Red Hat Linux 9

Guide de personnalisation de Red Hat Linux

Red Hat Linux 9: Guide de personnalisation de 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-cg(FR)-9-Print-RHI (2003-02-13T16:45)

Table des matières

Introduction

Bienvenue dans le *Guide de personnalisation de Red Hat Linux*.

Le *Guide de personnalisation de Red Hat Linux* fournit des informations sur la façon de personnaliser votre système Red Hat Linux afin qu'il réponde à vos besoins. Ce manuel vous sera très utile si vous êtes à la recherche d'un guide centré sur les tâches et vous présentant étape par étape la configuration ainsi que la personnalisation de votre système. Il traite de nombreux sujets appropriés pour les utilisateurs intermédiaires, tels que:

- l'installation d'une carte d'interface réseau
- l'exécution d'une installation Kickstart
- la configuration des partitions Samba
- la gestion du logiciel à l'aide de RPM
- l'obtention d'informations sur le système
- la mise à niveau du noyau

Ce manuel est divisé en catégories principales:

- Informations relatives à l'installation
- Informations relatives au réseau
- Configuration du système
- Gestion des paquetages

Ce guide suppose que vous disposez de connaissances élémentaires sur le système Red Hat Linux. Si vous souhaitez des informations sur des sujets plus élémentaires tels que la configuration de votre bureau ou la lecture de CD-ROM audio, veuillez vous reporter au *Guide de démarrage de Red Hat Linux*. Pour de la documentation plus avancée, comme par exemple une présentation du système de fichiers Red Hat Linux, reportez-vous au *Guide de référence de Red Hat Linux*.

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

Remarque

Même si ce manuel contient les informations les plus récentes, nous vous conseillons de prendre connaissance des *Notes de mise à jour de Red Hat Linux*; vous y trouverez peut-être des informations qui n'étaient pas disponibles au moment de l'impression de notre documentation. Vous trouverez ces notes sur le CD-ROM 1 de Red Hat Linux et en ligne à l'adresse:

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

1. Changements apportés à ce manuel

Ce manuel a été conçu afin de couvrir non seulement les nouvelles fonctions de Red Hat Linux 9 mais également des sujets demandés par nos lecteurs. Parmi les changements importants apportés à ce manuel figurent les points suivants:

Implémentation des quotas de disque

Ce nouveau chapitre explique comment configurer et gérer des quotas de disque.

Configuration de l'authentification

Ce nouveau chapitre explique comment utiliser le programme **Outil de configuration d'authentification**.

Configuration des utilisateurs

Ce chapitre été étoffé d'une part afin d'inclure les utilitaires en ligne de commande permettant de gérer les utilisateurs et les groupes et d'autre part, afin de fournir une explication sur ce qui se produit lors de l'ajout d'un nouvel utilisateur au système.

Samba

Ce chapitre été également étoffé afin d'inclure le nouveau programme **Outil de configuration du serveur Samba**.

Configuration de l'imprimante

Ce chapitre a été réécrit pour refléter les changements dûs au nouvel **Outil de configuration de l'imprimante**, au nouveau **Gestionnaire d'impression GNOME** et à la nouvelle fonctionnalité de déplacement par glissement de l'icône sur le panneau.

Kickstart

Les options kickstart ont été mises à jour afin d'inclure une nouvelle option présente dans Red Hat Linux 9; de plus, le chapitre **Configurateur Kickstart** a lui aussi été mis à jour afin d'inclure un certain nombre de nouvelles fonctions.

Configuration réseau

Ce chapitre a été mis à jour pour inclure les possibilités offertes par la nouvelle interface **Outil d'administration de réseau**.

Configuration de l'heure et de la date

Ce chapitre fait désormais partie du *Guide de démarrage de Red Hat Linux*.

2. Conventions de documentation

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

`commande`

Les commandes de Linux (et les commandes d'autres systèmes d'exploitation, lorsqu'elles sont utilisées) sont représentées de cette façon. Ce style vous indique que vous pouvez 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 représentés différemment (comme les noms de fichiers). Dans ces cas là, ils sont considérés comme une partie de la commande; toute la phrase sera donc affichée comme une commande. Par exemple:

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

`nom de fichier`

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

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

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

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

application

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

Utilisez **Mozilla** pour parcourir le Web.

[touche]

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

Pour utiliser l'achèvement [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 est représentée de cette façon. Par exemple:

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

texte trouvé sur une interface GUI

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

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

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

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

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

Si vous devez entrer une séquence de commandes depuis un menu GUI, elles apparaîtront de la façon suivante:

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

bouton sur un écran ou une fenêtre GUI

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

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

`sortie d'ordinateur`

Du texte dans ce style vous indique qu'il est affiché par l'ordinateur en ligne de commande. Vous verrez affiché de cette manière les réponses aux commandes que vous avez tapées, des messages d'erreur et des invites interactives pour vos saisies durant des scripts ou des programmes. Par exemple:

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

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

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

`invite`

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

```
$
```

```
#
```

```
[stephen@maturin stephen]$
```

```
leopard login:
```

`saisie de l'utilisateur`

Le texte que l'utilisateur doit entrer, que ce soit en ligne de commande ou dans une zone de texte sur un écran GUI, est affiché de cette façon. Dans l'exemple suivant, **`text`** est affiché de cette façon:

Pour démarrer votre système dans le programme d'installation en mode 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 éléments seront présentés sous forme de remarques, astuces, avertissements, messages importants ou attention. Par exemple:

Remarque

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

Astuce

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

Important

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

Attention

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

Avertissement

Si vous choisissez de ne pas partitionner manuellement, une installation 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.

3. Prochainement

Le *Guide de personnalisation de Red Hat Linux* s'inscrit dans le cadre de l'engagement de Red Hat d'offrir aux utilisateurs de Red Hat Linux une assistance utile et opportune. Par conséquent, au fur et à mesure du développement de nouvelles applications, ce guide sera mis à jour afin de les inclure.

3.1. Vos commentaires sont importants!

Nous vous invitons vivement à nous écrire si vous trouvez des fautes de frappe dans le *Guide de personnalisation de Red Hat Linux* ou si vous souhaitez nous faire part de vos suggestions pour l'améliorer. Pour ce faire, veuillez nous soumettre un rapport dans Bugzilla (à l'adresse http://www.redhat.com/bugzilla) après le composant `rhl-cg`.

N'oubliez pas d'indiquer les références de ce guide:

```
rhl-cg(FR)-9-Print-RHI (2003-02-13T16:45)
```

afin que nous puissions identifier de suite la version du guide que vous possédez et à laquelle vous faites référence.

Si vous avez des suggestions pour améliorer la documentation fournie, essayez d'être le plus précis possible. Si vous avez trouvé une erreur, indiquez le numéro de section où elle se trouve et ajoutez un extrait du texte qui l'entoure, afin que nous puissions facilement la retrouver.

4. Enregistrez-vous pour bénéficier de l'assistance

Si vous avez une édition de Red Hat Linux 9, n'oubliez pas de vous inscrire pour bénéficier des avantages auxquels vous avez droit en tant que client Red Hat.

Vous aurez droit à certains ou tous les avantages suivants, selon le produit Red Hat Linux que vous avez acheté:

- Support Red Hat — L'équipe d'assistance de Red Hat, Inc. répondra à vos questions sur l'installation.
- Red Hat Network — Mettez facilement à jour vos paquetages et recevez des nouvelles concernant la sécurité, personnalisées à votre système. Visitez http://rhn.redhat.com pour obtenir de plus amples informations.
- *Under the Brim: La E-Newsletter Red Hat* — Recevez chaque mois les dernières nouvelles et informations sur les produits directement de Red Hat.

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

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

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

L'équipe de documentation de Red Hat

I. Systèmes de fichiers

Le *système de fichiers* fait référence aux fichiers et répertoires stockés sur un ordinateur. Un système de fichiers peut se présenter sous différents formats appelés *types de systèmes de fichiers*. Ces formats déterminent la manière selon laquelle les informations sont stockées en tant que fichiers et répertoires. Certains types de systèmes de fichiers stockent des copies redondantes de données, alors que d'autres permettent d'accélérer l'accès au disque dur. Cette section examine les types de systèmes de fichiers suivants: ext3, swap, RAID et LVM. Elle se concentre également sur `parted`, un utilitaire permettant la gestion des partitions.

Table des matières

redhat.

Chapitre 1.

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* avec journalisation.

1.1. 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 dans le cas d'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 9 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, parce que la fonction de journalisation d'ext3 optimise le mouvement de la tête de l'unité de disques durs. Vous pouvez choisir parmi trois modes de journalisation pour optimiser la vitesse, sachant que votre choix entraînera une petite perte en matière d'intégrité des données.

Transition facile

Il est très facile de passer d'ext2 à ext3 et de profiter ce faisant, des avantages d'un système de fichiers à journalisation robuste, sans devoir reformater votre disque. Voir la Section 1.3 pour obtenir de plus amples informations sur la manière d'exécuter cette tâche.

Si vous procédez à une installation complète de Red Hat Linux 9, 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. Consultez l'annexe intitulée *Mise à jour du système courant* dans le *Guide d'installation de Red Hat Linux* pour obtenir de plus amples informations sur le sujet.

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 9, vous pouvez sauter les sections ci-dessous concernant le partitionnement et le formatage et vous rendre directement à la Section 1.3.

1.2. Création d'un système de fichiers ext3

Après l'installation, il est parfois nécessaire de créer un nouveau système de fichiers ext3 . Par exemple, si vous ajoutez un nouveau disque à un système Red Hat Linux vous devez commencer par partitionner le disque et utiliser le système de fichiers ext3.

Pour créer un système de fichiers ext3, suivez les étapes suivantes:

1. Créez la partition à l'aide de la commande `parted` ou `fdisk`.
2. Formatez la partition avec le système de fichiers ext3 à l'aide de `mkfs`.
3. Étiquetez la partition à l'aide de `e2label`.
4. Créez le point de montage.
5. Ajoutez la partition à `/etc/fstab`.

Reportez-vous au Chapitre 5 pour obtenir davantage d'informations sur cette procédure.

1.3. Conversion 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 en tant que 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 que super-utilisateur (root) et tapez:

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

Dans la commande ci-dessus, remplacez /dev/*hdb* par le nom du périphérique et *X* par le numéro de la partition.

Une fois cette modification effectuée, 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 bien le fichier `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.

1.4. Retour à un système de fichiers ext2

Le système ext3 étant relativement nouveau, certains utilitaires ne le prennent pas encore en charge. Par exemple, il sera peut-être nécessaire 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 retourner de façon temporaire à un système de fichiers ext2.

Pour reconvertir une partition, vous devez commencer par démonter la partition. Pour ce faire, tapez les instructions suivantes en étant connecté en tant que super-utilisateur:

```
umount /dev/hdbX
```

Dans la commande ci-dessus, remplacez /dev/*hdb* par le nom du périphérique et *X* par le numéro de la 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 (en tant que super-utilisateur ou root) la commande suivante:

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

Vérifiez que la partition ne comporte pas d'erreurs; pour ce faire, tapez (en tant qu'utilisateur root):

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

Ensuite, montez de nouveau la partition en tant que système de fichiers ext2 en tapant:

```
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 désormais d'une partition ext2.

Si vous changez de façon permanente la partition en partition ext2, n'oubliez pas de mettre à jour le fichier `/etc/fstab`.

Chapitre 2.

Espace de swap

2.1. Qu'est-ce que l'espace de swap?

L'*espace swap* dans Linux est utilisé lorsque la mémoire physique (RAM) est pleine. Si le système a besoin de plus de ressources de mémoire et que la mémoire physique est pleine, les pages inactives de la mémoire sont déplacées dans l'espace de swap. Même si l'espace de swap peut aider les ordinateurs disposant d'une quantité de RAM limitée, il ne faut pas le considérer comme un outil remplaçant la RAM. L'espace de swap est situé sur les disques durs ayant un temps d'accès plus lent que la mémoire physique.

L'espace de swap peut être une partition de swap consacrée (option recommandée), un fichier de swap ou une combinaisons de partitions et de fichiers de swap.

La taille de votre espace de swap devrait être équivalente à deux fois la RAM de votre ordinateur ou 32 Mo (selon la quantité la plus importante), mais ne doit pas déplacer 2048 Mo (ou 2 Go).

2.2. Ajout d'espace de swap

Il est parfois nécessaire d'ajouter de l'espace de swap après l'installation. Par exemple, vous pouvez faire passer votre système de 64 Mo à 128 Mo de RAM, mais la quantité d'espace de swap est seulement de 128 Mo. Le fait d'augmenter la quantité d'espace de swap jusqu'à 256 Mo pourrait être avantageux si vous réalisez des opérations utilisant beaucoup la mémoire ou si vous exécutez des applications nécessitant beaucoup de mémoire.

Deux options s'offrent à vous: vous pouvez soit ajouter une partition de swap, soit ajouter un fichier de swap. Nous vous recommandons d'ajouter une partition de swap, mais cela peut parfois s'avérer difficile si vous ne disposez pas d'espace libre.

Pour ajouter une partition de swap (en supposant que `/dev/hdb2` est la partition que vous voulez ajouter):

1. Le disque dur ne peut pas être en cours d'utilisation (les partitions ne peuvent pas être montées et l'espace de swap ne peut pas être activé). La manière la plus simple de procéder consiste à démarrer votre système en mode de secours. Reportez-vous au Chapitre 9 pour obtenir des instructions sur le démarrage en mode de secours. Lorsque l'on vous demande de monter le système de fichiers, sélectionnez **Ignorer**.

   Si le disque ne contient pas de partitions en cours d'utilisation, vous pouvez également les démonter et désactiver tout l'espace de swap du disque dur à l'aide de la commande `swapoff`.

2. Créez la partition de swap à l'aide de la commande `parted` ou `fdisk`. L'utilisation de `parted` est plus simple que celle de `fdisk`; nous n'expliquerons donc que `parted` Pour créer une partition de swap avec `parted`, suivez les étapes suivantes:

   - À l'invite du shell, en tant qu'utilisateur root, tapez la commande `parted /dev/`*`hdb`*, où /dev/*`hdb`* correspond au nom du périphérique pour le disque dur avec de l'espace libre.
   - À l'invite `(parted)`, tapez **`print`** pour afficher les partitions existantes et la quantité d'espace libre. Les valeurs de début et de fin sont en méga-octets. Déterminez la quantité d'espace libre sur le disque dur et la quantité à allouer à une nouvelle partition de swap.

- À l'invite `(parted)`, tapez **`mkpartfs`** ***`part-type`*** **`linux-swap`** ***`début fin`***, où *`part-type`* peut être primaire, étendue ou logique, où *`début`* correspond au point de départ de la partition et où *`fin`* est la fin de la partition.

  
  Avertissement

  Les modifications prennent effet immédiatement; faites donc bien attention à ce que vous tapez.

- Quittez `parted` en tapant **`quit`**.

3. Maintenant que vous disposez de la partition de swap, utilisez la commande `mkswap` pour la configurer. À l'invite du shell et en étant connecté en tant que super-utilisateur, tapez les instructions suivantes:
   ```
   mkswap /dev/hdb2
   ```
4. Pour activer immédiatement la partition de swap, tapez la commande suivante:
   ```
   swapon /dev/hdb2
   ```
5. Pour l'activer au démarrage, éditez `/etc/fstab` de façon à inclure:
   ```
   /dev/hdb2               swap                    swap    defaults        0 0
   ```
   Au prochain démarrage du système, la nouvelle partition de swap sera activée.
6. Après avoir ajouté et activé la nouvelle partition de swap, vérifiez qu'elle est bien activée en affichant les résultats de la commande `cat /proc/swaps` ou `free`.

Instructions pour ajouter un fichier de swap:

1. Déterminez la taille du nouveau fichier de swap et multipliez-la par 1024 pour déterminer la taille de blocs. Par exemple, la taille de blocs d'un fichier de swap de 64 Mo est 65536.
2. À l'invite du shell, en tant que super-utilisateur, tapez la commande suivante, dans laquelle `count` correspond à la taille de blocs souhaitée:
   ```
   dd if=/dev/zero of=/swapfile bs=1024 count=65536
   ```
3. Configurez le fichier de swap avec la commande:
   ```
   mkswap /swapfile
   ```
4. Pour activer le fichier de swap immédiatement, mais pas automatiquement au démarrage, tapez:
   ```
   swapon /swapfile
   ```
5. Pour l'activer au démarrage, éditez `/etc/fstab` de façon à inclure:
   ```
   /swapfile               swap                    swap    defaults        0 0
   ```
   Au prochain démarrage du système, le nouveau fichier de swap sera activé.
6. Après avoir ajouté et activé le nouveau fichier de swap, vérifiez qu'il est bien activé en affichant les résultats de la commande `cat /proc/swaps` ou `free`.

2.3. Suppression d'espace de swap

Instructions pour supprimer une partition de swap:

1. Le disque dur ne peut pas être en cours d'utilisation (les partitions ne peuvent pas être montées, et l'espace de swap ne peut pas être activé). La manière la plus simple de procéder consiste à démarrer votre système en mode de secours. Reportez-vous au Chapitre 9 pour obtenir des instructions sur le démarrage en mode de secours. Lorsque le système vous demande de monter le système de fichiers, sélectionnez **Ignorer**.

Si le disque ne contient pas de partitions en cours d'utilisation, vous pouvez également les démonter et désactiver tout l'espace de swap du disque dur à l'aide de la commande `swapoff`.

2. À l'invite du shell, en tant que super-utilisateur, exécutez la commande suivante pour vérifier que la partition de swap est bien désactivée (où `/dev/hdb2` correspond à la partition de swap):
   ```
   swapoff /dev/hdb2
   ```
3. Supprimez son entrée dans `/etc/fstab`.
4. Supprimez la partition à l'aide de `parted` ou `fdisk`. Nous ne traiterons ici que de la commande `parted`. Pour supprimer la partition avec `parted`, suivez les étapes suivantes:
   - À l'invite du shell et en tant que super-utilisateur root, tapez la commande `parted /dev/`*`hdb`*, où /dev/*hdb* correspond au nom du périphérique sur lequel figure l'espace de swap à effacer.
   - À l'invite `(parted)`, tapez **`print`** pour afficher les partitions existantes et déterminer le numéro mineur de la partition de swap que vous souhaitez effacer.
   - À l'invite `(parted)`, tapez **`rm`** ***`MINOR`***, où *`MINOR`* correspond au numéro mineur de la partition que vous souhaitez supprimer.

     Avertissement

     Les modifications prennant effet immédiatement, veillez à bien taper le numéro mineur approprié.
   - Tapez **`quit`** pour quitter `parted`.

Instructions pour supprimer un fichier de swap:

1. À l'invite du shell et en tant que super-utilisateur, exécutez la commande suivante pour désactiver le fichier de swap (où `/swapfile` correspond au fichier de swap):
   ```
   swapoff /swapfile
   ```
2. Supprimez son entrée dans `/etc/fstab`.
3. Supprimez le vrai fichier:
   ```
   rm /swapfile
   ```

2.4. Déplacement d'espace de swap

Pour déplacer de l'espace de swap d'un endroit à un autre, suivez d'abord les étapes pour la suppression d'espace de swap, puis suivez celles pour l'ajout d'espace de swap.

redhat.

Chapitre 3.

RAID (Redundant Array of Independent Disks)

3.1. Qu'est-ce que RAID?

L'idée qui a porté à la création de RAID est de rassembler de petites unités de disque économiques dans une matrice, de façon à pouvoir exécuter des opérations ou atteindre des buts redondants qui ne peuvent pas être exécutés ou atteints avec un grand disque coûteux. Cette matrice de disques apparaîtra à l'ordinateur comme une seule unité ou un seul disque de stockage logique.

Avec la méthode RAID, les informations sont dispersées sur plusieurs disques grâce à des techniques comme '*disk striping*' (ou mode d'agrégat par tranche - RAID Niveau 0), '*disk mirroring*' (ou mode miroir - RAID Niveau 1) et '*disk striping with parity*' (ou mode d'agrégat par tranche avec parité répartie - RAID Niveau 5). Vous pouvez ainsi non seulement obtenir la redondance, raccourcir les temps d'attente et/ou augmenter la largeur de bande pour écrire ou lire les disques, mais vous pouvez aussi optimiser la capacité de récupération en cas de blocage du disque dur.

Le concept de base de RAID est que les données peuvent êtres distribuées dans les disques de la matrice de façon logique. Pour cela, les données doivent avant tout être divisées en *morceaux* cohérents (en général 32K ou 64K, mais vous pouvez utiliser d'autres dimensions). Chaque morceau est écrit dans un disque dur RAID, conformément au niveau RAID utilisé. Lorsque les données doivent être lues, le processus est inversé, donnant ainsi l'impression que tous les disques ne sont en réalité qu'un seul grand disque.

3.2. Qui peut utiliser RAID?

Tous ceux qui ont besoin d'avoir de grandes quantités de données à portée de main (par exemple un administrateur système) ont intérêt à utiliser la technologie RAID. Les raisons principales sont les suivantes:

- Plus grande vitesse
- Plus grande capacité de stockage (disque virtuel unique)
- Conséquences moins importantes dans le cas de panne d'un disque

3.3. RAID matériel contre RAID logiciel

Deux approches s'offrent à vous: le RAID matériel et le RAID logiciel.

3.3.1. RAID matériel

Le système basé sur le matériel gère le sous-système indépendamment de l'hôte et ne présente à l'hôte qu'un seul disque par matrice RAID.

Un exemple de périphérique RAID matériel serait celui qui se connecte à un contrôleur SCSI et présente la matrice RAID comme un seul disque SCSI. Un système RAID externe transmet toute "l'intelligence" de gestion de RAID dans un contrôleur placé dans le sous-système extérieur au disque. Tout le sous-système est connecté à l'hôte via un contrôleur SCSI normal et apparaît à l'hôte comme un seul disque.

Les contrôleurs RAID ont également la forme de cartes qui *agissent* comme un contrôleur SCSI dans le système d'exploitation mais gèrent elles-même toutes les communications du disque. Dans ces cas, vous branchez les disques au contrôleur RAID comme vous le feriez avec un contrôleur SCSI, mais ensuite, vous les ajoutez à la configuration du contrôleur RAID et le système d'exploitation ne voit pas la différence.

3.3.2. RAID logiciel

Le RAID logiciel implémente les différents niveaux RAID dans le code du disque du noyau (périphérique de blocs). Cette solution est plus économique, les cartes de contrôleurs de disque ou châssis swap à chaud onéreux [1] n'étant pas nécessaires. Le RAID logiciel fonctionne aussi bien avec les disques IDE économiques qu'avec les disques SCSI. La rapidité des UCT actuels permet au RAID logiciel d'être plus performant que le RAID matériel.

Le pilote MD du noyau Linux est un exemple de solution RAID entièrement indépendante du matériel. Les performances d'une matrice basée sur un logiciel dépendent des performances et de la charge du serveur CPU.

Pour obtenir plus d'informations sur la configuration du RAID logiciel dans le programme d'installation de Red Hat Linux, rendez-vous au Chapitre 10.

Si vous voulez en savoir plus sur les qualités du RAID logiciel, consultez la liste ci-dessous énumérant ses principales fonctionnalités:

- Processus de reconstruction chaîné
- Configuration basée sur le noyau
- Matrices pouvant être transférées d'un ordinateur Linux à l'autre sans être reconstruites
- Matrice reconstruite en arrière-plan à l'aide des ressources de système inactives
- Disque pouvant être permuté à chaud
- Détection automatique d'UCT de façon à profiter de ses optimisations

3.4. Niveaux RAID et support linéaire

RAID supporte de nombreuses configurations, comme les niveaux 0, 1, 4, 5 et linéaire. Ces types de RAID sont définis de la façon suivante:

- *Niveau 0* — le niveau 0 de RAID, souvent appelé "mode d'agrégat par trnache" ou "dépouillement", est une technique de mappage rayé basée sur la performance. Ceci entend que les données stockées dans la matrice sont divisées en bandes et écrites dans les disques de la matrice, permettant ainsi des performances E/S élevées à faible coût, mais ne fournissant pas de redondance. La capacité de stockage de la matrice de niveau 0 est égale à la capacité totale des disques membres d'un RAID matériel ou de la capacité totale des partitions membres d'un RAID logiciel.
- *Niveau 1* — le niveau 1 de RAID, dit mode de "réflexion" ou "miroir", a été utilisé plus longtemps que toutes les autres formes de RAID. Il fournit la redondance en écrivant des données identiques dans chacun des disques membres de la matrice, laissant un exemplaire "reflété" sur chaque disque. La réflexion rencontre un grand succès en raison de sa simplicité et de la grande disponibilité des données. Le niveau 1 opère avec deux disques ou plus qui peuvent utiliser un accès parallèle pour des taux élevés de transferts de données en lecture. Il fonctionne cependant plus souvent de façon indépendante pour fournir un taux de transaction E/S élevé. Le niveau 1 fournit certes une très

1. Un châssis swap à chaud vous permet de supprimer un disque dur sans éteindre votre système.

bonne fiabilité des données et améliore la performance des applications de lecture intensive, mais son prix est relativement élevé. [2] La capacité de stockage de la matrice de niveau 1 est égale à la capacité de l'un des disques durs reflétés dans un RAID matériel ou une des partitions reflétées dans un RAID logiciel.

- *Niveau 4* — Le niveau 4 utilise la parité [3] concentrée sur un seul lecteur de disque pour protéger les données. Il est plus adapté à des transactions E/S qu'à des transferts de grands fichiers. Le disque de parité est un entonnoir, c'est la raison pour laquelle le niveau 4 est rarement utilisé sans des technologies d'appui comme un tampon lecture-écriture. Le niveau 4 de RAID est proposé comme option dans certains plans de partitionnement, mais n'est pas admis comme option dans les installations RAID de Red Hat Linux. [4] La capacité de stockage du RAID matériel niveau 4 est égale à la capacité des disques membres moins la capacité de l'un des disques. La capacité de stockage du RAID logiciel de niveau 4 est égale à la capacité de stockage des partitions membres moins la taille de l'une des partitions, si elles ont toutes la même taille.
- *Niveau 5* — C'est le type de RAID le plus commun. Il distribue de façon égale à certains ou à tous les disques membres de RAID et élimine ainsi le problème d'entonnoir du niveau 4. Le seul encombrement de la performance est le processus de calcul de la parité. Ceci n'est cependant pas un problème très important, grâce aux UCT modernes et au RAID logiciel. Tout comme le niveau 4, le résultat est une performance asymétrique où la lecture est plus rapide que l'écriture. Le niveau 5 est souvent utilisé avec un tampon lecture-écriture de façon à réduire l'asymétrie. La capacité de stockage du RAID matériel de niveau 5 est égale à la capacité des disques membres moins la capacité de l'un des disques. La capacité de stockage du RAID logiciel de niveau 5 est égale à la capacité de stockage des partitions membres moins la taille de l'une des partitions, si elles ont toutes la même taille.
- *RAID linéaire* — Le RAID linéaire est un regroupement simple de disques qui crée un disque virtuel plus grand. Dans le RAID linéaire les morceaux sont placés par séquences d'un disque à l'autre, n'allant au deuxième que lorsque le premier est plein. Ce regroupement n'offre aucune qualité de performance car il est improbable que les opérations E/S soient fractionnées entre les disques membres. Le RAID linéaire ne permet pas la redondance et diminue la fiabilité —— si l'un des disques membres se bloque, toute la matrice est bloquée. La capacité est le total de tous les disques membres.

2. Le prix est élevé car vous écrivez les mêmes informations sur tous les disques de la matrice, ce qui gaspille l'espace disque. Si vous avez par exemple paramétré le RAID niveau 1 de façon à ce que votre partition racine `/` existe sur deux disques de 40G, vous arrivez à un total de 80G, mais ne pouvez en fait accéder qu'à 40G puisque le reste fonctionne comme un miroir des premiers 40G.
3. Les informations de parité sont calculées en fonction du contenu du reste des disques membres de la matrice. Ces informations peuvent être utilisées pour reconstruire les données lorsque l'un des disques de la matrice se bloque. Les données reconstruites peuvent ensuite être utilisées pour satisfaire les demandes E/S faites au disque en panne avant qu'il ne soit remplacé et pour repeupler le disque lorsqu'il aura été remplacé.
4. Le RAID de niveau 4 utilise la même quantité d'espace que le niveau 5, mais ce dernier offre plus de qualités. C'est pourquoi le niveau 4 n'est pas pris en charge.

Chapitre 4.

Gestionnaire de volumes logiques (LVM)

En commençant avec Red Hat Linux 8.0, le Gestionnaire de volumes logiques (ou LVM de l'anglais 'Logical Volume Manager') est disponible pour l'allocation de disques durs.

LVM est une méthode d'allocation d'espace de disque dur en volumes logiques, dont la taille peut facilement être modifiée, au lieu d'utiliser des partitions.

Avec LVM, le disque dur ou l'ensemble de disques durs est alloué à un ou plusieurs *volumes physiques*. Un volume physique ne peut pas s'étendre sur plusieurs disques.

Les volumes physiques sont associés en *groupes de volumes logiques*, à l'exception de la partition `/boot`. La partition `/boot` ne peut pas se trouver sur un groupe de volumes logiques car le chargeur d'amorçage ne peut pas le lire. Si vous souhaitez que la partition root `/` se trouve sur un volume logique, vous devrez créer une partition `/boot` séparée, qui ne fera pas partie d'un groupe de volumes.

Étant donné qu'un volume physique ne peut pas s'étendre sur plusieurs disques, si vous souhaitez tout de même le faire, vous devrez créer un ou plusieurs volumes physiques par disque.

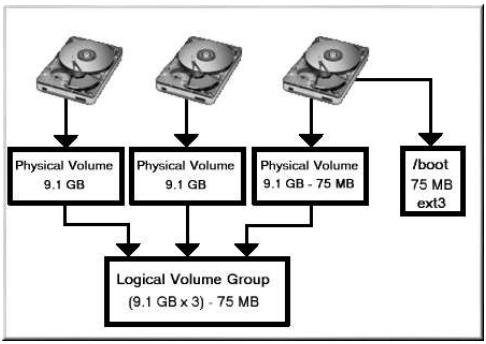

Figure 4-1. Groupe de volumes logiques

Le groupe de volumes logiques est divisé en *volumes logiques*, auxquels sont affectés des points de montage tels que `/home` et `/` ainsi que des types de systèmes de fichiers tels que ext3. Lorsque les "partitions" atteignent leur pleine capacité, l'espace libre du groupe de volumes logiques peut être ajouté au volume logique afin d'accroître la taille de la partition. Lorsqu'un nouveau disque dur est ajouté au système, il peut être ajouté au groupe de volumes logiques et les volumes logiques qui forment les partitions peuvent être étendus.

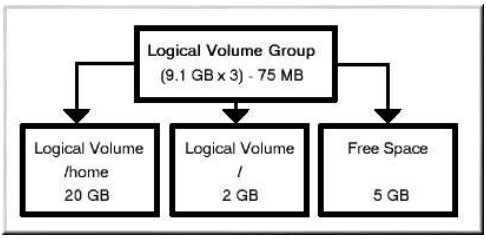

Figure 4-2. Volumes logiques

D'un autre côté, si un système est partitionné avec le système de fichiers ext3, le disque dur est divisé en partitions de tailles définies. Si une partition est pleine, il n'est pas facile d'étendre la taille de la partition. Même si la partition est déplacée sur un autre disque dur, l'espace du disque dur d'origine doit être alloué en tant qu'autre partition ou ne pas être utilisé.

La prise en charge LVM doit être compilée dans le noyau. Le noyau par défaut de Red Hat Linux 9 est compilé avec la prise en charge LVM.

Pour apprendre comment configurer LVM au cours du processus d'installation de Red Hat Linux, reportez-vous au Chapitre 11.

redhat.

Chapitre 5.

Gestion du stockage disque

Après avoir installé votre système Red Hat Linux, vous voudrez peut-être consulter la table des partition existantes, modifier la taille des partitions, supprimer des partitions ou ajouter des partitions à partir d'espace libre ou de disques durs supplémentaires. L'utilitaire `parted` vous permet de réaliser ces tâches. Ce chapitre traite de l'utilisation de `parted` pour la réalisation de tâches systèmes de fichiers. Vous pouvez également utiliser `fdisk` pour réaliser la plupart de ces tâches, à l'exception du redimensionnement de partitions. Pour en savoir plus sur `fdisk`, reportez-vous à la page de manuel ou d'info relative à `fdisk`.

Si vous souhaitez voir ou surveiller l'utilisation d'espace disque du système, reportez-vous à la Section 26.3.

Le paquetage `parted` doit être installé si vous voulez utiliser l'utilitaire `parted`. Pour lancer `parted`, connectez-vous en tant que super-utilisateur et, à l'invite du shell, tapez la commande `parted` *`/dev/hdb`* dans laquelle *`/dev/hdb`* correspond au nom de périphérique du disque que vous souhaitez configurer. Vous verrez apparaître une invite `(parted)`. Tapez `help`pour voir une liste des commandes disponibles.

Si vous voulez créer, supprimer ou redimensionner une partition, le périphérique ne peut pas être en cours d'utilisation (les partitions ne peuvent pas être montées, et l'espace de swap ne peut pas être activé). Le plus simple est de démarrer votre système en mode de secours. Reportez-vous au Chapitre 9 pour obtenir des instructions sur le démarrage en mode de secours. Lorsqu'on vous demandera de monter le système de fichiers, sélectionnez **Ignorer**.

Sinon, si le disque ne contient pas de partitions en cours d'utilisation, vous pouvez les démonter à l'aide de la commande `umount` et désactiver l'espace de swap du disque dur à l'aide de la commande `swapoff`.

Le Tableau 5-1 contient une liste des commandes `parted` communément utilisées. Les sections ci-dessous en détaillent certaines d'entre elles.

Commandes	Description
`check` *`num-mineur`*	Réaliser une vérification simple du système de fichiers
`cp` *`de à`*	Copier un système de fichiers d'une partition à une autre; *`de`* et *`à`* sont les numéros mineurs des partitions
`help`	Afficher une liste des commandes disponibles
`mklabel` *`étiquette`*	Créer une étiquette de disque pour la table des partitions
`mkfs` *`num-mineur type-système-fichiers`*	Créer un système de fichiers de type *`type-système-fichiers`*
`mkpart` *`type-partition type-fs mo-début mo-fin`*	Réaliser une partition sans créer de nouveau système de fichiers
`mkpartfs` *`type-partition type-fs mo-début mo-fin`*	Réaliser une partition et créer le système de fichiers spécifié
`move` *`num-mineur mo-début mo-fin`*	Déplacer la partition

Commandes	Description
`print`	Afficher la table des partitions
`quit`	Quitter `parted`
`resize num-mineur mo-début mo-fin`	Redimensionner la partition de *mo-début* à *mo-fin*
`rm num-mineur`	Supprimer la partition
`select périphérique`	Sélectionner un périphérique différent à configurer
`set num-mineur indicateur état`	Configurer l'indicateur sur une partition; *état* est réglé sur on ou off

Tableau 5-1. Commandes `parted`

5.1. Affichage de la table des partitions

Après avoir lancé `parted`, tapez la commande suivante pour afficher la table des partitions:

