemon, lp
mem	8	
kmem	9	
wheel	10	root
mail	12	mail
news	13	news
uucp	14	uucp
man	15	
games	20	
gopher	30	
dip	40	

ftp	50	
nobody	99	
users	100	
piranha	60	piranha
ident	98	ident
rpc	32	rpc
pvm	24	pvm
floppy	19	
utmp	22	
slocate	21	
pppusers	44	
popusers	45	
slipusers	46	
rpm	37	rpm
postgres	26	postgres
nscd	28	nscd
wnn	49	wnn
mailnull	47	mailnull
rpcusers	29	
nfsnobody	65534	
xfs	43	xfs
gdm	42	gdm
apache	48	apache
squid	23	squid
named	25	named
junkbust	73	junkbust
mysql	27	mysql

mailman	41	mailman
ldap	55	ldap

Précédent Sommaire Suivant
Utilisateurs standard Niveau supérieur Groupes propres à l'utilisateur

Groupes propres à l'utilisateur

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

Groupe propre à l'utilisateur

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

umask = 002

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

Bit setgid sur des répertoires

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

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

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

Vous pouvez ajouter un utilisateur à un groupe à l'aide de **redhat-config-users** (voir *Guide de*

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

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

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

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

Exposé raisonné concernant le groupe propre à l'utilisateur

Bien que le groupe propre à l'utilisateur ne soit pas une nouveauté dans Red Hat Linux, bon nombre de personnes se posent des questions à son sujet, notamment quant à son utilité. Etudiez le scénario suivant.

Vous souhaitez qu'un groupe de personnes travaillent sur une série de fichiers se trouvant dans le répertoire `/usr/lib/emacs/site-lisp`. Vous faites confiance à quelques personnes capables, selon vous, de modifier le répertoire, mais pas à toutes.

Tout d'abord, créez un groupe `emacs` :

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

Pour associer le contenu du répertoire au groupe `emacs`, exécutez la commande suivante :

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

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

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

Autorisez les utilisateurs à créer réellement des fichiers dans le répertoire à l'aide de la commande suivante :

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

Lorsqu'un utilisateur crée un nouveau fichier, ce dernier est attribué au groupe par défaut de l'utilisateur. Pour empêcher cela, exécutez la commande suivante, qui entraîne la création de tout ce qui figure dans le répertoire avec le groupe `emacs` :

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

Si le nouveau fichier doit être du mode 664 pour qu'un autre utilisateur du groupe emacs puis l'éditer, créez l'umask 002 par défaut.

A ce stade, en créant l'umask 002 par défaut, vous pouvez aisément constituer des groupes dont les utilisateurs puissent bénéficier sans effort supplémentaire à chaque fois que des utilisateurs écrivent des fichiers dans le répertoire commun du groupe. Créez simplement le groupe, ajoutez les utilisateurs et appliquez les commandes `chown` et `chmod` ci-dessus aux répertoires du groupe.

Précédent Groupes standard
Sommaire Niveau supérieur
Suivant Utilitaires masqués

Utilitaires masqués

Si vous êtes dans un environnement multi-utilisateur et n'utilisez ni PAM ni Kerberos, vous devriez envisager d'utiliser des utilitaires masqués (aussi connus sous le nom de *shadow passwords*) car ils offrent une protection accrue des fichiers d'authentification de votre système. Pendant l'installation de Red Hat Linux, les mots de passe masqués et les *mots de passe MD5* (une méthode alternative et sans doute plus sûre de cryptage des mots de passe pour le stockage sur votre système) sont activés par défaut.

Les mots de passe masqués offrent d'autres avantages par rapport au système standard de stockage des mots de passe sur UNIX et Linux, notamment :

- Une méthode permettant d'améliorer la sécurité du système en déplaçant les mots de passe cryptés (se trouvant normalement dans `/etc/passwd`) qui n'est lisible que par root.
- Des informations concernant le vieillissement du mot de passe (le temps qui s'est écoulé depuis la dernière modification du mot de passe).
- Un contrôle sur la durée de validité du mot de passe (le moment où l'utilisateur doit le modifier).
- La possibilité d'utiliser le fichier `/etc/login.defs` pour imposer une règle de sécurité, en particulier une règle concernant le vieillissement du mot de passe.

Le paquetage `shadow-utils` contient des utilitaires qui gèrent :

- la conversion des mots de passes normaux en mots de passe masqués et vice-versa (`pwconv`, `pwunconv`),
- la vérification du mot de passe, du groupe et des fichiers masqués associés (`pwck`, `grpck`),
- des méthodes standard d'ajout, de suppression et de modification des comptes utilisateurs (`useradd`, `usermod` et `userdel`),
- des méthodes standard d'ajout, de suppression et de modification des groupes utilisateurs (`groupadd`, `groupmod` et `groupdel`),
- des méthodes standard d'administration du fichier `/etc/group` au moyen de la commande `gpasswd`.

Ces utilitaires offrent d'autres avantages :

- Les utilitaires fonctionneront parfaitement que les mots de passe masqués soient activés ou non.
- Les utilitaires ont été légèrement modifiés pour gérer le schéma du groupe propre à l'utilisateur de Red Hat. Pour obtenir une description de ces modifications, reportez-vous à la page de manuel qui reporte la commande `useradd`. Pour plus de détails sur les groupes propres à l'utilisateur, passez

à la la section intitulée *Groupes propres à l'utilisateur*.

- Le script `adduser` a été remplacé par un lien symbolique à `/usr/sbin/useradd`.
- Les outils composant le paquetage `shadow-utils` ne sont pas compatibles avec Kerberos, NIS, hesiod et LDAP. Les nouveaux utilisateurs seront uniquement locaux. Pour plus d'informations sur Kerberos et LDAP, reportez-vous au Chapitre 11 et au Chapitre 19.

Précédent | Sommaire | Suivant
Groupes propres à l'utilisateur | Niveau supérieur | Serveurs et clients X

Chapitre 7. Serveurs et clients X

Le noyau constitue le coeur de Red Hat Linux, mais pour les utilisateurs de postes de travail, l'environnement X est la façade du système d'exploitation. Le noyau est le moteur de tout ce qui se passe, et gère des processus et ressources virtuellement invisibles. Cependant, les utilisateurs quotidiens de Linux passent la majorité de leur temps dans un environnement de bureau graphique, à ouvrir des applications, à redimensionner des fenêtres et à faire défiler du texte.

Ce chapitre a été conçu comme une introduction aux coulisses de *XFree86* et à la façon dont le *système X Window* — également appelé *X* — fonctionne sur votre ordinateur pour vous permettre de bénéficier de fonctionnalités de bureau avancées.

La puissance de X

Linux a commencé comme un système d'exploitation puissant basé sur serveur, se spécialisant dans le traitement efficace de programmes complexes requérant une utilisation importante de l'unité centrale et la gestion de requêtes de centaines de milliers de clients par le biais de connexions réseau. Cependant, grâce à sa nature ouverte et à sa stabilité, Linux est vite devenu un système d'exploitation graphique populaire pour les postes de travail, pour un usage personnel et professionnel.

Dans le monde d'UNIX, les environnements multifenêtres existent depuis des dizaines d'années, sur bon nombre des systèmes d'exploitation courants. Les ordinateurs UNIX emploient le système X Window, utilisant une relation client-serveur afin de créer une interface utilisateur graphique (GUI). Un processus *server X* est lancé ; les processus *client X* peuvent s'y connecter par l'intermédiaire d'une connexion réseau ou locale. Le processus de serveur gère la communication avec le matériel (carte vidéo, moniteur, clavier et souris). Le client X existe dans l'espace utilisateur, et émet des requêtes au serveur X pour l'accomplissement de certaines tâches à l'aide du matériel qu'il contrôle.

Sur les systèmes Red Hat Linux, le serveur XFree86 remplit le rôle du serveur X. Projet logiciel Open Source opérant à une échelle importante avec des centaines de développeurs dans le monde entier, XFree86 offre un développement rapide, une prise en charge étendue pour divers périphériques et architectures matériels, et la capacité de s'exécuter sur différents systèmes d'exploitation et plates-formes.

La plupart des utilisateurs de bureau Red Hat Linux ignorent l'existence du serveur XFree86 s'exécutant sur leur système. Ils s'intéressent beaucoup plus à l'environnement de bureau particulier dans lequel ils passent la majorité de leur temps. Le programme d'installation Red Hat Linux configure parfaitement

votre serveur XFree86 pendant le processus d'installation, et garantit ainsi un fonctionnement optimal de X au premier démarrage.

Le serveur X accomplit bon nombre de tâches complexes sur un éventail important de matériels ; une configuration très détaillée de certains fichiers est donc nécessaire. Si un aspect de votre système change, comme le moniteur ou la carte vidéo, XFree86 devra être reconfiguré. En outre, si vous vous occupez d'un problème avec XFree86 qui ne peut être résolu à l'aide d'un utilitaire de configuration, comme `Xconfigurator`, vous devrez peut-être accéder à ces fichiers de configuration.

Attention

`Xconfigurator` ne doit pas être utilisé pour configurer XFree86 lorsque le serveur X est actif. Si votre système démarre par défaut directement dans X, ou niveau d'exécution 5, passez au niveau d'exécution 3 avant d'exécuter `Xconfigurator`. Si votre système démarre par défaut en mode texte, ou niveaux d'exécution 1 à 4, assurez-vous que X ne s'exécute pas lors de la configuration de X via `Xconfigurator`. Si vous ne parvenez pas à arrêter le serveur X avant l'exécution de `Xconfigurator`, vous pourriez rencontrer verrouillages matériels et corruptions de données.

Précédent | Sommaire | Suivant
Utilitaires masqués | Niveau supérieur | Le serveur XFree86

Le serveur XFree86

Red Hat Linux utilise XFree86 4 comme système X Window de base, comprenant les bibliothèques, polices, utilitaires, documents et outils de développement X nécessaires. Afin de permettre une compatibilité maximum avec le matériel plus ancien, ainsi que le matériel n'étant pas actuellement correctement pris en charge par XFree86 4, Red Hat Linux fournit également les paquetages Serveur XFree86 3 plus anciens. Les deux versions de serveurs XFree86 ont chacun une conception spécifique, et proposent donc des caractéristiques et des détails de configuration différents.

Le serveur X principal (XFree86 4) comprend de nombreuses améliorations technologiques XFree86 importantes comme la prise en charge de l'accélération 3D matérielle, l'extension XRender pour les polices anticrénelées, une conception basée sur un pilote modulaire, la prise en charge du matériel vidéo et des périphériques d'entrée modernes, ainsi que de nombreuses autres fonctions.

Les paquetages serveur X XFree86 3 sont, quant à eux, des serveurs X autonomes non-modulaires, chacun jouant le rôle d'un pilote d'affichage pour du matériel vidéo spécifique. Si vous utilisez un serveur XFree86 3, il faut que le serveur X adapté à votre carte vidéo soit installé. Ces serveurs plus anciens ne prennent pas en charge bon nombre de fonctions présentes uniquement dans les serveurs XFree86 4 plus récents, et ne sont inclus que pour la compatibilité. Les serveurs XFree86 3 à compatibilité en amont sont moins appréciés et seront supprimés des versions futures de Red Hat Linux.

Le programme d'installation Red Hat Linux installe les composants de base de XFree86, les paquetages XFree86 facultatifs que vous choisissez d'installer, le cas échéant, le serveur XFree86 4 X et les paquetages serveur X XFree86 3 dont votre matériel pourrait avoir besoin.

Le système X Window réside principalement dans deux emplacements du système de fichiers.

`/usr/X11R6`

Un répertoire contenant les binaires client X (le répertoire `bin`), des fichiers en-tête assortis (le répertoire `include`), des bibliothèques (le répertoire `lib`), des pages de manuel (le répertoire `man`) et plusieurs autres documents concernant X (le répertoire `/usr/X11R6/lib/X11/doc/`).

`/etc/X11`

La hiérarchie du répertoire `/etc/X11` contient tous les fichiers de configuration des divers composants du système X Window : fichiers de configuration du serveur X lui-même, le serveur

de polices (`xfs`), le gestionnaire d'écran X (`xdm`) et de nombreux autres composants de base. Les gestionnaires d'affichage comme `gdm` et `kdm`, ainsi que divers autres gestionnaires de fenêtres et d'autres outils X stockent leur configuration dans cette hiérarchie.

Le serveur XFree86 version 4 est un exécutable binaire simple — `/usr/X11R6/bin/XFree86`. Ce serveur charge dynamiquement divers modules serveur X lors de l'exécution à partir du répertoire `/usr/X11R6/lib/modules/`, y compris des pilotes vidéo, des pilotes de moteurs de polices et d'autres modules, si nécessaire. Certains de ces modules sont automatiquement chargés par le serveur, et d'autres sont des options facultatives que vous devez spécifier dans le fichier de configuration du serveur XFree86 4 `/etc/X11/XF86Config-4` pour qu'elles puissent être utilisées. Les pilotes vidéo de XFree86 4 se situent dans le répertoire `/usr/X11R6/lib/modules/drivers/`. Les pilotes 3D accélération matérielle DRI se situent dans `/usr/X11R6/lib/modules/dri/`.

Les serveurs XFree86 version 3 sont des binaires serveur X individuels, chacun alimentant une gamme spécifique de matériel vidéo. Les binaires serveur XFree86 installées se trouvent dans le répertoire `/usr/X11R6/bin/` ; les noms ont le format `XF86_`*`type-serveur`*, où *`type-serveur`* correspond au nom du serveur utilisé. Il existe plusieurs serveurs XFree86 3 différents, y compris le serveur `XF86_VGA16` basique et les serveurs `XF86_SVGA`, ainsi que des serveurs accélérés plus spécialisés comme `XF86_Mach64`, `XF86_S3`, `XF86_AGX`.

Fichiers de configuration du serveur XFree86

Les fichiers de configuration du serveur XFree86 sont stockés dans le répertoire `/etc/X11/`. Etant donné que les serveurs XFree86 4 et XFree86 3 utilisent des syntaxes de fichier de configuration différentes et non- compatibles, chacun dispose de son propre fichier de configuration. Le serveur XFree86 4 utilise `/etc/X11/XF86Config-4`, tandis que le serveur XFree86 3 utilise `/etc/X11/XF86Config` pour la configuration du serveur X. Lorsque Red Hat Linux est installé, les fichiers de configuration des deux versions de XFree86 sont créés à l'aide d'informations recueillies lors du processus d'installation. Si vous utilisez `Xconfigurator` pour reconfigurer une nouvelle carte vidéo, les deux fichiers de configuration sont régénérés.

Les deux fichiers de configuration comportent diverses sections, chacune définissant un aspect particulier de l'opération du serveur XFree86. Bon nombre des sections de configuration sont similaires dans les deux fichiers ; cependant, il y a également beaucoup de différences. L'une des différences notables, par exemple, est que le fichier de configuration `XF86Config-4` utilisé par le serveur XFree86 4 contient de nouvelles sections, comme `ServerLayout` et `Module` qui ne se trouvent pas dans le fichier de configuration de la version 3. Le serveur XFree86 4 permet l'utilisation de plusieurs périphériques d'entrée (souris, claviers et tablettes de dessin). Chaque périphérique d'entrée est présenté dans sa propre section `InputDevice`, où un identifiant lui est assigné ; cet identifiant vous permet de le reconnaître. Le serveur XFree86 3 configure la souris et le clavier via les directives `Keyboard` et `Pointer`.

Vous aurez très rarement à éditer manuellement ces fichiers, mais il est utile de connaître les diverses

sections et les paramètres facultatifs qu'elles peuvent contenir.

Chaque section commence par une ligne `Section "<nom-section>"` et se termine par une ligne `EndSection`. Au sein de chacune des sections, vous trouverez plusieurs lignes contenant un nom d'option et au moins une valeur d'option, parfois entre guillemets. Etant donné les similarités existant entre les deux types de fichiers de configuration, la liste suivante explore les sections les plus utiles d'un fichier de XFree86 version 4 et les rôles de plusieurs réglages fréquents.

`Device`

Donne des informations sur la carte vidéo utilisée par le système. Vous devez avoir au moins une section `Device` dans votre fichier de configuration. Vous pouvez avoir plusieurs sections `Device` si vous disposez de plusieurs cartes vidéo ou de plusieurs configurations pouvant exécuter une seule carte. Les options suivantes sont nécessaires, ou fréquemment utilisées :

- `BusID` — Indique l'emplacement de bus de la carte vidéo. Cette option n'est nécessaire que pour les systèmes disposant de plusieurs cartes ; vous devez la régler de façon à ce que la section `Device` utilise la configuration adaptée.
- `Driver` — Indique au XFree86 quel pilote charger pour utiliser la carte vidéo.
- `Identifier` — Donne un nom unique pour cette carte vidéo. Généralement, ce nom est le nom exact de la carte vidéo utilisée dans la section `Device`.
- `Screen` — Un paramètre facultatif utilisé pour les cartes vidéo disposant de plusieurs *têtes* ou connecteurs pour des moniteurs séparés. Si vous disposez de plusieurs moniteurs connectés à une carte vidéo, il vous faut des sections `Device` séparées pour chacun d'eux, avec une valeur `Screen` différente pour chaque section `Device`. La valeur acceptée par cette option est un chiffre, commençant à `0` et augmentant de un en un pour chaque tête de la carte vidéo.
- `VideoRam` — Quantité de RAM disponible sur la carte vidéo, en kilo-octets. Ce réglage n'est généralement pas nécessaire, le serveur XFree86 pouvant normalement détecter automatiquement sur la carte vidéo la quantité de RAM vidéo. Etant donné qu'il existe des cartes vidéo pour lesquelles la détection automatique de XFree86 n'est pas possible, cette option vous permet de spécifier manuellement la quantité exacte de RAM vidéo.

`DRI`

L'infrastructure *Direct Rendering Infrastructure (DRI)* est une interface permettant principalement aux applications logicielles 3D de tirer parti des capacités d'accélération matérielle 3D du matériel vidéo moderne pris en charge. En outre, la DRI peut améliorer les performances d'accélération matérielle 2D avec des pilotes qui ont été mis à jour et utilisent la DRI pour les opérations 2D. Cette section est ignorée, sauf si la DRI est activée dans la section `Module`.

Toutes les cartes vidéo n'utilisent pas la DRI de la même façon. Avant de modifier des valeurs DRI, lisez le fichier `/usr/X11R6/lib/X11/doc/README.DRI` pour en savoir plus sur

votre carte vidéo.

`Files`

Cette section définit des chemins d'accès pour les services indispensables au serveur XFree86, tels que le chemin d'accès des polices. Parmi les options les plus courantes, on trouve :

- `FontPath` — Configure les emplacements où le serveur XFree86 pourra trouver des polices. Il est possible d'y placer différents chemins d'accès fixes vers des répertoires contenant des fichiers de polices, séparés par des virgules. Par défaut, Red Hat Linux utilise `xfs` comme serveur de polices et oriente `FontPath` vers `unix/:7100`. Cela indique au serveur XFree86 qu'il doit utiliser les prises du domaine UNIX pour obtenir des informations sur les polices pour la communication entre processus.

  Reportez-vous à la la section intitulée *Polices* pour obtenir davantage d'informations sur XFree86 et les polices.
- `ModulePath` — Vous permet de configurer plusieurs répertoires pour le stockage de modules chargés par le serveur XFree86.
- `RgbPath` — Indique au serveur XFree86 où se situe la base de données de couleurs RVB dans le système. Ce fichier de base de données définit tous les noms de couleurs valides dans XFree86 et les lie à des valeurs RVB spécifiques.

`InputDevice`

Configure un périphérique d'entrée tel qu'une souris ou qu'un clavier) utilisé pour soumettre des informations au système. La plupart des systèmes disposent d'au moins deux sections `InputDevice`, clavier et souris. Chaque section comprend ces deux lignes :

- `Driver` — Indique au XFree86 le nom du pilote à charger pour utiliser ce périphérique.
- `Identifier` — Règle le nom du périphérique ; il s'agit en général du nom du périphérique suivi d'un chiffre, en commençant par `0` pour le premier. Par exemple, le premier clavier `InputDevice` a l'`identifiant Keyboard0`.

La plupart des sections `InputDevice` contiennent des lignes assignant des options spécifiques à ce périphérique particulier. Chacune de ces lignes commence par `Option` et contient le nom de l'option entre guillemets, suivi de la valeur à assigner à cette option. Les souris ont généralement des options comme `Protocol`, `PS/2` et `Device`, désignant la souris à utiliser pour cette section. La section `InputDevice` est bien commentée, ce qui vous permet de configurer des options complémentaires pour vos périphériques en enlevant les commentaires de certaines lignes.

`Module`

Indique au serveur XFree86 quels modules du répertoire `/usr/X11R6/lib/modules/` il doit charger. Les modules donnent au serveur XFree86 des fonctionnalités supplémentaires. *Ne modifiez pas ces valeurs.*

`Monitor`

Se rapporte au type de moniteur utilisé par le système. Il peut y avoir plusieurs sections `Monitor`, correspondant à chacun des moniteurs utilisés, une section `Monitor` constituant le minimum.

Avertissement **Attention**

Faites attention lorsque vous éditez manuellement des valeurs dans les options de la section `Monitor`. En effet, des valeurs inappropriées pourrait endommager ou détruire votre moniteur. Consultez la documentation fournie avec votre moniteur pour connaître les paramètres d'utilisation sûrs.

Les options suivantes sont généralement configurées :

- `HorizSync` — Indique à XFree86 la gamme de fréquences horizontales compatibles avec le moniteur, en kHz. Ces valeurs servent de guide au serveur XFree86 ; celui-ci sait ainsi s'il doit utiliser les valeurs d'une entrée `Modeline` particulière avec ce moniteur.
- `Identifier` — Donne un nom unique à ce moniteur ; chaque moniteur est en général numéroté à partir de `0`. Le premier moniteur est appelé `Monitor0`, le deuxième `Monitor1`, etc.
- `Modeline` — Permet de spécifier les modes vidéo utilisés par le moniteur à des résolutions particulières, avec certaines résolutions horizontales et d'actualisation verticales. Les entrées `Modeline` sont généralement précédées d'un commentaire expliquant ce que la ligne de mode spécifie.

  Si votre fichier de configuration ne comprend pas de commentaires pour les diverses lignes de modes, vous pouvez analyser les valeurs (ou *mode descriptions*) pour connaître le fonctionnement des lignes de mode. Reportez-vous à la page de manuel `XF86Config` pour obtenir des explications détaillées concernant chaque mode.
- `ModelName` — Paramètre facultatif indiquant le nom de modèle du moniteur.
- `VendorName` — Paramètre facultatif affichant le vendeur qui a fabriqué le moniteur.
- `VertRefresh` — Répertorie les fréquences d'actualisation verticales prises en charge par le moniteur, en kHz. Ces valeurs servent de guide au serveur XFree86 ; celui-ci sait ainsi s'il doit utiliser les valeurs d'une entrée `Modeline` particulière avec ce moniteur.

`Screen`

Relie un `Device` qui peuvent être utilisés ensemble et présentent une configuration spécifique. Il vous faut au moins une section `Screen` dans votre fichier de configuration. Les options suivantes sont courantes :

- `DefaultDepth` — Indique à la section `Screen` quelle profondeur de couleurs, en bits, elle doit essayer par défaut. `8` correspond à la valeur par défaut ; `16` permet d'afficher des

milliers de couleurs et 32 d'afficher des millions de couleurs.

- Device — Indique le nom de la section Device à utiliser avec cette section Screen.
- Identifier — Identifie la section Screen de façon à ce qu'on puisse y faire référence par une section ServerLayout et qu'on puisse l'utiliser.
- Monitor — Donne le nom de la section Monitor à utiliser avec cette section Screen.

Vous pouvez également avoir une sous-section Display dans la section Screen ; cette sous-section indique au serveur XFree86 la profondeur de couleurs (Depth) et la résolution (Mode) à essayer en premier pour ce moniteur et cette carte vidéo particuliers.

ServerFlags

Contient divers réglages globaux du serveur XFree86. Ces réglages peuvent être annulés par des options placées dans la section ServerLayout. Parmi les réglages les plus utiles, on trouve :

- DontZap — Empêche l'utilisation de la combinaison de touches [Ctrl]-[Alt]-[Espace arrière] pour désactiver le serveur XFree86.
- DontZoom — Empêche de naviguer dans les résolutions vidéo configurées à l'aide des combinaisons de touches [Ctrl]-[Alt]-[Keypad-Plus] et [Ctrl]-[Alt]-[Keypad-Minus].

ServerLayout

Relie une section Screen aux sections InputDevice nécessaires et à diverses options permettant de créer un ensemble uni de préférences utilisées par le serveur XFree86 au démarrage. Si vous avez plusieurs sections ServerLayout et que la section à utiliser n'est pas spécifiée sur la ligne de commande lors de l'activation du serveur XFree86, la première section ServerLayout du fichier de configuration est utilisée.

Les options suivantes sont utilisées dans une section ServerLayout :

- Identifier — Nom unique utilisé pour décrire cette section ServerLayout.
- InputDevice — Les noms des sections InputDevice à utiliser avec le serveur XFree86. Dans la plupart des cas, il n'y a que deux lignes à cet endroit, Keyboard0 et Mouse0, correspondant au premier clavier et à la première souris configurés pour le système. Les options CoreKeyboard et CorePointer se rapportent au fait qu'il s'agit respectivement du clavier et de la souris préférés pour le serveur XFree86.
- Screen — Le nom de la section Screen à utiliser. Le chiffre à gauche du nom de la section Screen fait référence au numéro d'écran particulier à utiliser dans une configuration multitête. Pour les cartes vidéo à tête unique standard, cette valeur est 0. Les chiffres à droite donnent les coordonnées X et Y absolues du coin supérieur gauche de l'écran, par défaut 0 0.

  Voici un exemple d'une entrée d'écran type :

```
Screen      0  "Screen0" 0 0
```

Pour plus d'informations, référez-vous à la page de manuel `XF86Config`.

Pour revoir la configuration actuelle de votre serveur XFree86, tapez la commande `xset -q`. Vous obtenez ainsi des informations sur votre clavier, votre souris, votre économiseur d'écran et des chemins d'accès aux polices.

Précédent
Serveurs et clients X

Sommaire
Niveau supérieur

Suivant
Environnements de bureau et gestionnaires de fenêtres

Environnements de bureau et gestionnaires de fenêtres

La configuration d'un serveur XFree86 ne sert à rien tant qu'un client X qui s'en servira pour afficher un programme utilisant le matériel contrôlé par le serveur X n'y accède pas. Les clients X sont des programmes conçus pour tirer parti du matériel du serveur X, généralement pour permettre une interactivité avec un utilisateur.

Vous n'avez pas besoin d'exécuter un gestionnaire de fenêtres complexes conjointement à un environnement de bureau particulier pour utiliser les applications client X. En supposant que vous ne vous trouviez pas déjà dans un environnement X et que vous ne disposiez pas d'un fichier `.xinitrc` dans votre répertoire, tapez la commande `xinit` pour lancer X avec une fenêtre basique (l'application `xterm` par défaut). Vous verrez que cet environnement de base utilise votre clavier, votre souris, votre carte vidéo et votre moniteur avec le serveur XFree86, en se servant des préférences matérielles du serveur. Tapez **`exit`** à l'invite `xterm` pour quitter cet environnement X de base.

Bien sûr, la plupart des utilisateurs auront besoin d'une interface graphique plus élaborée. Les développeurs ont rajouté des couches de fonctions qui ont permis de créer des environnements hautement développés et interactifs exploitant au maximum la puissance du serveur XFree86. Ces couches sont classées dans deux catégories spécifiques, en fonction de leur utilisation.

Gestionnaires de fenêtres

Les gestionnaires de fenêtres sont des programmes client X contrôlant la façon dont d'autres clients X sont positionnés, redimensionnés ou déplacés. Les gestionnaires de fenêtres peuvent également fournir des barres de titre aux fenêtres, une concentration clavier par clavier ou souris, et des assignations définies par l'utilisateur pour les touches et les boutons de la souris. Les gestionnaires de fenêtres fonctionnent avec différents clients X, sur l'ensemble du programme, en définissant son apparence et son apparition à l'écran à un endroit précis.

Divers gestionnaires de fenêtres sont fournis avec Red Hat Linux :

- `twm` — Le *Tab Window Manager* minimaliste, proposant la boîte à outils la plus basique.
- `fvwm2` — Dérivé du gestionnaire de fenêtres `twm` incorporant une apparence 3D et des exigences de mémoire réduites.

- `sawfish` — Le gestionnaire de fenêtres par défaut pour l'environnement de bureau GNOME, qui peut être utilisé sans GNOME.
- `wmaker` — *WindowMaker* est un gestionnaire de fenêtres GNU complet, conçu pour émuler la présentation de l'environnement NEXTSTEP.

Vous avez la possibilité d'exécuter ces gestionnaires de fenêtres comme des clients X individuels pour mieux comprendre leurs différences. Tapez la commande `xinit <chemin-d'accès-au-gestionnaire-de-fenêtres>`, `<chemin-d'accès-au-gestionnaire-de-fenêtres>` correspondant à l'emplacement du fichier binaire du gestionnaire de fenêtres. Pour trouver le fichier binaire, tapez `which <nom-gestionnaire-de-fenêtres>` ou recherchez le nom du gestionnaire de fenêtres dans un répertoire `bin`.

Environnements de bureau

Un *environnement de bureau* réunit des clients X assortis pouvant être exécutés ensemble à l'aide de méthodes similaires, avec un environnement de développement commun.

Les environnements de bureau sont différents des gestionnaires de fenêtres, qui ne contrôlent que l'apparence et l'apparition des fenêtres des clients X. Les environnements de bureau contiennent des fonctions avancées permettant aux clients X et à d'autres processus en cours d'exécution de communiquer les uns avec les autres. Cela permet à toutes les applications conçues pour fonctionner dans cet environnement de s'intégrer ; cela permet également d'utiliser ces applications de façon différente, comme par exemple en autorisant du glisser-déplacer de texte.

GNOME est l'environnement de bureau par défaut de Red Hat Linux, utilisant les outils de base GTK+ et divers autres composants étendant la fonctionnalité de base. KDE, un autre environnement de bureau, utilise une boîte d'outils différente appelée Qt. GNOME et KDE contiennent tous deux des applications de productivité sophistiquées, comme des traitements de texte, des tableurs et des périphériques de panneau de configuration qui vous permettent de gérer totalement la présentation de votre espace utilisateur. Les deux environnements peuvent faire tourner des applications client X standards, et la plupart des applications KDE peuvent s'exécuter sous GNOME, si les bibliothèques Qt sont installées.

Lorsque vous démarrez X en utilisant la commande `startx`, un environnement de bureau défini à l'avance est utilisé. Pour changer l'environnement de bureau utilisé par défaut au démarrage de X, ouvrez un terminal et tapez la commande `switchdesk`. Vous activerez alors un utilitaire graphique grâce auquel vous pourrez sélectionner l'environnement de bureau ou le gestionnaire de fenêtres à utiliser au prochain démarrage de X.

Les environnements de bureau utilisent des gestionnaires de fenêtres pour fournir une apparence cohérente des différentes applications. KDE contient son propre gestionnaire de fenêtres appelé `kwm`, spécifiquement pour cette fonctionnalité.

Pour plus d'informations sur la personnalisation des environnements de bureau GNOME et KDE, consultez le *Guide de démarrage officiel Red Hat Linux*.

Précédent
Le serveur XFree86

Sommaire
Niveau supérieur

Suivant
Niveaux d'exécution

Niveaux d'exécution

La plupart des utilisateurs exécutent X au niveau d'exécution 3 ou 5. Le niveau d'exécution 3 place votre système en mode multi-utilisateur avec des capacités de réseau complètes. L'ordinateur démarrera avec une invite de connexion texte, tous les services préconfigurés nécessaires étant lancés. La plupart des serveurs s'exécutent au niveau d'exécution 3, X n'étant pas nécessaire pour les services utilisés par la plupart des utilisateurs. Le niveau d'exécution 5 est similaire au niveau d'exécution 3, à la différence près qu'il démarre automatiquement X et propose un écran de connexion graphique. Bon nombre d'utilisateurs de postes de travail préfèrent cette méthode, puisqu'ils ne voient pas d'invite de commande.

Vous trouverez dans le fichier `/etc/inittab` le niveau d'exécution utilisé par défaut au démarrage de votre système. Si dans ce fichier vous trouvez une ligne ressemblant à `id:3:initdefault:`, cela signifie que votre système démarrera au 3. Si vous trouvez une ligne ressemblant à `id:5:initdefault:`, votre système est réglé pour démarrer au niveau d'exécution 5. Modifiez le numéro de niveau d'exécution de ce fichier pour configurer un réglage par défaut différent. Enregistrez le fichier et redémarrez votre système pour vérifier qu'il démarre au niveau d'exécution approprié. Pour plus d'informations sur les niveaux d'exécution, référez-vous à la la section intitulée *Niveaux d'exécution d'Init* dans Chapitre 3.

Niveau d'exécution 3 : `startx`

Au niveau d'exécution 3, pour démarrer une session X, tapez la commande `startx` command. La commande `startx`, un ordinateur frontal au programme `xinit`, lance le serveur XFree86 et y connecte les clients X. Etant donné que vous devez déjà être connecté au système au niveau d'exécution 3 pour pouvoir taper des commandes, `startx` est conçue uniquement pour activer certains clients X, comme un environnement de bureau, par exemple, d'une façon particulière. Il n'y a pas d'authentification de l'utilisateur.

Lorsque `startx` commence, la commande recherche un fichier `.xinitrc` dans son répertoire pour les clients X à exécuter. Si elle ne trouve pas ce fichier, elle exécutera le script `/etc/X11/xinit/xinitrc` du système à la place. Le script `startx` passe ensuite au fichier `.xserverrc` ; le script le recherche dans le répertoire de l'utilisateur et exécute le script `/etc/X11/xinit/xserverrc` par défaut s'il ne le trouve pas. Etant donné qu'il existe de nombreux clients X différents, les fichiers `xinitrc` sont très importants. Le script `xserverrc` est moins important. Il ne sert qu'à configurer le serveur X pour qu'il se connecte aux clients X. Etant donné que le serveur X par défaut est déjà configuré avec le lien `/etc/X11/X`, Red Hat Linux n'installe pas de

`xserverrc` par défaut.

Le script `xinitrc` par défaut recherche ensuite des fichiers définis par l'utilisateur et des fichiers système par défaut, dont `.Xresources`, `.Xmodmap` et `.Xkbmap` dans le répertoire de l'utilisateur et `Xresources`, `Xmodmap` et `Xkbmap` dans le répertoire `/etc/X11/`. Les fichiers `Xmodmap` et `Xkbmap`, s'ils existent, sont utilisés par l'utilitaire `xmodmap` pour configurer le clavier. Les fichiers `Xresources` sont lus dans le but d'assigner des préférences spécifiques aux applications particulières.

Une fois ces options réglées, le script `xinitrc` exécute tous les scripts du répertoire `/etc/X11/xinit/xinitrc.d/`. Ce répertoire contient un script important `xinput`, qui permet de configurer par exemple la langue à utiliser par défaut et l'environnement de bureau pour le démarrage (à partir de (`/etc/sysconfig/desktop`).

Ensuite, le script `xinitrc` tente d'exécuter `.Xclients` dans le répertoire de l'utilisateur, et passe à `/etc/X11/xinit/Xclients` s'il ne le trouve pas. Le fichier `Xclients` a pour but de lancer l'environnement de bureau ou un gestionnaire de fenêtres basique. Le script `.Xclients` du répertoire de l'utilisateur démarre l'environnement de bureau ou le gestionnaire de fenêtres choisi par l'utilisateur dans le fichier `.Xclients-default`. Si `.Xclients` n'existe pas dans le répertoire de l'utilisateur, le script `/etc/X11/init/Xclients` standard tente de lancer un autre environnement de bureau ; il essaiera GNOME en premier, puis KDE. S'il n'est pas possible de trouver un environnement de bureau par là, `Xclients` essaie le gestionnaire de fenêtres par défaut indiqué dans le fichier `.wm_style` du répertoire de l'utilisateur. Si ceci échoue, il navigue alors dans une liste de gestionnaires de fenêtres prédéfinie

A ce stade, les applications client X choisies doivent être lancées, avec le serveur XFree86. Si vous voulez plus de détails concernant le démarrage de X au niveau d'exécution 3, référez-vous aux pages de manuel `startx` et `xinit` et examinez les scripts indiqués ci-dessus.

Niveau d'exécution 5 : `prefdm`

Le niveau d'exécution 5 utilise une méthode légèrement différente pour le démarrage de X. Lorsque le système démarre, personne n'est connecté au système par défaut. Pour démarrer une session, un utilisateur doit se connecter au système. Au niveau d'exécution 5, les utilisateurs s'identifiant à la console utilisent un *gestionnaire d'affichage*, client X spécial qui permet à l'utilisateur d'entrer son identifiant et son mot de passe de connexion.

En fonction des environnements de bureau installés sur votre système Red Hat Linux spécifique, trois gestionnaires d'affichage différents sont disponibles pour l'identification des utilisateurs. Le gestionnaire d'affichage `xdm` est l'outil d'authentification X d'origine. `xdm` vous permet uniquement de vous connecter et de démarrer une session X, rien de plus. Le gestionnaire d'affichage `gdm`, conçu pour fonctionner avec l'environnement de bureau GNOME, et le gestionnaire d'affichage `kdm`, utilisé avec l'environnement de

bureau KDE, vous permettent de configurer l'environnement de bureau, ou la *session*, que vous souhaitez utiliser après l'identification. En outre, vous pouvez redémarrer ou arrêter le système à partir de l'écran de connexion. Le gestionnaire d'affichage `gdm` vous permet également de configurer la langue à utiliser.

Lorsque le système entre dans le niveau d'exécution 5, une ligne du fichier `/etc/inittab` indique que le script `prefdm` est exécuté afin de déterminer le gestionnaire d'affichage à activer pour l'authentification de l'utilisateur. Le script `prefdm` utilise les préférences définies dans le fichier `/etc/sysconfig/desktop` pour trouver le gestionnaire d'affichage approprié. Si aucun environnement de bureau n'est spécifié, `prefdm` navigue dans les gestionnaires d'affichage `gdm`, `kdm` et `xdm` pour trouver celui qu'il pourra utiliser. Une fois que c'est fait, `prefdm` le lance pour l'identification de l'utilisateur.

Chacun des gestionnaires d'affichage utilise le fichier `/etc/X11/xdm/Xsetup_0` pour configurer l'écran de connexion. Une fois que l'utilisateur est connecté au système, le script `/etc/X11/xdm/GiveConsole` est exécuté afin d'assigner la propriété de la console à l'utilisateur. Ensuite, le script `/etc/X11/xdm/Xsession` s'exécute pour accomplir bon nombre des tâches normalement prises en charge par le script `xinitrc` lorsque X est démarré au niveau d'exécution 3, y compris le paramétrage des ressources système et utilisateur, ainsi que l'exécution des scripts du répertoire `/etc/X11/xinit/xinitrc.d/`.

L'utilisateur peut spécifier l'environnement de bureau qu'il veut utiliser lors de l'identification en se servant des gestionnaires d'affichage `gdm` ou `kdm` (sélection dans le menu **Session**. Si l'environnement de bureau n'est pas spécifié dans le gestionnaire d'affichage, le script `/etc/X11/xdm/Xsession` vérifiera les fichiers `.xsession` and `.Xclients` dans le répertoire de l'utilisateur afin de décider quel environnement de bureau charger. En dernier recours, le fichier `/etc/X11/xinit/Xclients` est utilisé pour la sélection d'un environnement de bureau ou d'un gestionnaire de fenêtres à utiliser, comme dans 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 à l'utilisateur de base. Le gestionnaire d'affichage d'origine, qui a continué à s'exécuter après la connexion de l'utilisateur, prend le contrôle en créant un nouveau gestionnaire d'affichage. Ceci a pour effet de redémarrer le serveur XFree86, d'afficher une nouvelle fenêtre de connexion et de recommencer le processus à zéro.

Pour plus d'informations sur le contrôle de l'identification par les gestionnaires d'affichage, lisez la page de manuel `xdm`.

Polices

Red Hat Linux utilise la commande `xfs` (serveur de polices X) pour fournir des polices au serveur XFree86 et aux applications client X qui s'y connectent. Même s'il est possible de ne pas utiliser `xfs` et de placer les chemins d'accès aux répertoires de police dans les fichiers de configuration `XF86Config` et `XF86Config-4`, `xfs` présente plusieurs avantages :

- *Il permet d'ajouter ainsi que de supprimer des polices plus facilement et d'éditer le chemin d'accès.* Le *chemin d'accès aux polices* est en fait un ensemble de chemins d'accès du système de fichiers où sont stockés des fichiers de polices. Le service `xfs` nserve le chemin d'accès en dehors des fichiers de configuration XFree86, en en facilitant ainsi l'édition.
- *Les polices peuvent être stockées sur une machine jouant le rôle de serveur de polices en réseau, et peuvent être partagées sur les divers serveurs X du réseau.* Un ensemble de polices commun peut être conservé à un endroit, et partagé facilement entre tous les utilisateurs.
- *Davantage de types de polices sont pris en charge.* `xfs` prend en charge les polices TrueType, Type1 et bitmap.

Les fichiers de configuration XFree86 savent s'ils doivent utiliser `xfs` ou des chemins d'accès aux polices spécifiques grâce au réglage `FontPath` de leurs sections `Files`. Par défaut, `FontPath` est réglé sur `unix/:7100`. Ceci indique au serveur XFree86 qu'il doit se connecter au port 7100 en utilisant un lien de communication interne. Le serveur `xfs` donnera des informations sur les polices au serveur XFree86 lorsque celui-ci y fera appel.

Le service `xfs` doit être en cours d'exécution au démarrage de X. Si ce n'est pas le cas, vous verrez une invite comportant une erreur ressemblant à `failed to set default font path 'unix/:7100'`. Vérifiez l'exécution de `xfs` à l'aide de la commande `ps aux | grep xfs`. Par défaut, `xfs` est réglé pour démarrer aux niveaux d'exécution 2, 3, 4 et 5, couvrant tous les niveaux d'exécution utilisés pour l'exécution de X. Si `xfs` ne s'exécute pas sur votre système, vous pouvez le démarrer comme base à l'aide de la commande `/sbin/service xfs start`. Utilisez les utilitaires `/usr/sbin/ntsysv`, `serviceconf` ou `/sbin/chkconfig` pour l'obliger à démarrer aux niveaux d'exécution appropriés. Pour plus d'informations sur la configuration du service pour un niveau d'exécution donné, référez-vous au chapitre intitulé *Controlling Access to Services* dans le *Guide de personnalisation officiel Red Hat Linux*.

Configuration de `xfs`

Le script `/etc/rc.d/init.d/xfs` démarre le serveur `xfs`. Plusieurs options peuvent être configurées dans le fichier `/etc/X11/fs/config` :

- `alternate-servers` — Configure une liste de serveurs de polices de rechange à utiliser si ce serveur de polices n'est pas disponible. Tous les serveurs de la liste doivent être séparés par une virgule.
- `catalogue` — Une liste de chemins d'accès aux polices à utiliser contenant les fichiers de polices. Tous les chemins d'accès doivent être suivis d'une virgule pour que l'ajout d'un nouveau chemin à la liste soit possible.

  Vous pouvez utiliser la chaîne `:unscaled` immédiatement après le chemin d'accès pour demander le chargement des polices non cadrées de ce chemin d'accès en premier. Ensuite, vous pouvez spécifier de nouveau le chemin complet, afin que les autres polices cadrées soient chargées.
- `client-limit` — Configure le nombre de clients que ce serveur de polices servira avant de refuser d'en gérer davantage. Par défaut, `10`.
- `clone-self` — Permet de décider si le serveur de polices se clonera ou non lorsque la limite `client-limit` is hit. sera atteinte. Par défaut, cette option est activée (`on`). Pour la désactiver, réglez-la sur `off`.
- `default-point-size` — Règle la taille de points par défaut pour les polices pour lesquelles cette valeur n'est pas spécifiée. La valeur utilisée pour cette option est en décipoints. La valeur par défaut, `120`, correspond à des polices de 12 points.
- `default-resolutions` — Liste des résolutions prises en charge par le serveur XFree86. Toutes les résolutions de la liste doivent être séparées par des virgules.
- `deferglyphs` — Indique à `xfs` s'il doit différer ou non le chargement de *glyphs*, images utilisées pour représenter une police. Vous pouvez désactiver cette fonction (`none`), l'activer pour toutes les polices (`all`) ou ne l'activer que pour les polices 16 bits (`16`), très utilisées pour les langues asiatiques.
- `error-file` — Vous permet de spécifier le chemin d'accès et le nom de fichier pour la consignation des erreurs `xfs`.
- `no-listen` — Indique à `xfs` de ne pas écouter pour un protocole particulier. Par défaut, cette option est réglée sur `tcp` afin d'empêcher `xfs` d'écouter sur les ports TCP, principalement pour des raisons de sécurité. Si vous voulez utiliser `xfs` pour servir des polices à des postes de travail sur un réseau LAN, supprimez l'option `tcp` de cette ligne.
- `port` — Indique le port TCP sur lequel `xfs` écoutera si `no-listen` n'existe pas ou est désactivé.
- `use-syslog` — Indique à `xfs` d'utiliser le journal des erreurs du système si l'option est réglée sur `on`.

Ajout de polices

Lorsque vous utilisez `xfs`, le processus d'ajout de polices au système est assez simple. Utilisez la

commande `chkfontpath --list` pour voir les chemins d'accès aux polices configurés actuellement sur votre système. Pour ajouter des polices dans un nouveau répertoire, suivez ces instructions en tant qu'utilisateur de base :

1. Créez un répertoire de polices, comme `/usr/share/fonts` et placez-y les polices. Vérifiez que vous avez réglé correctement les permissions ; il faut uniquement que les fichiers puissent être lus, aucune autre permission n'est nécessaire.
2. Tapez la commande `chkfontpath --add <chemin-répertoire-polices>`, `<chemin-répertoire-polices>` correspondant au chemin d'accès complet du répertoire contenant les polices. Ce chemin d'accès sera ainsi ajouté au fichier de configuration `xfs`.

   Note **Remarque**

   Pour que la commande `fonts.dir` fonctionne correctement, il faut que vous ayez un fichier `chkfontpath` dans votre nouveau répertoire. La création du fichier `fonts.dir`, ainsi que des autres fichiers utilisés par `xfs` avec ces polices, n'est pas couverte dans ce document.

   Bon nombre de collections de polices disponibles pour Linux incluent ces fichiers ; vous n'aurez pas forcément besoin de les créer.
3. Redémarrez `xfs` en utilisant la commande `/sbin/service xfs restart`. Vous devrez également redémarrer votre session X.
4. Lorsque vous taperez la commande `chkfontpath --list`, cela aura pour effet d'afficher le nouveau chemin d'accès. Toutes les polices que vous avez ajoutées sont à présent utilisables.

Le site Web d'assistance Red Hat contient de plus amples informations à ce sujet ; reportez-vous à :

http://www.redhat.com/support pour des documents d'aide complémentaires.

Autres ressources

Il y a encore beaucoup à dire concernant le serveur XFree86, les clients qui s'y connectent et les environnements de bureau ainsi que les gestionnaires de fenêtres. Les utilisateurs avancés souhaitant peaufiner leur configuration XFree86 pourront trouver les informations ci-dessous utiles.

Documentation installée

- `/usr/X11R6/lib/X11/doc` — Contient divers documents pour XFree86, y compris :
  - `README` — Décrit brièvement l'architecture XFree86 et la méthode permettant d'obtenir des informations complémentaires sur le projet XFree86 en tant que nouvel utilisateur.
  - `README.Config` — Explique les options de configuration avancées existant pour les utilisateurs de XFree86 version 3. users.
  - `RELNOTES` — Pour les utilisateurs avancés souhaitant en savoir plus sur les dernières fonctions disponibles dans XFree86.
- Les pages de manuel suivantes couvrent des aspects particuliers du serveur XFree86 et de la configuration d'un système Linux pour l'utilisation d'un environnement X :
  - `SuperProbe` — Fournit une explication du programme `SuperProbe` et des options utiles pouvant être utilisées lorsque le programme est exécuté à partir de la ligne de commande.
  - `Xconfigurator` — Etudie la façon dont le programme `Xconfigurator` configure divers aspects du serveur XFree86, en passant en revue les options avancées qui peuvent vous permettre de gagner du temps.
  - `XF86Config` — Contient des informations concernant les fichiers de configuration XFree86, y compris la signification et la syntaxe des différentes sections des fichiers.
  - `XFree86` — La page de manuel principale pour toutes les informations sur XFree86 ; détaille les différences existant entre les connexions serveur X locales et réseau, explore les variables d'environnement communes, répertorie les options de lignes de commande et fournit des combinaisons de touches utiles.
  - `Xserver` — Se concentre sur le serveur d'affichage utilisé par les clients X, localement ou sur une connexion réseau. connection.

Sites Web utiles

- http://www.xfree86.org — Page d'accueil du projet XFree86, produisant la version Open Source XFree86 du système X Window. XFree86 est fourni avec Red Hat Linux afin de contrôler le matériel nécessaire et de fournir un environnement graphique.
- http://dri.sourceforge.net — Page d'accueil du projet DRI (Direct Rendering Infrastructure). Le DRI constitue le composant d'accélération 3D matérielle de XFree86, et ce site Web contient diverses ressources pouvant être utiles.
- http://www.redhat.com/mirrors/LDP/HOWTO/XFree86-HOWTO — Un document explicatif détaillant l'installation manuelle et la configuration personnalisée de XFree86.
- http://www.gnome.org — Page d'accueil du projet GNOME.
- http://www.kde.org — Page d'accueil de l'environnement de bureau KDE.

Livres sur le sujet

- *The Concise Guide to XFree86 for Linux* de Aron Hsiao; Que — Offre le point de vue d'un expert concernant l'opération de XFree86 sur les systèmes Linux.
- *The New XFree86* de Bill Ball, publié par Prima Publishing — Propose une étude complète du XFree86 et de sa relation avec les environnements de bureau populaires, comme GNOME et KDE.
- *Beginning GTK+ and GNOME* de Peter Wright ; Wrox Press, Inc. — Explique l'architecture GNOME aux programmeurs, en leur montrant comment de débuter avec GTK+.
- *GTK+/GNOME Application Development* de Havoc Pennington, publié par New Riders Publishing — Une étude avancée du coeur de la programmation GTK+, basée sur des exemples de programmation et un examen approfondi des API disponibles.
- *KDE 2.0 Development* de David Sweet et Matthias Ettrich, publié par Sams Publishing — Permet aux développeurs débutants et avancés de tirer parti des diverses références d'environnement requises pour l'élaboration d'applications QT pour KDE.

II. Références liées à la sécurité

Table des matières

8. Modules d'authentification enfichables (PAM)
9. TCP Wrappers et `xinetd`
10. Protocole SSH
11. Kerberos
12. Installation et configuration de Tripwire

Chapitre 8. Modules d'authentification enfichables (PAM)

Les programmes qui donnent des privilèges aux utilisateurs doivent authentifier correctement chaque utilisateur. Lorsque vous ouvrez une session sur un système, il vous est nécessaire de fournir votre nom d'utilisateur et votre mot de passe. Le processus d'ouverture de session les utilise ensuite pour vérifier votre identité.

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

Dans la plupart des cas, vous n'aurez pas à modifier les fichiers de configuration PAM d'une application. En effet, lorsque vous utilisez RPM pour installer des programmes qui requièrent une authentification, les changements nécessaires pour l'utilisation de mots de passe d'authentification au moyen de PAM se font automatiquement. Toutefois, si vous devez personnaliser votre fichier de configuration PAM, vous devez bien comprendre la structure de ce fichier (plus de détails sont disponibles dans la la section intitulée *Fichiers de configuration PAM*).

Avantages des PAM

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

- Un modèle d'authentification pouvant être utilisé par un vaste éventail d'applications.
- Flexibilité et contrôle de l'authentification pour l'administrateur et le développeur d'applications.
- Les développeurs d'applications n'ont pas à créer leurs programmes de façon à ce qu'ils utilisent un modèle d'authentification particulier, ce qui leur permet de consacrer tous leurs efforts à d'autres détails de leurs programmes.

Précédent Sommaire Suivant
Références liées à la sécurité Niveau supérieur Fichiers de configuration PAM

Fichiers de configuration PAM

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

Chaque application prenant en charge PAM (ou *service*, comme les applications destinées à être utilisées par de nombreux utilisateurs sont communément appelées) a son propre fichier dans le répertoire `/etc/pam.d/`.

Ces fichiers ont une structure particulière qui contient des appels aux modules généralement contenus dans le répertoire `/lib/security/`. De plus, chaque ligne du fichier de configuration PAM doit spécifier un type de module, un indicateur de contrôle, un chemin d'accès au module et, parfois, des arguments.

Noms de service PAM

Le fichier de configuration PAM dans le répertoire `/etc/pam.d/` est nommé en fonction du service dont il contrôle l'accès. C'est au programme prenant en charge PAM de définir le nom de ses services et d'installer son fichier de configuration PAM dans le répertoire `pam.d`. Par exemple, le programme `login` attribue le nom `/etc/pam.d/login` à son service.

En général, le nom de service correspond au nom du programme utilisé pour *accéder* au service et non pas au nom du programme utilisé pour *fournir* le service. C'est la raison pour laquelle le service `wu-ftpd` s'attribue le nom de service `/etc/pam.d/ftp`.

Les quatre sections qui suivent décrivent le format de base des fichiers de configuration PAM et la façon dont ces derniers utilisent les modules PAM pour effectuer l'authentification des applications prenant en charge PAM.

Modules PAM

Quatre types de module PAM permettent de contrôler l'accès aux services. Ces modules dépendent de différents aspects du processus d'authorisation :

- `auth` — utilisé pour authentifier l'utilisateur, par exemple en lui demandant son mot de passe et en le vérifiant. Il peut également établir des certificats d'identité, tels qu'une inscription à un groupe ou des tickets Kerberos.
- `account` — utilisé pour vérifier que l'accès est autorisé. Par exemple, il peut vérifier si le compte n'a pas expiré ou si l'utilisateur est autorisé à se connecter à cette heure de la journée.
- `password` — utilisé pour définir les mots de passe.
- `session` — utilisé après l'authentification d'un utilisateur pour gérer la session de l'utilisateur. Ce type de module peut également effectuer des tâches supplémentaires requises pour autoriser l'accès (par exemple, pour monter le répertoire personnel de l'utilisateur ou activer sa boîte aux lettres).

Note **Remarque**

Un module peut utiliser plusieurs des modules ci-dessus. Par exemple, `pam_unix.so` contient des éléments qui utilisent les quatre modules.

Dans un fichier de configuration PAM, ce type de module est le premier a être défini. Par exemple, une ligne typique d'une configuration ressemble à ceci :

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

Ceci fait que PAM cherche l'élément `auth` dans le module `pam_unix.so` module.

Modules d'empilage

Des modules peuvent être *empilés* afin d'être utilisés ensemble pour un but particulier. Par conséquent, l'ordre des modules est très important dans le processus d'authentification.

L'empilage requiert différentes conditions pour que l'administrateur puisse procéder à l'authentification d'un utilisateur. Par exemple, `rlogin` utilise normalement cinq modules `auth` empilés, comme le montre son fichier de configuration PAM :

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

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

Création de modules

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

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

Précédent Fichiers de configuration PAM
Sommaire Niveau supérieur
Suivant Indicateurs de contrôle PAM

Indicateurs de contrôle PAM

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

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

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

Important **Important**

L'ordre dans lequel les modules `required` sont appelés n'est pas important. Ce sont les indicateurs de contrôle `sufficient` et `requisite` qui font que l'ordre devienne important. Voir ci-dessous l'explication de chaque type d'indicateur de contrôle.

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

Quatre types d'indicateurs de contrôle sont définis par le standard PAM :

- Les modules ayant l'indication `required` doivent être vérifiés avec succès pour que l'authentification soit accordée. Si la vérification d'un module portant l'indication `required` échoue, l'utilisateur n'en est pas averti tant que tous les modules du même type n'auront pas été vérifiés.
- Les modules ayant l'indication `requisite` doivent également être vérifiés avec succès pour que l'authentification soit accordée. Cependant, si la vérification d'un de ces modules échoue, l'utilisateur en est averti sur-le-champ au moyen d'un message lui indiquant l'échec du premier module `required` *ou* `requisite`.
- La vérification des modules ayant l'indication `sufficient` est ignorée en cas d'échec, mais, si

la vérification est réussie et qu'aucun module `required` précédent n'a échoué, aucun autre module de ce type ne sera vérifié et l'utilisateur sera authentifié.

- Les modules ayant l'indication `optional` ne sont pas cruciaux pour la réussite ou l'échec de l'authentification de ce type de module. Ils ne jouent un rôle que lorsque aucun autre module de ce type n'a réussi ou échoué. Dans ce cas, le succès ou l'échec d'un module portant l'indication `optional` détermine l'authentification PAM générale pour ce type de module.

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

Précédent
Modules PAM

Sommaire
Niveau supérieur

Suivant
Chemins d'accès aux modules PAM

Chemins d'accès aux modules PAM

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

Arguments PAM

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

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

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

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

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

Exemples de fichiers de configuration PAM

Un fichier de configuration PAM ressemble à ceci :

```
#%PAM-1.0
auth       required  /lib/security/pam_securetty.so
auth       required  /lib/security/pam_unix.so shadow nullok
auth       required  /lib/security/pam_nologin.so
account    required  /lib/security/pam_unix.so
password   required  /lib/security/pam_cracklib.so retry=3
password   required  /lib/security/pam_unix.so shadow nullok use_authtok
session    required  /lib/security/pam_unix.so
```

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

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

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

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

Cette ligne fait en sorte que le mot de passe de l'utilisateur soit demandé et le vérifié en utilisant les informations sockées dans `/etc/passwd` et, s'il existe, dans `/etc/shadow`. Le module `pam_unix.so` détecte et utilise automatiquement les mots de passe masqués stockés dans `/etc/shadow` afin d'authentifier les utilisateurs. Consultez la la section intitulée *Utilitaires masqués* dans Chapitre 6 pour plus d'informations sur les mots de passe masqués.

L'argument `nullok` indique au module `pam_unix.so`d'autoriser un mot de passe vide.

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

La dernière phase du processus d'authentification contrôle si le fichier `/etc/nologin` existe. Si `nologin` n'existe pas et que l'utilisateur n'est pas root, l'authentification échoue.

Note **Remarque**

Dans cet exemple, les trois modules `auth` sont vérifiés, même si le premier module `auth` échoue. Ceci empêche à l'utilisateur de savoir à quel moment l'authentification a échoué. Si des hackers s'appropriaient de ces informations, ils pourraient entrer plus facilement dans le système.