```
print
```

Une table similaire à celle reproduite ce-dessous apparaîtra alors:

```
Disk geometry for /dev/hda: 0.000-9765.492 megabytes
Disk label type: msdos
Minor    Start       End     Type      Filesystem  Flags
1          0.031   101.975  primary   ext3        boot
2        101.975   611.850  primary   linux-swap
3        611.851   760.891  primary   ext3
4        760.891  9758.232  extended              lba
5        760.922  9758.232  logical   ext3
```

La première ligne affiche la taille du disque, la deuxième le type d'étiquette du disque et le reste de cette sortie, la table des partitions. Dans cette dernière, le numéro **inférieur** correspond au numéro de la partition. Par exemple, la partition au numéro mineur 1 correspond à `/dev/hda1`. Les valeurs **Démarrer** et **Terminer** sont données en méga-octets. Le **Type** est primaire, étendue ou logique. Le **Système de fichiers** correspond au type de système de fichiers, ext2, ext3, FAT, hfs, jfs, linux-swap, ntfs, reiserfs, hp-ufs, sun-ufs ou xfs. La colonne **Indicateurs** (ou 'Flags' en anglais) répertorie l'ensemble des indicateurs pour la partition. Les indicateurs disponibles sont boot, root, swap, hidden, raid, lvm ou lba.

Astuces

Pour sélectionner un périphérique différent sans avoir à redémarrer `parted`, utilisez la commande `select` suivie du nom du périphérique, comme `/dev/hdb` par exemple. Ensuite, vous pouvez afficher sa table des partitions ou la configurer.

5.2. Création d'une partition

Avertissement

N'essayez pas de créer une partition sur un périphérique en cours d'utilisation.

Avant de créer une partition, démarrez en mode de secours (ou démontez toutes les partitions sur le périphérique et désactivez tout espace de swap du périphérique).

Lancez la commande `parted` dans laquelle /dev/*hda* correspond au périphérique sur lequel la partition doit être créée:

```
parted /dev/hda
```

Affichez la table des partitions en cours pour déterminer si l'espace disponible est suffisant:

```
print
```

S'il n'y a pas suffisamment d'espace disponible, vous pouvez redimensionner une partition existante. Pour de plus amples informations, reportez-vous à la Section 5.4.

5.2.1. Réalisation de la partition

À partir de la table des partitions, déterminez d'une part les points de début et de fin de la nouvelle partition et d'autre part, son type. Vous ne pouvez pas avoir plus de quatre partitions primaires (sans partition étendue) sur un périphérique. Si vous avez besoin de plus de quatre partitions, vous pouvez avoir trois partitions primaires, une partition étendue et de multiples partitions logiques dans la partition étendue. Afin d'obtenir un aperçu des partitions, reportez-vous à l'annexe intitulé *Introduction aux partitions de disque* figurant dans le *Guide d'installation de Red Hat Linux*.

Par exemple, pour créer une partition primaire avec un système de fichiers ext3 de 1024 méga-octets à 2048 méga-octets sur un disque dur, tapez la commande suivante:

```
mkpart primary ext3 1024 2048
```

Astuces

Si, à la place, vous utilisez la commande `mkpartfs`, le système de fichiers sera créé après la partition. Cependant, `parted` ne prend pas en charge la création d'un système de fichiers ext3. Si vous souhaitez créer ce dernier, utilisez `mkpart` et créez le système de fichiers avec la commande `mkfs`, comme nous le décrivons plus bas. Notez que la commande `mkpartfs` fonctionne pour le type de système de fichiers linux-swap.

Les modifications prennent effet dès que vous appuyez sur [Entrée]; vérifiez donc la commande avant de l'exécuter.

Une fois la partition créée, utilisez la commande `print` pour confirmer d'une part qu'elle existe bien dans la table des partitions et d'autre part que le type de partition, le type de système de fichiers et la taille sont bien corrects. Souvenez-vous également du numéro mineur de la nouvelle partition, afin de pouvoir l'étiqueter. Affichez également les résultats de la commande

```
cat /proc/partitions
```

pour vérifier que le noyau reconnaît bien la nouvelle partition.

5.2.2. Formatage de la partition

La partition n'a toujours pas de système de fichiers. Créez-le à l'aide de la commande:

```
/sbin/mkfs -t ext3 /dev/hdb3
```

Avertissement

Le formatage de la partition entraînera un effacement définitif des données présentes sur la partition.

5.2.3. Étiquetage de la partition

Ensuite, étiquetez la partition. Par exemple, si la nouvelle partition est `/dev/hda3` et que vous voulez lui donner l'étiquette `/work`, tapez la commande suivante:

```
e2label /dev/hda3 /work
```

Par défaut, le programme d'installation Red Hat Linux utilise le point de montage de la partition comme étiquette afin de garantir une étiquette unique. Vous pouvez néanmoins utiliser l'étiquette de votre choix.

5.2.4. Création du point de montage

En tant que super-utilisateur, créez le point de montage:

```
mkdir /work
```

5.2.5. Ajout à `/etc/fstab`

En tant que super-utilisateur, éditez le fichier `/etc/fstab` de manière à ce qu'il inclue la nouvelle partition. La nouvelle ligne devrait ressembler à celle reproduite ci-dessous:

```
LABEL=/work           /work                ext3    defaults        1 2
```

La première colonne devrait contenir `LABEL=` suivi de l'étiquette que vous avez donnée à la partition. La deuxième colonne devrait contenir le point de montage de la nouvelle partition, et la colonne suivante le type de système de fichiers (par exemple, ext3 ou swap). Pour en savoir plus sur le format, consultez la page de manuel reltive à la commande `man fstab`.

Si la quatrième colonne contient le mot `defaults`, la partition sera montée au démarrage. Pour monter la partition sans redémarrer le système, tapez la commande suivante en tant que super-utilisateur:

```
mount /work
```

5.3. Suppression d'une partition

 **Avertissement**

N'essayez pas de supprimer une partition d'un périphérique en cours d'utilisation.

Avant de supprimer une partition, démarrez en mode de secours (ou démontez les partitions et désactivez l'espace de swap sur le périphérique).

Lancez la commande `parted`, dans laquelle /dev/*hda* correspond au périphérique sur lequel la partition doit être supprimée:

```
parted /dev/hda
```

Affichez la table des partitions en cours afin de déterminer le numéro mineur de la partition à supprimer:

```
print
```

Supprimez la partition à l'aide de la commande `rm`. Par exemple, pour supprimer la partition portant le numéro mineur 3, tapez:

```
rm 3
```

Les modifications prenant effet dès que vous appuyez sur la touche [Entrée], vérifiez bien la commande avant de l'exécuter.

Une fois que vous avez supprimé la partition, utilisez la commande `print` pour confirmer sa suppression de la table de partition. Affichez également les résultats de la commande:

```
cat /proc/partitions
```

pour vous assurer que le noyau est informé de la suppression de la partition.

La dernière étape consiste à supprimer cette partition du fichier `/etc/fstab`. Trouvez la ligne déclarant la partition supprimée et supprimez-la du fichier.

5.4. Redimensionnement d'une partition

 **Avertissement**

N'essayez pas de redimensionner une partition d'un périphérique en cours d'utilisation.

Avant de redimensionner une partition, démarrez en mode de secours (ou démontez les partitions et désactiver l'espace de swap sur le périphérique).

Lancez la commande `parted`, dans laquelle /dev/*hda* correspond au périphérique sur lequel la partition doit être redimensionnée:

```
parted /dev/hda
```

Affichez la table des partitions en cours afin de déterminer le numéro mineur de la partition à redimensionner, ainsi que les points de début et de fin de la partition:

```
print
```

Avertissement

L'espace utilisé de la partition à redimensionner ne doit pas être plus important que la nouvelle taille.

Pour redimensionner la partition, utilisez la commande `resize` suivie du numéro mineur de la partition, du point de départ et du point de fin en méga-octets. Par exemple:

```
resize 3 1024 2048
```

Une fois le redimensionnement de la partition effectué, utilisez la commande `print` pour confirmer que la partition a été correctement redimensionnée, et que son type et le type de système de fichiers sont corrects.

Après avoir redémarré le système en mode normal, utilisez la commande `df` pour vérifier d'une part que la partition a été montée et d'autre part qu'elle est bien reconnue avec sa nouvelle taille.

redhat.

Chapitre 6.

Implémentation des quotas de disque

Outre le contrôle de l'espace disque utilisé sur un système (reportez-vous à la Section 26.3.1), il est également possible de restreindre l'espace disque en implémentant des quotas de disque. Ce faisant, l'administrateur système est averti avant qu'un utilisateur n'utilise trop d'espace disque ou qu'une partition ne se remplisse trop.

Des quotas de disque peuvent être configurés pour des utilisateurs individuels aussi bien que pour des groupes d'utilisateurs. Ce genre de flexibilité permet de donner à chaque utilisateur un petit quota d'espace disque pour ses fichiers 'personnels' (comme des emails ou des rapports), tout en conservant un quota plus important pour les projets sur lesquels ils travaillent (en supposant que les projets soient donnés à des groupes d'utilisateurs spécifiques).

De plus, les quotas permettent non seulement de contrôler le nombre de blocs de disques utilisés mais permettent également de contrôler le nombre d'inodes. Puisque les inodes servent à contenir des informations relatives aux fichiers, ceci permet aussi le contrôle du nombre de fichiers qui peuvent être créés.

Le RPM de `quota` doit être préalablement installé pour pouvoir implémenter les quotas de disque. Pour obtenir de plus amples informations sur l'installation de paquetages RPM, reportez-vous à la Partie V.

6.1. Configuration des quotas de disque

Pour implémenter les quotas de disque, suivez les étapes ci-dessous:

1. Activez les quotas par système de fichiers en modifiant `/etc/fstab`
2. Remontez le(s) système(s) de fichiers
3. Créez le fichier de quota et créez le tableau d'utilisation du disque dur
4. Assignez des quotas

Chacune de ces étapes est examinée en détails dans les sections suivantes:

6.1.1. Activations des Quotas

En tant que super-utilisateur et en utilisant l'éditeur de texte de votre choix, ajoutez les options `usrquota` et/ou `grpquota` aux systèmes de fichiers nécessitant des quotas:

```
LABEL=/          /              ext3    defaults        1 1
LABEL=/boot      /boot          ext3    defaults        1 2
none             /dev/pts       devpts  gid=5,mode=620  0 0
LABEL=/home      /home          ext3    defaults,usrquota,grpquota 1 2
none             /proc          proc    defaults        0 0
none             /dev/shm       tmpfs   defaults        0 0
/dev/hda2        swap           swap    defaults        0 0
/dev/cdrom       /mnt/cdrom     udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0         /mnt/floppy    auto    noauto,owner,kudzu 0 0
```

Dans cette exemple, des quotas pour l'utilisateur et le groupe d'utilisateurs sont activés dans le système de fichiers `/home`.

6.1.2. Remontage des systèmes de fichiers

Après avoir ajouté les options `userquota` et `grpquota`, remonter chaque système de fichiers dont l'entrée `fstab` a été modifiée. Si le système de fichiers n'est utilisé par aucun processus, utilisez la commande `umount` suivi de `mount` pour monter à nouveau le système de fichiers. Si le système de fichiers est actuellement utilisé, la méthode la plus simple pour remonter le système de fichier consiste à redémarrer le système.

6.1.3. Création de fichiers quota

Après avoir monté à nouveau chaque système de fichiers doté d'un quota, le système est à même de fonctionner en fonction des quotas de disque. Le système de fichiers lui, n'est toutefois pas encore prêt à prendre en charge les quotas. L'étape suivante consiste à exécuter la commande `quotacheck`.

La commande `quotacheck` examine le système de fichiers doté d'un quota et établit un tableau de l'utilisation actuelle du disque pour chaque système de fichiers. Ce tableau est alors utilisé pour mettre à jour la copie de l'utilisation du disque gérée par le système d'exploitation. En même temps, les fichiers quota de disque du système de fichiers sont mis à jour.

Afin de créer des fichiers quota (`aquota.user` et `aquota.group`) sur le système de fichiers, utilisez l'option `-c` de la commande `quotacheck`. Par exemple, si les quotas d'un utilisateur et d'un groupe sont activés dans la partiton `/home`, créez le fichier dans le répertoire `/home`:

```
quotacheck -acug /home
```

L'option `-a` permet de vérifier si tous les systèmes de fichiers montés qui ne sont pas des systèmes de fichiers NFS dans `/etc/mtab` ont des quotas activés. L'option `-c` quant à elle spécifie que les fichiers quota devraient être créés pour chaque système de fichiers avec des quotas activés, alors que l'option `-u` vérifie les quotas utilisateur et l'option `-g` vérifie les quotas groupe.

Si aucune des deux options `-u` ou `-g` n'est spécifiée, seul le fichier quota utilisateur sera créé. Si l'option `-g` est la seule option spécifiée, seul le fichier quota groupe sera créé.

Une fois les fichiers créés, exécutez la commande suivante pour créer le tableau de l'utilisation actuelle du disque pour chaque système de fichiers avec des quotas activés:

```
quotacheck -avug
```

Les options sont utilisées de la manière suivante:

- `a` — vérifie tous les systèmes de fichiers montés localement et dotés de quotas activés
- `v` — affiche des messages de statut (verbose) lors de la vérification du quota
- `u` — vérifie les informations relatives au quota de disque utilisateur
- `g` — vérifie les informations relatives au quota de disque groupe

Une fois les opérations de `quotacheck` terminées, les fichiers quota correspondants aux quotas activés (utilisateur et/ou groupe) sont remplis de données pour chaque système de fichiers doté de quotas activés comme `/home`, par exemple.

6.1.4. Attribution de quotas par utilisateur

La dernière étape consiste à attribuer les quotas de disque à l'aide de la commande `edquota`.

Pour permettre la configuration d'un quota pour un utilisateur, à l'invite du shell, exécutez la commande suivante en étant connecté en tant que super-utilisateur:

```
edquota nom d'utilisateur
```

Effectuez ces étapes pour chaque utilisateur auquel vous souhaitez attribuer un quota. Par exemple, si un quota est activé dans `/etc/fstab` pour la partition `/home` (`/dev/hda3`) et que la commande `edquota testuser` est exécutée, l'extrait suivant apparaîtra dans l'éditeur de texte configuré par défaut pour le système:

```
Disk quotas for user testuser (uid 501):
  Filesystem                   blocks       soft       hard     inodes     soft     hard
  /dev/hda3                    440436          0          0      37418        0        0
```

Remarque

L'éditeur de texte défini par la variable de l'environnement EDITOR est utilisée par `edquota`. Pour changer d'éditeur, précisez dans la variable de l'environnement EDITOR le chemin d'accès complet de l'éditeur de votre choix.

La première colonne correspond au nom du système de fichiers doté d'un quota activé. La deuxième colonne elle, affiche le nombre de blocs actuellement employés par un utilisateur. Les deux colonnes suivantes sont utilisées pour déterminer les limites douces (soft limits) et dures (hard limits) des blocs correspondant à l'utilisateur du système de fichiers. La colonne `inodes` affiche le nombre d'inodes actuellement employées par l'utilisateur. Les deux dernières colonnes servent à déterminer les limites douces et dures des inodes de l'utilisateur sur un système de fichiers.

Une limite dure correspond à la quantité maximale d'espace disque qu'un utilisateur ou groupe peut employer. Une fois la limite atteinte, aucun espace supplémentaire ne peut être utilisé.

La limite douce définit la quantité maximale d'espace disque pouvant être utilisée. Néanmoins, contrairement à la limite dure, la limite douce peut être dépassée pendant un certain temps. On se réfère à cette durée sous le terme *période de grâce*. Cette dernière peut être exprimée en secondes, minutes, heures, jours, semaines ou mois.

Si toute valeur correspond à 0, cette limite n'est pas déterminée. Dans l'éditeur de texte, changez les limites voulues. Par exemple,

```
Disk quotas for user testuser (uid 501):
  Filesystem                   blocks       soft       hard     inodes     soft     hard
  /dev/hda3                    440436     500000     550000      37418        0        0
```

Afin de vérifier que le quota pour l'utilisateur a bien été établi, utilisez la commande suivante:

```
quota testuser
```

6.1.5. Attribution de quotas par groupe

Des quotas peuvent également être attribués groupe par groupe. Par exemple, pour établir le quota groupe pour le groupe `devel`, utilisez la commande (le groupe doit bien sûr exister avant de déterminer un quota pour ce groupe):

```
edquota -g devel
```

Cette commande permet d'afficher dans l'éditeur de texte, le quota actuel pour le groupe:

```
Disk quotas for group devel (gid 505):
  Filesystem                   blocks       soft       hard     inodes     soft     hard
  /dev/hda3                    440400          0          0      37418        0        0
```

Modifiez les limites, enregistrez le fichier et configurez ensuite le quota.

Pour vérifier que le quota groupe a bien été établi, utilisez la commande suivante:

```
quota -g devel
```

6.1.6. Attribution de quotas par système de fichiers

Pour attribuer des quotas basés sur chaque système de fichiers activé pour l'utilisation de quotas, utilisez la commande suivante:

```
edquota -t
```

Comme les autres commandes `edquota`, celle-ci ouvre le quota actuel du système de fichiers dans l'éditeur de texte:

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
  Filesystem             Block grace period     Inode grace period
  /dev/hda3                     7days                  7days
```

Changez la période de grâce du bloc (block) ou la période de grâce de l'inode, enregistrez les changements dans le fichier et quittez l'éditeur de texte.