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

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

```
password   required  /lib/security/pam_cracklib.so retry=3
```

Si le mot de passe n'est plus valable, l'élément mot de passe du module `pam_cracklib.so` en demande un nouveau. Il vérifie ensuite le mot de passe créé pour établir s'il peut être facilement détecté par un programme de détermination de mots de passe utilisant un dictionnaire. Si le mot de passe n'est pas accepté, il offre à l'utilisateur deux autres possibilités de créer un mot de passe sûr, et ce grâce à l'argument `retry=3`.

```
password   required  /lib/security/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` décide que le mot de passe doit être changé, par exemple si un mot de passe masqué est périmé.

L'arguement `shadow` indique au module de créer des mots de passe masqués lors de la mise à jour d'un mot de passe utilisateur.

L'argument `nullok` fait en sorte que le module autorise l'utilisateur à changer son mot de passe *depuis* un mot de passe vide, autrement 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 d'empilage de modules PAM. Cet argument fait en sorte que le module ne demande pas à l'utilisateur un nouveau mot de passe. Il accepte tous les mots de passe qui passent à travers le précédent module mot de passe. Ainsi, tous les nouveaux mots de passe doivent passer le test de sécurité `pam_cracklib.so` avant d'être acceptés.

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

La dernière ligne spécifie que le module `pam_unix.so` gérera la session. Ce module connecte le nom d'utilisateur et le type de service à `/var/log/messages` au début et à la fin de chaque session. Il peut être également empilé avec d'autres modules si vous désirez obtenir des fonctions supplémentaires.

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

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

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

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

Ensuite le module `pam_securetty.so` empêche les connexions root sur des terminaux non sécurisés. Ceci a pour effet de refuser toute tentative de `rlogin` root. Si vous devez vous connecter en tant que root, utilisez OpenSSH à la place. Pour plus d'informations sur le protocole SSH, consultez le Chapitre 10.

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

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

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

Si `pam_rhosts_auth.so` procède à l'authentification de l'utilisateur au moyen de `.rhosts` dans le répertoire personnel de l'utilisateur, PAM authentifie immédiatement la session `rlogin`. Si `pam_rhosts_auth.so` échoue lors de l'authentification de l'utilisateur, cette tentative non réussie est ignorée.

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

Si `pam_rhosts_auth.so` ne réussit pas à authentifier l'utilisateur, le module `pam_stack.so` lance une authentification normale avec mot de passe.

L'argument `service=system-auth` indique que l'utilisateur doit passer à travers la configuration PAM pour l'autorisation du système qui se trouve dans `/etc/pam.d/system-auth`.

Note **Remarque**

Si vous ne voulez pas qu'une invite de mot de passe apparaisse lorsque la vérification `securetty` échoue et détermine que l'utilisateur essaie de se connecter à distance comme utilisateur root, vous pouvez changer le module `pam_securetty.so` de `required` à `requisite`.

Précédent
Arguments PAM

Sommaire
Niveau supérieur

Suivant
Propriété de PAM et des périphériques

Propriété de PAM et des périphériques

Red Hat Linux offre au premier utilisateur privilégié à s'être connecté à la console de la machine la possibilité de manipuler les périphériques et d'exécuter des tâches qui sont normalement réservés au super-utilisateur. Ceci est possible grâce au module PAM `pam_console.so`.

Propriété des périphériques

Lorsqu'un utilisateur se connecte à une machine utilisant Red Hat Linux, le module `pam_console.so` est appelé par `login` ou par le programme de connexion graphique **gdm**. Si l'utilisateur est le premier à s'ê,tre connecté à la console physique, appelé *utilisateur console*, le module lui attribue la propriéé de périphériques qui normalement appartiennent au super-utilisateur. L'utilisateur console est propriétaire de ces périphériques tant que la dernière session locale de cet utilisateur ne se termine pas. Une fois que l'utilisateur s'est déconnecté, la propriété de ces périphériques retourne à ses valeurs par défaut.

Les périphériques affectés incluent notamment les cartes son ainsi que les lecteurs de disquette et de CD-ROM.

Ainsi, un utilisateur local peut gérer ces périphériques sans être connecté en tant que root, ce qui simplifie les tâches de l'utilisateur console.

Vous pouvez modifier la liste des périphériques contrôlés par `pam_console.so` dans le fichier `/etc/security/console.perms`.

Accès aux applications

L'utilisateur console a aussi l'autorisation d'accéder à n'importe quel programme dont le nom de fichier et dans le répertoire `/etc/security/console.apps/`. Ces fichiers n'ont pas besoin de contenir de données, mais doivent avoir exactement le même nom que celui de la commande correspondante.

Un groupe d'applications auquel l'utilisateur console à accès contient trois programmes qui arrêtent ou redémarrent le système :

- /sbin/halt
- /sbin/reboot

- /sbin/poweroff

Puisqu'il s'agit d'applications prenant en charge PAM, elles font appel au fichier `pam_console.so` pour pouvoir fonctionner.

Pour plus d'informations, consultez les pages de manuel de `pam_console`, `console.perms` et `console.apps`.

Précédent
Exemples de fichiers de configuration PAM

Sommaire
Niveau supérieur

Suivant
Autres ressources

Autres ressources

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

Documentation installée

- Page de manuel `pam` — très bonne introduction à PAM, couvrant la structure et le but des fichiers de configuration PAM.
- `/usr/share/doc/pam-`*`numéro-version`* — contient un *System Administrators' Guide*, un *Module Writers' Manual* et un *Application Developers' Manual*. Il contient également une copie de DCE-RFC 86.0, le standard PAM.

Sites Web utiles

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

En plus de ces sources d'informations, nous vous suggérons aussi de lire le plus d'exemples possibles de fichiers de configuration lorsque vous commencez à utiliser PAM.

Chapitre 9. TCP Wrappers et `xinetd`

Le contrôle d'accès aux réseaux peut se révéler une opération complexe. Les pare-feu servent à contrôler les accès depuis et vers un réseau donné, mais leur configuration est parfois difficile. TCP Wrappers et `xinetd` contrôlent les accès à l'aide du nom d'hôte et de l'adresse IP. De plus, ces outils comprennent des fonctions de journalisation et de gestion simple à configurer.

But de TCP Wrappers

Un nombre important de services réseau modernes font usage de *TCP wrappers* ; SSH, Telnet et FTP, par exemple, utilisent cette application qui vient s'interfacer entre les demandes d'accès à un service et le service même. TCP Wrappers est installé par défaut lors des installations de classe Serveur de Red Hat Linux offrant toute une gamme d'avantages lors de l'utilisation de différents types de service, chacun disposant de ses propres méthodes de contrôle d'accès.

Le concept à la base de TCP wrappers est de "regrouper" des demandes d'accès du client aux applications serveur à l'aide d'un service de vérification, de laisser une connexion client entrante communiquer directement avec un ce qui offre un degré de contrôle d'accès et de journalisation du client essayant d'utiliser le service, plutôt que la méthode usuelle de connexion directe à un service.

Les fonctions de TCP wrappers sont fournies par le fichier `libwrap.a`, une bibliothèque utilisée par les services réseau, tels que `xinetd`, `sshd` et `portmap`, compilés à cet effet. D'autres services réseau, même des programmes réseau que vous écrivez, peuvent être compilés avec `libwrap.a` pour en utiliser les fonctions. Red Hat Linux regroupe les applications TCP wrappers et les bibliothèques dans le fichier RPM `tcp_wrappers-<`*`numéro-version`*`>`.

Avantages de TCP wrappers

Lorsque qu'un utilisateur cherche à se connecter à un serveur où est installé TCP wrappers, le "wrapper" établit un rapport détaillant le nom du service demandé et les informations concernant l'hôte client. Le programme wrapper ne renvoie pas directement ces informations au client ; une fois les conditions de contrôle d'accès satisfaites, il est déchargé et libère toutes les ressources qui lui sont associées. Le client et le serveur peuvent alors reprendre les actions sans autre intervention du wrapper.

Les avantages de TCP Wrappers par rapport aux méthodes traditionnelles de contrôle sont doubles :

- *Le client qui se connecte n'est pas au courant de sa présence.* Les utilisateurs habilités ne perçoivent aucune différence et les malintentionnés ne reçoivent aucune information quant au pourquoi du refus d'accès.
- *TCP Wrappers est indépendant des applications en cours qu'il a pour but de protéger.* Cela permet aux applications d'utiliser un même ensemble de fichiers de configuration, simplifiant ainsi leur gestion.

Précédent | Sommaire | Suivant
Autres ressources | Niveau supérieur | Listes de contrôle d'accès basé sur l'hôte

Listes de contrôle d'accès basé sur l'hôte

Les accès aux services basés sur le nom d'hôte qui utilisent TCP Wrappers dépendent de deux fichiers : `hosts.allow` et `hosts.deny`. Ces fichiers, situés dans le répertoire `/etc`, font appel à une méthode simple de contrôle de l'accès de certains systèmes ou usagers aux services d'un serveur.

La règle par défaut consiste à autoriser tous les accès aux services si aucune règle n'est spécifiée dans les fichiers `hosts.allow` ou `hosts.deny`. Cependant, les règles contenues dans `hosts.allow` ont la priorité par rapport à celles qui se trouvent dans `hosts.deny`. Même si une règle interdit tout accès à un service donné dans le fichier `hosts.deny`, les hôtes autorisés à y accéder selon le fichier `hosts.allow` seront autorisés à se connecter au service en question. Les règles définies dans ces deux fichiers sont prises en compte dans l'ordre à partir du sommet, ce qui implique une certaine rigueur dans leur écriture.

Chaque modification réalisée prend effet immédiatement. Il n'est pas nécessaire de procéder à un redémarrage du service.

Ecriture des règles

Toutes les règles de contrôle d'accès sont écrites sous forme de ligne dans les fichiers `hosts.allow` et `hosts.deny`. Chaque ligne vide ou commençant par le symbole de commentaire (#) n'est pas prise en compte. Chaque règle doit être écrite sur une ligne séparée.

Les règles doivent se présenter de la façon suivante :

```
<liste_démons>: <liste_clients>[: spawn <commande_shell> ]
```

Chacune de ces options fait référence à une portion différente de la règle :

- `liste_démons` — Ensemble d'un ou plusieurs noms de processus ou de caractères spéciaux, séparés par un espace.
- `client_list` — Un ou plusieurs noms d'hôte, adresses hôte, motifs ou caractères spéciaux, séparés par un espace, à utiliser lorsqu'un nom de processus correspond à un service demandé.
- `shell_command` — Commande optionnelle qui précise ce qui doit être fait lorsqu'une règle est utilisée.

Les motifs se révèlent pratiques lorsqu'il s'agit de définir des groupes de clients qui peuvent ou ne peuvent pas

avoir accès à un service donné. En plaçant le symbole "." (point) au début d'une chaîne, la même règle se verra appliquée à tous les hôtes qui ont en commun la fin de cette chaîne. Ainsi, `.domain.com` détecterait tant `system1.domain.com` que `system2.domain.com`. Le symbole "." (point) à la fin d'une chaîne a le même effet, mais dans la direction opposée. Ceci est surtout utilisé pour les adresses IP ; ainsi une règle s'appliquant à `192.168.0.` sera valable pour tout le bloc de classe C des adresses IP. On peut aussi utiliser des expressions de masque réseau comme motif pour contrôler l'accès à un groupe d'adresses IP donné. Vous pouvez même utiliser des astérisques (*) ou des points d'interrogation (?) pour définir des groupes entiers de noms d'hôte ou d'adresses IP. Toutefois, ceux-ci ne peuvent être utilisés dans la même chaîne que les autres types de motifs.

Si votre liste de noms d'hôte pouvant accéder à un service est trop longue ou difficile à contrôler à l'intérieur de `host.allow` ou `hosts.deny`, il est alors possible d'indiquer le chemin d'accès complet vers un fichier, tel que `/etc/telnet.hosts.deny`. Ce fichier doit contenir les différents noms d'hôte, adresses hôte ou motifs, séparés par un espace, qui sont autorisés ou non à accéder à ce service. Cette méthode peut être utilisée également de façon efficace pour partager des listes de contrôle d'accès entre différents services, en permettant les changements des paramètres dans un fichier seulement pour tous les services.

Les mots ou caractères spéciaux suivants peuvent être utilisés dans les règles de contrôle d'accès à la place d'hôtes ou de groupes d'hôtes spécifiques :

- `ALL` — Correspond à chaque client lié à ce service précis ou même chaque service utilisant le contrôle d'accès. `ALL` west aussi applicable aux démons.
- `LOCAL` — Correspond à tous les hôtes sans le symbole ".".
- `KNOWN` — Correspond à tous les hôtes dont le nom d'hôte, l'adresse hôte ou l'utilisateur est connu.
- `UNKNOWN` — Correspond à tous les hôtes dont le nom d'hôte, l'adresse hôte ou l'utilisateur est inconnu.
- `PARANOID` — Correspond à tout hôte dont le nom ne correspond pas à l'adresse d'hôte.

Attention **Avertissement**

`KNOWN`, `UNKNOWN` et `PARANOID` doivent être utilisés prudemment car la moindre erreur de frappe pourrait empêcher des utilisateurs légitimes d'accéder à un service réseau.

Le langage de contrôle d'accès contient également une variable puissante, `EXCEPT`, qui consent la mise en commun de plusieurs listes au sein d'une même ligne de règle. Lorsque `EXCEPT` est utilisé entre deux listes, la première s'applique sauf s'il y a correspondance entre un paramètre de la seconde liste et un autre spécifié dans la première. `EXCEPT` peut être employé avec des listes de démons ou de clients. Voici un exemple de fichier `hosts.allow` :

```
# tous les hôtes domain.com sont autorisés à se connecter
# à tous les services, sauf cracker.domain.com
ALL: .domain.com EXCEPT cracker.domain.com

# les adresses 123.123.123.* peuvent utiliser tous les services sauf FTP
ALL EXCEPT in.ftpd: 123.123.123.
```

Note **Remarque**

Il est préférable d'utiliser la variable `EXCEPT` avec parcimonie et d'inclure plutôt les exceptions à la règle dans un autre fichier de contrôle d'accès. Ceci permet aux administrateurs de visualiser rapidement quels hôtes ou noms d'hôte peuvent accéder ou non à quels services sans avoir à relire toutes les variables `EXCEPT` ou à vérifier leur élaboration.

La meilleure façon d'utiliser `hosts.allow` et `hosts.deny` pour contrôler l'accès, consiste à les utiliser ensemble pour obtenir le résultat escompté. Ainsi, les utilisateurs souhaitant empêcher tout hôte autre que des hôtes spécifiques à accéder aux services placent d'abord `ALL: ALL` dans le fichier `hosts.deny`. Ils placent ensuite des lignes dans `hosts.allow`, telles que `portmap, in.telnetd: 10.0.1.24` ou `in.ftpd: 10.0.1. EXCEPT 10.0.1.1`, pour permettre l'accès à certains hôtes seulement.

Autrement, certains administrateurs laissent libre accès aux services de réseau à tous, à l'exception de certains hôtes bien définis. Dans ce cas, rien n'est indiqué dans `hosts.allow` et les informations concernant les hôtes interdits sont placées dans `hosts.deny`, tel que `in.fingerd: 192.168.0.2`.

Avertissement **Attention**

Il faut toutefois prêter une certaine attention lors de l'écriture de noms d'hôte ou de noms de domaine dans ces deux fichiers de contrôle d'accès, plus particulièrement dans `hosts.deny`. Plusieurs modes de contournement des règles spécifiées par nom sont connus des pirates. De plus, si votre système autorise les accès en les sélectionnant sur la base de leur nom d'hôte ou de domaine, celui-ci deviendrait inaccessible aux utilisateurs autorisés en cas de rupture du service DNS.

On peut donc éviter beaucoup de désagréments en utilisant des adresses IP lors de la création de règles de contrôle d'accès chaque fois que cela s'avère faisable, surtout pour les règles interdisant les accès.

Au-delà de la simple autorisation ou du refus d'accès aux services à certains hôtes, le langage de contrôle d'accès prend également en charge l'utilisation de commandes du shell lorsque cette règle est utilisée. Ces commandes du shell sont utilisées essentiellement avec des règles d'interdiction (deny), dans le but de parer à des *bombes à retardement*, à l'origine d'actions créant rapidement des journaux contenant les accès manqués sous forme de fichier spécial ou de message électronique envoyé à l'administrateur du réseau. Voici l'exemple d'une bombe à retardement située dans le fichier `hosts.deny` qui génère l'écriture d'un journal contenant la

date et le client chaque fois qu'un hôte, dont l'adresse IP est comprise entre 10.0.1.0 et 10.0.1.255, tente de se connecter via Telnet :

```
in.telnetd: 10.0.1.: spawn (/bin/echo `date` %c >> /var/log/telnet.log) &
```

Voici une liste d'*extensions* contenant des informations spécifiques relatives au client, au serveur et aux processus utilisés disponibles aux commandes du shell :

- `%a` — Adresse IP du client.
- `%A` — Adresse IP du serveur.
- `%c` — Différents types d'informations sur le client, tels que nom d'utilisateur et nom d'hôte ou nom d'utilisateur et adresse IP.
- `%d` — Nom du processus démon.
- `%h` — Nom d'hôte du client (ou son adresse IP si le nom d'hôte n'est pas disponible).
- `%H` — Nom d'hôte du serveur (ou son adresse IP si le nom d'hôte n'est pas disponible).
- `%n` — Nom d'hôte du client. Si aucune information n'est disponible, le mot `unknown` est affiché. Dans le cas où le nom d'hôte du serveur et l'adresse d'hôte ne correspondraient pas, le mot `paranoid` est affiché.
- `%N` — Nom d'hôte du serveur. Si aucune information n'est disponible, le mot `unknown` est affiché. Dans le cas où le nom d'hôte du serveur et l'adresse d'hôte ne correspondraient pas, le mot `paranoid` est affiché.
- `%p` — Identifiant du processus démon.
- `%s` — Différents types d'informations sur le serveur, tels que processus démon, adresse d'hôte ou adresse IP du serveur.
- `%u` — Nom d'utilisateur du client. Si aucune information n'est disponible, le mot `unknown` est affiché.

Pour de plus amples informations concernant les commandes du shell, ainsi que d'autres exemples de contrôle d'accès, veuillez vous reporter à la page de manuel de hosts_access(5).

Note **Remarque**

Prêtez une attention particulière à la commande `portmap` lorsqu'elle est utilisée avec des listes de contrôle d'accès aux hôtes. Seules des adresses IP et l'option `ALL` devraient être employées lors de la définition d'autorisation et de refus d'accès aux hôtes, dans la mesure ou les noms d'hôte ne sont pas pris en charge. De plus, les changements apportés aux listes de contrôle d'accès d'hôtes qui concernent `portmap` ne sont pas nécessairement appliqués immédiatement.

Vu que certains services très utilisés, tels que NIS et NFS, dépendent de `portmap` pour leur fonctionnement, tenez compte de ces limitations avant de dépendre des fichiers `hosts.allow` et `hosts.deny` pour contrôler l'accès de certains hôtes.

TCP Wrappers et `xinetd` Niveau supérieur Contrôle d'accès à l'aide de `xinetd`

Contrôle d'accès à l'aide de `xinetd`

Les avantages de l'utilisation de TCP wrappers se multiplient lorsque la bibliothèque `libwrap.a` agit de concert avec `xinetd`, un *super-démon* qui offre des outils supplémentaires d'accès, de journalisation, de liaison, de réacheminement et d'utilisation des ressources.

Red Hat Linux configure de nombreux services réseaux très répandus à utiliser avec `xinetd`, tels que FTP, IMAP, POP et Telnet. Le démon `xinetd` gère les demandes d'accès à ces services depuis `/etc/services`, lorsque l'on y accède via leur numéro de port. Avant de rendre disponible le service demandé à l'utilisateur, `xinetd` s'assure de la conformité des informations d'hôte du client relatives aux règles d'accès ; le nombre d'instances pour ce service est maintenu sous un seuil particulier et chaque autre règle inhérente à ce service ou tout autre service `xinetd` est suivie. Une fois que le service demandé est autorisé au client, `xinetd` retourne en veille, attendant la prochaine demande de services de son ressort.

Fichiers de configuration de `xinetd`

Le service `xinet` service est contrôlé par le fichier `/etc/xinetd.conf` ainsi que les différents fichiers spécifiques à des services situés dans le répertoire `/etc/xinetd.d`.

`/etc/xinetd.conf`

Le fichier `xinetd.conf` est le parent de tous les fichiers de configuration de services contrôlés par `xinetd`, étant donné que chaque fichier spécifique à un service se voit analyser à chaque lancement de `xinetd`. Par défaut, `xinetd.conf` contient des paramètres de configuration de base qui s'appliquent à tous les services :

```
defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
        log_on_failure          = HOST
}

includedir /etc/xinetd.d
```

Ces lignes contrôlent les différentes modalités d'application de `xinetd` :

- `instances` — Définit le nombre maximum de demandes d'accès qu'un service peut traiter à la fois.
- `log_type` — Invite `xinetd` à utiliser le journal `authpriv`, spécifié dans `/etc/syslog.conf` et configuré par défaut sur `/var/log/secure`, plutôt que d'utiliser un autre fichier spécifique. Si on utilisait `FILE /var/log/xinetdlog` à la place, `xinetd` effectuerait la journalisation dans un fichier `/var/log/xinetdlog` séparé.
- `log_on_success` — Définit ce que `xinetd` doit journaliser lorsque la connexion est établie avec succès. L'adresse IP de l'hôte distant et l'identifiant de processus du serveur traitant la demande d'accès sont enregistrés par défaut.
- `log_on_failure` — Définit ce que `xinetd` doit journaliser lorsque la connexion n'est pas établie ou est refusée. Les paramètres `log_on_success` et `log_on_failure` du fichier `/etc/xinetd.conf` sont souvent rajoutés par chacun des différents services, ce qui signifie que les connexions réussies et refusées à chacun des services journalisent généralement plus d'informations que ce qui est indiqué ici.

`/etc/xinetd.conf` et les fichiers de configuration `xinetd` spécifiques à des services offrent de multiples options de journalisation :

- `ATTEMPT` — Journalise le fait qu'une connexion manquée a eu lieu (`log_on_failure`).
- `DURATION` — Journalise la durée d'utilisation d'un service par un système distant (`log_on_success`).
- `EXIT` — Journalise l'état ou le signal de fin du service (`log_on_success`).
- `HOST` — Journalise l'adresse IP de l'hôte distant (`log_on_failure` et `log_on_success`).
- `PID` — Journalise l'identifiant de processus du serveur qui reçoit la demande d'accès (`log_on_success`).
- `RECORD` — Journalise les informations relatives au système distant dans le cas où le service n'aurait pu être lancé. Seuls des services spéciaux, tels que `login` et `finger`, peuvent utiliser cette option (`log_on_failure`).
- `USERID` — Journalise les données concernant l'utilisateur distant selon les directives définies dans RFC 1413 pour tous les services de type multi-thread (`log_on_failure` et `log_on_success`).

D'autres options sont disponibles pour `/etc/xinetd.conf`, telles que `per_source`, qui limite le nombre maximum de connexions depuis une adresse IP donnée à un service spécifique.

Fichiers du répertoire `/etc/xinetd.d`

Les différents fichiers qui se trouvent dans le répertoire `/etc/xinetd.d` sont lus à chaque démarrage de `xinetd`, grâce à l'instruction `includedir /etc/xinetd.d` insérée à la fin de `/etc/xinetd.conf`. Ces fichiers, appelés notamment `finger`, `ipop3` et `rlogin`, se réfèrent aux différents services contrôlés par `xinetd`.

Les fichiers présents dans `/etc/xinetd.d` utilisent les mêmes règles et options que celles employées

dans `/etc/xinetd.conf`. La raison première de leur séparation dans des fichiers de configuration, un pour chaque service, est de simplifier l'ajout ou la suppression de services du domaine de `xinetd` sans affecter ses autres services.

Pour se familiariser avec la structure de ces fichiers, prenons l'exemple du fichier `wu-ftp` :

```
service ftp
{
        socket_type             = stream
        wait                    = no
        user                    = root
        server                  = /usr/sbin/in.ftpd
        server_args             = -l -a
        log_on_success          += DURATION USERID
        log_on_failure          += USERID
        nice                    = 10
        disable                 = yes
}
```

La première ligne définit le nom du service en cours de configuration. Ensuite, les lignes entre accolades renferment des paramètres de démarrage et d'utilisation de ce service. Le fichier `wu-ftp` indique que le service FTP utilise un type de socket `stream` (plutôt que `dgram`), le type de fichier binaire exécutable à utiliser, les arguments à passer au binaire, l'information à journaliser en plus des paramètres de réglage de `/etc/xinetd.conf`, l'ordre de priorité d'exécution du service, etc.

L'utilisation de `xinetd` avec un certain service peut aussi servir comme degré de protection de base contre les attaques du type refus de service (DoS). L'option `max_load` utilise une valeur de point flottant pour déterminer le seuil d'utilisation du processeur limitant ainsi le nombre de connexions possibles pour un service spécifique et évitant toute surcharge du système. L'option `cps` permet d'utiliser une valeur entière pour définir de façon numérique le nombre maximum de connexions disponibles par seconde. En imposant une valeur basse, 3 par exemple, on empêche toute attaque inondant le système de demandes d'accès simultanées à un service donné.

Contrôle d'accès dans `xinetd`

Les utilisateurs de `xinetd` ont le choix entre le recours aux fichiers de contrôle d'accès aux hôtes TCP wrappers (`hosts.allow` et `hosts.deny`), l'autorisation d'accès par le biais de fichiers de configuration `xinetd` ou un mélange des deux. Les informations concernant l'utilisation des fichiers de contrôle d'accès aux hôtes TCP wrappers se trouvent dans la la section intitulée *Listes de contrôle d'accès basé sur l'hôte*. La prochaine section traite de l'utilisation de `xinetd` pour contrôler l'accès aux services qu'il est censé surveiller.

Note **Remarque**

A la différence des fichiers de contrôle d'accès aux hôtes TCP wrappers, toute modification aux fichiers de configuration `xinetd` requiert un redémarrage d'un service `xinetd`, de même qu'un redémarrage de tout service affecté par la modification, pour que celle-ci soit appliquée.

Le contrôle d'accès aux hôtes `xinetd`, disponible par le biais de ses multiples fichiers de configuration, est différent de celui employé par TCP wrappers. Alors que TCP wrappers regroupe toutes les configurations d'accès dans deux fichiers, `/etc/hosts.allow` et `/etc/hosts.deny`, chaque fichier de service contenu dans `/etc/xinetd.d` peut contenir des règles d'accès basées sur les hôtes qui seront autorisés à utiliser ce service.

Les options suivantes sont acceptées dans les fichiers `xinetd` pour contrôler l'accès des hôtes :

- `only_from` — Autorise les hôtes spécifiés à accéder au service.
- `no_access` — Empêche les hôtes spécifiés de se servir du service.
- `access_times` — Définit les heures de disponibilité du service. Cette plage horaire doit être spécifiée comme suit : `HH:MM-HH:MM`, en utilisant la forme 24 heures.

Les options `only_from` et `no_access` peuvent utiliser une liste préétablie d'adresses IP ou de noms d'hôte ou encore un réseau entier. Tout comme avec TCP wrappers, il est possible de mettre en commun les contrôles d'accès `xinetd` avec les configurations de journalisation dans le but non seulement d'empêcher les connexions, mais aussi d'enregistrer toute tentative d'accès aux services.

Par exemple, le fichier `/etc/xinetd.d/telnet` suivant peut être utilisé pour interdire l'accès via `telnet` à un groupe précis d'utilisateurs et limiter la plage horaire disponible aux utilisateurs autorisés :

```
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, lorsqu'un ordinateur du sous-réseau 10.0.1.0/24, tel que 10.0.1.2, cherche à établir une

connexion `telnet` avec l'hôte `boo`, le message `Connection closed by foreign host.` (connexion fermée par l'hôte étranger) lui est envoyé. De plus, cette tentative d'accès est journalisée dans le fichier `/var/log/secure` :

```
May 15 17:35:47 boo xinetd[16188]: START: telnet pid=16191 from=10.0.1.2
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 booxinetd[16252]: EXIT: telnet status=0 pid=16256
```

Liaison et réacheminement de port

Les fichiers de configuration de service `xinetd` prennent également en charge les liaisons de services vers une adresse IP spécifique et le réacheminement des demandes d'accès au service vers une autre adresse IP, un autre nom d'hôte ou un autre port.

Les liaisons, telles que définies par l'option `bind` dans les fichiers de configuration de service, relient explicitement les services vers une autre adresse IP utilisée par le système, autorisant ainsi l'accès au service uniquement lorsqu'il arrive par cette adresse IP. Ceci se révèle tout particulièrement utile lorsque la configuration du système comprend plusieurs cartes réseau et utilise des adresses IP multiples, tels que sur des ordinateurs employés comme pare-feu, avec une carte en contact avec Internet et l'autre reliée au réseau local. Aussi est-il possible d'empêcher des pirates essayant de se connecter à un service donné, tel que Telnet ou FTP, via Internet de se connecter au service alors que les utilisateurs internes peuvent se connecter au service via le NIC branché au réseau local.

L'option `redirect`, qui accepte une adresse IP ou un nom d'hôte suivi d'un numéro de port, indique au service de réacheminer toute demande pour ce service vers l'emplacement spécifié. Cette fonction peut être utilisée pour pointer vers un autre numéro de port sur le même système, réacheminer la demande vers une adresse IP différente sur le même ordinateur, passer la demande à un système et un numéro de port totalement différents ou mélanger ces diverses possibilités. De cette façon, il est possible de dérouter la connexion d'un utilisateur à un service donné d'un système sur un autre système sans aucune perturbation.

Le démon `xinetd` est en mesure d'effectuer cette redirection en générant un processus qui demeure actif pendant toute la durée de la connexion entre l'ordinateur client effectuant la demande et l'hôte qui fournit le service, transférant les données entre les deux systèmes.

Tout l'intérêt des options `bind` et `redirect` se concrétisent lorsqu'elles sont utilisées simultanément. En reliant un service à une adresse IP spécifique sur un ordinateur donné et en redirigeant les demandes d'accès à ce service vers un autre ordinateur reconnu uniquement par le premier, vous pouvez utiliser un système interne pour offrir des services à un réseau complètement différent. Autrement, ces options peuvent être utilisées pour limiter le risque d'exposition d'un service particulier résidant sur un ordinateur "multihomed" à une adresse IP connue et pour réacheminer toute demande d'accès à ce service vers un autre ordinateur spécialement configuré à cet effet.

Prenons par exemple un système utilisé comme pare-feu avec les réglages suivants pour son service FTP :

```
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 21 23
}
```

Les options `bind` et `redirect` de ce fichier s'assurent que le service FTP sur cet ordinateur est lié à l'adresse IP externe (123.123.123.123), celle qui est en contact direct avec le monde Internet. En outre, toute demande d'accès FTP envoyée à l'adresse 123.123.123.123 est réacheminée à l'aide d'une deuxième carte interface de réseau vers une adresse IP interne (10.0.1.13), accessible uniquement par le pare-feu et les systèmes internes. Ce même pare-feu établit ensuite les communications entre les deux systèmes et le système qui se connecte pensera s'être connecté à l'adresse 123.123.123.123 alors qu'il est en fait connecté à un tout autre ordinateur.

Cette caractéristique est particulièrement utile aux utilisateurs ayant des connexions à bande large et une seule adresse IP fixe. Lorsque l'on utilise le NAT (traducteur des adresses réseau), les systèmes en amont de l'ordinateur passerelle, qui utilisent des adresses IP uniquement internes, ne sont pas disponibles à à l'extérieur de la passerelle. Cependant, lorsque certains services contrôlés par `xinetd` sont configurés avec les options `bind` et `redirect`, l'ordinateur passerelle peut se comporter en serveur proxy entre les systèmes extérieurs et un ordinateur interne spécifique configuré pour garantir un service. De plus, les différentes options d'accès et de contrôle d'accès de `xinetd` peuvent être utilisées pour augmenter la sécurité en limitant le nombre d'accès simultanés vers le service réacheminé.

Autres ressources

Des sources d'informations additionnelles concernant TCP Wrappers et `xinetd` sont disponibles dans les fichiers du système et sur Internet.

Documentation installée

La documentation disponible en ligne reste un excellent point de départ pour toute recherche d'informations sur TCP Wrappers, `xinetd` et les options de configuration possibles.

- `/usr/share/doc/tcp_wrappers-<version>` — Contient un fichier `README` ; on y trouve une explication sur le mode de fonctionnement de TCP wrappers et sur les risques d'usurpation liés à l'utilisation de noms d'hôte et adresses d'hôte.
- `/usr/share/doc/xinetd-<version>` — Contient un fichier `README` qui traite des différents aspects du contrôle d'accès et un fichier `sample.conf` qui donne un aperçu des possibilités de modification des fichiers de configuration de service `/etc/xinetd.d`.
- Pour de plus amples informations sur la création de règles de contrôle d'accès TCP wrappers, veuillez vous reporter aux pages de manuel de hosts_access(5) et hosts_options(5).
- Les pages de manuel de xinetd(8) et xinetd.conf(5) contiennent des informations supplémentaires sur la réalisation de fichiers de configuration `xinetd` et sur le mode de fonctionnement de `xinetd`.

Sites Web utiles

- http://www.xinetd.org — Page d'accueil de `xinetd`, qui présente des exemples de fichier de configuration, une liste détaillée des caractéristiques et une FAQ.
- http://www.macsecurity.org/resources/xinetd/tutorial.shtml — Sur ce site Internet, vous trouverez un tutoriel sur les différentes façons d'améliorer les fichiers de configuration `xinetd` par défaut, afin d'obtenir le niveau de sécurité requis.

Chapitre 10. Protocole SSH

SSH™ permet aux utilisateurs de se connecter à distance à un autre système hôte. Contrairement à `rlogin` ou `telnet`, SSH chiffre la session de connexion et empêche ainsi aux hackers de détecter les mots de passe en texte clair.

SSH est conçu pour remplacer les méthodes classiques de connexion distante à un autre système via le shell. Un programme similaire appelé `scp` remplace des programmes moins récents, tels que `ftp` ou `rcp`, qui copient les fichiers entre les différents hôtes. Puisque ces applications ne chiffrent pas les mots de passe entre le client et le serveur, évitez de les utiliser lorsque possible. En utilisant des méthodes sécurisées pour vous connecter à distance à d'autres systèmes, vous réduisez les risques en matière de sécurité, pour votre s ystème et le système distant.

Introduction

SSH (ou *S*ecure *SH*ell) est un protocole servant à créer une connexion sécurisée entre deux systèmes. Dans le protocole SSH, un ordinateur client établit une connexion avec un ordinateur serveur.

SSH offre les garanties de sécurité suivantes :

- Après avoir effectué une connexion initiale, le client peut s'assurer de se connecter au même serveur lors des sessions suivantes.
- Le client peut transmettre ses données d'authentification au serveur, telles que son nom d'utilisateur et son mot de passe, en format crypté.
- Toutes les données envoyées et reçues pendant la connexion sont transférées de façon chiffrée, ce qui les rend extrêmement difficiles à déchiffrer et à lire.
- Le client a la possibilité d'utiliser des applications X11 [1] lancées à partir de l'invite du shell. Cette technique, appelée *X11 forwarding*, permet d'utiliser de façon sécurisée des applications graphiques sur un réseau.

Puisque le protocole SSH chiffre tout ce qu'il envoie et reçoit, il peut être utilisé pour sécuriser des protocoles non sûrs. Grâce à la technique de *retransmission de port*, un serveur SSH peut être employé pour sécuriser des protocoles non sûrs, tel que POP, augmentant ainsi la sécurité du système et des données.

Red Hat Linux 7.3 contient le paquetage OpenSSH général, (`openssh`), le serveur OpenSSH (`openssh-server`) ainsi que des paquetages client (`openssh-clients`). Consultez le chapitre *OpenSSH* du *Guide de personnalisation officiel Red Hat Linux* pour avoir des instructions d'installation et d'utilisation d'OpenSSH. Notez également que les paquetages OpenSSH requièrent le paquetage OpenSSL (`openssl`). OpenSSL installe de nombreuses bibliothèques cryptographiques importantes qui aident OpenSSH à chiffrer les communications.

Un grand nombre de programmes client et serveur peuvent utiliser le protocole SSH. Il existe plusieurs versions de clients SSH pour les principaux systèmes d'exploitation utilisés aujourd'hui. Donc, même si un utilisateur se connectant à votre système n'utilise pas Red Hat Linux, il peut tout de même avoir recours à un client SSH fait pour son propre système d'exploitation.

Pourquoi utiliser SSH ?

L'interception de paquets, la mystification DNS et IP spoofing [2] ainsi que la diffusion de fausses informations de routage ne sont que quelques exemples des menaces qui planent lors des communications en réseau. En d'autres termes, nous pourrions catégoriser ces menaces de la façon suivante :

- *Interception d'une communication entre deux systèmes* — ce scénario implique la présence d'un troisième élément quelque part sur le réseau entre les deux systèmes connectés qui copie l'information échangée entre eux. Celui-ci peut copier et garder l'information ou alors la modifier avant de l'envoyer au destinataire prévu.
- *Usurpation de l'identité d'un hôte* — grâce à cette technique, un système intercepteur prétend être le destinataire désiré d'un message. Si cela fonctionne, le client ne s'en rend pas compte et continue de lui envoyer toute l'information, comme s'il était connecté au bon destinataire.

Dans les deux cas, l'information est interceptée, probablement pour des raisons hostiles. Le résultat peut être catastrophique, peu importe qu'il soit obtenu par l'interception de tous les paquets sur un réseau local d'entreprise ou au moyen d'un serveur DNS piraté qui pointe vers un hôte mal intentionné.

L'utilisation du protocole SSH pour effectuer une connexion shell à distance ou copier des fichiers permet de faire diminuer sensiblement ces menaces à la sécurité. La signature numérique d'un serveur fournit la vérification pour son identité. En outre, la communication complète entre un système client et un système serveur ne peut être utilisée si elle est interceptée car tous les paquets sont chiffrés. De plus, il n'est pas possible d'usurper l'identité d'un des deux systèmes, parce que les paquets sont chiffrés et leurs clés ne sont connues que par les systèmes local et distant.

Notes

[1] X11 fait référence au système d'affichage de fenêtres X11R6, généralement appelé X. Red Hat Linux comprend **XFree86**, un système X Window Open Source très utilisé, basé sur X11R6.

[2] La mystification est l'acte de laisser croire aux autres que les paquetages envoyées sur un réseau proviennent d'un système sécurisé.

Précédent
Autres ressources

Sommaire
Niveau supérieur

Suivant
Séquence des événements d'une connexion SSH

Séquence des événements d'une connexion SSH

Pour aider à protéger l'intégrité d'une communication SSH entre deux ordinateurs hôtes, une certaine série d'événements doit être utilisée.

D'abord, une *couche transport* sécurisée doit être créée pour que le client sache qu'il communique bien avec le bon serveur. Ensuite, la communication est chiffrée entre le client et le serveur au moyen d'un chiffre symétrique.

Puis, une fois la connexion sécurisée établie avec le serveur, le client peut s'authentifier auprès de celui-ci sans craindre que ses informations ne puissent être compromises.

Enfin, après l'authentification du client auprès du serveur, de nombreux services différents peuvent être utilisés de façon sécurisée au cours de la connexion, tels qu'une session shell interactive, des applications X11 et des ports TCP/IP tunnellisés.

Couches de sécurité SSH

Le protocole SSH permet à tout programme client et serveur créé selon les spécifications du protocole de communiquer de façon sécurisée et d'être utilisé de manière interchangeable.

A l'heure actuelle, il existe deux types différents de protocoles SSH. La version 1 contient de nombreux algorithmes de chiffrement brevetés (toutefois, bon nombre de ces brevets sont périmés) et un trou de sécurité qui donne la possibilité éventuelle d'insérer des données dans le flux de données. La suite OpenSSH des Red Hat Linux 7.3 utilise par défaut la version SSH 2.0, bien qu'elle gère également la version 1. Nous vous conseillons d'utiliser, si possible, des serveurs et clients compatibles avec la version 2.

Les versions 1 et 2 du protocole SSH ajoutent des couches de sécurité qui fournissent leur propre type de protection.

Couche transport

Le rôle principal d'une couche transport est de faciliter une communication sécurisée entre deux ordinateurs hôtes au moment de l'authentification et par la suite également. Elle utilise généralement le protocole TCP/IP et accomplit sa tâche en s'occupant du chiffrement et du déchiffrement des données et en offrant la protection nécessaire aux paquets de données lors de leur envoi et de leur réception. En outre, la couche transport peut également faire la compression des données pour accélérer la vitesse de transfert de l'information.

Lorsqu'un client communique avec un serveur au moyen d'un protocole SSH, de nombreux éléments importants sont négociés afin que les deux systèmes puissent créer correctement la couche transport . Les opérations ci-dessous ont lieu durant cet échange :

- l'échange des clés
- l'algorithme de clé publique à utiliser
- l'algorithme de chiffrement symétrique à utiliser
- l'algorithme d'authentification de message à utiliser
- l'algorithme repère (hash) à utiliser

Durant l'échange des clés, le serveur s'identifie au client au moyen d'une *clé hôte*. Evidemment, si le client communique pour la première fois avec ce serveur, la clé du serveur lui est inconnue. OpenSSH

contourne ce problème en permettant au client d'accepter la clé hôte du serveur lors de leur première connexion SSH. Ensuite, lors des connexions suivantes, la clé hôte du serveur peut être vérifiée au moyen d'une version enregistrée sur le client, ce qui permet au client de s'assurer qu'il communique bien avec le serveur désiré.

Attention **Attention**

Un hacker pourrait se faire passer pour le serveur SSH lors de la première connexion car le système local ne reconnaît pas le serveur desiré d'un autre serveur. Afin d'éviter cela, contrôlez l'intégrité d'un nouveau serveur SSH en contactant l'administrateur du serveur avant d'établir la première connexion.

Le protocole SSH est conçu pour fonctionner avec la plupart des types d'algorithme de clé publique ou de format de codage. Après la création de deux valeurs lors de l'échange initial des clés (une valeur repère utilisée pour les échanges et une valeur secrète partagée), les deux systèmes commencent immédiatement à calculer de nouveaux algorithmes et de nouvelles clés pour protéger l'authentification et les données qui seront envoyées au cours de la connexion.

Après qu'une certaine quantité de données a été transmise au moyen d'une clé et d'un algorithme précis (la quantité exacte dépend de la mise en application du protocole SSH), il y a à nouveau échange de clés, ce qui produit un autre ensemble de valeurs repère et une autre valeur secrète partagée. De cette façon, même si un hacker réussit à déterminer les valeurs repère et la valeur secrète partagée au départ, il doit refaire l'opération chaque fois qu'un nouvel échange de clés se fait s'il désire continuer d'intercepter la communication.

Authentification

Une fois que la couche transport a créé un tunnel sécurisé pour envoyer les informations entre les deux systèmes, le serveur indique au client quelles sont les différentes méthodes d'authentification prises en charge, telles que l'utilisation d'une signature chiffrée privée ou l'entrée d'un mot de passe. Le client doit ensuite essayer de s'authentifier au serveur au moyen d'une des méthodes spécifiées.

Etant donné que les serveurs peuvent être configurés de façon à permettre différents types d'authentification, cette méthode donne aux deux parties un niveau de contrôle optimal. Le serveur peut décider quelles méthodes d'authentification prendre en charge en fonction de son modèle de sécurité et le client peut choisir l'ordre des méthodes d'authentification à utiliser parmi celles qui sont disponibles. Grâce à la nature sécurisée de la couche transport SSH, même les méthodes d'authentification qui, de prime abord, semblent non sécurisées, telles que l'authentification d'ordinateur hôte, peuvent être utilisées en toute sécurité.

La plupart des utilisateurs exigeant un shell sécurisé procèdent à l'authentification au moyen d'un mot de passe. Comme ce mot de passe est complètement chiffré, il peut être envoyé sans problème sur n'importe

quel réseau.

Connexion

Après avoir effectué avec succès l'authentification au moyen de la couche transport SSH, des *canaux* multiples sont ouverts en transformant la connexion simple entre les deux systèmes en connexion multiplex[1]. Chaque canal peut ainsi s'occuper de la communication d'une session de terminal différente, du transfert d'informations X11 ou de tout autre service séparé essayant d'utiliser la connexion SSH.

Le client et le serveur peuvent tous deux créer un nouveau canal et chaque canal reçoit un numéro différent aux deux extrémités de la connexion. Lorsque le client essaye d'ouvrir un nouveau canal, les clients envoient le numéro du canal accompagné de la requête. Cette information est stockée par le serveur et utilisée pour adresser la communication à ce canal. Ainsi, des types différents de session ne peuvent se nuire entre eux et, lorsqu'une session se termine, son canal peut être fermé sans que la connexion SSH primaire ne s'interrompe.

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 par 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, selon le type de service demandé par le client et le mode de connexion de l'utilisateur au réseau. Ceci permet de gérer facilement différents types de connexions distantes sans devoir changer l'infrastructure de base du protocole.

Notes

[1] Une connexion multiplex envoie plusieurs signaux sur un support commun et partagé. Avec le protocole SSH, divers canaux sont envoyés sur une connexion sécurisée commune.

Précédent
Séquence des événements d'une connexion SSH

Sommaire
Niveau supérieur

Suivant
Fichiers de configuration d'OpenSSH

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` :

- `moduli` — contient les groupes Diffie-Hellman utilisés pour l'échange de clés Diffie-Hellman qui est crucial pour la création d'une couche transport sécurisée. Lorsque les clés sont échangées au début d'une session SSH, une valeur secrète partagée qui ne peut être déterminée par aucune des parties seule est créée. Cette valeur est ensuite utilisée pour accorder l'authentification 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 `sshd`.
- `ssh_host_dsa_key` — clé DSA privée utilisée par `sshd`.
- `ssh_host_dsa_key.pub` — clé DSA publique utilisée par `sshd`.
- `ssh_host_key` — clé RSA privée utilisée par `sshd` pour la version 1 du protocole SSH.
- `ssh_host_key.pub` — clé RSA publique utilisée par `sshd` pour la version 1 du protocole SSH.
- `ssh_host_rsa_key` — clé RSA privée utilisée par `sshd` pour la version 2 du protocole SSH.
- `ssh_host_rsa_key.pub` — clé RSA publique utilisée par `sshd` pour la version 2 du protocole SSH.

Les informations de configuration SSH spécifiques à l'utilisateur sont stockées dans son répertoire personnel à l'intérieur du répertoire `~/.ssh/` :

- `authorized_keys` — ce fichier contient une liste de clés publiques "autorisées". Si un utilisateur se connecte et prouve qu'il connaît la clé privée correspondant à l'une de ces clés, il obtient l'authentification. Notez qu'il ne s'agit que d'une méthode d'authentification facultative.
- `id_dsa` — contient l'identité d'authentification DSA de l'utilisateur.
- `id_dsa.pub` — la clé DSA publique de l'utilisateur.
- `id_rsa` — la clé RSA publique utilisée par `sshd` pour la version 2 du protocole SSH.
- `identity` — la clé RSA privée utilisée par `sshd` pour la version 1 du protocole SSH.
- `known_hosts` — Ce fichier contient les clés hôte DSA des serveurs SSH auxquels l'utilisateur s'est connecté. Ce fichier est très important car il garantit que le client SSH se connecte au bon serveur SSH. Si une clé hôte a changé et que vous ne savez pas pourquoi, vous devriez contacter

l'administrateur système du serveur SSH pour vous assurer que le serveur n'a pas été compromis. Si les clés hôte d'un serveur sont modifiées par une nouvelle installation de Red Hat Linux à la prochaine connexion au serveur vous serez averti que la clé hôte stokée dans le fichier `known_hosts` ne correpond pas. Pour vous connecter au serveur, ouvrez le fichier `known_hosts` dans un éditeur de texte et effacez la clé de cet hôte. Ceci permet au client SSH de créer une nouvelle clé hôte.

Veuillez lire les pages de manuel concernant `ssh` et `sshd` pour avoir plus de détails sur les différentes directives disponibles dans les fichiers de configuration SSH.

Précédent
Couches de sécurité SSH

Sommaire
Niveau supérieur

Suivant
Beaucoup plus qu'un shell sécurisé

Beaucoup plus qu'un shell sécurisé

Une interface sécurisée en ligne de commande n'est que la première des nombreuses façons dont SSH peut être utilisé. En ayant la quantité nécessaire de bande passante, les sessions X11 peuvent être dirigées sur un canal SSH ou bien, en utilisant la retransmission TCP/IP, les connexions par port entre systèmes, considérées auparavant comme étant non sécurisés, peuvent être appliquées à des canaux SSH spécifiques.

Retransmission X11

Ouvrir une session X11 par le biais d'une connexion SSH établie est aussi facile que d'exécuter un programme X sur le système local. Lorsqu'un programme X est exécuté à partir de l'invite 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 par ce canal de façon transparente.

La retransmission X11 peut être très utile. Vous pourriez, par exemple, l'utiliser pour créer une session sécurisée et interactive sur le serveur avec `up2date` pour mettre à jour des paquetages. Pour ce faire, connectez-vous au serveur en utilisant `ssh` et entrez :

```
up2date &
```

Le système vous demandera de fournir le mot de passe root pour le serveur. Ensuite, l' **agent de mise à jour Red Hat** s'affiche à l'écran et vous pouvez mettre à jour vos paquetages sur le serveur comme si vous étiez confortablement assis devant cette machine.

Retransmission de port

Grâce à SSH vous pouvez sécuriser des protocoles TCP/IP via la retransmission de port. Lorsque vous utilisez cette technique, le serveur SSH devient un conduit crypté vers le client SSH.

La retransmission de port mappe un port local du client vers un port distant du serveur. SSH permet de mapper tous les ports du serveur vers tous les ports du client. Les numéros de port ne doivent pas correspondre pour que le mappage ait lieu.

Pour créer un canal de retransmission de port TCP/IP qui attend les connexions sur l'hô,te local, utilisez la commande suivante :

```
ssh -L port-local:nomhôte-distant:port-distant nomutilisateur@nomhôte
```

Note **Remarque**

Afin de pouvoir définir la retransmission TCP/IP pour qu'elle puisse être en mode réception des ports inférieurs à 1024, il est nécessaire d'avoir un accès super-utilisateur.

Par exemple, si vous voulez vérifier votre courrier sur un serveur appelé mail.domain.com au moyen du protocole POP et avec une connexion cryptée, utilisez la commande ci-dessous :

```
ssh -L 1100:mail.domain.com:110 mail.domain.com
```

Une fois que le canal de retransmission de port est en place entre les deux ordinateurs, vous pouvez diriger votre client POP mail pour qu'il utilise le port 1100 sur l'hô,te local afin de vérifier le nouveau courrier. Toute requête envoyée au port 1100 de votre système sera dirigée de façon sécurisée au serveur mail.domain.com.

Si mail.domain.com n'exécute aucun démon de serveur SSH, mais que vous pouvez tout de même vous connecter via SSH à un ordinateur du même réseau, vous pouvez toujours utiliser SSH pour sécuriser la partie de connexion POP. Dans ce cas, la commande est légèrement différente :

```
ssh -L 1100:mail.domain.com:110 other.domain.com
```

Dans cet exemple, vous transférez votre requête POP du port 1100 de votre ordinateur au moyen de la connexion SSH au port 22 de other.domain.com. Ensuite, `other.domain.com` se connecte au port 110 de `mail.domain.com` pour vous permettre de vérifier votre courrier. Avec cette technique, seule la connexion entre votre système et `other.domain.com` est sécurisée.

La retransmission TCP/IP peut être très utile pour obtenir des informations de façon sécurisée à travers un pare-feu. Si le pare-feu est configuré de façon à permettre le trafic SSH par son port standard (22), mais bloque l'accès aux autres ports, une connexion entre deux ordinateurs hôtes qui utilisent des ports bloqués est tout de même possible en redirigeant leur communication sur une connexion SSH établie entre eux.

Note **Remarque**

L'utilisation de la retransmission de port pour transférer des connexions de cette façon permet à tout utilisateur sur le système client de se connecter au service auquel vous transférez des connexions. Si le système client est compromis, les hackers auront également accès aux services retransmis.

Les administrateurs système concernés par 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 redémarrer le service `sshd`.

Précédent
Fichiers de configuration d'OpenSSH

Sommaire
Niveau supérieur

Suivant
Exiger SSH pour les connexions à distance

Exiger SSH pour les connexions à distance

Afin que le protocole SSH soit vraiment efficace et protège vos connexions réseau, vous devez absolument cesser d'utiliser des protocoles de connexion non sécurisés, tels que `telnet` et `rsh`. Autrement, le mot de passe d'un utilisateur pourrait être protégé au moyen de `ssh`, mais être capté lors d'une connexion ultérieure de ce même utilisateur au moyen de `telnet`.

Pour désactiver des méthodes de connexion non sécurisées sur votre système, utilisez le programme à ligne de commande `chkconfig`, le programme ncurses `ntsysv` ou l'application graphique **serviceconf**. Tous ces outils demandent les privilèges du super-utilisateur.

Ci-dessous quelques services que vous devez désactiver :

- `telnet`
- `rsh`
- `ftp`
- `rlogin`
- `wu-ftpd`
- `vsftpd`

Pour plus d'informations sur les niveaux d'exécution et la configuration des services à l'aide de `chkconfig`, `ntsysv` et **serviceconf**, consultez le chapitre *Contrôle de l'accès aux services* du *Guide de personnalisation officiel Red Hat Linux*.

Chapitre 11. Kerberos

Kerberos est un protocole d'authentification réseau créé par MIT et utilisant une cryptographie à clés secrètes pour sécuriser les mots de passe sur le réseau. Le fait de coder les mots de passe à l'aide de Kerberos permet d'éviter que des utilisateurs non autorisés essaient d'intercepter des mots de passe sur le réseau, et ajoute donc une nouvelle couche de sécurité sur le réseau.

Avantages de Kerberos

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

Cependant, dans certains services, la transmission des mots de passe s'effectue sous forme de texte en clair. Tout pirate de système ayant accès au réseau et à un analyseur de paquets (généralement appelé "sniffer" de paquets) peut intercepter tout mot de passe envoyé de cette manière.

Le principe de base ayant présidé à la conception de Kerberos est d'éliminer la transfert de mots de passe en texte clair sur un réseau. L'utilisation appropriée de Kerberos éliminera le risque de "sniffers" de paquets interceptant des mots de passe sur votre réseau .

Désavantages de Kerberos

Kerberos permet d'éliminer une menace commune pour la sécurité, mais plusieurs raisons font que Kerberos peut être difficile à implémenter :

- Il n'existe pas de solution rapide pour la migration de mots de passe utilisateur d'une base de données de mots de passe UNIX standard (par exemple `/etc/passwd` ou `/etc/shadow`) vers une base de données de mots de passe Kerberos. Consultez le site (Question 2.23) ou la section la section intitulée *Autres ressources* pour obtenir des informations plus détaillées sur ce point.
- Kerberos n'est que partiellement compatible avec le système PAM (Pluggable Authentication Module, module d'authentification enfichable) utilisé par la plupart des serveurs exécutant Red Hat Linux. Pour plus d'informations, reportez-vous à la la section intitulée *Kerberos et PAM (modules d'authentification enfichables)*.
- Pour qu'une application utilise Kerberos, ses sources doivent être modifiées afin de faire les appels appropriés dans les bibliothèques Kerberos. Pour certaines applications, ceci peut exiger un effort de programmation trop important. Pour d'autres, des modifications doivent être apportées au protocole utilisé entre les serveurs de réseau et leurs clients ; une fois encore, il se peut que l'effort requis soit trop important. En outre, il peut être impossible de faire fonctionner avec Kerberos certaines applications dont les sources ne sont pas accessibles.
- Kerberos suppose que vous utilisiez des hôtes sécurisés sur un réseau non sécurisé. Son but principal est d'empêcher l'envoi de mots de passe en texte clair sur le réseau. Si quelqu'un d'autre que l'utilisateur normal a physiquement accès à l'un des hôtes, et en particulier à celui qui délivre les tickets d'authentification, tout le système d'authentification Kerberos est menacé d'être compromis.
- Enfin, si vous décidez d'utiliser Kerberos sur votre réseau, sachez qu'il s'agit d'un pari du type "tout ou rien". N'oubliez pas que tous les mots de passe transférés à un service n'utilisant pas Kerberos pour l'authentication courent le risque d'être interceptés par des sniffers, et votre réseau ne tirera aucun avantage de l'utilisation de Kerberos. Pour sécuriser votre réseau avec Kerberos, vous devez *kerbériser* () *toutes* les applications qui envoient des mots de passe en texte clair, ou ne pas utiliser du tout ces applications sur votre réseau.

Terminologie Kerberos

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

ciphertext

Données cryptées.

texte en clair

Données non codées, lisibles par l'homme.

client

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

cache de certificat d'identité ou fichier de ticket

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

hache crypté

Hache unidirectionnel utilisé pour l'authentification des utilisateurs. Plus sûr que le texte clair, mais relativement facile à décoder pour un pirate expérimenté.

clé

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

KDC (Key Distribution Center, centre distributeur de tickets)

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

key table ou keytab

Fichier contenant une liste cryptée des "principaux" et de leurs clés respectives. Les serveurs extraient les clés dont ils ont besoin des fichiers keytab au lieu d'utiliser `kinit`. Le fichier keytab

par défaut est `/etc/krb5.keytab`. La commande `/usr/kerberos/sbin/kadmind` est le seul service connu utilisant n'importe quel autre fichier (il utilise `/var/kerberos/krb5kdc/kadm5.keytab`).

principal

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

realm

Un réseau utilisant Kerberos, composé d'un ou plusieurs serveurs (appelés également KDC) et un nombre potentiel très élevé de clients.

service

Programme accessible via le réseau.

ticket

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

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

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

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

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

Précédent | Sommaire | Suivant
Désavantages de Kerberos | Niveau supérieur | Fonctionnement de Kerberos

Fonctionnement de Kerberos

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

Sur un réseau "normal" utilisant des mots de passe pour authentifier les utilisateurs, lorsqu'un utilisateur demande un service réseau nécessitant une authentification, il est invité à entrer son mot de passe. Celui-ci est transmis sous forme de texte en clair ou de hache crypté via le réseau, et l'accès au service réseau est autorisé. Malheureusement, cela signifie que toute personne interceptant des paquets sur le réseau peut potentiellement trouver le nom d'utilisateur et le mode de passe des utilisateurs du réseau.

Pour contrer ce problème, Kerberos utilise un cryptage symétrique et un programme fiable — connu sous le nom de KDC — afin d'authentifier les utilisateurs sur un réseau. Une fois l'authentification effectuée, Kerberos stocke un ticket spécifique à cette session sur l'ordinateur de l'utilisateur et les services kerbérisés rechercheront ce ticket au lieu de demander à l'utilisateur de s'authentifier à l'aide d'un mot de passe.

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

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

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

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

Avertissement **Avertissement**

Le système Kerberos peut être compromis à chaque fois qu'un utilisateur présent sur le réseau un service non "kerbérisé" en envoyant un mot de passe en texte en clair. L'utilisation de versions de services non "kerbérisées" devrait être déconseillée. Parmi ces services, on retrouve telnet et ftp. L'utilisation d'autres protocoles sûrs, tels que les services sécurisés OpenSSH ou SSL, est acceptable.

Ceci est bien sûr une présentation générale du fonctionnement typique de l'authentification de Kerberos sur un réseau. Pour obtenir des informations plus détaillées sur ce sujet, reportez-vous à la la section intitulée *Autres ressources*.

Note **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 ordinateurs du réseau. Si vous n'avez pas installé de programme de synchronisation d'horloge pour le réseau, vous allez devoir le faire. Etant donné que certains aspects de Kerberos reposent sur le DNS (Domain Name Service), veillez à ce que les entrées DNS et les hôtes sur le réseau soient tous correctement configurés. Pour plus d'informations, reportez-vous au Guide de l'administrateur système Kerberos V5, disponible aux formats PostScript et HTML dans `/usr/share/doc/krb5-server-`*`numéro-version`*, (où *`numéro-version`* correspond à la version installée sur le système).

Précédent: Terminologie Kerberos
Sommaire
Niveau supérieur
Suivant: Kerberos et PAM (modules d'authentification enfichables)

Kerberos et PAM (modules d'authentification enfichables)

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

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

La section suivante va décrire de quelle façon configurer un serveur Kerberos de base.

Configurer un serveur Kerberos 5

Lors de la configuration de Kerberos, installez tout d'abord le serveur. Si vous devez configurer des serveurs esclaves, les détails des relations de configuration entre les serveurs maître et esclaves sont présentées dans le *Guide d'installation Kerberos V5* (dans le `/usr/share/doc/krb5-server-<numéro-de-version>`).

Pour installer un serveur Kerberos :

1. Assurez-vous que la synchronisation de l'horloge et le DNS fonctionnent sur votre serveur avant d'installer Kerberos 5. Prêtez une attention toute particulière à la synchronisation de l'heure entre le serveur Kerberos et ses différents clients. Si les horloges du serveur et du client diffèrent de plus de cinq minutes (ce chiffre par défaut est configurable dans Kerberos 5), les clients ne pourront pas s'authentifier sur le serveur. Cette synchronisation de l'horloge est nécessaire pour empêcher un agresseur d'utiliser un ancien authentificateur pour se déguiser en un utilisateur valide.

   Vous devriez configurer un réseau client/serveur compatible NTP (protocole de synchronisation de réseau) à l'aide de Red Hat Linux, même si vous n'utilisez pas Kerberos. Red Hat Linux 7.3 inclut le paquetage `ntp` afin de faciliter l'installation. Pour obtenir des informations complémentaires sur NTP, consultez http://www.eecis.udel.edu/~ntp.
2. Installez les paquetages `krb5-libs`, `krb5-server` et `krb5-workstation` sur la machine sur laquelle tournera votre KDC. Cette machine doit être sécurisée — si possible ; elle ne devrait pas exécuter de services autres que le KDC.

   Si vous souhaitez utiliser un utilitaire d'interface utilisateur graphique GUI pour gérer Kerberos, vous devez également installer le paquetage `gnome-kerberos`. Celui-ci contient `krb5`, un outil GUI pour gérer les tickets, et `gkadmin`, un outil GUI pour gérer les zones de Kerberos.
3. Editez les fichiers de configuration `/etc/krb5.conf` et `/var/kerberos/krb5kdc/kdc.conf` afin de refléter votre nom de zone et les configurations domaine-à-zone. Une simple zone peut être construite en remplaçant les instances de *`EXEMPLE.COM`* et *`exemple.com`* avec votre nom de domaine — assurez-vous de bien garder les noms en majuscules et minuscules dans le format approprié — et en changeant le KDC de *`kerberos.exemple.com`* par le nom de votre serveur Kerberos. Par convention, tous les noms de zones sont en majuscules et tous les noms d'hôtes DNS ainsi que les noms de domaines en minuscules. Pour obtenir des informations complètes sur les formats de ces fichiers, reportez-vous aux pages respectives de leur manuel.
4. Créez la base de données à l'aide de l'utilitaire `kdb5_util` à partir d'une invite shell :

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

La commande `create` crée la base de données qui sera utilisée pour stocker les clés de votre zone Kerberos. Le commutateur `-s` force la création d'un fichier *stash* dans lequel est stocké la clé du serveur maître. S'il n'existe aucun fichier stash à partir duquel lire la clé, le serveur Kerberos (`krb5kdc`) demandera à l'utilisateur le mot de passe du serveur maître (qui peut être utilisé pour régénérer la clé) à chaque fois qu'il sera lancé.

5. Editez le fichier `/var/kerberos/krb5kdc/kadm5.acl`. Ce fichier est utilisé par `kadmind` afin de déterminer quels éléments principaux ont accès à la base de données de Kerberos et de définir leur niveau d'accès. Une seule ligne suffira à la plupart des organisations :

```
*/admin@EXEMPLE.COM  *
```

La plupart des utilisateurs seront représentés dans la base de données par un seul élément principal (avec une instance *NULL*, ou vide, telle que *joe@EXEMPLE.COM*). Avec cette configuration, les utilisateurs ayant un second élément principal avec comme instance *admin* (par exemple, *joe/admin@EXEMPLE.COM*) pourront exercer un pouvoir total sur la base de données Kerberos de la zone.

Une fois `kadmind` lancé sur le serveur, n'importe quel utilisateur pourra accéder à ses services en exécutant `kadmin` ou `gkadmin` sur tous les clients ou serveurs de la zone. Toutefois, les utilisateurs non spécifiés dans le fichier `kadm5.acl` ne pourront en aucun cas modifier la base de données ; le seul changement qu'il leur sera possible d'effectuer sera celui de leurs propres mots de passe.

Note **Remarque**

Les utilitaires `kadmin` et `gkadmin` communiquent avec le serveur `kadmind` sur le réseau et ils utilisent Kerberos pour gérer l'authentification. Bien sûr, vous devez créer le premier élément principal avant de pouvoir vous connecter au serveur sur le réseau afin qu'il puisse le gérer. Pour ce faire, utilisez la commande `kadmin.local`, qui est spécifiquement conçue pour être utilisée sur le même hôte que le KDC et qui n'emploie pas Kerberos pour l'authentification.