6.2. Gestion des quotas de disque

Si des quotas sont utilisés, ils doivent être maintenus — essentiellement grâce à un contrôle afin de déterminer si les quotas sont dépassés et afin que s'assurer que ces derniers ont exacts. Bien sûr, si des utilisateurs dépassent souvent leurs quotas ou atteignent leurs limites douces en permanence, un administrateur système doit prendre les décisions appropriées en fonction du type d'utilisateur et de la quantité d'espace disque influençant leur travail. L'administrateur peut soit aider l'utilisateur à déterminer comment utiliser moins d'espace disque soit augmenter le quota de disque de l'utilisateur si nécessaire.

6.2.1. Rapport sur les quotas de disque

Un rapport sur l'utilisation du disque peut être établi en exécutant l'utilitaire `repquota`. La commande `repquota /home` par exemple, fournit la sortie suivante:

```
*** Report for user quotas on device /dev/hda3
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root      --      36       0       0              4     0     0
tfox      --     540       0       0            125     0     0
testuser  --  440400  500000  550000          37418     0     0
```

Pour afficher un rapport sur l'utilisation du disque pour tous les systèmes de fichiers dotés de quotas activés, utilisez la commande ci-dessous:

```
repquota -a
```

Bien que le rapport soit d'une lecture facile, un certain nombre de points doivent être clarifiés. Les signes `--` affichés après chaque utilisateur permettent de déterminer rapidement si les limites du bloc

ou de l'inode ont été dépassées. Si l'une ou l'autre des limites douces a été dépassée, un signe + apparaîtra au lieu du signe –; le premier signe – correspond à la limite du bloc et le second signe à la limite de l'inode.

Les colonnes intitulées `grace` sont normalement vierges. Toutefois, si la limite douce a été dépassée, la colonne contiendra une indication de temps égale à la durée restante de la période de grâce. Si la période de grâce est dépassée, la durée sera remplacée par `none`, signifiant que la période de grâce a expiré.

6.2.2. Maintien de quotas justes

Dès lors qu'un système de fichiers n'est pas démonté correctement (suite à un plantage du système par exemple), il est nécessaire d'exécuter la commande `quotacheck`. Ceci étant, vous pouvez exécuter `quotacheck` de façon régulière, même si le système n'a pas planté. L'exécution périodique de cette commande permet de maintenir la justesse des quotas (les options décrites sont décrites dans la Section 6.1.1):

```
quotacheck -avug
```

Pour faciliter l'exécution périodique de la commande ci-dessus, utilisez `cron`. En étant connecté en tant que super-utilisateur, vous pouvez soit utiliser la commande `crontab -e` pour organiser une exécution périodique de `quotacheck`, soit placer un script exécutant `quotacheck` dans l'un des répertoires suivants (en utilisant l'intervalle qui correspond le mieux à vos besoins):

- `/etc/cron.hourly`
- `/etc/cron.daily`
- `/etc/cron.weekly`
- `/etc/cron.monthly`

Vous obtiendrez les statistiques les plus justes lorsque le ou les systèmes de fichiers ne sont pas utilisés de façon active. Par conséquent, l'exécution de la tâche cron devrait être prévue pendant un moment où le ou les systèmes de fichiers sont le moins utilisés. Si ce moment est différent selon les systèmes de fichiers dotés de quotas, exécutez `quotacheck` pour chacun d'eux à différents moments et avec de multiples tâches cron.

Reportez-vous au Chapitre 28 pour obtenir de plus amples informations sur la configuration de `cron`.

6.2.3. Activation et désactivation

Il est possible de désactiver des quotas sans pour autant devoir leur donner une valeur équivalente à 0. Pour désactiver tout les quotas utilisateur et groupe, utilisez la commande suivante:

```
quotaoff -vaug
```

Si aucune des options `-u` ou `-g` n'est spécifiée, seuls les quotas utilisateur seront désactivés. En revanche si seule l'option `-g` est spécifiée, seuls les quotas groupe seront désactivés.

Pour réactiver des quotas, utilisez la commande `quotaon` avec les mêmes options.

Par exemple, pour activer les quotas utilisateur et groupe pour tous les systèmes de fichiers, vous utiliserez la commande suivante:

```
quotaon -vaug
```

Pour activer les quotas pour un système de fichiers spécifique, comme par exemple `/home`, vous utiliserez la commande suivante:

```
quotaon -vug /home
```

Si aucune des options `-u` ou `-g` n'est spécifiée, seuls les quotas utilisateurs sont activés. Si seule l'option `-g` est spécifiée, seuls les quotas groupe sont activés.

6.3. Ressources supplémentaires

Pour des informations supplémentaires au sujet des quotas de disque, consultez les ressources ci-dessous.

6.3.1. Documentation installée

- Les page de manuel relatives à `quotacheck`, `edquota`, `repquota`, `quota`, `quotaon` et `quotaoff`

6.3.2. Livres sur le sujet

- *Guide d'administration système de Red Hat Linux* — Disponible à l'adresse suivante http://www.redhat.com/docs et sur le CD-ROM de documentation. Ce manuel contient des informations complémentaires sur la gestion du stockage (y compris les quotas de disque) particulièrement utiles pour les nouveaux administrateur de système Red Hat Linux.

II. Informations relatives à l'installation

Le *Guide d'installation de Red Hat Linux* se concentre sur l'installation de Red Hat Linux et sur certaines solutions élémentaires aux problèmes pouvant survenir après l'installation. Ceci étant, des options d'installation avancées sont également couvertes dans ce guide. Cette section offre des instructions pour *kickstart* (une méthode d'installation automatisée) et examine les modes de secours du système (manière permettant de démarrer votre système s'il ne s'amorce pas au niveau d'exécution normal), la manière de configurer RAID et LVM lors de l'installation. Utilisez cette section conjointement avec le *Guide d'installation de Red Hat Linux* pour effectuer toute tâche d'installation avancée mentionnée ici.

Table des matières

redhat.

Chapitre 7.

Installations kickstart

7.1. Qu'est-ce qu'une installation kickstart?

De nombreux administrateurs préfèrent utiliser une méthode automatisée pour installer Red Hat Linux sur leur ordinateur. Pour répondre à cette nécessité, Red Hat a créé la méthode d'installation kickstart. Grâce à cette méthode, un administrateur système peut créer un simple fichier contenant les réponses à toutes les questions posées durant l'installation normale de Red Hat Linux.

Les fichiers kickstart peuvent être conservés sur un simple système serveur et lus par les ordinateurs durant l'installation. Cette méthode d'installation peut prendre en charge l'utilisation d'un simple fichier kickstart pour installer Red Hat Linux sur plusieurs ordinateurs, ce qui en fait l'outil idéal pour les administrateurs système et réseau.

Kickstart vous permet d'automatiser une installation de Red Hat Linux.

7.2. Comment effectuer une installation kickstart?

Il est possible d'effectuer des installations kickstart à l'aide d'un CD-ROM local, d'un disque dur local ou encore via NFS, FTP ou HTTP.

Pour utiliser le mode kickstart, vous devez:

1. Créer un fichier kickstart;
2. Placer le fichier kickstart sur une disquette de démarrage ou sur le réseau;
3. Rendre l'arborescence d'installation disponible;
4. Démarrer l'installation kickstart.

Ce chapitre détaille ces étapes.

7.3. Création du fichier kickstart

Le fichier kickstart est un simple fichier texte contenant une liste d'éléments dont chacun est identifié par un mot-clé. Vous pouvez le créer en éditant une copie du fichier `sample.ks` contenu dans le répertoire `RH-DOCS` du CD-ROM de documentation de Red Hat Linux ou en utilisant l'application **Configurateur Kickstart**; vous pouvez également le créer de toutes pièces. Le programme d'installation de Red Hat Linux crée également un exemple de fichier kickstart à partir des options sélectionnées lors de l'installation. Il est enregistré dans le fichier `/root/anaconda-ks.cfg`. Vous devriez pouvoir le modifier à l'aide de n'importe quel éditeur ou traitement de texte acceptant l'enregistrement des fichiers au format texte ASCII.

Voici, pour commencer, quelques règles de base à garder à l'esprit lors de la création de votre fichier kickstart:

- Les sections doivent être indiquées *dans l'ordre*. Sauf spécification contraire, les éléments contenus dans les sections n'ont pas à être placés dans un ordre spécifique. Tel est l'ordre de la section:
  - La section commandes — la Section 7.4 contient une liste des options de kickstart. Vous devez fournir les options requises.

- La section `%packages` — Pour plus d'informations, reportez-vous à la Section 7.5.
- Les sections `%pre` et `%post` — Ces deux sections n'ont pas à respecter un ordre précis et ne sont pas obligatoires. Pour plus d'informations, reportez-vous à la Section 7.6 ainsi qu'à la Section 7.7.

- Les éléments qui ne sont pas obligatoires peuvent être omis.
- L'omission d'un élément obligatoire amène le programme d'installation à demander à l'utilisateur une réponse pour cet élément, exactement comme cela se passerait lors d'une installation normale. Une fois la réponse fournie, l'installation continue sans assistance (sauf s'il manque un autre élément).
- Les lignes commençant par le signe dièse (#) sont traitées comme des commentaires et ignorées.
- Pour les *mises à niveau* de kickstart, les éléments suivants sont requis:
  - Langue
  - Prise en charge de la langue
  - Méthode d'installation
  - Spécification du périphérique (si un périphérique est nécessaire pour exécuter l'installation)
  - Configuration du clavier
  - Mot-clé `upgrade`
  - Configuration du chargeur d'amorçage

  Si d'autres éléments sont spécifiés pour une mise à niveau, ces éléments sont ignorés (ceci inclut la sélection de paquetages).

7.4. Options de kickstart

Les options suivantes peuvent être regroupées dans un fichier kickstart. Si vous préférez utiliser une interface graphique pour la création du fichier kickstart, vous pouvez utiliser l'application **Configurateur Kickstart**. Consultez le Chapitre 8 pour obtenir de plus amples informations.

Remarque

Si l'option est suivie du signe égal (=), vous devez indiquer une valeur après ce signe. Dans les exemples de commandes, les options entre parenthèses ([]) sont des arguments facultatifs pour la commande.

`autostep` (facultatif)

Cette commande est semblable à `interactive`, mais elle passe à l'écran suivant à votre place. Cette commande est surtout utilisée pour le débogage.

`auth` ou `authconfig` (obligatoire)

Définit les options d'authentification pour le système. Cette commande est similaire à la commande `authconfig` qui peut être exécutée après l'installation. Par défaut, les mots de passe sont normalement cryptés et non masqués.

`--enablemd5`

Utilise le cryptage md5 pour les mots de passe utilisateur.

`--enablenis`

Active la prise en charge NIS. Par défaut, `--enablenis` utilise tout domaine trouvé sur le réseau. Un domaine doit presque toujours être défini manuellement à l'aide de l'option `--nisdomain=`.

`--nisdomain=`

Nom de domaine NIS à utiliser pour les services NIS.

`--nisserver=`

Serveur à utiliser pour les services NIS (diffusions par défaut).

`--useshadow` ou `--enableshadow`

Utilise des mots de passe masqués.

`--enableldap`

Active la prise en charge LDAP dans `/etc/nsswitch.conf`, en permettant à votre système de récupérer des informations sur les utilisateurs (UID, répertoires personnels, shells, etc.) dans un répertoire LDAP. Vous devez installer le paquetage `nss_ldap` pour utiliser cette option. Vous devez également spécifier un serveur et un DN de base avec `--ldapserver=` et `--ldapbasedn=`.

`--enableldapauth`

Utilise LDAP comme méthode d'authentification. Ceci active le module `pam_ldap` pour l'authentification et le changement de mots de passe à l'aide d'un répertoire LDAP. Cette option ne peut être utilisée que si le paquetage `nss_ldap` est installé. Vous devez également spécifier un serveur et un nom distinct ou DN (de l'anglais 'Distinguished Name') de base avec `--ldapserver=` et `--ldapbasedn=`.

`--ldapserver=`

Si vous avez spécifié `--enableldap` ou `--enableldapauth`, utilisez cette option pour préciser le nom du serveur LDAP à utiliser. Cette option est définie dans le fichier `/etc/ldap.conf`.

`--ldapbasedn=`

Si vous avez spécifié `--enableldap` ou `--enableldapauth`, utilisez cette option pour préciser le DN dans l'arborescence de votre répertoire LDAP (emplacement où sont stockées les informations utilisateur). Cette option est définie dans le fichier `/etc/ldap.conf`.

`--enableldaptls`

Utilise les recherches TLS ('Transport Layer Security'). Cette option permet à LDAP d'envoyer des noms d'utilisateur ainsi que des mots de passe cryptés à un serveur LDAP avant l'authentification.

`--enablekrb5`

Utilise Kerberos 5 pour authentifier des utilisateurs. Kerberos lui-même n'a aucune notion des répertoires personnels, des UID ou des shells. Si vous l'activez, vous devez donc faire connaître les comptes des utilisateurs à ce poste de travail en activant LDAP, NIS ou Hesiod ou en utilisant la commande `/usr/sbin/useradd`. Pour pouvoir utiliser cette option, le paquetage `pam_krb5` doit avoir été installé.

`--krb5realm=`

La partition de Kerberos 5 à laquelle appartient votre poste de travail.

`--krb5kdc=`

Le KDC servant les requêtes pour la partition. Si votre partition comporte plusieurs KDC, séparez leurs noms par des virgules (,).

`--krb5adminserver=`

Le KDC de votre partition qui exécute également kadmind. Ce serveur, qui ne peut être exécuté que sur le KDC maître si vous avez plusieurs KDC, gère les changements de mot de passe et autres requêtes administratives.

`--enablehesiod`

Activer la prise en charge Hesiod pour rechercher les répertoires personnels de l'utilisateur, les UID et les shells. Vous trouverez plus d'informations sur la configuration et l'utilisation d'Hesiod sur votre réseau dans `/usr/share/doc/glibc-2.x.x/README.hesiod`, inclus dans le paquetage `glibc`. Hesiod est une extension de DNS qui utilise des enregistrements DNS pour stocker des informations sur des utilisateurs, des groupes et divers autres éléments.

`--hesiodlhs`

Option Hesiod LHS ('left-hand side', côté gauche) définie dans `/etc/hesiod.conf`. Cette option est utilisée par la bibliothèque Hesiod pour déterminer le nom permettant de rechercher un DNS en cas de recherche d'informations, comme l'utilisation d'un DN de base par LDAP.

`--hesiodrhs`

Option Hesiod RHS ('right-hand side', côté droit), définie dans `/etc/hesiod.conf`. Cette option est utilisée par la bibliothèque Hesiod pour déterminer le nom permettant de rechercher un DNS en cas de recherche d'informations, comme l'utilisation d'un DN de base par LDAP.

Astuce

Pour rechercher 'jim' dans les informations utilisateur, la bibliothèque Hesiod recherche *jim.passwd<LHS><RHS>*, ce qui devrait générer un enregistrement TXT ressemblant à son entrée passwd (`jim:*:501:501:Jungle Jim:/home/jim:/bin/bash`). Pour les groupes, la situation est identique; vous devez juste utiliser *jim.group<LHS><RHS>*.

La recherche d'utilisateurs ainsi que de groupes par numéro se gère en faisant de "501.uid" un CNAME pour "jim.passwd" et de "501.gid" un CNAME pour "jim.group". Veuillez noter que LHS et RHS ne sont pas précédés d'un point ([.]) lorsque la bibliothèque détermine le nom à rechercher; LHS et RHS commencent généralement par un point.

`--enablesmbauth`

Active l'authentification des utilisateurs sur un serveur SMB (le plus souvent un serveur Samba ou Windows). La prise en charge de l'authentification SMB ne connaît pas les répertoires personnels, les UID ou les shells. Ainsi, si vous l'activez, vous devrez faire connaître les comptes des utilisateurs au poste de travail en activant LDAP, NIS ou Hesiod ou en utilisant la commande `/usr/sbin/useradd`. Pour pouvoir utiliser cette option, le paquetage `pam_smb` doit être installé sur votre système.

`--smbservers=`

Le nom du ou des serveurs à utiliser pour l'authentification SMB. Si vous devez spécifier plusieurs serveurs, séparez-les par des virgules (,).

`--smbworkgroup=`

Le nom du groupe de travail pour les serveurs SMB.

`--enablecache`

Active le service `nscd`. Ce service met en cache les informations relatives aux utilisateurs, aux groupes ainsi qu'à d'autres types d'informations. Cette mise en cache est particulièrement utile si vous choisissez de diffuser sur votre réseau des informations sur des groupes et des utilisateurs en utilisant NIS, LDAP ou Hesiod.

`bootloader` (obligatoire)

Spécifie la façon dont le chargeur d'amorçage doit être installé et s'il est préférable de choisir LILO ou GRUB. Cette option est requise pour les installations ainsi que pour les mises à niveau. Pour les mises à niveau, si `--useLilo` n'est pas spécifié et que LILO est le chargeur d'amorçage actuel, ce dernier sera changé en GRUB. Pour conserver LILO dans les mises à jour, utilisez `bootloader --upgrade`.

`--append=`

Spécifie les paramètres du noyau. Pour préciser des paramètres multiples, séparez-les par des espaces. Par exemple:

```
bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"
```

`--location=`

Spécifie l'emplacement de l'enregistrement d'amorçage. Les valeurs possibles sont: `mbr` (par défaut), `partition` (installe le chargeur d'amorçage dans le premier secteur de la partition qui contient le noyau) ou `none` (n'installe pas de chargeur d'amorçage).

`--password=`

Si vous utilisez GRUB, configurez le mot de passe du chargeur d'amorçage GRUB sur celui spécifié avec cette option. Cela vous permet de limiter l'accès au shell de GRUB où des options arbitraires de noyau peuvent être transmises.

`--md5pass=`

Si vous utilisez GRUB, cette commande ressemble à `--password=` si ce n'est que le mot de passe doit déjà être crypté.

`--useLilo`

Utilise LILO au lieu de GRUB comme chargeur d'amorçage.

`--linear`

Si vous avez choisi LILO, utilisez l'option `linear`. Ceci ne sert qu'à une compatibilité en amont (et linéaire est maintenant utilisé par défaut).

`--nolinear`

Si vous avez choisi LILO, utilisez l'option `nolinear`; linéaire est l'option par défaut.

`--lba32`

Si vous avez choisi LILO, cette commande force l'utilisation du mode lba32 au lieu de la détection automatique.

`--upgrade`

Met à niveau la configuration actuelle du chargeur d'amorçage tout en conservant les anciennes entrées. Cette option n'est disponible que pour les mises à jour.

`clearpart` (facultatif)

Supprime des partitions du système, avant d'en créer de nouvelles. Par défaut, aucune partition n'est supprimée.

Remarque

Si `clearpart` est utilisée, la commande `--onpart` ne peut pas être utilisée sur une partition logique.

`--linux`

Supprime toutes les partitions Linux.

`--all`

Supprime toutes les partitions du système.

`--drives=`

Spécifie les disques dans lesquels des partitions doivent être supprimées. Par exemple, la commande suivante permet de supprimer les partitions des deux premiers disques sur le contrôleur IDE primaire:

```
clearpart --drives hda,hdb
```

`--initlabel`

Initialise l'étiquette de disque selon la configuration par défaut de votre architecture (par exemple `msdos` pour x86 et `gpt` pour Itanium). Cette commande est utile pour éviter que le programme d'installation ne demande s'il doit initialiser l'étiquette de disque lorsqu'il installe un nouveau disque dur.

`périphérique` (facultatif)

Sur la plupart des systèmes PCI, le programme d'installation détecte automatiquement les cartes Ethernet et SCSI. Sur des systèmes plus anciens et certains systèmes PCI, kickstart a cependant besoin d'une indication pour trouver les périphériques appropriés. La commande `périphérique` indique au programme d'installer des modules supplémentaires. Elle se présente sous le format suivant:

```
device <type>
<Nom-module>
--opts=<options>
```

<type>

Remplacez par `scsi` ou `eth`

`<Nom-module>`

Remplacez par le nom du module de noyau qui doit être installé.

`--opts=`

Options à transmettre au module de noyau. Veuillez noter que plusieurs options peuvent être transmises si elles sont mises entre guillemets, comme par exemple:
`--opts="aic152x=0x340 io=11"`

`deviceprobe` (facultatif)

Force une détection du bus PCI et charge des modules pour tous les périphériques trouvés lorsqu'un module est disponible.

`driverdisk` (facultatif)

Les disquettes de pilotes peuvent être utilisées lors d'installations kickstart. Vous devrez copier le contenu de la disquette de pilote dans le répertoire racine d'une partition sur le disque dur du système. Vous devrez ensuite utiliser la commande `driverdisk` afin d'indiquer au programme d'installation où rechercher la disquette de pilotes.
`driverdisk <partition>`
`[--type=<fstype>]`

`<partition>`

Partition qui contient la disquette de pilotes.

`--type=`

Type de système de fichiers (par exemple, vfat ou ext2).

`firewall` (facultatif)

Cette option correspond à l'écran **Configuration du pare-feu** du programme d'installation:
`firewall <niveau-de-sécurité> [--trust=]`
`<entrant> [--port=]`

`<niveau-de-sécurité>`

Remplacez par l'un des niveaux de sécurité suivants:

- `--high` (élevé)
- `--medium` (moyen)
- `--disabled` (désactivé)

`--trust=`

Si vous ajoutez un périphérique à cet endroit (eth0, par exemple), vous permettez au trafic en provenance de ce périphérique de traverser le pare-feu. Pour ajouter plusieurs périphériques à la liste, suivez le modèle suivant: `--trust eth0 --trust eth1`. Ne mettez PAS de virgule entre les périphériques énumérés, comme par exemple `--trust eth0, eth1`.

`<entrant>`

Remplacez par aucun élément ou par plusieurs des éléments ci-dessous pour permettre aux services spécifiés de traverser le pare-feu.

- `--dhcp`
- `--ssh`
- `--telnet`
- `--smtp`
- `--http`
- `--ftp`

`--port=`

Vous pouvez spécifier les ports par lesquels il est possible de traverser le pare-feu en utilisant le format port:protocole. Par exemple, pour permettre l'accès IMAP au travers de votre pare-feu, indiquez `imap:tcp`. Vous pouvez également spécifier les ports numériques de façon explicite; par exemple, pour autoriser les paquets UDP sur le port 1234, indiquez `1234:udp`. Pour spécifier plusieurs ports, séparez-les par une virgule (,).

`install` (facultatif)

Indique au système d'installer un nouveau système au lieu de mettre à niveau un système existant. Il s'agit du mode par défaut. Pour une installation, vous devez spécifier le type d'installation parmi les options suivantes: `cdrom`, `harddrive` (Disque dur), `nfs` ou `url` (pour des installations ftp ou http). La commande `install` et la commande relative à la méthode d'installation doivent se trouver sur des lignes différentes.

`cdrom`

Effectue l'installation à partir du premier lecteur de CD-ROM du système.

`harddrive`

Effectue l'installation à partir d'une arborescence Red Hat sur un disque local, qui doit être de type vfat ou ext2.

- `--partition=`

  Partition à partir de laquelle l'installation doit être exécutée (sdb2, par exemple).

- `--dir=`

  Répertoire contenant le répertoire `RedHat` de l'arborescence d'installation.

Par exemple:

```
harddrive --partition=hdb2 --dir=/tmp/install-tree
```

`nfs`

Effectue l'installation à partir du serveur NFS spécifié.

- `--server=`

  Serveur à partir duquel l'installation doit être effectuée (nom d'hôte ou IP).

- `--dir=`

  Répertoire contenant le répertoire `RedHat` de l'arborescence d'installation.

Par exemple:

```
nfs --server=nfsserver.example.com --dir=/tmp/install-tree
```

`url`

Effectue l'installation à partir d'une arborescence d'installation sur un serveur distant via FTP ou HTTP.

Par exemple:

```
url --url
http://<serveur>/<dir>
```

ou:

```
url --url
ftp://<nom-utilisateur>:<mot-de-passe>@<serveur>/<dir>
```

`interactive` (facultatif)

Utilise les informations fournies dans le fichier kickstart lors de l'installation, mais permet d'examiner et de modifier les valeurs fournies. Chaque écran du programme d'installation vous sera présenté avec les valeurs du fichier kickstart. Acceptez les valeurs en cliquant sur **Suivant** ou modifiez-les et cliquez sur **Suivant** pour continuer. Reportez-vous également à `autostep`.

`keyboard` (obligatoire)

Définit le type de clavier du système. Ci-dessous figure la liste des claviers disponibles sur les ordinateurs i386, Itanium et Alpha:

```
be-latin1, bg, br-abnt2, cf, cz-lat2, cz-us-qwertz, de,
de-latin1, de-latin1-nodeadkeys, dk, dk-latin1, dvorak, es, et,
fi, fi-latin1, fr, fr-latin0, fr-latin1, fr-pc, fr_CH, fr_CH-latin1,
gr, hu, hu101, is-latin1, it, it-ibm, it2, jp106, la-latin1, mk-utf,
no, no-latin1, pl, pt-latin1, ro_win, ru, ru-cp1251, ru-ms, ru1, ru2,
ru_win, se-latin1, sg, sg-latin1, sk-qwerty, slovene, speakup,
speakup-lt, sv-latin1, sg, sg-latin1, sk-querty, slovene, trq, ua,
uk, us, us-acentos
```

Le fichier `/usr/lib/python2.2/site-packages/rhpl/keyboard_models.py` contient également cette liste et fait partie du paquetage `rhpl`.

`lang` (obligatoire)

Définit la langue à utiliser durant l'installation. Par exemple, si vous souhaitez choisir l'anglais, le fichier kickstart doit contenir la ligne suivante:

```
lang en_US
```

Le fichier `/usr/share/redhat-config-language/locale-list` fournit une liste des codes valides pour les différentes langues dans la première colonne de chaque ligne et fait partie du paquetage `redhat-config-languages`.

`langsupport` (obligatoire)

Définit la ou les langue(s) à installer sur le système. Les codes utilisés avec `lang` peuvent également être utilisés avec `langsupport`.