Tapez la commande `kadmin.local` suivante au terminal KDC afin de créer le premier élément principal :

```
/usr/kerberos/sbin/kadmin.local -q "addprinc nom-d'utilisateur/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 éléments principaux pour vos utilisateurs à l'aide de la commande `addprinc` avec `kadmin` ou à l'aide de l'optionde menu **Principal** => **Add** dans `gkadmin`. `kadmin` et `kadmin.local`, sur le KDC maître, sont des interfaces de ligne de commande pour le système d'administration de Kerberos. En tant que telles, de nombreuses commandes sont disponibles après le lancement du programme `kadmin`. Veuillez vous référez à la page de manuel `kadmin` pour plus d'informations.
8. Vérifiez que votre serveur émettra bien des tickets. Tout d'abord, exécutez `kinit` afin d'obtenir un ticket et de le stocker dans un fichier cache de certificats d'identité. Utilisez ensuite `klist` afin de visualiser la liste des certificats d'identité dans votre cache et utilisez `kdestroy` pour détruire le cache ainsi que les certificats qu'il contient.

Note **Remarque**

Par défaut, `kinit` tente de vous authentifier en utilisant le nom d'utilisateur de connexion du compte utilisé lorsque vous vous êtes connecté pour la première fois à votre système (pas au serveur Kerberos). Si le nom d'utilisateur de ce système ne correspond pas à un élément principal dans votre base de données Kerberos, un message d'erreur s'affichera. Le cas échéant, indiquez simplement à `kinit` le nom de votre élément principal en tant qu'argument sur la ligne de commande (`kinit` *`élément principal`*).

Une fois les étapes ci-dessus réalisées, votre serveur Kerberos devrait être opérationnel. Vous devrez ensuite configurer vos clients Kerberos.

Précédent
Kerberos et PAM (modules d'authentification enfichables)

Sommaire
Niveau supérieur

Suivant
Configurer un client Kerberos 5

Configurer 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 "kerbérisées" de `rsh` et `rlogin` nécessiteront également des changements au niveau de la configuration.

1. Assurez-vous que la synchronisation de l'heure est effective entre le client Kerberos et le KDC. Reportez-vous à la section intitulée *Configurer un serveur Kerberos 5* afin d'obtenir davantage d'informations. DNS doit également fonctionner correctement sur le client Kerberos avant d'installer les programmes de ce client.
2. Installez les paquetages `krb5-libs` et `krb5-workstation` sur tous les clients de votre zone. Vous devez fournir votre propre version de `/etc/krb5.conf` pour les stations de travail de vos clients ; cela peut généralement être le même `krb5.conf` que celui utilisé par le KDC.
3. Avant qu'une station de travail donnée de votre zone puisse permettre aux utilisateurs de se connecter à l'aide des commandes `rsh` et `rlogin` "kerbérisées", le paquetage `xinetd` devra y être installé et l'élément principal de l'hôte propre à la station devra être présent dans la base de données Kerberos. Les programmes de serveur `kshd` et `klogind` auront également besoin d'un accès aux clés pour l'élément principal de leur service.

   A l'aide de `kadmin`, ajoutez un élément principal d'hôte pour la station de travail. L'instance sera dans ce cas le nom d'hôte de la station. Parce que vous n'aurez jamais besoin de taper à nouveau le mot de passe pour cet élément principal, vous ne voudrez probablement pas perdre de temps à chercher un bon mot de passe. Vous pouvez utiliser l'option `-randkey` de la commande `addprinc` de kadmin afin de créer l'élément principal et de lui attribuer une clé aléatoire :

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

   Maintenant que vous avez créé l'élément principal, vous pouvez extraire les clés de la station de travail en exécutant `kadmin` *sur la station de travail elle-même* et utiliser la commande `ktadd` dans `kadmin` :

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

Afin d'utiliser les versions "kerbérisées" de `rsh` et de `rlogin`, vous devez activer `klogin`, `eklogin` et `kshell`. [1]

4. D'autres services de réseau "kerbérisés" devront être lancés. Pour utiliser la commande `telnet` kerbérisée, vous devez activer `krb5-telnet`. [1]

   Afin de fournir un accès FTP, créez puis extrayez une clé pour un élément principal avec un root de ftp, l'instance étant configurée au nom d'hôte du serveur ftp. Activez ensuite `gssftp`. [1]

   Le serveur IMAP inclus dans le paquetage `imap` utilisera l'authentification GSS-API à l'aide de Kerberos 5 s'il parvient à trouver la clé appropriée dans `/etc/krb5.keytab`. Le root de l'élément principal doit être `imap`. Le gserveur CVS utilise un élément principal avec un root de `cvs` et est en dehors de cela identique à un `pserver`.

Ceci devrait couvrir toutes les informations dont vous avez besoin pour configurer une zone Kerberos simple.

Notes

[1] Reportez-vous au chapitre intitulé *Contrôle de l'accès aux services* dans le *Guide de personnalisation officiel Red Hat Linux* afin d'obtenir des détails sur l'activation des services.

Autres ressources

Pour plus d'informations sur Kerberos, reportez-vous aux sources d'information suivantes.

Documentation installée

- `/usr/share/doc/krb5-server-<numéro-version>` — Le *Guide d'installation Kerberos V5* et le *Guide de l'administrateur système Kerberos V5*, aux formats PostScript et HTML. Le paquetage RPM `krb5-server` doit être installé.
- `/usr/share/doc/krb5-workstation-<numéro-version>` — Le *Guide de l'utilisateur Kerberos V5 UNIX*, aux formats PostScript et HTML. Le paquetage RPM `krb5-workstation` doit être installé.

Sites Web utiles

- http://web.mit.edu/kerberos/www — La page *Kerberos: The Network Authentication Protocol* sur le site Web du MIT.
- http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html — Le Forum Aux Questions (FAQ) de Kerberos.
- ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS — Lien vers la version PostScript de *Kerberos: An Authentication Service for Open Network Systems* par Jennifer G. Steiner, Clifford Neuman et Jeffrey I. Schiller. Il s'agit du document original décrivant Kerberos.
- http://web.mit.edu/kerberos/www/dialogue.html — *Designing an Authentication System: a Dialogue in Four Scenes* écrit par Bill Bryant en 1988, puis modifié par Theodore Ts'o en 1997. Ce document relate une conversation entre deux développeurs réfléchissant à la création d'un système d'authentification de type Kerberos. La présentation sous forme de dialogue en font un bon point de départ pour les néophytes.
- http://www.ornl.gov/~jar/HowToKerb.html — *How to Kerberize your Site* (Comment "kerbébériser" votre site).

Chapitre 12. Installation et configuration de Tripwire

Le logiciel Tripwire aide à assurer l'intégrité de répertoires et de systèmes de fichiers importants en identifiant tout changement apporté à ceux-ci. Les options de configuration de Tripwire comprennent notamment l'envoi de messages d'alerte par courrier électronique lorsqu'un fichier spécifique est modifié et la vérification automatique de l'intégrité du système par l'entremise de`cron`. L'utilisation de Tripwire pour détecter des intrusions dans le système et analyser les dommages causés, vous aide à contrôler les changements apportés au système et accélère la vitesse de sa remise en état lorsqu'il est victime d'une violation, en réduisant le nombre de fichiers devant être restaurés pour le réparer.

Tripwire compare des fichiers et des répertoires avec des informations, telles que des emplacements de fichier, des dates de modification de fichier et d'autres données de ce genre, contenues dans une base de données référentielle. Il crée cette base de données en faisant un instantané de répertoires et de fichiers spécifiques dont l'état est certain et sécuritaire. (Pour avoir un maximum de sécurité, Tripwire devrait être installé et sa base de données référentielle créée avant que le système ne coure le risque d'être victime d'une intrusion.) Une fois la base de données référentielle créée, Tripwire compare le système en cours avec cette base de données et produit un rapport des modifications, des suppressions et des ajouts effectués.

Avertissement **Avertissement**

Bien qu'étant un outil valide qui permet de contrôler l'état de sécurité de votre système, Tripwire n'est pas pris en charge par Red Hat, Inc.. Pour obtenir des options de support, contactez Tripwire, Inc. (http://www.tripwire.com).

Comment utiliserTripwire

L'organigramme suivant illustre comment utiliser Tripwire :

Figure 12-1. Comment utiliser Tripwire

Suivez les étapes suivantes pour installer, utiliser et maintenir correctement Tripwire :

1. *Installation de Tripwire et personnalisation du fichier de politiques* — si ce n'est déjà fait, installez le RPM `tripwire` (voir la la section intitulée *Instructions d'installation du RPM*). Ensuite, personnalisez les exemples de fichiers de configuration (`/etc/tripwire/twcfg.txt`) et de politiques (`/etc/tripwire/twpol.txt`) et exécutez le script de configuration (`/etc/tripwire/twinstall.sh`). Pour plus de détails, reportez-vous à la la section intitulée *Instructions à suivre après l'installation*.
2. *Initialisation de la base de données de Tripwire* — créez une base de données des fichiers système critiques devant être contrôlés en fonction des directives contenues dans le tout nouveau fichier de politiques Tripwire signé(`/etc/tripwire/tw.pol`). Consultez la la section intitulée *Initialisation de la base de données* pour en savoir plus.
3. *Exécution d'une vérification d'intégrité Tripwire* — comparez la base de données de Tripwire nouvellement créée avec les fichiers système pour vérifier s'il en manque ou si certains d'entre eux ont été modifiés. Reportez-vous à la la section intitulée *Exécution d'une vérification d'intégrité* pour avoir plus de renseignements à ce sujet.
4. *Analyse d'un fichier rapport de Tripwire* — visualisez le fichier rapport Tripwire au moyen de `twprint` afin d'identifier les violations d'intégrité du système. Pour en savoir plus, reportez-vous à la la section intitulée *Impression des rapports*.
5. *Prise de mesures appropriées* — si les fichiers contrôlés ont été modifiés de façon non voulue, deux choix s'offrent à vous : vous pouvez remplacer les fichiers originaux par des copies de sauvegarde ou tout simplement réinstaller le programme.
6. *Mise à jour du fichier de la base de données de Tripwire* — si les violations de l'intégrité du système sont intentionnelles, dans le cas où vous avez modifié un fichier volontairement ou remplacé un programme donné par exemple, vous devez indiquer au fichier de la base de données Tripwire de ne plus souligner ces violations dans les rapports suivants. Pour plus de détails, veuillez lire la la section intitulée *Mise à jour de la base de données après une vérification d'intégrité*.
7. *Mise à* si vous avez besoin de changer la liste des fichiers contrôlés par Tripwire ou la façon dont les violations d'intégrité sont traitées, vous devez mettre à jour votre exemple de fichier de politiques (`/etc/tripwire/twpol.txt`), régénérer une copie signée (`/etc/tripwire/tw.pol`) et mettre à jour votre base de données Tripwire. Pour plus de renseignements, reportez-vous à la la section intitulée *Mise à jour du fichier de politiques*.

Pour obtenir des instructions plus détaillées sur ces différentes étapes, consultez les sections de ce chapitre les concernant.

Instructions d'installation

Une fois installé, Tripwire doit être initialisé correctement afin de contrôler de façon efficace vos fichiers. Les sections qui suivent expliquent comment installer le programme (s'il n'est pas déjà sur votre système) et comment initialiser la base de données de Tripwire.

Instructions d'installation du RPM

La façon la plus simple d'installer Tripwire est d'installer le RPM `tripwire` lors du processus d'installation de Red Hat Linux 7.3. Toutefois, si Red Hat Linux 7.3 est déjà installé, vous pouvez utiliser **RPM**, **Gnome-RPM**, ou **Kpackage** pour installer le RPM Tripwire à partir des CD-ROM de Red Hat Linux 7.3. Les étapes suivantes illustrent le processus d'installation faisant usage de **RPM**:

1. Localisez le répertoire `RedHat/RPMS` sur le CD-ROM de Red Hat Linux 7.3.

2. Localisez le RPM binaire `tripwire` en tapant `ls -l tripwire*` dans le répertoire `RedHat/RPMS`.
3. Entrez `rpm -Uvh <`*`nom`*`>` (où <*nom*> correspond au nom du RPM Tripwire trouvé à l'étape 2).
4. Une fois le RPM `tripwire` installé, suivez les instructions ci-dessous, qui soulignent ce qui doit être fait après l'installation.

Note **Remarque**

Les notes de mise à jour et le fichier `README` sont situés dans le fichier `/usr/share/doc/tripwire-<`*`numéro-version`*`>`. Ces documents contiennent d'importantes informations sur le fichier de politiques par défaut et d'autres sujets.

Instructions à suivre après l'installation

Le RPM `tripwire` installe les fichiers du programme nécessaires au bon fonctionnement du logiciel. Une fois Tripwire installé, vous devez le configurer pour votre système, comme l'expliquent les étapes suivantes :

1. Si vous savez déjà quelles modifications doivent être apportées au fichier de configuration (`/etc/tripwire/twcfg.txt`) ou au fichier de politiques

(`/etc/tripwire/twpol.txt`), effectuez-les maintenant.

Note **Remarque**

Bien que vous deviez modifier les fichiers de configuration et de politiques pour personnaliser Tripwire selon vos besoins spécifiques, la modification de ces fichiers n'est pas obligatoire pour pouvoir utiliser Tripwire. Cependant, si vous prévoyez de les modifier, vous devez apporter les changements avant d'exécuter le script de configuration (`/etc/tripwire/twinstall.sh`) car si vous le faites après l'exécution du script de configuration, vous devrez l'exécuter à nouveau avant d'initialiser le fichier de la base de données. Rappelez-vous que vous *pouvez* modifier les fichiers de configuration et de politiques *après* avoir initialisé le fichier de la base de données et exécuté une vérification d'intégrité.

2. Entrez `/etc/tripwire/twinstall.sh` à la ligne de commande en tant que root et appuyez sur la touche [Entrée] pour exécuter le script de configuration. Le script `twinstall.sh` vous fait parcourir le processus permettant de définir des phrases d'accès, de générer des clés cryptographiques qui protègent les fichiers de configuration et de politiques de Tripwire et de signer ces fichiers. Reportez-vous à la la section intitulée *Sélection des phrases d'accès* pour avoir plus de renseignements concernant la définition des phrases d'accès.

   Note **Remarque**

   Une fois codés et signés, le fichier de configuration (`/etc/tripwire/tw.cfg`) et le fichier de politiques (`/etc/tripwire/tw.pol`) générés lors de l'exécution du script `/etc/tripwire/twinstall.sh`, ne doivent pas être renommés ou déplacés.

3. Initialisez le fichier de la base de données de Tripwire en entrant la commande `/usr/sbin/tripwire --init` à la ligne de commande.
4. Effectuez une première vérification d'intégrité du système pour comparer la nouvelle base de données de Tripwire avec vos fichiers système, au moyen de la commande `/usr/sbin/tripwire --check` à la ligne de commande et vérifiez s'il y a des erreurs dans le rapport généré.

Une fois ces étapes réalisées avec succès, Tripwire possède l'instantané référentiel de votre système de fichiers dont il a besoin pour contrôler les changements apportés aux fichiers importants. De plus, le RPM `tripwire` ajoute un fichier appelé `tripwire-check` au répertoire `/etc/cron.daily`, qui a pour but d'effectuer automatiquement une vérification d'intégrité journalière.

Installation et configuration de Tripwire | Niveau supérieur | Emplacements des fichiers

Emplacements des fichiers

Avant de commencer à utiliser Tripwire, vous devez savoir où se trouvent les fichiers importants de cette application. Tripwire stocke ses fichiers à différents endroits en fonction de leur rôle :

- Le répertoire `/usr/sbin` stocke les programmes `tripwire`, `twadmin` et `twprint`.
- Le répertoire `/etc/tripwire` contient la clé du site et la clé locale (fichiers `*.key`), le script d'initialisation (`twinstall.sh`), ainsi que les fichiers de configuration et de politiques et leur exemple.
- Le répertoire `/var/lib/tripwire` contient la base de données Tripwire des fichiers de votre système (`*.twd`) et un répertoire `report` dans lequel les rapports Tripwire sont enregistrés. Les rapports Tripwire, appelés *`nom_hôte-date_du_rapport-heure_du_rapport`*`.twr`, établissent les différences entre la base de données de Tripwire et les fichiers de votre système.

Composants de Tripwire

Le fichier de politiques de Tripwire est un fichier texte qui contient des commentaires, des règles, des directives et des variables. Ce fichier dicte la façon dont Tripwire doit vérifier votre système. Chaque règle dans le fichier de politiques spécifie un objet système devant être contrôlé. Les règles indiquent également quels changements rapporter ou ignorer.

Les objets système sont les fichiers et les répertoires que vous désirez contrôler. Chaque objet est identifié par un nom. Une propriété fait référence à une caractéristique unique d'un objet que le logiciel Tripwire peut surveiller. Les directives contrôlent le traitement conditionnel d'ensembles de règles dans un fichier de politiques. Durant l'installation, le fichier texte de politiques (`/etc/tripwire/twpol.txt`) est crypté et renommé, devenant ainsi le fichier de politiques actif (`/etc/tripwire/tw.pol`).

Lorsqu'il est initialisé pour la première fois, Tripwire utilise les règles du fichier de politiques signé pour créer le fichier de la base de données (`/var/lib/tripwire/`*`nom_d'hôte`*`.twd`). Le fichier de la base de données est un instantané référentiel du système à un moment où son état est certain et sécuritaire. Tripwire compare ce fichier référentiel avec le système en cours pour déterminer si des changements ont eu lieu. Cette comparaison est appelée *vérification d'intégrité*.

Lorsque vous effectuez une vérification d'intégrité, Tripwire produit des fichiers rapport, situés dans le répertoire `/var/lib/tripwire/report`. Ces fichiers rapport indiquent toutes les modifications apportées aux fichiers violant les règles du fichier de politiques lors de la vérification d'intégrité.

Le fichier de configuration de Tripwire (`/etc/tripwire/tw.cfg`) stocke des informations spécifiques au système, telles que l'emplacement des fichiers de données de Tripwire. Tripwire génère les informations nécessaires au fichier de configuration lors de l'installation, mais l'administrateur système peut ensuite à tout moment changer les paramètres du fichier de configuration. Notez qu'un fichier de configuration modifié doit être signé, tout comme le fichier de politiques, afin de pouvoir être utilisé par défaut.

Les variables `POLFILE`, `DBFILE`, `REPORTFILE`, `SITEKEYFILE` et `LOCALKEYFILE` du fichier de configuration spécifient les emplacements du fichier de politiques, du fichier de la base de données, des fichiers rapport et des fichiers des clés du site et locale. Ces variables sont définies par défaut au moment de l'installation. Si vous modifiez le fichier de configuration et laissez l'une de ces variables non définie, le fichier de configuration sera considéré comme non valide par Tripwire. Cela provoque une erreur lors de l'exécution de `tripwire` et la fermeture du programme.

Veuillez prendre note que le fichier de configuration modifié doit être signé, tout comme le fichier de politiques, afin de pouvoir être utilisé par Tripwire. Reportez-vous à la la section intitulée *Signature du fichier de configuration* pour avoir les instructions concernant la signature du fichier de configuration.

Précédent
Emplacements des fichiers

Sommaire
Niveau supérieur

Suivant
Modification du fichier de politiques

Modification du fichier de politiques

Vous pouvez spécifier la façon dont Tripwire contrôle votre système en modifiant le fichier de politiques de Tripwire (`twpol.txt`). Si vous modifiez ce fichier en fonction de la configuration particulière de votre système, vous augmentez l'efficacité des rapports de Tripwire car vous minimisez les fausses alertes concernant des fichiers ou des programmes que vous n'utilisez pas, mais que Tripwire identifie comme étant modifiés ou manquants.

Localisez le fichier de politiques par défaut dans `/etc/tripwire/twpol.txt`. Un exemple de fichier de politiques (situé dans `/usr/share/doc/tripwire-<`*`numéro-version`*`>/policyguide.txt`) est aussi inclus pour vous aider à apprendre le langage des politiques. Lisez le fichier d'exemples de politiques pour avoir des instructions sur la façon de modifier le fichier de politiques par défaut.

Si vous modifiez le fichier de politiques immédiatement après avoir installé le paquetage `tripwire`, assurez-vous de taper `/etc/tripwire/twinstall.sh` pour exécuter le script de configuration. Ce script signe le fichier de politiques modifié et le renomme `tw.pol`. Il s'agit du fichier de politiques actif utilisé par le programme `tripwire` lorsqu'il est exécuté.

Si vous modifiez l'exemple de fichier de politiques après avoir exécuté le script de configuration, veuillez lire la la section intitulée *Mise à jour du fichier de politiques* pour savoir comment le signer afin de créer le fichier `tw.pol` requis.

Note **Remarque**

Si vous modifiez l'exemple de fichier de politiques, celui-ci n'est pas utilisé par Tripwire tant qu'il n'est pas signé, crypté et devenu le nouveau fichier `/etc/tripwire/tw.pol` (voir la la section intitulée *Mise à jour du fichier de politiques*).

Sélection des phrases d'accès

Les fichiers Tripwire sont signés ou cryptés au moyen de la clé locale et de la clé du site, qui empêchent ainsi que les fichiers de configuration, de politiques, de la base de données et des rapports ne soient visualisés ou modifiés par des individus connaissant les phrases d'accès locale ou du site. Cela signifie qu'un intrus ayant l'accès root à votre système ne peut modifier les fichiers Tripwire pour effacer ses traces sans avoir également les phrases d'accès. Lorsque vous choisissez des phrases d'accès, vous devez utiliser un minimum de 8 caractères alphanumériques et symboliques pour chaque phrase. La longueur maximum d'une phrase d'accès est de 1023 caractères. Les guillemets ne doivent pas être utilisés comme caractères pour ces phrases. De plus, assurez-vous que vos phrases d'accès sont complètement différentes du mot de passe root du système.

La clé locale et la clé du site devraient toutes deux avoir leur propre phrase d'accès. La phrase d'accès de la clé du site protège la clé du site, utilisée pour signer les fichiers de configuration et de politiques de Tripwire, alors que la clé locale signe les fichiers de la base de données et des rapports de Tripwire.

Attention **Attention**

Mettez vos phrases d'accès en lieu sûr. *Il n'existe aucun moyen de décrypter un fichier signé si vous oubliez ou perdez vos phrases d'accès.* Si cela devait se produire, les fichiers seraient alors inutilisables et vous devriez exécuter à nouveau le script de configuration, ce qui initialise encore une fois la base de données de Tripwire.

Initialisation de la base de données

Lorsque la base de donnée est initialisée, Tripwire crée un ensemble d'objets du système de fichiers en se basant sur les règles contenues dans le fichier de politiques. Cette base de données est utilisée comme référence lors des vérifications d'intégrité.

Pour initialiser la base de données de Tripwire, utilisez la commande suivante :

```
/usr/sbin/tripwire --init
```

De nombreuses minutes peuvent s'écouler avant que la commande ne soit exécutée.

Exécution d'une vérification d'intégrité

Lors d'une vérification d'intégrité, Tripwire compare les objets actuels du système de fichiers avec leurs propriétés, qui sont enregistrées dans la base de données. Les violations sont imprimées sur la sortie standard et enregistrées dans un fichier rapport accessible par la suite au moyen de `twprint`. Pour plus de détails sur la visualisation des rapports de Tripwire, consultez la la section intitulée *Impression des rapports*.

Une option de configuration de messagerie électronique dans le fichier de politiques permet d'envoyer des messages à des adresses spécifiques lorsque certaines violations de l'intégrité du système sont découvertes. Reportez-vous à la la section intitulée *Tripwire et courrier électronique* pour savoir comment la mettre en place.

Utilisez la commande suivante pour effectuer une vérification d'intégrité :

```
/usr/sbin/tripwire --check
```

En général, l'exécution de cette commande prend un peu de temps, tout dépend du nombre de fichiers à contrôler.

Impression des rapports

La commande `twprint -m r` affiche le contenu d'un rapport Tripwire en texte en clair. Vous devez préciser à `twprint` quel rapport afficher.

Une commande `twprint` pour imprimer des rapports Tripwire ressemble à ce qui suit (sur une seule ligne) :

```
/usr/sbin/twprint -m r --twrfile
          /var/lib/tripwire/report/<nom>.twr
```

L'option `-m r` de cette commande indique à `twprint` de décoder un rapport Tripwire. L'option `--twrfile` indique à `twprint` d'utiliser un fichier rapport Tripwire spécifique.

Le nom du rapport Tripwire que vous voulez visualiser contient le nom de l'hôte que Tripwire a contrôlé pour générer le rapport, ainsi que la date et l'heure de sa création. Vous pouvez à tout moment consulter des rapports enregistrés précédemment. Pour cela, vous n'avez qu'à taper `ls /var/lib/tripwire/report` pour faire apparaître une liste de rapports Tripwire.

Les rapports Tripwire peuvent être assez longs, selon le nombre de violations trouvées ou d'erreurs générées. Voici à quoi peut ressembler le début d'un de ces rapports :

```
Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:          root
Report created on:            Fri Jan 12 04:04:42 2001
Database last updated on:     Tue Jan  9 16:19:34 2001

===============================================================
Report Summary:
===============================================================
Host name:                    some.host.com
Host IP address:              10.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
```

```
Database file used:           /var/lib/tripwire/some.host.com.twd
Command line used:            /usr/sbin/tripwire --check

===============================================================================
Rule Summary:
===============================================================================
-------------------------------------------------------------------------------
Section: Unix File System
-------------------------------------------------------------------------------
  Rule Name                Severity Level    Added    Removed  Modified
  ---------                --------------    -----    -------  --------
  Invariant Directories    69                0        0        0
  Temporary directories    33                0        0        0
* Tripwire Data Files      100               1        0        0
  Critical devices         100               0        0        0
  User binaries            69                0        0        0
  Tripwire Binaries        100               0        0        0
```

Utilisation de `twprint` pour visualiser la base de données de Tripwire

Vous pouvez également utiliser `twprint` pour visualiser la base de données complète ou certaines informations sur des fichiers de votre choix dans la base de données de Tripwire. C'est très pratique pour avoir une idée de la quantité d'informations contrôlées par Tripwire sur votre système.

Pour visualiser la base de données complète de Tripwire, entrez cette commande :

```
/usr/sbin/twprint -m d --print-dbfile | less
```

Vous obtenez ainsi une grande quantité de données et les premières lignes que vous voyez ressemblent à ceci :

```
Tripwire(R) 2.3.0 Database

Database generated by:        root
Database generated on:        Tue Jan  9 13:56:42 2001
Database last updated on:     Tue Jan  9 16:19:34 2001

===============================================================
Database Summary:
===============================================================
Host name:                    some.host.com
Host IP address:              10.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/some.host.com.twd
Command line used:            /usr/sbin/tripwire --init

===============================================================
Object Summary:
===============================================================
---------------------------------------------------------------
# Section: Unix File System
---------------------------------------------------------------
     Mode        UID          Size       Modify Time
     ------      ----------   ---------- ----------
 /
     drwxr-xr-x  root (0)     XXX        XXXXXXXXXXXXXXXXX
 /bin
     drwxr-xr-x  root (0)     4096       Mon Jan  8 08:20:45 2001
 /bin/arch
     -rwxr-xr-x  root (0)     2844       Tue Dec 12 05:51:35 2000
 /bin/ash
     -rwxr-xr-x  root (0)     64860      Thu Dec  7 22:35:05 2000
 /bin/ash.static
     -rwxr-xr-x  root (0)     405576     Thu Dec  7 22:35:05 2000
```

Pour avoir des renseignements sur un fichier en particulier, contrôlé par Tripwire, tel que `/etc/hosts`, tapez une commande `twprint` différente :

```
/usr/sbin/twprint -m d --print-dbfile /etc/hosts
```

Voici à quoi ressemble le résultat :

```
Object name:  /etc/hosts

Property:               Value:
-------------           -----------
Object Type             Regular File
Device Number           773
Inode Number            216991
Mode                    -rw-r--r--
Num Links               1
UID                     root (0)
GID                     root (0)
```

Consultez la page de manuel `twprint` pour connaître d'autres options.

Précédent
Exécution d'une vérification d'intégrité

Sommaire
Niveau supérieur

Suivant
Mise à jour de la base de données après une vérification d'intégrité

Mise à jour de la base de données après une vérification d'intégrité

Lorsque Tripwire décèle des violations du système à la suite d'une vérification d'intégrité, vous devez d'abord déterminer si ces violations sont causées par des brèches du système de sécurité ou si elles sont provoquées de façon autorisée. Si, par exemple, vous avez récemment installé une application ou modifié des fichiers système critiques, Tripwire rapporte (avec raison) ces violations lors de la vérification d'intégrité. Dans ce cas précis, vous devez mettre à jour votre base de données Tripwire afin que ces changements ne soient plus considérés comme des violations du système. Toutefois, si des changements non autorisés ont été apportés à des fichiers système et provoquent des violations lors de la vérification d'intégrité, vous devez alors restaurer les fichiers originaux à partir d'une copie de sauvegarde ou réinstaller le programme.

Pour mettre à jour votre base de données Tripwire, afin qu'elle accepte les violations trouvées dans un rapport, vous devez spécifier quel rapport vous désirez utiliser pour la mise à jour de la base de données. Assurez-vous toujours d'utiliser le rapport le plus récent lorsque vous donnez la commande d'intégrer ces violations valides à la base de données. Tapez la commande suivante (sur une seule ligne), où *nom* correspond au nom du rapport à utiliser :

```
/usr/sbin/tripwire --update --twrfile
          /var/lib/tripwire/report/<nom>.twr
```

TTripwire affiche le rapport au moyen de l'éditeur de texte par défaut (spécifié dans le fichier de configuration de Tripwire à la ligne `EDITOR` line). C'est à ce moment que vous avez la possibilité de désélectionner les fichiers que vous ne désirez pas inclure dans la mise à jour de la base de données Tripwire. Il est important de ne permettre que la modification des violations autorisées du système dans la base de données.

Tous les fichiers proposés pour la mise à jour de la base de données Tripwire sont précédés d'un `[x]`. Si vous voulez spécifiquement exclure une violation valide afin qu'elle ne fasse pas partie de la mise à jour de la base de données Tripwire, enlevez le `x`. Pour accepter le changement d'un fichier précédé d'un `x`, écrivez le fichier dans l'éditeur de texte et quittez ce programme. Ce faisant, vous indiquez à Tripwire de modifier sa base de données et de ne plus rapporter les fichiers indiqués comme étant des violations du système.

Par exemple, l'éditeur de texte par défaut de Tripwire est `vi`. Pour écrire le fichier dans `vi` et apporter les changements à la base de données de Tripwire lorsque vous faites sa mise à jour à l'aide d'un rapport donné, tapez `:wq` dans le mode de commande de `vi` et appuyez sur la touche [Entrée]. On vous demande alors de fournir votre phrase d'accès. Ensuite, un nouveau fichier de la base de données est créé pour inclure les violations valides du système.

Une fois la nouvelle base de données Tripwire créée, les violations d'intégrité venant tout juste d'être autorisées ne seront plus indiquées lors des vérifications d'intégrité successives.

Précédent
Impression des rapports

Sommaire
Niveau supérieur

Suivant
Mise à jour du fichier de politiques

Mise à jour du fichier de politiques

Si vous désirez changer les fichiers que Tripwire enregistre dans sa base de données ou modifier la sévérité avec laquelle les violations sont rapportées, vous devez modifier le fichier de politiques de Tripwire.

Premièrement, apportez tous les changements nécessaires à l'exemple de fichier de politiques (`/etc/tripwire/twpol.txt`). L'un des changements couramment apportés à ce fichier est d'indiquer (mettre un # devant) tous les fichiers qui n'existent pas sur le système, afin qu'ils ne puissent générer un message d'erreur `file not found` dans les rapports de Tripwire. Si, par exemple, votre système ne possède pas le fichier `/etc/smb.conf`, vous pouvez spécifier à Tripwire de ne pas essayer de le trouver en mettant un # devant sa ligne dans `twpol.txt`, comme ceci :

```
#     /etc/smb.conf                          -> $(SEC_CONFIG) ;
```

Ensuite, vous devez indiquer à Tripwire de générer un nouveau fichier `/etc/tripwire/tw.pol` signé puis une mise à jour du fichier de la base de données en fonction des nouvelles informations contenues dans le fichier de politiques. Imaginons que `/etc/tripwire/twpol.txt` est le fichier de politiques modifié. Il faudrait alors utiliser la commande suivante :

```
/usr/sbin/twadmin --create-polfile -S site.key /etc/tripwire/twpol.txt
```

Puis, on vous demande la phrase d'accès du site ; après quoi le fichier `twpol.txt` est analysé et signé.

Il est très important que vous mettiez à jour votre base de données Tripwire après la création d'un nouveau fichier `/etc/tripwire/tw.pol`. La façon la plus efficace de le faire est d'éliminer votre base de données Tripwire existante et d'en créer une nouvelle au moyen du nouveau fichier de politiques.

Si votre fichier de base de données Tripwire s'appelle `wilbur.domain.com.twd`, entrez cette commande :

```
rm /var/lib/tripwire/wilbur.domain.com.twd
```

Ensuite, entrez la commande suivante pour créer une nouvelle base de données :

```
/usr/sbin/tripwire --init
```

Une nouvelle base de données est ainsi créée selon les instructions contenues dans le nouveau fichier de politiques. Pour vous assurer que la base de données a été correctement modifiée, faites manuellement une première vérification d'intégrité et visualisez le contenu du rapport produit. Consultez la la section intitulée *Exécution d'une vérification d'intégrité* et la la section intitulée *Impression des rapports* pour avoir des instructions plus spécifiques sur ce sujet.

Signature du fichier de configuration

Le fichier texte contenant les changements du fichier de configuration (généralement `/etc/tripwire/twcfg.txt`) doit être signé afin qu'il remplace le fichier `/etc/tripwire/tw.cfg` et qu'il soit utilisé par Tripwire lors de l'exécution des vérifications d'intégrité. Tripwire ne reconnaît aucun changement de configuration tant que le fichier texte de configuration n'est pas correctement signé et utilisé à la place du fichier `/etc/tripwire/tw.pol`.

Si votre fichier texte de configuration modifié est `/etc/tripwire/twcfg.txt`, tapez la commande suivante pour le signer et faire en sorte qu'il remplace le fichier `/etc/tripwire/tw.cfg` existant :

```
/usr/sbin/twadmin --create-cfgfile -S site.key /etc/tripwire/twcfg.txt
```

Etant donné que le fichier de configuration ne modifie pas les politiques Tripwire ou les fichiers qu'il contrôle, il est inutile de régénérer la base de données des fichiers système contrôlés.

Tripwire et courrier électronique

Tripwire peut envoyer des messages électroniques d'alerte si un type de règle spécifié contenu dans le fichier de politiques est enfreint. Pour configurer Tripwire afin qu'il exécute cette fonction, vous devez d'abord connaître l'adresse électronique du destinataire des messages en cas de violation et le nom de la règle que vous voulez surveiller. Notez également que sur les systèmes importants ayant plusieurs administrateurs système, vous pouvez faire en sorte que des groupes d'individus différents soient avertis selon les violations commises ou que personne ne soit averti lors de violations mineures.

Une fois que vous savez qui avertir et pour quelles raisons, ajoutez une ligne `emailto=` dans la section des directives des règles de chaque règle désirée. Vous n'avez qu'à ajouter une virgule après la ligne `severity=` d'une règle désirée et entrer `emailto=` sur la ligne suivante, suivi des adresses électroniques des personnes à qui vous voulez qu'un rapport de violation soit envoyé pour cette règle. Les messages seront envoyés à plus d'une personne si plusieurs adresses sont spécifiées et qu'elles sont séparées par un point-virgule.

Par exemple, si vous désirez avertir deux administrateurs, Sam et Bob, lorsqu'un programme de connexion au réseau est modifié, changez la directive de la règle des programmes de connexion au réseau dans le fichier de politiques afin qu'elle ressemble à ceci :

```
(
  rulename = "Networking Programs",
  severity = $(SIG_HI),
  emailto = bob@domain.com;sam@domain.com
)
```

Après la génération d'un nouveau fichier de politiques signé à partir du fichier `/etc/tripwire/twpol.txt`, des messages sont envoyés aux adresses électroniques indiquées dès qu'il y a violation des règles spécifiées. Si vous désirez avoir plus de détails sur la façon de signer votre fichier de politiques, reportez-vous à la la section intitulée *Mise à jour du fichier de politiques*.

Envoi d'un message électronique de test

Afin de vous assurer que la configuration de l'envoi de messages électroniques d'avertissement est correcte et que Tripwire est en mesure d'envoyer les messages, utilisez la commande suivante :

```
/usr/sbin/tripwire --test --email vos@adresses_électroniques
```

Un message de test est ainsi envoyé immédiatement par le programme `tripwire` aux adresses électroniques indiquées.

Précédent
Mise à jour du fichier de politiques

Sommaire
Niveau supérieur

Suivant
Autres ressources

Autres ressources

Tripwire peut également accomplir des tâches dont nous n'avons pas parlé au cours de ce chapitre. Aussi, pour en apprendre davantage sur Tripwire, nous vous invitons à consulter les sources d'informations supplémentaires énumérées ci-dessous.

Documentation installée

- `/usr/share/doc/tripwire-<numéro-version>` — excellent point de départ pour apprendre à personnaliser les fichiers de configuration et de politiques dans le répertoire `/etc/tripwire`.
- De plus, lisez les pages de manuel `tripwire`, `twadmin` et `twprint` pour obtenir de l'aide sur l'utilisation de ces programmes utilitaires.

Sites Web utiles

- http://www.tripwire.org — site Web du projet Open Source Tripwire, où vous trouverez les toutes dernières nouvelles sur cette application et une liste de questions fréquemment posées.

III. Références liées aux services réseau

Table des matières

13. Scripts réseau
14. Techniques de mise en oeuvre de pare-feu avec `iptables`
15. Apache
16. Courrier électronique
17. Berkeley Internet Name Domain (BIND)
18. NFS (Network File System)
19. Protocole LDAP (Lightweight Directory Access Protocol)

Chapitre 13. Scripts réseau

Avec Red Hat Linux, toutes les communications réseau se font entre des *interfaces* et les périphériques réseau connectés au système, configurés de façon spécifique, et utilisant au minimum un protocole pour échanger des données avec d'autres systèmes. Les différents types d'interfaces sont aussi divers que les périphériques qu'elles prennent en charge.

Les fichiers de configuration permettant d'activer et de désactiver les interfaces réseau et les scripts se situent dans le répertoire `/etc/sysconfig/network-scripts`. Même si certains fichiers d'interface peuvent différer d'un système à l'autre en fonction de l'utilisation, les trois types de fichiers existant dans ce répertoire, *les fichiers de configuration d'interface*, *les scripts de contrôle d'interface* et *les fichiers de fonctionnement réseau*, permettent d'activer Red Hat Linux pour utiliser les divers périphériques réseau disponibles.

Dans ce chapitre, nous allons explorer la relation entre ces fichiers et différentes options d'utilisation.

Fichiers de configuration d'interface

Les fichiers de configuration d'interface contrôlent le fonctionnement d'un périphérique d'interface réseau particulier. 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-<périphérique>`, `<périphérique>` se rapportant au nom du périphérique contrôlé par le fichier de configuration.

Interfaces Ethernet

`ifcfg-eth0` constitue l'un des fichiers d'interface les plus communs ; il contrôle la première *carte d'interface réseau*, ou *NIC* dans le système. Dans un système comportant plusieurs cartes, il y aura plusieurs fichiers `ifcfg-eth`, avec un numéro à la fin du nom de chaque fichier. Etant donné que chaque périphérique a son propre fichier de configuration, vous disposez d'un contrôle étendu sur le fonctionnement de chaque interface.

Un fichier `ifcfg-eth0` pour un système utilisant une adresse IP fixe ressemble à ce qui suit :

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
BROADCAST=10.0.1.255
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'interface 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 dans ce cas :

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

En général, vous utiliserez un utilitaire graphique, comme **Network Configurator** (`redhat-config-network`) ou `netconfig` pour procéder à des modifications des divers fichiers de configuration d'interface. Reportez-vous au *Guide de personnalisation officiel Red Hat Linux* pour obtenir des instructions sur l'utilisation de ces outils.

Vous pouvez aussi éditer manuellement le fichier de configuration pour une interface réseau donnée. Vous trouverez ci-dessous une liste de paramètres que l'on configure communément dans un fichier de configuration réseau.

Au sein de chacun des fichiers de configuration d'interface, les valeurs suivantes sont communes :

- `BOOTPROTO=<`*`protocole`*`>`, `<`*`protocole`*`>` correspondant à l'une des valeurs suivantes :
  - `none` — Aucun protocole de démarrage à utiliser.
  - `bootp` — Le protocole BOOTP doit être utilisé.
  - `dhcp` — Le protocole DHCP doit être utilisé.
- `BROADCAST=<`*`adresse`*`>`, `<`*`adresse`*`>` correspondant à l'adresse de diffusion.
- `DEVICE=<`*`nom`*`>`, `<`*`nom`*`>` correspondant au nom du périphérique physique (à l'exception des périphériques PPP à affectation dynamique, où il s'agit du *nom logique*).
- `IPADDR=<`*`adresse`*`>`, `<`*`adresse`*`>` correspondant à l'adresse IP.
- `NETMASK=<`*`masque`*`>`, `<`*`masque`*`>` correspondant à la valeur de masque de réseau.
- `NETWORK=<`*`adresse`*`>`, `<`*`adresse`*`>` correspondant à l'adresse du réseau.

- ONBOOT=<*réponse*>, <*réponse*> correspondant à l'une des valeurs suivantes :
    - yes — Ce périphérique doit être activé au démarrage.
    - no — Ce périphérique ne doit pas être activé au démarrage.
- USERCTL=<*réponse*>, <*réponse*> correspondant à l'une des valeurs suivantes :
    - true — Les utilisateurs ne faisant pas partie de la base sont autorisés à contrôler ce périphérique.
    - false — Les utilisateurs ne faisant pas partie de la base ne sont pas autorisés à contrôler ce périphérique.

Parmi les autres fichiers de configuration d'interface communs utilisant ces options : ifcfg-lo, qui contrôle le périphérique de boucle local du protocole IP, ifcfg-irlan0, qui règle les paramètres du premier périphérique infrarouge, ifcfg-plip0, qui contrôle le premier périphérique PLIP, et ifcfg-tr0, utilisé avec le premier périphérique à anneau à jeton.

Une *interface de boucle locale* est fréquemment utilisée pour les tests, ainsi que pour diverses applications nécessitant une adresse IP désignant le mê,me système. Les données envoyées au périphérique de boucle sont immédiatement renvoyées à la couche de réseau de l'hô,te.

L'interface infrarouge permet l'échange d'informations entre périphériques, comme par exemple entre un ordinateur portable et une imprimante, par l'intermédiaire d'une liaison infrarouge, fonctionnant comme un périphérique Ethernet, à la différence près que la connexion utilisée est en général une liaison d'égal à égal.

Une connexion à protocole *d'interface ligne parallèle (PLIP)* fonctionne de la même façon, mais utilise un port parallèle.

Les topologies à *anneau à jeton* ne sont plus aussi communes sur les réseaux LAN qu'elles ne l'étaient ; elles ont été doublées par Ethernet.

Interfaces commutées

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.

Ce fichier est créé automatiquement pour vous lorsque vous utilisez **RP3** ou **Kppp** pour créer un compte de numérotation. De plus, tous changements dans les réglages de compte de numérotation est inscrit dans ces fichiers de configuration d'interface. Le *Guide de démarrage officiel Red Hat Linux* contient des instructions pour l'utilisation de ces outils graphiques de connexion basée sur un modem par numérotation. Vous pouvez aussi créér et éditer ce fichier manuellement. Un fichier ifcfg-ppp0

ressemble à ce qui suit :

```
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) 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 ressemblant à `ifcfg-sl0`.

Parmi les options dont nous n'avons pas encore parlé, et qui peuvent être utilisées dans ces fichiers :

- `DEFROUTE=<`*`réponse`*`>`, `<`*`réponse`*`>` correspondant à l'une des valeurs suivantes :
  - `yes` — Cette interface est configurée comme itinéraire par défaut.
  - `no` — Cette interface n'est pas configurée comme itinéraire par défaut.
- `DEMAND=<`*`réponse`*`>`, `<`*`réponse`*`>` correspondant à l'une des valeurs suivantes :
  - `yes` — Cette interface permettra à `pppd` d'initialiser une connexion quand quelqu'un essaiera de l'utiliser.
  - `no` — Une connexion doit être établie manuellement pour cette interface.
- `IDLETIMEOUT=<`*`valeur`*`>`, `<`*`valeur`*`>` correspond au nombre de secondes d'inactivité déclenchant la déconnexion de l'interface.
- `INITSTRING=<`*`chaîne`*`>`, `<`*`chaîne`*`>` correspondant à la chaîne initiale transférée au modem. Cette option est principalement utilisée avec les interfaces SLIP .
- `LINESPEED=<`*`valeur`*`>`, `<`*`valeur`*`>` correspondant au débit en bauds du périphérique. Parmi les valeurs standards possibles : `57600`, `38400`, `19200` et `9600`, entre autres.
- `MODEMPORT=<`*`périphérique`*`>`, `<`*`périphérique`*`>` correspondant au nom du périphérique (un modem en général) utilisé pour établir la connexion pour l'interface.
- `MTU=<`*`valeur`*`>`, `<`*`valeur`*`>` correspondant au paramètre d'*unité de transfert maximum (MTU)* pour l'interface. MTU correspond au nombre maximal d'octets de données qu'un cadre peut

comporter, sans compter les informations en-tête et en-queue. Dans certaines situations de connexion commutée, si vous réglez ce paramètre sur `576`, le nombre de paquets éliminés sera moins important et le débit de connexion légèrement amélioré.

- `NAME=<nom>`, *<nom>* correspondant à la référence au titre donné à un ensemble de configurations de connexion commutée.
- `PAPNAME=<nom>`, *<nom>* correspondant au nom d'utilisateur donné durant l'échange *de protocole d'authentification du mot de passe (PAP)* suite auquel vous pouvez vous connecter à un système à distance.
- `PEERDNS=<réponse>`, *<réponse>* correspondant à l'une des valeurs suivantes :
  - `yes` — Cette interface modifiera les entrées `/etc/resolv.conf` de votre système pour utiliser les serveurs DNS fournis par le système à distance lorsqu'une connexion est établie.
  - `no` — Le fichier `/etc/resolv.conf` ne sera pas modifié.
- `PERSIST=<réponse>`, *<réponse>* correspondant à l'une des valeurs suivantes :
  - `yes` — Cette interface doit rester active en permanence, même si elle est désactivée lorsqu'un modem raccroche.
  - `no` — Cette interface ne doit pas rester active en permanence.
- `REMIP=<adresse>`, *<adresse>* correspondant à l'adresse IP du système à distance. Cette valeur n'est en général pas spécifiée.
- `WVDIALSECT=<nom>`, *<nom>* associant cette interface à une configuration de composeur dans `/etc/wvdial.conf`, contenant le numéro de téléphone à composer et d'autres informations importantes pour l'interface.

Fichiers alias et clone

Il existe deux types de fichiers de configuration d'interface moins utilisés et se trouvant dans `/etc/sysconfig/network-scripts` : les fichiers *alias* et *clone*, incluant un composant supplémentaire dans le nom du fichier.

Le format du nom des fichiers de configuration d'interface alias correspond à `ifcfg-<if-nom>:<valeur-alias>`. Ces fichiers permettent à un alias de désigner une interface. 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`. A ce point, le périphérique `eth0` est lié à une adresse IP dynamique, mais il est toujours possible d'y faire référence sur ce système via l'adresse IP fixe 10.0.0.2.

Le nom d'un fichier de configuration d'interface clone ressemble à `ifcfg-<if-nom>-<nom-clone>`. Alors qu'un fichier alias permet de faire référence à un fichier de configuration d'interface existant, un fichier clone permet de spécifier des options complémentaires pour une interface. Par exemple, si vous avez une interface Ethernet DHCP standard appelée `eth0`, le fichier pourrait

ressembler à :

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
```

Puisque `USERCTL` n'est pas réglé sur `yes`, les utilisateurs ne peuvent pas mettre cette interface en fonction ou hors service. Pour leur permettre de le faire, créez un clone appelé `user` à partir de `ifcfg-eth0`, permettant à un utilisateur de mettre l'interface `eth0` en fonction et hors service. Le nom du clone serait donc `ifcfg-eth0-user` et ne nécessiterait qu'une ligne :

```
USERCTL=yes
```

Lorsqu'un utilisateur met en fonction l'interface `eth0` avec la commande `ifup eth0-user`, à la fois les options de configuration de `ifcfg-eth0` et de `ifcfg-eth0-user` sont utilisées. Ceci est un exemple basique, mais cette méthode peut être utilisée avec diverses options et interfaces.

La méthode la plus simple pour la création de fichiers de configuration d'interface alias et clone consiste à utiliser l'outil graphique **Network Configurator** (`redhat-config-network`).

Précédent
Références liées aux services réseau

Sommaire
Niveau supérieur

Suivant
Scripts de contrôle d'interface

Scripts de contrôle d'interface

Les scripts de contrôle d'interface contrôlent la mise en fonction (activation) et hors service (désactivation) des connexions d'interface. Il existe deux principaux scripts de contrôle, `/sbin/ifdown` et `/sbin/ifup`, utilisant d'autres scripts de contrôle situés dans le répertoire `/etc/sysconfig/network-scripts` pour activer et désactiver les interfaces réseau.

Les deux principaux scripts de contrôle d'interface du répertoire `/etc/sysconfig/network-scripts`, `ifdown` et `ifup`, constituent des liaisons symboliques vers les scripts du répertoire `/sbin`. Lorsque l'un ou l'autre de ces scripts est appelé, il accepte une valeur de l'interface à utiliser, comme par exemple :

```
 ifup eth0
Indentification des informations IP pour eth0... terminé.
```

A ce point, les fichiers `/etc/sysconfig/network-scripts/network-functions` et `/etc/rc.d/init.d/functions` sont approvisionnés et des fonctions de ces fichiers sont utilisées pour diverses tâches. Reportez-vous à la la section intitulée *Fonctions réseau* pour en savoir plus sur ces tâches.

Après avoir vérifié qu'une interface a été spécifiée et que l'utilisateur effectuant la requête est autorisé à activer ou désactiver l'interface, le script correspondant au type de périphérique d'interface est activé. Il s'agit du script qui active et désactive véritablement l'interface. Voici les scripts de contrôle d'interface les plus courants pour ce type :

- `ifup-aliases` — Configure des alias IP à partir des fichiers de configuration d'interface quand plusieurs adresses IP sont associées à une interface.
- `ifdown-cipcb` et `ifup-cipcb` — Permettent d'activer et de désactiver les connexions *Crypto IP Encapsulation (CIPE)* vers le haut et le bas.
- `ifdown-ipv6` et `ifup-ipv6` — Contiennent des fonctions associées IPv6 utilisant les variables d'environnement dans divers fichiers de configuration d'interface et `/etc/sysconfig/network`.
- `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.

- `ifdown-post` et `ifup-post` — Contiennent des commandes à exécuter après l'activation ou la désactivation d'une interface spécifique :.
- `ifdown-ppp` et `ifup-ppp` — Permettent d'activer ou de désactiver une interface PPP en utilisant un périphérique particulier.
- `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.
- `ifdown-sl` et `ifup-sl` — Permettent d'activer ou de désactiver une interface SLIP.

Gardez à l'esprit que la suppression ou la modification de ces scripts dans le répertoire `/etc/sysconfig/network-scripts` peut provoquer le dysfonctionnement ou l'échec de diverses connexions. Seuls les utilisateurs chevronnés peuvent se permettre de modifier les scripts concernant une interface réseau.

Vous pouvez également utiliser le script d'initialisation `/etc/rc.d/init.d/network` afin d'activer et désactiver toutes les interfaces réseau configurées pour démarrer au lancement de l'ordinateur avec la commande :

```
/sbin/service network action
```

`action` correspondant à `start` pour démarrer les interfaces réseau, `stop` pour les arrêter, ou `restart` pour les redémarrer. Vous pouvez également utiliser la commande `/sbin/service/network status` pour voir une liste des périphériques configurés et des périphériques actifs.

Fonctions réseau

Red Hat Linux utilise plusieurs fichiers contenant des fonctions importantes utilisées de diverses façons pour activer et désactiver les interfaces. Plutôt que de forcer chaque fichier de contrôle d'interface à contenir les mêmes fonctions que les autres, ces fonctions sont regroupées dans quelques fichiers utilisés en fonction des besoins.

Le fichiers de fonctions réseau le plus courant est `network-functions`, situé dans le répertoire `/etc/sysconfig/network-scripts`. Ce fichier contient divers fonctions IPv4 courantes utilisées par bon nombre de scripts de contrôle d'interface, tels que contacter des programmes en cours d'exécution ayant demandé des informations sur les modifications du statut d'une interface, configurer des noms d'hôte, trouver un périphérique passerelle, vérifier le statut d'un périphérique particulier et ajouter un itinéraire par défaut.

Les fonctions requises pour les interfaces IPv6 étant différentes de celles requises pour les interfaces IPv4, un fichier `network-functions-ipv6` est spécifiquement conçu pour contenir ces informations. La prise en charge IPv6 doit être activée dans le noyau pour la communication via ce protocole. Une fonction de ce fichier vérifie la présence de la prise en charge IPv6. Ce fichier contient également des fonctions permettant de configurer et d'effacer des itinéraires IPv6 statiques, de créer et de supprimer des tunnels, d'ajouter à et de supprimer des adresses IPv6 d'une interface et de rechercher l'existence d'une adresse IPv6 sur une interface.

Chapitre 14. Techniques de mise en oeuvre de pare-feu avec `iptables`

Le noyau Linux contient une série d'outils de *filtrage de paquetages*. On appelle filtrage de paquetages le contrôle de paquetages se déplaçant à l'intérieur d'un système, qu'ils tentent d'y entrer, d'en sortir ou qu'ils se déplacent tout simplement à l'intérieur de celui-ci. Avant la version 2.4, les noyaux offraient la possibilité de gérer ces paquetages en utilisant la commande `ipchains`, qui faisait appel à une liste de règles relatives à chaque étape du processus de filtrage. L'introduction du noyau 2.4 signifie l'entrée en service de `iptables`, semblable à la commande `ipchains`, si ce n'est qu'elle multiplie les potentialités et le degré de contrôle disponible lors du filtrage de paquetages.

Ce chapitre décrit en détail les principes des techniques de filtrage de paquetages en expliquant les différences entre `ipchains` et `iptables`, en présentant les différentes options disponibles avec `iptables` et en montrant comment maintenir l'intégrité des règles de filtrage entre chaque démarrage de votre système.

Avertissement

Avertissement

Le mécanisme de pare-feu par défaut dans le noyau 2.4 est `iptables`, mais `iptables` ne peut pas être utilisé si les `ipchains` sont déjà à l'oeuvre. Si les `ipchains` sont présentes au démarrage, le noyau annoncera une erreur et ne pourra pas lancer les `iptables`.

Ces messages d'erreur lors du démarrage n'affectent pas la fonctionnalité des `ipchains`.

Si vous avez besoin d'instructions pour la construction des règles d' `iptables` ou le montage d'un pare-feu basé sur ces règles, veuillez consulter la la section intitulée *Sources d'informations additionnelles*.

Filtrage de paquetages

Les informations se déplacent à l'intérieur d'un réseau sous la forme de *paquetages*, qui représentent un ensemble de données de dimension particulière. Un fichier échangé via réseau par deux ordinateurs peut être constitué de plusieurs paquetages, chacun d'entre eux renfermant des éléments dudit fichier. L'ordinateur émetteur décompose ce fichier en plusieurs paquetages pour l'envoyer via le réseau en se

conformant aux règles du protocole réseau employé. L'ordinateur qui reçoit ces paquetages les rassemble ensuite à l'aide de la méthode spécifiée par le protocole pour reformer le fichier.

Chaque paquetage dispose de ses propres informations de navigation lui consentant de se déplacer sur le réseau jusqu'à sa destination finale. Il est capable d'informer les autres systèmes informatiques rencontrés tout au long de son parcours, ainsi que l'ordinateur vers lequel il se dirige, de sa provenance, sa destination et son identité, entre autres choses. La plupart des paquetages servent au transport de données, bien que certains protocoles les utilisent autrement. Par exemple, le protocole de transmission connu sous l'appellation de *TCP (Transmission Control Protocol)*, utilise un paquetage dénommé SYN qui ne contient aucune donnée, mais sert au lancement des communications entre deux systèmes.

Le noyau Linux possède une fonction intrinsèque lui permettant de filtrer des paquetages en choisissant de laisser pénétrer certains d'entre eux dans le système et de bloquer les autres. La version 2.4 du noyau contient trois tables de chaînes ; nous décrirons dans ce chapitre le fonctionnement de la table de filtrage. La table de filtrage est constituée de trois groupes de listes de règles par défaut appelés chaînes INPUT, OUTPUT et FORWARD. Chaque paquetage qui entre ou sort de l'ordinateur est sujet à l'une de ces listes de règles. Lorsqu'un paquetage pénètre à l'intérieur du système par le biais d'une interface réseau, le noyau décide s'il est destiné au système local (chaîne INPUT) ou bien à une autre destination (chaîne FORWARD), dans le but de déterminer quel type de liste de règles utiliser. De la même façon, si un paquetage originaire du système cherche à le quitter, le noyau procède à son contrôle grâce à la chaîne OUTPUT.

Chaque paquetage avant sa sortie d'une chaîne peut être soumis à un très grand nombre de règles. La structure et le rôle de ces règles peuvent changer, mais elles visent généralement à l'identification de paquetages en provenance ou à destination d'une adresse IP donnée ou à un groupe d'adresses lors de l'utilisation d'un protocole ou d'un service de réseau particulier.

Indépendamment de leur destination, lorsque les paquetages satisfont à une règle précise d'une liste de règles donnée, ils se voient désigner une *cible*, ou mission à accomplir. Si la règle spécifie la cible ACCEPT pour un paquetage contrôlé, celui-ci évite le reste des contrôles de la règle et se voit octroyé l'autorisation de procéder vers sa destination. Si une règle indique la cible DROP, le paquetage est "abandonné", ce qui revient à dire qu'il se voit refuser l'accès au système et que rien n'est retourné à l'hôte qui a expédié le paquetage. Si une règle indique la cible de REJECT, le paquetage est "abandonné", mais, dans ce cas, un "paquetage d'erreur" est renvoyé à l'expéditeur.

Chaque chaîne dispose de sa propre politique par défaut pour accepter (ACCEPT), abandonner (DROP) ou rejeter (REJECT) un paquetage, ou bien, si possible, mettre en attente (QUEUE) un paquetage qui doit être passé à l'espace utilisateur. 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` vous permet de configurer ces listes de règles et de créer également de nouvelles chaînes et tables à utiliser en fonction de votre situation spécifique.

Précédent
Fonctions réseau

Sommaire
Niveau supérieur

Suivant
Différences entre `iptables` et `ipchains`

Différences entre `iptables` et `ipchains`

A première vue, les commandes `ipchains` et `iptables` sont assez similaires. De fait, ces deux méthodes de filtrage de paquetages font appel à des chaînes de règles actives à l'intérieur du noyau Linux pour décider non seulement du type de paquetages autorisés ou non à l'accès au système, mais aussi du sort des paquetages qui répondent à certaines règles. Cependant, la commande `iptables` représente une manière plus flexible de filtrer les paquetages car elle donne la possibilité à l'administrateur système d'effectuer un contrôle bien plus précis sans augmenter la complexité du système en entier.

De fait, les utilisateurs à l'aise avec la commande `ipchains` devront tenir compte des différences importantes existant entre les commandes `ipchains` et `iptables` avant d'essayer de se servir de `iptables` :

- *Si l'on utilise `iptables`, chaque paquetage filtré est traité en utilisant les règles d'une chaîne uniquement, plutôt que celles de plusieurs chaînes*. Cela signifie qu'un paquetage avec la mention FORWARD pénétrant dans un système à l'aide de `ipchains` devrait passer les chaînes INPUT, FORWARD et OUTPUT tout au long de son parcours pour pouvoir poursuivre vers sa destination. En revanche, `iptables` envoie les paquetages uniquement à la chaîne INPUT s'ils sont destinés au système local et vers la chaîne OUTPUT s'ils ont été créés par le système local. C'est la raison pour laquelle il faut être sûr de placer la règle destinée au contrôle d'un paquetage spécifique dans la bonne chaîne qui, elle, détectera le paquetage.

  L'avantage réside dans la possibilité de contrôler avec une plus grande précision la disposition de chaque paquetage. Il devient alors possible de bloquer les tentatives d'accès de la part de clients se connectant depuis des hôtes utilisant votre hôte comme passerelle. Une règle OUTPUT interdisant les accès n'empêchera plus les accès aux ordinateurs qui utilisent votre hôte comme passerelle.
- *La cible DENY a été remplacée par la cible DROP*. Dans `ipchains`, les paquetages qui satisfaisaient à une règle d'une chaîne pouvaient être dirigés vers une cible DENY qui abandonnait sans avertissement le paquetage. Cette cible doit être substituée par une cible DROP dans `iptables` pour avoir le même effet.
- *L'ordre d'écriture des options dans une règle de chaîne est primordial*. Auparavant, avec `ipchains`, cet ordre d'écriture importait peu. La commande `iptables` est un peu plus sensible quant à l'usage de ces options. Par exemple, il est maintenant nécessaire de préciser le port de destination ou d'origine après avoir précisé le type de protocole (ICMP, TCP ou UDP) à utiliser dans une règle de chaîne.
- *En précisant le type d'interface réseau à utiliser dans une règle, il n'est possible d'utiliser que des interfaces d'entrée (option `-i`) avec les chaînes INPUT ou FORWARD et des interfaces de sortie*

(option `-o`) avec les chaînes FORWARD ou OUTPUT. Cela devient nécessaire parce que les chaînes OUTPUT ne sont plus utilisées par les interfaces d'entrée et que les chaînes INPUT ne sont pas vues par les paquetages se déplaçant au travers des interfaces de sortie.

Cette liste de changements n'est absolument pas exhaustive étant donné que `iptables` représente un type de filtre réseau à utiliser avec le noyau complètement repensé. Des informations détaillées sont disponibles dans le document *Linux 2.4 Packet Filtering HOWTO* et dans la [la section intitulée *Sources d'informations additionnelles*](#).

[Précédent](#) Techniques de mise en oeuvre de pare-feu avec `iptables`

[Sommaire](#)

[Niveau supérieur](#)

[Suivant](#) Options utilisées avec les commandes `iptables`

Options utilisées avec les commandes `iptables`

Les règles permettant le filtrage de paquetages par le noyau sont appliquées en exécutant la commande `iptables` suivie de certaines de ses options qui définissent le type de paquetages à filtrer, l'origine ou la destination et le sort de ces paquetages s'ils satisfont à ces règles. Les options utilisées avec une commande `iptables` spécifique doivent être groupées de façon logique selon l'usage et les conditions mêmes de la règle générale dans le but de la rendre valide.

Tables

Un des points forts de `iptables` réside dans la possibilité d'utiliser des tables multiples pour décider du sort d'un paquetage donné selon le type de paquetage en cours de surveillance. Grâce à la nature flexible de `iptables`, des tables spécifiques peuvent être créées et enregistrées dans le répertoire `/etc/modules/<version-du-noyau>/kernel/net/ipv4/netfilter` afin d'obtenir des résultats précis. On peut alors considérer `iptables` comme étant capable d'exécuter plusieurs groupes de règles `ipchains` appartenant à des chaînes spécifiques, chaque groupe ayant un rôle particulier.

La table par défaut, appelée `filter`, contient les chaînes résidantes INPUT, OUTPUT et FORWARD. Cela est assez semblable aux chaînes standard en usage avec `ipchains`. Cependant, `iptables` possède aussi par défaut deux tables supplémentaires d'opérations spécifiques de filtrage. La table `nat` peut être utilisée pour modifier les adresses d'origine et de destination enregistrées dans les paquetages et la table `mangle` vous permet d'altérer la forme des paquetages selon des méthodes particulières.

Chaque table contient des chaînes par défaut dont le but est d'exécuter des tâches selon l'objectif même de la table, mais il est également possible de définir de nouvelles chaînes dans chaque table.

Structure

Beaucoup de commandes `iptables` ont la structure suivante :