Si vous souhaitez installer une seule langue, spécifiez-la. Par exemple, pour installer et utiliser le français, `fr_FR`, la ligne suivante est nécessaire:

```
langsupport fr_FR
```

`--default=`

Si vous souhaitez installer la prise en charge de plusieurs langues, vous devez spécifier une langue à utiliser par défaut.

Par exemple, pour installer l'anglais ainsi que le français et utiliser l'anglais comme langue par défaut, la commande suivante sera nécessaire:

```
langsupport --default=en_US fr_FR
```

Si vous utilisez `--default` avec une seule langue, toutes les langues seront installées et la langue spécifiée sera utilisée par défaut.

`lilo` (remplacé par `bootloader`)

Avertissement

Cette option a été remplacée par `bootloader` est n'est disponible que pour une compatibilité en amont. Reportez-vous à `bootloader`.

Spécifie la façon dont le chargeur d'amorçage doit être installé sur le système. Par défaut, LILO est installé sur le bloc de démarrage maître du premier disque et installe un système à double démarrage s'il trouve une partition DOS (le système DOS/Windows démarre si l'utilisateur tape `dos` à l'invite `LILO:`) .

`--append` <*paramètres*>

Spécifie les paramètres du noyau.

`--linear`

Utilise l'option LILO `linear`; elle sert uniquement à la compatibilité en amont (et 'linear' est désormais utilisée par défaut).

`--nolinear`

Utilisez l'option LILO `nolinear`; l'option linéaire est désormais utilisée par défaut.

`--location=`

Spécifie l'emplacement de l'enregistrement d'amorçage LILO. Les valeurs possibles sont: `mbr` (par défaut) ou `partition` (installe le chargeur d'amorçage sur le premier secteur de la partition contenant le noyau). Si aucun emplacement n'est spécifié, LILO n'est pas installé.

`--lba32`

Force l'utilisation du mode lba32 au lieu de la détection automatique.

`lilocheck` (facultatif)

En présence de la commande `lilocheck`, le programme d'installation vérifie si LILO figure sur le bloc de démarrage maître du premier disque dur, puis redémarre le système s'il le trouve — aucune installation n'est alors effectuée. Ceci peut empêcher kickstart de réinstaller un système déjà présent.

`logvol` (facultatif)

Crée un volume logique pour la gestion du volume logique (LVM de l'anglais 'Logical Volume Management') avec la syntaxe suivante:

```
logvol point-de-montage
--vgname=nom --size=taille
```

`--name=`*nom*

Crée tout d'abord la partition, puis le groupe de volume logique et enfin le volume logique. Par exemple:

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

`mouse` (obligatoire)

Configure la souris pour le système, aussi bien en mode graphique qu'en mode texte. Les options sont les suivantes:

`--device=`

Le périphérique sur lequel se trouve la souris (`--device=ttyS0`, par exemple).

`--emulthree`

Si cette commande est présente, le système X Window reconnaît l'utilisation simultanée des boutons gauche et droit de la souris comme étant le bouton du milieu. N'utilisez cette option que si votre souris n'a que deux boutons.

Après les options, l'un des types de souris suivants peut être spécifié:

```
alpsps/2, ascii, asciips/2, atibm, generic, generic3, genericps/2,
generic3ps/2, genericwheelps/2, genericusb, generic3usb, genericwheelusb,
geniusnm, geniusnmps/2, geniusprops/2, geniusscrollps/2, geniusscrollps/2+,
thinking, thinkingps/2, logitech, logitechcc, logibm, logimman,
logimmanps/2, logimman+, logimman+ps/2, logimmusb, microsoft, msnew,
msintelli, msintellips/2, msintelliusb, msbm, mousesystems, mmseries,
mmhittab, sun, none
```

Cette liste se trouve également dans le fichier `/usr/lib/python2.2/site-packages/rhpl/mouse.py` qui fait partie du paquetage `rhpl`.

Si la commande relative à la souris est fournies sans aucun argument ou si elle est omise, le système d'installation essaiera de détecter automatiquement la souris. Cette procédure fonctionne pour la plupart des souris modernes.

`network` (facultatif)

Configure les options réseau du système. Si l'installation de kickstart ne requiert pas de connexion au réseau (c'est-à-dire si l'installation ne s'effectue pas par NFS, HTTP ou FTP), aucune connexion n'est configurée pour le système. En revanche, si l'installation requiert une connexion au réseau et que les informations de réseau ne sont pas fournies dans le fichier kickstart, le programme d'installation de Red Hat Linux suppose que l'installation doit être effectuée par eth0 via une adresse IP dynamique (BOOTP/DHCP) et configure le système installé de façon à ce qu'il détermine de manière dynamique son adresse IP. L'option `network` configure les informations de connexion au réseau, pour les installations kickstart via un réseau ainsi que pour le système installé.

`--bootproto=`

`dhcp`, `bootp` ou `static`.

`dhcp` est la valeur par défaut. `bootp` et `dhcp` sont traités de la même façon.

La méthode DHCP utilise un serveur DHCP pour obtenir la configuration de connexion au réseau. Comme vous pouvez l'imaginer, la méthode BOOTP est similaire et requiert un serveur BOOTP pour fournir la configuration de connexion au réseau. Pour demander à un système d'utiliser DHCP, la ligne suivante est nécessaire:

```
network --bootproto=dhcp
```

Pour demander à un ordinateur d'utiliser BOOTP afin d'obtenir sa configuration de connexion au réseau, utilisez la ligne suivante dans le fichier kickstart:

```
network --bootproto=bootp
```

La méthode statique requiert la saisie de toutes les informations de connexion au réseau requises dans le fichier kickstart. Comme leur nom l'indique, ces informations sont statiques et seront utilisées pendant et après l'installation. La ligne pour une connexion au réseau statique est plus complexe, dans la mesure où vous devez inclure toutes les informations de configuration réseau sur une ligne. Vous devez indiquer l'adresse IP, le masque réseau, la passerelle ainsi que le nom du serveur. Par exemple: (la barre oblique '\' indique que toute les informations se trouvent sur une seule ligne, contrairement à l'extrait reproduit):

```
network --bootproto=static --ip=10.0.2.15 --netmask=255.255.255.0 \
--gateway=10.0.2.254 --nameserver=10.0.2.1
```

Deux restrictions doivent être gardées à l'esprit lors de l'utilisation d'une la méthode statique, à savoir:

- Toutes les informations de configuration de la connexion au réseau statique doivent être spécifiées sur *une* ligne; vous ne pouvez pas, par exemple, insérer des retours à la ligne à l'aide de barres obliques inverses.
- Vous ne pouvez spécifier ici qu'un seul serveur de noms. Vous pouvez cependant utiliser la section `%post` du fichier kickstart (décrite dans la Section 7.7) pour ajouter, si nécessaire, davantage de serveurs de noms.

`--device=`

Utilisée pour sélectionner un périphérique Ethernet spécifique pour l'installation. L'utilisation de `--device=` n'est vraiment possible que si kickstart est un fichier local (tel que `ks=floppy`); dans ce cas en effet, le programme d'installation configure le réseau pour rechercher le fichier kickstart. Par exemple:

```
network --bootproto=dhcp --device=eth0
```

`--ip=`

Adresse IP pour l'ordinateur sur lequel effectuer l'installation.

`--gateway=`

Passerelle par défaut, sous la forme d'une adresse IP.

`--nameserver=`

Serveur de noms principal, sous la forme d'une adresse IP.

`--nodns`

Indique au système de ne pas configurer de serveur DNS.

`--netmask=`

Masque réseau pour le système installé.

`--hostname=`

Nom d'hôte pour le système installé.

`part` ou `partition` (obligatoire pour les installations mais à ignorer pour les mises à niveau)

Crée une partition sur le système.

Si plusieurs installations Red Hat Linux cohabitent sur différentes partitions du système, le programme d'installation demande à l'utilisateur quelle installation mettre à niveau.

Avertissement

Toutes les partitions créées seront formatées dans le cadre du processus d'installation, à moins que les commandes `--noformat` et `--onpart` ne soient utilisées.

<point-de-montage>

Le *<point-de-montage>* est l'endroit où la partition sera montée; il doit se présenter sous l'une des formes suivantes:

- */<chemin>*

  Par exemple, `/`, `/usr`, `/home`

- `swap`

  La partition sera utilisée comme espace de swap.

  Pour déterminer automatiquement la taille de la partition swap, utilisez l'option `--recommended`:

  ```
  swap --recommended
  ```

  La taille minimale de la partition swap générée automatiquement ne pourra être ni inférieure à la quantité de RAM du système, ni supérieure à deux fois cette quantité.

- `raid.`*<id>*

  La partition sera utilisée pour le RAID logiciel (reportez-vous à `raid`).

- `pv.`*<id>*

  La partition sera utilisée pour LVM (reportez-vous à `logvol`).

`--size=`

La taille minimale de la partition en méga-octets. Indiquez un nombre entier, 500 par exemple. Ne rajoutez pas "Mo" à la fin.

`--grow`

Indique à la partition d'occuper, le cas échéant, tout l'espace disponible ou l'espace maximal défini.

`--maxsize=`

Définit la taille de partition maximale, en méga-octets, lorsque la partition est paramétrée pour occuper davantage d'espace. Spécifiez un nombre entier et ne rajoutez pas "Mo" à la fin.

`--noformat`

Indique au programme d'installation de ne pas formater la partition; à utiliser avec la commande `--onpart`.

`--onpart=` ou `--usepart=`

Place la partition sur le périphérique *déjà existant*. Par exemple:

```
partition /home --onpart=hda1
```

place `/home` sur `/dev/hda1`, qui doit déjà exister.

`--ondisk=` ou `--ondrive=`

Force la création de la partition sur un disque spécifique. Par exemple, `--ondisk=sdb` place la partition sur le second disque SCSI du système.

`--asprimary`

Force l'allocation automatique de la partition en tant que partition primaire; si cette condition n'est pas respectée, le partitionnement échoue.

`--bytes-per-inode=`

Le nombre indiqué représente le nombre d'octets par inode sur le système de fichiers lors de sa création. Il doit avoir un format décimal. Cette option est utile pour les applications pour lesquelles vous souhaitez augmenter le nombre d'inodes sur le système de fichiers.

`--type=` (remplacé par `fstype`)

Cette option n'est plus disponible. Utilisez `fstype`.

`--fstype=`

Configure le type de système de fichiers pour la partition. Les valeurs valides sont `ext2`, `ext3`, `swap` et `vfat`.

`--start=`

Spécifie le premier cylindre de la partition. Cette commande requiert qu'un disque soit spécifié à l'aide de `--ondisk=` ou de `ondrive=`. Elle requiert également que le dernier cylindre soit spécifié avec `--end=` ou que la taille de la partition soit spécifiée avec `--size=`.

`--end=`

Spécifie le dernier cylindre de la partition. La commande requiert que le premier cylindre soit spécifié à l'aide de `--start=`.

`--badblocks`

Spécifie que l'état de la partition doit être contrôlé.

Remarque

Si le partitionnement échoue pour une raison quelconque, des messages de diagnostic s'affichent sur la console virtuelle 3.

`raid` (facultatif)

Assemble un périphérique RAID logiciel. Cette commande se présente sous la forme:

```
raid <point-de-montage>
--level=<niveau>
--device=<mddevice>
<partitions*>
```

<point-de-montage>

Emplacement où est monté le système de fichiers RAID. S'il s'agit de `/`, le niveau de RAID doit être égal à 1, à moins qu'une partition de démarrage (`/boot`) ne soit présente. Dans ce cas, la partition `/boot` doit être de niveau 1 et la partition root (`/`) peut être de n'importe quel type disponible. *<partitions*>* (qui indique que plusieurs partitions peuvent être répertoriées) affiche la liste des identificateurs RAID à ajouter à la matrice RAID.

`--level=`

Niveau de RAID à utiliser (0, 1 ou 5).

`--device=`

Nom du périphérique RAID à utiliser (md0 ou md1, par exemple). Les périphériques RAID vont de md0 à md7; chacun d'eux ne peut être utilisé qu'une seule fois.

`--spares=`

Spécifie le nombre de périphériques de rechange alloués à la matrice RAID. Ces périphériques servent à reconstruire la matrice en cas de mauvais fonctionnement des périphériques.

`--fstype=`

Définit le type de système de fichiers pour la matrice RAID. Les valeurs valides sont ext2, ext3, swap et vfat.

`--noformat`

Indique au système de ne pas formater la matrice RAID.

L'exemple suivant vous montre comment créer une partition RAID de niveau 1 pour `/` et une partition RAID de niveau 5 pour `/usr`, en supposant que trois disques SCSI soient présents sur le système. Le système crée également trois partitions swap, une sur chaque disque.

```
part raid.01 --size=60 --ondisk=sda
part raid.02 --size=60 --ondisk=sdb
part raid.03 --size=60 --ondisk=sdc
part swap --size=128 --ondisk=sda
part swap --size=128 --ondisk=sdb
part swap --size=128 --ondisk=sdc
part raid.11 --size=1 --grow --ondisk=sda
part raid.12 --size=1 --grow --ondisk=sdb
part raid.13 --size=1 --grow --ondisk=sdc
raid / --level=1 --device=md0 raid.01 raid.02 raid.03
raid /usr --level=5 --device=md1 raid.11 raid.12 raid.13
```

`reboot` (facultatif)

Redémarre une fois l'installation terminée (pas d'argument). Normalement, kickstart affiche un message, puis attend que l'utilisateur appuie sur une touche avant de redémarrer.

`rootpw` (obligatoire)

Définit le mot de passe root du système sur l'argument *<mot-de-passe>*.

```
rootpw [--iscrypted] <mot-de-passe>
```

`--iscrypted`

Si cette option est présente, l'argument du mot de passe est supposé être déjà crypté.

`skipx` (facultatif)

Si cette option est présente, X n'est pas configuré sur le système installé.

`text` (facultatif)

Effectue l'installation de kickstart en mode texte. Par défaut, les installations de kickstart sont effectuées en mode graphique.

`timezone` (obligatoire)

Définit le fuseau horaire du système sur <*fuseau-horaire*>; il peut s'agir de n'importe quel fuseau horaire répertorié par `timeconfig`.

`timezone [--utc]` <*fuseau-horaire*>

`--utc`

Si cette option est présente, le système suppose que l'horloge temps réel est réglée sur l'heure GMT (heure de Greenwich).

`upgrade` (facultatif)

Indique au système de mettre à niveau un système existant plutôt que d'en installer un nouveau. Vous devez indiquer l'emplacement de l'arborescence d'installation: cdrom, harddrive (disque dur), nfs ou url (pour ftp et http). Pour plus d'informations, reportez-vous à `install`.

`xconfig` (facultatif)

Configure le système X Window. Si cette option n'est pas spécifiée, l'utilisateur doit configurer X Window manuellement durant l'installation, à condition que X Window ait été installé; cette option ne doit pas être utilisée si X Window n'est pas installé sur le système final.

`--noprobe`

Indique au système de ne pas essaiyer de détecter l'écran.

`--card=`

Utilise la carte spécifiée; ce nom de carte doit provenir de la liste des cartes de `/usr/share/hwdata/Cards` du paquetage `hwdata`. La liste des cartes est également disponible sur l'écran **Configuration de X** du programme **Configuration de Kickstart**. Si cet argument n'est pas fourni, le programme d'installation cherche à détecter le bus PCI de la carte. Étant donné que AGP fait partie du bus PCI, les cartes AGP seront détectées si elles sont prises en charge. L'ordre de détection est défini par l'ordre de balayage PCI de la carte mère.

`--videoram=`

Spécifie la quantité de mémoire vidéo de la carte vidéo.

`--monitor=`

Utilise le moniteur spécifié ; ce nom de moniteur doit provenir de la liste des moniteurs de `/usr/share/hwdata/MonitorsDB` du paquetage `hwdata`. La liste des moniteurs est également disponible sur l'écran **Configuration de X** du programme **Configuration de Kickstart**. Cette option est ignorée si `--hsync` ou `--vsync` est fourni. Si aucune information sur le moniteur n'est fournie, le programme d'installation essaie de le détecter automatiquement.

`--hsync=`

Spécifie la fréquence de synchronisation horizontale de l'écran.

`--vsync=`

Spécifie la fréquence de synchronisation verticale de l'écran.

`--defaultdesktop=`

Spécifie GNOME ou KDE pour définir le bureau par défaut (suppose que l'environnement de bureau GNOME et/ou KDE a été installé avec `%packages`).

`--startxonboot`

Utilise une connexion graphique sur le système installé.

`--resolution=`

Spécifie la résolution par défaut du système X Window sur le système installé. Les valeurs valides sont 640x480, 800x600, 1024x768, 1152x864, 1280x1024, 1400x1050, 1600x1200. La résolution spécifiée doit être compatible avec la carte vidéo et l'écran.

`--depth=`

Spécifie la profondeur des couleurs par défaut du système X Window sur le système installé. Les valeurs utilisables sont 8, 16, 24 et 32. La profondeur choisie doit être compatible avec la carte vidéo et l'écran.

`volgroup` (facultatif)

Crée un groupe de gestion du volume logique (LVM) avec la syntaxe suivante:

```
volgroup nom
partition
```

Crée tout d'abord la partition, puis le groupe de volume logique et enfin le volume logique. Par exemple:

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

`zerombr` (facultatif)

Si `zerombr` est spécifié et que `yes` est son seul argument, toute table des partitions non valide trouvée sur les disques est initialisée. Ceci détruira tout le contenu des disques contenant des tables des partitions non valides. Cette commande doit être utilisée comme suit:

```
zerombr yes
```

Aucun autre format n'est pris en compte.

`%include`

Utilisez la commande `%include /chemin/vers/fichier` afin d'inclure le contenu d'un autre fichier dans le fichier kickstart comme si le contenu se trouvait à l'emplacement de la commande `%include` dans le fichier Kickstart.

7.5. Sélection de paquetages

Utilisez la commande `%packages` pour commencer une section de fichier kickstart indiquant la liste des paquetages que vous voulez installer (ceci ne vaut que pour les installations, étant donné que la sélection de paquetages au cours des mises à niveau n'est pas prise en charge).

Les paquetages peuvent être spécifiés par groupe ou par nom de paquetage individuel. Le programme d'installation définit plusieurs groupes qui contiennent les paquetages connexes. Reportez-vous au fichier `RedHat/base/comps.xml` sur le premier CD-ROM Red Hat Linux CD-ROM pour obtenir une liste de groupes. Chaque groupe dispose d'un ID, d'une valeur de visibilité utilisateur, d'un nom, d'une description et d'une liste des paquetages. Dans cette liste, les paquetages indiqués comme étant obligatoires sont toujours installés si le groupe est sélectionné; les paquetages indiqués comme 'défaut' sont choisis par défaut si le groupe est sélectionné; finalement les paquetages considérés comme facultatifs doivent être individuellement choisis, même si l'installation du groupe a été sélectionnée.

Le plus souvent, il suffit de répertorier les groupes souhaités et non des paquetages individuels. Veuillez noter que les groupes `Core` et `Base` sont toujours sélectionnés par défaut; il n'est donc pas nécessaire de les spécifier dans la section `%packages`.

Ci-après figure un exemple de sélection `%packages`:

```
%packages
@ X Window System
@ GNOME Desktop Environment
@ Graphical Internet
@ Sound and Video
galeon
```

Comme vous le voyez, les groupes sont spécifiés, un par ligne, en commençant par le symbole `@`, suivi d'un espace, puis du nom complet du groupe tel qu'il figure dans le fichier `comps.xml`. Spécifiez des paquetages individuels sans caractères supplémentaires (la ligne `galeon` dans l'exemple ci-dessus désigne un paquetage individuel).

Vous pouvez également spécifier dans la liste des paquetages par défaut, ceux qui ne doivent pas être installés:

```
@ Games and Entertainment
-kdegames
```

Deux options sont disponibles pour l'option `%packages`.

`--resolvedeps`

Cette option installe non seulement les paquetages sélectionnés mais résout également les dépendances paquetage. Si cette option n'est pas spécifiée et qu'il existe des dépendances, l'installation automatisée s'arrêtera et invitera l'utilisateur à fournir des instructions. Par exemple:

```
%packages --resolvedeps
```

`--ignoredeps`

Cette option ne prend pas en compte les dépendances non-résolues et installe les paquetages listés sans les dépendances. Par exemple:

```
%packages --ignoredeps
```

`--ignoremissing`[1]

Cette option ne prend pas en compte les paquetages et groupes manquants et continue l'installation sans s'arrêter pour demander si cette dernière devrait être abandonnée ou poursuivie. Par exemple:

1. Cette option est un nouvel ajout à Red Hat Linux 9.

```
%packages --ignoremissing
```

7.6. Script avant-installation

Vous avez la possibilité d'ajouter des commandes à exécuter sur le système immédiatement après l'analyse du fichier `ks.cfg`. Cette section doit figurer à la fin du fichier kickstart (après les commandes) et doit commencer par la commande `%pre`. Vous pouvez accéder au réseau dans la section `%pre`; toutefois, le *service de noms* n'a pas encore été configuré à ce stade. Par conséquent, seules les adresses IP fonctionneront.

Remarque

Le script de pré-installation n'est pas exécuté dans l'environnement chroot.

`--interpreter` *`/usr/bin/python`*

Vous permet de spécifier un autre langage de script, tel que Python. Remplacez *`/usr/bin/python`* par le langage de script de votre choix.

7.6.1. Exemple

Ci-dessous figure un exemple de section `%pre`:

```
%pre

#!/bin/sh

hds=""
mymedia=""

for file in /proc/ide/h*
do
  mymedia=`cat $file/media`
  if [ $mymedia == "disk" ] ; then
      hds="$hds `basename $file`"
  fi
done

set $hds
numhd=`echo $#`

drive1=`echo $hds | cut -d' ' -f1`
drive2=`echo $hds | cut -d' ' -f2`

#Write out partition scheme based on whether there are 1 or 2 hard drives

if [ $numhd == "2" ] ; then
  #2 drives
  echo "#partitioning scheme generated in %pre for 2 drives" >
/tmp/part-include
  echo "clearpart --all" >> /tmp/part-include
  echo "part /boot --fstype ext3 --size 75 --ondisk hda" >>
/tmp/part-include
  echo "part / --fstype ext3 --size 1 --grow --ondisk hda" >>
/tmp/part-include
```

```
  echo "part swap --recommended --ondisk $drive1" >> /tmp/part-include
  echo "part /home --fstype ext3 --size 1 --grow --ondisk hdb" >>
/tmp/part-include
else
  #1 drive
  echo "#partitioning scheme generated in %pre for 1 drive" >
/tmp/part-include
  echo "clearpart --all" >> /tmp/part-include
  echo "part /boot --fstype ext3 --size 75" >> /tmp/part-includ
  echo "part swap --recommended" >> /tmp/part-include
  echo "part / --fstype ext3 --size 2048" >> /tmp/part-include
  echo "part /home --fstype ext3 --size 2048 --grow" >> /tmp/part-include
fi
```

Ce script détermine le nombre de disques durs présents sur le système et enregistre un fichier texte avec un schéma de partitionnement différent s'il dispose d'un ou de deux disques. Au lieu d'avoir un ensemble de commandes de partitionnement dans le fichier kickstart, incorporez la ligne:

```
%include /tmp/part-include
```

Les commandes de partitionnement sélectionnées dans le script seront utilisées.

7.7. Script après-installation

Vous avez la possibilité d'ajouter des commandes à exécuter sur le système une fois l'installation terminée. Cette section doit se trouver à la fin du fichier kickstart et commencer par la commande `%post`. Cette section est utile pour des fonctions telles que l'installation de logiciels supplémentaires et la configuration d'un serveur de noms supplémentaire.

Remarque

Si vous avez configuré votre réseau avec des informations IP statiques, y compris un serveur de noms, vous pouvez accéder au réseau et résoudre les adresses IP dans la section `%post`. Si vous avez configuré votre réseau pour DHCP, le fichier `/etc/resolv.conf` n'a pas été complété lors de l'exécution de la section `%post` au cours de l'installation. Vous pouvez accéder au réseau, mais vous ne pouvez pas résoudre d'adresses IP. Ainsi, si vous utilisez DHCP, vous devez spécifier des adresses IP dans la section `%post`.

Remarque

Le script post-installation est exécuté dans un environnement chroot; c'est pourquoi l'exécution de tâches telles que la copie de scripts ou de RPM à partir des supports d'installation ne fonctionnera pas.

`--nochroot`

Vous permet de spécifier des commandes que vous souhaitez exécuter en dehors de l'environnement chroot.

L'exemple suivant montre comment copier le fichier `/etc/resolv.conf` dans le système de fichiers qui vient d'être installé.

```
%post --nochroot
cp /etc/resolv.conf /mnt/sysimage/etc/resolv.conf
```

`--interpreter` *`/usr/bin/python`*

Vous permet de spécifier un autre langage de script, tel que Python. Remplacez *`/usr/bin/python`* par le langage de script de votre choix.

7.7.1. Exemples

Activer ou désactiver des services:

```
/sbin/chkconfig --level 345 telnet off
/sbin/chkconfig --level 345 finger off
/sbin/chkconfig --level 345 lpd off
/sbin/chkconfig --level 345 httpd on
```

Exécuter un script appelé `runme` depuis un partage NFS:

```
mkdir /mnt/temp
mount 10.10.0.2:/usr/new-machines /mnt/temp
open -s -w -- /mnt/temp/runme
umount /mnt/temp
```

Ajouter un utilisateur au système:

```
/usr/sbin/useradd bob
/usr/bin/chfn -f "Bob Smith" bob
/usr/sbin/usermod -p 'kjdf$04930FTH/ ' bob
```

7.8. Mise à disposition du fichier kickstart

Un fichier kickstart doit être placé dans un des emplacements suivants:

- Sur une disquette de démarrage
- Sur un CD-ROM de démarrage
- Sur un réseau

Un fichier kickstart est normalement copié sur la disquette de démarrage ou mis à disposition sur le réseau. L'approche réseau est la plus couramment utilisée, la plupart des installations kickstart étant réalisées sur des ordinateurs en réseau.

Examinons plus attentivement les emplacements où peuvent se trouver le fichier kickstart.