```
iptables [-t <nom-table>] <commande> <nom-chaîne> <paramètre-1> <option-1>
     <paramètre-n> <option-n>
```

Dans cet exemple, l'option *<nom-table>* permet à l'utilisateur de sélectionner une autre table que la table par

défaut `filter` à utiliser avec cette commande. L'option *<commande>* est le centre de la commande, imposant une action spécifique à accomplir, telle que l'ajout ou l'élimination d'une règle d'une chaîne particulière, qui est précisée par l'option *<nom-chaîne>*. On trouve juste après l'option *<nom-chaîne>* une paire de paramètres et d'options qui servent à définir la façon dont la règle sera respectée et l'action à entreprendre lorsqu'un paquetage correspond à la définition de la règle.

En examinant la structure d'une commande `iptables`, il est important de se rappeler que contrairement aux autres commandes, la longueur et la complexité d'une commande `iptables` est variable en fonction de son usage. Une simple commande servant à éliminer une règle d'une chaîne peut être très courte, alors qu'une commande servant à filtrer les paquetages d'un sous-réseau faisant appel à un certain nombre de paramètres et d'options sera plutôt longue. Il est nécessaire de se rappeler qu'avec les commandes `iptables` les paramètres et options utilisés peuvent susciter le besoin de créer des paramètres et options supplémentaires pour mieux définir les besoins des premiers. Pour écrire une règle efficace, cette chaîne d'actions doit être complètement respectée.

Entrez la commande `iptables -h` pour obtenir une liste exhaustive de structures de commandes `iptables`.

Commandes

Les commandes indiquent à `iptables` d'exécuter une action spécifique et une seule commande n'est autorisée par chaîne de commande `iptables`. A l'exception de la commande d'aide, toutes les autres commandes doivent être écrites en majuscules.

Les commandes `iptables` disponibles sont les suivantes :

- `-A` — Ajoute une règle `iptables` à la fin d'une chaîne donnée. On l'utilise dans les cas où l'ordre à l'intérieur de la chaîne n'est pas primordial.
- `-C` — Contrôle une règle donnée avant de l'ajouter à une chaîne spécifiée par l'utilisateur. Cette commande peut vous aider pour l'écriture de règles `iptables` compliquées en vous indiquant les paramètres et options supplémentaires.
- `-D` — Elimine une règle à l'intérieur d'une chaîne donnée de façon numérique (ex. : `5`, correspondant à la cinquième règle d'une chaîne). Il est également possible d'écrire la règle complète et `iptables` effacera la règle dans la chaîne correspondante.
- `-E` — Sert à changer le nom d'une chaîne spécifiée par un utilisateur. La structure de la table n'est modifiée en aucun cas. En fait, ceci vous évite de devoir éliminer la chaîne, la recréer sous un nouveau nom et reconfigurer toutes vos règles pour cette chaîne.
- `-F` — Supprime la chaîne sélectionnée, qui a pour effet d'éliminer toutes les règles de la chaîne. Si aucune chaîne n'est indiquée, cette commande supprime chaque règle de chaque chaîne.
- `-h` — Fournit une liste pratique de structures de commande, ainsi qu'un bref résumé de leurs paramètres et options.
- `-I` — Insère une règle à l'intérieur d'une chaîne, à un point précis. Assigne un numéro à la règle devant être insérée et `iptables` se charge de l'opération. Si aucun numéro n'est spécifié, `iptables` place votre commande au sommet de la liste de règles.

Attention **Avertissement**

Soyez attentif quant au choix de l'option (`-A` ou `-I`) que vous utilisez lors de l'ajout d'une règle. L'ordre dans lequel se présentent les règles peut se révéler très important pour définir si un paquetage se rapporte à une règle ou à une autre. Assurez-vous qu'aucune autre règle n'est concernée par l'ajout ou le retrait d'une règle dans une chaîne.

- `-L` — Etablit la liste complète des règles dans la chaîne indiquée après la commande. Pour afficher toutes les règles de toutes les chaînes dans la table par défaut `filter`, ne précisez pas de chaîne ni de table. Autrement, la syntaxe à utiliser pour établir la liste des règles dans une chaîne donnée d'une table précise doit être la suivante :

```
iptables -L <nom-chaîne> -t <nom-table>
```

  Des options puissantes pour la commande `-L` fournissant le nombre de règles et permettant une description très détaillée de ces dernières sont décrites dans la la section intitulée *Options de listage*.
- `-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 lorsque des paquetages traversent une chaîne entière sans satisfaire à une règle, ils seront envoyés à une cible donnée, 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 pour que s'effectue le changement. La première règle dans une chaîne se réfère au numéro de règle `1`.
- `-X` — Supprime une chaîne spécifiée par un utilisateur. L'élimination d'une chaîne intrinsèque d'une table n'est pas permise.
- `-Z` — Remet à zéro les compteurs d'octets et de paquetages dans toutes les chaînes d'une table particulière.

Paramètres

Une fois que certaines commandes `iptables` ont été spécifiées, y compris celles utiles à 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 paquetages.

- `-c` Effectue une remise à zéro des compteurs pour une règle donnée. Ce paramètre accepte les options PKTS (paquetages) et BYTES (octets) pour indiquer quel compteur remettre à zéro.
- `-d` Définit le nom d'hôte du destinataire, l'adresse IP ou le réseau du paquetage qui vérifiera la règle. Lors de la vérification de concordance réseau, il existe deux méthodes pour définir les masques de réseau, telles que `192.168.0.0/255.255.255.0` ou `192.168.0.0/24`.
- `-f` Applique cette règle aux paquetages fragmentés uniquement.

  En insérant l'option `!` après ce paramètre, seuls les paquetages non fragmentés seront contrôlés.

- `-i` Règle l'interface réseau d'entrée, telle que `eth0` ou `ppp0`, à utiliser avec une règle particulière. Avec `iptables`, ce paramètre optionnel ne peut être utilisé qu'avec des chaînes INPUT et FORWARD, lorsqu'elles sont utilisées avec les tables `filter` et la chaîne PREROUTING avec les tables `nat` et `mangle`.

  Ce paramètre présente plusieurs options utiles qui peuvent être utilisées avant de préciser le nom d'une interface :

  - `!` — Ordonne à ce paramètre de ne pas comparer, signifiant que n'importe quelle interface spécifiée est exclue de cette règle.
  - `+` — Caractère spécial utilisé pour comparer toutes les interfaces qui correspondent à une chaîne particulière. Exemple : le paramètre `-i eth+` appliquera cette règle à n'importe quelle interface Ethernet de votre système, mais ne prendra pas en compte les autres interfaces, telles que `ppp0`.

  Si le paramètre `-i` est utilisé sans qu'aucune interface ne soit spécifiée, alors toutes les interfaces se voient concernées par la règle.
- `-j` Indique à `iptables` de passer directement à une cible donnée lorsqu'un paquetage correspond à une règle particulière. Les cibles autorisées après l'option `-j` incluent les options standard `ACCEPT`, `DROP`, `QUEUE` et `RETURN`, ainsi que des options étendues qui sont disponibles dans des modules chargés automatiquement avec le paquetage RPM de commandes `iptables` Red Hat Linux, telles que `LOG`, `MARK` et `REJECT`, entre autres. Consultez la page de manuel relatives à `iptables` pour plus d'informations sur ces cibles, ainsi que sur les règles concernant leur usage. Beaucoup de cibles ne peuvent en effet être utilisées qu'avec certaines tables.

  En plus de spécifier des actions de cible, il est également possible de diriger un paquetage correspondant à une règle vers une chaîne définie par un utilisateur située en dehors de la chaîne courante. Ceci vous permet d'appliquer d'autres règles à ce paquetage et de le filtrer davantage avec des critères supplémentaires.

  Si aucune cible n'est spécifiée, le paquetage continue sans aucune autre action entreprise. Cependant, le compteur de cette règle avance tout de même d'un point car le paquetage correspond à la règle spécifiée.
- `-o` Règle l'interface de sortie pour une règle donnée et ne peut être utilisé 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 d'entrée (`-i`).
- `-p` Règle le protocole IP pour la règle, qui peut être `icmp`, `tcp`, `udp` ou `all`, pour comparer tous les protocoles possibles. De plus, les protocoles les moins courants indiqués dans `/etc/protocols` peuvent également être employés. 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 la source d'un paquetage particulier en utilisant la même syntaxe que pour le paramètre de destination (`-d`).

Options de concordance

Les différents protocoles de réseau offrent des options de contrôle de concordance spécifiques qui peuvent être configurées de manière à comparer un paquetage donné utilisant ce protocole. Evidemment, il est nécessaire d'identifier le protocole en question dans la commande `iptables`, tel qu'en utilisant l'option `-p tcp <nom-du-protocole>`, afin de rendre disponibles les options pour ce protocole.

Protocole TCP

Voici les options de concordance disponibles pour le protocole TCP (`-p tcp`) :

- `--dport` Indique le port de destination pour le paquetage. Vous pouvez utiliser un nom de service de réseau (comme `www` ou `smtp`), un numéro de port ou une gamme de numéros de port pour configurer cette option. Pour parcourir les noms et alias de services réseau et les numéros de port utilisés, visualisez le fichier `/etc/services`. Vous pouvez aussi utiliser `--destination-port` pour indiquer cette option de concordance.

  Pour indiquer une gamme précise de numéros de port, il suffit de séparer les numéros avec un deux points (`:`), comme ceci : `-p tcp --dport 3000:3200`. La plus grande gamme possible est `0:65535`.

  Vous pouvez aussi utiliser un point d'exclamation (`!`) comme indicateur après l'option `--dport` pour indiquer à `iptables` la comparaison de tous les paquetages qui n'utilisent pas ce service de réseau ou port.
- `--sport` Indique le port d'origine du paquetage, en utilisant les mêmes options que `--dport`. Vous pouvez utiliser aussi `--source-port` pour indiquer cette option de concordance.
- `--syn` Oblige un début de communication pour tous les paquetages TCP désignés, appelés communément *paquetages SYN*, pour vérifier la concordance avec cette règle. Tous les paquetages transportant des données seront ignorés. En plaçant un point d'exclamation (`!`) comme indicateur après l'option `--syn`, tous les paquetages non-SYN seront comparés.
- `--tcp-flags` Permet la comparaison de paquetages TCP ayant une taille en octets ou des indicateurs spécifiques avec une règle. L'option de concordance `--tcp-flags` accepte deux paramètres après celle-ci, qui sont les indicateurs de tailles en octets diverses mis dans une liste séparée par des virgules. Le premier paramètre est le masque, qui définit l'indicateur à examiner pour le paquetage. Le second se rapporte aux indicateurs qui doivent être définis dans le paquetage pour la réalisation d'une concordance. Les indicateurs disponibles sont les suivants : `ACK`, `FIN`, `PSH`, `RST`, `SYN` et `URG`. De plus, `ALL` et `NONE` peuvent aussi être utilisés pour comparer tous les indicateurs ou aucun d'entre eux respectivement.

  Par exemple, une règle `iptables` contenant `-p tcp --tcp-flags ACK,FIN,SYN SYN` ne comparera que les paquetages TCP reportant l'indicateur SYN défini et les indicateurs ACK et FIN non définis.

  Comme pour beaucoup d'autres options, utiliser un point d'exclamation (`!`) après `--tcp-flags` inverse l'effet de l'option de concordance, ce qui signifie que le second paramètre ne doit pas être défini pour garantir la comparaison.

- `--tcp-option` Essaie la comparaison d'options spécifiques à TCP qui peuvent être définies avec un paquetage donné. Cette option de comparaison peut aussi être inversée par un point d'exclamation (`!`).

Protocole UDP

Les options de concordance suivantes s'appliquent au protocole UDP (`-p udp`) :

- `--dport` Indique le port de destination du paquetage UDP, en utilisant le nom du service, le numéro de port ou une gamme de numéros de port. L'option de concordance `--destination-port` peut être employée à la place de `--dport`. Consultez l'option de concordance `--dport` dans la la section intitulée *Protocole TCP* pour les modalités d'usage de cette option.
- `--sport` Indique le port d'origine du paquetage UDP en utilisant le nom de service, le numéro de port ou une gamme de numéros de port. L'option de concordance `--source-port` peut être utilisée à la place de `--sport`. Consultez l'option de concordance `--dport` dans la la section intitulée *Protocole TCP* pour les modalités d'usage de cette option.

Protocole ICMP

Les paquetages faisant appel au protocole ICMP (Internet Control Message Protocol) peuvent être contrôlés par le biais de l'option suivante quand `-p icmp` est indiqué :

- `--icmp-type` Définit le nom ou le numéro de type d'ICMP à comparer avec cette règle. Une liste de noms ICMP valides est disponible en tapant la commande `iptables -p icmp -h`.

Modules avec options de concordance supplémentaires

Des options de concordance supplémentaires, non spécifiques à un protocole en particulier, sont disponibles par l'entremise des modules chargés lorsqu'une commande `iptables` les utilise. Pour l'emploi d'un module d'option de concordance, il vous faut charger le module en l'appelant par son nom, c'est-à-dire en incluant `-m <nom-du-module>` dans la commande `iptables` lors de la création d'une règle.

Un nombre assez important de modules, ayant chacun leurs options de concordance spécifiques, sont disponibles par défaut. Il vous est même possible de créer vos propres modules pour fournir des options de concordance supplémentaires, tel que pour répondre à des exigences réseau spécifiques par exemple. Il existe de nombreux modules, mais seuls les plus fréquents sont abordés ici.

Le module `limit` vous permet de placer une limite au nombre de paquetages qui sont comparés à une règle donnée. Ceci se révèle tout particulièrement pratique lors de la concordance avec des règles de journalisation, afin d'éviter que les résultats n'envahissent vos journaux de messages répétitifs ou ne consomment trop de ressources système.

- `--limit` — Limite le nombre de concordances dans un espace-temps donné, grâce à un modificateur de nombre et de temps paramétré sous la forme suivante : `<nombre>/<temps>`. Par exemple, en

écrivant `--limit 5/hour`, une règle effectue son contrôle de concordance seulement cinq fois par heure.

Lorsque rien n'est spécifié, une valeur de `3/hour` est la règle par défaut.

- `--limit-burst` — Limite le nombre de paquetages comparés à une règle à la fois. Cette option est à utiliser conjointement à l'option `--limit` et accepte un numéro pour en définir le seuil.

  Si aucun numéro n'est indiqué, seulement cinq paquetages sont en mesure d'être contrôlés.

Le module `state`, qui fait appel à l'option de concordance `--state`, peut comparer un paquetage avec les états de connexion particuliers suivants :

- `ESTABLISHED` Le paquetage contrôlé est associé à d'autres paquetages dans une connexion établie.
- `INVALID` Le paquetage contrôlé ne peut être associé à une connexion connue.
- `NEW` Le paquetage contrôlé crée une nouvelle connexion ou fait partie d'une connexion à double sens qui n'a pas encore été vue.
- `RELATED` Le paquetage contrôlé commence une nouvelle connexion liée d'une façon ou d'une autre à une connexion existante.

Ces états de connexion peuvent être employés de concert avec d'autres en les séparant par des virgules, tel que : `-m state --state INVALID,NEW`.

Pour contrôler la concordance d'une adresse matérielle MAC d'un périphérique Ethernet, utilisez le module `mac`, qui accepte `--mac-source` plus une adresse MAC comme option. Pour exclure une adresse MAC d'une règle, placez un point d'exclamation (`!`) après l'option de concordance `--mac-source`.

D'autres options de concordance sont disponibles dans les modules. Reportez-vous à la page de manuel de `iptables`.

Options de cible

Une fois que la concordance d'un paquetage a été contrôlée par une règle, celle-ci peut diriger le paquetage vers un certain nombre de cibles qui décideront de son traitement et, si possible, entreprendront des actions supplémentaires, telles que la journalisation de l'action. De plus, chaque chaîne possède une cible par défaut qui est utilisée si aucune des règles de la chaîne ne correspond à un paquetage ou si aucune des règles qui correspondent à un paquetage ne spécifie de cible particulière.

Il n'existe que très peu de cibles standard pour décider comment gérer les paquetages :

- *<chaîne-spécifiée-par-l'utilisateur>* Nom d'une chaîne définie et créée antérieurement au sein de cette table de règles qui sera comparée avec ce paquetage, outre à toute autre règle dans toute autre chaîne qui doit être comparée avec ce paquetage. Ce type de cible est pratique pour une plus grande analyse du paquetage avant d'en décider le sort et de procéder à sa journalisation.
- `ACCEPT` — Permet au paquetage de continuer sa progression vers sa destination (ou une autre chaîne si

sa configuration l'y oblige).

- `DROP` — Abandonne le paquetage. Le système ayant expédié ce paquetage n'est pas informé de l'échec de l'opération et ce paquetage est tout simplement enlevé de la règle contrôlant la chaîne et rejeté.
- `QUEUE` — Le paquetage est mis en attente de passer dans l'espace utilisateur, où il sera traité d'une autre façon (par un utilisateur ou une application par exemple).
- `RETURN` — Arrête le contrôle du paquetage avec les règles en vigueur dans la chaîne en usage. Si le paquetage avec la cible `RETURN` correspond à une certaine règle appelée depuis une autre chaîne, le paquetage est renvoyé à la première chaîne pour la continuation de son contrôle au point où celui-ci s'était arrêté. Dans le cas où la règle `RETURN` est utilisée dans une chaîne résidente et que le paquetage ne peut revenir vers la chaîne précédente, la cible appliquée par défaut décide alors de l'action à entreprendre.

Outre ces cibles standards, plusieurs autres cibles peuvent être utilisées avec des extensions appelées *modules cibles*, qui fonctionnent d'une manière semblable aux modules d'options de concordance (reportez-vous à la la section intitulée *Modules avec options de concordance supplémentaires*).

Il existe de nombreux modules cibles étendus ; la plupart d'entre eux s'appliquent à des tables ou des situations spécifiques. Voici quelques-uns des modules cibles les plus répandus inclus par défaut dans Red Hat Linux :

- `LOG` Journalise tous les paquetages correspondant à cette règle. Etant donné que les paquetages sont journalisés par le noyau, le fichier `/etc/syslog.conf` détermine l'emplacement où écrire ces entrées. Par défaut, ils sont placés dans le fichier `/var/log/messages`.

  Différentes options peuvent être utilisées après la cible `LOG` pour indiquer le mode de fonctionnement de la journalisation :

  - `--log-level` Définit le niveau de priorité d'un événement de journalisation. Une liste de niveaux de priorité est disponible dans la page de manuel de `syslog.conf` et leurs noms peuvent être utilisés comme option après `--log-level`.
  - `--log-ip-options` Toute option indiquée dans l'en-tête d'un paquetage IP est journalisée.
  - `--log-prefix` Ajoute une chaîne de texte avant la ligne du journal lors de l'écriture, avec un nombre maximum de 29 caractères après l'option `--log-prefix`. Cette option est pratique pour l'écriture de filtres de journalisation système à utiliser conjointement avec la journalisation de paquetages.
  - `--log-tcp-options` Toute option indiquée dans l'en-tête d'un paquetage TCP est journalisée.
  - `--log-tcp-sequence` Ecrit le numéro de séquence TCP relatif au paquetage dans le journal.
- `REJECT` Retourne un paquetage d'erreur au système ayant expédié le paquetage, puis abandonne ce dernier. Cette cible s'avère utile si vous souhaitez informer le système expéditeur du résultat du contrôle du paquetage.

  La cible `REJECT` accepte une option `--reject-with <type>` pour fournir davantage de détails avec le paquetage d'erreur. Le message d'erreur `port-unreachable` est le `<type>` d'erreur par défaut affiché si aucune autre option n'est sélectionnée. Une liste complète des options `<type>` pouvant

être utilisées est disponible dans la page de manuel de `iptables`.

D'autres extensions, dont bon nombre étant très utiles avec le masquerading faisant appel à la table `nat`, peuvent être trouvées dans la page de manuel de `iptables`.

Options de listage

La commande de listage par défaut, `iptables -L`, offre une vue générale des chaînes de règles actuellement contenues dans la table par défaut. Des options supplémentaires existent et disposent l'information de manière spécifique :

- `-v` Affiche un résultat prolixe, indiquant le nombre de paquetages et octets lus par chaque chaîne, le nombre de paquetages et d'octets contrôlés par chaque règle et quelles interfaces sont liées aux règles.
- `-x` Présente les nombres selon leur valeur exacte. Dans un système très chargé, le nombre de paquetages 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 oblige l'affichage du vrai nombre.
- `-n` Affiche les adresses IP et les numéros de port de façon numérique, plutôt qu'en utilisant le nom d'hôte et le format du service de réseau.
- `--line-numbers` Enumère les règles dans chaque chaîne aux côtés de leur ordre numérique dans la chaîne. Cette option est pratique lorsque l'on tente d'éliminer une règle donnée dans une chaîne ou de localiser l'emplacement d'une règle à insérer dans une chaîne.

Précédent
Différences entre `iptables` et `ipchains`

Sommaire
Niveau supérieur

Suivant
Stockage de l'information `iptables`

Stockage de l'information `iptables`

Les règles créées avec la commande `iptables` sont stockées dans la mémoire vive. Si vous deviez redémarrer votre système après la configuration des différentes règles `iptables`, toutes les données seraient perdues et vous seriez obligé de les entrer de nouveau. Pour que des règles spécifiques soient effectives au démarrage du système, il est nécessaire de les enregistrer dans le fichier `/etc/sysconfig/iptables`.

Pour ce faire, disposez vos tables, chaînes et règles de la façon dont vous souhaitez les voir se présenter au prochain démarrage ou au prochain lancement de `iptables` et saisissez la commande `/sbin/service iptables save` en tant que super-utilisateur. Cela aura pour effet d'indiquer au script initial `iptables` de lancer le programme `/sbin/iptables-save` et d'écrire la configuration `iptables` courante dans le fichier `/etc/sysconfig/iptables`. Ce fichier ne devrait être lisible que par le super-utilisateur, ce qui rend vos règles de filtrage invisibles aux utilisateurs normaux.

Au prochain démarrage, le script initial `iptables` fera appliquer les règles enregistrées dans `/etc/sysconfig/iptables` grâce à la commande `/sbin/iptables-restore`.

Tester une nouvelle règle `iptables` avant de la joindre au fichier `/etc/sysconfig/iptables` est une bonne habitude à prendre, mais il est également possible de copier des règles `iptables` dans ce fichier à partir d'une version de ce fichier provenant d'un autre système. Ainsi, vous pourrez distribuer facilement des groupes de règles `iptables` sur d'autres ordinateurs en un seul geste.

Sources d'informations additionnelles

Veuillez consulter les informations ci-dessous pour des informations supplémentaires sur le filtrage de paquetages avec `iptables`.

Documentation installée

- La page de manuel de `iptables` renferme une description complète des différents paramètres, commandes, et options servant de support à la création de nouvelles tables et de règles de chaînes supplémentaires.

Sites Web utiles

- http://netfilter.samba.org — A cette adresse Internet, on peut trouver une série d'informations sur `iptables`, ainsi qu'une FAQ traitant des différents problèmes que l'on peut rencontrer et plusieurs fichiers d'aide pratiques écrits par Rusty Russell, le responsable du pare-feu IP de Linux. Les documents HOWTO couvrent des sujets de base, tels que les concepts élémentaires de mise en oeuvre de réseaux, les techniques de filtrage de paquetages par le noyau 2.4, les configurations NAT et Netfilter.
- http://www.linuxnewbie.org/nhf/intel/security/iptables_basics.html — Une présentation simple concernant le déplacement de paquetages 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 contient plusieurs liens mis à jour vers diverses ressources sur le filtrage de paquetages.

Chapitre 15. Apache

Le produit Apache contient un logiciel développé par Apache Software Foundation (http://www.apache.org).

Le serveur Apache HTTP est un serveur Web Open Source robuste de niveau commercial utilisé par la plupart des sites Web sur Internet. La distribution de Red Hat Linux comprend Apache, de même que de nombreux modules complémentaires conçus pour améliorer les fonctionnalités du serveur et lui donner de puissantes capacités de cryptage. La configuration par défaut d'Apache devrait être adéquate pour satisfaire les besoins de la plupart des utilisateurs. En effet, vous n'aurez peut-être jamais besoin de changer quoi que ce soit à sa configuration. Cependant, si vous souhaitez modifier certaines directives par défaut de la configuration d'Apache, vous devrez savoir quelles sont les options possibles et où les trouver. Ce chapitre couvre l'utilisation et la configuration du serveur Web Apache.

Avertissement

Attention

Si vous envisagez d'utiliser l'**outil de configuration Apache** (`apacheconf`), un utilitaire graphique fourni avec Red Hat Linux, *n'éditez pas* le fichier de configuration `/etc/httpd/conf/httpd.conf` de votre serveur Apache. Inversement, si vous voulez éditer `httpd.conf` manuellement, *n'utilisez pas* l'**outil de configuration Apache**.

Pour obtenir plus d'informations concernant l'**outil de configuration Apache**, consultez le *Guide de personnalisation officiel Red Hat Linux*.

Après avoir installé le paquetage `apache` vous pouvez obtenir la documentation du serveur Web Apache en installant le paquetage `apache-manual` et en vous rendant à l'adresse http://localhost/manual/ ; vous pouvez également trouver la documentation Apache sur le Web à l'adresse http://httpd.apache.org/docs/. La documentation sur le serveur Web Apache contient une liste exhaustive et des descriptions complètes de toutes les options de configuration d'Apache. Pour plus de commodité, ce guide fournit de brèves descriptions des directives de configuration de la version d'Apache fournie avec Red Hat Linux.

La version d'Apache comprise avec Red Hat Linux offre la possibilité de définir des serveurs Web sécurisés au moyen du cryptage SSL offert par les paquetages **mod_ssl** et **OpenSSL**. Lorsque vous examinez le fichier de configuration de votre serveur Web, sachez que votre configuration par défaut comprend un serveur Web non sécurisé et un serveur Web sécurisé. Le serveur Web sécurisé fonctionne

comme un hôte virtuel, qui est aussi configuré dans le fichier `httpd.conf`. Pour plus d'informations sur les hôtes virtuels, reportez-vous à la section intitulée *Utilisation d'hôtes virtuels*.

Note **Remarque**

Nous n'incluons pas d'extensions FrontPage. La licence de Microsoft(TM) interdit l'inclusion de telles extensions dans des produits d'autres éditeurs. Pour en savoir plus sur les extensions FrontPage, reportez-vous à l'adresse http://www.rtr.com/fpsupport/.

Modules par défaut

Apache est distribué avec un certain nombre de modules. Par défaut, les modules suivants sont installés et activés avec le paquetage Apache sur Red Hat Linux :

```
mod_vhost_alias
mod_env
mod_log_config
mod_log_agent
mod_log_referer
mod_mime
mod_negotiation
mod_status
mod_info
mod_include
mod_autoindex
mod_dir
mod_cgi
mod_asis
mod_imap
mod_actions
mod_userdir
mod_alias
mod_rewrite
mod_access
mod_auth
mod_auth_anon
mod_auth_db
mod_expires
mod_headers
mod_setenvif
```

Les modules suivants sont installés, mais ils sont désactivés (voir la section intitulée *Ajout de modules au serveur*) :

```
mod_mmap_static
mod_mime_magic
mod_speling
mod_auth_any
mod_auth_dbm
mod_auth_ldap
mod_auth_mysql
mod_auth_pgsql
mod_digest
libproxy
mod_cern_meta
mod_usertrack
mod_example
mod_unique_id
```

Les modules suivants sont disponibles en installant des paquetages complémentaires :

```
mod_bandwidth
mod_throttle
libperl
mod_php
libphp3
libphp4
libdav
mod_roaming
libssl
mod_put
mod_python
```

Démarrage et arrêt de `httpd`

Durant le processus d'installation, un script shell Bourne appelé `httpd` a été enregistré dans `/etc/rc.d/init.d/`. Pour arrêter, démarrer et voir manuellement le statut de votre serveur, exécutez `httpd` avec les argments `stop`, `start`, ou `status`.

Pour démarrer votre serveur, tapez la commande :

```
/sbin/service httpd start
```

Si vous exécutez Apache comme serveur sécurisé, une invite vous demandera votre mot de passe. Votre serveur démarrera dès que vous l'aurez tapé.

Pour arrêter votre serveur, tapez la commande :

```
/sbin/service httpd stop
```

La commande `restart` est la façon la plus rapide d'arrêter et de redémarrer votre serveur. La commande `restart` arrête puis redémarre votre serveur. Une invite vous demande alors votre mot de passe, si vous exécutez Apache en tant que serveur sécurisé. La commande `restart` ressemble à ceci :

```
/sbin/service httpd restart
```

Si vous venez de finir de modifier quelque chose dans votre fichier `httpd.conf`, il n'est pas nécessaire d'arrêter et de redémarrer votre serveur. Vous devriez par contre utiliser la commande `reload`. When you use `reload`, vous ne devez pas taper votre mot de passe. Votre mot de passe demeure en cache durant les rechargements, mais pas durant les arrêts et redémarrages. La commande `reload` ressemble à ceci :

```
/sbin/service httpd reload
```

Par défaut, le processus `httpd` démarre automatiquement au lancement de votre ordinateur. Si vous exécutez Apache en tant que serveur sécurisé, une invite vous demandera le mot de passe après le lancement de l'ordinateur, à moins que vous n'ayez généré une clé pour votre serveur sécurisé sans protection avec mot de passe.

Précédent
Apache

Sommaire
Niveau supérieur

Suivant
Directives de configuration dans `httpd.conf`

Directives de configuration dans `httpd.conf`

Le fichier de configuration du serveur Web Apache est `/etc/httpd/conf/httpd.conf`. Le fichier `httpd.conf` est bien commenté et parle de lui-même. Sa configuration par défaut fonctionnera pour la plupart des gens. Vous ne devrez donc probablement pas changer ses directives dans `httpd.conf`. Vous pourriez cependant vouloir vous familiariser avec les options de configuration les plus importantes.

Les fichiers vides `srm.conf` et `access.conf` se trouvent également dans le répertoire `/etc/httpd/conf/`. Les fichiers `srm.conf` et `access.conf` étaient auparavant utilisés, avec `httpd.conf`, comme fichiers de configuration pour Apache.

Si vous voulez configurer Apache, il vous suffit de modifier `httpd.conf` et de recharger (ou d'arrêter et rallumer) le processus `httpd`. La la section intitulée *Démarrage et arrêt de `httpd`* illustre comment recharger, arrêter et relancer Apache.

Avant de modifier `httpd.conf`, copiez avant tout le fichier original sous un nom du genre `httpd.conf-old` (ou tout autre nom). for example. Ainsi, si vous commettez ensuite une erreur durant la modification du fichier de configuration, vous pourrez utiliser la copie de sauvegarde.

Si vous commettez une erreur et que votre serveur Web ne fonctionne pas correctement, la première chose à vérifier est ce que vous avez modifié dans le fichier `httpd.conf`. Vérifiez si vous n'avez pas commis de faute de frappe. La seconde chose à vérifier est le journal des erreurs du serveur Web (`/var/log/httpd/error_log`). Le journal des erreurs peut vous sembler difficile à interpréter si vous manquez d'expérience. Toutefois, si vous venez de rencontrer un problème, les dernières entrées du journal des erreurs devraient fournir certaines indications sur ce qui est arrivé.

Les sections suivantes contiennent de brèves descriptions des directives incluses dans le fichier `httpd.conf`. Ces descriptions ne sont pas exhaustives. Pour plus d'informations, reportez-vous à la documentation d'Apache fournie au format HTML à l'adresse http://localhoast/manual/ ou à la documentation en ligne du groupe Apache à l'adresse http://httpd.apache.org/docs/. Pour plus d'informations sur les directives mod_ssl, reportez-vous à la documentation incluse au format HTML à l'adresse http://localhost/manual/mod/mod_ssl/ ou consultez le *Guide de l'utilisateur* de mod_ssl à l'adresse http://www.modssl.org/docs/2.8/.

`ServerType`

`ServerType` doit être réglée sur `standalone`. Par défaut, votre serveur est paramétré sur `ServerType standalone`.

`ServerType standalone` signifie que le serveur est démarré une fois, après quoi il s'occupe de toutes les connexions.

`ServerRoot`

`ServerRoot` est le répertoire de niveau supérieur qui contiendra les fichiers du serveur. Les serveurs tant sécurisé que non sécurisé sont paramétrés pour utiliser le répertoire `ServerRoot "/etc/httpd"`.

`LockFile`

`LockFile` est le chemin d'accès du fichier de verrouillage utilisé lorsque le serveur Apache est compilé avec

USE_FCNTL_SERIALIZED_ACCEPT ou USE_FLOCK_SERIALIZED_ACCEPT. LockFile doit normalement conserver sa valeur par défaut.

PidFile

PidFile est le nom du fichier dans lequel le serveur consigne son identifiant de processus (pid). Votre serveur Web est paramétré pour consigner son pid dans /var/run/httpd.pid.

ScoreBoardFile

The ScoreBoardFile stocke les informations internes au processus serveur utilisées pour la communication entre le processus serveur père et ses processus fils. Red Hat Linux utilise la mémoire partagée pour stocker ScoreBoardFile, la valeur par défaut /etc/httpd/logs/apache_runtime_status n'est utilisée qu'en cas de secours.

ResourceConfig

La directive ResourceConfig donne pour instruction au serveur de lire le fichier nommé ResourceConfig pour plus de directives. La directive ResourceConfig est identifiée comme un commentaire car votre serveur Web utilise httpd.conf uniquement pour les directives de configuration.

AccessConfig

La directive AccessConfig donne pour instruction au serveur de lire le fichier nommé AccessConfig pour plus de directives, après avoir lu le fichier nommé par ResourceConfig. La directive AccessConfig est identifiée comme un commentaire car votre serveur Web utilise uniquement httpd.conf pour les directives de configuration.

Timeout

Timeout définit, en secondes, le temps pendant lequel votre serveur attend des réceptions et des émissions en cours de communication. Plus spécifiquement, Timeout définit le temps pendant lequel le serveur attend de recevoir une demande GET, le temps pendant lequel il attend de recevoir des paquets TCP sur une requête POST ou PUT et le temps pendant lequel il attend entre des ACK répondant aux paquets TCP. Timeout est définie sur 300 secondes, ce qui convient dans la plupart des cas.

KeepAlive

KeepAlive définit si votre serveur autorisera des connexions persistantes (c'est-à-dire plusieurs demandes par connexion). KeepAlive peut être utilisée pour empêcher tout client de consommer trop de ressources du serveur.

Par défaut, Keepalive est définie sur off. Si Keepalive est définie sur on et que le serveur devient très occupé, le serveur peut générer rapidement un maximum de processus fils. Dans ce cas, les serveur sera considérablement ralenti. Si vous activez Keepalive, vous devriez tenir la valeur de KeepAliveTimeout basse (reportez-vous à la la section intitulée *KeepAliveTimeout*) et contrôler votre fichier /var/log/httpd/error_log. Ce fichier vous indique s'il vous manque des processus fils pour traiter les requêtes.

MaxKeepAliveRequests

Cette directive définit le nombre maximum de demandes autorisées par connexion persistante. Le groupe Apache recommande d'utiliser un paramétrage élevé, qui améliorera les performances de votre serveur. Par défaut, `MaxKeepAliveRequests` est paramétrée sur `100`, ce qui convient dans la plupart des cas.

KeepAliveTimeout

`KeepAliveTimeout` définit la durée en secondes pendant laquelle votre serveur attendra, après avoir servi une demande, la demande suivante, avant d'interrompre la connexion. Une fois une demande reçue, c'est la directive `Timeout` qui s'applique à sa place.

MinSpareServers and MaxSpareServers

Le serveur Web Apache s'adapte de façon dynamique à la charge reçue en maintenant un nombre de processus serveur de rechange approprié en fonction du trafic. Le serveur vérifie le nombre de serveurs attendant une requête et en supprime s'ils sont plus nombreux que `MaxSpareServers` ou en crée s'ils sont moins nombreux que `MinSpareServers`.

La valeur `MinSpareServers` par défaut de votre serveur est `5` ; la valeur `MaxSpareServers` par défaut de votre serveur est `20`. Ces paramètres par défaut devraient être appropriés dans presque toutes les situations. Ne définissez pas une valeur très élevée pour `MinSpareServers` car cela créera une charge de traitement importante sur le serveur, même si le trafic est faible.

StartServers

`StartServers` définit le nombre de processus créés au démarrage. Du fait que le serveur Web supprime et crée des processus serveur, de façon dynamique en fonction de la charge du trafic, il est inutile de modifier ce paramètre. Votre serveur Web est réglé pour lancer huit processus serveur au démarrage.

MaxClients

`MaxClients` définit une limite au nombre total de processus serveur (c'est-à-dire le nombre de clients connectés simultanément) pouvant s'exécuter en même temps. Conservez une valeur élevée pour `MaxClients` (par défaut, la valeur du serveur est réglée sur 150) car personne d'autre ne sera autorisé à se connecter une fois ce nombre atteint. Vous ne pouvez pas définir pour `MaxClients` une valeur supérieure à 256 sans recompiler Apache. La principale raison d'être de `MaxClients` est d'éviter qu'un serveur Web surchargé ne perturbe votre système d'exploitation.

MaxRequestsPerChild

`MaxRequestsPerChild` définit le nombre total de demandes que chaque processus serveur fils sert avant de disparaître. La principale raison justifiant de définir `MaxRequestsPerChild` consiste à éviter des pertes de mémoire induites par les processus longs. La valeur par défaut de `MaxRequestsPerChild` pour votre serveur est `1000`.

Listen

`Listen` identifie les ports sur lesquels votre serveur Web accepte les demandes entrantes. Votre serveur Web est paramétré pour écouter sur le port 80 pour les communications Web non sécurisées et (dans les balises d'hôte virtuel définissant le serveur sécurisé) sur le port 443 pour les communications Web sécurisées.

Si vous paramétrez Apache pour écouter sur un port dont le numéro est inférieur à 1024, vous devrez être super-utilisateur pour le

lancer. Pour les ports dont le numéro est égal ou supérieur à 1024, `httpd` peut être démarré par un utilisateur normal.

`Listen` peut également être utilisée pour spécifier des adresses IP particulières sur lesquelles le serveur acceptera des connexions.

BindAddress

`BindAddress` permet de spécifier les adresses IP pour lesquelles votre serveur réagira. Utilisez plutôt la directive `Listen` si vous avez besoin de cette fonctionnalité. `BindAddress` n'est pas utilisée par votre serveur Web ; par défaut, elle est identifiée comme un commentaire dans `httpd.conf`.

LoadModule

`LoadModule` est utilisée pour charger des modules DSO (Dynamic Shared Object, objet partagé dynamique). Pour plus d'informations sur le support DSO d'Apache, y compris la manière précise d'utiliser la directive `LoadModule`, reportez-vous à la la section intitulée *Ajout de modules au serveur*. Notez que l'ordre des modules est important, alors ne les déplacez pas.

IfDefine

Les balises `<IfDefine>` et `</IfDefine>` entourent des directives de configuration. Elles s'appliquent si le " test " indiqué dans la balise `<IfDefine>` est vrai. Les directives sont ignorées si le test est faux.

Le test dans les balises `<IfDefine>` est un nom de paramètre (par exemple, `HAVE_PERL`). Si le paramètre est défini (c'est-à-dire spécifié comme argument de la commande de démarrage du serveur), le test est vrai. Dans ce cas, votre serveur Web est démarré, le test est vrai et les directives contenues dans les balises `IfDefine` sont appliquées.

Par défaut, les balises `<IfDefine HAVE_SSL>` entourent les balises d'hôtes virtuels pour votre serveur sécurisé. Les balises `<IfDefine HAVE_SSL>` entourent également les directives `LoadModule` et `AddModule` pour `ssl_module`.

ClearModuleList

La directive `ClearModuleList` est située immédiatement avant la longue liste de directives `AddModule`. `ClearModuleList` efface la liste de modules actifs dans le serveur. Ensuite, la liste de directives `AddModule` recrée la liste, immédiatement après `ClearModuleList`.

AddModule

`AddModule` est la directive utilisée pour créer une liste complète de tous les modules disponibles. Vous utiliserez la directive `AddModule` si vous ajoutez votre propre module comme DSO. Pour plus d'informations sur la manière dont `AddModule` est utilisée pour la prise en charge de DSO, reportez-vous à la la section intitulée *Ajout de modules au serveur*.

ExtendedStatus

Les directives `ExtendedStatus` contrôlent le fait qu'Apache génère des informations d'état sommaires (`off`)ou détaillées (`on`), lorsque le module de commande `server-status` est appelé. `Server-status` est appelé à l'aide des balises `Location`. Pour plus d'informations sur l'appel de `server-status`, reportez-vous à la la section intitulée *`Location`*.

Port

Normalement, Port définit le port sur lequel votre serveur écoute. Toutefois, votre serveur Web contrôle plusieurs ports par défaut, du fait que la directive Listen est également utilisée. Lorsque les directives Listen sont activées, votre serveur contrôle tous ces ports. Pour plus d'informations sur Listen, reportez-vous à la description de la directive Listen.

La commande Port est également utilisée pour spécifier le numéro de port utilisé pour créer un nom canonique pour votre serveur. Reportez-vous à la la section intitulée *UseCanonicalName* pour plus d'informations sur le nom canonique de votre serveur.

User

La directive User définit l'ID utilisateur utilisé par le serveur pour répondre aux demandes. Le paramétrage de User détermine l'accès au serveur. Tous les fichiers inaccessibles à cet utilisateur seront également inaccessibles aux visiteurs de votre site Web. La valeur par défaut pour User est apache.

La directive User doit correspondre uniquement aux fichiers auxquels tous les utilisateurs et tous les visiteurs ont le droit d'accéder. La directive User correspond également au propriétaire des processus CGI éventuellement générés par le serveur. La directive User ne doit pas permettre d'exécuter des codes n'étant pas prévus pour répondre aux demandes HTTP.

Note **Remarque**

Pour des raisons de sécurité, Apache refuse d'être exécuté en tant que User root. Le fait d'utiliser root comme valeur pour User risque d'ouvrir une brèche importante dans la sécurité de votre serveur Web.

Le processus httpd parent commence par s'exécuter comme root en cours de fonctionnement normal, puis est immédiatement transmis à l'utilisateur apache. Le serveur doit démarrer comme root parce qu'il doit se relier à un port sous 1024 (le port par défaut pour les communications Web sécurisées est le port 443 ; le port par défaut pour les communications Web non sécurisées est le port 80). Les ports sous 1024 étant réservés à l'usage du système, ils ne peuvent être utilisés que par quelqu'un connecté en tant que root. Cependant, une fois que le serveur s'est connecté à son port, il transmet le processus au User avant d'accepter la moindre demande de connexion.

Group

La directive Group est similaire à User. Group définit le groupe sous lequel le serveur répondra à des demandes. La valeur de Group par défaut est également apache.

ServerAdmin

ServerAdmin indique l'adresse électronique de l'administrateur du serveur Web. Cette adresse électronique apparaîtra dans les messages d'erreur sur les pages Web générées par le serveur afin que les utilisateurs puissent signaler un problème en envoyant un message électronique à l'administrateur du serveur. La valeur par défaut estServerAdmin root@localhost.

Généralement, une bonne manière de configurer ServerAdmin consiste à utiliser la valeur webmaster@your_domain.com. Ensuite, créez un alias pour webmaster au nom de la personne responsable du serveur Web, dans /etc/aliases. Enfin, exécutez /usr/bin/newaliases pour ajouter le nouvel alias.

ServerName

`ServerName` permet de définir un nom d'hôte pour votre serveur, qui diffère du nom réel de votre hôte. Par exemple, vous pouvez utiliser www.votre_domaine.com alors que le nom réel de votre serveur est foo.votre_domaine.com. Notez que `ServerName` doit être un nom de domaine valide que vous avez le droit d'utiliser (ne vous contentez pas simplement d'en inventer un).

Si vous spécifiez un `ServerName`, assurez-vous que son adresse IP et son nom de serveur sont inclus dans votre fichier `/etc/hosts` file.

DocumentRoot

`DocumentRoot` est le répertoire contenant la plupart des fichiers HTML qui seront servis en réponse aux demandes. La valeur de `DocumentRoot` par défaut pour les serveurs Web sécurisés et non sécurisés est `/var/www/html`. Par exemple, le serveur pourrait recevoir une demande pour le document suivant :

```
http://votre_domaine/foo.html
```

Le serveur recherchera le fichier suivant dans le répertoire par défaut

```
/var/www/html/foo.html
```

Si vous voulez modifier le `DocumentRoot` afin qu'il ne soit pas partagé par les serveurs Web sécurisés et non sécurisés, reportez-vous à la la section intitulée *Utilisation d'hôtes virtuels*.

Directory

Les balises `<Directory /path/to/directory>` et `</Directory>` sont utilisées pour entourer un groupe de directives de configuration devant uniquement s'appliquer à ce répertoire et ses sous-répertoires. Toute directive applicable à un répertoire peut être utilisée à l'intérieur des balises `<Directory>`. Les balises `<File>` peuvent être utilisées de la même manière, appliquées à un ou plusieurs fichiers spécifiques.

Par défaut, des paramètres très restrictifs sont appliqués au répertoire racine, à l'aide des directives `Options` (voir la section intitulée *`Options`*) et `AllowOverride` (voir la section intitulée *`AllowOverride`*). Dans cette configuration, il faut explicitement attribuer ces paramètres à tout répertoire du système ayant besoin de paramètres plus permissifs.

Les balises `Directory` permettent de définir le `DocumentRoot` avec des paramètres moins rigides, de manière à ce qu'il puisse servir des demandes HTTP.

Le répertoire `cgi-bin` st configuré pour permettre l'exécution de scripts CGI avec l'option `ExecCGI`. Si vous devez exécuter un script CGI dans un autre répertoire, vous devez définir `ExecCGI` pour ce répertoire. Par exemple, si votre répertoire `cgi-bin` est `/var/www/cgi-bin`, mais que vous vouliez exécuter des scripts CGI depuis `/home/my_cgi_directory`, ajouter une directive `ExecCGI` à un ensemble de directives `Directory` tel que le suivant dans votre fichier `httpd.conf` :

```
<Directory /home/mon_répertoire_cgi>
    Options +ExecCGI
</Directory>
```

Pour permettre l'exécution de scripts CGI dans `/home/my_cgi_directory`, il vous faudra entreprendre des démarches supplémentaires au paramétrage de `ExecCGI`. Vous devrez aussi décommenter la directive `AddHandler` pour identifier les fichiers qui ont une extension `.cgi` (scripts CGI). Vous trouverez des instructions sur le paramétrage de `AddHandler` dans la la section intitulée *`AddHandler`*. Les autorisations pour les scripts CGI et le chemin d'accès aux scripts doivent être paramétrés à 0755.

Options

La directive `Options` contrôle les fonctions du serveur disponibles dans un répertoire particulier. Par exemple, en vertu des paramètres restrictifs spécifiés pour le répertoire racine, `Options` est définie uniquement sur `FollowSymLinks`. Aucune fonction n'est activée, à l'exception du fait que le serveur est autorisé à suivre les liens symboliques dans le répertoire racine.

Par défaut, dans votre répertoire `DocumentRoot`, `Options` est paramétrée pour inclure `Indexes`, `Includes` et `FollowSymLinks`. `Indexes` permet au serveur de générer le contenu d'un répertoire si aucun `DirectoryIndex` (par exemple, `index.html`) n'est spécifié. `Includes` signifie que des fichiers à inclure côté serveur sont autorisés. `FollowSymLinks` permet au serveur de suivre des liens symboliques dans ce répertoire.

Vous devez également inclure des instructions `Options` pour les répertoires à l'intérieur de directives d'hôtes virtuels si vous voulez que vos hôtes virtuels reconnaissent ces `Options`.

Par exemple, les fichiers à inclure côté serveur sont déjà activés dans le répertoire `/var/www/html` en raison de la présence de la ligne `Options Includes` dans la section des directives `<Directory "/var/www/html">`. Toutefois, si vous voulez qu'un hôte virtuel reconnaisse les fichiers à inclure côté serveur, vous devez inclure une section telle que la suivante à l'intérieur des balises de votre hôte virtuel :

```
<Directory /var/www/html>
Options Includes
</Directory>
```

AllowOverride

La directive `AllowOverride` définit si des `Options` peuvent être invalidées par les instructions d'un fichier `.htaccess`. Par défaut, tant le répertoire super-utilisateur que `DocumentRoot` sont réglés pour interdire les invalidations `.htaccess`.

Order

La directive `Order` contrôle simplement l'ordre dans lequel les directives `allow` et `deny` sont analysées. Votre serveur est configuré pour analyser les directives `Allow` avant les directives `Deny` pour votre répertoire `DocumentRoot`.

Allow

`Allow` spécifie quel demandeur peut accéder à un répertoire donné. Le demandeur peut être `all`, un nom de domaine, une adresse IP, une adresse IP partielle, une paire réseau/masque réseau, etc. Votre répertoire `DocumentRoot` est configuré pour `Allow` (permettre) les demandes de `all` (tous).

Deny

`Deny` fonctionne exactement comme `Allow`, sauf que vous spécifiez à qui l'accès est refusé. Votre `DocumentRoot` n'est pas configuré pour `Deny` (refuser) les demandes de qui que ce soit.

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, le sous-répertoire est `public_html`. Par exemple, le serveur pourrait recevoir la demande suivante :

```
http://votre_domaine/~nom d'utilisateur/foo.html
```

Le serveur rechercherait le fichier :

```
/home/nom d'utilisateur/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 aux répertoires personnels des utilisateurs peut être différent sur votre système).

Assurez-vous que les autorisations relatives aux répertoires personnels des utilisateurs sont correctement définies. Les répertoires personnels des utilisateurs doivent être définis sur 0711. Les bits de lecture (r) et d'exécution (x) doivent être définis sur les répertoires `public_html` des utilisateurs (0755 fonctionnera). Les fichiers qui seront servis dans les répertoires `public_html` des utilisateurs doivent être définis sur au moins 0644.

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 la page http://*votre_domaine*/*ce_répertoire*/, il obtient soit la page `DirectoryIndex` si elle existe, soit la liste du contenu du répertoire générée par le serveur. La valeur par défaut pour `DirectoryIndex` est `index.html` `index.htm` `index.shtml` `index.php` `index.php4` `index.html` `index.cgi`. Le serveur essaie de trouver l'un de ces fichiers et retourne le premier qu'il trouve. S'il ne trouve aucun de ces fichiers et si `Options Indexes` est paramétrée pour ce répertoire, le serveur génère et retourne une liste, au format HTML, des fichiers et sous-répertoires contenus dans le répertoire.

AccessFileName

`AccessFileName` nomme le fichier que le serveur doit utiliser pour les informations de contrôle d'accès dans chaque

répertoire. Par défaut, votre serveur Web est paramétré pour utiliser `.htaccess`, s'il existe, afin d'accéder aux informations de contrôle d'accès dans chaque répertoire.

Juste après la directive `AccessFileName`, une série de balises `Files` appliquent un contrôle d'accès à tout fichier commençant par `.ht`. Ces directives refusent l'accès Web à tous les fichiers `.htaccess` (ou d'autres commençant par `.ht`) pour des raisons de sécurité.

CacheNegotiatedDocs

Par défaut, votre serveur Web demande aux serveurs proxy de ne pas mettre en cache des documents négociés sur la base du contenu (c'est-à-dire qui peuvent changer avec le temps ou suite à l'entrée du demandeur). Si vous annulez le caractère de commentaire de `CacheNegotiatedDocs`, vous désactivez cette fonction et les serveurs proxy seront autorisés à mettre en cache les documents à partir de ce moment.

UseCanonicalName

`UseCanonicalName` est paramétrée par défaut sur `on`. `UseCanonicalName` permet au serveur de créer une URL qui se référence elle-même, en utilisant `ServerName` et `Port`. Lorsque le serveur fait référence à lui-même en réponse aux demandes des clients, il utilise cette URL. Si vous paramétrez `UseCanonicalName` sur `off`, le serveur utilisera plutôt la valeur figurant dans la demande du client pour pointer sur lui-même.

TypesConfig

`TypesConfig` nomme le fichier qui définit la liste par défaut des correspondances de type MIME (extensions de nom de fichier associées à des types de contenu). Le fichier `TypesConfig` par défaut est `/etc/mime.types`. Au lieu d'éditer `/etc/mime.types`, il est recommandé d'ajouter des types MIME à l'aide de la directive `AddType`.

Pour plus d'informations sur `AddType`, reportez-vous à la la section intitulée *`AddType`*.

DefaultType

`DefaultType` définit un type de contenu par défaut pour le serveur Web à utiliser pour des documents dont les types MIME ne peuvent pas être déterminés. Par défaut, votre serveur Web suppose que tout fichier au contenu indéterminé est de type texte brut.

IfModule

Les balises `<IfModule>` et `</IfModule>` entourent des directives conditionnelles. Les directives contenues à l'intérieur des balises `IfModule` sont traitées dans l'un des deux cas suivants. Les directives sont traitées si le module contenu dans la balise de début `<IfModule>` est compilé dans le serveur Apache. Si un point d'exclamation (" ! ") est inclus devant le nom du module, les directives ne sont traitées que si le module dans la balise de départ `<IfModule>` n'est *pas* compilé.

Le fichier `mod_mime_magic.c` est inclus dans ces balises `IfModule`. Le module mod_mime_magic est comparable à la commande UNIX `file`, qui examine quelques octets du contenu d'un fichier, puis utilise des " nombres magiques " et d'autres indices pour déterminer le type MIME du fichier.

Si le module mod_mime_magic est compilé dans Apache, ces balises `IfModule` indiquent au module mod_mime_magic où se trouve le fichier de définition des indices : `/usr/share/magic` dans ce cas.

Le module mod_mime_magic n'est pas compilé par défaut. Si vous voulez l'utiliser, reportez-vous à la la section intitulée *Ajout de modules au serveur*, pour plus de détails sur la manière d'ajouter des modules à votre serveur.

HostnameLookups

`HostnameLookups` peut être définie sur `on`, `off` ou `double`. Si vous autorisez `HostnameLookups` (en la paramétrant sur `on`), votre serveur résoudra automatiquement l'adresse IP pour chaque connexion demandant un document de votre serveur Web. La résolution de l'adresse IP signifie que votre serveur établit une ou plusieurs connexions avec le DNS pour rechercher le nom d'hôte correspondant à une adresse IP particulière. Si vous paramétrez `HostnameLookups` sur `double`, votre serveur établira un DNS double inversé. En d'autres termes, après la recherche inverse, une recherche en avant est lancée sur le résultat. Au moins une des adresses IP de la recherche en avant doit correspondre à l'adresse de la première recherche inverse.

Généralement, vous devez laisser `HostnameLookups` paramétrée sur `off`, du fait que les demandes de DNS ajoutent une charge à votre serveur et peuvent le ralentir. Si votre serveur est occupé, les effets de `HostnameLookups` peuvent être sensibles.

`HostnameLookups` pose également un problème pour Internet dans son ensemble. Les connexions individuelles établies pour rechercher chaque nom d'hôte s'additionnent. C'est pourquoi, pour le bien de votre propre serveur Web, de même que pour celui d'Internet dans son ensemble, vous devriez laisser `HostnameLookups` paramétrée sur `off`.

Si vous voulez voir les noms d'hôte dans vos fichiers journaux, vous pourriez songer à exécuter l'un des nombreux outils d'analyse de journal qui effectuent des recherches DNS plus efficaces et en bloc lorsque vous faites la rotation de vos fichiers journaux.

ErrorLog

`ErrorLog` nomme le fichier dans lequel sont consignées les erreurs du serveur. Comme cette directive l'indique, le fichier journal des erreurs relatif à votre serveur Web se trouve dans `/var/log/httpd/error_log`.

Le journal des erreurs est intéressant si votre serveur Web génère des erreurs ou des pannes dont vous ne connaissez pas la cause.

LogLevel

`LogLevel` définit le niveau de détail des messages d'erreur des journaux des erreurs. `LogLevel` peut être définie (du moins détaillé au plus détaillé) sur `emerg`, `alert`, `crit`, `error`, `warn`, `notice`, `info` ou `debug`. Par défaut, la directive `LogLevel` est définie sur `warn`.

LogFormat

Les directives `LogFormat` de votre fichier `httpd.conf` définissent un format pour les messages d'erreur. Le `LogFormat` utilisé dépend des paramètres attribués dans la directive `CustomLog` (reportez-vous à la la section intitulée *`CustomLog`*).

CustomLog

`CustomLog` identifie le fichier journal et le format de fichier journal. Dans la configuration par défaut de votre serveur Web, `CustomLog` définit le fichier journal dans lequel sont consignés les accès à votre serveur Web : `/var/log/httpd/access_log`. Vous devez connaître l'emplacement de ce fichier pour pouvoir générer des statistiques

concernant les performances d'accès à votre serveur Web.

`CustomLog` définit également le format du fichier journal ordinaire. Le format du fichier journal ordinaire ressemble à ceci :

```
hôte distant rfc931 auth-utilisateur [date] "demande" état octets referer utilisateur-agent
```

hôte distant

Nom d'hôte distant. Si le nom d'hôte n'est pas disponible auprès du DNS ou si `HostnameLookups` est paramétré sur `Off`, *hôte distant* sera l'adresse IP de l'hôte distant.

rfc931

Non utilisé. Le signe `-` figure dans le fichier journal à sa place.

auth-utilisateur

Si l'authentification est requise, il s'agit du nom sous lequel l'utilisateur s'est identifié. Habituellement, il n'est pas utilisé, de sorte que vous voyez le signe `-` à sa place.

[date]

La date et l'heure de la demande.

"demande"

La chaîne de demande telle qu'elle est venue du navigateur ou du client.

état

Code d'état HTTP retourné au navigateur ou au client.

octets

Taille du document.

referer

Cela peut permettre de donner l'URL de la page Web qui lie à la demande courante.

utilisateur-agent

Cela donne le nom du navigateur ou du client qui fait la demande.

ServerSignature

La directive `ServerSignature` ajoute une ligne contenant la version du serveur Apache et le `ServerName` de l'hôte servant à tout document généré par le serveur (par exemple, les messages d'erreur renvoyés aux clients). `ServerSignature` est paramétrée sur `on` par défaut. Vous pouvez définir la valeur `off`, afin qu'aucune ligne de signature ne soit ajoutée ou définir la valeur `EMail`. `EMail` ajoute une balise HTML `mailto:ServerAdmin` à la ligne de signature.

Alias

Le paramètre `Alias` permet aux répertoires de se trouver en dehors du répertoire `DocumentRoot` tout en restant accessibles au serveur Web. Toute URL se terminant par l'alias sera automatiquement convertie en chemin d'accès vers l'alias. Par défaut, un

alias est déjà configuré. Un répertoire `icons` est accessible par le serveur Web, mais le répertoire n'est pas le `DocumentRoot`. Le répertoire `icons`, un alias, est en réalité `/var/www/icons/`, pas `/var/www/html/icons/`.

ScriptAlias

Le paramètre `ScriptAlias` définit l'endroit où les scripts CGI (ou d'autres types de script) peuvent être trouvés. Généralement, il est préférable de ne pas laisser de scripts CGI dans `DocumentRoot`. Si des scripts CGI figurent dans `DocumentRoot`, ils pourraient être considérés comme des documents de texte. Même s'il vous est indifférent que certaines personnes puissent voir (et utiliser) vos scripts CGI, le fait de révéler la manière dont ils fonctionnent peut permettre à des personnes peu scrupuleuses d'exploiter d'éventuelles failles de sécurité du script, menaçant ainsi la sécurité de votre serveur. Par défaut, le répertoire `cgi-bin` est un `ScriptAlias` de `/cgi-bin/` et se trouve en réalité dans `/var/www/cgi-bin/`.

`Options ExecCGI` est sélectionné pour votre répertoire `/var/www/cgi-bin`, ce qui signifie que l'exécution de scripts CGI est autorisée dans ce répertoire.

Reportez-vous à la la section intitulée *`AddHandler`* et à la la section intitulée *`Directory`* pour obtenir des instructions sur la manière d'exécuter des scripts CGI dans des répertoires autres que `cgi-bin`.

Redirect

Lorsqu'une page Web est déplacée, la commande `Redirect` peut être utilisée pour mapper l'ancienne URL sur une autre URL. Le format est le suivant :

```
Redirect /chemin/foo.html http://nouveau_domaine/chemin/foo.html
```

Ainsi, si une demande HTTP est reçue pour une page qui se trouve habituellement à l'URL http://*`votre_domaine`*/*`chemin`*/foo.html, le serveur retourne la nouvelle URL (http://*`nouveau_domaine`*/*`chemin`*/foo.html) au client, qui essaie d'extraire le document de la nouvelle URL.

Pour une méthode de redirection plus avancée, utilisez le module `mod_rewrite` fourni avec le serveur.

IndexOptions

`IndexOptions` contrôle l'aspect des listes de contenu de répertoire générées par le serveur en ajoutant des icônes et des descriptions de fichier, etc. Si `Options Indexes` est définie (voir la section intitulée *`Options`*), votre serveur Web peut générer une liste du contenu du répertoire lorsqu'il reçoit une demande HTTP telle que celle-ci :

http://*`votre_domaine`*/*`ce_répertoire`*/

Tout d'abord, votre serveur Web recherche dans ce répertoire un fichier de la liste figurant après la directive `DirectoryIndex` (en général, `index.html`). Si votre serveur Web ne trouve aucun de ces fichiers, il génère une liste HTML des fichiers et sous-répertoires figurant dans ce répertoire. Vous pouvez modifier l'aspect de cette liste du contenu du répertoire à l'aide de certaines directives de `httpd.conf`, notamment `IndexOptions`.

Par défaut, `FancyIndexing` est activée. Si `FancyIndexing` est activée, le fait de cliquer sur les en-têtes de colonne de la liste modifie l'ordre d'affichage en fonction des en-têtes. Un autre clic sur le même en-tête permet de basculer de l'ordre ascendant à l'ordre descendant, et inversement. `FancyIndexing` affiche également des icônes différentes pour les différents fichiers, en

fonction des extensions de fichier. Si vous utilisez la directive `AddDescription` et activez `FancyIndexing`, une brève description de fichier sera incluse dans la liste du contenu du répertoire générée par le serveur.

`IndexOptions` comprend un certain nombre d'autres paramètres qui peuvent être définis pour contrôler l'aspect des répertoires générés par le serveur. Les paramètres incluent `IconHeight` et `IconWidth`, pour faire en sorte que le serveur inclue des balises HTML `HEIGHT` et `WIDTH` pour les icônes dans les pages Web générées par le serveur ; `IconsAreLinks`, pour faire en sorte que les icônes agissent comme une partie de l'ancre du lien HTML, en même temps que le nom de fichier, et autres.

AddIconByEncoding

Cette directive nomme des icônes qui seront affichées par fichier, avec codage MIME, dans des listes de répertoire générées par le serveur. Exemple : par défaut, votre serveur Web montre l'icône `compressed.gif` à côté des fichiers codés MIME x-compress et x-gzip dans des listes de répertoire générées par serveur.