7.8.1. Création d'une disquette de démarrage kickstart

Pour réaliser une installation kickstart à partir d'une disquette, le fichier kickstart doit être nommé `ks.cfg` et situé dans le répertoire de niveau supérieur de la disquette de démarrage. Reportez-vous à la section *Création d'une disquette de démarrage de l'installation* du *Guide d'installation de Red Hat Linux* pour obtenir des informations sur la création d'une disquette de démarrage. Étant donné que les disquettes de démarrage Red Hat Linux sont dans un format MS-DOS, il est facile de copier le fichier kickstart sous Linux à l'aide de la commande `mcopy`:

```
mcopy ks.cfg a:
```

Vous pouvez également utiliser Windows pour copier le fichier. Vous pouvez aussi monter la disquette de démarrage MS-DOS dans Red Hat Linux avec le type de système de fichiers vfat et utiliser la commande `cp` pour copie le fichier sur la disquette.

7.8.2. Création d'un CD-ROM de démarrage kickstart

Pour réaliser une installation kickstart à partir d'un CD-ROM, le fichier kickstart doit être nommé `ks.cfg` et situé dans le répertoire de niveau supérieur de la disquette de démarrage. Étant donné que le CD-ROM est en accès de lecture-seule, le fichier doit être ajouté au répertoire utilisé pour la création de l'image enregistrée sur le CD-ROM. Reportez-vous à la section *Création d'un CD-ROM de démarrage de l'installation* du *Guide d'installation de Red Hat Linux* pour obtenir des informations sur la création d'un CD-ROM de démarrage; toutefois, avant de créer le fichier image `file.iso`, copiez le fichier kickstart `ks.cfg` dans le répertoire `isolinux/`.

7.8.3. Mise à disposition du fichier kickstart sur le réseau

Les installations réseau utilisant kickstart sont assez courantes; les administrateurs système pouvent en effet aisément automatiser l'installation sur de nombreux ordinateurs en réseau. Cette tâche peut être réalisée rapidement et sans problème. En général, l'approche la plus couramment utilisée consiste, pour l'administrateur, à avoir à la fois un serveur BOOTP/DHCP et un serveur NFS sur le réseau local. Le serveur BOOTP/DHCP sert à communiquer au système client ses informations de connexion au réseau, tandis que les fichiers réellement utilisés pendant l'installation se trouvent sur le serveur NSF. Ces deux serveurs fonctionnent souvent sur le même ordinateur, mais ce n'est pas une obligation.

Pour réaliser une installation kickstart à partir d'un réseau, un serveur BOOTP/DHCP doit se trouver sur votre réseau. Il doit également comporter des informations de configuration pour l'ordinateur sur lequel vous installez Red Hat Linux. Le serveur BOOTP/DHCP fournit au client ses informations de connexion au réseau ainsi que l'emplacement du fichier kickstart.

Si un fichier kickstart est spécifié par le serveur BOOTP/DHCP, le système client tente un montage NFS du chemin du fichier et copie le fichier spécifié sur le client, en l'utilisant comme fichier kickstart. Les paramètres exacts requis dépendent du serveur BOOTP/DHCP utilisé.

Ci-dessous figure un exemple d'une ligne tirée du fichier `dhcpd.conf` pour le serveur DHCP livré avec Red Hat Linux:

```
filename
"/usr/new-machine/kickstart/";
next-server blarg.redhat.com;
```

Veuillez noter que vous devez remplacer la valeur indiquée après `filename` par le nom du fichier kickstart (ou du répertoire dans lequel se trouve ce fichier) ainsi que la valeur indiquée après `Serveur-suivant` par le nom du serveur NFS.

Si le nom de fichier renvoyé par le serveur BOOTP/DHCP se termine par une barre oblique ("/"), il n'est interprété que comme un chemin. Dans ce cas, le système client monte ce chemin à l'aide de NFS et recherche un fichier particulier. Le nom de fichier recherché par le client est:

`<adresse-ip>-kickstart`

La section `<adresse-ip>` du nom de fichier doit être remplacée par l'adresse IP du client sous forme décimale séparée par des points. Par exemple, le nom de fichier pour un ordinateur ayant comme adresse IP 10.10.0.1 est `10.10.0.1-kickstart`.

Veuillez noter que si vous ne précisez pas un nom de serveur, le système client essaie d'utiliser comme serveur NFS celui ayant répondu à la requête BOOTP/DHCP. Si vous ne spécifiez pas un chemin ou un nom de fichier, le système client essaie de monter `/kickstart` à partir du serveur BOOTP/DHCP et de trouver le fichier kickstart à l'aide du même nom de fichier `<adresse-ip>-kickstart` que celui décrit ci-dessus.

7.9. Mise à disposition de l'arborescence d'installation

L'installation kickstart doit accéder à une *arborescence d'installation*. Il s'agit d'une copie des CD-ROM Red Hat Linux binaires comportant la même structure de répertoires.

Si vous effectuez une installation à partir de CD-ROM, insérez le CD-ROM 1 de Red Hat Linux dans votre lecteur avant de lancer l'installation kickstart.

Si vous effectuez une installation à partir d'un disque dur, assurez-vous que les images ISO des CD-ROM Red Hat Linux binaires se trouvent sur un disque dur de l'ordinateur.

Si vous effectuez une installation réseau (NFS, FTP ou HTTP), l'arborescence d'installation doit être mise à disposition sur le réseau. Reportez-vous à la section *Préparation pour une installation réseau* du *Guide d'installation de Red Hat Linux* afin d'obtenir de plus amples informations.

7.10. Lancement d'une installation kickstart

Pour commencer une installation kickstart, vous devez lancer le système à partir d'une disquette de démarrage Red Hat Linux ou du CD-ROM de démarrage Red Hat Linux ou du CD-ROM 1 Red Hat Linux et taper une commande spéciale à l'invite boot:. Le programme d'installation cherche un fichier kickstart si l'argument de ligne de commande `ks` est transmis au noyau.

disquette de démarrage

Si le fichier kickstart se trouve sur la disquette de démarrage (aussi appelée disque d'amorçage), comme l'explique la Section 7.8.1, démarrez le système avec la disquette dans le lecteur et entrez à l'invite `boot:`, la commande suivante:

```
linux ks=floppy
```

CD-ROM 1 et disquette

La commande **`linux ks=floppy`** fonctionne également si le fichier `ks.cfg` est situé sur un système de fichiers vfat ou ext2 sur une disquette et que vous démarrez à partir du CD-ROM 1 Red Hat Linux.

Il existe une autre commande permettant de démarrer à partir du CD-ROM 1 Red Hat Linux et d'avoir le fichier kickstart sur un système de fichiers vfat ou ext2 sur une disquette. Pour ce faire, entrez à l'invite `boot:` la commande suivante:

```
linux ks=hd:fd0:/ks.cfg
```

Avec une disquette de pilotes

Si vous devez utiliser une disquette de pilotes avec kickstart, spécifiez également l'option **dd**. Par exemple, pour amorcer la disquette de démarrage et utiliser une disquette de pilotes, entrez à l'invite `boot:` la commande suivante:

```
linux ks=floppy dd
```

CD-ROM de démarrage

Si le fichier kickstart se trouve sur un CD-ROM de démarrage, comme l'explique la Section 7.8.2, insérez le CD-ROM dans le système, démarrez le système et entrez à l'invite `boot:` la commande suivante (où `ks.cfg` correspond au nom du fichier kickstart):

```
linux ks=cdrom:/ks.cfg
```

Ci-dessous figurent d'autres options pour démarrer une installation kickstart:

`ks=nfs:`<*serveur*>`/`<*chemin*>

Le programme d'installation cherche le fichier kickstart sur le serveur NFS <*serveur*>, en tant que fichier <*chemin*>. Le programme d'installation utilise DHCP afin de configurer la carte Ethernet. Par exemple, si votre serveur NFS se nomme exemple.serveur.com et que le fichier kickstart se trouve dans le partage NFS `/mydir/ks.cfg`, la commande de démarrage appropriée est `ks=nfs:exemple.serveur.com:/mydir/ks.cfg`.

`ks=http://`<*serveur*>`/`<*chemin*>

Le programme d'installation cherche le fichier kickstart sur le serveur HTTP <*serveur*>, en tant que fichier <*chemin*>. Le programme d'installation utilise DHCP afin de configurer la carte Ethernet. Par exemple, si votre serveur HTTP se nomme exemple.serveur.com et que le fichier kickstart se trouve dans le répertoire HTTP `/mydir/ks.cfg`, la commande de démarrage appropriée est `ks=http://server.example.com/mydir/ks.cfg`.

`ks=floppy`

Le programme d'installation cherche le fichier `ks.cfg` sur un système de fichiers vfat ou ext2 sur la disquette dans `/dev/fd0`.

`ks=floppy:/`<*chemin*>

Le programme d'installation cherchera le fichier kickstart sur la disquette dans `/dev/fd0`, en tant que fichier <*chemin*>.

`ks=hd:`<*périphérique*>`:/`<*fichier*>

Le programme d'installation montera le système de fichier <*périphérique*> (qui doit être de type vfat ou ext2) et cherchera le fichier de configuration en tant que <*fichier*> dans le système de fichiers (par exemple, `ks=hd:sda3:/mydir/ks.cfg`).

Remarque

Les deuxièmes deux points (":") correspondent à un changement de syntaxe pour Red Hat Linux 9.

`ks=file:/`<*fichier*>

Le programme d'installation essaiera de lire le fichier <*fichier*> à partir du système de fichiers; aucun montage de sera effectué. Cette commande est généralement utilisée si le fichier kickstart est déjà sur l'image `initrd`.

`ks=cdrom:/<chemin>`

Le programme d'installation cherche le fichier kickstart sur le CD-ROM, en tant que fichier `<chemin>`.

`ks`

Si `ks` est utilisé seul, le programme d'installation configure la carte Ethernet dans le système à l'aide de DHCP. Le système utilise le "bootServer" de la réponse DHCP en tant que serveur NFS à partir duquel lire le fichier kickstart (par défaut, c'est le même que le serveur DHCP). Le nom du fichier kickstart correspond à l'un des cas suivants:

- Si DHCP est spécifié et que le fichier de démarrage commence par un `/`, le fichier fourni par DHCP est recherché sur le serveur NFS.
- Si DHCP est spécifié et que le fichier de démarrage commence par autre chose que `/`, le fichier fourni par DHCP est recherché sur le serveur NFS dans le répertoire `/kickstart`.
- Si DHCP n'a pas spécifié de fichier de démarrage, le programme d'installation essaie de lire le fichier `/kickstart/1.2.3.4-kickstart`, où *`1.2.3.4`* correspond à l'adresse IP numérique de l'ordinateur sur lequel l'installation est effectuée.

`ksdevice=<périphérique>`

Le programme d'installation utilise ce périphérique réseau pour se connecter au réseau. Par exemple, pour lancer une installation avec le fichier kickstart situé sur un serveur NFS connecté au système via le périphérique eth1, utilisez la commande `ks=nfs:<serveur:>/<chemin> ksdevice=eth1` à l'invite `boot:` .

Chapitre 8.

Configuration de Kickstart

Configuration de Kickstart vous permet de créer un fichier kickstart à l'aide d'une interface utilisateur graphique, afin que vous n'ayez pas à vous rappeler la syntaxe correcte du fichier.

Pour utiliser **Configuration de Kickstart**, le système X Window doit être en cours d'exécution. Pour lancer **Configuration de Kickstart**, sélectionnez le bouton **Menu Principal** (sur le panneau) => **Outils de système** => **Kickstart** ou tapez la commande `/usr/sbin/redhat-config-kickstart`.

Durant la création d'un fichier kickstart, vous pouvez sélectionner **Fichier** => **Aperçu** à tout moment pour obtenir un aperçu de vos sélections actuelles.

8.1. Configuration de base

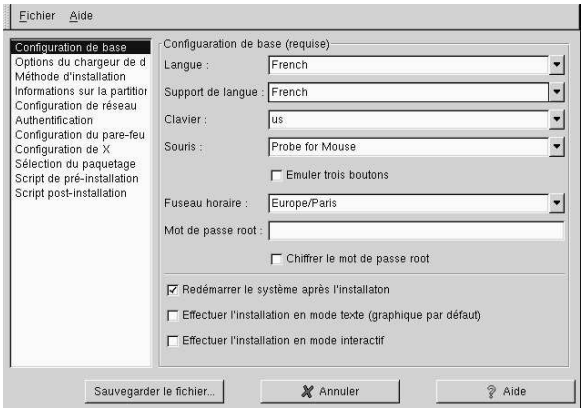

Figure 8-1. Configuration de base

Choisissez la langue à utiliser pendant l'installation en tant que langue par défaut depuis le menu **Langue**.

Choisissez le type de clavier dans le menu **Clavier**.

Choisissez la souris pour le système depuis le menu **Souris**. Si vous optez pour **Pas de souris**, aucune souris ne sera configurée. Si vous optez pour **Détecter la souris**, le programme d'installation essaiera de détecter automatiquement votre souris. La détection fonctionne généralement avec la plupart des souris modernes.

Si vous avez une souris à deux boutons, vous pouvez simuler une souris à trois boutons en sélectionnant **Émulater 3 Boutons**. Si cette option est sélectionnée, vous n'aurez qu'à cliquer sur les deux boutons de la souris en même temps pour faire comme si vous cliquiez sur le troisième bouton, soit celui du milieu.

Dans le menu **Fuseau horaire**, choisissez le fuseau horaire à utiliser pour le système. Pour configurer le système afin qu'il utilise le temps universel (UTC), sélectionnez **Utiliser horloge en temps universel**.

Entrez le mot de passe super-utilisateur (ou root) souhaité pour le système dans la zone de texte **Mot de passe Root**. Pour enregistrer le mot de passe en tant que mot de passe crypté dans le fichier, sélectionnez **Crypter mot de passe root**. Si l'option de cryptage est retenue, lorsque le fichier sera enregistré, le mot de passe en texte clair que vous avez entré sera crypté et enregistré dans le fichier kickstart. N'entrez pas de mots de passe déjà cryptés pour ensuite sélectionner l'option de cryptage.

Pour installer des langues en plus de celle sélectionnée dans le menu déroulant **Langue**, cochez-les dans la liste **Suppport de Langues**. La langue sélectionnée dans le menu déroulant **Langue** est utilisée par défaut après l'installation. Elle peut toutefois être modifiée à l'aide de l'**Outil de configuration de la langue** (`redhat-config-language`) après l'installation.

Si vous choisissez **Redémarrer le système après l'installation**, votre système redémarrera automatiquement lorsque l'installation sera terminée.

Les installations kickstart sont effectuées en mode graphique par défaut. Pour annuler cet choix par défaut et utiliser le mode texte à la place, sélectionnez **Effectuer installation en mode texte**.

Vous pouvez effectuer une installation Kickstart en mode interactif. Dans ce cas, le programme d'installation utilise toutes les options pré-configurées dans le fichier kickstart tout en vous laissant visualiser les options dans chaque écran avant de passer à l'écran suivant. Pour passer à l'écran suivant, cliquez simplement sur le bouton **Suivant** après avoir accepté ou modifié (s'il ne vous convenaient pas) les paramètres, avant de poursuivre l'installation. Pour choisir ce type d'installation, sélectionnez l'option **Effectuer installation en mode interactif**.

8.2. Méthode d'installation

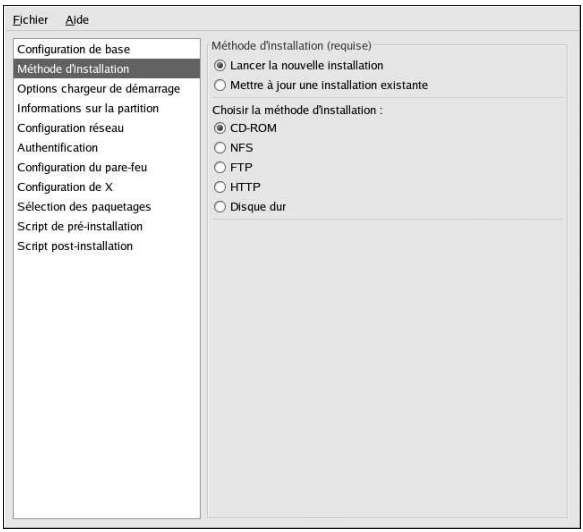

Figure 8-2. Méthode d'installation

L'écran **Méthode d'installation** vous permet de choisir si vous voulez exécuter une installation complète ou une mise à niveau. Si vous sélectionnez la mise à niveau, les options **Informations sur la partition** et **Sélection des paquetages** seront désactivées. Elles ne sont pas prises en charge pour les mises à niveau de kickstart.

Choisissez aussi le type d'installation kickstart à exécuter depuis cet écran. À ce stade, vous avez le choix entre les options suivantes:

- **CD-ROM** — Sélectionnez cette option pour installer Red Hat Linux à partir des CD-ROM Red Hat Linux.
- **NFS** — Sélectionnez cette option pour installer Red Hat Linux à partir d'un répertoire partagé NFS. Deux zones de texte, une pour le serveur NFS et l'autre pour le répertoire NFS, s'afficheront alors. Entrez le nom de domaine pleinement qualifié ou l'adresse IP du serveur NFS. Pour le répertoire NFS, entrez le nom du répertoire NFS contenant le répertoire `RedHat` de l'arborescence d'installation. Par exemple, si votre serveur NFS contient le répertoire `/mirrors/redhat/i386/RedHat/`, entrez `/mirrors/redhat/i386/` pour le répertoire NFS.
- **FTP** — Sélectionnez cette option pour installer Red Hat Linux à partir d'un serveur FTP. Deux zones de texte, une pour le serveur FTP et l'autre pour le répertoire FTP, s'afficheront alors. Entrez le nom de domaine pleinement qualifié ou l'adresse IP du serveur FTP. Pour le répertoire FTP, entrez le nom du répertoire FTP contenant le répertoire `RedHat`. Par exemple, si votre serveur FTP contient le répertoire `/mirrors/redhat/i386/RedHat/`, entrez `/mirrors/redhat/i386/` pour le répertoire FTP. Si le serveur FTP nécessite un nom d'utilisateur et mot de passe, spécifiez-les également.
- **HTTP** — Sélectionnez cette option pour installer Red Hat Linux à partir d'un serveur HTTP. Deux zones de texte, une pour le serveur HTTP et l'autre pour le répertoire HTTP, s'afficheront alors. Entrez le nom de domaine pleinement qualifié ou l'adresse IP du serveur HTTP. Pour le répertoire HTTP, entrez le nom du répertoire HTTP contenant le répertoire `RedHat`. Par exemple, si votre serveur HTTP contient le répertoire `/mirrors/redhat/i386/RedHat/`, entrez `/mirrors/redhat/i386/` pour le répertoire HTTP.
- **Disque dur** — Sélectionnez cette option pour installer Red Hat Linux à partir du disque dur. Deux zones de texte, une pour la partition de disque et l'autre pour le répertoire du disque dur, s'afficheront alors. Les installations à partir du disque dur nécessitent l'utilisation d'images ISO (ou CD-ROM). Assurez-vous que ces images sont intactes avant de commencer l'installation. Pour ce faire, utilisez un programme `md5sum` ainsi que l'option de démarrage `linux mediacheck` comme l'explique le *Guide d'installation de Red Hat Linux*. Entrez la partition du disque dur contenant les images ISO (par exemple, `/dev/hda1`) dans la zone de texte **Partition de disque dur**. Entrez le répertoire contenant les images ISO dans la zone de texte **Répertoire de disque dur**.

8.3. Options du chargeur d'amorçage

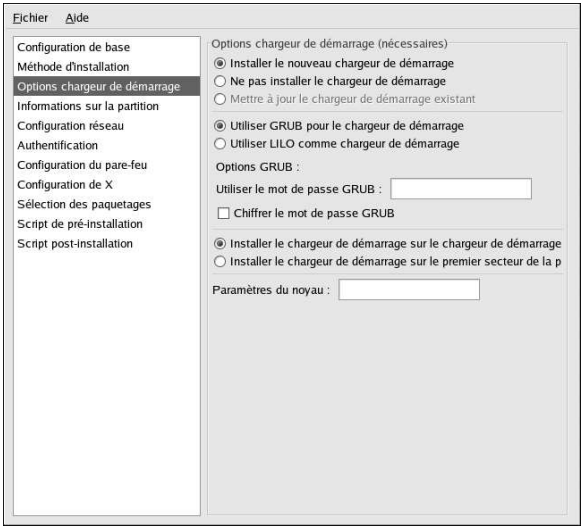

Figure 8-3. Options du chargeur d'amorçage

Vous avez le choix entre l'installation du chargeur d'amorçage GRUB ou celle du chargeur de démarrage LILO. Si vous ne souhaitez pas installer de chargeur d'amorçage, sélectionnez **Ne pas installer le chargeur de démarrage**. Si vous décidez de ne pas installer de chargeur d'amorçage, assurez-vous bien de créer une disquette de démarrage ou de disposer d'un autre moyen pour démarrer votre système (un chargeur d'amorçage tiers par exemple).

Si vous choisissez d'installer un chargeur d'amorçage, vous devez aussi préciser celui que vous allez installer (GRUB ou LILO) ainsi que l'endroit où il devra être installé (le bloc de démarrage maître - MBR - ou le premier secteur de la partition `/boot`). Installez le chargeur d'amorçage sur le bloc de démarrage maître si vous prévoyez de l'utiliser en tant que chargeur d'amorçage. Si vous utilisez un chargeur d'amorçage différent, installez LILO ou GRUB sur le premier secteur de la partition `/boot` et configurez l'autre chargeur d'amorçage pour démarrer Red Hat Linux.

Pour transmettre au noyau des paramètres spéciaux devant être utilisés lors du démarrage, entrez-les dans la zone de texte **Paramètres du noyau**. Par exemple, si vous avez un graveur de CD-ROM IDE, vous pouvez indiquer au noyau d'utiliser le pilote d'émulation SCSI qui doit être chargé avant l'utilisation de `cdrecord` en entrant **`hdd=ide-scsi`** en tant que paramètre du noyau (où **`hdd`** représente le périphérique CD-ROM).

Si vous choisissez le chargeur d'amorçage GRUB, vous pouvez le protéger à l'aide d'un mot de passe en configurant un mot de passe GRUB. Entrez un mot de passe dans la zone de texte **Utiliser un mot de passe GRUB**. Pour enregistrer le mot de passe en tant que mot de passe crypté dans le fichier, sélectionnez **Crypter le mot de passe GRUB**. Avec cette option, lorsque le fichier est enregistré, le mot de passe en texte clair que vous avez entré sera crypté et enregistré dans le fichier kickstart. N'entrez pas de mots de passe déjà cryptés pour ensuite sélectionner l'option de cryptage.

Si vous choisissez LILO en tant que chargeur d'amorçage, décidez si vous voulez utiliser le mode linéaire et si vous voulez forcer l'utilisation du mode lba32.

Si vous avez sélectionné **Mettre à niveau une installation existante** sur la page **Méthode d'installation**, sélectionnez **Mettre à niveau le chargeur de démarrage actuel** pour mettre à niveau la configuration du chargeur d'amorçage existant, tout en préservant les anciennes entrées.

8.4. Informations sur les partitions

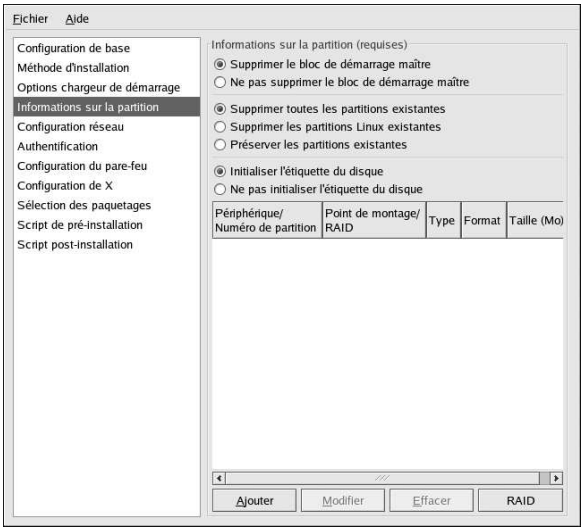

Figure 8-4. Informations sur les partitions

Indiquez si vous souhaitez ou non effacer les blocs de démarrage maîtres (ou MBR de l'anglais 'Master Boot Record'). Vous pouvez également choisir de supprimer toutes les partitions existantes, de supprimer toutes les partitions Linux existantes ou de conserver les partitions actuelles.

Vous pouvez initialiser l'étiquette du disque (ou label disque) sur la valeur par défaut pour l'architecture du système (par exemple, `msdos` pour x86 et `gpt` pour Itanium). Sélectionnez **Initialiser l'étiquette du disque** si vous effectuez l'installation sur un tout nouveau disque dur.

8.4.1. Création de partitions

Pour créer une partition, cliquez sur le bouton **Ajouter**. La fenêtre **Options de partition** reproduite dans la Figure 8-5 apparaîtra alors. Sélectionnez le point de montage, le type de système de fichiers et la taille de la nouvelle partition. Vous pouvez également choisir les options suivantes:

- Dans la section **Options supplémentaires de taille**, choisissez une taille de partition fixe, une taille maximale ou d'occuper tout l'espace disponible sur le disque dur. Si vous avez sélectionné swap comme type de système de fichiers, vous pouvez demander au programme d'installation de créer la partition swap à la taille recommandée au lieu de préciser une taille.
- Forcez la partition devant être créée en tant que partition primaire.

- Créez la partition sur un disque dur spécifique. Par exemple, pour créer la partition sur le premier disque dur IDE (`/dev/hda`), spécifiez **`hda`** comme disque. N'incluez pas `/dev` dans le nom du disque.
- Utilisez une partition existante. Par exemple pour créer la partition sur la première partition du premier disque dur IDE (`/dev/hda1`), spécifiez **`hda1`** comme partition. N'incluez pas `/dev` dans le nom de la partition.
- Formatez la partition comme le type de système de fichiers choisi.