AddIconByType

Cette directive nomme des icônes qui s'afficheront à côté des fichiers avec des types MIME dans des listes de répertoire générées par serveur. Par exemple, votre serveur est paramétré pour afficher l'icône `text.gif` à côté de fichiers avec un type MIME " texte " dans des listes de répertoire générées par serveur.

AddIcon

`AddIcon` indique au serveur l'icône à afficher dans les listes de répertoire générées par le serveur pour certains types de fichier ou pour des fichiers avec certaines extensions. Par exemple, votre serveur Web est paramétré pour afficher l'icône `binary.gif` pour les fichiers portant les extensions `.bin` ou `.exe`.

DefaultIcon

`DefaultIcon` nomme l'icône à afficher dans les listes de répertoire générées par le serveur pour les fichiers pour lesquels aucune autre icône n'est spécifiée. `unknown.gif` est la `DefaultIcon` par défaut pour ces fichiers.

AddDescription

Vous pouvez utiliser `AddDescription` pour afficher le texte que vous spécifiez pour certains fichiers dans les listes du contenu de répertoire générées par le serveur (vous devez également activer `FancyIndexing` comme une `IndexOptions`). Vous pouvez nommer des fichiers spécifiques, utiliser des expressions comprenant des caractères spéciaux de recherche ou des extensions de fichier pour spécifier les fichiers auxquels cette directive devrait s'appliquer. Par exemple, vous pourriez utiliser la ligne suivante :

```
AddDescription "Fichier se terminant par .ni" .ni
```

Dans les listes de répertoire générées par serveur, les noms de tous les fichiers portant des extensions `.ni` seraient suivis de la description `Fichier se terminant par .ni`. Il faut également que vous activiez `FancyIndexing`.

ReadmeName

ReadmeName nomme le fichier qui (s'il existe dans le répertoire) sera ajouté à la fin des listes de répertoire générées par serveur. Le serveur Web commencera par essayer d'inclure le fichier comme document HTML, puis essaiera de l'inclure comme texte brut. Par défaut, ReadmeName est paramétré sur README.

HeaderName

HeaderName nomme le fichier qui (s'il existe dans le répertoire) sera ajouté au début des listes de répertoire générées par serveur. Comme ReadmeName, le serveur essaiera, si possible, de l'inclure sous la forme d'un document HTML ou, sinon, comme texte brut.

IndexIgnore

IndexIgnore affiche une liste d'extensions de fichier, de noms de fichier partiels, d'expressions contenant des caractères spéciaux de recherche ou de noms de fichiers complets. Le serveur Web n'inclura pas les fichiers correspondant à l'un de ces paramètres dans les listes de répertoire générées par serveur.

AddEncoding

AddEncoding nomme des extensions de nom de fichier qui devraient spécifier un type de codage particulier. AddEncoding permet également de donner pour instruction à certains navigateurs (pas tous) de décompresser certains fichiers pendant leur téléchargement.

AddLanguage

AddLanguage associe des extensions de nom de fichiers à des langues spécifiques. Cette directive est essentiellement utile pour la négociation de contenu, lorsque le serveur retourne un document parmi d'autres, en fonction de la préférence linguistique du client, telle que définie dans son navigateur.

LanguagePriority

LanguagePriority permet de définir l'ordre de préférence des langues pour le service des fichiers, qui produit un effet si le client n'a paramétré aucune préférence linguistique dans son navigateur.

AddType

Utilisez la directive AddType pour définir des paires de type MIME et d'extension de fichier. Par exemple, si vous utilisez PHP4, votre serveur Web utilise la directive AddType afin de reconnaître les fichiers portant l'extension PHP (.php4, .html .phtml et .php) comme des types MIME PHP. La directive qui suit indique à Apache de reconnaître l'extension de fichier .shtml :

```
AddType text/html .shtml
```

Vous devrez inclure la ligne ci-dessus à l'intérieur des balises de l'hôte virtuel pour tous les hôtes virtuels devant autoriser des fichiers à inclure côté serveur.

AddHandler

`AddHandler` mappe des extensions de fichier sur des modules de commande spécifiques. Par exemple, le module de commande `cgi-script` peut être utilisé en association avec l'extension `.cgi` pour traiter automatiquement un fichier dont le nom se termine par `.cgi` comme un script CGI. Ceci fonctionnera même pour les fichiers situés hors du répertoire `ScriptAlias` (si vous suivez les instructions fournies ici).

Vous avez une ligne CGI `AddHandler` dans votre fichier `httpd.conf` :

```
AddHandler cgi-script .cgi
```

Il faut supprimer le caractère de commentaire de la ligne. Ensuite, Apache exécutera les scripts CGI pour les fichiers se terminant par `.cgi`, même s'ils se trouvent hors du répertoire `ScriptAlias`, qui est défini par défaut pour contenir votre répertoire `/cgi-bin/` dans `/var/www/cgi-bin/`.

Vous devez également définir `ExecCGI` comme `Options` pour tout répertoire contenant un script CGI. Reportez-vous à la la section intitulée *`Directory`* pour plus d'informations sur la définition de `ExecCGI` pour un répertoire. Vous devrez en outre vous assurer que les autorisations sont correctement définies pour les scripts CGI et les répertoires contenant des scripts CGI. Les scripts CGI et tout le chemin d'accès aux scripts doivent être paramétrés sur 0755.

Vous devrez ajouter la même ligne `AddHandler` à votre configuration `VirtualHost` si vous utilisez des hôtes virtuels et voulez qu'ils reconnaissent également des scripts CGI hors de `ScriptAlias`.

Outre les scripts CGI, votre serveur Web utilise également `AddHandler` pour traiter des fichiers HTML et imagemap analysés par le serveur.

Action

`Action` vous permet d'associer un type MIME à un CGI, de sorte que chaque demande d'un fichier de ce type déclenche l'exécution d'un script CGI particulier.

MetaDir

`MetaDir` spécifie le nom d'un répertoire où votre serveur Web doit rechercher des fichiers contenant des informations META (en-têtes HTTP supplémentaires) à inclure lorsqu'il sert des documents.

MetaSuffix

`MetaSuffix` spécifie le suffixe du nom du fichier contenant les informations META (en-têtes HTTP supplémentaires), qui devrait se trouver dans le répertoire `MetaDir`.

ErrorDocument

Par défaut, en cas de problème ou d'erreur, votre serveur Web renvoie un simple message d'erreur (habituellement obscur) au client ayant formulé la demande. Au lieu d'utiliser le paramétrage par défaut, vous pouvez utiliser `ErrorDocument` afin de configurer votre serveur Web pour qu'il renvoie un message personnalisé ou redirige le client vers une URL locale ou externe.

`ErrorDocument` associe simplement un code de réponse HTTP à un message ou à une URL qui sera renvoyé au client.

BrowserMatch

La directive `BrowserMatch` permet à votre serveur de définir des variables d'environnement ou de prendre des mesures appropriées en fonction du champ d'en-tête Utilisateur-Agent HTTP qui identifie le navigateur du client. Par défaut, votre serveur Web utilise `BrowserMatch` pour refuser des connexions à certains navigateurs présentant des problèmes connus de même que pour désactiver les keepalives et vidages d'en-tête HTTP pour les navigateurs ayant des problèmes avec ces actions.

Location

Les balises `<Location>` et `</Location>` permettent de spécifier un contrôle d'accès basé sur l'URL.

L'utilisation suivante des balises `Location` est incluse à l'intérieur des balises `IfModule mod_perl.c`. Ces directives de configuration sont effectives si le DSO `mod_perl.so` est chargé. Reportez-vous à la la section intitulée *Ajout de modules au serveur* pour plus d'informations sur l'ajout de modules à Apache.

Les balises `Location` nomment le répertoire `/var/www/perl` (`Alias` pour `/perl`) comme celui à partir duquel les scripts Perl seront servis. Si un document est demandé avec une URL dans le chemin de laquelle figure la chaîne `/perl` votre serveur Web recherche le script Perl approprié dans `/var/www/perl/`.

Plusieurs autres options de `<Location>` sont identifiées comme des commentaires dans votre fichier `httpd.conf` Si vous voulez activer leur fonctionnalité, supprimez le caractère de commentaire de la section appropriée des directives.

Note **Remarque**

Le module put n'est plus distribué avec le paquetage Apache. Vous devez charger le paquetage `mod_put` séparément.

Immédiatement après les directives Perl décrites plus haut, il y a une section de directives permettant d'activer HTTP PUT (utilisé par la fonction de publication de Netscape Gold qui permet de publier des pages Web sur un serveur Web). Si vous voulez autoriser HTTP PUT, vous devez supprimer le commentaire des lignes suivantes :

```
#Alias /upload /tmp
#<Location /upload>
#    EnablePut On
#    AuthType Basic
#    AuthName Temporary
#    AuthUserFile /etc/httpd/conf/passwd
#    EnableDelete Off
#    umask 007
#    <Limit PUT>
#       require valid-user
#    </Limit>
#</Location>
```

Vous devrez aussi annuler les commentaires des lignes suivantes au début de `httpd.conf`, de façon à ce que le module mod_put se charge au démarrage d'Apache :

```
#LoadModule put_module          modules/mod_put.so

#AddModule mod_put.c
```

Si vous voulez permettre aux personnes qui se connectent depuis votre domaine de consulter des rapports sur l'état du serveur, annulez les caractères de commentaire de la section de directives suivante :

```
#<Location /server-status>
#    SetHandler server-status
#    Order deny,allow
#    Deny from all
#    Allow from .your_domain.com
#</Location>
```

Vous devez remplacer `.votre_domaine.com` par votre nom de domaine de second niveau.

Si vous voulez fournir des rapports de configuration de serveur (y compris des modules installés et des directives de configuration) en réponse à des demandes en provenance de votre domaine, vous devez supprimer les caractères de commentaire des lignes suivantes :

```
#<Location /server-info>
#    SetHandler server-info
#    Order deny,allow
#    Deny from all
#    Allow from .your_domain.com
#</Location>
```

Une fois encore, vous devez remplacer `.votre_domain.com`.

La section de directives suivante utilise des balises `Location` pour permettre l'accès à la documentation dans `/usr/share/doc` (par exemple, avec une URL telle que http://*votre_domaine*/doc/whatever.html). Ces directives permettent uniquement cet accès aux demandes faites depuis l'hôte local.

Une autre utilisation des balises `Location` est définie dans une section identifiée comme un commentaire destinée à permettre un suivi des attaques dirigées contre votre serveur Web qui exploitent un vieux bogue d'avant Apache 1.1. Si vous voulez effectuer le suivi de ces demandes, supprimez le commentaire des lignes suivantes :

```
#<Location /cgi-bin/phf*>
#    Deny from all
#    ErrorDocument 403 http://phf.apache.org/phf_abuse_log.cgi
#</Location>
```

Si ces lignes ne sont pas identifiées comme des commentaires, votre serveur Web redirige toute demande se terminant par `/cgi-bin/phf*` vers un script CGI de journalisation exécuté par le groupe Apache.

ProxyRequests

Si vous supprimez le commentaire des balises `IfModule` entourant la section `ProxyRequests` , votre serveur Apache fonctionnera également comme un serveur Proxy. Vous devez aussi charger le module `mod_proxy`. Pour obtenir des instructions sur la manière de charger des modules, reportez-vous à la la section intitulée *Ajout de modules au serveur*.

ProxyVia

La commande `ProxyVia` contrôle si une ligne d'en-tête HTTP Via: est envoyée en même temps que les demandes ou les réponses transitant par le serveur proxy Apache. L'en-tête Via: indique le nom d'hôte si `ProxyVia` a pour valeur `On`, le nom d'hôte et la version d'Apache s'il a pour valeur `Full`, toutes les lignes Via: sont transférées inchangées s'il a pour valeur `Off`, et les lignes Via: sont supprimées s'il a pour valeur `Block`.

Directives cache

Plusieurs directives cache sont identifiées comme des commentaires dans les balises proxy `IfModule` mentionnées plus haut. Si vous utilisez la fonctionnalité du serveur proxy et voulez également activer le cache proxy, supprimez le commentaire des directives cache en procédant de la manière décrite. Les paramètres par défaut pour vos directives cache devraient être appropriés pour la plupart des configurations.

`CacheRoot` définit le nom du répertoire qui contiendra les fichiers mis en cache. Le `CacheRoot` par défaut est `/var/cache/httpd`.

`CacheSize` définit la quantité d'espace que le cache peut utiliser, exprimée en Ko. La valeur de `CacheSize` par défaut est `5` KB.

`CacheGcInterval` définit un nombre d'heures. Une fois ce délai écoulé, les fichiers du cache sont supprimés si le cache utilise un espace supérieur à celui défini par `CacheSize`. La valeur par défaut de `CacheGcInterval` est de quatre heures.

Les documents HTML mis en cache seront retenus (sans rechargement du serveur Web dont ils proviennent) dans le cache pendant le nombre d'heures maximum défini par `CacheMaxExpire`. La valeur par défaut est de `24` hours.

Le paramètre `CacheLastModifiedFactor` affecte la création d'une date d'expiration pour un document qui a été reçu du serveur sans date d'expiration définie. La valeur par défaut de `CacheLastModifiedFactor` est `0.1`, ce qui signifie que la date d'expiration d'un document de ce type est égale à un dixième du temps écoulé depuis la dernière modification du document.

`CacheDefaultExpire` est le temps d'expiration, exprimé en heures, d'un document reçu à l'aide d'un protocole ne prenant pas en charge les délais d'expiration. La valeur par défaut est d'une heure.

Tout document récupéré sur un hôte ou un domaine correspondant à celui défini dans `NoCache` ne sera pas mis en cache. Si vous avez connaissance d'hôtes ou de domaines dont vous ne voulez pas mettre les documents en cache, supprimez le commentaire devant `NoCache` et définissez ici leurs noms de domaine ou d'hôte.

NameVirtualHost

Vous devrez utiliser la directive `NameVirtualHost` pour l'adresse IP (et le numéro de port, si nécessaire) de tout hôte virtuel nommé que vous configurez. La configuration d'hôtes virtuels nommés est utilisée pour configurer plusieurs hôtes virtuels pour plusieurs domaines, lorsque vous n'avez pas (ou ne voulez pas utiliser) d'adresses IP différentes pour les différents noms de

domaine pour lesquels votre serveur Web sert des documents.

Note **Remarque**

Vous ne pouvez pas utiliser d'hôtes virtuels nommés avec votre serveur sécurisé. Tout hôte virtuel nommé que vous configurez ne peut fonctionner qu'avec des connexions HTTP non sécurisées et avec des connexions non-SSL.

Vous ne pouvez pas utiliser d'hôtes virtuels nommés avec votre serveur sécurisé parce que l'établissement de liaison SSL (lorsque le navigateur accepte le certificat d'authentification du serveur Web sécurisé) intervient avant la demande HTTP qui identifie l'hôte virtuel nommé correct. Autrement dit, l'authentification intervient avant l'identification des différents hôtes virtuels nommés. Si vous voulez utiliser des hôtes virtuels avec votre serveur sécurisé, vous devez opter pour des hôtes virtuels basés sur l'adresse IP.

Si vous utilisez des hôtes virtuels basés sur le nom, supprimez le caractère de commentaire de la directive de configuration `NameVirtualHost` et ajoutez l'adresse IP correcte de votre serveur derrière `NameVirtualHost`. Ajoutez ensuite des informations supplémentaires sur les différents domaines utilisant les balises `VirtualHost` qui entourent `ServerName` pour chaque hôte virtuel, plus toutes les autres directives de configuration exclusivement applicables à cet hôte virtuel.

`VirtualHost`

Des balises `<VirtualHost>` et `</VirtualHost>` entourent toutes les directives de configuration destinées à être appliquées à un hôte virtuel. La plupart des directives de configuration peuvent être utilisées à l'intérieur de balises d'hôte virtuel et s'appliquent exclusivement à cet hôte virtuel particulier.

Un ensemble de balises `VirtualHost` commentées entourent certains exemples de directives de configuration et paramètres fictifs pour les informations que vous devriez fournir pour régler un hôte virtuel. Reportez-vous à la la section intitulée *Utilisation d'hôtes virtuels*, pour avoir plus de détails sur les hôtes virtuels.

`SetEnvIf`

La directive de configuration Apache `SetEnvIf` peut être utilisée pour régler des variables d'environnement en fonction des en-têtes dans les demandes. Dans le fichier `httpd.conf` fourni, elle permet de désactiver la fonction keep-alive HTTP et d'autoriser SSL à fermer la connexion sans générer d'alerte de notification de fermeture du navigateur client. Ce paramètre est nécessaire pour certains navigateurs qui n'interrompent pas la connexion SSL avec une grande fiabilité.

Directives de configuration SSL

Les directives SSL figurant dans le fichier `httpd.conf` de votre serveur sont incluses pour permettre des communications Web sécurisées à l'aide de SSL et TLS.

Pour plus d'informations sur les directives SSL, utilisez votre navigateur pour consulter la page http://localhost/manual/mod/mod_ssl/. Pour plus d'informations sur les directives SSL, reportez-vous à la page http://www.modssl.org/docs/2.8/ssl_reference.html, un chapitre sur mod_ssl rédigé par Ralf Engelschall. Ce document, le *Guide de l'utilisateur*de mod_ssl, commence à l'URL http://www.modssl.org/docs/2.8/ et constitue une excellente référence pour mod_ssl et pour la cryptographie Web en général.

Note **Remarque**

Ne modifiez pas vos directives SSL si vous n'êtes pas absolument certain de savoir ce que vous faites. Dans la plupart des cas, la configuration par défaut des directives SSL convient parfaitement.

Précédent | Sommaire | Suivant
Démarrage et arrêt de `httpd` | Niveau supérieur | Ajout de modules au serveur

Ajout de modules au serveur

Du fait qu'Apache 1.3 prend en charge les objets partagés dynamiques, vous pouvez aisément charger des modules Apache ou compiler vos propres modules pour votre serveur Web. La prise en charge des objets partagés dynamiques signifie qu'il est possible de charger des modules lors de l'exécution. Du fait que les modules ne sont chargés que lorsque c'est nécessaire, ils n'utilisent de mémoire que s'ils sont chargés.

Le groupe Apache fournit une documentation DSO complète sur les objets partagés dynamiques à l'adresse http://httpd.apache.org/docs/dso.html. Une fois votre serveur installé, vous pouvez également consulter la page http://localhost/manual/mod/ afin d'obtenir une documentation sur les modules Apache au format HTML (si vous avez installé le paquetage `apache-manual`).

Pour qu'Apache utilise un module partagé dynamique, celui-ci doit comprendre une ligne `LoadModule` et une ligne `AddModule` dans `httpd.conf`. Par défaut, de nombreux modules comprennent déjà ces deux lignes dans `httpd.conf` ; toutefois, quelques-uns des modules les moins souvent utilisés sont identifiés comme des commentaires. Les modules identifiés comme des commentaires ont été inclus durant la compilation, mais ne sont pas chargés par défaut.

Si vous devez utiliser l'un de ces modules non chargés, reportez-vous au fichier `httpd.conf` pour voir tous les modules disponibles. A chaque module disponible correspond une ligne `LoadModule`. Par exemple, la section `LoadModule` commence par ces sept lignes :

```
#LoadModule mmap_static_module modules/mod_mmap_static.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule env_module         modules/mod_env.so
LoadModule config_log_module  modules/mod_log_config.so
LoadModule agent_log_module   modules/mod_log_agent.so
LoadModule referer_log_module modules/mod_log_referer.so
#LoadModule mime_magic_module  modules/mod_mime_magic.so
```

La plupart des lignes ne sont pas identifiées comme des commentaires, ce qui indique que le module qui y est associé a été compilé et est chargé par défaut. La première ligne est identifiée comme un commentaire, ce qui signifie que le module correspondant (`mmap_static_module`), a été compilé, mais non chargé.

Pour faire en sorte qu'Apache charge un module non chargé, commencez par supprimer le caractère de commentaire de la ligne `LoadModule`. Par exemple, si vous voulez faire en sorte qu'Apache charge `mime_magic_module`, enlevez le caractère de commentaire de cette ligne :

```
#LoadModule mime_magic_module modules/mod_mime_magic.so
```

Supprimez ensuite le caractère de commentaire de la ligne correspondante dans la section `AddModule` du fichier `httpd.conf`. Pour continuer avec l'exemple précédent, supprimez le commentaire de la ligne `mod_mime_magic`, ressemble à ceci :

```
#AddModule mod_mime_magic.c
```

Après avoir supprimé le commentaire des lignes `LoadModule` et `AddModule` pour le module que vous voulez charger, arrêtez, puis démarrez votre serveur Web, comme expliqué à la la section intitulée *Démarrage et arrêt de `httpd`*. Après le démarrage, le module devrait être chargé dans Apache.

Si vous avez votre module personnel, vous pouvez l'ajouter au fichier `httpd.conf`, afin qu'il soit compilé et chargé comme un objet partagé dynamique. Vous avez besoin du paquetage `apache-devel` parce qu'il installe les fichiers à inclure, les fichiers d'en-tête et l'outil de support APache eXtenSion (APXS). APXS utilise les fichiers à inclure et les fichiers d'en-tête pour compiler votre module de manière à ce qu'il fonctionne avec Apache.

Si vous avez écrit votre module personnel ou emprunté celui de quelqu'un d'autre, vous devriez être en mesure d'utiliser APXS pour compiler les sources de votre module en dehors de l'arbre source Apache, sans devoir utiliser d'indicateurs pour compilateur ou éditeur de liens. Pour plus d'informations sur APXS, reportez-vous à la documentation sur Apache à l'adresse http://httpd.apache.org/docs/dso.html.

Après avoir compilé votre module à l'aide d'APXS, placez-le dans `/usr/lib/apache/`. Ensuite, votre module a besoin d'une ligne `LoadModule` et d'une ligne `AddModule` dans le fichier `httpd.conf`. Après la liste `LoadModule` dans `httpd.conf`, ajoutez une ligne indiquant le fichier d'objet partagé pour votre module, comme suit :

```
LoadModule foo_module   modules/mod_foo.so
```

Vous devez modifier le nom du module et celui de votre fichier d'objet partagé de manière appropriée.

A la fin de la liste `AddModule` dans `httpd.conf`, ajoutez une ligne indiquant le fichier de code

source pour votre module, comme suit :

```
AddModule mod_foo.c
```

Vous devez modifier le nom du fichier de code source de façon appropriée.

Une fois les étapes précédentes accomplies, arrêtez et démarrez votre serveur Web en procédant de la manière décrite à la [la section intitulée *Démarrage et arrêt de* `httpd`](). Si vous avez tout fait correctement et si votre module est codé correctement, votre serveur Web doit trouver le module et le charger au démarrage.

Module de sécurité mod_ssl

La portion de sécurité mod_ssl du serveur Web est fournie comme DSO (Dynamic Shared Object, objet partagé dynamique). Ceci signifie que si vous recompilez le serveur Web Apache vous devez vous assurer que le correctif d'extension EAPI du module mod_ssl est appliqué à Apache. Suivez les instructions relatives à la création de mod_ssl dans Apache, incluses dans la documentation mod_ssl, mais ajoutez l'indicateur suivant :

```
./configure [indicateurs utilisateur] --with-eapi-only
```

Ensuite, compilez et installez Apache.

Note **Remarque**

Red Hat ne peut pas prendre en charge des versions recompilées du serveur Web Apache. L'installation de la version fournie est prise en charge, mais si vous recompilez Apache, vous serez livré à vous-même. Ne recompilez pas Apache si vous n'êtes pas absolument certain de savoir ce que vous faites.

Utilisation d'hôtes virtuels

Vous pouvez utiliser la fonction des hôtes virtuels d'Apache pour exécuter différents serveurs pour différentes adresses IP, différents noms d'hôte ou différents ports sur le même ordinateur. Si l'utilisation des hôtes virtuels vous intéresse, vous trouverez des informations exhaustives dans la documentation d'Apache installée sur votre ordinateur ou sur le Web à l'adresse http://httpd.apache.org/docs/vhosts/.

Note **Remarque**

Vous ne pouvez pas utiliser d'hôtes virtuels basés sur le nom avec Red Hat Linux Advanced Server parce que l'établissement de la liaison SSL (lorsque le navigateur accepte le certificat sécurisé du serveur Web) se produit avant la demande HTTP identifiant l'hôte virtuel nommé approprié. Si vous voulez utiliser des hôtes virtuels basés sur le nom, ils ne fonctionneront qu'avec votre serveur Web non sécurisé.

Les hôtes virtuels sont configurés dans le fichier `httpd.conf`, de la manière décrite à la la section intitulée *Directives de configuration dans `httpd.conf`*. Lisez cette section avant de commencer à changer la configuration des hôtes virtuels sur votre ordinateur.

Hôte virtuel du serveur Web sécurisé

La configuration par défaut de votre serveur Web utilise un serveur non sécurisé et un serveur sécurisé. Les deux serveurs utilisent la même adresse IP et le même nom d'hôte, mais contrôlent des ports différents et le serveur sécurisé est un hôte virtuel. Cette configuration vous permet de servir des documents sécurisés et non sécurisés avec un maximum d'efficacité. Comme vous le savez, les transmissions HTTP sécurisées sont plus lentes que les transmissions non sécurisées, par conséquent vous servirez beaucoup moins de pages à la seconde avec un serveur sécurisé. Vous devez en tenir compte lorsque vous choisissez les informations à inclure sur votre serveur sécurisé et non sécurisé.

Les directives de configuration pour votre serveur sécurisé se trouvent entre des balises d'hôte virtuel dans le fichier `httpd.conf`. Si vous devez modifier la configuration de votre serveur sécurisé, il faudra modifier les directives de configuration entre les balises d'hôte virtuel.

Le serveur Web non sécurisé est configuré comme hôte « non virtuel » dans le fichier `httpd.conf`. Si vous voulez apporter une modification à votre serveur Web non sécurisé, il faudra modifier les directives de configuration hors des balises d'hôte virtuel.

Par défaut, les serveurs Web sécurisé et non sécurisé partagent le même `DocumentRoot`. Pour modifier `DocumentRoot` de manière à ce qu'il ne soit plus partagé par les serveurs sécurisé et non sécurisé, modifiez l'une des directives `DocumentRoot`. Le `DocumentRoot` situé hors des balises d'hôte virtuel définit le `DocumentRoot` pour votre serveur Web non sécurisé. Le `DocumentRoot` situé à l'intérieur des balises d'hôte virtuel qui définissent votre serveur sécurisé lui sera destiné.

Votre serveur sécurisé contrôle le port 443, tandis que votre serveur Web non sécurisé contrôle le port 80. Pour empêcher le serveur Web non sécurisé d'accepter des connexions, recherchez la ligne suivante :

```
Port 80
```

Modifiez la ligne ci-dessus comme suit :

```
Port 443
```

Ensuite, modifiez la ligne `Listen 80` en lui ajoutant un caractère de commentaire.

Configuration d'hôtes virtuels

Pour créer un hôte virtuel, vous devez modifier les lignes d'hôtes virtuels (exemple dans `httpd.conf`) ou cré votre propre section d'hôte virtuel.

Les exemples de lignes d'hôte virtuel correspondent à ce qui suit.

```
#<VirtualHost ip.address.of.host.some_domain.com>
#    ServerAdmin webmaster@host.some_domain.com
#    DocumentRoot /www/docs/host.some_domain.com
#    ServerName host.some_domain.com
#    ErrorLog logs/host.some_domain.com-error_log
#    CustomLog logs/host.some_domain.com-access_log common
#</VirtualHost>
```

Supprimez le commentaire de toutes les lignes. Ajoutez ensuite les informations correctes concernant votre hôte virtuel.

Dans la première ligne, remplacez `ip.address.of.host.some_domain.com` par l'adresse IP de

votre serveur. Remplacez `ServerName` par un nom de domaine *valide* à utiliser pour l'hôte virtuel.

Vous devrez aussi supprimer le caractère de commentaire de l'une des lignes `NameVirtualHost` :

```
#NameVirtualHost 12.34.56.78:80
#NameVirtualHost 12.34.56.78
```

Remplacez l'adresse IP par celle (ainsi que le port, si nécessaire) de l'hôte virtuel.

Si vous configurez un hôte virtuel et souhaitez qu'il contrôle un port non défini par défaut, il faudra configurer un hôte virtuel pour ce port, puis ajouter une directive `Listen` correspondant à ce port.

Ajoutez ensuite le numéro de port à la première ligne de la configuration de l'hôte virtuel. La première ligne doit ressembler à ceci :

```
<VirtualHost ip_address_of_your_server:12331>
```

Cette ligne crée un hôte virtuel contrôlant le port 12331.

Vous devez redémarrer `httpd` pour lancer un nouvel hôte virtuel. Pour obtenir des instructions sur le démarrage et l'arrêt de `httpd`, reportez-vous à la la section intitulée *Démarrage et arrêt de `httpd`*.

Pour plus d'informations sur la création et la configuration d'hôtes virtuels nommés et d'hôtes virtuels basés sur l'adresse IP, consultez la page Web http://httpd.apache.org/docs/vhosts/. Reportez-vous à la documentation relative à l'hôte virtuel du groupe Apache pour plus de détails sur l'utilisation des hôtes virtuels.

Autres ressources

Pour en savoir plus sur Apache, veuillez vous reporter aux ressources qui suivent.

Sites Web utiles

- http://httpd.apache.org — le site Web officiel du serveur Web Apache, offrant de l'information sur toutes les directives et tous les modules par défaut.
- http://www.modssl.org — site Web officiel de mod_ssl.
- http://www.apacheweek.com — Apache Week de Red Hat est la ressource en ligne par excellence publié toutes les semaines en ligne .

Livres sur le sujet

- *Apache Desktop Reference* de Ralf S. Engelschall; Addison Wesley

  Ecrit par Ralf Engelshall, membre de l'ASF et auteur de mod_ssl, *Apache Desktop Reference* est un guide de référence concis et exhaustif pour l'utilisation d'Apache, plus spécialement pour sa compilation, sa configuration et son exécution. Vous pouvez également télécharger ce livre en ligne à l'adresse http://www.apacheref.com/.
- *Professional Apache* de Peter Wainwright; Wrox Press Ltd

  Professional Apache est un des nombreux livres de la collection " Programmer to Programmer " de de la maison d'édition Wrox Press Ltd, destiné aux utilisateurs d'Apache d'expérience et aux administrateurs Web qui utilisent Apache pour la première fois.
- *Administering Apache* de Mark Allan Arnold; Osborne Media Group

  Ce livre est destiné aux fournisseurs d'accès à Internet désireux d'offrir plus de services sécurisés.
- *Apache Server Unleashed* de Richard Bowen, et al ; SAMS BOOKS

  Le livre de aspire à devenir l'ultime source encyclopédique pour Apache.
- *Apache Pocket Reference* d'Andrew Ford, Gigi Estabrook ; O'Reilly

  est la dernière nouveauté de la collection O'Reilly Pocket Reference.

Précédent
Utilisation d'hôtes virtuels

Sommaire
Niveau supérieur

Suivant
Courrier électronique

Chapitre 16. Courrier électronique

Le courrier électronique est l'un des services les plus utilisés sur Internet. Red Hat Linux vous offre de nombreuses façons d'utiliser le courrier électronique, que vous soyez un utilisateur de bureau ou un administrateur système.

Ce chapitre traite des protocoles de courrier électronique couramment utilisés aujourd'hui et des divers programmes conçus pour accomplir des tâches variées relatives à la messagerie électronique.

Protocoles

Le courrier électronique, tout comme d'autres services réseau, fait appel à une panoplie de protocoles. Ceux-ci permettent à des ordinateurs différents, exécutant souvent des systèmes d'exploitation et des programmes de messagerie électronique différents, de communiquer entre eux et de transférer le courrier de façon à ce qu'il arrive à destination.

Les protocoles suivants sont les plus fréquemment utilisés pour le transfert de courrier électronique entre systèmes.

IMAP

Le protocole IMAP (*Internet Message Access Protocol*) est une méthode utilisée par des applications client de messagerie pour accéder à distance à des messages stockés. Lorsque l'on utilise IMAP, souvent appelé IMAP4 en raison de la version utilisée, les messages électroniques restent sur le serveur distant, où les utilisateurs peuvent les lire ou les supprimer, de même que créer, renommer ou supprimer des boîtes aux lettres pour stocker du courrier.

En outre, IMAP est compatible à 100 % avec d'importantes normes de messagerie Internet, telles que MIME (Multipurpose Internet Mail Extensions) pour permettre l'envoi de fichiers joints. De nombreux clients de messagerie électronique utilisant IMAP peuvent aussi être configurés pour mettre en cache une copie des messages localement, de sorte qu'il soit possible de parcourir les messages lus précédemment sans être directement connecté au serveur IMAP.

IMAP est surtout utilisé par les utilisateurs qui veulent pouvoir avoir accès à leur courrier électronique depuis différents ordinateurs, étant donné que les messages sont stockés dans un emplacement centralisé

et sont accessibles depuis tout système muni d'un client de messagerie IMAP et d'une connexion au serveur IMAP distant. De plus, les utilisateurs qui se branchent à Internet ou à un réseau privé via une connexion bas débit utilisent souvent IMAP car seule l'information d'en-tête du message est d'abord récupérée. Cela leur permet de remettre le téléchargement de messages accompagnés de pièces jointes de grande taille à un moment où leur connexion limitée est moins utilisée. Cette méthode permet aussi de supprimer des messages non désirés sans voir leur corps de message et, par conséquent, sans devoir les télécharger via la connexion réseau.

Les documents RFC (*Request for Comment*) qui couvrent IMAP contiennent des détails et éclaircissements sur le fonctionnement de ce protocole. RFC-1730 a d'abord défini la façon d'utilisation d'IMAP de la version 4, mais RFC-2060 traite des mises en application du protocole IMAP actuel, utilisé avec de nombreux serveurs IMAP, appelé IMAP4rev1.

Le paquetage `imap` dans Red Hat Linux permet aux utilisateurs de se connecter à votre système et de recevoir leur courrier à l'aide d'IMAP. Des connexions IMAP sécurisées sont prises en charge au moyen de la technologie SSL (Secure Socket Layer) construite dans le démon `imapd`, qui permet d'utiliser le fichier de certificat `/usr/share/ssl/certs/imapd.pem`. Le programme `stunnel` n'est pas requis pour offrir un cryptage SSL aux connexions IMAP, bien qu'il puisse être utilisé. Reportez-vous à la la section intitulée *Serveurs de messagerie sécurisés* pour en savoir plus sur ces deux options de cryptage.

D'autres clients IMAP, gratuits ou commerciaux, sont aussi disponibles, plusieurs desquels offrent d'ailleurs des fonctionnalités supplémentaires par rapport à IMAP. Vous trouverez une liste exhaustive à l'adresse http://www.imap.org/products/longlist.htm.

POP

Le protocole POP (*Post Office Protocol*) permet aux clients de messagerie de retirer du courrier depuis des serveurs distants et de l'enregistrer sur leur ordinateur local. La plupart des clients de messagerie POP sont configurés automatiquement pour supprimer les messages sur le serveur de messagerie une fois qu'ils ont été transférés sur le système client, mais cela peut être modifié.

Pour se connecter à un serveur POP, le client de messagerie ouvre une connexion TCP au port 110 sur le serveur. Lorsque la connexion est effectuée, le serveur POP envoie un message de bienvenue au client POP, après quoi les deux ordinateurs s'envoient des commandes et des réponses spécifiées par le protocole. Dans le cadre de cette communication, le client POP doit effectuer l'authentification dans *Authentication State*, où le nom d'utilisateur et le mot de passe sont envoyés au serveur POP. Si l'authentification réussit, alors le client POP passe à *Transaction State*, où il est possible d'utiliser des commandes, telles que `LIST`, `RETR` et `DELE` pour afficher la liste, télécharger et supprimer des messages depuis le serveur. Les messages supprimés directement depuis le serveur ne sont pas retirés du serveur tant que le client n'a pas envoyé la commande `QUIT` pour terminer la session. A ce stade, le

serveur POP entre dans *Update State*, où il supprime les messages indiqués pour la suppression et nettoie toute ressource résiduelle de cette session.

POP est un protocole beaucoup plus simple qu'IMAP car il nécessite l'envoi d'un moins grand nombre de commandes entre le client et le serveur. POP est aussi un peu plus utilisé, bien que la plupart des principaux clients de messagerie puissent utiliser l'un ou l'autre des deux protocoles sans problème.

La plupart des utilisateurs de POP n'utilisent qu'un système pour lire leur courrier et téléchargent leurs messages sur cet ordinateur pour les stocker. POP fonctionne très bien également si vous n'avez pas une connexion continue à Internet ou au réseau sur lequel se trouve votre serveur de messagerie.

De nombreux documents RFC traitent du protocole POP, mais RFC-1939 définit les bases de POP3, la version actuelle.

Vous pourriez, à l'occasion, rencontrer des variantes moins utilisées du protocole POP :

- *APOP* — POP3 avec authentification MDS, où une portion codée de votre mot de passe est envoyée du client de messagerie au serveur plutôt que de l'envoyer en texte en clair.
- *KPOP* — POP3 avec authentification Kerberos. Reportez-vous au Chapitre 11 pour avoir plus d'informations sur l'authentification Kerberos.
- *RPOP* — POP3 avec authentification RPOP, qui utilise un identificateur (ID) publié pour chaque utilisateur, semblable à un mot de passe, pour identifier les requêtes POP. Cependant, cet ID n'est pas crypté, donc RPOP n'est pas plus sécurisé que le POP standard.

De nombreux serveurs, clients et autres applications variées POP sont disponibles sous Red Hat Linux. Si vous préférez un client de messagerie graphique, **Mozilla Mail** est un excellent choix. De plus, d'autres utilitaires de courrier électronique, tels que Fetchmail, peuvent récupérer des messages via le protocole POP. Si vous utilisez votre système Red Hat Linux en tant que serveur de messagerie, le paquetage `imap` contient les démons POP2 (`ipop2`) et POP3 (`ipop3`) dans le répertoire `/usr/sbin`.

SMTP

Alors que les protocoles IMAP et POP permettent aux utilisateurs de recevoir et lire leur courrier électronique, le protocole SMTP (*Simple Mail Transfer Protocol*) est utilisé pour envoyer du courrier. Les messages sortant font appel à SMTP pour passer de l'ordinateur client à l'ordinateur serveur, d'où ils partent pour leur destination finale. Autrement, deux serveurs de messagerie essaient de transférer un message entre eux à l'aide de SMTP de façon à ce qu'ils puissent communiquer, même s'il s'agit de deux plates-formes complètement différentes.

SMTP utilise le port 25 sur le serveur pour ses communications. Un échange SMTP de base se déroule comme suit : le système qui se connecte (1) émet une commande `MAIL From:`

<adresse_électronique> pour commencer l'échange ; le système qui reçoit (2) le message répond par un message `250` pour accuser réception de la première commande. Ensuite, le système 1 transmet les adresses électroniques de destination au système 2, suivies d'un message `DATA`. Cela indique au système 2 que la prochaine partie de la communication sera le corps de message. Lorsque le système 1 a terminé de traiter le message électronique, il place un point (`.`) sur une ligne. A ce stade, le message est considéré comme envoyé.

SMTP prend également en charge des cas nécessitant le réacheminement de messages entre systèmes, lorsque le système qui reçoit sait où envoyer le message. Le protocole peut s'assurer que certains utilisateurs sont servis par un serveur précis (commande `VRFY`) ou ouvrir une liste d'adresses (commande `EXPN`). Le courrier électronique peut aussi être retransmis entre deux serveurs SMTP, si les deux systèmes autorisent ce genre de pratique.

Contrairement à IMAP et POP, SMTP ne nécessite aucune authentification sous sa forme de base absolue. Cela encourage malheureusement le pollupostage (spam), étant donné qu'un utilisateur non local pourrait utiliser votre système pour envoyer ou retransmettre des messages à des listes entières de participants, donc utiliser les ressources et la bande passante de votre système pour envoyer des spams. Les applications SMTP modernes ont fait des pas de géant pour minimiser ces situations en limitant la retransmission et en n'autorisant que les hôtes connus à envoyer du courrier électronique.

Le document RFC-821 souligne le comportement de base de SMTP, mais de nombreuses extensions SMTP, rendues possibles par RFC-1869, ont ajouté des fonctionnalités supplémentaires à SMTP avec les années et de nouvelles commandes. Si vous commencez une communication avec un serveur SMTP à l'aide de la commande `EHLO` au lieu de la commande `HELO`, le serveur qui se connecte peut s'identifier en tant que serveur prenant en charge les extensions SMTP. Le serveur qui reçoit répond alors par une ligne `250` qui contient les diverses extensions SMTP prises en charge. Puis, le serveur qui se connecte peut utiliser les extensions prises en charge à sa guise pour atteindre les objectifs de la communication.

Une des extensions notables concerne l'ajout de l'authentification SMTP par le biais de la commande `AUTH`, tel qu'indiqué dans RFC-2554. Une autre extension SMTP très utilisée est décrite dans RFC-2034, qui traite de l'utilisation de codes d'erreur normalisés et séparés par des points entre les applications SMTP. Les divers documents RFC sur SMTP fournissent un bon aperçu de la façon dont les messages électroniques se déplacent sur Internet. De plus, vous pouvez vous connecter à un serveur SMTP via Telnet en spécifiant le port 25, tel que `telnet hôte_local 25`. L'une des meilleures façons d'apprendre le fonctionnement des communications SMTP est d'exécuter quelques commandes et d'envoyer des messages électroniques manuellement.

Red Hat Linux 7.3 utilise Sendmail comme programme SMTP par défaut, bien que d'autres applications, avec les mêmes fonctionnalités et plus simples à utiliser, telles que Postfix, soient disponibles.

Autres ressources Niveau supérieur Les différents types de programme de messagerie électronique

Les différents types de programme de messagerie électronique

Il existe trois types de programme de messagerie électronique, ayant chacun un rôle bien précis dans le processus de déplacement et de gestion des messages. 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 de programme est important pour assurer que les messages arrivent à la bonne destination.

Agent de gestion de courrier

Un AGC (*agent de gestion de courrier*) est un programme qui permet (au moins) à l'utilisateur de lire et composer des messages électroniques. On utilise souvent l'expression *client de messagerie* lorsque l'on parle d'AGC. Bien entendu, de nombreux AGC aident les utilisateurs à faire bien plus que cela ; ils leur permettent notamment de recevoir des messages via les protocoles POP ou IMAP, de créer des boîtes aux lettres pour stocker les messages ou de les aider à présenter de nouveaux messages à des programmes agent de transfert de courrier qui s'occupent d'envoyer les messages à la destination finale.

Les programmes AGC peuvent être graphiques, tels que **Mozilla Mail** ou avoir une interface texte très simple, tels que **Mutt** ou **Pine**.

Agent de transfert de courrier

Un ATC (*agent de transfert de courrier*) sert à transférer des messages électroniques entre des ordinateurs qui utilisent SMTP. Un message peut requérir l'utilisation de plusieurs ATC lorsqu'il se déplace vers sa destination finale. Dans la plupart des cas, les utilisateurs ignorent complètement la présence des ATC, et ce même si tous les messages sont envoyés à l'aide d'au moins un ATC.

Alors que l'acheminement de messages entre ordinateurs peut sembler plutôt simple et direct, l'ensemble du processus qui a pour but de décider si un ATC donné peut ou devrait accepter un message à envoyer à un hôte distant est en fait assez complexe. De plus, en raison des problèmes créés par les spams, l'utilisation d'un ATC donné est généralement limitée par la configuration même de l'ATC ou par l'accès réseau au système qui l'exécute.

Nombre d'AGC plus gros et plus complexes peuvent aussi être utilisés pour envoyer des messages. Toutefois, il ne faut pas confondre cette opération avec l'opération d'un vrai ATC. Pour que des utilisateurs n'exécutant pas leur propre ATC puissent déplacer leurs messages à l'extérieur de leur ordinateur et les envoyer vers des ordinateurs distants, ils doivent utiliser une fonction de l'AGC qui transfère les messages vers un ATC qu'ils sont autorisés à utiliser. Cependant, l'AGC n'achemine pas directement le message au serveur de messagerie du destinataire — ce rôle est réservé à l'ATC.

Red Hat Linux utilise Sendmail en tant qu'ATC par défaut, bien que d'autres ATC puissent être utilisés. Il est important que vous désactiviez l'ATC courant avant d'en activer un autre, sinon ils essaieront tous deux d'obtenir le port 25, le port par défaut de SMTP.

Agent de distribution du courrier

L'ADC (*agent de distribution du courrier*) est utilisé par l'ATC pour acheminer le courrier vers la boîte aux lettres d'un utilisateur spécifique. Dans de nombreuses situations, un ADC est en fait un ADL (*agent de distribution locale*), tel que `/bin/mail` ou Procmail. Cependant, Sendmail peut aussi jouer le rôle d'un ADC, notamment lorsqu'il accepte un message pour un utilisateur local et l'ajoute à son fichier spoole de courrier électronique. Tout programme traitant un message pour la distribution au point où il peut être lu par un AGC peut être considéré comme un ADC. Notez que les ADC ne transportent pas les messages entre les systèmes ou ne s'interfacent pas avec l'utilisateur final.

De nombreux utilisateurs n'utilisent pas directement les ADC car seuls les ATC et AGC sont nécessaires à l'envoi et la réception de courrier. Toutefois, certains ADC peuvent être utilisés pour trier les messages avant qu'ils ne soient lus par l'utilisateur, ce qui aide grandement si ce dernier reçoit beaucoup de courrier.

Sendmail

Red Hat Linux se sert de Sendmail en tant qu'ATC pour acheminer les messages, qu'ils soient destinés à des utilisateurs sur un même système ou à des destinations distantes. Il existe d'autres ATC (qui peuvent être utilisés avec Red Hat Linux), mais la plupart des administrateurs choisissent Sendmail comme ATC pour sa puissance, son évolutivité et sa conformité à des normes Internet importantes, telles que SMTP.

La tâche principale de Sendmail, tout comme les autres ATC, est de déplacer de façon sécurisée des messages électroniques entre des hôtes, utilisant généralement le protocole SMTP. Toutefois, Sendmail est hautement configurable, ce qui vous permet de contrôler presque tous les aspects du traitement des messages, y compris le protocole à utiliser.

Histoire

Les racines de Sendmail remontent à la naissance du courrier électronique, soit au cours de la décennie précédant l'arrivée d'ARPANET, le précurseur d'Internet. A cette époque, la boîte aux lettres de chaque utilisateur était en fait un fichier que seul l'utilisateur en question pouvait lire et les applications de messagerie se limitaient à ajouter du texte dans ce fichier. Les utilisateurs devaient alors parcourir tout leur fichier courrier pour trouver d'anciens messages et la lecture des nouveaux messages était une corvée. Le premier véritable transfert de fichier de message électronique entre deux hôtes n'eut lieu qu'en 1972, alors que l'on commença à déplacer des messages par FTP sur le protocole de réseau NCP. Cette forme simplifiée de communication devint rapidement très populaire, au point où elle finit par constituer l'essentiel du trafic d'ARPANET et cela en moins d'un an.

Toutefois, le manque de normalisation entre les protocoles concurrents fit en sorte qu'il était beaucoup plus difficile d'envoyer des messages à partir de certains systèmes et cela se poursuivit jusqu'à la normalisation TCP/IP d'ARPANET en 1982. Un nouveau protocole, SMTP, se matérialisa alors pour l'acheminement des messages. Toutes ces améliorations, conjuguées aux fichiers HOST qui furent remplacés par DNS, permirent à des ATC complets de voir le jour. Sendmail, qui dérive d'un système de distribution de courrier précédent, appelé Deliverymail, devint vite la norme alors qu'Internet grandissait et devenait de plus en plus utilisé.

Objectif et limites

Il est important de bien comprendre ce qu'est Sendmail et ce qu'il peut faire pour vous, de même que ce

qu'il n'est pas. En cette période d'applications monolithiques qui ont des rôles multiples, vous pourriez penser que Sendmail est la seule application dont vous avez besoin pour exécuter un serveur de messagerie au sein de votre organisation. Techniquement, cela est vrai car Sendmail peut désynchroniser du courrier sur vos répertoires utilisateur et accepter de nouveaux messages via la ligne de commande. Cependant, la plupart des utilisateurs désirent 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 alors, ils pourraient préférer une interface Web pour avoir accès à leur boîte aux lettres. Ces autres applications fonctionnent de concert avec Sendmail et SMTP, mais existent en réalité pour différentes raisons et peuvent fonctionner séparément les unes des autres.

Cette section n'a pas comme objectif d'expliquer tout ce pourquoi Sendmail devrait ou pourrait être configuré. Vu les centaines d'options différentes et réglages possibles, des volumes entiers ont été écrits pour vous aider et vous expliquer tout ce qu'il est possible de faire avec Sendmail et les façons de régler d'éventuels problèmes. Vous devriez consulter les nombreuses sources de renseignements en ligne ou imprimées sur Sendmail afin de l'utiliser au meilleur de ses possibilités pour vos propres besoins.

Enfin, vous devriez tout de même savoir quels sont les fichiers installés par défaut avec Sendmail sur votre système et savoir comment procéder à des modifications élémentaires de sa configuration. Vous devriez aussi connaître les façons de faire cesser les messages électroniques indésirables (spams) et d'étendre Sendmail avec le protocole LDAP (*Lightweight Directory Access Protocol*).

Installation de Sendmail par défaut

Bien qu'il vous soit possible de télécharger le code source de Sendmail et de construire votre propre copie, la plupart des utilisateurs préfèrent utiliser la version de Sendmail installée par défaut avec leur système Red Hat Linux. Vous pouvez aussi utiliser les CD-ROM de Red Hat Linux pour réinstaller le paquetage RPM `sendmail` à un autre moment. Notez que vous devez modifier le fichier de configuration par défaut de Sendmail pour l'utiliser en tant que serveur de courrier électronique pour plus d'un seul hôte. Voyez la section intitulée *Modifications courantes de la configuration de Sendmail* pour plus de détails.

Après l'installation, le fichier exécutable `sendmail` est placé dans le répertoire `/usr/sbin`.

Le fichier de configuration de Sendmail (`sendmail.cf`), long et détaillé, est installé dans `/etc`. Vous ne devriez pas modifier directement le fichier `sendmail.cf`, à moins de très bien savoir ce que vous faites car il est très long et complexe. Si vous souhaitez apporter des modifications à Sendmail, modifiez plutôt le fichier `/etc/mail/sendmail.mc` et utilisez le processeur de macros `m4` qui est inclus pour créer un nouveau `/etc/sendmail.cf` (après avoir fait une copie de sauvegarde du fichier `/etc/sendmail.cf` original bien entendu). Vous trouverez plus de renseignements sur la configuration de Sendmail à la la section intitulée *Modifications courantes de la configuration de*

Sendmail.

Divers fichiers de configuration Sendmail sont installés dans `/etc/mail`, notamment :

- `access` — Spécifie les systèmes qui peuvent utiliser Sendmail pour retransmettre du courrier électronique.
- `domaintable` — Vous permet d'offrir le mappage de noms de domaine.
- `local-host-names` — L'endroit où vous placez tous les alias pour votre ordinateur.
- `mailertable` — Spécifie des instructions qui écrasent le routage de domaines spécifiques.
- `virtusertable` — Vous permet de faire une forme de dénomination spécifique au domaine, ce qui permet à des domaines virtuels multiples d'être hébergés sur un ordinateur.

Plusieurs fichiers de configuration 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 puisse appliquer les modifications apportées à la configuration. Pour placer les changements apportés à ces fichiers de configuration dans leurs fichiers de base de données, vous devez exécuter la commande `makemap hash /etc/mail/<nom> < /etc/mail/<nom>`, où *<nom>* est le nom du fichier de configuration à convertir.

Exemple : si vous voulez que tous les messages électroniques destinés à tout compte `domaine.com` soient envoyés à <bob@autredomaine.com>, vous devez ajouter une ligne au fichier `virtusertable` :

```
@domaine.com        bob@autredomaine.com
```

Figure 16-1. Exemple `virtusertable`

Ensuite, pour ajouter cette nouvelle information au fichier `virtusertable.db`, exécutez `makemap hash /etc/mail/virtusertable < /etc/mail/virtusertable` en tant que super-utilisateur. Cela aura pour effet de créer un nouveau fichier `virtusertable.db` qui contient la nouvelle configuration.

Modifications courantes de la configuration de Sendmail

Bien qu'un fichier `sendmail.cf` soit installé par défaut dans `/etc` lors de l'installation de Red Hat Linux, vous devez le modifier pour utiliser quelques unes des fonctions les plus avancées du programme.

Lorsque vous modifiez le fichier de configuration Sendmail, il vaut mieux générer un fichier

`/etc/sendmail.cf` entièrement nouveau au lieu d'en éditer un existant.

Important **Important**

Avant de modifier le fichier `sendmail.cf`, il vaut mieux effectuer une sauvegarde de la version par défaut.

Pour ajouter la fonctionnalité désirée à Sendmail, éditez le fichier `/etc/mail/sendmail.mc`. Quand vous avez fini, utilisez le processeur de macros`m4` pour générer un nouveau fichier `sendmail.cf` en exécutant la commande `m4 /etc/mail/sendmail.mc > /etc/sendmail.cf`. Après avoir créé un nouveau fichier `/etc/sendmail.cf`, vous devez redémarrer Sendmail pour qu'il devienne effectif. Le moyen le plus simple pour cela est de taper la commande `/sbin/service sendmail restart`, connecté en tant que root.

Par défaut, le processeur de macros `m4` est installé avec Sendmail. Il est inclus dans le paquetage `sendmail-cf`.

Important **Important**

Le fichier `sendmail.cf` par défaut n'autorise pas Sendmail à accepter des connexions réseau de tout autre hôte que l'ordinateur local. Si vous souhaitez configurer sendmail en tant que serveur pour d'autres clients, éditez `/etc/mail/sendmail.mc` et modifiez les `DAEMON_OPTIONS` pour une écoute des périphériques de réseau ou des commentaires généraux sur cette option. Puis régénérez `/etc/sendmail.cf`.

Cette configuration sera suffisante pour la plupart des sites exclusivement SMTP. Elle *ne fonctionnera pas* pour les sites UUCP (UNIX to UNIX Copy); vous devrez générer un nouveau fichier `sendmail.cf` si vous devez utiliser les transferts de courrier UUCP.

Vous devriez consulter le fichier `/usr/share/sendmail-cf/README` avant de modifier l'un ou l'autre des fichiers contenus dans les répertoires sous le répertoire `/usr/share/sendmail-cf` car ils peuvent affecter la configuration des futurs fichiers `/etc/sendmail.cf`.

Mascarade

L'une des configurations Sendmail communes est d'avoir un seul ordinateur qui agit comme passerelle de messagerie pour tous les ordinateurs sur un réseau. Par exemple, une société pourrait vouloir avoir un ordinateur appelé `mail.bigcorp.com` qui s'occupe de tout son courrier. Ajoutez sur cet ordinateur le nom des ordinateurs pour lesquels `mail.bigcorp.com` gère le courrier dans `/etc/mail/local-host-names`. Voici un exemple :

```
# sendmail.cw - indiquez tous les alias pour votre ordinateur
# here.
torgo.bigcorp.com
poodle.bigcorp.com
devel.bigcorp.com
```

Figure 16-2. Exemple de réglages pour `local-host-names`

Sur les autres ordinateurs, `torgo`, `poodle` et `devel`, éditez `/etc/sendmail.cf` pour les "déguiser" en tant que `mail.bigcorp.com` lorsqu'ils envoient du courrier ou réacheminent du courrier local vers `bigcorp.com`. Trouvez les lignes `DH` et `DM` dans `/etc/sendmail.cf` et modifiez-les comme suit :

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

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

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

Figure 16-3. Exemple de réglages pour `sendmail.cf`

Avec ce genre de configuration, l'on pensera que tout le courrier envoyé provient de `bigcorp.com` et tout le courrier envoyé à `torgo.bigcorp.com` ou aux deux autres hôtes sera acheminé à `mail.bigcorp.com`.

Faire cesser les spams avec Sendmail

Les *spams* peuvent être définis comme étant des messages électroniques inutiles et indésirables reçus par un utilisateur qui ne connaît probablement pas l'expéditeur ni n'a demandé de recevoir ces messages. Il s'agit d'un abus très perturbateur, coûteux et répandu des normes de communication Internet.

Sendmail facilite (relativement) le blocage des nouvelles techniques utilisées pour envoyer des spams depuis votre système. Il bloque même un grand nombre des méthodes d'envoi de spams les plus communes par défaut. Il vous faudrait donc les activer volontairement en modifiant votre fichier `/etc/mail/sendmail.mc` d'une certaine manière pour que votre système puisse envoyer des spams.

Exemple : le réacheminement de messages SMTP, aussi appelé *retransmission SMTP* (relaying), a été désactivé par défaut depuis la version 8.9. de Sendmail. Auparavant, Sendmail aurait dirigé votre hôte de messagerie (`x.org`) de façon à ce qu'il accepte des messages d'un individu (`y.com`) et les envoie à un autre individu (`z.net`). Maintenant cependant, vous devez indiquer de façon spécifique à Sendmail d'autoriser un domaine à retransmettre du courrier par le biais de votre domaine. Editez simplement le fichier `/etc/mail/relay-domains` et redémarrez Sendmail en entrant la commande `service sendmail restart` en tant que super-utilisateur pour activer les changements.

Par contre, il arrive souvent que vos utilisateurs soient bombardés de spams provenant d'autres serveurs via Internet qui ne sont pas sous votre contrôle. Dans ce cas, vous pouvez utiliser les fonctions de contrôle d'accès de Sendmail, disponibles par l'entremise du fichier `/etc/mail/access`. En tant que super-utilisateur, ajoutez les domaines que vous aimeriez bloquer ou autoriser. Exemple :

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

Figure 16-4. Exemple de réglages pour `access`

Vu que `/etc/mail/access` est une base de données, vous devez utiliser `makemap` pour activer vos changements en recréant la mappe de la base de données. Cela est très simple à faire ; il suffit d'exécuter la commande `makemap hash /etc/mail/access < /etc/mail/access` en tant que super-utilisateur.

Cet exemple montre que tout message électronique envoyé par `badspammer.com` sera bloqué à l'aide d'un code d'erreur 550 conforme à RFC-821 et qu'un message est retourné à l'expéditeur, sauf pour les messages envoyés par le sous-domaine `tux.badspammer.com`, qui seront acceptés. La dernière ligne montre que tout message envoyé depuis le réseau 10.0.*.* peut être retransmis au moyen de votre serveur de messagerie.

Comme vous pouvez l'imaginer, cet exemple ne fait qu'effleurer la surface du potentiel de Sendmail en termes d'autorisation ou d'interdiction d'accès. Reportez-vous à `/usr/share/doc/sendmail/README.cf` pour avoir des renseignements plus détaillés et d'autres exemples.

Utilisation de Sendmail avec LDAP

L'utilisation de LDAP (*Lightweight Directory Access Protocol*) est une façon très rapide et puissante de trouver des informations spécifiques sur un utilisateur d'un groupe. Exemple : vous pourriez utiliser un

serveur LDAP pour chercher une adresse électronique spécifique d'un répertoire d'entreprise à partir du nom de famille de l'utilisateur. Pour ce genre de mise en application, LDAP est en grande partie séparé de Sendmail ; LDAP stocke les informations hiérarchiques des utilisateurs et 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. Bref, vous pouvez utiliser LDAP pour abstraire le niveau de routage du courrier depuis Sendmail et ses fichiers de configuration séparés en un cluster LDAP puissant qui influence de nombreuses autres applications.

La version actuelle de Sendmail comprend la prise en charge pour LDAP. Pour étendre votre serveur Sendmail à l'aide de LDAP, prenez d'abord un serveur LDAP, tel que **OpenLDAP**, fonctionnel et correctement configuré. Ensuite, vous aurez besoin de modifier votre fichier `/etc/mail/sendmail.mc` pour y inclure :

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

Figure 16-5. Exemple de réglages pour LDAP dans `sendmail.mc`

Note **Remarque**

Ceci n'est que pour une configuration de base de Sendmail avec LDAP. Votre configuration devrait différer considérablement de celle-ci selon votre mise en application de LDAP, tout spécialement si vous souhaitez configurer plusieurs ordinateurs Sendmail qui utilisent un serveur LDAP commun.

Consultez `/usr/share/doc/sendmail/README.cf` pour avoir des informations de configuration de routage LDAP détaillées et des exemples.

Ensuite, recréez votre fichier `/etc/sendmail.cf` en exécutant `m4` et redémarrant Sendmail. Reportez-vous à la la section intitulée *Modifications courantes de la configuration de Sendmail* pour savoir comment procéder.

Pour plus d'informations sur LDAP, reportez-vous au Chapitre 19.

Les différents types de programme de messagerie électronique

Niveau supérieur

Fetchmail

Fetchmail

Fetchmail est un programme qui permet de récupérer du courrier depuis des serveurs distants pour des connexions TCP-IP à la demande. De nombreux utilisateurs apprécient le fait de pouvoir séparer le processus de téléchargement de leurs messages situés sur un serveur distant du processus de lecture et de gestion de leur courrier dans un AGC. Conçu tout spécialement pour les utilisateurs qui se connectent par modem, Fetchmail se connecte et télécharge rapidement tous les messages électroniques dans votre fichier spoole de messagerie à l'aide de différents protocoles, tels que POP3 et IMAP. Il permet même de réacheminer vos messages vers un serveur SMTP, si nécessaire.

Avant d'essayer Fetchmail, assurez-vous qu'il est installé sur votre système. S'il ne l'est pas, vous pouvez l'installer à l'aide du paquetage RPM `fetchmail`, qui est compris sur les CD-ROM de Red Hat Linux.

Fetchmail est configuré pour chacun des utilisateurs grâce à un fichier `.fetchmailrc` situé dans leur répertoire personnel. Un programme accompagnant Fetchmail, appelé `fetchmailconf`, est très utile pour configurer un fichier `.fetchmailrc` de base que vous pouvez ensuite personnaliser comme bon vous semble.

Fetchmail recherche les messages électroniques sur un serveur distant et les récupère sur la base des préférences spécifiées dans le fichier `.fetchmailrc`, il essaie ensuite de les acheminer au port 25 de l'ordinateur local, au moyen de l'ATC local, pour placer les messages sur le fichier spoole de l'utilisateur. Si Procmail est disponible, il peut ensuite être utilisé pour filtrer les messages et les placer dans une boîte aux lettres de sorte qu'ils puissent être lus avec un AGC.

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 lorsque l'on exécute Fetchmail, il est beaucoup plus simple d'utiliser un fichier `.fetchmailrc`. Toutes les options de configuration vont dans le fichier `.fetchmailrc`, mais vous pouvez les écraser lorsque Fetchmail est en cours en spécifiant cette option à la ligne de commande.