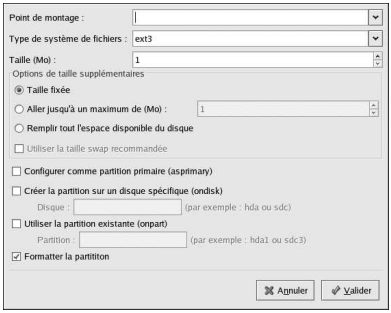

Figure 8-5. Création de partitions

Pour modifier une partition existante, sélectionnez-la dans la liste et cliquez sur le bouton **Éditer**. La même fenêtre **Options de partition** que celle apparaissant lors de l'ajout d'une partition (reproduite dans la Figure 8-5) s'affichera alors, à la différence près toutefois, qu'elle contient les valeurs de la partition sélectionnée. Modifiez les options de la partition et validez en cliquant sur **OK** pour valider.

Pour supprimer une partition existante, sélectionnez-la dans la liste et cliquez sur le bouton **Effacer**.

8.4.1.1. Création de partitions RAID logicielles

Pour obtenir davantage d'informations concernant RAID et ses différents niveaux, consultez le Chapitre 3. Des RAID 0, 1 et 5 peuvent être configurés.

Pour créer une partition RAID logicielle, suivez les étapes suivantes:

1. Cliquez sur le bouton **RAID**.
2. Sélectionnez **Créer une partition de logiciel RAID**.
3. Configurez les partitions de la façon décrite précédemment, mais sélectionnez cette fois-ci **RAID logiciel** en tant que type de système de fichiers. Vous devez également indiquer un disque dur sur lequel créer la partition ou à partir duquel utiliser une partition existante.

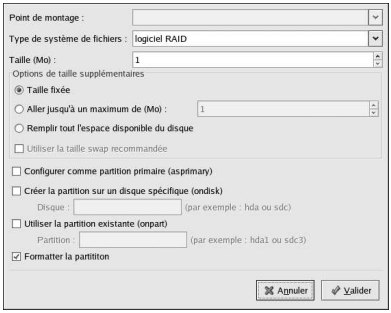

Figure 8-6. Création d'une partition RAID logicielle

Répétez ces étapes pour créer autant de partitions que n'en a besoin votre configuration RAID. Toutes vos partitions ne doivent pas obligatoirement être des partitions RAID.

Après avoir créé toutes les partitions nécessaires à la formation d'un périphérique RAID, suivez ces étapes:

1. Cliquez sur le bouton **RAID**.
2. Sélectionnez **Créer un périphérique RAID**.
3. Sélectionnez un point de montage, un type de système de fichiers, un nom de périphérique RAID, un niveau RAID, des membres RAID, un nombre d'éléments de rechange pour le périphérique RAID logiciel et indiquez si de périphérique RAID doit être formaté ou non.

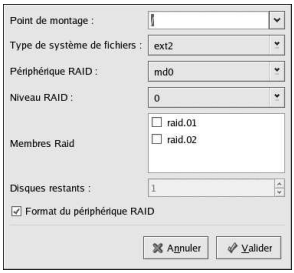

Figure 8-7. Création d'un périphérique RAID logiciel

4. Cliquez sur **OK** pour valider votre choix et ajouter le périphérique à la liste.

8.5. Configuration réseau

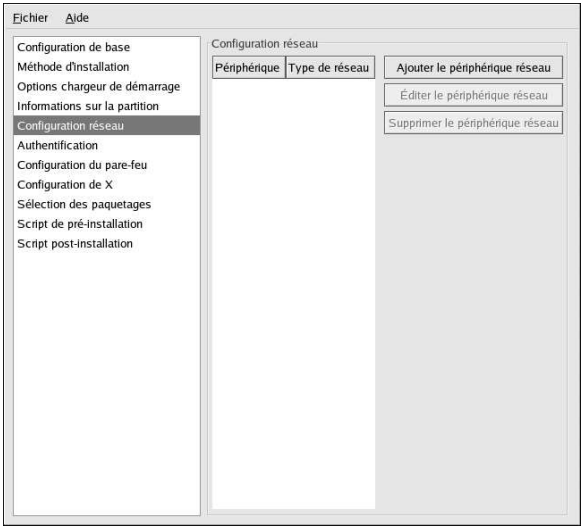

Figure 8-8. Configuration réseau

Si le système devant être installé via kickstart ne dispose pas d'une carte Ethernet, n'en configurer pas une sur la page **Configuration réseau**.

La mise en réseau n'est requise que si vous choisissez une méthode d'installation de type réseau (NFS, FTP ou HTTP). La mise en réseau peut être configurée après l'installation à l'aide de **Outil d'administration de réseau** (`redhat-config-network`). Reportez-vous au Chapitre 12 pour de plus amples informations.

Pour chaque carte Ethernet sur le système, cliquez sur **Ajouter un périphérique réseau** et sélectionnez le périphérique réseau et son type. Sélectionnez **eth0** comme périphérique réseau pour la première carte Ethernet, **eth1** pour la deuxième carte Ethernet et ainsi de suite.

8.6. Authentification

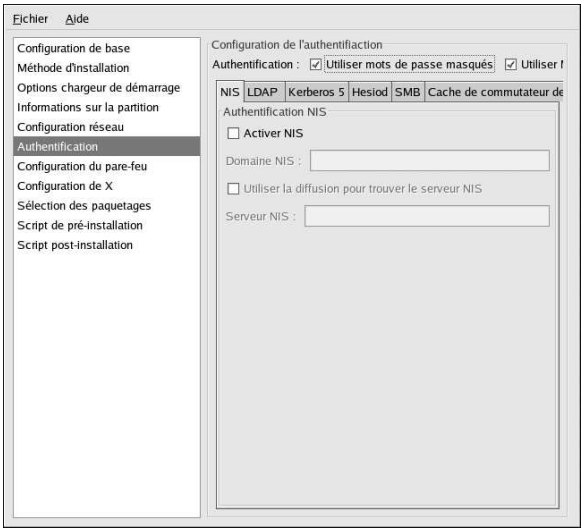

Figure 8-9. Authentification

Dans la section **Authentification**, décidez si vous voulez utiliser des mots de passe masqués et le cryptage MD5 pour les mots de passe utilisateur. Ces options sont fortement recommandées et sélectionnées par défaut.

Les options **Configuration de l'authentification** vous permettent de configurer les méthodes d'authentification suivantes:

- NIS
- LDAP
- Kerberos 5
- Hesiod
- SMB
- Cache de commutateur de nom

Ces méthodes ne sont pas activées par défaut. Pour activer une ou plusieurs de ces méthodes, cliquez sur l'onglet adéquat, cliquez sur la case de pointage située à côté de **Activer** et entrez les informations appropriées pour la méthode d'authentification.

8.7. Configuration du pare-feu

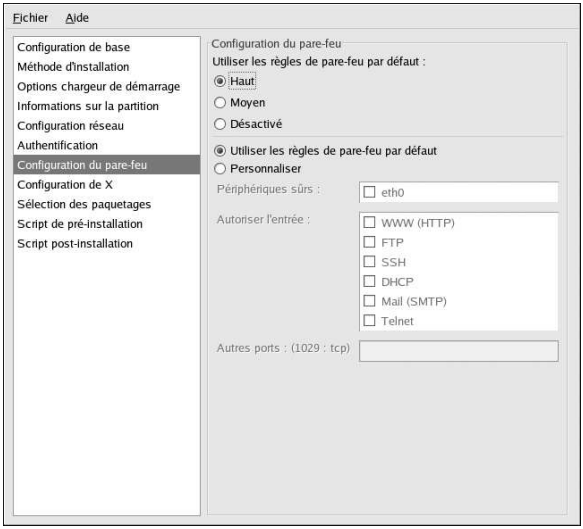

Figure 8-10. Configuration du pare-feu

La fenêtre **Configuration du pare-feu** est identique à l'écran du programme d'installation de Red Hat Linux ainsi que celle du **Outil de configuration du niveau de sécurité** et offre les mêmes fonctionnalités. Vous avez le choix entre les niveaux de sécurité **High** (élevé), **Medium** (moyen) et **Disabled** (désactivé). Reportez-vous à la Section 13.1 pour avoir des informations détaillées sur ces niveaux de sécurité.

8.8. Configuration de X Window

Si vous installez le système X Window, vous pouvez le configurer durant l'installation kickstart en sélectionnant l'option **Configurer le système X Window** dans la fenêtre **Configuration X** comme le montre la Figure 8-11. Si cette option n'est pas sélectionnée, les options de configuration de X Window seront désactivées et l'option `skipx` sera enregistrée dans le fichier kickstart.

8.8.1. Général

La première étape à franchir pour la configuration de X Window est le choix de l'intensité des couleurs et de la résolution par défaut. Sélectionnez-les depuis leur menu déroulant respectif. Assurez-vous de bien spécifier une intensité et une résolution compatibles avec votre carte vidéo et votre écran.

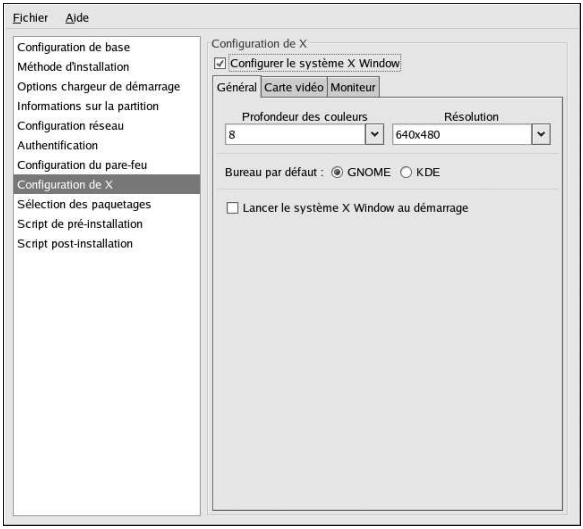

Figure 8-11. Configuration de X Window - Général

Si vous installez les bureaux GNOME et KDE, vous devez décider lequel des deux sera le bureau par défaut. Si vous n'installez qu'un seul bureau, n'oubliez pas de le choisir. Une fois le système installé, les utilisateurs pourront préciser leur choix de bureau par défaut. Pour en savoir plus sur GNOME et KDE, reportez-vous au *Guide d'installation de Red Hat Linux* et au *Guide de démarrage de Red Hat Linux*.

Ensuite, vous devez décider si vous voulez que X Window soit lancé au démarrage du système. Cette option permet de démarrer le système au niveau d'exécution 5 avec l'écran de connexion graphique. Après l'installation du système, ce paramètre peut être modifié en apportant des changements au fichier de configuration `/etc/inittab`.

8.8.2. Carte vidéo

Détecter la carte vidéo est sélectionné par défaut. Acceptez cette option si vous souhaitez que le programme d'installation recherche la carte vidéo pendant l'installation. Cette détection fonctionne pour la plupart des cartes vidéo modernes. Si vous sélectionnez cette option et que le programme d'installation ne parvient pas à trouver la carte vidéo, il s'arrêtera à l'écran de configuration de la carte vidéo. Pour continuer l'installation, sélectionnez votre carte vidéo dans la liste et cliquez sur **Suivant**.

Vous pouvez également sélectionner la carte vidéo dans la liste fournie avec l'onglet **Carte vidéo**, comme le montre la Figure 8-12. Spécifiez la quantité de mémoire vidéo (RAM) de la carte dans le menu déroulant **RAM de la carte vidéo**. Ces valeurs seront utilisées par le programme d'installation pour configurer le système X Window.

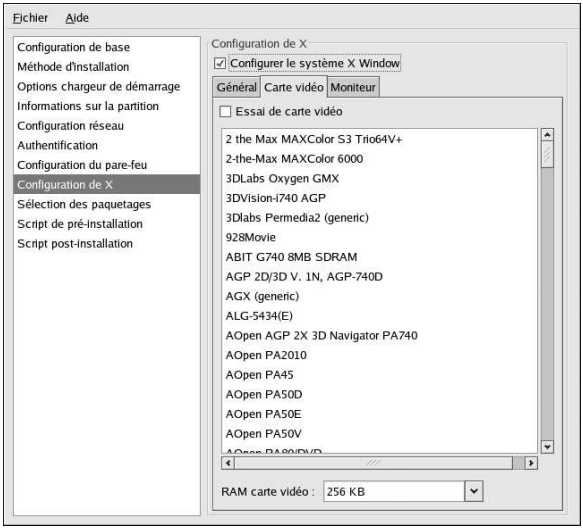

Figure 8-12. Configuration de X Window - Carte vidéo

8.8.3. Écran

Une fois la configuration de la carte vidéo terminée, cliquez sur l'onglet **Moniteur** comme le montre la Figure 8-13.

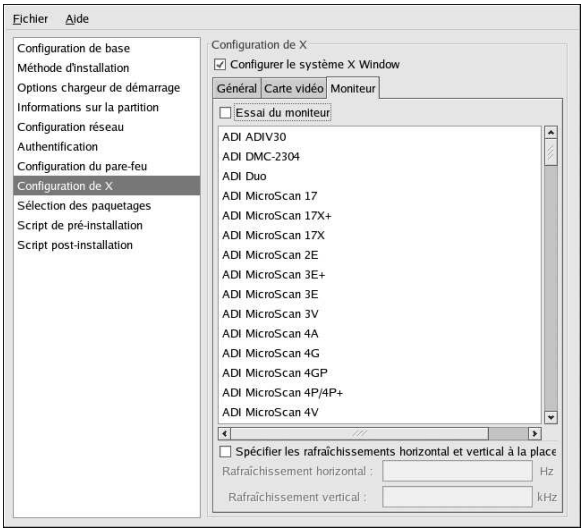

Figure 8-13. Configuration de X Window - Écran

Détecter le moniteur est sélectionné par défaut. Acceptez cette option si vous souhaitez que le programme d'installation recherche le moniteur pendant l'installation. Cette détection fonctionne pour la plupart des moniteurs modernes. Si vous sélectionnez cette option et que le programme d'installation ne parvient pas à détecter le moniteur, il s'arrêtera à l'écran de configuration du moniteur. Pour continuer l'installation, sélectionnez votre écran dans la liste et cliquez sur **Suivant**.

Vous pouvez également sélectionner votre moniteur dans la liste. Vous pouvez aussi indiquer les fréquences de synchronisation horizontale et verticale au lieu de spécifier un moniteur particulier en cochant l'option **Spécifier hysnc et vsync au lieu du moniteur**. Cette option est utile si votre moniteur n'apparaît pas dans la liste. Veuillez noter que lorsque cette option est activée, la liste de moniteurs est désactivée.

8.9. Sélection de paquetages

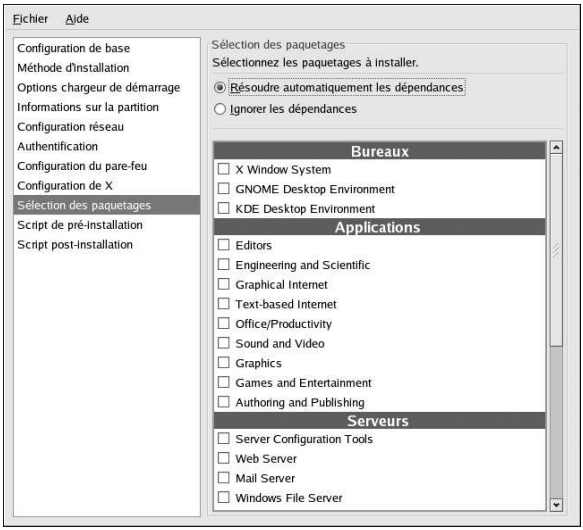

Figure 8-14. Sélection de paquetages

La fenêtre **Sélection des paquetages** vous permet de choisir les groupes de paquetages que vous désirez installer.

Il existe également des options permettant de résoudre ou d'ignorer automatiquement les dépendances de paquetages.

À l'heure actuelle, **Configuration de Kickstart** ne vous offre pas la possibilité de choisir des paquetages individuels. Si c'est pourtant ce que vous souhaitez faire, modifiez la section `%packages` (paquetages) du fichier kickstart après l'avoir enregistré. Reportez-vous à la la Section 7.5 pour de plus amples informations.

8.10. Script avant-installation

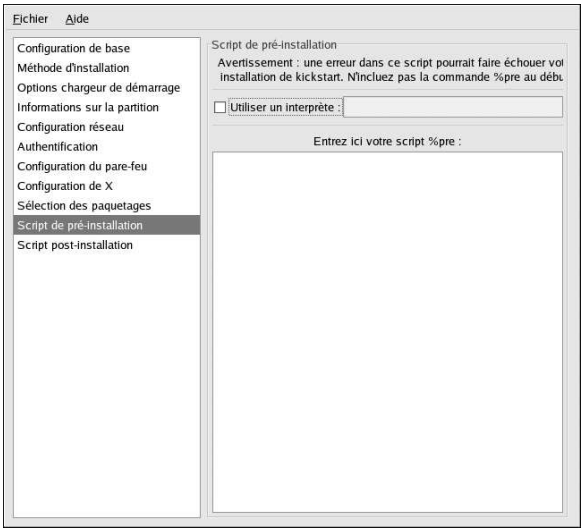

Figure 8-15. Script pré-installation

Vous pouvez ajouter des commandes devant être exécutées sur le système immédiatement après l'analyse syntaxique du fichier kickstart et avant que l'installation ne commence. Si vous avez correctement configuré le réseau dans le fichier kickstart, le réseau est activé avant le traitement de cette section. Si vous souhaitez ajouter un script après-installation, entrez-le dans la zone de texte.

Si vous souhaitez spécifier un langage de script à utiliser pour exécuter le script, sélectionnez l'option **Utiliser un interpréteur** et entrez l'interpréteur dans la zone de texte à côté de cette option. Par exemple, vous pouvez spécifier **`/usr/bin/python2.2`** pour un script Python. Cette option correspond en fait à l'utilisation de `%pre --interpreter` *`/usr/bin/python2.2`* dans votre fichier kickstart.

Attention

N'incluez pas la commande `%pre`. Elle sera en effet automatiquement ajoutée.

8.11. Script après-installation

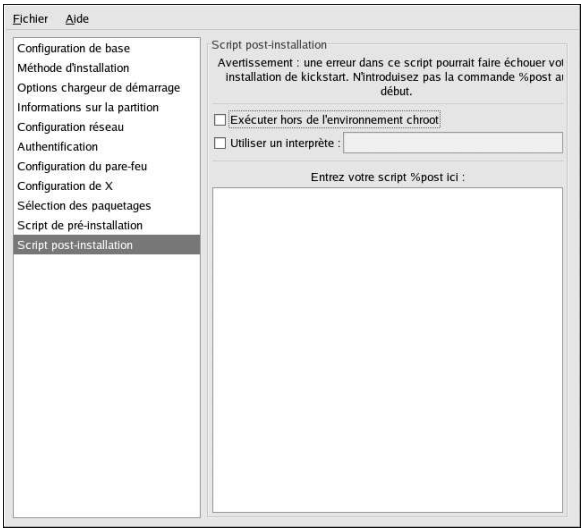

Figure 8-16. Script post-installation

Vous pouvez également ajouter des commandes devant être exécutées sur le système une fois l'installation terminée. Si vous avez correctement configuré le réseau dans le fichier kickstart, le réseau est activé et le script peut inclure des commandes permettant d'accéder à des ressources du réseau. Si vous souhaitez inclure un script après-installation, entrez-le dans la zone de texte.

Attention

N'incluez pas la commande `%post`. Elle sera en effet automatiquement ajoutée.

Par exemple, pour modifier le message du jour du nouveau système installé, ajoutez la commande ci-dessous dans la section `%post`:

```
echo "Hackers will be punished!" > /etc/motd
```

Astuce

Des exemples supplémentaires sont disponibles dans la Section 7.7.1.

8.11.1. Environnement chroot

Si vous désirez que votre script après installation s'exécute en dehors de l'environnement chroot, cochez la case qui se trouve près de cette option en haut de la fenêtre **Post-Installation**. Cette option correspond en fait à l'utilisation de l'option `--nochroot` dans la section `%post`.

Si vous désirez apporter des changements au système de fichiers nouvellement installé dans la section après-installation en dehors de l'environnement chroot, vous devez ajouter `/mnt/sysimage/` au nom du répertoire. .

Par exemple, si vous sélectionnez le bouton **Exécuter hors de l'environnement chroot**, l'exemple précédent doit être modifié de la façon indiquée ci-dessous:

```
echo "Hackers will be punished!" > /mnt/sysimage/etc/motd
```

8.11.2. Utilisation d'un interpréteur

Si vous souhaitez spécifier un langage de script à utiliser pour exécuter votre script, sélectionnez l'option **Utiliser un interpréteur** et entrez l'interpréteur dans la zone de texte à côté de cette option. Par exemple, vous pouvez spécifier **`/usr/bin/python2.2`** pour un script Python. Cette option correspond en fait à l'utilisation de `%post --interpreter` *`/usr/bin/python2.2`* dans votre fichier kickstart.

8.12. Enregistrement du fichier

Pour obtenir un aperçu du contenu du fichier kickstart, une fois votre choix d'options kickstart effectué, sélectionnez **Fichier => Aperçu** dans le menu déroulant.

Figure 8-17. Aperçu

Pour enregistrer le fichier kickstart, cliquez sur le bouton **Enregistrer dans le fichier** dans la fenêtre de l'aperçu. Pour enregistrer le fichier sans obtenir préalablement un aperçu de son contenu, sélectionnez **Fichier => Enregistrer le fichier** ou appuyez sur [Ctrl]-[S]. Une boîte de dialogue s'affichera alors vous permettant de choisir où enregistrer le fichier.

Après avoir enregistré le fichier, reportez-vous à la Section 7.10 pour avoir des instructions sur la façon de lancer l'installation kickstart.

Chapitre 9.

Restauration de base du système

En cas de problèmes, vous pouvez compter sur un certain nombre de méthodes pour vous aider à les résoudre. Toutefois, il est nécessaire de bien connaître le système pour pouvoir les utiliser. Ce chapitre illustre d'une part, les différentes façons qui vous permettent d'effectuer le démarrage en mode de secours et en mode mono-utilisateur et, d'autre part, la manière d'utiliser vos propres connaissances pour réparer le système.

9.1. Problèmes courants

Il se peut que, pour l'une des raisons suivantes, vous deviez démarrer votre système dans l'un de ces modes de restauration:

- Vous ne pouvez pas démarrer manuellement dans Red Hat Linux (niveau d'exécution 3 ou 5).
- Vous rencontrez des problèmes logiciels et matériels et vous souhaitez retirer un certain nombre de fichiers importants du disque dur de votre système.
- Vous avez oublié le mot de passe super-utilisateur (ou root).

9.1.1. Vous ne pouvez pas démarrer Red Hat Linux

Ce problème est souvent causé par l'installation d'un autre système d'exploitation après avoir installé Red Hat Linux. Certains système d'exploitation supposent que vous n'en avez pas d'autres sur votre ordinateur et écrasent le bloc de démarrage maître (MBR) qui contient les chargeurs de démarrage GRUB ou LILO. Si le chargeur de démarrage est écrasé de cette façon, il vous est impossible de démarrer Red Hat Linux, à moins que vous ne puissiez utiliser le mode de secours et reconfiguriez le chargeur de démarrage.

Ce problème peut également survenir lors de l'utilisation d'un outil de partitionnement pour redimensionner une partition ou créer une nouvelle partition à partir de l'espace libre restant après l'installation, ce qui peut entraîner la modification de l'ordre de vos partitions. Si le numéro de votre partition cette référence `/` change, le chargeur de démarrage ne pourra pas trouver pour monter la partition. Pour résoudre ce problème, démarrez le système en mode de secours et modifiez `/boot/grub/grub.conf` si vous utilisez GRUB ou `/etc/lilo.conf` si vous utilisez LILO. Vous *devez* exécuter la commande `/sbin/lilo` chaque fois que vous modifiez le fichier de configuration LILO.

9.1.2. Problèmes logiciels et matériels

Cette catégorie regroupe un grand éventail de situations différentes. Parmi ces dernières figurent une panne du disque dur et la spécification d'un périphérique root ou noyau non-valide dans le fichier de configuration du chargeur de démarrage. Dans l'une ou l'autre de ces situations, vous ne pourrez peut-être pas démarrer Red Hat Linux. Toutefois, si vous pouvez entrer en mode de restauration, vous arriverez peut-être à résoudre le problème ou du moins, à obtenir des copies de vos fichiers les plus importants.

9.1.3. Mot de passe root (ou super-utilisateur)

Que pouvez-vous faire si vous oubliez votre mot de passe root? Afin de créer un nouveau mot de passe, démarrez dans un mode de secours ou un mode mono-utilisateur et utilisez la commande `passwd` pour réinitialiser le mot de passe root.

9.2. Démarrage en mode de secours

Le mode de secours permet de démarrer un petit environnement Red Hat Linux entièrement à partir d'une disquette, d'un CD-ROM ou tout autre méthode de démarrage, au lieu d'utiliser le disque dur du système.

Comme son nom l'indique, ce mode est fourni pour vous porter secours lorsque vous en avez besoin. Lors d'une exécution normale, votre système Red Hat Linux utilise des fichiers situés sur le disque dur pour effectuer toutes ses tâches: exécution de programmes, stockage de fichiers, etc.

Cependant, il est parfois impossible de faire fonctionner Red Hat Linux suffisamment pour qu'il puisse accéder à ses fichiers sur le disque dur. Le mode de secours vous permet alors d'accéder aux fichiers stockés sur le disque dur et ce, même si vous ne pouvez exécuter Red Hat Linux depuis ce disque dur.

Pour démarrer en mode de secours, vous devez être en mesure de démarrer le système à l'aide d'une des méthodes suivantes:

- En démarrant le système à partir d'une disquette de démarrage d'installation créée d'après l'image `bootdisk.img`. [1]
- En démarrant le système à l'aide du CD-ROM de démarrage d'installation. [2]
- En démarrant le système à partir du CD-ROM 1 Red Hat Linux.

Une fois que vous avez démarré à l'aide de l'une des méthodes décrites ci-dessus, entrez la commande suivante à l'invite de démarrage de l'installation:

```
linuxrescue
```

Le système vous demande de répondre à quelques questions élémentaires telles que la langue que vous souhaitez utiliser. Il vous demande également de sélectionner l'endroit où se trouve une image de secours valide. Choisissez parmi les options suivantes: **CD-ROM local** , **Disque dur**, **Image NFS**, **FTP** ou **HTTP**. L'emplacement retenu doit contenir un arbre d'installation valide; cet arbre d'installation doit de plus, correspondre à la même version de Red Hat Linux que le CD-ROM 1 Red Hat Linux à partir duquel vous avez démarrer. Si vous avez utilisé un CD-ROM or disquette de démarrage pour lancer le mode de secours, l'arbre d'installation doit appartenir au même arbre que celui à partir duquel le support a été crée. Pour plus d'informations sur la configuration d'un arbre d'installation sur un disque dur, de serveur NFS, FTP ou HTTP, reportez-vous au *Guide d'installation de Red Hat Linux*.

Si vous avez sélectionné une image de secours qui ne nécessite pas de connexion réseau, le système vous demandera de préciser si vous souhaitez ou non, établir une connexion réseau. Cette dernière est utile si vous devez sauvegarder des fichiers sur un ordinateur différent ou si vous devez installez certains paquetages RPM à partir d'un emplacement réseau partagé, par exemple.

Le message suivant (en anglais) s'affichera à l'écran:

```
The rescue environment will now attempt to find your Red Hat
```

1. Pour créer une disquette de démarrage d'installation, insérez une disquette vierge et utilisez le fichier `images/bootdisk.img` du CD-ROM #1 Red Hat Linux avec la commande `dd if=bootdisk.img of=/dev/fd0`.
2. Pour créer un CD-ROM de démarrage d'installation, reportez-vous aux instructions contenues dans le *Guide d'installation de Red Hat Linux*.

```
Linux installation and mount it under the directory
/mnt/sysimage.  You can then make any changes required to your
system.  If you want to proceed with this step choose
'Continue'. You can also choose to mount your file systems
read-only instead of read-write by choosing 'Read-only'.
If for some reason this process fails you can choose 'Skip'
and this step will be skipped and you will go directly to a
command shell.
```

Si vous sélectionnez **Continuer**, il essaiera de monter votre système de fichiers sous le répertoire `/mnt/sysimage`. S'il ne parvient pas à monter une partition, il vous en informera. Si vous sélectionnez **Lecture-seule**, il essaiera de monter votre système de fichiers sous le répertoire `/mnt/sysimage`, mais en mode lecture seule. Si vous sélectionnez **Ignorer**, votre système de fichiers ne sera pas monté. Choisissez **Ignorer** si vous craignez que votre système de fichiers ne soit corrompu.

Une fois le système en mode de secours, l'invite suivante apparaît sur les consoles virtuelles (ou CV) 1 et 2 (utilisez la combinaison de touches [Ctrl]-[Alt]-[F1] pour accéder à la CV 1 et [Ctrl]-[Alt]-[F2] pour accéder à la CV 2):

```
-/bin/sh-2.05b#
```

Si vous avez sélectionné **Continuer** pour monter vos partitions de façon automatique et que vos partitions ont effectivement été montées, vous vous trouvez dans le mode mono-utilisateur.

Même si votre système de fichiers est monté, la partition root par défaut, sous le mode de secours, est une partition root temporaire, et non pas la partition root du système de fichiers utilisé durant un mode utilisateur normal (niveau d'exécution 3 ou 5). Si vous avez sélectionné de monter votre système de fichiers et il est monté avec succès, vous pouvez changer la partition root de l'environnement du mode de secours à la partition root de votre système de fichiers en exécutant la commande suivante:

```
chroot/mnt/sysimage
```

Ceci est utile si vous devez exécuter des commandes comme `rpm` qui nécessite que votre partition root soit montée en tant que `/`. Pour quitter l'environnement chroot, tapez `exit` et vous reviendrez à l'invite de la console.

Si vous avez sélectionné **Ignorer**, vous pouvez toujours essayer de monter une partition manuellement dans un mode de secours, en créant un répertoire comme */foo* et en tapant la commande suivante:

```
mount-text3/dev/hda5/foo
```

Dans la commande suivante, */foo* est un répertoire que vous avez créé et */dev/hda5* est la partition que vous souhaitez monter. Si la partition est de type `ext2`, remplacez `ext3` par `ext2`.

Si vous ne connaissez pas les noms de vos partitions, affichez-les à l'aide de la commande ci-dessous:

```
fdisk-l
```

Depuis l'invite, vous pouvez exécuter de nombreuses commandes utiles, comme:

- `list-harddrives` pour obtenir une liste des disques durs de votre système;
- `ssh`, `scp` et `ping` pour vérifier si la mise en réseau a eu lieu;
- `dump` et `restore` pour effectuer ces tâches, si les utilisateurs disposent de lecteurs de bandes;
- `parted` et `fdisk` pour effectuer la gestion des partitons;
- `rpm` pour effectuer l'installation ou la mise à niveau de logiciels;
- `joe` pour modifier les fichiers de configuration (Si vous entrez `joe`, `emacs`, `pico` ou `vi`, l'éditeur `joe` sera lancé.)

9.3. Démarrage en mode mono-utilisateur

L'un des avantage du mode mono-utilisateur est qu'il ne nécessite pas de disquette ou CD-ROM de démarrage; toutefois, il ne vous donne pas la possibilité de monter des systèmes de fichiers en lecture-seule et parfois même, ne vous permet pas de les monter du tout.

Dans un mode mono-utilisateur, votre ordinateur démarre au niveau d'exécution 1. Vos systèmes de fichiers locaux sont montés, mais votre réseau n'est pas activé. Vous avez un shell utilisable permettant la maintenance de votre système. Contrairement au mode de secours, le mode mono-utilisateur essayer automatiquement de monter votre système de fichiers; *n'utilisez pas* un mode mono-utilisateur si votre système de fichiers ne peut pas être monté de manière réussie. Vous ne pouvez pas utiliser un mode mono-utilisateur si le niveau d'exécution 1 sur votre système est corrompu.

Si votre système démarre, mais ne vous permet pas de vous connecter lorsque le démarrage est terminé, essayez le mode mono-utilisateur.

Si vous utilisez GRUB, suivez les étapes ci-dessous:

1. Si vous avez configuré un mot de passe GRUB, entrez `p` et tapez le mot de passe.
2. Sélectionnez le système **Red Hat Linux** avec la version de noyau que vous souhaitez démarrer et tapez `e` pour procéder à sa modification. Une liste d'éléments s'affichera dans le fichier de configuration pour le titre sélectionné.
3. Sélectionnez la ligne qui commence par `kernel` et entrez `e` pour la modifier.
4. Allez à la fin de la ligne et entrez **`single`** comme mot séparé (appuyez sur la [Barre espace] et ensuite tapez **`single`**). Appuyez sur [Entrée] pour sortir du mode de modification.
5. Vous êtes maintenant de nouveau à l'écran de GRUB. Tapez `b`pour démarrer le mode mono-utilisateur.

Si vous utilisez LILO, spécifiez l'une de ces options à l'invite de démarrage de LILO (si vous utilisez le chargeur de démarrage LILO graphique, appuyez sur [Ctrl]-[x] pour sortir de l'écran graphique et afficher l'invite `boot:`) tapez:

```
linuxsingle
```

9.4. Démarrage en mode d'urgence

En mode d'urgence, vous démarrez dans l'environnement le plus primaire qu'il existe. Le système de fichiers root est monté en lecture-seule et presque rien n'est configuré. Le avantage principal du mode d'urgence par rapport au mode mono-utilisateur est que les fichiers `init` ne sont pas chargés. Ainsi, si `init` est corrompu ou n'est pas fonctionnel, vous pouvez toujours monter des systèmes de fichiers pour récupérer les données qui pourraient être perdues lors d'une nouvelle installation.

Pour démarrer en mode d'urgence, utilisez la même méthode que celle décrite pour le mode mono-utilisateur dans la Section 9.3 mais à cette exception près: remplacez le mot-clé **`single`** par le mot-clé **`emergency`**.

Chapitre 10.

Configuration du RAID logiciel

Veuillez avant tout lire le Chapitre 3 qui vous fournit des informations sur RAID, compare le RAID matériel au RAID logiciel ainsi que les RAID 0, 1 et 5.

Le RAID logiciel peut être configuré durant l'installation graphique de Red Hat Linux ou au cours d'une installation kickstart. Ce chapitre examine la manière de configurer le RAID logiciel lors de l'installation, en utilisant l'interface **Disk Druid**.

Avant de créer un périphérique RAID, vous devez tout d'abord créer des partitions RAID en suivant les instructions suivantes:

1. À l'écran **Configuration du partitionnement de disque**, sélectionnez **Partitionnement manuel à l'aide de Disk Druid**.
2. Dans **Disk Druid**, choisissez **Nouveau** pour créer une nouvelle partition.
3. Vous ne pourrez pas entrer de point de montage (vous pourrez le faire lorsque vous aurez créé votre périphérique RAID).
4. Choisissez **RAID logiciel** dans le menu déroulant **Type de système de fichiers** comme indiqué dans la Figure 10-1.

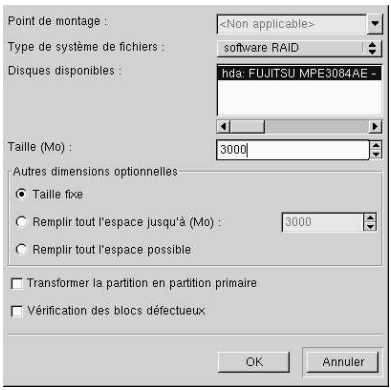

Figure 10-1. Création d'une nouvelle partition RAID

5. Pour **Disques disponibles**, sélectionnez le(s) disque (s) sur lequel(lesquels) RAID sera créé. Si vous avez plusieurs disques, ils seront tous sélectionnés, et vous devrez dé-sélectionner ceux qui ne contiendront *pas* de RAID.
6. Entrez la taille de la partition.
7. Sélectionnez **Taille fixée** pour donner à la partition la taille spécifiée, sélectionnez **Remplir tout l'espace jusqu'à (Mo)** et entrez une taille en Mo pour donner une fourchette pour la taille de la partition, ou sélectionnez **Remplir jusqu'à la taille autorisée maximale** si vous voulez que la partition occupe tout l'espace disponible sur le disque. Si plusieurs partitions peuvent occuper tout l'espace possible, celles-ci se répartiront entre elles l'espace disponible.

8. Sélectionnez **Forcer pour en faire la première partition** si vous souhaitez que la partition soit une partition primaire.
9. Sélectionnez **Vérifier les blocs défectueux** pour que le programme d'installation vérifie les blocs défectueux sur le disque dur avant de le formater.
10. Cliquez sur **OK** pour retourner à l'écran principal.

Répétez ces étapes pour toutes les partitions que vous devrez créer pour l'installation de RAID. Notez qu'il n'est pas nécessaire que toutes les partitions soient des partitions RAID. Par exemple, vous pouvez ne configurer que `/home` comme périphérique RAID logiciel.

Une fois que toutes vos partitions ont été créées en tant que partitions **RAID logicielles**, suivez les étapes ci-dessous:

1. Sélectionnez le bouton **RAID** à l'écran de partitionnement principal de **Disk Druid** (consulter la Figure 10-3).
2. Ensuite, la Figure 10-2 s'affichera et vous pourrez créer un périphérique RAID.

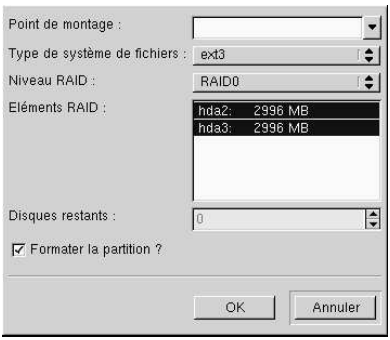

Figure 10-2. Création d'un périphérique RAID

3. Entrez un point de montage.
4. Choisissez ensuite le type de système de fichiers pour la partition.
5. Choisissez un nom de périphérique tel que **md0** pour le périphérique RAID.
6. Choisissez votre type de RAID. Vous pouvez choisir entre **RAID 0**, **RAID 1** et **RAID 5**.

Remarque

Si vous faites de `/boot`, une partition RAID, vous devez choisir RAID niveau 1 et utiliser l'un des deux premiers disques (d'abord IDE, puis SCSI). Si vous ne faites pas de `/boot` une partition RAID et que vous faites de `/` une partition RAID, vous devez choisir RAID niveau 1 et utiliser l'un des deux premiers disques (d'abord IDE, puis SCSI).

7. La partition RAID que vous venez de créer apparaît dans la liste **Éléments RAID**. Dans cette liste, sélectionnez la partition sur laquelle le périphérique RAID devrait être créé.
8. Si vous configurez RAID 1 ou RAID 5, spécifiez le nombre de partitions disponibles. Si une partition logicielle RAID ne peut-être créée, le disque restant sera automatiquement utilisé comme partition de remplacement. Pour tout disque restant que vous souhaiteriez créer, vous devez créer une partition RAID logicielle supplémentaire (en plus des partitions pour le périphérique

RAID). Dans l'étape précédente, sélectionnez les partitions pour le périphérique RAID et la ou les partition(s) pour le ou les disque(s) restant(s).

9. Après avoir cliqué sur **OK**, le périphérique RAID apparaîtra dans la liste **Résumé périphérique** comme il l'est montré dans la Figure 10-3. Maintenant, vous pouvez poursuivre l'installation. Pour plus d'informations, consultez le *Guide d'installation de Red Hat Linux*.

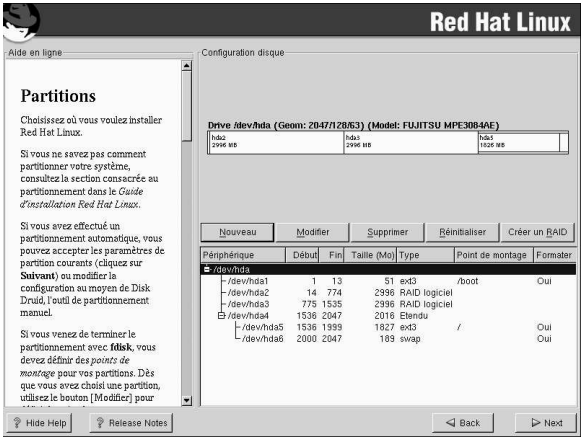

Figure 10-3. Dipositif RAID créé

Chapitre 11.

Configuration LVM

LVM peut être configuré au cours de l'installation graphique de Red Hat Linux ou d'une installation kickstart. Vous pouvez utiliser les utilitaires du paquetage `lvm` pour créer votre configuration LVM, mais ces instructions se concentrent sur l'utilisation de **Disk Druid** au cours de l'installation Red Hat Linux pour terminer cette tâche.

Consultez tout d'abord le Chapitre 4 afin d'obtenir davantage d'informations sur LVM. Ci-après figure un aperçu des étapes requises pour configurer LVM:

- créer des *volumes physiques* à partir des disques durs;
- créer des *groupes de volumes* à partir des volumes physiques;
- créer des *volumes logiques* à partir des groupes de volumes et affecter les points de montage des volumes logiques.

Remarque

Vous ne pouvez modifier les groupes de volumes LVM qu'en mode d'installation graphique. En mode d'installation texte, vous pouvez affecter des points de montage aux volumes logiques existants.

Pour créer un groupe de volumes logiques avec des volumes logiques lors de l'installation Red Hat Linux:

1. Sur l'écran **Paramétrage du partitionnement du disque**, sélectionnez **Partitionner manuellement à l'aide de Disk Druid**.
2. Sélectionnez **Nouveau**.
3. Vous ne pourrez pas entrer un point de montage (cela ne sera possible que lorsque vous aurez créé votre groupe de volumes).
4. Sélectionnez **volume physique (LVM)** dans le menu déroulant **Type de système de fichiers** comme cela est présenté dans la Figure 11-1.

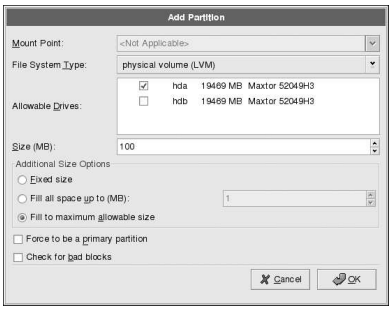

Figure 11-1. Création d'un volume physique

5. Un volume physique doit être limité à un lecteur. Pour **Lecteurs autorisés**, sélectionnez le lecteur sur lequel le volume physique sera créé. Si vous avez plusieurs lecteurs, ils seront tous sélectionnés, mais vous ne devrez en garder qu'un seul.
6. Entrez la taille souhaitée pour le volume physique.
7. Sélectionnez **Taille définie** afin que le volume physique soit à la taille souhaitée, sélectionnez **Remplir tout l'espace jusqu'à (Mo)** et entrez une taille en Mo afin de donner une plage de taille ou sélectionnez **Remplir jusqu'à taille maximum autorisée** pour qu'il se développe jusqu'à ce qu'il remplisse l'espace disponible sur le disque dur. Si vous sélectionnez cette dernière option pour plusieurs volumes physiques, ils se partageront l'espace disponible sur le disque.
8. Sélectionnez **Forcer pour en faire une partition primaire** si vous souhaitez que la partition soit une partition primaire.
9. Sélectionnez **Vérifier les blocs défectueux** si vous souhaitez que le programme d'installation recherche les mauvais blocs du disque avant de le formater
10. Cliquez sur **OK** pour retourner à l'écran principal.

Répétez ces étapes pour créer autant de volumes physique que nécessaire pour votre configuration LVM. Par exemple, si vous souhaitez que le groupe de volumes s'étende sur plusieurs lecteurs, créez un volume physique sur chacun des lecteurs.

Avertissement

La partition `/boot` ne peut pas se trouver sur un groupe de volumes car le chargeur d'amorçage ne peut pas le lire. Si vous souhaitez que votre partition root se trouve sur un volume logique, vous devrez créer une partition `/boot` séparée, qui ne fera pas partie d'un groupe de volumes.

Une fois que tous les volumes physiques sont créés, suivez les étapes suivantes:

1. Cliquez sur le bouton **LVM** afin de regrouper les volumes physiques dans des groupes de volumes. Un groupe de volumes est principalement un ensemble de volumes physiques. Vous pouvez avoir plusieurs groupes de volumes, mais un volume physique ne peut se trouver que dans un groupe de volumes.

Remarque

Le groupe de volumes logiques contient de l'espace disque de déperdition réservé. Il est possible que la somme des volumes physiques ne soit pas égale à la taille du groupe de volumes; la taille des volumes logiques indiquée est toutefois correcte.

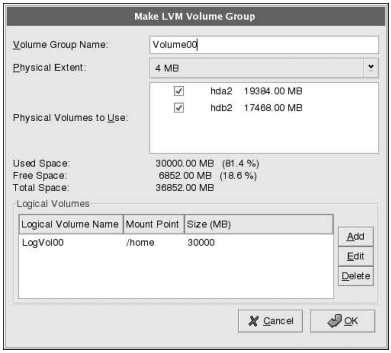

Figure 11-2. Création d'un périphérique LVM

2. Modifiez **Nom du groupe de volume** si vous le souhaitez.
3. Tous les volumes logiques du groupe de volumes doivent être situés dans des unités de *domaine physique*. Par défaut, le domaine physique est défini à 4 Mo; la taille des volumes logiques doit donc être divisible par 4 Mo. Si vous entrez une taille qui n'est pas un multiple de 4 Mo, le programme d'installation sélectionnera automatiquement la taille la plus proche par unités de 4 Mo. Nous vous recommandons de modifier ce paramètre.
4. Sélectionnez les volumes physiques à utiliser pour le groupe de volumes.
5. Créez des volumes logiques avec des points de montage tels que `/home`. N'oubliez pas que `/boot` ne peut pas être un volume logique. Pour ajouter un volume logique, cliquez sur le bouton **Ajouter** de la section **Volumes logiques**. Une fenêtre de dialogue semblable à celle reproduite dans la Figure 11-3 s'affiche.

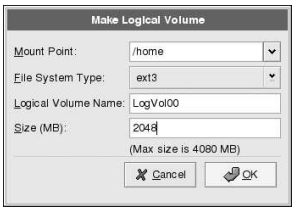

Figure 11-3. Création d'un volume logique

Répétez ces étapes pour chaque groupe de volumes que vous voulez créer.

Astuce

Vous pouvez laisser de l'espace libre dans le groupe de volumes logiques afin de pouvoir étendre ensuite les volumes logiques.

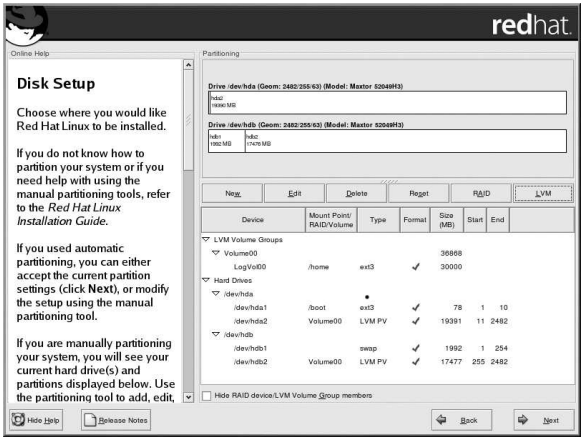

Figure 11-4. Volumes logiques créés

III. Informations relatives à la configuration du réseau

Ce chapitre fournit non seulement des informations sur la manière de configurer le réseau mais examine également des thèmes en relation avec la mise en réseau elle-même comme la manière permettant d'instaurer des connexions distantes, de partager des fichiers et répertoires sur le réseau et d'installer un serveur Web.

Table des matières

Chapitre 12.

Configuration du réseau

Pour communiquer avec d'autres ordinateurs, ces derniers ont besoin d'une connexion réseau. Il faut donc que le système d'exploitation reconnaisse une carte d'interface (Ethernet, modem RNIS ou anneau à jeton) et que l'interface à connecter au réseau soit configurée.

L'**Outil d'administration de réseau** permet de configurer les types d'interface réseau suivants:

- Ethernet
- RNIS
- modem
- xDSL
- anneau à jeton
- CIPE
- périphériques sans fil

Pour utiliser l'**Outil d'administration de réseau**, vous devez avoir des privilèges de super-utilisateur (ou root). Pour lancer l'application, sélectionnez le bouton **Menu principal** (sur le panneau) **=> Paramètres de système => Réseau**, ou tapez la commande `redhat-config-network` à l'invite du shell (dans un terminal **XTerm** ou **GNOME**par exemple). Si vous tapez la commande, la version graphique s'affiche si X est en cours d'exécution, sinon, la version basée sur le texte s'affiche. Pour forcer l'exécution de la version basée sur le texte, utilisez la commande `redhat-config-network-tui` command.

Figure 12-1. Outil d'administration de réseau

Si vous préférez modifier directement les fichiers de configuration, reportez-vous au *Guide de référence de Red Hat Linux* pour plus d'informations sur leur emplacement et leur contenu.

Astuce

Consultez à la liste de compatibilité matérielle Red Hat (http://hardware.redhat.com/hcl/) pour savoir si votre périphérique est pris en charge par Red Hat Linux.

12.1. Présentation

Pour configurer une connexion réseau avec l'**Outil d'administration de réseau**, suivez les étapes ci-dessous:

1. Ajoutez le périphérique matériel à la liste du matériel.
2. Ajoutez un périphérique réseau associé au périphérique matériel.
3. Configurez les paramètres de nom d'hôte et DNS.
4. Configurez tout hôte ne pouvant pas être pas être trouvés par l'intermédiaire de DNS.

Ce chapitre présente chacune de ces étapes pour chaque type de connexion réseau.

12.2. Mise en place d'une connexion Ethernet

Pour établir une connexion Ethernet, différents éléments sont nécessaires: une carte d'interface réseau, un câble réseau (généralement de type CAT5) ainsi qu'un réseau auquel se connecter. Différents réseaux sont configurés pour utiliser différentes vitesses de réseau; assurez-vous que votre carte est compatible avec le réseau auquel vous souhaitez vous connecter

Suivez les étapes suivantes afin d'ajouter une connexion Ethernet:

1. Cliquez sur l'onglet **Périphériques**.
2. Cliquez sur le bouton **Nouveau** dans la barre d'outils.
3. Sélectionnez **Connexion Ethernet** à partir de la liste **Type de périphérique** et cliquez sur **Suivant**.
4. Si vous avez déjà ajouté la carte d'interface réseau à la liste du matériel, sélectionnez-la à partir de la liste **Carte Ethernet**. Sinon, sélectionnez **Autre Carte Ethernet** afin d'ajouter le périphérique matériel.

   

   Remarque

   Le programme d'installation détecte généralement les périphériques Ethernet pris en charge et vous invite à les configurer. Si vous en avez configurés au cours de l'installation, ils apparaissent déjà dans la liste du matériel sur l'onglet **Matériel**.

5. Si vous avez sélectionné **Autre Carte Ethernet**, la fenêtre **Sélectionner adaptateur Ethernet** apparaît alors. Sélectionnez le fabricant ainsi que le modèle de la carte Ethernet, puis le nom du périphérique. S'il s'agit de la première carte Ethernet du système, sélectionnez **eth0** comme nom; s'il s'agit de la deuxième carte Ethernet, sélectionnez **eth1** (et ainsi de suite) L'**Outil d'administration de réseau** permet également de configurer les ressources pour la carte. Cliquez sur **Suivant** pour continuer.
6. Dans la fenêtre **Configurer les paramètres réseau**, comme le montre la Figure 12-2, choisissez entre DHCP et une adresse IP statique. Si le périphérique reçoit une adresse IP différente à chaque démarrage du réseau, n'indiquez pas de nom d'hôte. Cliquez sur **Suivant** pour continuer.

7. Cliquez sur **Appliquer** sur la page **Créer un périphérique Ethernet**.

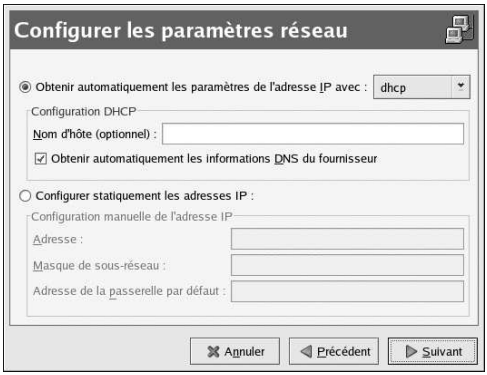

Figure 12-2. Paramètres Ethernet

Après configuration, le périphérique Ethernet apparaît dans la liste des périphériques, comme le montre la Figure 12-3.