Le fichier `.fetchmailrc` d'un utilisateur est divisé en trois types d'option de configuration :

- *options d'ensemble* — donne à Fetchmail des instructions qui contrôlent l'exploitation du programme ou fournit des réglages pour toute connexion de vérification du courrier.

- *options serveur* — Spécifie les informations nécessaires sur le serveur scruté, telles que le nom d'hôte, de même que les préférences que vous souhaitez utiliser avec un serveur de messagerie donné, telles que le port à vérifier ou le nombre de secondes d'attente avant d'interrompre. Ces options affectent chaque option utilisateur utilisée avec ce serveur.
- *options utilisateur* — Contient des informations, telles que le nom d'utilisateur et le mot de passe, nécessaires à l'authentification et la vérification du courrier à l'aide d'un serveur de messagerie donné.

Les options d'ensemble sont placées au sommet du fichier `.fetchmailrc`, suivies d'une option serveur ou plus, désignant chacune un serveur de messagerie différent devant être vérifié par Fetchmail. Les options utilisateur vont à la suite des options serveur pour chaque compte utilisateur que vous désirez vérifier sur ce serveur de messagerie. Tout comme les options serveur, il est possible de spécifier plusieurs options utilisateur à utiliser avec un serveur donné, comme lorsque vous voulez vérifier plusieurs comptes de courrier sur un même serveur.

Les options serveur sont appelées à être utilisées dans le fichier `.fetchmailrc` par l'emploi d'un verbe d'option spécial, `poll` ou `skip`, qui précède toute information serveur. L'action `poll` indique à Fetchmail d'utiliser cette option serveur lorsqu'il est exécuté, qui vérifie en fait le courrier à l'aide des différentes options utilisateur. Cependant, toute option serveur précédée d'une action `skip` n'est pas vérifiée, à moins que vous ne spécifiiez le nom d'hôte de ce serveur lorsque Fetchmail est invoqué. L'option `skip` vous permet de régler des configurations de test dans `.fetchmailrc` et de n'utiliser ce serveur que lorsque vous en avez besoin, sans affecter toute autre configuration actuellement en cours.

Voici un exemple de fichier `.fetchmailrc` :

```
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
```

Figure 16-6. Exemple de fichier `.fetchmailrc` de base

Dans cet exemple, les options d'ensemble sont réglées de façon à ce que l'utilisateur reçoive le courrier en dernier ressort (option `postmaster` option) et que toutes les erreurs soient envoyées au "postmaster" plutôt qu'à l'expéditeur (option `bouncemail`). L'action `set` indique à Fetchmail que cette ligne contient une option d'ensemble. Puis, deux serveurs de messagerie sont spécifiés ; le premier 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 serveur, mais tout message électronique trouvé pour l'un ou l'autre des utilisateurs est envoyé dans le fichier spoole de messagerie de l'utilisateur 1. Cela permet de vérifier des boîtes aux lettres multiples sur des serveurs multiples, en affichant dans un seul AGC. Chaque information spécifique à une option utilisateur commence par l'action `user`.

Note **Remarque**

Vous n'avez pas à placer votre mot de passe dans le fichier `.fetchmailrc`. Vous pouvez omettre la section `with password '<mot de passe>'`. Fetchmail vous demande alors votre mot de passe lorsqu'il il est lancé à l'aide de la commande `fetchmail`.

Bien que vous puissiez configurer manuellement votre fichier `.fetchmailrc`, il est beaucoup plus simple de laisser le programme (inclus) `fetchmailconf` le faire à votre place. Cependant, lorsque vous testez de nouvelles configurations, il est normalement plus simple de modifier le fichier `.fetchmailrc` directement.

Comme on peut s'attendre d'un programme offrant un tel service réseau comme messagerie électronique et utilisant autant de protocoles, Fetchmail a de nombreuses options d'ensemble, serveur et utilisateur. Un grand nombre de ces options 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 communes sont énumérées ci-dessous.

Options d'ensemble

Chaque option d'ensemble devrait être placée sur une ligne individuelle et précédée de l'action `set`.

- `daemon <secondes>` — Indique à Fetchmail d'utiliser automatiquement le mode démon ; le démon demeure en tâche de fond et récupère le courrier en fonction de l'intervalle spécifié.
- `postmaster` — Donne à Fetchmail un utilisateur local auquel envoyer le courrier en cas de problèmes de distribution.
- `syslog` — Indique à Fetchmail de commencer à journaliser les messages d'erreur et d'état dans le fichier journal du système. Par défaut, il s'agit de `/var/log/maillog`.

Options serveur

Placez les options serveur sur leur propre ligne dans `.fetchmailrc`, précédées de l'action `poll` ou `skip`.

- `auth <auth-type>` — Spécifie 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 utilisé, Fetchmail essaiera d'abord des méthodes qui ne nécessitent aucun mot de passe, puis des méthodes qui masquent votre mot de passe et, enfin, il essaiera d'envoyer votre mot de passe en texte en clair pour effectuer l'authentification au serveur.

- `interval <nombre>` — Indique à Fetchmail de ne scruter que ce serveur chaque `<nombre>` de fois qu'il vérifie le courrier sur tous les serveurs configurés. Cette option peut être utilisée pour les serveurs de messagerie sur lesquels vous recevez peu de messages.
- `port <numéro-de-port>` — Ecrase le numéro de port par défaut pour un protocole spécifié.
- `proto <protocole>` — Indique à Fetchmail d'utiliser un protocole spécifique, tel que `pop3` ou `imap`, pour vérifier le courrier sur ce serveur.
- `timeout <secondes>` — Configure Fetchmail de façon à ce qu'il abandonne après un certain intervalle de temps d'inactivité du serveur. Si cette valeur n'est pas réglée, le système utilise `300` secondes par défaut.

Options utilisateur

Les options utilisateur peuvent être placées sur leurs propres lignes sous une option serveur ou alors sur la même ligne qu'une option serveur. Dans les deux cas, les options utilisateur sont précédées de l'option `user` (définie ci-dessous).

- `fetchall` — Ordonne à Fetchmail de télécharger tous les messages d'une file, y compris les messages qui ont déjà été visualisés. Par défaut, Fetchmail ne récupère que les nouveaux messages.
- `fetchlimit <nombre>` — Ne permet le téléchargement que d'un certain nombre de messages avant l'arrêt.
- `flush` — Indique à Fetchmail de supprimer tous les messages de la file visualisés précédemment avant de télécharger les nouveaux messages.
- `limit <nombre-max-octets>` — Vous permet de spécifier que seuls les messages dont la taille est inférieure à la taille spécifiée peuvent être récupérés. Cette option est pratique si vos connexions réseau sont lentes ou lorsqu'un gros message est trop long à télécharger.
- `password '<mot de passe>'` — Spécifie le mot de passe à utiliser pour cet utilisateur.
- `preconnect "<commande>"` — Indique à Fetchmail d'exécuter la commande spécifiée avant de récupérer les messages pour cet utilisateur.
- `postconnect "<commande>"` — Indique à Fetchmail d'exécuter la commande spécifiée après avoir récupéré les messages pour cet utilisateur.
- `ssl` — Autorise Fetchmail à recueillir le message via une connexion SSL cryptée, si le serveur prend en charge ce genre d'opération.
- `user "<nom d'utilisateur>"` — Définit le nom d'utilisateur utilisé par Fetchmail pour récupérer le courrier. Cette option doit être placée en premier, soit avant toute autre option utilisateur.

Options de commande Fetchmail

La plupart des options utilisées à la ligne de commande lors de l'exécution de la commande `fetchmail` répliquent les options de configuration de `.fetchmailrc`. Cela permet d'utiliser Fetchmail avec ou sans fichier de configuration. La plupart des utilisateurs n'utilisent jamais ces options à la ligne de commande car il est plus simple de les laisser dans le fichier `.fetchmailrc` ; elles sont ainsi utilisées chaque fois que Fetchmail est exécuté.

Toutefois, il peut arriver que vous ayez envie d'utiliser la commande `fetchmail` avec d'autres options dans un but précis. Comme les options spécifiées à la ligne de commande écrasent les options du fichier de configuration, vous pouvez indiquer une option de commande pour écraser temporairement les réglages de `.fetchmailrc` qui causent une erreur.

Options d'information ou de débogage

Certaines options utilisées après la commande `fetchmail` permettent d'obtenir d'importantes informations.

- `--configdump` — Affiche toutes les options possibles sur la base des informations de `.fetchmailrc` et les valeurs par défaut de Fetchmail. Aucun message électronique n'est téléchargé lorsque vous utilisez cette option, et ce pour aucun utilisateur.
- `-s` — Exécute Fetchmail en mode silencieux, empêchant tout message, autre que des messages d'erreur, d'apparaître après la commande `fetchmail`.
- `-v` — Exécute Fetchmail en mode prolixe, affichant toute communication entre Fetchmail et les serveurs de messagerie distants.
- `-V` — Fait en sorte que Fetchmail affiche des informations détaillées sur sa version, la liste des options d'ensemble et les réglages à utiliser avec chaque utilisateur, y compris le protocole de messagerie et la méthode d'authentification. Aucun message n'est téléchargé lorsque vous utilisez cette option, et ce pour aucun utilisateur.

Options spéciales

Ces options peuvent parfois être pratiques pour écraser 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 déjà visualisés. Par défaut, Fetchmail ne télécharge que les nouveaux messages.
- `-k` — Fait en sorte que Fetchmail laisse les messages sur le serveur de messagerie distant après les avoir téléchargés. Cette option écrase le comportement par défaut qui consiste à supprimer les messages après les avoir téléchargés.
- `-l <nombre-max-octets>` — Indique à Fetchmail de ne pas télécharger les messages dont la taille est supérieure à la taille spécifiée et de les laisser sur le serveur de messagerie distant.

- `--quit` — Quitte le processus démon de Fetchmail.

Vous trouverez plus de commandes et d'options `.fetchmailrc` dans la page de manuel `fetchmail`.

Précédent Sommaire Suivant
Sendmail Niveau supérieur Procmail

Procmail

Procmail vous permet de filtrer le courrier lors de sa réception depuis un serveur de messagerie distant ou lorsqu'il est placé dans votre fichier spoole sur un serveur de messagerie local ou distant. Il est puissant, peu exigeant en matière de ressources de système et très utilisé. Procmail, communément appelé *agent de distribution locale* (ADL), joue un petit rôle dans la distribution du courrier devant être lu par l'AGC.

Evidemment, Procmail doit être installé pour pouvoir être utilisé. Entrez la commande `rpm -q procmail` pour vérifier si le paquetage `procmail` est installé. S'il ne l'est pas, installez-le à l'aide des CD-ROM d'installation de Red Hat Linux.

Il existe différentes façons d'invoquer Procmail. Comme le courrier est placé sur votre fichier spoole, Procmail peut être configuré pour s'exécuter, filtrer le courrier vers les emplacements configurés à utiliser avec votre AGC et quitter. Ou alors, vous pourriez configurer votre AGC de sorte qu'il exécute Procmail chaque fois qu'un message est reçu afin que les messages soient placés dans les bonnes boîtes aux lettres. Souvent, la présence d'un fichier `.procmailrc` dans le répertoire personnel d'un utilisateur invoque Procmail, si Sendmail est utilisé.

Les actions effectuées sur un message électronique par Procmail dépendent des instructions de *recettes* particulières, ou règles, par rapport auxquelles les messages sont comparés. Si un message correspond à la recette, il peut alors être placé dans un fichier donné, supprimé ou traité d'une autre façon.

Lorsque Procmail est lancé, il lit les messages électroniques et sépare le corps de message des informations d'en-tête. Puis, Procmail cherche les fichiers `/etc/procmailrc` et `rc` dans le répertoire `/etc/procmailrcs` pour trouver les variables d'environnement Procmail, d'ensemble et par défaut, ainsi que les recettes. Ensuite, Procmail cherche un fichier `.procmailrc` dans le répertoire personnel de l'utilisateur pour trouver des règles spécifiques à cet utilisateur. De nombreux utilisateurs créent des fichiers `rc` supplémentaires pour Procmail, qui sont référencés par leur fichier `.procmailrc`, mais peuvent être activés ou désactivés rapidement si un problème de filtration de messages surgit.

Par défaut, aucun fichier `rc` pour l'ensemble du système n'existe dans le répertoire `/etc` et aucun fichier `.procmailrc` utilisateur n'existe. Pour commencer à utiliser Procmail, vous devrez créer un fichier `.procmailrc` ayant des variables d'environnement et des recettes spécifiques qui expliquent ce que vous aimeriez faire avec certains messages.

Dans la plupart des configurations, la décision de lancer Procmail et de tenter de filtrer le courrier est basée sur l'existence d'un fichier `.procmailrc` utilisateur. Pour désactiver Procmail, mais enregistrer

votre travail dans le fichier `.procmailrc`, déplacez-le vers un nom de fichier similaire à l'aide de la commande `mv ~/.procmailrc ~/.procmailrcSAVE`. Lorsque vous êtes prêt à tester Procmail de nouveau, redonnez au fichier son nom original, soit `.procmailrc`. Procmail recommencera à fonctionner immédiatement.

Configuration de Procmail

Fichiers de configuration de Procmail, mieux connus comme étant les fichiers utilisateur `.procmailrc`, contiennent d'importantes variables d'environnement. Celles-ci indiquent à Procmail quels messages trier, quoi faire avec les messages qui ne correspondent à aucune recette, etc.

Ces variables d'environnement se trouvent généralement dans le fichier `.procmailrc` au début, sous la forme suivante et chacune sur sa propre ligne :

```
<variable-env>="<valeur>"
```

Figure 16-7. Structure d'une ligne de variable d'environnement

Dans cet exemple, *<variable-env>* est le nom de la variable et la section *<valeur>* définit la variable.

La plupart des utilisateurs de Procmail se servent d'un petit nombre de variables et la plupart des variables d'environnement les plus importantes sont déjà définies à l'aide d'une valeur par défaut. Généralement, vous aurez affaire aux variables suivantes :

- `DEFAULT` — Définit la boîte aux lettres où seront placés les messages qui ne correspondent à aucune recette.

  La valeur `DEFAULT` par défaut est la même que `$ORGMAIL`.
- `INCLUDERC` — Spécifie des fichiers `rc` supplémentaires qui contiennent d'autres recettes servant à comparer les messages. Cela vous permet de diviser vos listes de recettes Procmail en fichiers individuels qui jouent différents rôles, tels que le blocage de spams et la gestion de listes d'adresses, qui peuvent ensuite être activés ou désactivés à l'aide de caractères de commentaire dans le fichier `.procmailrc` de l'utilisateur.

  Exemple : deux lignes d'un fichier `.procmailrc` d'un utilisateur peuvent ressembler à ceci :

```
MAILDIR=$HOME/Msgs
INCLUDERC=$MAILDIR/lists.rc
INCLUDERC=$MAILDIR/spam.rc
```

Figure 16-8. Exemple d'utilisation de l'option `INCLUDERC`

Si l'utilisateur veut désactiver la filtration Procmail de ses listes d'adresses, mais laisser le contrôle des spams en place, il n'a qu'à commenter la première ligne `INCLUDERC` avec le caractère #.

- `LOCKSLEEP` — Définit la durée, en secondes, entre les tentatives de Procmail d'utiliser un fichier de verrouillage donné. La valeur par défaut est 8 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 1024 secondes.
- `LOGFILE` — L'emplacement et le fichier devant contenir tout message d'erreur ou d'information Procmail.
- `MAILDIR` — Règle le répertoire de travail en cours pour Procmail. S'il est réglé, tous les autres chemins 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 requis par la recette.

  Par défaut, une valeur de `/var/spool/mail/$LOGNAME` est utilisée.
- `SUSPEND` — Définit la durée, en secondes, de pause de Procmail 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 l'option `INCLUDERC`, sauf que la vérification des recettes est arrêtée sur le fichier de configuration traitant et seules les recettes sur le fichier spécifié avec `SWITCHRC` sont utilisées.
- `VERBOSE` — Fait en sorte que Procmail journalise beaucoup plus d'informations. Cette option est pratique pour le débogage.

D'autres variables d'environnement importantes sont obtenues depuis votre shell, telles que `LOGNAME`, votre nom de connexion, `HOME`, l'emplacement de votre répertoire personnel et `SHELL`, votre shell par défaut.

Consultez la page de manuel de `procmailrc` si vous désirez obtenir des explications exhaustives sur les variables d'environnement, de même que leurs valeurs par défaut.

Recettes Procmail

Les nouveaux utilisateurs trouvent généralement que les recettes constituent l'élément le plus difficile de l'apprentissage d'utilisation de Procmail. Cela est compréhensible, jusqu'à un certain point, étant donné que les recettes procèdent à la comparaison avec les messages à l'aide d'*expressions régulières*, un format particulier utilisé pour spécifier des qualifications de concordance de chaînes. Toutefois, les expressions régulières ne sont pas très compliquées à créer et le sont encore moins à comprendre et à lire. De plus, la cohérence avec laquelle les recettes Procmail sont écrites, sans tenir compte des expressions régulières, permet de comprendre facilement ce qui se passe.

L'explication exhaustive des expressions régulières va au-delà des objectifs de ce chapitre. La structure des recettes Procmail est plus importante et des exemples pratiques de recettes Procmail peuvent être trouvés à différents endroits sur Internet, comme à l'adresse suivante par exemple : http://www.iki.fi/era/procmail/links.html. Le bon usage et l'adaptation des expressions régulières qui se trouvent dans ces exemples de recettes dépendent de la compréhension de la structure des recettes Procmail. Vous trouverez des informations d'introduction spécifiques aux règles d'expressions régulières de base dans la page de manuel `grep`.

Une recette Procmail a la forme suivante :

```
:0<indicateurs>: <nom-fichier-verrouillage>

* <caractère-condition-spéciale> <condition-1>
* <caractère-condition-spéciale> <condition-2>
* <caractère-condition-spéciale> <condition-N>

<caractère-action-spéciale><action-à-exécuter>
```

Figure 16-9. Structure d'une recette Procmail

Les deux premiers caractères d'une recette Procmail sont un deux-points et un zéro. Divers indicateurs (flags) peuvent être placés après le zéro pour contrôler ce que fait Procmail lors du traitement de cette recette. Un deux-points placé après la section *<indicateurs>* spécifie qu'un fichier de verrouillage sera créé pour ce message. Si tel est le cas, vous spécifiez son nom dans l'espace *<nom-fichier-verrouillage>*.

Une recette peut contenir plusieurs conditions servant à vérifier la concordance d'un message. S'il n'y a aucune condition, tous les messages auront une concordance positive avec la recette. Les expressions régulières sont placées dans quelques conditions de façon à faciliter la concordance avec les messages. Si l'on utilise des conditions multiples, elles doivent toutes obtenir la concordance pour qu'une action soit exécutée. Les conditions sont vérifiées sur la base des indicateurs spécifiés à la première ligne de la recette. Des caractères spéciaux facultatifs placés après le caractère `*` permettent de contrôler ultérieurement la condition.

<action-à-exécuter> spécifie ce qui arrive aux messages qui correspondent 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 à cet endroit pour envoyer les messages dans ce fichier, ce qui permet en fait de trier le courrier. Des caractères d'action spéciale peuvent également être utilisés avant que l'action ne soit spécifiée.

Recettes de distribution et de non-distribution

L'action utilisée si la recette correspond à un message donné détermine si la recette est considérée comme étant 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. Les blocs d'imbrication peuvent être emboîtés, donnant plus de contrôle pour l'identification et l'exécution d'actions sur les messages.

Les recettes de distribution qui correspondent à des messages font en sorte que Procmail exécute l'action spécifiée et cesse de comparer les messages en question aux autres recettes. Les messages qui correspondent aux conditions de recettes de non-distribution continuent d'être comparés aux autres recettes dans les fichiers `rc` courant et suivants. Autrement dit, les recettes de non-distribution font en sorte que les messages continuent vers les autres recettes après qu'une action a été exécutée sur eux.

Indicateurs

Les indicateurs sont très importants pour déterminer la façon dont les conditions d'une recette sont comparées à un message et pour décider si elles doivent l'être ou non. Les indicateurs suivants sont couramment utilisés :

- `A` — Spécifie que cette recette ne sera utilisée que si la dernière recette précédente sans indicateur `A` ou `a` a également obtenu la concordance avec ce message.

  Pour vous assurer que l'action sur cette dernière recette précédente correspondante a bel et bien été complétée avant d'accorder la concordance à la recette actuelle, utilisez plutôt l'indicateur `a`.
- `B` — Analyse le corps de message et recherche des conditions de concordance.
- `b` — Utilise le corps de message pour toute action résultante, telle que l'écriture du message dans un fichier ou son réacheminement. Il s'agit du comportement par défaut.
- `c` — Génère une copie du message électronique. Cela peut être pratique 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 d'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 ne sont comparées aux messages que si la recette immédiatement précédente sans indicateur `E` n'a pas obtenu la

concordance. Cette action ressemble à l'action *else*.

Utilisez plutôt l'indicateur `e` si vous voulez que cette recette soit vérifiée uniquement si la recette précédente a obtenu une concordance, mais que l'action a échoué.

- `f` — Utilise le conduit comme filtre.
- `H` — Analyse l'en-tête du message et recherche des conditions de concordance. Cela se fait par défaut.
- `h` — Utilise l'en-tête dans une action résultante. Cela est le comportement par défaut.
- `w` — Indique à Procmail d'attendre que le filtre ou le programme spécifié ait terminé et fait son rapport, réussi ou non, avant de considérer le message comme étant filtré.

  Si vous voulez ignorer les messages "Program failure" lors de la décision du succès d'un filtre ou d'une action, utilisez l'option `W` à la place.

D'autres indicateurs sont expliqués dans la page de manuel `procmailrc`.

Spécification d'un fichier de verrouillage local

Les fichiers de verrouillage sont très utiles avec Procmail pour garantir qu'il n'y a pas plus d'un processus qui essaie de modifier un certain message à un moment précis. Vous pouvez spécifier un fichier de verrouillage local en plaçant un caractère `:` après chaque indicateur sur la première ligne d'une recette. Cela a pour effet de créer un fichier de verrouillage local en fonction du nom de fichier de destination et de tout ce qui a été réglé dans la variable d'environnement d'ensemble `LOCKEXT`.

Autrement, vous pouvez spécifier le nom du fichier de verrouillage local à utiliser avec cette recette après le caractère `:`.

Conditions et actions spéciales

Des caractères particuliers utilisés devant les conditions et les actions des recettes Procmail modifient la façon dont elles sont interprétées.

Les caractères suivants peuvent être utilisés après le caractère `*`, au début d'une ligne de condition d'une recette :

- `!` — Inverse la condition, ce qui fait en sorte que la concordance ne s'obtient que si la condition ne correspond pas au message.
- `<` — Vérifie si la taille du message est inférieure au nombre d'octets spécifié.
- `>` — Vérifie si la taille du message est supérieure au nombre d'octets spécifié.

Les caractères suivants sont utilisés pour exécuter des actions spéciales :

- `!` — Indique à Procmail de réacheminer le message aux adresses électroniques spécifiées.
- `$` — Se réfère à une variable réglée précédemment dans le fichier `rc`. Ceci est généralement utilisé pour définir une boîte aux lettres commune à laquelle feront référence diverses recettes.
- `|` — Le caractère de conduit indique à Procmail de lancer un programme spécifique pour traiter ce message.
- `{` et `}` — Construit un bloc d'imbrication, utilisé pour contenir des recettes supplémentaires à appliquer aux messages comparés.

Si aucun caractère spécial n'est utilisé au début de la ligne d'action, Procmail considère alors que la ligne d'action spécifie une boîte aux lettres où les messages devraient être écrits.

Exemples de recettes

Procmail est un programme extrêmement flexible, vous permettant de comparer des messages sur la base de conditions très spécifiques et ensuite d'exécuter des actions détaillées sur ces messages. Cette flexibilité cependant fait qu'il peut être assez difficile pour les nouveaux utilisateurs de composer une recette Procmail de toutes pièces dans le but d'atteindre un objectif bien précis.

La meilleure façon de développer vos aptitudes en matière de création de recettes Procmail consiste à bien comprendre les expressions régulières et à examiner attentivement de nombreux exemples de recettes créées par d'autres utilisateurs. Les quelques exemples simples suivants ont pour but de vous montrer la structure des recettes Procmail et peuvent servir de base pour la construction de structures plus complexes.

Les recettes les plus élémentaires ne contiennent aucune condition, tel que le montre la Figure 16-10.

```
:0:
new-mail.spool
```

Figure 16-10. Exemple sans condition

La première ligne commence la recette en spécifiant qu'un fichier de verrouillage local sera créé, mais n'indique aucun nom, laissant Procmail utiliser le nom de fichier de la destination et `LOCKEXT` le nommer. Aucune condition n'est spécifiée, donc tous les messages correspondront à cette recette et, par conséquent, seront placés dans le fichier spoole individuel appelé `new-mail.spool`, situé dans le répertoire spécifié par la variable d'environnement `MAILDIR`. Un AGC peut ensuite visualiser les messages dans ce fichier.

Cette recette de base pourrait être placée à la fin de tous les fichiers `rc` pour acheminer les messages vers

un emplacement par défaut. Un exemple plus complexe pourrait prendre des messages provenant d'une adresse électronique donnée et les supprimer, tel qu'indiqué à la Figure 16-11.

```
:0
* ^From: spammer@domain.com
/dev/null
```

Figure 16-11. Exemple de message électronique envoyé à `/dev/null`

Dans le cas de cet exemple, tout message envoyé par `spammer@domain.com` est automatiquement déplacé vers `/dev/null`, qui le supprime.

Attention

Avertissement

Soyez très prudent lorsque vous effectuez ce genre d'opération et assurez-vous que la règle fonctionne correctement avant de déplacer les messages qui y correspondent vers `/dev/null` car ils y seront supprimés de façon permanente. Si les conditions de votre recette attrapent accidentellement des messages qui ne devraient pas l'être, vous ne le saurez même pas, à moins que l'expéditeur ne vous le dise.

Une solution plus appropriée serait de pointer l'action de la recette vers une boîte aux lettres spéciale que vous pouvez vérifier de temps en temps, afin de voir s'il s'y trouve de *fausses concordances* ou des messages qui correspondent par accident aux conditions. Lorsque vous avez bien regardé et que vous savez qu'il n'y a aucun message ayant fait l'objet d'une concordance accidentelle, vous pouvez supprimer la boîte aux lettres et diriger l'action de façon à envoyer les messages vers `/dev/null`.

Procmail est avant tout un filtre de courrier électronique, qui place automatiquement le courrier au bon endroit pour vous éviter de le trier manuellement. La recette indiquée à la Figure 16-12 prend les messages envoyés par une liste d'adresses donnée et les met dans le bon dossier pour vous.

```
:0:
* ^(From|CC|To).*tux-lug
tuxlug
```

Figure 16-12. Exemple de filtration de listes

Tout message envoyé depuis la liste d'adresses `tux-lug@domain.com` sera automatiquement placé dans la boîte aux lettres `tuxlug` pour votre AGC. Notez que la condition dans cet exemple permet

d'obtenir une concordance avec des messages ayant des adresses électroniques de la liste d'adresses sur l'une des lignes suivantes : `From`, `CC` ou `To`.

Procmail peut aussi être utilisé pour bloquer les spams, bien que cela ne soit pas une bonne solution à long terme pour remédier au problème du pollupostage. Examinez l'exemple de solution temporaire de filtration contre les spams donné à la Figure 16-13, dans lequel des recettes multiples sont réglées de façon à utiliser une boîte aux lettres commune pour stocker les spams.

```
SPAM=junk

:0:
* To??^$
$SPAM

:0:
* ^(To|CC):.*,.*,.*,.*,.*,.*,.*,.*,.*,.*,.*,
$SPAM

:0:
* ^Message-Id:.*<[^@]*>
$SPAM
```

Figure 16-13. Exemple de filtre anti spams de base

Dans cet exemple, la boîte aux lettres `junk` est associée à la variable `SPAM`, de sorte que vous puissiez changer la boîte aux lettres qui contient vos spams en un endroit. Puis, trois recettes cherchent les messages devant être envoyés à la boîte aux lettres `junk`.

La première recette cherche des messages qui n'ont aucun destinataire à la ligne `To`. La deuxième recette cherche les messages qui ont 12 destinataires ou plus. La troisième recette cherche les messages qui ont un mauvais identificateur de message.

Ces exemples simples vous sont fournis pour vous aider à commencer à créer des recettes. Consultez les nombreuses sources d'informations en ligne sur Procmail, disponibles à la la section intitulée *Autres ressources*, pour avoir des recettes plus détaillées et puissantes.

Sécurité

Comme pour tout autre service devant voyager sur un réseau non crypté, des informations importantes de messagerie, telles que les noms d'utilisateur, les mots de passe et les messages en entier peuvent être interceptées et visualisées, à l'insu du serveur ou du client de messagerie. Lorsque vous utilisez les protocoles POP et IMAP, toutes les informations d'authentification sont envoyées en "texte en clair", ce qui signifie qu'une personne située sur un réseau entre le client et le serveur distant peut facilement les visualiser.

Clients de messagerie sécurisés

Heureusement, la plupart des AGC Linux conçus pour vérifier le courrier sur des serveurs distants prennent en charge SSL pour crypter les messages alors qu'ils sont envoyés et reçus via réseau. Pour pouvoir utiliser SSL lorsque vous récupérez du courrier, il doit être activé sur le client et le serveur de messagerie.

SSL est généralement très simple à activer du côté client, il suffit même parfois de cliquer sur un bouton dans la section de configuration de l'AGC. Les IMAP et POP sécurisés ont des numéros de port connus (993 et 995 respectivement) que l'AGC utilise pour authentifier et télécharger les messages.

Les AGC très utilisés fournis avec Red Hat Linux, tels que **Mozilla Mail**, **Mutt** et **Pine**, offrent des sessions de courrier électronique cryptées avec SSL.

Serveurs de messagerie sécurisés

Il est presque aussi facile d'offrir le cryptage SSL aux utilisateurs d'IMAP et POP sur le serveur de messagerie. Red Hat Linux fournit également le paquetage `stunnel`, qui est un wrapper de cryptage SSL qui "enveloppe" le trafic réseau standard non sécurisé pour certains services et empêche ainsi que des intercepteurs puissent mettre le nez dans les communications entre le client et le serveur. Bien que `stunnel` ne se limite pas aux communications de courrier électronique, il est vraiment excellent pour offrir une protection aux protocoles qui, autrement, ne seraient pas sécurisés.

Le programme `stunnel` utilise des bibliothèques SSL externes, telles que les bibliothèques OpenSSL fournies avec Red Hat Linux, pour offrir un cryptage puissant et protéger vos connexions. Vous pouvez faire la demande d'un certificat SSL auprès d'un *fournisseur de certificats* ou vous pouvez créer un

certificat auto signé pour offrir les avantages de communications SSL cryptées.

Pour créer un certificat SSL auto signé, passez au répertoire `/usr/share/ssl/certs`, entrez la commande `make stunnel.pem` et répondez aux questions. Ensuite, utilisez `stunnel` pour lancer le démon de messagerie que vous souhaitez utiliser.

Exemple : la commande suivante pourrait être utilisée pour lancer le serveur IMAP fourni avec Red Hat Linux :

```
/usr/sbin/stunnel -d 993 -l /usr/sbin/imapd imapd
```

Vous devriez maintenant pouvoir ouvrir un client de messagerie IMAP et connecter votre serveur de messagerie en utilisant le cryptage SSL. Bien entendu, vous voudrez probablement aller plus loin et configurer votre serveur IMAP enveloppé avec `stunnel` de façon à ce qu'il soit lancé automatiquement aux bons niveaux d'exécution.

Pour plus d'informations sur la façon d'utiliser `stunnel`, lisez la page de manuel de `stunnel` ou consultez les documents dans le répertoire `/usr/share/doc/stunnel-<`*`numéro de version`*`>`.

Autrement, le paquetage `imap` fourni avec Red Hat Linux permet d'offrir le cryptage SSL sans `stunnel`. Pour avoir des connexions IMAP sécurisées, créez le certificat SSL en passant au répertoire `/usr/share/ssl/certs` et en exécutant la commande `make imapd.pem`. Puis, configurez le service `imaps` de façon à ce qu'il démarre aux bons niveaux d'exécution et redémarrez `xinetd` pour activer le service.

Vous pouvez aussi utiliser le paquetage `ipop3` fourni avec Red Hat Linux, qui offre le cryptage SSL sans `stunnel`.

Précédent Procmail | Sommaire | Niveau supérieur | Suivant Autres ressources

Autres ressources

De nombreux utilisateurs trouvent les programmes de messagerie électronique difficiles à configurer au début, en raison des nombreuses options disponibles principalement. Il peut donc être très utile de consulter d'autres sources d'informations, surtout lorsque vous devez spécifier des options de configuration délicates.

Documentation installée

- Les paquetages `sendmail` et `sendmail-cf` contiennent des informations sur la manière de configurer Sendmail.

  - `/usr/share/doc/sendmail/README.cf` — Informations sur `m4`, emplacements de fichier pour Sendmail, boîtes d'envoi prises en charge, façons d'accéder à des fonctions avancées, etc.
  - `/usr/share/doc/sendmail/README` — Informations sur la structure de répertoires de Sendmail, prise en charge de protocoles IDENT, détails sur les autorisations de répertoire et les problèmes communs que ces autorisations peuvent causer si elles ne sont pas configurées correctement.

  En outre, les pages de manuel `sendmail` et `aliases` contiennent des informations utiles sur les options de Sendmail et la configuration adéquate du fichier Sendmail `/etc/mail/aliases`.
- `/usr/share/doc/fetchmail-<numéro de version>` — Liste complète de fonctions Fetchmail dans le fichier `FEATURES` et document `FAQ` d'introduction.
- `/usr/share/doc/procmail-<numéro de version>` — Fichier `README` qui offre un aperçu de Procmail, fichier `FEATURES` qui explore toutes les fonctions du programme et fichier `FAQ` qui offre les réponses à de nombreuses questions fréquentes.

  Lorsque vous apprenez comment fonctionne Procmail et comment créer de nouvelles recettes, les pages de manuel suivantes sont précieuses :

  - `procmail` — offre un aperçu du fonctionnement de Procmail et des étapes de filtration 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 "weighted scoring" utilisée par Procmail pour vérifier s'il y a concordance entre une recette donnée et un message.

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 — met en lumière le courrier électronique du point de vue de l'utilisateur, teste diverses applications client de messagerie très utilisées et offre une introduction sur des sujets variés, tels que le réacheminement, la réponse automatique, les listes d'adresses, les filtres de courrier et les spams.
- http://www.redhat.com/mirrors/LDP/HOWTO/mini/Secure-POP+SSH.html — explique une façon de récupérer du courrier POP en utilisant SSH avec le réacheminement de port, de sorte que vos mots de passe et vos messages soient transférés de manière sécurisée.
- http://www.sendmail.net — contient des nouvelles, 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://tuxedo.org/~esr/fetchmail — page d'accueil de Fetchmail, comprenant un manuel en ligne et une FAQ exhaustive.
- http://www.procmail.org — page d'accueil de Procmail, avec des liens menant à diverses listes de participants dédiées à Procmail, de même que de nombreux documents FAQ.
- http://www.ling.helsinki.fi/users/reriksso/procmail/mini-faq.html — excellente FAQ Procmail, offrant des conseils pour le dépannage, des informations au sujet du verrouillage de fichiers et l'utilisation de caractères génériques.
- http://www.uwasa.fi/~ts/info/proctips.html — souligne une douzaine de conseils qui rendent l'utilisation de Procmail plus aisée dans de nombreuses situations, tels que la façon de tester des fichiers `.procmailrc` et d'utiliser le marquage de Procmail pour décider si une action donnée doit être exécutée ou non.

Livres sur le sujet

- *Sendmail* de Bryan Costales avec Eric Allman et al ; O'Reilly & Associates — une bonne référence 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 qui a pour but d'examiner 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 les spams.
- *Internet Email Protocols: A Developer's Guide* de Kevin Johnson ; Addison-Wesley Publishing

Company — fournit des 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 — explique les étapes nécessaires à la configuration d'un serveur IMAP.

Précédent Sécurité | Sommaire Niveau supérieur | Suivant Berkeley Internet Name Domain (BIND)

Chapitre 17. Berkeley Internet Name Domain (BIND)

De nos jours, l'Internet et presque tous les réseaux locaux dépendent d'un *Service de Nom de Domaine (Domain Name Service, DNS)* efficace et fiable, qui est utilisé pour associer les noms de systèmes aux adresses IP et vice-versa.

Dans le but de faciliter le DNS sur votre réseau, un *serveur de noms* est nécessaire pour traduire ces noms en adresses IP nécessaires à leur connexion. De plus, un serveur de noms peut effectuer à rebours la traduction dans le nom du système, ce que l'on appelle souvent un *reverse lookup*, ou résolution inversée.

Le présent chapitre décrit BIND, la structure de ses fichiers de configuration, et la façon dont il peut être administré localement ou à distance.

Vous trouverez les instructions de configuration de BIND à l'aide de l'outil **BIND Configuration Tool** avec interface graphique dans le *Guide de personnalisation officiel Red Hat Linux*. Si vous utilisez l'outil **BIND Configuration Tool**, pensez à ne pas éditer manuellement vos fichiers de configuration BIND, car les changements manuels seront écrasés par l'outil **BIND Configuration Tool**.

Introduction au DNS et à BIND

Les systèmes utilisant les réseaux IP doivent connaître l'adresse IP d'un ordinateur distante afin de s'y connecter. Toutefois, la plupart des utilisateurs préfèrent utiliser des noms d'ordinateur, comme un nom d'hôte ou un *fully qualified domain name (FQDN)*, pour spécifier un système au moment de la connexion. De plus, de nombreux programmes utilisent des noms de domaine dans leurs fichiers de configuration quand ils font référence à un système distant. Ils permettent ainsi de changer des adresses IP sans devoir modifier le nom du système (entre autres raisons). Le service qui rend cette opération plus facile est appelé DNS. Il est normalement mis en oeuvre par des serveurs centralisés qui font autorité pour quelques domaines, et se réfèrent à d'autres serveurs DNS pour les informations qu'ils ne possèdent pas encore.

Le DNS est rendu possible par l'utilisation de démons de serveurs de noms qui effectuent une traduction IP/nom. Une application client demande des informations au serveur de noms, en s'y connectant généralement sur le port de serveur 53. Le serveur de noms va tenter de résoudre le FQDN d'après sa

bibliothèque de solutions qui peut contenir des informations importantes sur l'hôte demandé ou des données cachées sur ce nom suite à une requête antérieure. Si le serveur de nom ne possède pas encore la réponse dans sa bibliothèque de solutions, il se tourne vers d'autres serveurs de noms, appelés *root nameservers*, ou serveurs de noms racines, afin de déterminer quels serveurs de noms font autorité pour le FQDN en question. Il effectuera ensuite, grâce à cette information, une requête auprès des serveurs de noms qui font autorité pour déterminer l'adresse IP du nom. S'il effectue une opération dans le sens inverse (reverse lookup), c'est 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.

Zones

Sur Internet, le FQDN d'un hôte peut être structuré en sections qui sont ensuite organisées hiérarchiquement, comme un arbre avec un tronc principal, des branches primaires, des branches secondaires, etc. Prenons par exemple le FQDN suivant :

```
bill.sales.domain.com
```

Figure 17-1. Un exemple de FQDN (fully qualified domain name)

Lorsque vous regardez un FQDN pour trouver l'adresse IP qui concerne un système particulier, lisez le nom de droite à gauche, chaque niveau de la hiérarchie étant distingué par un point (`.`). Dans notre exemple, le `com` définit le *domaine de niveau supérieur* pour ce FQDN. Le nom de `domain` est un sous-domaine de `com` et `sales` un sous-domaine de `domain`. Le nom le plus à gauche dans un FQDN est le nom d'hôte, qui identifie une machine particulière.

A l'exception du nom de domaine, chaque section s'appelle *zone*, ce qui définit un espace de nom particulier (namespace). Un *namespace*, ou espace de nom, contrôle le nom des sous-domaines à sa gauche. 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 de l'espace de nom choisie.

Les zones sont définies sur des serveurs de nom autorisé par l'intermédiaire; de *fichiers de zone*, qui décrivent l'espace de nom de cette zone, les serveurs de mail qui doivent être utilisés pour un domaine ou sous-domaine particulier, et bien plus encore. Les fichiers de zone sont stockés dans des *serveurs de noms maîtres* (qu'on appelle aussi des *serveurs de noms primaires*), sur lesquels les fichiers peuvent être modifiés, et des *serveurs de noms esclaves* (qu'on appelle aussi des *serveurs de noms secondaires*), qui reçoivent leurs fichiers de zone des serveurs de noms maîtres. 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.

Types de serveurs de noms

Il existe quatre types de configuration de serveurs de nom :

- *Maître* — Stocke les enregistrements de zone originaux importants pour un certain espace de nom et répond aux questions d'autres serveurs de noms qui cherchent des réponses concernant cet espace de nom.
- *Esclave* — Répond aussi 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 noms des serveurs de noms maîtres par l'intermédiaire d'une *zone de transfert*,dans laquelle l'esclave envoie au maître une requête dite `NOTIFY` pour une certaine zone. Le maître répond en fournissant les informations, si l'esclave est autorisé à recevoir le transfert.
- *Caching-only* — Offre des services de résolution nom vers IP mais ne fonctionne pas dans n'importe quelle zone. Les réponses pour toutes les résolutions sont en général placées en cache dans une base de données stockée en mémoire pour une période établie, le plus souvent spécifiée par l'enregistrement de zone importé, ce qui permet d'obtenir une résolution plus rapide pour d'autres clients DNS après la première résolution.
- *Forwarding* — Fait suivre des requêtes pour 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 peut être d'un ou plus de ces types. Par exemple, un serveur de noms peut être maître pour certaines zones, esclave pour d'autres, et n'offrir que la transmission d'une résolution.

BIND en tant que serveur de noms

Red Hat Linux contient BIND, est un serveur de noms Open Source puissant et très populaire. BIND utilise le démon `named` pour fournir ses services de résolution de noms. Toutes les informations de configuration pour BIND sont stockées dans le fichier `/etc/named.conf` et ses fichiers de zone se trouvent dans le répertoire `/var/named`. La structure et les options de ces différents types de fichiers peut être consultée dans la la section intitulée *Fichiers de configuration BIND*.

La version 9 de BIND contient un utilitaire appelé `/usr/sbin/rndc` qui permet d'administrer le démon `named` en cours. Vous trouverez des informations supplémentaires concernant `rndc` dans la la section intitulée *Utiliser `rndc`*.

Fichiers de configuration BIND

Le démon `named` du serveur de noms BIND utilise le fichier `/etc/named.conf` pour la configuration. Tous les fichiers de zone sont stockés dans le répertoire `/var/named`.

Avertissement **Avertissement**

N'éditez pas manuellement le fichier `/etc/named.conf` ou tout autre fichier dans le répertoire `/var/named` si vous êtes en train d'utiliser l'outil **BIND Configuration Tool**. Tout changement manuel dans ce fichier ou dans tout fichier de ce répertoire sera écrasé la prochaine fois que l'outil **BIND Configuration Tool** sera utilisé.

Le fichier `/etc/named.conf` ne doit pas comporter d'erreurs pour pouvoir démarrer `named`. Quelques options erronées dans certaines déclarations ne sont pas considérées comme assez critiques pour bloquer le serveur. Par contre une erreur dans les déclarations elles-mêmes empêchera `named` de démarrer.

`/etc/named.conf`

Le fichier `/etc/named.conf` est une suite de déclarations utilisant des options insérées placées entre accolades `{ }`. Un fichier `/etc/named.conf` commun est organisé comme le montre la Figure 17-2.

```
<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>;
```

```
};
```

Figure 17-2. Organisation commune de `/etc/named.conf`

Le "*<statement-name>*" n'est nécessaire qu'avec les déclarations `acl`, `include`, `server`, `view` et `zone`. Le *<statement-N-class>* ne peut être spécifié qu'avec la déclaration `zone`.

Des commentaires peuvent être placés dans `/etc/named` en caractères insérés de style C `/* */` ou après les caractères `//` et #.

Les déclarations suivantes peuvent être utilisées dans `/etc/named.conf`:

- `acl` *<acl-name>* — Configure une liste de contrôle d'accès d'adresses IP qui se verront autoriser ou interdire certains services `named`. La plupart du temps, les adresses IP individuelles ou la notation de réseau IP (comme `10.0.1.0/24`) servent à identifier les IP exactes.

  Quelques listes de contrôle d'accès sont déjà définies. Vous n'avez donc pas besoin de configurer une déclaration `acl` pour les définir :

  - `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 se connecte avec ses interfaces.
  - `none` — Ne correspond à aucune adresse IP.

  Lorsqu'elles sont utilisées avec d'autres déclarations `/etc/named.conf` et leurs options, les déclarations `acl` peuvent se révéler très utiles pour mieux utiliser votre serveur de noms BIND. Observez l'exemple dans la Figure 17-3.

```
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; };
```

```
}
```

Figure 17-3. Exemple d'utilisation de déclaration `acl`

Ce fichier `named.conf` contient deux listes de contrôle d'accès (`black-hats` et `red-hats`.

- `controls` — Configure diverses contraintes de sécurité nécessaires â l'utilisation de la commande `rndc` pour utiliser le service `named`.

  Consultez la la section intitulée */etc/named.conf* pour voir à quoi devrait ressembler la déclaration `controls`, y compris les options diverses qui peuvent ne peuvent être utilisées qu'avec elle.
- `include "<file-name>"` — Comprend le fichier spécifié dans le fichier de configuration en cours, permettant de placer des données de configuration sensibles (comme `keys`) dans un fichier séparé avec des permissions qui empêchent les utilisateurs sans privilèges de les lire.
- `key "<key-name>"` — Définit une clé par son 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>` — Le type d'algorythme utilisé, comme `dsa` ou `hmac-md5`.
  - `secret "<key-value>"` — La clé cryptée.

  Vous trouverez dans la Figure 17-22 un exemple de la déclaration `key`.
- `logging` — Permet d'utiliser de multiples types de logs, appelés des *channels*. En utilisant l'option `channel` dans la déclaration `logging`, vous pouvez construire un type de log personnalisé, avec son propre nom de fichier (`file`), sa limite de taille (`size`), sa version (`version`) et son niveau d'importance (`severity`). Une fois qu'un canal personnalisé a été défini, une option `category` est utilisée pour qualifier le canal et commencer le logging lorsque `named` est redémarré.

  Par défaut, `named` envoie des messages de log standards au démon `syslog`, qui les place dans `/var/log/messages`. Cela est dû au fait que plusieurs canaux standards sont compris dans BIND, avec plusieurs niveaux d'importance, comme celui qui traite les messages de logging 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 le logging normal sans configuration spéciale.

  La personnalisation du processus de logging peut être un processus très détaillé et cela dépasse le cadre du présent chapitre. Pour obtenir plus d'informations sur la création de logs personnalisés dans BIND, consultez le *BIND 9 Administrator Reference Manual*.

- `options` — assigne des valeurs à de nombreuses options liées, y compris des commandes pour faire suivre, l'emplacement du répertoire de fonctionnement de `named`, le nom de divers fichiers et bien plus.

  Les options suivantes sont parmi les plus couramment utilisées :

  - `allow-query` — Spécifie les hôtes qui seront autorisés à entamer des requêtes auprès de ce serveur de noms. Par défaut, tous les hôtes sont autorisés à présenter des requêtes. Ici une liste de contrôle d'accès ou collection d'adresses IP peut être utilisée pour n'autoriser que certains hôtes à entamer des requêtes auprès du serveur de noms.
  - `allow-recursion` — Similaire à l'option `allow-query`, si ce n'est qu'elle s'applique à des requêtes récursives. Par défaut, tous les hôtes sont autorisés à présenter des requêtes récursives auprès du serveur de noms.
  - `directory` — Transforme le répertoire de fonctionnement de `named` en autre chose que le répertoire par défaut `/var/named`.
  - `forward` — Contrôle la façon de faire suivre, si l'option `forwarders` contient des adresses IP valides désignant où envoyer les requêtes.

    Si l'option `first` est utilisée, alors les serveurs de noms spécifiés dans l'option `forwarders` font l'objet des premières requêtes d'informations. S'ils ne les possèdent pas, `named` va tenter la résolution lui-même.

    Si l'option `only` est utilisée, `named` ne tentera pas la résolution lui-même si les serveurs de noms pour faire suivre ont échoué.
  - `forwarders` — Spécifie une liste de serveurs de noms vers lesquels il faut faire suivre les requêtes pour résolution.
  - `listen-on` — Spécifie l'interface de réseau que `named` va utiliser pour percevoir les requêtes. Par défaut, toutes les interfaces sont utilisées.

    Cette option est utile si vous disposez de plusieurs interfaces de réseau et voulez limiter les systèmes qui peuvent effectuer des requêtes auprès de votre serveur de noms. Par exemple, si votre ordinateur sert de portail et de serveur de noms et que vous voulez bloquer toutes les requêtes exceptées celles qui proviennent de votre réseau privé, votre option `listen-on` devrait ressembler à la Figure 17-4.

```
options {
  listen-on { 10.0.1.1; };
};
```

Figure 17-4. Exemple d'option `listen-on`

De cette manière, seules les requêtes qui proviennent de l'interface de réseau servant le

réseau privé (`10.0.1.1`) seront acceptées.

- `notify` — Détermine si `named` envoie notification aux serveurs esclaves quand une zone est mise à jour. Par défaut le choix est `yes`, mais vous pouvez régler sur `no`, pour empêcher que les esclaves en soient notifiés, ou `explicit`, pour n'envoyer de notification qu'aux serveurs de la liste `also-notify`.
- `pid-file` — Vous permet de spécifier l'emplacement du fichier de processus ID créé par `named` lorsqu'il démarre.
- `statistics-file` — Vous permet de spécifier l'emplacement du fichier de statistiques qui est créé. Par défaut, les statistiques de `named` sont enregistrées dans `/var/named/named.stats`.

De nombreuses autres options sont également disponibles, dont beaucoup dépendant l'une de l'autre pour fonctionner correctement. Consultez le *BIND 9 Administrator Reference Manual* pour plus de détails.

- `server` — Définit des options particulières qui affectent la façon dont `named` doit se comporter envers les serveurs de noms distants, particulièrement en ce qui concerne les notifications et les transferts de zone.

L'option `transfer-format` détermine si un enregistrement de ressource est envoyé avec chaque message (`one-answer`) ou si des enregistrements de ressource multiples sont envoyés avec chaque message (`many-answers`). Bien que `many-answers` soit plus efficace, seuls les plus récents serveurs de noms BIND peuvent la comprendre.

- `trusted-keys` — Contient des clés publiques assorties utilisées pour DNSSEC. Consultez la la section intitulée *Sécurité* pour une introduction à la sécurité sous BIND.
- `view "<view-name>"` — Crée des vues spéciales qui répondent par un type d'informations particulier selon l'hôte qui contacte le serveur de noms. Ceci permet à certains hôtes de recevoir une réponse concernant une zone particulière pendant que d'autres hôtes reçoivent des informations totalement différentes. Alternativement, certains hôtes peuvent se voir accorder l'accès à certaines zones alors que les autres hôtes non autorisés continuent à effectuer des requêtes pour d'autres zones.

Vous pouvez utiliser de multiples `view`, pour autant que leurs noms soient uniques. L'option `match-clients` spécifie les adresses IP qui s'appliquent à une vue particulière. Toute déclaration `option` 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 listées est important, puisque c'est la première déclaration `view` qui correspond à l'adresse IP d'un client qui est utilisée.

Consultez la la section intitulée *Vues multiples* pour obtenir plus d'informations sur la déclaration `view`.

- `zone "<zone-name>"` — Spécifie des zones particulières pour lesquelles ce serveur de noms fait autorité. La déclaration `zone` est surtout utilisée pour spécifier le fichier contenant la configuration de la zone et transmettre certaines options concernant cette zone à `named`. Ces options auront la priorité sur la totalité des autres déclarations `option` situées dans `/etc/named.conf`.

Le nom de la zone est important, puisqu'il constitue la valeur par défaut assignée à la directive `$ORIGIN` utilisée dans le fichier zone et qu'il est lié aux non-FQDN. Par exemple, si cette déclaration `zone` définit l'espace de nom pour `domain.com`, il faut utiliser `domain.com` en tant que *<zone-name>* pour qu'il soit placé à la fin des noms d'hôtes utilisés dans le fichier de zone.

Les options les plus courantes de la déclaration `zone` comprennent :

- `allow-query` — Spécifie les clients qui sont autorisés à requérir 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 requérir un transfert des informations de la zone. Par défaut toutes les requêtes de transfert sont autorisées.
- `allow-update` — Spécifie les hôtes qui sont autorisés à mettre à jour dynamiquement des 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 à propos de leur zone. Ne mettez en oeuvre cette option que si vous accordez une confiance absolue à l'hôte. C'est une bien meilleure idée de laisser un administrateur mettre à jour manuellement les enregistrements de la zone et recharger le service `named`, si possible.
- `file` — Spécifie le nom du fichier qui contient les données de configuration de la zone dans le répertoire de fonctionnement de `named` (par défaut `/var/named`).
- `masters` — Utilisée si la zone est définie comme de `type` esclave. L'option `masters` indique au `named` d'un esclave la(les) adresse(s) d'où l'on peut requérir des informations de zone.
- `notify` — Fonctionne de manière similaire à l'option `notify` utilisée avec la déclaration `option`.
- `type` — Définit le type de zone. Les types suivants peuvent être utilisés :

  - `forward` — Dit au serveur de noms de faire suivre toutes les requêtes d'informations à propos de cette zone vers d'autres serveurs de noms.
  - `hint` — Un type spécial de zone qui est utilisé pour orienter vers les serveurs de noms racines, servant à résoudre des requêtes lorsqu'une zone n'est pas connue par ailleurs. Normalement vous n'aurez pas besoin de configurer une zone d'indication au-delà du `/etc/named.conf` par défaut.
  - `master` — Désigne le serveur de noms présent comme faisant autorité pour cette zone. Une zone devrait être configurée comme de type `master` si vous possédez les fichiers de configuration de la zone sur le présent système.
  - `slave` — Désigne le serveur de nomsprésent comme serveur esclave pour cette zone, disant à `named` de requérir les fichiers de configuration de la zone depuis l'adresse IP du serveur de noms maître pour cette zone.
- `zone-statistics` — Dit à `named` de conserver des statistiques concernant cette zone, en les écrivant soit dans l'emplacement par défaut (`/var/named/named.stats`), soit à l'emplacement expressément désigné par l'option `statistics-file` dans la déclaration `server`, s'il existe.

Exemples de déclarations de zone

La plupart des changements apportés au fichier `/etc/named.conf` d'un serveur de noms maître ou esclave concerne l'ajout, la modification ou la suppression de déclarations de `zone`. Bien que ces déclarations de `zone` puissent contenir de nombreuses options, la plupart des noms de serveurs en utilise peu. Les déclarations de `zone` suivantes sont des exemples très basiques qui peuvent ê utilisés dans une relation de serveurs de noms maître/esclave.

Une déclaration de `zone` sur un serveur de noms primaire hôte du domaine `domain.com` peut ressembler à la Figure 17-5.

```
zone "domain.com" IN {
  type master;
  file "domain.com.zone";
  allow-update { none; };
};
```

Figure 17-5. Exemple d'une déclaration de `zone` maître simple

Cette déclaration de `zone` nomme la zone `domain.com`, définit le `type` comme `maître`, dit à `named` de lire le fichier `/var/named/domain.com.zone` pour configurer la zone et de ne permettre de mise à jour par aucun autre hôte.

La déclaration de `zone` pour `domain.com` devrait ressembler à la Figure 17-6.

```
zone "domain.com" {
  type slave;
  file "domain.com.zone";
  masters { 192.168.0.1; };
};
```

Figure 17-6. Exemple de déclaration de `zone` esclave simple

Cette déclaration de `zone` dit à `named` sur le serveur esclave de chercher le serveur maître `192.168.0.1` pour y trouver les informations de configuration pour la zone appelée `domain.com`. Les informations que le serveur esclave reçoit du serveur maître sont enregistrées dans le fichier `/var/named/domain.com.zone`.

Fichiers de zone

Les *fichiers de zone* qui contiennent des informations sur un espace de nom particulier sont stockés dans le répertoire de fonctionnement de `named`, qui est par défaut `/var/named`. Chaque fichier de zone est nommé selon les données d'options de `file` dans la déclaration `zone`, généralement d'une manière qui se réfère au domaine en question et identifie le fichier comme contenant des données de zone, comme `example.com.zone`.

Chaque fichier de zone peut contenir des directives et enregistrements de ressources. Les *directives* disent au serveur de noms d'effectuer un certain acte ou d'appliquer une configuration spéciale à la zone. Les *enregistrements de ressources* définissent les paramètres de la zone, assignant une identité à des systèmes à l'intérieur de l'espace de nom de la zone. Les directives sont facultatives, mais les enregistrements de ressources sont requis pour fournir un service de noms à cette zone. Toutes les directives et enregistrements de ressources doivent se situer sur leur propre ligne.

Des commentaires peuvent être placés dans les fichiers de zone après les caractères point-virgules (`;`).

Directives de fichiers de zone

Les directives sont identifiées par le caractère de tête `$` placé avant le nom de la directive et généralement en haut du fichier de zone.

Les directives les plus couramment utilisées sont les suivantes :

- `$INCLUDE` — Dit à `named` d'inclure un autre fichier de zone dans ce fichier de zone à l'endroit où la directive est utilisée. Cela permet de stocker des configurations de zone supplémentaires à l'écart du fichier de zone principal.
- `$ORIGIN` — Détermine que le nom de domaine sera attaché à tout enregistrement non qualifié, comme ceux qui spécifient seulement l'hôte et rien de plus.

  Par exemple, un fichier de zone peut contenir la ligne suivante:

  ```
  $ORIGIN domain.com
  ```

  Tous les noms qui sont utilisés dans les enregistrements de ressources et ne finissent pas par un point (`.`) se verront ajouter ce nom de domaine. Autrement dit, lorsque l'enregistrement de zone est lu par le serveur de noms, la première ligne en-dessous sera interprétée en tant que seconde ligne:

```
ftp                IN   CNAME   server1
ftp.domain.com.    IN   CNAME   server1.domain.com.
```

Note **Remarque**

L'utilisation de la directive `$ORIGIN` n'est pas nécessaire si l'on nomme la zone dans `/etc/named.conf` similairement à la valeur à assigner à `$ORIGIN`. Le nom de la zone est utilisé par défaut comme valeur de la directive `$ORIGIN`.

- `$TTL` — Règle la valeur par défaut *Time to Live (TTL)* pour la zone. C'est le nombre, en secondes, donné aux serveurs de noms pour dire combien de temps les enregistrements de ressources de la zone resteront valides. Un enregistrement de ressources peut contenir sa propre valeur TTL, qui le cas échéant aura la priorité sur la présente directive.

  Lorsque vous décidez d'accroître cette valeur, les serveurs de noms distants mettent en cache ces informations de zone pendant plus longtemps. Cela réduit le nombre de requêtes effectuées au sujet de cette zone, mais rallonge aussi le temps nécessaire pour proliférer les changements des enregistrements de ressources.

Enregistrements de ressources de fichiers de zone

Les enregistrements de ressources de fichiers de zone contiennent des colonnes de données, séparées par le caractère Espace, qui définissent ces enregistrements. Tous les enregistrements de ressources de fichier de zone se voient assigner un type qui désigne le motif de l'enregistrement. Les types d'enregistrements de ressources les plus couramment utilisés sont les suivants :

- `A` — Enregistrement d'adresse qui spécifie une adresse IP à assigner à un nom.

  ```
  <host>      IN      A      <IP-address>
  ```

  Figure 17-7. Exemple de configuration de l'enregistrement `A`

  Si la valeur *`<host>`* est omise, alors un enregistrement `A` désigne une adresse IP par défaut pour le haut de l'espace de nom. Ce système sera la cible de toutes les requêtes non-FQDN.

  Examinons les exemples d'enregistrement `A` suivants pour le fichier de zone `domain.com`:

  ```
                IN      A       10.0.1.3
  server1       IN      A       10.0.1.5
  ```

Figure 17-8. Exemples d'enregistrements A

Les requêtes pour `domain.com` sont orientées vers 10.0.1.3, alors que les requêtes pour `server1.domain.com` sont orientées vers 10.0.1.5.

- `CNAME` — Enregistrement de nom canonique qui dit au serveur de noms qu'un nom donné est aussi connu qu'un autre.

```
<alias-name>      IN      CNAME        <real-name>
```

Figure 17-9. Exemple de configuration de l'enregistrement CNAME

Dans la Figure 17-9, toute requête envoyée à *<alias-name>* se dirigera vers l'hôte appelé *<real-name>*. Les enregistrements `CNAME` sont le plus souvent utilisés pour orienter vers les services qui utilisent un procédé commun de nommage pour les hôtes appropriés.

Examinons l'exemple dans la Figure 17-10, où un enregistrement `A` fixe un nom d'hôte à une adresse IP et un enregistrement `CNAME` y oriente les noms d'hôte `www` les plus courrament utilisés.

```
server1       IN      A        10.0.1.5
www           IN      CNAME    server1
```

Figure 17-10. Exemple d'enregistrement CNAME

- `MX` — Enregistrement Mail eXchange, qui dit où doit se diriger le courrier envoyé à un nom d'espace particulier contrôlé par cette zone.

```
        IN      MX      <preference-value>  <email-server-name>
```

Figure 17-11. Exemple d'enregistrement MX configuration

Dans Figure 17-11, l'option *<preference-value>* vous permet de lister numériquement les serveurs de mail que vous sélectionnez pour recevoir les messages pour cet espace de nom, donnant une préférence à certains systèmes de courrier sur d'autres. L'enregistrement de ressource `MX` à la *<preference-value>* la plus basse est préféré aux autres, mais vous pouvez régler de multiples serveurs de courrier avec la même valeur pour distribuer le trafic des mails entre eux.

L'option *<email-server-name>* peut être un nom d'hôte ou un FQDN, du moment qu'il oriente vers le système approprié.

```
        IN      MX      10      mail.domain.com.
        IN      MX      20      mail2.domain.com.
```

Figure 17-12. Exemple d'enregistrement MX

Dans cet exemple, le premier serveur de courrier `mail.domain.com` est préféré au serveur de courrier `mail2.domain.com` pour recevoir les mails destinés au domaine `domain.com`.

- NS — Enregistrement de serveur de noms (NameServer) qui annonce les serveurs de noms faisant autorité pour une zone particulière.

```
        IN      NS      <nameserver-name>
```

Figure 17-13. Exemple de configuration de l'enregistrement NS

L'option *<nameserver-name>* doit être un FQDN.

Dans la Figure 17-14, deux serveurs de noms autorisé sont listés pour un domaine. Le fait que ces serveurs de noms soient esclaves ou maîtres n'a pas d'importance. Ils sont tous les deux considérés comme faisant autorisés.

```
        IN      NS      dns1.domain.com.
        IN      NS      dns2.domain.com.
```

Figure 17-14. Exemple d'enregistrement NS

- PTR — Enregistrement PoinTeR record, conçu pour orienter vers une autre partie de l'espace de nom.

  Les enregistrements PTR servent surtout à la résolution inverse des noms, puisqu'ils ré-orientent les adresses IP vers un nom particulier. Consultez les la section intitulée *Fichiers de résolution de noms inversée* pour obtenir plus d'exemples d'utilisations d'enregistrements PTR.
- SOA — Enregistrement "Start Of Authority", qui proclame des informations importantes faisant autorité à propos des espaces de nom pour les serveurs de noms.

  Situé après les directives, un enregistrement SOA est le premier enregistrement de ressources dans un fichier de zone.

```
@     IN     SOA    <primary-name-server>     <hostmaster-email> (
                    <serial-number>
                    <time-to-refresh>
                    <time-to-retry>
                    <time-to-expire>
                    <minimum-TTL> )
```

Figure 17-15. Exemple de configuration d'enregistrement SOA

Le symbole @ place la directive $ORIGIN (ou le nom de zone, si la directive $ORIGIN n'est pas installée) en tant qu'espace de nom défini par le présent enregistrement de ressources SOA. Le serveur de nom primaire autorisé pour ce domaine est utilisé pour la *<primary-name-server>* et l'adresse e-mail de la personne à contacter à propos de cet espace de nom est substituée au *<hostmaster-email>*.

L'option *<serial-number>* est incrémentée chaque fois que vous changez le fichier de zone afin que named sache qu'il doit recharger cette zone. *<time-to-refresh>* dit à tout serveur esclave combien de temps 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 périmées ou s'il doit les rafraîchir.

L'option *<time-to-retry>* informe le serveur de noms esclave de l'intervalle à 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 *<time-to-expire>* ne soit écoulée, alors le serveur esclave cesse de répondre en se présentant comme faisant autorité pour les requêtes au sujet de cet espace de nom.

L'option *<minimum-TTL>* demande que d'autres serveurs de noms placent en cache les informations pour cette zone pendant au moins cette période.

Dans BIND, tous les temps sont exprimés en secondes. Toutefois, vous pouvez aussi utiliser des abbréviations pour des unités de temps autres que des secondes, comme les minutes (M), heures (H), jours (D) et semaines (W). Le tableau de la Tableau 17-1 montre la quantité de temps en secondes et la période équivalente dans un autre format.

Tableau 17-1. Les secondes comparées à d'autres unités de temps

Les secondes	Autres unités de temps
60	1M

1800	30M
3600	1H
10800	3H
21600	6H
43200	12H
86400	1D
259200	3D
604800	1W
31536000	365D

L'exemple suivant montre à quoi l'enregistrement d'une ressource de base SOA peut ressembler.

```
@     IN     SOA    dns1.domain.com.     hostmaster.domain.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
                    3600       ; retry after 1 hour
                    604800     ; expires after 1 week
                    86400 )    ; minimum TTL of 1 day
```

Figure 17-16. Exemples d'enregistrements SOA

Exemples de fichiers de zone

Si on les observe individuellement, les directives et enregistrements de ressources peuvent être difficiles à comprendre. Toutefois, tout devient bien plus limpide lorsqu'on peut les observer ensemble dans un fichier commun.

Dans Figure 17-17 un exemple de fichier de zone très classique est montré.

```
$ORIGIN domain.com
$TTL 86400
@     IN     SOA    dns1.domain.com.     hostmaster.domain.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
                    3600       ; retry after 1 hour
                    604800     ; expires after 1 week
                    86400 )    ; minimum TTL of 1 day

      IN     NS     dns1.domain.com.
      IN     NS     dns2.domain.com.

      IN     MX     10     mail.domain.com.
      IN     MX     20     mail2.domain.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
```

Figure 17-17. Exemple de fichier de zone de base

Dans cet exemple sont utilisées les directives standard et les valeurs SOA. On décide que les serveurs de noms autorisés seront `dns1.domain.com` et `dns2.domain.com`, qui ont des enregistrements A les liant respectivement à `10.0.1.2` et `10.0.1.3`.

Les serveurs de courrier configurés par les enregistrements MX orientent vers le `server1` et le `server2` grâce aux enregistrements CNAME. Puisque les noms du `server1` et du `server2` ne finissent pas par un point (`.`), le domaine `$ORIGIN` est placé à leur suite, ce qui les étend à `server1.domain.com` et `server2.domain.com`. Grâce aux enregistrements de ressources A concernés, leurs adresses IP peuvent être déterminées.

Les services ftp et Web populaires, disponibles aux noms standards `ftp.domain.com` et `www.domain.com`, sont orientés vers des machines qui fournissent les services appropriés pour ces noms, en utilisant les enregistrements CNAME.

Fichiers de résolution de noms inversée

Une résolution de nom inversée sert à traduire une adresse IP dans un espace de nom particulier en un FQDN. Cela ressemble beaucoup à un fichier de zone standard, si ce n'est que les enregistrements de ressources `PTR` servent à lier les adresses IP au nom d'un certain système.

L'écriture d'un enregistrement `PTR` se fera comme dans la Figure 17-18.

```
<last-IP-digit>      IN     PTR    <FQDN-of-system>
```

Figure 17-18. Exemple de configuration d'enregistrement `PTR`

`<last-IP-digit>` fait référence au dernier nombre dans une adresse IP qui doit orienter le FQDN d'un système particulier.

Dans la Figure 17-19, les adresses IP de `10.0.1.20` à `10.0.1.25` orientent vers les FQDN correspondants.

```
$ORIGIN 1.0.10.in-addr.arpa
$TTL 86400
@     IN     SOA    dns1.domain.com.     hostmaster.domain.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.domain.com.
      IN     NS     dns2.domain.com.

20    IN     PTR    alice.domain.com.
21    IN     PTR    betty.domain.com.
22    IN     PTR    charlie.domain.com.
23    IN     PTR    doug.domain.com.
24    IN     PTR    ernest.domain.com.
25    IN     PTR    fanny.domain.com.
```

Figure 17-19. Un exemple de fichier basique de résolution inversée de zone

Ce fichier de zone doit être mis en service avec une déclaration `zone` dans le fichier `/etc/named.conf` semblable à la Figure 17-20.

```
zone "1.0.10.in-addr.arpa" IN {
  type master;
  file "domain.com.rr.zone";
  allow-update { none; };
};
```

Figure 17-20. Un exemple de déclaration `zone` de résolution inversée

Il existe peu de différences entre cet exemple et une déclaration `zone` standard, si ce n'est dans la manière de nommer l'hôte. Notez qu'une zone de résolution de nom inversée nécessite que les trois premiers blocs de l'adresse IP soient inversés et que "`.in-addr.arpa`" soit inclu à leur suite. Cela permet d'attacher correctement à cette zone le bloc unique de nombres utilisé dans le fichier de zone de résolution de nom inversée.

Utiliser rndc

BIND contient un utilitaire appelé `rndc` qui permet d'administrer, localement ou à distance, le démon `named` grâce à des déclarations en lignes de commandes. Le programme `rndc` utilise le fichier `/etc/rndc.conf` pour ses options de configuration qui seront outrepassées par la priorité des options de lignes de commandes.

Afin d'empêcher des utilisateurs non autorisés sur d'autres systèmes de contrôler BIND sur votre serveur, on utilise une méthode de clé secrète partagée pour accorder explicitement des privilèges à certains hôtes. Pour que `rndc` émette des commandes vers n'importe quel `named`, même sur un ordinateur local, les clés utilisées dans `/etc/named.conf` et `/etc/rndc.conf` doivent se correspondre.

Fichiers de configuration

Avant d'essayer la commande `rndc`, vérifiez que les lignes de configuration adéquates sont en place dans les fichiers nécessaires. Il est probable que vos fichiers de configuration ne soient pas installés comme il le faudrait si après avoir lancé `rndc` vous voyez le message suivant :

```
rndc: connect: connection refused
```

/etc/named.conf

Pour que `rndc` soit autorisé à se connecter à votre service `named`, vous devez disposer d'une déclaration `controls` placée dans votre fichier `/etc/named.conf` quand `named` démarre. L'exemple de déclaration `controls` montré dans la Figure 17-21 vous permet d'exécuter des commandes `rndc` localement.

```
controls {
  inet 127.0.0.1 allow { localhost; } keys { <key-name>; };
};
```

Figure 17-21. Exemple de déclaration `controls` dans `/etc/named.conf`

Cette déclaration dit à `named` de se mettre à l'écoute du port TCP 953 par défaut de l'adresse inversée et d'autoriser les commandes `rndc` provenant de l'hôte local, si la clé adéquate est présentée. *<key-name>* fait référence à la déclaration `key`, qui se trouve aussi dans le fichier `/etc/named.conf`. Un exemple de déclaration `key` est montré dans la Figure 17-22.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
};
```

Figure 17-22. Exemple de déclaration `key` dans `/etc/named.conf`

Dans ce cas, *<key-value>* est une clé HMAC-MD5. Vous pouvez générer vos propres clés HMAC-MD5 à l'aide de 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 bonne clé qui doit être placée dans la zone *<key-value>* se trouve dans *<key-file-name>*.

Le nom de la clé utilisée dans `/etc/named.conf` doit être différent de `key`.

`/etc/rndc.conf`

Afin de configurer `rndc` pour qu'il utilise automatiquement la clé spécifiée dans `/etc/named.conf` pour l'hôte local, vous avez besoin de trois déclarations. La déclaration `options` vous permet de régler le serveur et la clé par défaut pour utilisation par `rndc`, comme on le voit dans la Figure 17-23.

```
options {
  default-server  localhost;
  default-key     "<key-name>";
};
```

Figure 17-23. Exemple de déclaration `options` dans `/etc/rndc.conf`

L'option existe de dire à la commande `rndc` d'utiliser une clé par défaut quand elle accède à un serveur

particulier, comme on le voit dans la Figure 17-24.

```
server localhost {
  key  "<key-name>";
};
```

Figure 17-24. Exemple de déclaration `server` dans `/etc/rndc.conf`

Toutefois, cette déclaration `server` n'est réellement utile que si vous vous connectez à de multiples serveur avec `rndc`.

La déclaration `key` est la plus importante dans `/etc/rndc.conf`.

```
key "<key-name>" {
  algorithm hmac-md5;
  secret "<key-value>";
};
```

Figure 17-25. Exemple de déclaration `key` dans `/etc/rndc.conf`

<key-name> et *<key-value>* doivent être absolument identiques à leur configuration dans `/etc/named.conf`.

Pour tester toutes les configurations, essayez la commande`rndc reload`. Vous devriez voir une réponse ressemblant à ceci:

```
rndc: reload command successful
```

Si la commande a échoué, examinez avec précaution les fichiers `/etc/named.conf` et `/etc/rndc.conf` pour chercher les erreurs.

Attention **Attention**

Il faut s'assurer que les utilisateurs sans privilèges ne peuvent pas lire ou écrire dans le fichier `/etc/rndc.conf`.

Options de ligne de commande

Une commande `rndc` se présente selon la forme suivante :

```
rndc <options> <commande> <commande-options>
```

Figure 17-26. Structure d'une commande `rndc`

La zone *<options>* n'est pas nécessaire, et vous n'êtes pas obligé d'utiliser *<command-options>* sauf si la commande le requiert.

Quand on exécute `rndc` sur un hôte local configuré de façon appropriée, les commandes suivantes sont disponibles :

- `halt` — Arrête immédiatement le service `named`.
- `querylog` — Déclenche le logging pour toutes les requêtes effectuées par des clients vers le présent serveur de noms.
- `refresh` — Rafraîchit la base de données du serveur de noms.
- `reload` — Dit au serveur de noms de recharger les fichiers de zone mais conserve toutes les réponses précédemment placées en cache. Cela vous permet d'opérer des changements sur les fichiers de zone et de leur faire prendre effet sur vos serveurs maîtres et esclaves sans perdre toutes les résolutions de nom stockées.

  Si vos changements n'affectent qu'une zone particulière, vous pouvez dire à `named` de ne recharger que cette zone-là. Tapez le nom de la zone après la commande `reload`.
- `stats` — Evacue les statistiques du `named` en cours vers le fichier `/var/named/named.stats`.
- `stop` — Arrête le serveur avec égards, en enregistrant toute mise à jour dynamique et donnée IXFR avant l'arrêt complet.

On peut à l'occasion vouloir passer outre les réglages par défaut dans le fichier `/etc/rndc.conf`. Sont disponibles les options suivantes :

- `-c` *<fichier-configuration>* — Dit à `rndc` d'utiliser un autre fichier de configuration que le fichier par défaut `/etc/rndc.conf`.
- `-p` *<numéro-port->* — Spécifie l'utilisation d'un numéro de port différent du port par défaut 953 pour la connexion de `rndc`.
- `-s` *<serveur>* — Dit à `rndc` d'envoyer la commande vers un autre serveur que celui que désigne l'option`default-server` dans le fichier `/etc/rndc.conf`.

  Afin d'accomplir ce travail, vous devez avoir configuré le service `named` pour qu'il accepte des

commandes de la part de votre hôte et qu'il possède la clé pour ce service de noms.

- `-y <key-name>` — Vous permet de spécifier une clé autre que l'option `default-key` dans le fichier `/etc/rndc.conf`.

Des informations supplémentaires sur ces options peuvent être consultées dans la page de manuel `rndc`.

Précédent | Sommaire | Suivant
Fichiers de configuration BIND | Niveau supérieur | Propriétés avancées de BIND

Propriétés avancées de BIND

La plupart des mises en oeuvres de BIND n'utilisent `named` que pour fournir un service de résolution de noms ou pour faire autorité pour un domaine ou sous-domaine particulier. Mais la version 9 de BIND possède aussi un certain nombre de propriétés avancées qui, quand on les configure et utilise de manière adéquate, permettent d'offrir un service DNS plus efficace et plus sécurisé.

Attention **Attention**

Quelques unes des ces propriétés avancées, comme DNSSEC, TSIG et IXFR, ne doivent être utilisées que dans les environnements de réseau munis de serveurs de noms qui supportent ces propriétés. Si votre environnement de réseau inclue des serveurs de noms non-BIND ou des versions de BIND plus anciennes, il vous faut vérifier si une propriété avancée est bien supportée avant d'essayer de la mettre en oeuvre.

Il ne faut pas présumer qu'un autre type de serveur de noms supportera ces propriétés, en fait beaucoup ne le font pas.

Toutes les propriétés évoquées ici sont décrites en détail dans le *BIND 9 Administrator Reference Manual*. Consultez la la section intitulée *Autres ressources* pour trouver les endroits où vous pourrez vous procurer ce manuel.

Améliorations du protocole DNS

BIND supporte les *Transferts de zone incrémentaux (Incremental Zone Transfers, IXFR)*, 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 AXFR standard nécessite que la zone entière soit transférée vers chaque serveur de noms esclave même pour le plus petit changement. Pour des domaines très populaires avec des fichiers de zones très longs, 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 en même temps le *dynamic updating* pour opérer des changements sur les enregistrements de zone maître. Si vous éditez manuellement des fichiers de zone pour opérer des changements, c'est AXFR qui doit être utilisé. Vous trouverez plus d'informations sur les mises à jour dynamiques dans le *BIND 9 Administrator Reference Manual*.

Vues multiples

BIND vous permet, en utilisant la déclaration `view` dans `/etc/named.conf`, de configurer un serveur de noms pour répondre aux requêtes de certains clients d'une manière différente que pour les autres clients.

Cela est utile surtout si vous souhaitez que des clients extérieurs à votre réseau ne puissent pas exécuter un service DNS particulier ou accéder à un certain type d'information, tout en y autorisant les clients internes.

La déclaration `view` utilise l'option `match-clients` pour faire correspondre les adresses IP ou des réseaux entiers et leur attribuer des options et des données de zones spéciales.

Sécurité

BIND supporte plusieurs méthodes différentes pour protéger la mise à jour et le transfert de zones, à la fois sur les serveurs de noms maîtres et esclaves :

- *DNSSEC* — Abbréviation de *DNS SECurity*, cette propriété permet de signer cryptographiquement des zones avec une *clé de zone (zone key)*.

  De cette façon, on peut vérifier que les informations au sujet d'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 supporte aussi la méthode de clé publique/privée SIG(0) d'authentification de messages.
- *TSIG* — Abbréviation de *Transaction SIGnatures*, installe une clé secrète partagée sur le serveur maître et le serveur esclave, et vérifie qu'un transfert de maître à esclave est autorisé.

  Cette propriété renforce la méthode d'autorisation de transfert basée sur l'adresse IP standard. Un agresseur n'aura pas seulement besoin d'accéder à l'adresse IP pour transférer la zone, mais devra aussi connaître la clé secrète.

  La version 9 de BIND supporte aussi *TKEY*, qui est une autre méthode de clé secrète partagée pour autoriser les transferts de zone.

IP version 6

La version 9 de BIND peut fournir un service de noms en environnement IP version 6 (IPv6), grâce aux enregistrements de zone `A6`.

Si votre environnement de réseau inclue à la fois des hôtes IPv4 et IPv6, il vous faut utiliser le démon de résolution très léger `lwresd` sur vos clients de réseau. Ce démon est essentiellement un serveur de noms très efficace et fonctionnant uniquement en cache, qui supporte les nouveaux enregistrements `A6` et `DNAME` qui fonctionnent avec IPv6. Consultez la page de manuel `lwresd` pour plus d'informations.

Précédent: Utiliser `rndc`
Sommaire
Niveau supérieur
Suivant: Erreurs fréquentes à éviter

Erreurs fréquentes à éviter

Il est très fréquent que les débutants fassent des erreurs en éditant des fichiers de configuration BIND ou rencontrent des difficultés en activant `named`. Prévenez-vous des problèmes suivants :

- *Assurez-vous que vous incrémentez le numéro de série quand vous éditez un fichier de zone.*

  Si le numéro de série n'est pas incrémenté, il se peut que votre serveur de noms maître possède les informations nouvelles et correctes, mais que vos serveurs de noms esclaves ne soient jamais notifiés du changement ou ne tentent pas de rafraîchir leurs données sur cette zone.
- *Faites attention à bien utiliser ellipses et point-virgules correctement dans le fichier `/etc/named.conf` file.*

  L'omission d'un point-virgule ou une ellipse non fermée empêcheront `named` de démarrer.
- *Rappelez-vous de placer les points (`.`) dans les fichiers de zone après tous les FQDN et de les éviter pour les noms d'hôte.*

  Le point signifie que le nom donné est complet. Si le point est omis, alors `named` placera le nom de la zone ou la valeur `$ORIGIN` à la suite du nom pour le compléter.
- *Si votre pare-feu cause des problèmes en bloquant les connexions depuis votre `named` vers d'autres serveurs de noms, il vous faudra dire manuellement à `named` d'utiliser le port 53 pour les requêtes montantes.*

  La version 9 de BIND utilise des ports au hasard au delà de 1024 pour demander à d'autres serveurs de noms de résoudre des noms, comme tout autre client DNS le ferait, en se connectant au port 53 du serveur de noms distant. Il existe toutefois des pare-feux qui exigent que les serveurs de noms communiquent entre eux en utilisant tous deux le port 53. Vous pouvez ajouter la ligne suivante dans la déclaration `options` pour forcer `named` à envoyer des requêtes depuis le port 53 :

```
query-source address * port 53;
```

Autres ressources

Les sources d'information suivantes fournissent une documentation supplémentaire sur l'utilisation de BIND.

Documentation installée

- BIND propose une gamme complète de documentation installée couvrant de nombreux sujets, chacun placé dans son répertoire respectif :
  - `/usr/share/doc/bind-<numéro-version>` — Contient un fichier `README` avec une liste des propriétés les plus récentes.
  - `/usr/share/doc/bind-<numéro-version>/arm` — Contient les versions HTML et SGML de *BIND 9 Administrator Reference Manual*, qui décrit en détail les ressources nécessaires pour BIND, la façon de configurer les différents types de serveurs de noms, d'opérer un équilibrage des charges et d'autres sujets avancés. Pour la plupart des nouveaux utilisateurs de BIND, c'est le meilleur point de départ.
  - `/usr/share/doc/bind-<numéro-version>/draft` — Contient des documents techniques assortis concernant des questions de service DNS et quelques méthodes proposées pour y répondre.
  - `/usr/share/doc/bind-<numéro-version>/misc` — Contient des documents conçus pour des questions avancées spécifiques. Les utilisateurs de la version 8 de BIND devraient consulter le document `migration` au sujet des changements importants quand on passe à la version 9 de BIND. Le fichier `options` liste toutes les options disponibles dans BIND 9 qui sont utilisées dans `/etc/named.conf`.
  - `/usr/share/doc/bind-<numéro-version>/rfc` — Tout document RFC concernant BIND est par commodité placé dans ce répertoire.
- Les pages de manuel suivantes sont utiles :
  - `named` — Examine les arguments assortis qui peuvent être utilisés pour contrôler le démon du serveur de noms BIND, comme le fichier de configuration alternative et le fonctionnement sur un port différent ou en tant qu'utilisateur différent.
  - `rndc` — Explique les différentes options disponibles lorsqu'on utilise la commande `rndc` pour contrôler un serveur de noms BIND.

Sites Web utiles

- http://www.isc.org/products/BIND — La page du projet BIND, où vous pourrez trouver des informations sur les versions actuelles et télécharger au format PDF le *BIND 9 Administrator Reference Manual*.
- http://www.redhat.com/mirrors/LDP/HOWTO/DNS-HOWTO.html — Couvre l'utilisation de BIND en tant que serveur de noms de résolution en cache, ou bien la configuration de divers fichiers de zone nécessaire dans le serveur de noms primaire pour un domaine.

Livres sur le sujet

- *DNS and BIND* par Paul Albitz et Cricket Liu, publié par O'Reilly & Associates — Une référence populaire qui explique à la fois les options de configuration de BIND les plus simples et les plus ésotériques, et vous fournit aussi des stratégies pour sécuriser votre serveur DNS.
- *The Concise Guide to DNS and BIND* par Nicolai Langfeldt, publié par Que — Etudie la connexion entre les services de réseaux multiples et BIND, en mettant l'accent sur des sujets techniques et orientés vers les applications pratiques.

Précédent Erreurs fréquentes à éviter | Sommaire Niveau supérieur | Suivant NFS (Network File System)

Chapitre 18. NFS (Network File System)

NFS (Network File System) est conçu pour permettre à des hôtes distants de monter des partitions sur un système spécifique et les utiliser comme s'il s'agissait de systèmes de fichiers locaux. Cela permet d'organiser les fichiers dans un emplacement central, tout en offrant la possibilité de laisser des utilisateurs autorisés y accéder.

Deux versions de NFS sont actuellement utilisées. NFS version 2, qui est en circulation depuis plusieurs années, est pris en charge par de nombreux systèmes d'exploitation. NFS version 3 a beaucoup plus de fonctionnalités, telles qu'une taille variable d'indicateurs de fichier et des rapports d'erreur plus avancés. Red Hat Linux prend en charge ces deux versions et emploie la version 3 par défaut lors d'une connexion avec un serveur qui permet son utilisation.

Ce chapitre se concentre sur NFS version 2, bien que de nombreux concepts s'appliquent également à la version 3. En outre, seuls les concepts fondamentaux et les informations supplémentaires sont fournis. Pour avoir des instructions spécifiques concernant la configuration et l'utilisation de NFS sur des ordinateurs client et serveur, reportez-vous au chapitre intitulé *Network File System (NFS)* dans *Guide de personnalisation officiel Red Hat Linux*.

Méthodologie

Linux utilise une combinaison de supports au niveau du noyau et de processus démon exécutés de façon continue pour offrir le partage de fichier NFS ; la prise en charge NFS doit cependant être activée dans le noyau Linux pour fonctionner. NFS utilise des *appels de procédure à distance* (RPC) pour router les demandes entre les clients et les serveurs, ce qui signifie que le service `portmap` doit être activé et actif aux niveaux d'exécution adéquats pour que des communications NFS aient lieu. Conjugués à `portmap`, de nombreux autres processus assurent qu'une connexion NFS est autorisée et peut s'effectuer sans erreur :

- `rpc.mountd` — Processus en cours d'exécution qui reçoit la demande de montage du client NFS et vérifie si elle correspond à un système de fichiers actuellement exporté.
- `rpc.nfsd` — Processus qui applique la partie au niveau utilisateur du service NFS. Il travaille avec le noyau Linux pour répondre aux demandes dynamiques des clients NFS, leur offrant par exemple des threads serveur supplémentaires à utiliser.
- `rpc.lockd` — Démon non nécessaire avec les noyaux modernes. Le verrouillage de fichiers NFS est maintenant effectué par le noyau. Ce démon est compris dans le paquetage `nfs-utils`

pour les utilisateurs qui se servent d'anciens noyaux n'offrant pas cette fonctionnalité par défaut.

- `rpc.statd` — Applique le protocole RPC *Network Status Monitor (NSM)*. Cela fournit un avis de redémarrage lorsqu'un serveur NFS est relancé sans avoir été éteint correctement.
- `rpc.rquotad` — Serveur RPC qui fournit des informations de quotas utilisateur pour les utilisateurs distants.

Ces programmes ne sont pas tous nécessaires pour le service NFS. Les seuls services qui doivent être activés sont `rpc.mountd`, `rpc.nfsd` et `portmap`. Les autres démons offrent des fonctionnalités additionnelles, en fonction des exigences particulières de votre environnement serveur.

NFS version 2 utilise le protocole UDP (*User Datagram Protocol*) pour offrir une connexion réseau "sans statut" entre le client et le serveur (NFS version 3 peut utiliser UDP ou TCP en exécution sur un IP). La connexion UDP sans statut minimise le trafic réseau car le serveur NFS envoie un cookie après que le client a reçu l'autorisation d'accéder au volume partagé. Ce cookie, ou valeur aléatoire stockée du côté serveur, est transmis avec toute demande RPC du client au serveur. Le serveur NFS peut être redémarré sans affecter les clients et le cookie demeure intact.

En utilisant NFS, l'authentification ne se fait que lorsque le client essaie d'effectuer le montage sur un système de fichier distant. Le serveur NFS utilise les fichiers `/etc/hosts.allow` et `/etc/hosts.deny` pour déterminer si l'accès via NFS d'un hôte donné doit être autorisé ou refusé. Puis, le serveur NFS utilise le fichier `/etc/exports` afin de connaître les privilèges de cet hôte pour les différents montages disponibles. Après avoir accordé l'accès, toutes les opérations effectuées sur les fichiers et répertoires sont envoyées au serveur à l'aide d'appels de procédure à distance.

Avertissement

Attention

Les privilèges de montage NFS sont accordés de façon spécifique à un hôte et non à un utilisateur. Si vous accordez à un hôte l'accès à une partie donnée de votre disque dur avec NFS, tous les utilisateurs de cet ordinateur auront accès aux données partagées.

En configurant le fichier `/etc/exports`, soyez extrêmement prudent lors du partage des répertoires ayant des autorisations de lecture et d'écriture (`rw`) à un hôte distant. Les utilisateurs des systèmes distants en mesure de monter vos systèmes de fichiers exportés pourront modifier les données qui s'y trouvent.

NFS et `portmap`

Le fonctionnement de NFS dépend des appels de procédure à distance (RPC). `portmap` est requis pour mapper les demandes RPC aux bons services. Les processus RPC avertissent `portmap` lorsqu'ils se lancent, révélant le numéro du port qu'ils contrôlent et les numéros des programmes qu'ils prévoient de servir. Le système client contacte alors `portmap` sur le serveur avec un numéro de programme

spécifique. `portmap` redirige ensuite le client vers le bon numéro de port pour communiquer avec le service désiré.

Comme les services basés sur RPC dépendent de `portmap` pour réaliser des connexions avec les demandes client entrantes, `portmap` doit être disponible avant que l'un de ces services ne commence. Si, pour une raison quelconque, le service `portmap` s'arrête de manière inattendue, relancez-le et relancez également tous les services qui étaient en cours d'exécution lors de son lancement.

Le service `portmap` peut être utilisé avec les fichiers d'accès hôte (`/etc/hosts.allow` et `/etc/hosts.deny`) pour contrôler les systèmes distants autorisés à utiliser les services basés sur RPC sur votre ordinateur. Reportez-vous au Chapitre 9 pour plus d'informations. Les règles de contrôle d'accès pour `portmap` affectent tous les services basés sur RPC ; vous pouvez également spécifier chaque démon RPC NFS devant être affecté par une règle particulière de contrôle d'accès. Les pages de manuel de `rpc.mountd` et `rpc.statd` contiennent des informations sur la syntaxe précise de ces règles.

Etat de `portmap`

Comme `portmap` fournit la coordination entre les services RPC et les numéros de port utilisés pour communiquer avec eux, il peut être pratique d'être en mesure d'avoir un aperçu des services RPC courants qui utilisent `portmap` en cas de dépannage. La commande `rpcinfo` affiche chaque service basé sur RPC, ainsi que son numéro de port, son numéro de programme RPC, sa version et son type de protocole (TCP ou UDP).

Pour vous assurer que les bons services RPC NFS sont activés pour `portmap`, `rpcinfo` peut être utile :

```
[root@bleach /]# rpcinfo -p some.machine.com
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp   1024  status
    100024    1   tcp   1024  status
    100011    1   udp    819  rquotad
    100011    2   udp    819  rquotad
    100005    1   udp   1027  mountd
    100005    1   tcp   1106  mountd
    100005    2   udp   1027  mountd
    100005    2   tcp   1106  mountd
    100005    3   udp   1027  mountd
    100005    3   tcp   1106  mountd
    100003    2   udp   2049  nfs
```

```
    100003    3   udp   2049  nfs
    100021    1   udp   1028  nlockmgr
    100021    3   udp   1028  nlockmgr
    100021    4   udp   1028  nlockmgr
[root@bleach /]#
```

L'option `-p` détecte le mappeur de port sur les hôtes spécifiés ou se met par défaut sur l'hôte local si aucun hôte spécifique n'est énuméré. D'autres options sont disponibles dans la page de manuel de `rpcinfo`.

A partir de la sortie ci-dessus, il est possible de voir que divers services NFS sont en cours d'exécution. Si l'un des services NFS ne démarre pas correctement, `portmap` est incapable de mapper les demandes des clients pour ce service vers le port adéquat. Dans de nombreux cas, le redémarrage de NFS en tant que super-utilisateur (`/sbin/service nfs restart`) permet d'enregistrer correctement les services en question avec `portmap` et de les faire fonctionner.

Précédent
Autres ressources

Sommaire
Niveau supérieur

Suivant
Fichiers de configuration du serveur NFS

Fichiers de configuration du serveur NFS

Il est aisé de configurer un système afin qu'il puisse partager des fichiers et des répertoires à l'aide de NFS ; tout système de fichiers exporté vers des utilisateurs distants via NFS, de même que les droits d'accès relatifs au système de fichiers en question, sont situés dans le fichier `/etc/exports`. Ce fichier est lu par la commande `exportfs` pour donner à `rpc.mountd` et `rpc.nfsd` les informations nécessaires afin d'accorder le montage à distance d'un système de fichiers à un hôte autorisé.

La commande `exportfs` vous permet d'exporter ou d'annuler de façon sélective l'exportation des répertoires sans relancer les différents services NFS. Lorsque vous indiquez les bonnes options à `exportfs`, les systèmes de fichiers devant être exportés sont écrits dans `/var/lib/nfs/xtab`. Comme `rpc.mountd` se réfère au fichier `xtab` pour accorder les privilèges d'accès à un système de fichiers, les modifications apportées à la liste de systèmes de fichiers exportés sont appliquées immédiatement.

Différentes options sont disponibles lorsque vous utilisez `exportfs` :

- `-r` fait en sorte que tous les répertoires énumérés dans `/etc/exports` soient exportés en créant une nouvelle liste d'exportation dans `/etc/lib/nfs/xtab`. Cette option actualise en fait la liste d'exportation avec tous les changements apportés à `/etc/exports`.
- `-a` fait en sorte que tous les répertoires soient exportés ou non, selon les autres options transmises à `exportfs`.
- `-o` *`options`* permet à l'utilisateur de spécifier les répertoires devant être exportés qui ne sont pas inclus dans la liste de `/etc/exports`. Ces systèmes de fichiers partagés supplémentaires doivent être écrits de la même manière que leurs spécifications dans `/etc/exports`. Cette option est utilisée pour tester un système de fichiers avant de l'ajouter de façon permanente à la liste des systèmes de fichiers à exporter.
- `-i` indique à `exportfs` d'ignorer `/etc/exports` ; seules les options données depuis la ligne de commande sont utilisées pour définir les systèmes de fichiers exportés.
- `-u` annule l'exportation de répertoires pouvant être montés par des utilisateurs distants. La commande `exportfs -ua` suspend le partage de fichiers NFS tout en conservant les divers démons NFS en marche. Pour permettre au partage de fichiers NFS de se poursuivre, entrez `exportfs -r`.
- `-v` opération prolixe, où les systèmes de fichiers exportés et non exportés sont affichés de façon plus détaillée lorsque la commande `exportfs` est exécutée.

Si aucune option n'est transmise à la commande `exportfs`, une liste de systèmes de fichiers

actuellement exportés s'affiche.

Les changements apportés à `/etc/exports` peuvent aussi être lus en rechargeant le service NFS à l'aide de la commande `service nfs reload`. Cela permet de maintenir les démons NFS en marche tout en exportant de nouveau le fichier `/etc/exports`.

/etc/exports

Le fichier `/etc/exports` est la norme pour contrôler quels fichiers doivent être exportés vers des hôtes donnés, de même que pour spécifier des options particulières qui contrôlent tout. Les lignes vides sont ignorées, des lignes de commentaire peuvent être créées à l'aide du caractère # et les longues lignes peuvent être coupées avec une barre oblique inverse (\). Chaque système de fichiers exporté doit se trouver sur sa propre ligne. Les listes d'hôtes autorisés, placées à la suite d'un système de fichiers exporté, doivent être séparées par des caractères d'espacement. Les options pour chacun des hôtes doivent être placées entre parenthèses directement après l'identificateur d'hôte, sans espace séparant l'hôte de la première parenthèse.

Dans sa forme la plus simple, `/etc/exports` n'a besoin de connaître que le répertoire à exporter et les hôtes autorisés à l'utiliser :

```
/some/directory bob.domain.com
/another/exported/directory 192.168.0.3
```

Après avoir exporté de nouveau `/etc/exports` avec la commande `/sbin/service nfs reload`, l'hôte `bob.domain.com` peut monter `/some/directory` et `192.168.0.3` peut monter `/another/exported/directory`. Comme aucune option n'est spécifiée dans cet exemple, de nombreuses préférences NFS par défaut sont appliquées :

- `ro` lecture seule : les hôtes qui montent ce système de fichiers ne peuvent le modifier. Pour permettre aux hôtes d'y effectuer des changements, vous devez spécifier `rw` (lecture-écriture).
- `async` permet au serveur d'écrire des données sur le disque lorsqu'il le juge opportun. Alors que cela n'a aucune importance dans le cas d'un hôte qui effectue l'accès en lecture seule, la situation est différente si un hôte fait des changements sur un système de fichiers en lecture-écriture et que le serveur se bloque car des données pourraient être perdues. En spécifiant l'option `sync`, toute modification de fichier doit être engagée sur le disque avant que la demande d'écriture du client ne soit terminée. Cela peut ralentir les performances.
- `wdelay` fait en sorte que le serveur NFS retarde l'écriture sur le disque s'il pense qu'une autre demande d'écriture est imminente. Cela peut améliorer les performances en réduisant le nombre d'accès au disque par des commandes d'écriture différentes et le temps-système dédié à l'écriture. Utilisez `no_wdelay` pour désactiver cette fonction, qui ne fonctionne que si vous utilisez

l'option `sync`.

- `root_squash` fait en sorte que tout accès client au système de fichiers exporté, exécuté en tant que super-utilisateur sur l'ordinateur client, se fasse en tant qu'ID utilisateur "nobody" (personne). Cela permet de "réduire" la puissance du super-utilisateur distant à celle de l'utilisateur local le plus bas, l'empêchant ainsi d'agir comme s'il était le super-utilisateur du système local. Vous pouvez désactiver la diminution du super-utilisateur avec l'option `no_root_squash`. Pour diminuer tout utilisateur distant, y compris le super-utilisateur, utilisez l'option `all_squash`. Pour spécifier quels ID utilisateur et groupe utiliser avec les utilisateurs distants d'un hôte spécifique, utilisez les options `anonuid` et `anongid`, respectivement. De cette façon, vous pouvez créer un compte utilisateur spécial à partager pour les utilisateurs NFS distants et spécifier `(anonuid=<`*`valeur-uid`*`>,anongid=<`*`valeur-gid`*`>)`, où `<`*`valeur-uid`*`>` est le numéro d'ID utilisateur et `<`*`valeur-gid`*`>` est le numéro d'ID groupe.

Pour écraser les valeurs par défaut, vous devez spécifier une option qui les remplace. Exemple : si vous ne spécifiez pas `rw`, le système de fichiers exporté ne sera alors partagé qu'en lecture seule. Chaque valeur par défaut pour chacun des systèmes de fichiers exportés doit être écrasée explicitement. De plus, d'autres options sont disponibles là où aucune valeur par défaut n'est en place. Cela inclut la possibilité de désactiver la vérification de sous-arborescences, d'autoriser l'accès depuis des ports non sécurisés et le verrouillage de fichiers non sécurisés (nécessaires pour certaines mises en oeuvre de clients NFS plus anciens). Consultez la page de manuel de `exports` pour avoir plus de détails sur ces options moins souvent utilisées.

Vous pouvez avoir recours à toute une série de méthodes pour spécifier des hôtes autorisés à utiliser un système de fichiers exporté donné, notamment :

- *hôte unique* — Un hôte spécifique est spécifié avec un nom de domaine, un nom d'hôte ou une adresse IP pleinement qualifié.
- *caractères spéciaux* — Un caractère `*` ou `?` est utilisé pour prendre en considération un groupe de noms de domaine ou d'adresses IP pleinement qualifiés ou ceux qui correspondent à une chaîne spécifique de lettres.

  Toutefois, soyez prudent lorsque vous utilisez des caractères spéciaux avec des noms de domaine pleinement qualifiés car ils ont tendance à être plus précis que vous ne le croyez. Exemple : l'utilisation du caractère spécial `*.domain.com` permet à sales.domain.com d'accéder au système de fichiers exporté, mais pas à bob.sales.domain.com. Pour que les deux possibilités puissent fonctionner, de même que sam.corp.domain.com, vous devriez spécifier `*.domain.com *.*.domain.com`.
- *IP networks* — permet la concordance des hôtes sur la base de leur adresse IP au sein d'un réseau plus étendu. Exemple : `192.168.0.0/28` autorise les 16 premières adresses, de 192.168.0.0 à 192.168.0.15, à accéder au système de fichiers exporté, mais n'autorise pas l'adresse 192.168.0.16 et les adresses supérieures.
- *netgroups* — permet d'utiliser un nom de groupe de réseau NIS, écrit sous la forme `@<`*`nom-de-groupe`*`>`. Cela place le serveur NIS en charge du contrôle d'accès pour le système de fichiers en

question ; il est ainsi possible d'ajouter et de supprimer des utilisateurs du groupe NIS sans affecter `/etc/exports`.

Avertissement **Avertissement**

La façon dont le fichier `/etc/exports` est formaté est très importante, surtout en ce qui concerne l'utilisation des caractères d'espacement. N'oubliez jamais de séparer les systèmes de fichiers exportés des hôtes, et un hôte d'un autre hôte, avec un caractère d'espacement. Cependant, aucun autre de ces caractères ne doit être utilisé dans ce fichier, sauf dans les lignes de commentaire.

Dans l'exemple ci-dessous, les deux lignes n'ont pas la même signification :

```
/home bob.domain.com(rw)
/home bob.domain.com (rw)
```

La première ligne accorde uniquement l'accès lecture-écriture au répertoire `/home` aux utilisateurs de `bob.domain.com`. La seconde autorise les utilisateurs de `bob.domain.com` à monter le répertoire en lecture seule (par défaut), mais les autres utilisateurs peuvent le monter en lecture-écriture. Soyez prudent lorsque des caractères d'espacement sont utilisés dans `/etc/exports`.

Précédent
NFS (Network File System)
Sommaire
Niveau supérieur
Suivant
Fichiers de configuration d'un client NFS

Fichiers de configuration d'un client NFS

Tout partage NFS disponible depuis un serveur peut être monté de différentes façons. Bien entendu, le partage peut être monté manuellement, à l'aide de la commande `mount`, pour acquérir le système de fichiers exporté à un point de montage spécifique. Pour ce faire toutefois, le super-utilisateur doit entrer la commande `mount` à chaque fois que le système redémarre. En outre, le super-utilisateur ne doit pas oublier de démonter le système de fichiers lorsqu'il éteint l'ordinateur. Deux autres méthodes de configuration des montages NFS consistent à modifier `/etc/fstab` ou utiliser le service `autofs`.

/etc/fstab

Une ligne correctement formatée dans le fichier `/etc/fstab` produit le même effet que de monter manuellement le système de fichiers exporté. Le fichier `/etc/fstab` est lu par le script `/etc/rc.d/init.d/netfs` au démarrage du système. Les bons montages du système de fichiers, y compris NFS, sont mis en place.

Un exemple de ligne `/etc/fstab` pour monter un système de fichiers exporté NFS ressemble à ce qui suit :

```
<serveur>:</chemin/du/répertoire> </point/montage/local> nfs <options> 0 0
```

<serveur-hôte> fait référence au nom d'hôte, à l'adresse IP ou au nom de domaine pleinement qualifié du serveur qui exporte le système de fichiers. *</chemin/vers/partage/répertoire>* indique au serveur ce qu'il faut exporter au montage. *</point/montage/local>* spécifie à quel endroit sur le système de fichiers local monter le répertoire exporté. Ce point de montage doit exister avant que `/etc/fstab` ne soit lu ; sinon, le montage échoue. L'option `nfs` indique le type de système de fichiers monté.

La section *<options>* indique la façon dont le système de fichiers doit être monté. Exemple : si la section options spécifie `rw,suid` sur un montage donné, le système de fichiers exporté est monté en lecture-écriture et les ID groupe et utilisateur définis par le serveur sont utilisés. N.B. : les parenthèses ne doivent pas être utilisées. Pour plus d'options de montage, reportez-vous à la la section intitulée *Options de montage NFS courantes*.

autofs

L'un des inconvénients provoqués par l'utilisation de `/etc/fstab` est que, peu importe le temps consacré à utiliser le système de fichiers monté, le système doit y dédier des ressources pour le maintenir en place. Cela n'est pas problématique si l'on parle de quelques montages, mais peut le devenir lorsque le système maintient dans le même temps les montages d'une douzaine d'autres systèmes, car les performances d'ensemble du système peuvent en souffrir. Donc, au lieu d'avoir recours à `/etc/fstab`, vous pouvez vous servir de l'utilitaire `automount` basé sur le noyau, qui monte et démonte automatiquement des systèmes de fichiers NFS et permet de limiter les ressources employées.

Le script `autofs`, situé dans `/etc/rc.d/init.d`, est utilisé pour contrôler `automount` par l'entremise du fichier

de configuration primaire `/etc/auto.master`. Bien que `automount` puisse être spécifié à la ligne de commande, il est plus pratique d'indiquer les points de montage, le nom d'hôte, le répertoire exporté et les options dans un ensemble de fichiers plutôt que de tous les entrer manuellement. En exécutant `autofs` en tant que service qui se lance et s'arrête aux niveaux d'exécution désignés, les configurations de montage dans les divers fichiers peuvent être appliquées automatiquement. Pour utiliser `autofs`, le paquetage RPM `autofs` doit être installé sur votre système.

Les fichiers de configuration `autofs` sont arrangés selon la structure "parent-enfant". Un fichier de configuration principal (`/etc/auto.master`) se réfère à des points de montage sur votre système qui sont liés à un *type de mappe* particulier, qui prend la forme d'autres fichiers de configuration, de programmes, de mappes NIS et d'autres méthodes de montage moins communes. Le fichier `auto.master` contient des lignes qui se réfèrent à chacun de ces points de montage, organisées comme suit :

```
<point-de-montage>    <type-de-mappe>
```

<point-de-montage> indique l'endroit où le périphérique ou le système de fichiers exporté doit être monté sur votre système de fichiers local. *<type-de-mappe>* fait référence à la façon dont le point de montage sera monté. La méthode la plus utilisée pour monter automatiquement des systèmes de fichiers exportés NFS est d'utiliser un fichier comme type de mappe pour le point de montage spécifique. Le fichier mappe, généralement appelé `auto.`*<point-de-montage>*, où *<point-de-montage>* est le point de montage désigné dans `auto.master`, contient des lignes qui ressemblent à ceci :

```
<répertoire>  <options-de-montage>  <hôte>:<système-de-fichiers-exporté>
```

<répertoire> indique le répertoire du point de montage où le système de fichiers exporté doit être monté. De façon semblable à la commande `mount`, l'hôte exportant le système de fichiers, ainsi que le système de fichiers exporté sont requis dans la section *<hôte>*:*<système-de-fichiers-exporté>*. Pour spécifier des options spéciales à utiliser lors du montage du système de fichiers exporté, placez-les dans la section *<options-de-montage>*, séparées par des virgules. Pour les montages NFS qui utilisent `autofs`, vous devez placer au moins `-fstype=nfs` dans la section *<options-de-montage>*.

En plus de pouvoir être utilisés pour toute une série de montages de nombreux types de périphérique et de système de fichiers, les fichiers de configuration `autofs` sont également particulièrement utiles pour créer des montages NFS. Exemple : certaines organisations stockent le répertoire personnel (`/home`) d'un utilisateur sur un serveur central via un partage NFS. Puis, elles configurent le fichier `auto.master` sur chaque station de travail de façon à pointer vers un fichier `auto.home` contenant les instructions spécifiques pour le montage du répertoire `/home` via NFS. Cela permet à l'utilisateur d'accéder à ses données personnelles et aux fichiers de configuration dans son répertoire `/home` en se connectant n'importe où sur le réseau local. Le fichier `auto.master` dans cet exemple ressemblerait à ceci :

```
/home   /etc/auto.home
```

Cela définit le point de montage de `/home` sur le système local devant être configuré par le fichier `/etc/auto.home`, qui peut ressembler à ceci :

```
*  -fstype=nfs,soft,intr,rsize=8192,wsize=8192,nosuid  server.domain.com:/home/&
```

Cette ligne indique que tout répertoire auquel un utilisateur essaie d'accéder sous le répertoire local `/home` (en raison de l'astérisque) devrait donner un montage NFS sur le système server.domain.com dans son système de fichiers exporté `/home`. Les options de montage indiquent que tout montage NFS du répertoire `/home` doit utiliser un ensemble précis de réglages. Pour en savoir plus sur les options de montage, y compris les options utilisées dans cet exemple, reportez-vous à la la section intitulée *Options de montage NFS courantes*.

Options de montage NFS courantes

Lors du montage d'un système de fichiers via NFS ou un hôte distant, de nombreuses options peuvent être spécifiées pour faciliter l'utilisation. Ces options peuvent être utilisées avec des commandes `mount` manuelles, des réglages `/etc/fstab` et `autofs` ou d'autres méthodes de montage.

Les options suivantes sont les plus utilisées pour les montages NFS :

- `hard` ou `soft` spécifient si le programme qui utilise un fichier via une connexion NFS doit s'arrêter ou attendre (`hard`) que le serveur soit de nouveau en ligne lorsque l'hôte qui sert le système de fichiers exporté n'est pas disponible ou s'il doit rapporter une erreur (`soft`).

  Si vous spécifiez `hard`, vous ne pourrez arrêter le processus qui attend le rétablissement de la connexion NFS, à moins de spécifier également l'option `intr`.

  Si vous spécifiez `soft`, vous pouvez également définir une option additionnelle, `timeo=<valeur>`, où `<valeur>` indique le nombre de secondes devant s'écouler avant que l'erreur ne soit rapportée.
- `intr` permet aux demandes NFS d'être annulées si le serveur est en panne ou ne peut être joint.
- `nolock` est parfois nécessaire lors de connexions à un serveur plus ancien. Pour demander le verrouillage, utilisez l'option `lock`.
- `noexec` n'autorise pas l'exécution de binaires sur le système de fichiers monté. Cela est utile si votre système Red Hat Linux monte un système de fichiers non-Linux via NFS qui contient des binaires qui ne seront pas exécutés sur votre ordinateur.
- `nosuid` ne permet pas aux bits set-user-identifier ou set-group-identifier d'être appliqués.
- `rsize=8192` et `wsize=8192` peuvent accélérer les communications NFS en lecture (`rsize`) et écriture (`wsize`) en paramétrant une taille de bloc de données plus grande, en octets, devant être transféré en même temps. Soyez prudent lorsque vous modifiez ces valeurs ; certains noyaux Linux plus anciens et cartes réseaux pourraient ne pas fonctionner correctement avec des tailles de bloc plus grandes.
- `nfsvers=2` ou `nfsvers=3` spécifie la version du protocole NFS à utiliser.

De nombreuses autres options sont disponibles dans la page de manuel de `mount`, notamment les options à utiliser lors du montage de systèmes de fichiers non-NFS.

Sécuriser NFS

NFS fonctionne bien pour partager de façon très transparente des systèmes de fichiers entiers avec de nombreux hôtes connus. Nombre d'utilisateurs ont accès à des fichiers sur un montage NFS sans même s'apercevoir que le système de fichiers qu'ils utilisent n'appartient pas à leur système local. Cependant, la facilité d'utilisation va de pair avec toute une série de problèmes potentiels de sécurité.

Vous devriez tenir compte des informations suivantes lorsque vous exportez des systèmes de fichiers NFS sur un serveur ou les montez sur un client. Ainsi, vous minimiserez les risques de sécurité NFS et protégerez mieux vos données ainsi que votre équipement.

Accès hôte

NFS contrôle qui peut monter et exporter un système de fichiers en fonction de l'hôte présentant la demande de montage et non en fonction de l'utilisateur qui utilise le système de fichiers. Les hôtes doivent obtenir des droits explicites pour monter un système de fichiers. Le contrôle d'accès n'est cependant pas possible pour les utilisateurs, si ce n'est au niveau des autorisations de fichier et de répertoire. Autrement dit, lorsque vous exportez un système de fichiers via NFS vers un hôte distant, vous ne faites pas confiance uniquement à l'hôte qui monte le système de fichiers, mais aussi aux utilisateurs qui ont accès à cet hôte et, par conséquent, à votre système de fichiers. Ce risque peut être contrôlé, en exigeant des montages en lecture seule par exemple ou en réduisant les utilisateurs à un ID utilisateur et groupe commun, ce qui peut empêcher toutefois que le montage ne soit utilisé de la façon souhaitée à l'origine.

De plus, si l'auteur d'une attaque prend le contrôle du serveur DNS utilisé par le système qui exporte le système de fichiers NFS, le système associé à un nom d'hôte spécifique ou à un nom de domaine pleinement qualifié peut être pointé vers un ordinateur non autorisé. A ce stade, l'ordinateur non autorisé *est* le système autorisé à monter le partage NFS car aucune information de nom d'utilisateur ou de mot de passe n'est échangée pour fournir plus de sécurité au montage NFS. Les mêmes risques s'appliquent aux serveurs NIS compromis, si les groupes réseau NIS sont utilisés pour permettre à certains hôtes de monter un partage NFS. En utilisant une adresse IP dans `/etc/exports`, ce genre d'attaque est plus difficile.

Utilisez les caractères spéciaux avec modération lorsque vous accordez à un hôte l'accès à un partage NFS. La portée du caractère spécial peut englober des systèmes dont vous ignorez l'existence et qui ne devraient pas être autorisés à monter le système de fichiers.

Autorisations de fichier

Lorsqu'un système de fichiers est monté en lecture-écriture par un hôte distant, la seule protection pour les fichiers partagés repose dans leurs autorisations et leur appartenance à un utilisateur et un groupe. Si deux utilisateurs partageant la même valeur d'ID utilisateur montent le même système de fichiers NFS, ils pourront modifier l'un et l'autre leurs fichiers. De plus, tout individu connecté en tant que super-utilisateur sur le système client peut utiliser la commande `su -` afin de devenir un utilisateur ayant accès à des fichiers spécifiques via le partage NFS.

Le comportement par défaut lors de l'exportation d'un système de fichiers via NFS consiste à utiliser *root squashing*. Cela a pour effet de paramétrer sur une valeur du compte nobody du serveur l'ID utilisateur de tout utilisateur se servant du partage NFS en tant que super-utilisateur sur son ordinateur local. Vous ne devriez pas désactiver la réduction du super-utilisateur, à moins que la présence de nombreux super-utilisateurs sur votre système ne vous dérange pas.

Si vous n'autorisez les utilisateurs qu'à lire les fichiers via votre partage NFS, vous pouvez utiliser l'option `all_squash`, qui fait en sorte que tous les utilisateurs accédant à votre système de fichiers exporté aient l'ID utilisateur de l'utilisateur nobody.

Précédent
Fichiers de configuration d'un client NFS

Sommaire
Niveau supérieur

Suivant
Autres ressources

Autres ressources

L'administration d'un serveur NFS peut être une gageure. De nombreuses options (certaines n'ayant même pas été mentionnées dans ce chapitre) sont disponibles pour exporter des systèmes de fichiers NFS ou en monter en tant que client. Consultez les sources d'informations suivantes pour avoir plus de détails à ce sujet.

Documentation installée

- `/usr/share/doc/nfs-utils-<numéro-de-version>` — Donne des informations sur la façon dont NFS est appliqué sous Linux, notamment sur les différentes configurations de NFS et leurs effets sur les performances de transfert de fichiers.
- Les pages de manuel suivantes sont très utiles :
  - `mount` — Aperçu détaillé des options de montage, aussi bien pour la configuration serveur que client.
  - `fstab` — Détails sur le format du fichier `/etc/fstab` utilisé pour monter des systèmes de fichiers au démarrage du système.
  - `nfs` — Détails sur l'exportation de systèmes de fichiers NFS et les options de montage.
  - `exports` — Options couramment utilisées dans le fichier `/etc/exports` lors de l'exportation de systèmes de fichiers NFS.

Livres sur le sujet

- *Managing NFS and NIS* bde Hal Stern, Mike Eisler et Ricardo Labiaga ; O'Reilly & Associates — Excellent guide de référence sur les nombreuses options de montage et d'exportation NFS disponibles.
- *NFS Illustrated* de Brent Callaghan ; Addison-Wesley Publishing Company — Fournit des comparaisons entre les systèmes de fichiers NFS et d'autres réseaux et montre, de façon détaillée, comment se font les communications NFS.

Chapitre 19. Protocole LDAP (Lightweight Directory Access Protocol)

Qu'est-ce que le protocole LDAP ?

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

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

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

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

Ce chapitre décrit la configuration et l'utilisation de OpenLDAP, une implémentation " Open Source " de LDAP. OpenLDAP comprend `slapd` (un serveur LDAP autonome), `slurpd` (un serveur de

duplication LDAP autonome), des bibliothèques implémentant le protocole LDAP, des utilitaires, des outils, des exemples de clients.

Précédent
Autres ressources

Sommaire
Niveau supérieur

Suivant
Avantages et inconvénients de LDAP

Avantages et inconvénients de LDAP

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

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

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

Utilisations du protocole LDAP

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

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

Applications LDAP

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

- **Navigateur LDAP/Editeur** — Un outil convivial entièrement écrit en langage Java, pour un déploiement facile sur plusieurs plates-formes. Vous le trouverez à l'adresse suivante : http://www.iit.edu/~gawojar/ldap
- **GQ** — Client LDAP basé sur GTK, fourni avec la distribution sous emballage Red Hat Linux 7.3 ou à l'adresse http://biot.com/gq

LDAP et PAM

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

Avantages et inconvénients de LDAP

Niveau supérieur

Terminologie LDAP

Terminologie LDAP

Une *entrée*< correspond à une unité dans un annuaire LDAP. Une entrée est identifiée ou référencée par son *Identificateur unique* (*IU*).

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

Certains attributs sont obligatoires, tandis que d'autres sont facultatifs. Une *classe d'objets* définit les attributs obligatoires et les attributs facultatifs. Vous trouverez des définitions de classes d'objets dans le répertoire `/etc/openldap/schema`.

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

```
[<id>]
dn: <nom unique>
<typeattr>: <valeurattr>
<typeattr>: <valeurattr>
<typeattr>: <valeurattr>
```

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

Attention **Attention**

Vos paires `<typeattr>` et `<valeurattr>` *doivent* être définies par un schéma avant de pouvoir être utilisés. Vous ne pouvez pas vous contenter de les définir dans un fichier LDIF et vous attendre à ce qu'un serveur LDAP n'ayant pas de données correspondantes dans ses fichiers schéma puisse utiliser ces informations.

Tout ce qui est contenu dans < > est variable et vous pouvez le paramétrer lorsque vous ajoutez une

entrée LDAP, à l'exception de *<id>*. *<id>* est un nombre qui est habituellement paramétré par les outils LDAP lorsque vous ajoutez une entrée, et vous n'aurez sans doute jamais à en paramétrer manuellement.

Précédent | Sommaire | Suivant
Utilisations du protocole LDAP | Niveau supérieur | Mises à jour de OpenLDAP 2.0

Mises à jour de OpenLDAP 2.0

OpenLDAP 2.0 représente une des plus importantes mises à jour de l'application, grâce à :

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

Fichiers OpenLDAP

Les fichiers de configuration OpenLDAP sont installés dans le répertoire `/etc/openldap`. Si vous appliquez la commande `ls` à `/etc/openldap`, vous verrez les fichiers ainsi que le répertoire suivants :

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

`slapd.conf`

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

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

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

de façon à reflèter votre nom de domaine. Par exemple

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

ou

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

L'entrée rootdn est le nom de domaine pour un utilisateur non restreint par les paramètres de contrôle d'accès ou de limite administrative définis pour les opérations sur l'annuaire LDAP. On peut se

représenter l'utilisateur rootdn comme l'utilisateur root pour l'annuaire LDAP. La ligne rootdn doit être modifiée de :

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

en quelque chose comme :

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

or

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

Modifiez la ligne rootpw de :

```
rootpw          secret
```

en quelque chose comme :

```
rootpw          {crypt}s4L9sOIJo4kBM
```

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

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

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

Vous pourriez également copier une entrée `passwd` de `/etc/passwd`, mais ceci ne fonctionnera pas si l'entrée `passwd` est un mot de passe MD5 (valeur par défaut dans Red Hat Linux 7.3).

Le répertoire schema

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

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

Attention **Attention**

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

Vous pouvez étendre le schéma utilisé par OpenLDAP pour prendre en charge des types d'attributs et classes d'objets supplémentaires, en utilisant comme guide les fichiers schéma 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 sous 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`. De nombreuses organisations utilisent des types d'attributs et classes d'objets existants dans les fichiers schéma installés par défaut, et les modifient pour les utiliser dans le fichier `local.schema`. Ceci peut vous aider à apprendre la syntaxe de schéma tout en répondant aux besoins immédiats de votre organisation.

Etendre les schémas pour répondre à certaines nécessités spécifiques est un sujet complexe qui ne rentre pas dans le cadre de ce chapitre. Pour plus d'informations sur l'écriture de nouveaux fichiers schéma, consultez http://www.openldap.org/doc/admin/schema.html.

Précédent
Mises à jour de OpenLDAP 2.0
Sommaire
Niveau supérieur
Suivant
Démons et utilitaires OpenLDAP

Démons et utilitaires OpenLDAP

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

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

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

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

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

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

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

- `slapadd` — Ajoute des entrées depuis un fichier LDIF ou un répertoire LDAP. Par exemple, exécutez `/usr/sbin/slapadd -l` *`ldif`* où *`ldif`* est le nom du fichier LDIF contenant de nouvelles entrées.
- `slapcat` — Retire les entrées d'un répertoire LDAP et les sauvegarde dans un fichier LDIF. Par exemple, exécutez `/usr/sbin/slapcat -l` *`ldif`* où *`ldif`* est le nom du fichier cible qui contient les entrées du répertoire LDAP.
- `slapindex` — Réindexe la base données `slapd` basée sur le contenu de l'actuelle base de

données. Exécutez `/usr/sbin/slapindex` pour commencer à réindexer.

- `slappasswd` — Génère une valeur de mot de passe utilisateur à utiliser avec `ldapmodify` ou la valeur `rootpw` dans `/etc/openldap/slapd.conf`. Exécutez `/usr/sbin/slappasswd` pour créer le mot de passe.

Avertissement **Avertissement**

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

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

Précédent
Fichiers OpenLDAP

Sommaire
Niveau supérieur

Suivant
Modules pour l'ajout de fonctionnalités à LDAP

Modules pour l'ajout de fonctionnalités à LDAP

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

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

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

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

Configuration de OpenLDAP : présentation rapide

Cette section fournit une présentation rapide des opérations à accomplir pour installer et configurer un annuaire OpenLDAP. Pour plus d'informations, reportez-vous au *Quick-Start Guide* sur le site Web d'OpenLDAP disponible à l'adresse

```
http://www.openldap.org/doc/admin/quickstart.html
```

et à *Linux LDAP HOWTO* disponible à l'adresse

```
(http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO.html
```

1. Installez les RPM `openldap`, `openldap-servers` et `openldap-clients`, ainsi que tout autre RPM nécessaire en rapport avec LDAP qui ne l'a pas encore été.
2. Editez le fichier `/etc/openldap/slapd.conf` afin de référencer votre domaine ainsi que votre serveur LDAP. Reportez-vous à la section intitulée *`slapd.conf`* afin d'obtenir davantage d'informations.
3. Lancez `slapd` en tapant :

   ```
   /sbin/service/ldap start
   ```

   Après avoir correctement configuré LDAP, utilisez `chkconfig` ou **serviceconf** pour configurer LDAP de façon à lancer le système.
4. Créez votre annuaire LDAP. Des exemples d'entrées LDAP figurent sur le site Web de PADL Software à l'adresse :

   ```
   http://www.padl.com/ldap_examples.html
   ```
5. Ajoutez des entrées à votre annuaire LDAP à l'aide de `ldapadd`.

6. Utilisez `ldapsearch` afin de vérifier si `slapd` fonctionne.
7. A ce stade, votre annuaire LDAP devrait exister. L'étape suivante consiste à configurer vos applications compatibles LDAP de manière à ce qu'elles puissent utiliser l'annuaire LDAP.

Précédent
Modules pour l'ajout de fonctionnalités à LDAP

Sommaire
Niveau supérieur

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

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

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

Installez les paquetages LDAP nécessaires

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

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

Editez les fichiers de configuration

Editer `slapd.conf`

Ensuite, éditez le fichier `/etc/openldap/slapd.conf` pour vous assurer qu'il correspond aux besoins spécifiques de votre organisation.

Pour obtenir des informations sur l'édition de `slapd.conf`, consultez la la section intitulée *`slapd.conf`*.

Editer `ldap.conf`

Editez le fichier `ldap.conf` sur le serveur LDAP et les clients.

Editez `/etc/ldap.conf`, le fichier de configuration pour `nss_ldap` et `pam_ldap`, afin refléter votre organisation et votre base de recherche. Le fichier `/etc/openldap/ldap.conf` est le fichier de configuration pour les outils de la ligne de commande tels que `ldapsearch` et `ldapadd` ; il devra

aussi être édité pour le paramétrage de votre LDAP. Les ordinateurs clients auront besoin de ces deux fichiers modifiés.

Editer `/etc/nsswitch.conf`

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

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

PAM et LDAP

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

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

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

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

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

en quelque chose comme :

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

La base par défaut devrait également être changée de

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

en quelque chose comme :

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

Ensuite, vous devez choisir le script à utiliser, en fonction du Tableau 19-1.

Tableau 19-1. Scripts de migration LDAP

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

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

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

Autres ressources

Il existe d'autres informations concernant LDAP. Consultez ces sources, en particulier le site Web OpenLDAP et le HOWTO LDAP, avant de commencer à configurer LDAP sur votre système.

Documentation installée

- La page du manuel `ldap` constitue un bon point de départ pour une introduction à LDAP. Vous trouverez aussi des pages du manuel consacrées aux démons et utilitaires de LDAP. Si vous avez besoin de plus d'informations sur `ldapmodify`, `ldapsearch` et autres, consultez les pages du manuel correspondantes.
- `/usr/share/docs/openldap-`*`version`* — Contient un document `README` général ainsi que des informations diverses.

Sites Web utiles

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

personnalisation.

Livres sur le sujet

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

---

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

Sommaire
Niveau supérieur

Suivant
Annexes

IV. Annexes

Table des matières

A. Paramètres généraux et modules

Annexe A. Paramètres généraux et modules

Cette annexe est fournie pour illustrer *quelques-uns* des paramètres dont peuvent avoir besoin certains pilotes[1] pour des périphériques. Dans la plupart des cas, ces paramètres supplémentaires sont inutiles car le noyau est déjà en mesure d'utiliser les périphériques sans eux. Vous ne devriez utiliser les paramètres fournis dans cette annexe que lorsque vous avez de la difficulté à faire fonctionner un périphérique donné sous Red Hat Linux ou devez modifier les paramètres par défaut du système pour le périphérique.

Durant l'installation de Red Hat Linux, certaines limites sont appliquées aux systèmes de fichiers et d'autres pilotes pris en charge par le noyau. Toutefois, après l'installation, il y a une prise en charge pour tous les systèmes de fichiers disponibles sous Linux. Lors de l'installation, le noyau modularisé prend en charge des périphériques (E)IDE (notamment les lecteurs de CD-ROM ATAPI), des cartes SCSI et des cartes réseau.

Note **Remarque**

Du fait que Red Hat Linux prend en charge l'installation sur de nombreux types de matériel différents, certains pilotes (dont ceux pour les cartes SCSI, les cartes réseau et nombre de lecteurs de CD-ROM) ne sont pas intégrés dans le noyau Linux utilisé par le programme d'installation. Ils sont plutôt disponibles comme modules et chargés en fonction de vos besoins durant le processus d'installation. Le cas échéant, vous avez la possibilité de spécifier des options pour ces modules au moment de leur chargement à partir du disque du pilote.

Pour spécifier les paramètres du module lorsqu'un pilote est chargé, tapez **`linux expert`** à l'invite `boot:` et insérez le disque du pilote lorsque le programme d'installation vous le demande. Après avoir lu le disque, le programme d'installation vous demande de sélectionner le type de périphérique que vous configurez. Vous pouvez alors faire votre sélection dans cet écran pour spécifier le paramètre du module. Ensuite, le programme d'installation affiche un écran où il vous est possible d'entrer les paramètres en fonction du type spécifique de périphérique que vous êtes en train de configurer.

Une fois l'installation terminée, vous pouvez recréer un noyau incluant la prise en charge de votre configuration matérielle spécifique. Prenez note que dans la plupart des cas, un noyau personnalisé n'est pas nécessaire. Reportez-vous au *Guide de personnalisation officiel Red Hat Linux* pour avoir plus de renseignements au sujet de la recompilation de votre noyau.

Spécification des paramètres d'un module

Si vous fournissez les paramètres au moment du chargement d'un module, vous pouvez habituellement les spécifier de deux façons différentes :

- Spécifier un ensemble complet de paramètres au moyen d'une seule instruction. Par exemple, le paramètre `cdu31=0x340,0` pourrait être utilisé avec un CDU Sony 31 ou 33 sur le port 340 sans IRQ.
- Spécifier les paramètres un par un. Cette méthode est utilisée lorsqu'un ou plusieurs paramètres du premier ensemble ne sont pas nécessaires. Par exemple, `cdu31_port=0x340 cdu31a_irq=0` peut être utilisé comme paramètre pour le même lecteur de CD-ROM donné dans l'exemple précédent. On utilise un *OU* dans les tableaux CD-ROM, SCSI et Ethernet de cette annexe pour montrer où la première méthode de paramétrage s'arrête et où la seconde commence.

Note **Remarque**

N'utilisez qu'une seule méthode, et non les deux, lorsque vous chargez un module avec des paramètres particuliers.

Attention **Avertissement**

Lorsqu'un paramètre contient une virgule, assurez-vous de *ne pas* mettre d'espace après la virgule.

Notes

[1] Un *pilote* est un type de logiciel qui aide le système à utiliser un périphérique donné. Sans ce pilote, le noyau pourrait ne pas savoir comment utiliser correctement le périphérique.

Précédent Annexes | Sommaire Niveau supérieur | Suivant Paramètres des modules pour CD-ROM

Paramètres des modules pour CD-ROM

Note **Remarque**

Les lecteurs de CD-ROM répertoriés ne sont pas tous pris en charge. Veuillez consulter la liste de compatibilité des composants matériels sur le site Web de Red Hat à l'adresse http://hardware.redhat.com pour vous assurer que votre lecteur de CD-ROM est pris en charge.

Bien que les paramètres soient spécifiés une fois le disque du pilote a été chargé et le périphérique défini, l'un des paramètres les plus couramment utilisés (`hd`*`X`*`=cdrom`) *peut* être entré à l'invite de démarrage (`boot:`) lors de l'installation. Cette exception à la règle est due au fait que ce paramètre a trait à la prise en charge de CD-ROM IDE/ATAPI, faisant déjà partie du noyau.

Dans les tableaux suivants, la plupart des modules dépourvus de paramètres sont capables d'une détection automatique du matériel, ou requièrent un changement manuel de paramètres dans le code source du module et une recompilation.

Tableau A-1. Paramètres du matériel

Matériel	Module	Paramètres
Lecteurs de CD-ROM ATAPI/IDE		hd*X*=cdrom
Aztech CD268-01A, Orchid CD-3110, Okano/Wearnes CDD110, Conrad TXC, CyCDROM CR520, CyCDROM CR540 (non IDE)	`aztcd.o`	aztcd= *`port_es`*
CD-ROM Sony CDU-31A	`cdu31a.o`	cdu31a=*`port_es`*,*`IRQ`* *OU* cdu31a_port=*`adr_base`* cdu31a_irq=*`irq`*
Lecteur de CD-ROM Philips/LMS 206 avec carte adaptateur hôte cm260	`cm206.o`	cm206=*`port_es`*,*`IRQ`*

CD-ROM Goldstar R420	`gscd.o`	gscd=*`port_es`*
Interface CD-ROM de carte son ISP16, MAD16 ou Mozart (OPTi 82C928 et OPTi 82C929) avec lecteurs Sanyo/Panasonic, Sony ou Mitsumi	`isp16.o`	isp16=*`port_es`*,*`IRQ`*,*`dma`*, *`lecteur_type`* *OU* isp16_cdrom_base=*`port_es`* isp16_cdrom_irq=*`IRQ`* isp16_cdrom_dma=*`dma`* isp16_cdrom_type=*`lecteur_type`*
CD-ROM Mitsumi standard	`mcd.o`	mcd=*`port_es`*,*`IRQ`*
CD-ROM Mitsumi expérimental	`mcdx.o`	mcdx=*`port_es_1`*,*`IRQ_1`*, *`port_es_n`*,*`IRQ_n`*
Lecteur de CD-ROM de stockage optique "Dolphin" 8000 AT, Lasermate CR328A	`optcd.o`	
CD-ROM IDE port parallèle	`pcd.o`	
SB Pro 16 compatible	`sbpcd.o`	sbpcd=*`port_es`*
CDR-H94A Sanyo	`sjcd.o`	sjcd=*`port_es`* *OU* sjcd_base=*`port_es`*
CDU-535 et 531 de Sony (certains lecteurs Procomm)	`sonycd535.o`	sonycd535=*`port_es`*

Voici quelques exemples des modules utilisés :

Tableau A-2. Exemples de configuration de paramètres matériels

Configuration	**Exemple**
CD-ROM ATAPI, branché comme maître sur le deuxième canal IDE	hdc=cdrom
CD-ROM Mitsumi non IDE sur port 340, IRQ 11	mcd=0x340,11
Trois lecteurs de CD-ROM Mitsumi non IDE utilisant le pilote expérimental, les ports E/S 300, 304 et 320 avec IRQ 5, 10 et 11	mcdx=0x300,5,0x304,10,0x320,11
Sony CDU 31 ou 33 au port 340, sans IRQ	cdu31=0x340,0 *OU* cdu31_port=0x340 cdu31a_irq=0

CD-ROM Aztech sur port 220	aztcd=0x220
CD-ROM de type Panasonic sur interface SoundBlaster connecté au port 230	sbpcd=0x230,1
Phillips/LMS cm206 et cm260 à E/S 340 et IRQ 11	cm206=0x340,11
Goldstar R420 à E/S 300	gscd=0x300
Lecteur Mitsumi sur carte son MAD16 à adresse ES 330 et IRQ 1, test DMA	isp16=0x330,11,0,Mitsumi
Sony CDU 531 à adresse E/S 320	sonycd535=0x320

Note **Remarque**

La plupart des cartes Sound Blaster récentes sont livrées avec des interfaces IDE. Pour ces cartes, vous ne devez pas utiliser de paramètres `sbpcd`, mais uniquement des paramètres `hdX`.

Précédent Sommaire Suivant
Paramètres généraux et modules Niveau supérieur Paramètres SCSI

Paramètres SCSI

Tableau A-3. Paramètres SCSI

Matériel	Module	Paramètres
Adaptec 28xx, R9xx, 39xx	`aic7xxx.o`	
Contrôleur de mémoire 3ware	`3w-xxxx.o`	
NCR53c810/820/720, NCR53c700/710/700-66	`53c7,8xx.o`	
Pilote AM53/79C974 (PC-SCSI)	`AM53C974.o`	
La plupart des cartes Buslogic (maintenant Mylex) avec numéro de référence "BT"	`BusLogic.o`	
DAC960 RAID Controller Mylex</	`DAC960.o`	
SCSI base sur MCR53c406a	`NCR53c406a.o`	
Initio INI-9100UW	`a100u2w.o`	a100u2w=*es*,*IRQ*,*scsi_id*
AACRAID Adaptec	`aacraid.o`	
Cartes SCSI Advansys	`advansys.o`	
Adaptec AHA-152x	`aha152x.o`	aha152x=*es*,*IRQ*,*scsi_id*
AHA 154x et 631x de type Adaptec	`aha1542.o`	
Adaptec AHA 1740	`aha1740.o`	

Adaptec AHA-274x, AHA-284x, AHA-29xx, AHA-394x, AHA-398x, AHA-274x, AHA-274xT, AHA-2842, AHA-2910B, AHA-2920C, AHA-2930/U/U2, AHA-2940/W/U/UW/AU/, U2W/U2/U2B/, U2BOEM, AHA-2944D/WD/UD/UWD, AHA-2950U2/W/B, AHA-3940/U/W/UW/, AUW/U2W/U2B, AHA-3950U2D, AHA-3985/U/W/UW, AIC-777x, AIC-785x, AIC-786x, AIC-787x, AIC-788x , AIC-789x, AIC-3860	`aic7xxx.o`	
Contrôleur SCSI PCI ACARD ATP870U	`atp870u.o`	
Contrôleur Compaq Smart Array 5300	`cciss.o`	
Contrôleur Compaq Smart/2 RAID	`cpqarray.o`	
Contrôleur Compaq FibreChannel	`cpqfc.o`	
Domex DMX3191D	`dmx3191d.o`	
Data Technology Corp DTC3180/3280	`dtc.o`	
Cartes hôtes SCSI DTP (EATA/DMA)PM2011B/9X ISA, PM2021A/9X ISA, PM2012A, PM2012B, PM2022A/9X EISA, PM2122A/9X, PM2322A/9X, SmartRAID PM3021, PM3222, PM3224	`eata.o`	

Cartes SCSI DTP PM2011, PM2021, PM2041, PM3021, PM2012B, PM2022, PM2122, PM2322, PM2042, PM3122, PM3222, PM3332, PM2024, PM2124, PM2044, PM2144, PM3224, PM3334	`eata_dma.o`	
Sun Enterprise Network Array (FC-AL)	`fcal.o`	
Future Domain TMC-16*xx* SCSI	`fdomain.o`	
NCR5380 (pilote générique)	`g_NCR5380.o`	
Contrôleur ICP RAID	`gdth.o`	
I2O Block Driver	`i2o_block.o`	
Carte SCSI pour port parallèle IOMEGA MatchMaker	`imm.o`	
Carte SCSI ISA Always IN2000	`in2000.o`	in2000= *`setup_chaîne`* :*`valeur`* *OU* in2000 *`setup_chaîne=valeur`*
Cartes hôtes SCSI Initio INI-9X00U/UW	`initio.o`	
IBM ServeRAID	`ips.o`	
AMI MegaRAID 418, 428, 438, 466, 762	`megaraid.o`	
Cartes SCSI NCR avec circuits 810/810A/815/ 825/825A/860/875/876/895	`ncr53c8xx.o`	ncr53c8xx=*`option1`*:*`valeur1`*,*`option2`*:*`valeur2`*,… *OU* ncr53c8xx="*`option1`*:*`valeur1 option2`*:*`valeur2`*…"
Pro Audio Spectrum/Studio 16	`pas16.o`	
PCI-2000 IntelliCache	`pci2000.o`	
PCI-2220I EIDE RAID	`pci2220i.o`	
Carte hôte SCSI pour port parallèle IOMEGA PPA3	`ppa.o`	

Perceptive Solutions PSI-240I EIDE	`psi240i.o`	
Qlogic 1280	`qla1280.o`	
Qlogic 2*x*00	`qla2x00.o`	
QLogic Fast SCSI FASXXX ISA/VLB/PCMCIA	`qlogicfas.o`	
QLogic ISP2100 SCSI-FCP	`qlogicfc.o`	
Cartes SCSI QLogic ISP1020 Intelligent IQ-PCI, IQ-PCI-10, IQ-PCI-D	`qlogicisp.o`	
SBUS SCSI Qlogic ISP1020	`qlogicpti.o`	
Future Domain TMC-885, TMC-950 Seagate ST-01/02, Future Domain TMC-8*xx*	`seagate.o`	controller_type=2 adresse_base = *`adr_base`* irq=*`IRQ`*
Cartes avec circuit sym53c416	`sym53c416.o`	sym53c416=*`PORTBASE`*,*`[IRQ]`* *OU* sym53c416 io=*`PORTBASE`* irq=*`IRQ`*
Carte hôte SCSI Trantor T128/T128F/T228	`t128.o`	
Tekram DC-390(T) PCI	`tmscsim.o`	
UltraStor 14F/34F (pas 24F)	`u14-34f.o`	
UltraStor 14F, 24F et 34F	`ultrastor.o`	
Série WD7000	`wd7000.o`	

Voici quelques exemples des modules utilisés :

Tableau A-4. Exemples de configuration des paramètres SCSI</

Configuration	**Exemple**
Adaptec AHA1522 sur port 330, IRQ 11, SCSI ID 7	aha152x=0x330,11,7
Adaptec AHA1542 sur port 330	bases=0x330
Future Domain TMC-800 à CA000, IRQ 10	controller_type=2 base_address=0xca000 irq=10

Précédent
Paramètres des modules pour CD-ROM

Sommaire
Niveau supérieur

Suivant
Paramètres Ethernet

Paramètres Ethernet

Tableau A-5. Paramètres de modules Ethernet

Matériel	Module	Paramètres
3Com 3c501	`3c501.o`	3c501= *`port_es,IRQ`*
3Com 3c503 et 3c503/16	`3c503.o`	3c503= *`port_es ,IRQ`* *OU* 3c503 io= *`port_es_1, port_es_n`* irq=*`IRQ_1,IRQ_n`*
3Com EtherLink Plus (3c505)	`3c505.o`	3c505= *`port_es,IRQ`* *OU* 3c505 io=*`port_es 1,port_es n`* irq=*`IRQ_1,IRQ_2`*
3Com EtherLink 16	`3c507.o`	3c507= *`port_es,IRQ`* *OU* 3c507 io= *`port_es`* irq=*`IRQ`*
3Com EtherLink III	`3c509.o`	3c509=*`port_es,IRQ`*
3Com ISA EtherLink XL "Corkscrew"	`3c515.o`	
3Com EtherLink PCI III/XL Vortex (3c590, 3c592, 3c595, 3c597) Boomerang (3c900, 3c905, 3c595)	`3c59x.o`	
RTL8139, SMC EZ Card Fast Ethernet	`8139too.o`	
Cartes RealTek utilisant RTL8129 ou circuits RTL8139 Fast Ethernet	`8139too.o`	
Apricot 82596	`82596.o`	

Ansel Communications Modèle 3200	`ac3200.o`	ac3200= *`port_es`* ,*`IRQ`* *OU* ac3200 io= *`port_es_1`*,*`port_es_n`* irq=*`IRQ_1`*,*`IRQ_n`*
Alteon AceNIC Gigabit	`acenic.o`	
Aironet Arlan 655	`arlan.o`	
Allied Telesis AT1700	`at1700.o`	at1700= *`port_es`* ,*`IRQ`* *OU* at1700 io= *`port_es`* irq=*`IRQ`*
Crystal SemiconductorCS89[02]0	`cs89x0.o`	
Cartes EtherWORKS DE425 TP/COAX EISA, DE434 TP PCI, DE435/450 TP/COAX/AUI PCI DE500 10/100 PCI Kingston, LinkSys, SMC8432, SMC9332, Znyx31[45] etZnyx346 10/100 Avec circuits DC21040 (pas de SROM), DC21041[A], DC21140[A], DC21142, DC21143	`de4x5.o`	de4x5= *`port_es`* *OU* de4x5 io= *`port_es`* de4x5 args='eth*`X[fdx]`* autosense=*`MEDIA_STRING`*'
Ethernet Pocket Adapter D-Link DE-600	`de600.o`	
Ethernet Pocket Adapter D-Link DE-620	`de620.o`	
DIGITAL DEPCA & EtherWORKS DEPCA, DE100, DE101, DE200 Turbo, DE201Turbo DE202 Turbo TP/BNC, DE210, DE422 EISA	`depca.o`	depca= *`port_es`* ,*`IRQ`* *OU* depca io= *`port_es`* irq=*`IRQ`*
Digi Intl. RightSwitch SE-X EISA et PCI	`dgrs.o`	

Davicom DM9102(A)/DM9132/ DM9801 Fast Ethernet	`dmfe.o`	
Intel EtherExpress/1000 Gigabit	`e1000.o`	
Cabletron E2100	`e2100.o`	e2100=*`port_es,IRQ,mem`* *OU* e2100 io= *`port_es`* irq=*`IRQ`* mem=*`mem`*
Intel EtherExpress Pro10	`eepro.o`	eepro= *`port_es`* ,*`IRQ`* *OU* eepro io= *`port_es`* irq=*`IRQ`*
Pilote Intel i82557/i82558 PCI EtherExpressPro	`eepro100.o`	
Intel EtherExpress 16 (i82586)	`eexpress.o`	eexpress= *`port_es`* ,*`IRQ`* *OU* eexpress io= *`port_es`* irq=*`IRQ`*
SMC EtherPower II 9432 PCI (série 83c170/175 EPIC)	`epic100.o`	
Racal-Interlan ES3210 EISA	`es3210.o`	
ICL EtherTeam 16i/32 EISA	`eth16i.o`	eth16i= *`port_es`* ,*`IRQ`* *OU* eth16i ioaddr= *`port_es`* IRQ=*`IRQ`*
EtherWORKS 3 (DE203, DE204 et DE205)	`ewrk3.o`	ewrk= *`port_es`* ,*`IRQ`* *OU* ewrk io= *`port_es`* irq=*`IRQ`*
A Packet Engines GNIC-II Gigabit	`hamachi.o`	
HP PCLAN/plus	`hp-plus.o`	hp-plus= *`port_es`* ,*`IRQ`* *OU* hp-plus io= *`port_es`* irq=*`IRQ`*
HP LAN Ethernet	`hp.o`	hp= *`port_es`* ,*`IRQ`* *OU* hp io= *`port_es`* irq=*`IRQ`*
Cartes réseau 100VG-AnyLan HP J2585B, J2585A, J2970, J2973, J2573 Compex ReadyLink ENET100-VG4, FreedomLine 100/VG	`hp100.o`	hp100= *`port_es</,name`* *OU* hp100 hp100_port= *`port_es</`* hp100_name=*`nom`*

Bus annulaire à jeton (Token Ring) IBM 16/4	`ibmtr.o`	ibmtr= *`port_es`* *OU* io= *`port_es`*
AT1500, HP J2405A et la plupart des clones NE2100	`lance.o`	
Mylex LNE390 EISA	`lne390.o`	
NatSemi DP83815 Fast Ethernet	`natsemi.o`	
NE1000 / NE2000 (non pci)	`ne.o`	ne= *`port_es`* ,*`IRQ`* *OU* ne io= *`port_es`* irq=*`IRQ`*
Cartes PCI NE2000 RealTEk RTL-8029, Winbond 89C940, Compex RL2000, clones PCI NE2000, NetVin, NV5000SC, Via 82C926, SureCom NE34	`ne2k-pci.o`	
Novell NE3210 EISA	`ne3210.o`	
MiCom-Interlan NI5010	`ni5010.o`	
Carte NI5210 (puce Ethernet i82586)	`ni52.o`	ni52= *`port_es`* ,*`IRQ`* *OU* ni52 io= *`port_es`* irq=*`IRQ`*
NI6510 Ethernet	`ni65.o`	
AMD PCnet32 et AMD PCnetPCI	`pcnet32.o`	
SysKonnect SK-98*XX* Gigabit	`sk98lin.o`	
Ethercard ISA SMS Ultra et SMC EtherEZ (8K, 83c790)	`smc-ultra.o`	smc-ultra= *`port_es`* ,*`IRQ`* *OU* smc-ultra io= *`port_es`* irq=*`IRQ`*
Carte Ethernet EISA SMC Ultra32 (32K)	`smc-ultra32.o`	
Sun BigMac Ethernet	`sunbmac.o`	
Sundance ST201 Alta	`sundance.o`	
Sun Happy Meal Ethernet	`sunhme.o`	

Sun Quad Ethernet	`sunqe.o`	
ThunderLAN	`tlan.o`	
Cartes Ethernet PCI Digital 21x4x Tulip PCI SMC EtherPower 10 (8432T/8432BT) PCI SMC EtherPower 10/100 (9332DST) PCI DEC EtherWorks 100/10 (DE500-XA) PCI DEC EtherWorks 10 (DE450) DEC QSILVER's, Znyx 312 etherarray Allied Telesis LA100PCI-T Danpex EN-9400, Cogent EM110	`tulip.o`	io=*`port_es`*
Cartes PCI Fast Ethernet VIA Rhine avec VIA VT86c100A Rhine-II PCI ou 3043 Rhine-I D-Link DFE-930-TX PCI 10/100	`via-rhine.o`	
Carte ISA AT&T GIS (nee NCR) WaveLan	`wavelan.o`	wavelan=*`[IRQ,0],port_es,NWID`*
WD8003 et Cartes Ethernet compatibles WD8013	`wd.o`	wd= *`port_es`* ,*`IRQ`*,*`mem`*, *`mem_end`* *OU* wd io= *`port_es`* irq=*`IRQ`* mem=*`mem`* mem_end=*`end`*
PCI Compex RL100ATX	`winbond.o`	
Packet Engines Yellowfin	`yellowfin.o`	
Cartes Ethernet Broadcom BCM5700 10/100/1000	`bcm5700`	
Pilote Intel Ether Express/100	`e100`	
Bus annulaire à jeton (Token Ring) IBM 16/4 à mémoire partagée	`ibmtr`	

Bus annulaire à jeton (Token Ring) PCI Olympic-based IBM	`olympic`	
Carte Ethernet Fast PCI SIS 900/701G	`sis900`	

Voici quelques exemples des modules utilisés :

Tableau A-6. Exemples de configuration des paramètres Ethernet</

Configuration	**Exemple**
Carte ISA NE2000 à l'adresse E/S 300 et IRQ 11</	ne=0x300,11 ether=0x300,11,eth0
Carte Wavelan à l'E/S 390, détection automatique d'IRQ et utilisation de NWID pour 0x4321	wavelan=0,0x390,0x4321 ether=0,0x390,0x4321,eth0

Utilisation de plusieurs cartes Ethernet

Vous pouvez utiliser plusieurs cartes Ethernet dans un ordinateur. Si chaque carte utilise un pilote différent (par exemple, 3c509 et DE425), vous devez simplement ajouter des lignes `alias` (et éventuellement `options`) pour chaque carte dans le fichier `/etc/modules.conf`. Veuillez vous reporter au *Guide de personnalisation officiel Red Hat Linux* pour avoir plus de détails à ce sujet.

Si deux cartes Ethernet utilisent le même pilote (par exemple, deux cartes 3c509 ou une 3c595 et une 3c905), vous devez soit indiquer les adresses des deux cartes dans la ligne d'options du pilote (pour les cartes ISA), soit simplement ajouter une ligne `alias` pour chaque carte (pour les cartes PCI).

Pour plus d'informations sur l'utilisation de plusieurs cartes Ethernet, consultez la section *Linux Ethernet-HOWTO* à l'adresse http://www.redhat.com/mirrors/LDP/HOWTO/Ethernet-HOWTO.html.

Index

Symboles

.fetchmailrc, Options de configuration de Fetchmail
    options d'ensemble, Options d'ensemble
    options serveur, Options serveur
    options utilisateur, Options utilisateur
.procmailrc, Configuration de Procmail
/etc/exports, /etc/exports
/etc/fstab, Passer à un système de fichiers ext3, /etc/fstab
    ajout de partitions à, Allocation d'une étiquette avec e2label
/etc/hosts.allow, Listes de contrôle d'accès basé sur l'hôte
/etc/hosts.deny, Listes de contrôle d'accès basé sur l'hôte
/etc/lilo.conf, configuration dans , Options dans /etc/lilo.conf
/etc/named.conf, /etc/named.conf
/etc/pam.conf, Fichiers de configuration PAM
/etc/pam.d, Fichiers de configuration PAM
/etc/sysconfig, Les répertoires dans le répertoire /etc/sysconfig/
    amd, /etc/sysconfig/amd
    apmd, /etc/sysconfig/apmd
    arpwatch, /etc/sysconfig/arpwatch
    authconfig, /etc/sysconfig/authconfig
    clock, /etc/sysconfig/clock
    desktop, /etc/sysconfig/desktop
    dhcpd, /etc/sysconfig/dhcpd
    firewall, /etc/sysconfig/firewall
    gpm, /etc/sysconfig/gpm
    harddisks, /etc/sysconfig/harddisks
    hwconf, /etc/sysconfig/hwconf
    identd, /etc/sysconfig/identd
    init, /etc/sysconfig/init
    ipchains, /etc/sysconfig/ipchains

iptables, /etc/sysconfig/iptables, Stockage de l'information iptables
irda, /etc/sysconfig/irda
keyboard, /etc/sysconfig/keyboard
kudzu, /etc/sysconfig/kudzu
mouse, /etc/sysconfig/mouse
named, /etc/sysconfig/named
netdump, /etc/sysconfig/netdump
network, /etc/sysconfig/network
ntpd, /etc/sysconfig/ntpd
pcmcia, /etc/sysconfig/pcmcia
radvd, /etc/sysconfig/radvd
rawdevices, /etc/sysconfig/rawdevices
redhat-config-users, /etc/sysconfig/redhat-config-users
répertoire "networking" (réseau), Les répertoires dans le répertoire /etc/sysconfig/
répertoire apm-scripts , Les répertoires dans le répertoire /etc/sysconfig/
répertoire cbq , Les répertoires dans le répertoire /etc/sysconfig/
répertoire network-scripts, Les répertoires dans le répertoire /etc/sysconfig/
Voir aussi network
répertoire rhn , Les répertoires dans le répertoire /etc/sysconfig/
samba, /etc/sysconfig/samba
sendmail, /etc/sysconfig/sendmail
soundcard, /etc/sysconfig/soundcard
squid, /etc/sysconfig/squid
tux, /etc/sysconfig/tux
ups, /etc/sysconfig/ups
vncservers, /etc/sysconfig/vncservers
xinetd, /etc/sysconfig/xinetd
/etc/sysconfig, fichiers dans , Information Sysconfig
/etc/sysconfig/network-scripts, Scripts réseau
/etc/X11/XF86Config, Fichiers de configuration du serveur XFree86
/etc/X11/XF86Config-4, Fichiers de configuration du serveur XFree86
/etc/xinetd.conf, /etc/xinetd.conf
/initrd, Emplacement de fichiers Red Hat Linux spéciaux
/proc
apm, /proc/apm
cmdline, /proc/cmdline
cpuinfo, /proc/cpuinfo
devices, /proc/devices
dma, /proc/dma

execdomains, /proc/execdomains
fb, /proc/fb
fichiers
    niveau supérieur, Les fichiers du niveau supérieur dans /proc
filesystems, /proc/filesystems
interrupts, /proc/interrupts
iomem, /proc/iomem
ioports, /proc/ioports
isapnp, /proc/isapnp
kcore, /proc/kcore
kmsg, /proc/kmsg
ksyms, /proc/ksyms
loadavg, /proc/loadavg
locks, /proc/locks
mdstat, /proc/mdstat
meminfo, /proc/meminfo
misc, /proc/misc
modules, /proc/modules
mounts, /proc/mounts
mtrr, /proc/mtrr
partitions, /proc/partitions
pci, /proc/pci
ressources supplémentaires
    documentation installée, Documentation installée
répertoire bus, /proc/bus
répertoire driver, /proc/driver
répertoire ide, /proc/ide
    répertoires de périphérique, Répertoires de périphérique
répertoire irq, /proc/irq
répertoire net, /proc/net
répertoire scsi, /proc/scsi
répertoire self, /proc/self
répertoire sys, /proc/sys
    répertoire dev, /proc/sys/dev
    répertoire fs, /proc/sys/fs
    répertoire kernel, /proc/sys/kernel
    répertoire net, /proc/sys/net
    répertoire vm, /proc/sys/vm
répertoire sysvipc, /proc/sysvipc

répertoire tty, /proc/tty
répertoires, Répertoires dans /proc
répertoires de processus, Répertoires de processus
slabinfo, /proc/slabinfo
sources d'informations complémentaires, Autres ressources
sites Web utiles, Sites Web utiles
stat, /proc/stat
swaps, /proc/swaps
sys répertoire
contrôle avec sysctl, Utilisation de sysctl
uptime, /proc/uptime
version, /proc/version
visualisation de fichiers, Visualisation de fichiers virtuels
/var/named/, Fichiers de zone
arrêt , Arrêt
démarrage
mode mono-utilisateur
GRUB, SysV Init
LILO, SysV Init
noyau , Paramètres généraux et modules
pilotes , Paramètres généraux et modules
paramètres
module, Paramètres généraux et modules
modules Ethernet , Paramètres Ethernet
modules pour CD-ROM , Paramètres des modules pour CD-ROM
paramètres d'un module
spécification , Spécification des paramètres d'un module
paramètres du module , Paramètres généraux et modules
processus de démarrage , Processus de démarrage, Init et arrêt
init, Init
x86, Dans les coulisses du processus de démarrage
utilitaires initscript , Utilitaires de gestion des scripts Init
étiquetage de partitions
Voir e2label

A

AccessConfig
directive de configuration Apache, AccessConfig

AccessFileName
directive de configuration Apache, AccessFileName
Action
directive de configuration Apache, Action
ADC
Voir Agent de distribution du courrier
AddDescription
directive de configuration Apache, AddDescription
AddEncoding
directive de configuration Apache, AddEncoding
AddHandler
directive de configuration, AddHandler
AddIcon
directive de configuration Apache, AddIcon
AddIconByEncoding
directive de configuration Apache, AddIconByEncoding
AddIconByType
directive de configuration Apache, AddIconByType
AddLanguage
directive de configuration Apache, AddLanguage
AddModule
directive de configuration Apache, AddModule
AddType
directive de configuration Apache, AddType
AGC
Voir Agent de gestion de courrier
Agent de distribution du courrier, Agent de distribution du courrier
Agent de gestion de courrier, Agent de gestion de courrier
Agent de transfert de courrier, Agent de transfert de courrier
ajout
polices
XFree86, Ajout de polices
ajout de polices
xfs, Ajout de polices
Alias
directive de configuration Apache, Alias
Allow
directive de configuration Apache, Allow
AllowOverride
directive de configuration Apache, AllowOverride
Apache, Apache

arrêt, Démarrage et arrêt de httpd
autres ressources, Autres ressources
livres sur le sujet, Livres sur le sujet
sites Web utiles, Sites Web utiles
configuration, Apache, Directives de configuration dans httpd.conf
démarrage, Démarrage et arrêt de httpd
exécution sans sécurité, Utilisation d'hôtes virtuels
rapports sur l'état du serveur, Location
rechargement, Démarrage et arrêt de httpd
recompilation, Module de sécurité mod_ssl
redémarrage, Démarrage et arrêt de httpd
arrêt
Apache, Démarrage et arrêt de httpd
serveur sécurisé, Démarrage et arrêt de httpd
ATC
Voir Agent de transfert de courrier
autofs, autofs
autres ressources
XFree86, Autres ressources
documentation installée, Documentation installée
livres, Livres sur le sujet

B

Berkeley Internet Name Domain
Voir BIND
BIND, Berkeley Internet Name Domain (BIND)
autres ressources, Autres ressources
configuration, Fichiers de configuration BIND
directives de fichiers de zone, Directives de fichiers de zone
enregistrements de ressources de fichiers de zone, Enregistrements de ressources de fichiers de zone
exemples de fichiers de zone, Exemples de fichiers de zone
fichiers de zone, Fichiers de zone
résolution de nom inversée, Fichiers de résolution de noms inversée
erreurs fréquentes, Erreurs fréquentes à éviter
exemples de déclarations zone , Exemples de déclarations de zone
introduction, Introduction au DNS et à BIND
spécificités, BIND en tant que serveur de noms

types de serveurs de noms, Types de serveurs de noms
zones, Zones
propriétés
améliorations du DNS, Améliorations du protocole DNS
IPv6, IP version 6
sécurité, Sécurité
vues multiples, Vues multiples
propriétés avancées, Propriétés avancées de BIND
ressources supplémentaires
documentation installée, Documentation installée
livres sur le sujet, Livres sur le sujet
sites web utiles, Sites Web utiles
rndc, Utiliser rndc
/etc/named.conf, /etc/named.conf
/etc/rndc.conf, /etc/rndc.conf
fichiers de configuration, Fichiers de configuration
options de ligne de commande, Options de ligne de commande
BindAddress
directive de configuration Apache, BindAddress
BrowserMatch
directive de configuration Apache, BrowserMatch

C

CacheNegotiatedDocs
directive de configuration Apache, CacheNegotiatedDocs
CD-ROM
paramètres des modules , Paramètres des modules pour CD-ROM
CGI scripts
permettre une exécution à l'extérieur du répertoire cgi-bin, Directory
chkconfig, Utilitaires de gestion des scripts Init
ClearModuleList
directive de configuration Apache, ClearModuleList
client X
Voir XFree86
clients X
XFree86, Environnements de bureau et gestionnaires de fenêtres
configuration
Apache, Directives de configuration dans httpd.conf

hôtes virtuels, Utilisation d'hôtes virtuels
polices
XFree86, Configuration de xfs
réseau, Fichiers de configuration d'interface
serveur
XFree86, Fichiers de configuration du serveur XFree86
SSL, Directives de configuration SSL
xfs, Configuration de xfs
contrôle d'accès, Listes de contrôle d'accès basé sur l'hôte
conventions
documentation, Conventions de documentation
copier et coller du texte
en utilisant X, Copier et coller du texte avec X
courrier électronique, Courrier électronique
autres sources d'informations, Autres ressources
documentation installée, Documentation installée
livres sur le sujet, Livres sur le sujet
sites Web utiles, Sites Web utiles
Fetchmail, Fetchmail
Procmail, Procmail
protocoles, Protocoles
IMAP, IMAP
POP, POP
SMTP, SMTP
Sendmail, Sendmail
sécurité, Sécurité
clients, Clients de messagerie sécurisés
serveurs, Serveurs de messagerie sécurisés
types, Les différents types de programme de messagerie électronique
Agent de distribution du courrier, Agent de distribution du courrier
Agent de gestion de courrier, Agent de gestion de courrier
Agent de transfert de courrier, Agent de transfert de courrier
CustomLog
directive de configuration Apache, CustomLog

D

DefaultIcon
directive de configuration Apache, DefaultIcon

DefaultType
directive de configuration Apache, DefaultType
Deny
directive de configuration Apache, Deny
directives cache pour Apache, Directives cache
directives de configuratio, Apache
ErrorLog, ErrorLog
directives de configuration, Apache, Directives de configuration dans httpd.conf
AccessConfig, AccessConfig
AccessFileName, AccessFileName
Action, Action
AddDescription, AddDescription
AddEncoding, AddEncoding
AddHandler, AddHandler
AddIcon, AddIcon
AddIconByEncoding, AddIconByEncoding
AddIconByType, AddIconByType
AddLanguage, AddLanguage
AddModule, AddModule
AddType, AddType
Alias, Alias
Allow, Allow
AllowOverride, AllowOverride
BindAddress, BindAddress
BrowserMatch, BrowserMatch
CacheNegotiatedDocs, CacheNegotiatedDocs
ClearModuleList, ClearModuleList
CustomLog, CustomLog
DefaultIcon, DefaultIcon
DefaultType, DefaultType
Deny, Deny
Directory, Directory
DirectoryIndex, DirectoryIndex
DocumentRoot, DocumentRoot
ErrorDocument, ErrorDocument
ExtendedStatus, ExtendedStatus
Group, Group
HeaderName, HeaderName
HostnameLookups, HostnameLookups

IfDefine, IfDefine
IfModule, IfModule
IndexIgnore, IndexIgnore
IndexOptions, IndexOptions
KeepAlive, KeepAlive
KeepAliveTimeout, KeepAliveTimeout
LanguagePriority, LanguagePriority
Listen, Listen
LoadModule, LoadModule
Location, Location
LockFile, LockFile
LogFormat, LogFormat
LogLevel, LogLevel
MaxClients, MaxClients
MaxKeepAliveRequests, MaxKeepAliveRequests
MaxRequestsPerChild, MaxRequestsPerChild
MaxSpareServers, MinSpareServers and MaxSpareServers
MetaDir, MetaDir
MetaSuffix, MetaSuffix
MinSpareServers, MinSpareServers and MaxSpareServers
NameVirtualHost, NameVirtualHost
Options, Options
Order, Order
PidFile, PidFile
Port, Port
pour la fonctionnalité de cache, Directives cache
pour SSL, Directives de configuration SSL
ProxyRequests, ProxyRequests
ProxyVia, ProxyVia
ReadmeName, ReadmeName
Redirect, Redirect
ScoreBoardFile, ScoreBoardFile
ScriptAlias, ScriptAlias
ServerAdmin, ServerAdmin
ServerName, ServerName
ServerRoot, ServerRoot
ServerSignature, ServerSignature
ServerType, ServerType

SetEnvIf, SetEnvIf
StartServers, StartServers
Timeout, Timeout
TypesConfig, TypesConfig
UseCanonicalName, UseCanonicalName
User, User
UserDir, UserDir
VirtualHost, VirtualHost
directives de configuration, Apache</
ResourceConfig, ResourceConfig
directives SSL, Directives de configuration SSL
Directory
directive de configuration Apache, Directory
DirectoryIndex
directive de configuration Apache, DirectoryIndex
documentation
débutants, Documentation pour les débutants
groupes de discussion, Introduction aux groupes de discussion Linux
livres, Livres sur Linux pour les utilisateurs débutants
sites Web, Introduction aux sites Web de Linux
trouver appropriée, Trouver la documentation appropriée
utilisateur chevronné, Documentation pour les utilisateurs chevronnés
utilisateur expérimenté, Pour les utilisateurs expérimentés
DocumentRoot
directive de configuration Apache, DocumentRoot
modification, Utilisation d'hôtes virtuels
modification du partage, Hôte virtuel du serveur Web sécurisé
DSO
chargement, Ajout de modules au serveur
démarrage
Apache, Démarrage et arrêt de httpd
serveur sécurisé, Démarrage et arrêt de httpd
dépannage
après modification de httpd.conf, Directives de configuration dans httpd.conf
journal des erreurs, ErrorLog

E

e2fsck, Revenir à un système de fichiers ext2

e2label
allocation d'étiquettes de partition avec, Allocation d'une étiquette avec e2label
emplacement de fichiers Red Hat Linux spéciaux, Emplacement de fichiers Red Hat Linux spéciaux
emplacements de fichiers Red Hat Linux spéciaux
/etc/sysconfig/, Emplacement de fichiers Red Hat Linux spéciaux
Voir aussi /etc/sysconfig
/usr/lib/rhs, Emplacement de fichiers Red Hat Linux spéciaux
/var/lib/rpm, Emplacement de fichiers Red Hat Linux spéciaux
/var/spool/up2date/, Emplacement de fichiers Red Hat Linux spéciaux
environnements de bureau, Environnements de bureau
Voir aussi XFree86
clients
XFree86, Environnements de bureau
XFree86, Environnements de bureau et gestionnaires de fenêtres
ErrorDocument
directive de configuration Apache, ErrorDocument
ErrorLog
directive de configuration Apache, ErrorLog
Ethernet, Interfaces Ethernet
paramètres de modules , Paramètres Ethernet
prise en charge de plusieurs cartes , Utilisation de plusieurs cartes Ethernet
ExtendedStatus
directive de configuration Apache, ExtendedStatus

F

fdisk
commandes, Partitionnement à l'aide de fdisk
partitionnement avec, Partitionnement à l'aide de fdisk
Fetchmail, Fetchmail
autres sources d'informations, Autres ressources
options de commande, Options de commande Fetchmail
information, Options d'information ou de débogage
spéciales, Options spéciales
options de configuration, Options de configuration de Fetchmail
options d'ensemble, Options d'ensemble
options serveur, Options serveur
options utilisateur, Options utilisateur
FHS, Aperçu du FHS (Filesystem Hierarchy Standard), Organisation de FHS

fichiers journaux, Directives de configuration dans httpd.conf
format de fichier journal courant, CustomLog
fichiers à inclure côté serveur, Options , AddType
hôtes virtuels, Options
filtrage de paquetages, Filtrage de paquetages
fonctions
réseau, Fonctions réseau
format de fichier journal courant, CustomLog
formatages de lecteurs
Voir mkfs
FrontPage, Apache

G

gestionnaire d'affichage, Niveau d'exécution 5 : prefdm
gestionnaires de fenêtres, Gestionnaires de fenêtres
Voir aussi XFree86
clients
XFree86, Gestionnaires de fenêtres
XFree86, Environnements de bureau et gestionnaires de fenêtres
glisser et poser, Utilisation de la souris
Group
directive de configuration Apache, Group
groupes, Utilisateurs et groupes
propres à l'utilisateur, Utilisateurs et groupes, Groupes propres à l'utilisateur
exposé raisonné, Exposé raisonné concernant le groupe propre à l'utilisateur
standard, Groupes standard
groupes propres à l'utilisateur, Utilisateurs et groupes, Groupes propres à l'utilisateur
exposé raisonné, Exposé raisonné concernant le groupe propre à l'utilisateur
GRUB, GRUB
autres ressources, Autres ressources
documentation installée, Documentation installée
sites Web utiles, Sites Web utiles
caractéristiques, Caractéristiques de GRUB
changement de niveaux d'exécution avec, Interface éditeur d'entrée de menu
changer les niveaux d'exécution avec, SysV Init
commandes, Commandes
définition, Définition de GRUB
fichier de configuration du menu, Fichier de configuration du menu

commandes, Commandes spéciales du fichier de configuration
structure, Structure des fichiers de configuration
installation, Installation de GRUB
interfaces, Interfaces
ligne de commande, L'interface de ligne de commande
menu, Interfaces menu
ordre d'utilisation, Ordre d'utilisation de l'interface
éditeur d'entrée de menu, Interface éditeur d'entrée de menu
processus de démarrage, Processus de démarrage x86
terminologie, Terminologie
fichiers, Noms de fichier
périphériques, Noms de périphérique
système de fichiers root, Système de fichiers root de GRUB

H

HeaderName
directive de configuration Apache, HeaderName
hiérarchie, système de fichiers, Aperçu du FHS (Filesystem Hierarchy Standard)
HostnameLookups
directive de configuration Apache, HostnameLookups
http put, Location
httpd.conf
Voir directives de configuration, Apache
hôtes virtuels
basés sur le nom, Utilisation d'hôtes virtuels
commande Listen, Configuration d'hôtes virtuels
configuration, Utilisation d'hôtes virtuels
fichiers à inclure côté serveur, Options , AddType
Options, Options

I

IfDefine
directive de configuration Apache, IfDefine
IfModule
directive de configuration Apache, IfModule
IndexIgnore

directive de configuration Apache, IndexIgnore
IndexOptions
directive de configuration Apache, IndexOptions
init, Init
init, SysV-style, SysV Init
interfaces
réseau, Fichiers de configuration d'interface
alias, Fichiers alias et clone
clone, Fichiers alias et clone
commutées, Interfaces commutées
Ethernet, Interfaces Ethernet
introduction, Introduction
iptables, Techniques de mise en oeuvre de pare-feu avec iptables
différente de ipchains, Différences entre iptables et ipchains
options, Options utilisées avec les commandes iptables
cible, Options de cible
commandes, Commandes
listage, Options de listage
paramètres, Paramètres
structure, Structure
tables, Tables
options de concordance, Options de concordance
modules, Modules avec options de concordance supplémentaires
protocoles
ICMP, Protocole ICMP
TCP, Protocole TCP
UDP, Protocole UDP
sources d'informations additionnelles, Sources d'informations additionnelles
documentation installée, Documentation installée
sites Web utiles, Sites Web utiles
Stockage de l'information, Stockage de l'information iptables

K

KeepAlive
directive de configuration Apache, KeepAlive
KeepAliveTimeout
directive de configuration Apache, KeepAliveTimeout

Kerberos, Kerberos
autres ressources
documentation installée, Documentation installée
sites web utiles, Sites Web utiles
avantages de, Avantages de Kerberos
configurer des clients, Configurer un client Kerberos 5
configurer un serveur, Configurer un serveur Kerberos 5
désavantages de, Désavantages de Kerberos
et PAM, Kerberos et PAM (modules d'authentification enfichables)
fonctionnement, Fonctionnement de Kerberos
informations supplémentaires, Autres ressources
KDC (Key Distribution Center, centre distributeur de tickets), Fonctionnement de Kerberos
kerbériser, Désavantages de Kerberos
Service d'émission de tickets (TGS, ticket granting service), Fonctionnement de Kerberos
terminologie, Terminologie Kerberos
Ticket d'émission de tickets (TGT, ticket granting ticket), Fonctionnement de Kerberos

L

LanguagePriority
directive de configuration Apache, LanguagePriority
LDAP
applications, Applications LDAP
authentification à l'aide de, Configuration de votre système pour l'authentification à l'aide de OpenLDAP
autres ressources, Autres ressources
documentation installée, Documentation installée
livres sur le sujet, Livres sur le sujet
sites Web utiles, Sites Web utiles
avantages et inconvénients, Avantages et inconvénients de LDAP
démons et utilitaires, Démons et utilitaires OpenLDAP
fichiers, Fichiers OpenLDAP
répertoire schema, Le répertoire schema
slapd.conf, slapd.conf
mises à jour, Mises à jour de OpenLDAP 2.0
modules pour l'ajout de fonctionnalités<, Modules pour l'ajout de fonctionnalités à LDAP
présentation, Qu'est-ce que le protocole LDAP ?
terminology, Terminologie LDAP

utilisation avec PAM, LDAP et PAM
utilisations, Utilisations du protocole LDAP
les répertoires dans /etc/sysconfig, Les répertoires dans le répertoire /etc/sysconfig/
Listen
directive de configuration Apache, Listen
LoadModule
directive de configuration Apache, LoadModule
Location
directive de configuration Apache, Location
LockFile
directive de configuration Apache, LockFile
LogFormat
directive de configuration Apache, LogFormat
LogLevel
directive de configuration Apache, LogLevel

M

masqués
Voir mots de passe
utilitaires, Utilitaires masqués
MaxClients
directive de configuration Apache, MaxClients
MaxKeepAliveRequests
directive de configuration Apache, MaxKeepAliveRequests
MaxRequestsPerChild
directive de configuration Apache, MaxRequestsPerChild
MaxSpareServers
directive de configuration Apache, MinSpareServers and MaxSpareServers
MetaDir
directive de configuration Apache, MetaDir
MetaSuffix
directive de configuration Apache, MetaSuffix
MinSpareServers
directive de configuration Apache, MinSpareServers and MaxSpareServers
mkfs
formatage de partitions ext3 avec, Formatage de systèmes de fichiers ext3 avec mkfs
modules
Apache
chargement, Ajout de modules au serveur

personnels, Ajout de modules au serveur
par défaut, Modules par défaut
modules d'authentification enfichables
Voir PAM
modules par défaut, Modules par défaut
mod_ssl
fourni comme un DSO, Module de sécurité mod_ssl
mots de passe, Exemples de fichiers de configuration PAM
Voir aussi PAM
masqués, Exemples de fichiers de configuration PAM

N

NameVirtualHost
directive de configuration Apache, NameVirtualHost
Netscape Navigator
fonction de publication, Location
Network File System
Voir NFS
NFS, NFS (Network File System)
client
/etc/fstab, /etc/fstab
autofs, autofs
configuration, Fichiers de configuration d'un client NFS
options de montage, Options de montage NFS courantes
méthodologie, Méthodologie
portmap, NFS et portmap
serveur
configuration, Fichiers de configuration du serveur NFS
sources d'informations complémentaires, Autres ressources
documentation installée, Documentation installée
livres sur le sujet, Livres sur le sujet
sécurité, Sécuriser NFS
accès hôte, Accès hôte
autorisations de fichier, Autorisations de fichier
niveau d'exécution
3
XFree86, Niveau d'exécution 3 : startx
5

XFree86, Niveau d'exécution 5 : prefdm
niveaux d'exécution, Niveaux d'exécution d'Init
changement avec GRUB, Interface éditeur d'entrée de menu
changer avec GRUB, SysV Init
XFree86, Niveaux d'exécution
ntsysv, Utilitaires de gestion des scripts Init

O

objets partagés dynamiques
Voir DSOs
OpenLDAP, Qu'est-ce que le protocole LDAP ?
OpenSSH, Protocole SSH
fichiers de configuration, Fichiers de configuration d'OpenSSH
Options
directive de configuration Apache, Options
Order
directive de configuration Apache, Order

P

PAM, Modules d'authentification enfichables (PAM)
arguments, Arguments PAM
autres ressources, Autres ressources
documentation installée, Documentation installée
sites Web utiles, Sites Web utiles
avantages, Avantages des PAM
chemins d'accè, Chemins d'accès aux modules PAM
configurations d'exemple, Exemples de fichiers de configuration PAM
fichiers de configuration, Fichiers de configuration PAM
indicateurs de contrôle, Indicateurs de contrôle PAM
modules, Modules PAM
composants, Modules PAM
empilage, Modules d'empilage
empilage de modules, Exemples de fichiers de configuration PAM
types, Modules PAM
mots de passe masqués, Exemples de fichiers de configuration PAM
noms de service, Noms de service PAM

pam_console
propriété des périphériques locaux, Propriété de PAM et des périphériques
PAM (modules d'authentification enfichables)
et Kerberos, Kerberos et PAM (modules d'authentification enfichables)
pam_console
Voir PAM
partitionnement
Voir fdisk
PidFile
directive de configuration Apache, PidFile
polices
XFree86, Polices
xfs, Polices
Port
directive de configuration Apache, Port
portmap, NFS et portmap
rpcinfo, Etat de portmap
prefdm, Niveau d'exécution 5 : prefdm
processus de démarrage
chargement de chaîne, Processus de démarrage x86
chargement direct, Processus de démarrage x86
Procmail, Procmail
autres sources d'informations, Autres ressources
configuration, Configuration de Procmail
recettes, Recettes Procmail
actions spéciales, Conditions et actions spéciales
conditions spéciales, Conditions et actions spéciales
distribution, Recettes de distribution et de non-distribution
exemples, Exemples de recettes
fichier de verrouillage local, Spécification d'un fichier de verrouillage local
indicateurs, Indicateurs
non-distribution, Recettes de distribution et de non-distribution
programmes
exécution au démarrage , Exécution de programmes au démarrage
ProxyRequests
directive de configuration Apache, ProxyRequests
ProxyVia
directive de configuration Apache, ProxyVia
périphériques, locaux
propriété des, Propriété de PAM et des périphériques

Voir aussi PAM

R

rc.local
modification , Exécution de programmes au démarrage
ReadmeName
directive de configuration Apache, ReadmeName
Redirect
directive de configuration Apache, Redirect
resize2fs, Revenir à un système de fichiers ext2
ResourceConfig
directive de configuration Apache, ResourceConfig
ressources complémentaires
XFree86
sites Web utiles, Sites Web utiles
rpcinfo, Etat de portmap
réactions
informations sur le contact, Vos réactions sont les bienvenues
répertoire /dev, Le répertoire /dev
répertoire /etc/xinetd.d, Fichiers du répertoire /etc/xinetd.d
répertoire /mnt, Le répertoire /mnt
répertoire /proc, Le répertoire /proc, Le système de fichiers /proc
répertoire /sbin, Le répertoire /sbin
répertoire /usr, Le répertoire /usr
répertoire /usr/local, /usr/local dans Red Hat Linux
répertoire/etc, Le répertoire /etc
répertoire/lib, Le répertoire /lib
répertoire/opt, Le répertoire /opt
répertoire/usr/local, Le répertoire /usr/local
répertoire/var, Le répertoire /var
répertoires
/dev, Le répertoire /dev
/etc, Le répertoire /etc
/lib, Le répertoire /lib
/mnt, Le répertoire /mnt
/opt, Le répertoire /opt
/proc, Le répertoire /proc, Le système de fichiers /proc
/sbin, Le répertoire /sbin

/usr, Le répertoire /usr
/usr/local, Le répertoire /usr/local, /usr/local dans Red Hat Linux
/var, Le répertoire /var
répertoires public_html, UserDir

S

ScoreBoardFile
directive de configuration Apache, ScoreBoardFile
ScriptAlias
directive de configuration Apache, ScriptAlias
scripts
réseau, Scripts réseau
scripts CGI
hors du répertoire ScriptAlias, AddHandler
scripts de contrôle
réseau, Scripts de contrôle d'interface
SCSI, Paramètres généraux et modules
Sendmail, Sendmail
alias, Mascarade
autres sources d'informations, Autres ressources
avec UUCP, Modifications courantes de la configuration de Sendmail
histoire, Histoire
installation par défaut, Installation de Sendmail par défaut
LDAP et, Utilisation de Sendmail avec LDAP
limites, Objectif et limites
mascarade, Mascarade
modifications courantes de la configuration, Modifications courantes de la configuration de Sendmail
objectif, Objectif et limites
spams, Faire cesser les spams avec Sendmail
ServerAdmin
directive de configuration Apache, ServerAdmin
ServerName
directive de configuration Apache, ServerName
ServerRoot
directive de configuration Apache, ServerRoot
ServerSignature
directive de configuration Apache, ServerSignature

ServerType
directives de configuration Apache, ServerType
serveur
XFree86, Le serveur XFree86
serveur proxy, ProxyRequests , Directives cache
serveur sécurisé
arrêt, Démarrage et arrêt de httpd
rechargement, Démarrage et arrêt de httpd
redémarrage, Démarrage et arrêt de httpd
serveur sécurisé</
démarrage, Démarrage et arrêt de httpd
serveur Web non sécurisé
désactivation, Hôte virtuel du serveur Web sécurisé
serveur X
Voir XFree86
serviceconf, Utilitaires de gestion des scripts Init
services
système
configuration au moyen de chkconfig, Utilitaires de gestion des scripts Init
configuration au moyen de ntsysv, Utilitaires de gestion des scripts Init
configuration au moyen de serviceconf, Utilitaires de gestion des scripts Init
SetEnvIf
directive de configuration Apache, SetEnvIf
souris
comment l'utiliser, Utilisation de la souris
SSH, Protocole SSH
couches, Couches de sécurité SSH
exiger, Exiger SSH pour les connexions à distance
fichiers de configuration, Fichiers de configuration d'OpenSSH
introduction, Introduction, Séquence des événements d'une connexion SSH
pourquoi utiliser, Pourquoi utiliser SSH ?
protocole, Protocole SSH, Couches de sécurité SSH
authentification, Authentification
connexion, Connexion
couche transport, Couche transport
retransmission de port, Retransmission de port
retransmission TCP/IP, Beaucoup plus qu'un shell sécurisé
retransmission X11, Retransmission X11
sessions X11, Beaucoup plus qu'un shell sécurisé
standard

groupes, Groupes standard
utilisateurs, Utilisateurs standard
StartServers
directive de configuration Apache, StartServers
startx, Niveau d'exécution 3 : startx
structure
commune, Pourquoi partager une structure commune ?
XFree86, La puissance de X
structure, système de fichiers, Structure d'un système de fichiers
stunnel, Serveurs de messagerie sécurisés
sysctl, Utilisation de sysctl
system
arrêt , Arrêt
système de fichiers
ext2
reconvertir ext3, Revenir à un système de fichiers ext2
ext3, Le système de fichiers ext3, Allocation d'une étiquette avec e2label, Formatage de systèmes de fichiers ext3 avec mkfs
Voir aussi mkfs
convertir ext2, Passer à un système de fichiers ext3
création, Création d'un système de fichiers ext3
fonctions, Fonctions d'ext3
hiérarchie, Aperçu du FHS (Filesystem Hierarchy Standard)
organisation, Organisation de FHS
standard, Organisation de FHS
structure, Structure d'un système de fichiers
virtuels, Un système de fichiers virtuels
étiquetage
Voir e2label
Système X Window
Voir XFree86
client X, La puissance de X
présentation, La puissance de X
serveur X, La puissance de X
SysV init, SysV Init
niveaux d'exécution utilisés par, Niveaux d'exécution d'Init
répertoires utilisés par , SysV Init
sécurité
configuration, Directives de configuration SSL
exécution d'Apache sans, Utilisation d'hôtes virtuels

T

TCP wrappers, TCP Wrappers et xinetd
    avantages de, Avantages de TCP wrappers
    contrôle d'accès, Listes de contrôle d'accès basé sur l'hôte
        caractères spéciaux, Ecriture des règles
        commandes du shell, Ecriture des règles
        motifs, Ecriture des règles
        variables, Ecriture des règles
    fonction, But de TCP Wrappers
    sources d'informations additionnelles, Autres ressources
        documentation installée, Documentation installée
        sites Web utiles, Sites Web utiles
    xinetd, Contrôle d'accès à l'aide de xinetd
Timeout
    directive de configuration Apache, Timeout
touche d'appel système
    activation, /proc/sys
Tripwire, Installation et configuration de Tripwire
    autres ressources, Autres ressources
        documentation déjà installée, Documentation installée
        sites Web utiles, Sites Web utiles
    base de données
        initialisation, Initialisation de la base de données
        mise à jour, Mise à jour de la base de données après une vérification d'intégrité
    composants, Composants de Tripwire
    configuration, Instructions à suivre après l'installation
    emplacements des fichiers, Emplacements des fichiers
    fichier de configuration
        signature, Signature du fichier de configuration
    fichier de politique
        modification, Modification du fichier de politiques
    fichier de politiques
        mise à jour, Mise à jour du fichier de politiques
    fonctions de messagerie électronique, Tripwire et courrier électronique
        test, Envoi d'un message électronique de test
    impression des rapports, Impression des rapports
    installation, Instructions d'installation

installation du RPM, Instructions d'installation du RPM
phrases d'accès
sélection, Sélection des phrases d'accès
twprint et la base de données, Utilisation de twprint pour visualiser la base de données de Tripwire
utilisation, Comment utiliserTripwire
vérification d'intégrité
exécution, Exécution d'une vérification d'intégrité
tune2fs
passer à ext3 avec, Passer à un système de fichiers ext3
revenir à ext2 avec, Revenir à un système de fichiers ext2
vérifications des étiquettes avec, Allocation d'une étiquette avec e2label
TypesConfig
directive de configuration Apache, TypesConfig

U

UseCanonicalName
directive de configuration Apache, UseCanonicalName
User
directive de configuration Apachee, User
UserDir
directive de configuration Apache, UserDir
utilisateurs, Utilisateurs et groupes
répertoires HTML personnels, UserDir
standard, Utilisateurs standard
utilitaire Apache APXS, Ajout de modules au serveur
utilitaires
masqués, Utilitaires masqués

V

VirtualHost
directive de configuration Apache, VirtualHost

W

webmestre

adresse électronique du, ServerAdmin

X

x86
processus de démarrage, Processus de démarrage x86
XFree86, Serveurs et clients X
Xconfigurator, La puissance de X
xfs, Polices
Voir aussi XFree86
xinetd, Contrôle d'accès à l'aide de xinetd
/etc/xinetd.conf, /etc/xinetd.conf
configuration, Fichiers de configuration de xinetd
contrôle d'accès, Contrôle d'accès dans xinetd
liaison, Liaison et réacheminement de port
réacheminement de port, Liaison et réacheminement de port
xinit, Environnements de bureau et gestionnaires de fenêtres