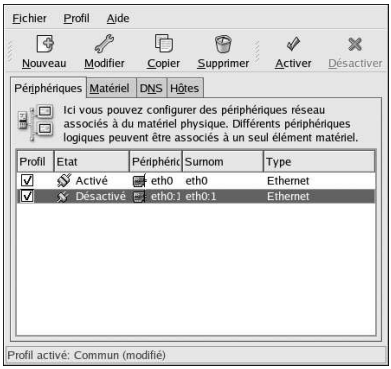

Figure 12-3. Périphérique Ethernet

Assurez-vous de bien sélectionner **Fichier => Enregistrer** afin d'enregistrer vos modifications.

Après avoir ajouté le périphérique Ethernet, vous pouvez modifier sa configuration en le sélectionnant dans la liste des périphériques puis en cliquant sur **Éditer**. Par exemple, lorsque le périphérique est ajouté, il est configuré pour être lancé par défaut lors du démarrage. Pour changer ce paramètre, choisissez d'éditer le périphérique, modifiez la valeur **Activer le périphérique au démarrage de l'ordinateur** et enregistrez les modifications.

Lorsque le périphérique est ajouté, il n'est pas activé immédiatement, comme le montre son statut **Inactif**. Afin d'activer le périphérique, sélectionnez-le dans la liste des périphériques et cliquez sur le bouton **Activer**. Si le système est configuré de telle sorte que le périphérique sera activé lors du démarrage de l'ordinateur (la valeur par défaut), il ne sera pas nécesaire de répéter cette étape à nouveau.

Si vous associez plus d'un périphériques à une carte Ethernet, ces périphériques sont des *alias de périphériques*. Un alias de périphériques vous permet de configurer de multiples périphériques virtuels pour un périphérique physique, dotant ainsi ce périphérique physique de plusieurs adresses IP. Par exemple, vous pouvez configurer un périphérique eth1 et un périphérique eth1:1. Pour de plus amples informations, reportez-vous à la Section 12.13.

12.3. Mise en place d'une connexion RNIS

Une connexion RNIS est une connexion Internet établie à l'aide d'une carte modem RNIS au travers d'une ligne téléphonique spéciale installée par la compagnie téléphonique. Les connexions RNIS sont populaires en Europe.

Suivez les étapes suivantes afin d'ajouter une connexion RNIS:

1. Cliquez sur l'onglet **Périphériques**.
2. Cliquez sur bouton **Nouveau** dans la barre d'outils.
3. Sélectionnez **connexion ISDN** à partir de la liste **Type de périphérique** et cliquez sur **Suivant**.
4. Sélectionnez la carte RNIS dans le menu déroulant. Configurez ensuite les ressources ainsi que le protocole de canal D pour cette carte. Cliquez sur **Suivant** pour continuer.

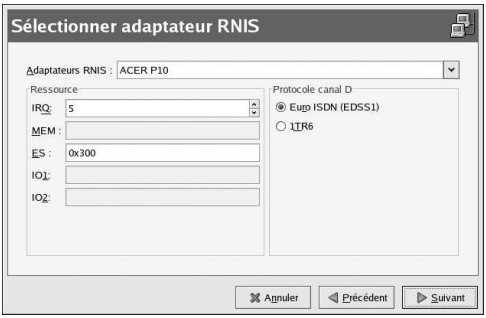

Figure 12-4. Paramètres RNIS

5. Si votre fournisseur d'accès Internet (FAI ou ISP de l'anglais 'Internet Service Provider') fait partie de la liste prè-configurée, sélectionnez-le. Sinon, fournissez les informations nécessaires sur votre compte FAI. Si vous ne connaissez pas les valeurs de ce dernier, contactez votre FAI. Cliquez alors sur **Suivant**.
6. Dans la fenêtre **Paramètres IP**, sélectionnez le **Mode d'encapsulation** et choisissez si vous voulez obtenir une adresse IP via DHCP ou si vous voulez en définir une de manière statique. Cliquez sur **Suivant** à la fin de ces opérations.
7. Sur la page **Créer connexion d'accès réseau**, cliquez sur **Appliquer**.

Après avoir configuré le périphérique ISDN, il apparaît dans la liste des périphériques en tant que périphérique de type **ISDN**, comme le montre la Figure 12-5.

Assurez-vous de bien sélectionner **Fichier => Enregistrer** afin d'enregistrer vos modifications.

Après avoir ajouté le périphérique ISDN, vous pouvez modifier sa configuration en sélectionnant le périphérique dans la liste des périphériques puis en cliquant sur **Éditer**. Par exemple, lorsque le périphériques est ajouté, il est configurer pour ne pas se lancer au démarrage par défaut. Éditez sa

configuration pour modifier de paramètre. D'autres éléments peuvent également être changés, tels que la compression, les options PPP, le nom de connexion, le mot de passe parmi tant d'autres.

Lorsque le périphérique est ajouté, il n'est pas activé immédiatement, comme le montre son statut **Inactif**. Afin d'activer le périphérique, sélectionnez-le dans la liste des périphériques et cliquez sur le bouton **Activer**. Si le système est configuré de telle sorte que le périphérique sera activé lors du démarrage de l'ordinateur (la valeur par défaut), il ne sera pas nécesaire de répéter cette étape à nouveau.

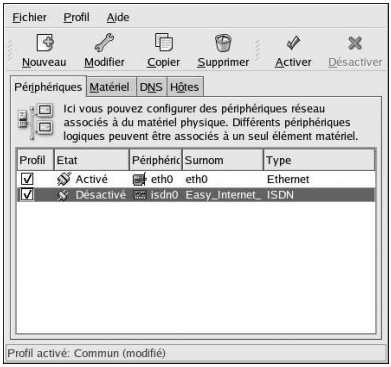

Figure 12-5. Périphérique RNIS

12.4. Mise en place d'une connexion modem

Un modem peut être utilisé pour configurer une connexion Internet sur une ligne téléphonique active. Un compte de fournisseur d'accès Internet est requis.

Suivez les étapes suivantes afin d'ajouter une connexion modem:

1. Cliquez sur l'onglet **Périphériques**.
2. Cliquez sur le bouton **Nouveau** dans la barre d'outils.
3. Sélectionnez **Connexion par Modem** à partir de la liste **Type de périphérique** et cliquez sur **Suivant**.
4. Si un modem est déjà configuré dans la liste du matériel (sous l'onglet **Matériel**), l'**Outil d'administration de réseau** suppose que vous voulez l'utiliser pour établir une connexion modem. Si aucun modem n'est déjà configuré, il essaie de détecter des modems dans le système. Cette opération peut prendre un certain temps. Si aucun modem n'est détecté, un message apparaît pour vous avertir que les paramètres affichés ne correspondent pas aux valeurs obtenues par l'opération de détection.
5. Après la détection, la fenêtre reproduite dans la Figure 12-6 apparaît.

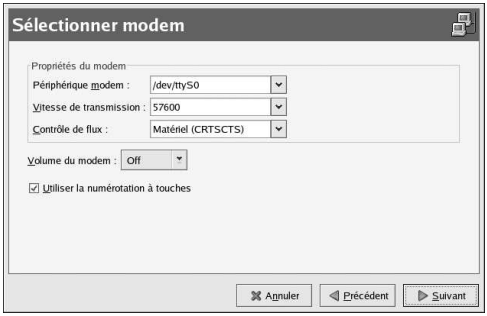

Figure 12-6. Paramètres du modem

6. Configurez le périphérique du modem, taux de baud, le taux de transmission et volume du modem. Si vous ne connaissez pas ces valeurs, acceptez les valeurs par défaut si le modem a été détecté par le système. Si vous ne disposez pas de la numérotation à touche, annulez la sélection dans la case de pointage lui correspondant. Cliquez ensuite sur **Suivant**.
7. Si votre FAI fait partie de la liste préconfigurée, sélectionnez-le. Sinon, fournissez les informations nécessaires sur votre compte FAI. Si vous ne connaissez pas ces valeurs, contactez votre FAI. Cliquez ensuite sur **Suivant**.
8. Dans la page **Paramètres IP**, sélectionnez si vous souhaitez obtenir votre adresse IP via DHCP ou si vous préférez la configurer de manière statique. Cliquez ensuite sur **Suivant** un fois ces opérations terminées.
9. Sur la page **Créer connexion d'accès réseau**, cliquez sur **Appliquer**.

Après avoir configuré le périphérique du modem, il apparaît dans la liste des périphériques en tant que type `Modem`, comme le montre la Figure 12-7.

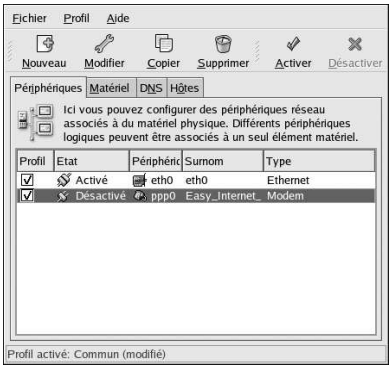

Figure 12-7. Périphérique modem

Assurez-vous de bien sélectionner **Fichier => Enregistrer** afin d'enregistrer vos modifications.

Après avoir ajouté le périphérique modem, vous pouvez modifier sa configuration en le sélectionnant dans la liste des périphériques puis en cliquant sur **Éditer**. Par exemple, lorsque le périphérique est ajouté, il est par défaut configuré pour ne pas être lancé lors du démarrage. Modifiez sa configuration

afin de changer ce paramètre. De nombreuses options, telles que la compression, les options PPP, le nom de connexion, le mot de passe, etc. peuvent également être modifiées.

Lorsque le périphérique est ajouté, il n'est pas activé immédiatement, comme le montre son statut **Inactif**. Afin d'activer le périphérique, sélectionnez-le dans la liste des périphériques et cliquez sur le bouton **Activer**. Si le système est configuré de telle sorte que le périphérique sera activé lors du démarrage de l'ordinateur (la valeur par défaut), il ne sera pas nécesaire de répéter cette étape à nouveau.

12.5. Mise en place d'une connexion xDSL

DSL signifie 'Digital Subscriber Lines' (lignes d'abonnés numériques). Il existe différents types de DSL, notamment ADSL, IDSL et SDSL. Le terme xDSL employé par l'**Outil d'administration de réseau** regroupe tous les types de connexions DSL.

Certains fournisseurs DSL demandent que vous configuriez votre système afin d'obtenir une adresse IP par DHCP via une carte Ethernet, alors que d'autres vous demandent de configurer avec une carte Ethernet une connexion PPPoE (Point-to-Point Protocol over Ethernet), un protocole point à point sur Ethernet. Demandez à votre fournisseur DSL quelle méthode utiliser.

Si vous devez utiliser DHCP, reportez-vous à la Section 12.2 afin de configurer votre carte Ethernet.

Suivez les étapes suivantes si vous devez utiliser PPPoE:

1. Cliquez sur l'onglet **Périphériques**.
2. Cliquez sur le bouton **Nouveau**.
3. Sélectionnez **Connexion xDSL** à partir de la liste **Type de périphérique** et cliquez sur **Suivant**.
4. Si votre carte Ethernet se trouve déjà dans la liste de matériel, sélectionnez **Périphérique Ethernet** à partir du menu déroulant de la page présentée dans la Figure 12-8. Sinon, la fenêtre **Sélectionner adaptateur Ethernet** apparaît.

Remarque

Le programme d'installation détecte généralement les périphériques Ethernet pris en charge et vous invite à les configurer. Si vous en avez configurés au cours de l'installation, ils apparaissent déjà dans la liste du matériel sur l'onglet **Matériel**.

Figure 12-8. Paramètres xDSL

5. Si la fenêtre **Sélectionner adaptateur Ethernet** apparaît, sélectionnez le fabricant ainsi que le modèle de la carte Ethernet, puis le nom du périphérique. S'il s'agit de la première carte Ethernet du système, sélectionnez **eth0** comme nom de périphérique; s'il s'agit de la deuxième, sélectionnez **eth1** (et ainsi de suite). L'**Outil d'administration de réseau** vous permet également de configurer les ressources pour la carte. Cliquez sur **Suivant** pour continuer.
6. Entrez le **Nom du fournisseur**, **Nom de connexion**, (login) et **Mot de passe**. Si vous avez un compte T-Online, au lieu d'entrer **Nom de connexion** et **Mot de passe** dans la fenêtre par défaut, cliquez sur le bouton **Configuration du compte T-Online** et rentrez les informations requises. Cliquez sur **Suivant** pour continuer.
7. Sur la page **Créer connexion DSL**, cliquez sur **Appliquer**.

Après configuration, la connexion DSL apparaît dans la liste des périphériques, comme le montre la Figure 12-7.

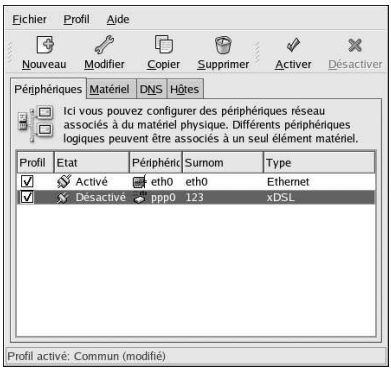

Figure 12-9. Périphérique xDSL

Assurez-vous de bien sélectionner **Fichier => Enregistrer** afin d'enregistrer vos modifications.

Après avoir ajouté la connexion xDSL, vous pouvez modifier sa configuration en sélectionnant le périphérique dans la liste des périphériques puis en cliquant sur **Éditer**. Par exemple, lorsque le périphérique est ajouté, il est par défaut configuré pour ne pas être lancé lors du démarrage. Modifiez sa configuration afin de changer ce paramètre.

Lorsque le périphérique est ajouté, il n'est pas activé immédiatement, comme le montre son statut **Inactif**. Afin d'activer le périphérique, sélectionnez-le dans la liste des périphériques et cliquez sur le bouton **Activer**. Si le système est configuré de telle sorte que le périphérique sera activé lors du démarrage de l'ordinateur (la valeur par défaut), il ne sera pas nécesaire de répéter cette étape à nouveau.

12.6. Mise en place d'une connexion de bus annulaire à jeton

Un réseau de bus annulaire à jeton est un réseau ('Token Ring' en anglais) auquel tous les ordinateurs sont connectés sur un modèle circulaire. Un *jeton*, ou un paquet spécial de réseau, voyage autour d'un bus annulaire à jeton et permet ainsi aux ordinateurs de se transmettre des informations.

Astuce

Pour plus d'informations sur l'utilisation du bus annulaire à jeton sous Linux, reportez-vous au site Web *Linux Token Ring Project* à l'adresse: http://www.linuxtr.net/.

Suivez les étapes suivantes afin d'ajouter un bus annulaire à jeton:

1. Cliquez sur l'onglet **Périphériques**.
2. Cliquez sur le bouton **Nouveau** dans la barre d'outils.
3. Sélectionnez **Connexion Token Ring** à partir de la liste **Type de périphérique** et cliquez sur **Suivant**.
4. Si vous avez déjà ajouté la carte de bus annulaire à jeton à la liste du matériel, sélectionnez-la à partir de la liste **Carte Token Ring**. Sinon, sélectionnez **Autre carte Token Ring** afin d'ajouter le périphérique matériel.
5. Si vous avez sélectionné **Autre carte Token Ring**, la fenêtre **Sélectionner un adaptateur Token Ring** apparaît alors, comme le montre la Figure 12-10. Sélectionnez le fabricant ainsi que le modèle de la carte puis le nom du périphérique. S'il s'agit de la première carte de bus annulaire à jeton du système, sélectionnez **tr0**; s'il s'agit de la deuxième, sélectionnez **tr1** (et ainsi de suite). L'**Outil d'administration de réseau** permet également à l'utilisateur de configurer les ressources pour l'adaptateur. Cliquez sur **Suivant** pour continuer.

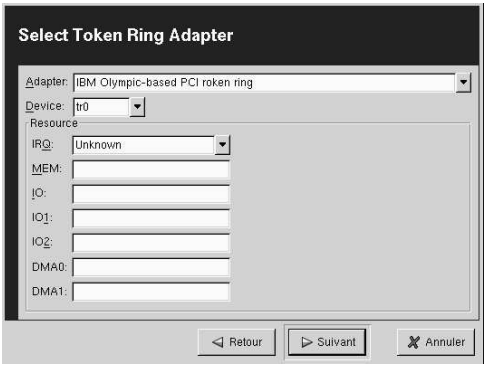

Figure 12-10. Paramètres du bus annulaire à jeton ('Token Ring')

6. Sur la page **Configurer paramètres réseau**, choisissez entre DHCP et une adresse IP statique. Vous pouvez également spécifier un nom d'hôte pour le périphérique. Si celui-ci reçoit une adresse IP dynamique à chaque démarrage du réseau, n'indiquez pas de nom d'hôte. Cliquez sur **Suivant** pour continuer.
7. Cliquez sur **Appliquer** sur la page **Créer Périphérique Token Ring**.

Après configuration, le périphérique de bus annulaire à jeton apparaît dans la liste des périphériques, comme le montre la Figure 12-11.

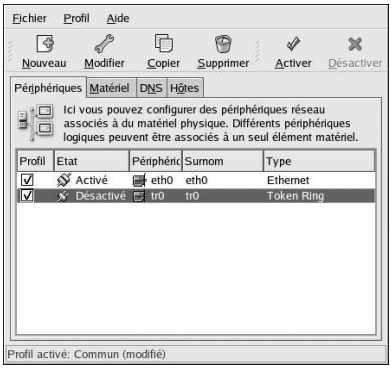

Figure 12-11. Périphérique de bus annulaire à jeton ('Token Ring')

Assurez-vous de bien sélectionner **Fichier => Enregistrer** afin d'enregistrer vos modifications.

Après avoir ajouté le périphérique, vous pouvez modifier sa configuration en le sélectionnant dans la liste des périphériques puis en cliquant sur **Éditer**. Vous pouvez par exemple indiquer s'il doit être lancé lors du démarrage.

Lorsque le périphérique est ajouté, il n'est pas activé immédiatement, comme le montre son statut **Inactif**. Afin d'activer le périphérique, sélectionnez-le dans la liste des périphériques et cliquez sur le bouton **Activer**. Si le système est configuré de telle sorte que le périphérique sera activé lors du

démarrage de l'ordinateur (la valeur par défaut), il ne sera pas nécesaire de répéter cette étape à nouveau.

12.7. Mise en place d'une connexion CIPE

CIPE est l'abréviation de 'Crypto IP Encapsulation'. Cette encapsulation sert à configurer un périphérique de 'tunnellisation' IP. CIPE peut par exemple être utilisée pour autoriser l'accès du monde extérieur à un réseau privé virtuel. Si vous devez configurer un périphérique CIPE, contactez votre administrateur système afin qu'il vous communique les valeurs appropriées.

Figure 12-12. Paramètres CIPE

Astuce

Pour obtenir de plus amples informations sur CIPE et sa configuration, reportez-vous au *Guide de sécurité de Red Hat Linux*.

12.8. Mise en place d'une connexion sans fil

Les périphériques Ethernet sans fil deviennent de plus en plus populaires. Leur configuration est semblable à la configuration Ethernet, mis à part qu'elle vous permet de configurer des paramètres tels que le ESSID et la clé de votre périphérique sans fil.

Suivez les étapes suivantes afin d'ajouter une connexion Ethernet sans fil:

1. Cliquez sur l'onglet **Périphériques**.
2. Cliquez sur le bouton **Suivant** dans la barre d'outils.

3. Sélectionnez **Connexion sans fil** à partir de la liste **Type de périphérique** et cliquez sur **Suivant**.
4. Si vous avez déjà ajouté la carte d'interface de réseau sans fil à la liste du matériel, sélectionnez-la à partir de la liste **Carte sans fil**. Sinon, sélectionnez **Autre carte sans fil** afin d'ajouter le périphérique matériel.

Remarque

>Le programme d'installation détecte généralement les périphériques Ethernet sans fil pris en charge et vous invite à les configurer. Si vous en avez configurés au cours du programme d'installation, ils apparaissent déjà dans la liste du matériel sur l'onglet **Matériel**.

5. Si vous avez sélectionné **Autre Carte sans fil**, la fenêtre **Sélectionner adaptateur Ethernet** apparaît alors. Sélectionnez le fabricant ainsi que le modèle de la carte Ethernet, puis le périphérique. S'il s'agit de la première carte Ethernet du système, sélectionnez **eth0**; s'il s'agit de la deuxième, sélectionnez **eth1** (et ainsi de suite). L'**Outil d'administration de réseau** permet également à l'utilisateur de configurer les ressources pour la carte d'interface réseau sans fil. Cliquez sur **Suivant** pour continuer.
6. Sur la page **Configurer connexion sans fil** comme le montre la Figure 12-13, configurez les paramètres pour le périphérique sans fil.

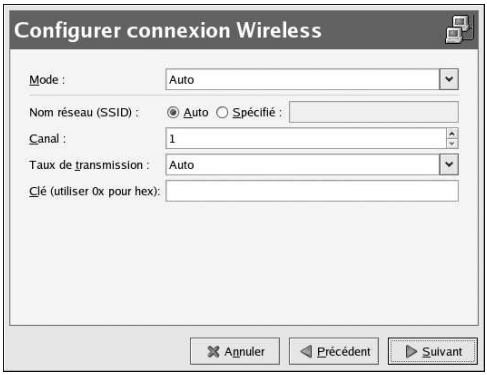

Figure 12-13. Paramètres de connexions sans fil

7. Sur la page **Configurer paramètres réseau**, choisissez entre DHCP et une adresse IP statique. Vous pouvez également spécifier un nom d'hôte pour le périphérique. Si celui-ci reçoit une adresse IP dynamique à chaque démarrage du réseau, n'indiquez pas de nom d'hôte. Cliquez sur **Suivant** pour continuer.
8. Cliquez sur **Appliquer** sur la page **Créer périphérique sans fil**.

Après configuration, le périphérique sans fil apparaît dans la liste des périphériques, comme le montre la Figure 12-14.

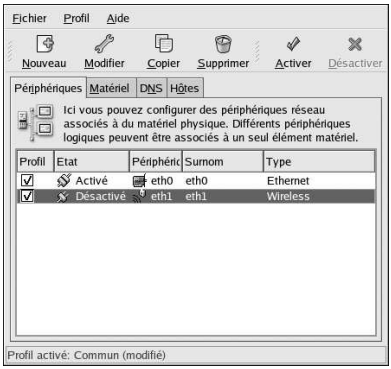

Figure 12-14. Périphérique sans fil

Assurez-vous de bien sélectionner **Fichier => Enregistrer** afin d'enregistrer vos modifications.

Après avoir ajouté le périphérique sans fil, vous pouvez modifier sa configuration en le sélectionnant dans la liste des périphériques puis en cliquant sur **Éditer**. Par exemple, vous pouvez le configurer pour qu'il soit activé lors du démarrage.

Lorsque le périphérique est ajouté, il n'est pas activé immédiatement, comme le montre son statut **Inactif**. Afin d'activer le périphérique, sélectionnez-le dans la liste des périphériques et cliquez sur le bouton **Activer**. Si le système est configuré de telle sorte que le périphérique sera activé lors du démarrage de l'ordinateur (la valeur par défaut), il ne sera pas nécesaire de répéter cette étape à nouveau.

12.9. Gestion des paramètres DNS

L'onglet **DNS** vous permet de configurer le nom d'hôte du système, son domaine, ses serveurs de noms ainsi que le domaine de recherche. Les serveurs de noms sont utilisés pour la recherche d'hôtes supplémentaires sur le réseau.

Si le serveur de noms DNS est récupéré de DHCP ou PPPoE (ou bien à partir du fournisseur d'accès Internet), n'ajoutez pas de serveurs DNS principaux, secondaires ou tertiaires.

Si le nom d'hôte est récupéré dynamiquement de DHCP ou PPPoE (ou bien à partir du fournisseur d'accès Internet), ne le changez pas.

Figure 12-15. Configuration DNS

Remarque

La section des serveurs de noms ne configure pas le système comme serveur de noms. À la place, il configure les serveurs de noms à utiliser lors de la résolution de l'adresse IP avec le nom d'hôte et vice versa.

12.10. Gestion des hôtes

L'onglet **Hosts** vous permet d'ajouter, de modifier ou de supprimer des hôtes du fichier `/etc/hosts`. Celui-ci contient les adresses IP ainsi que les noms d'hôtes correspondants.

Lorsque votre système tente de convertir un nom d'hôte en une adresse IP ou de déterminer le nom d'hôte pour une adresse IP, il se réfère au fichier `/etc/hosts` avant d'utiliser les serveurs de noms (si vous utilisez la configuration Red Hat Linux par défaut). Si l'adresse IP est répertoriée dans le fichier `/etc/hosts`, les serveurs de noms ne sont pas utilisés. Si votre réseau comporte des ordinateurs dont les adresses IP ne sont pas répertoriées dans DNS, nous vous recommandons de les ajouter au fichier `/etc/hosts`.

Pour ajouter une entrée au fichier `/etc/hosts` utilisez l'onglet **Hôtes**, cliquez sur le bouton **Nouveau** dans la barre d'outils et fournissez les informations requises avant de cliquer sur **OK**. Sélectionnez **Fichier => Enregistrer** ou pressez sur les touches [Ctrl]-[S] pour enregistrer les modifications dans le fichier `/etc/hosts`. Le réseau ou les services du réseau n'ont pas à être relancés étant donné que le système fait appel à la version courante du fichier lors de chaque résolution d'adresse.

Avertissement

Ne supprimez pas l'entrée `localhost`. Même si le système n'a pas de connexion réseau ou a une connexion réseau permanente, certains programmes doivent se connecter au système via l'interface de bouclage ('loopback') de l'hôte local.

Figure 12-16. Configuration des hôtes

Astuce

Pour modifier l'ordre de recherche, modifiez le fichier `/etc/host.conf` La ligne `order hosts, bind` spécifie que `/etc/hosts` a la priorité sur les serveurs de noms. Si vous changez la ligne en `order bind, hosts` vous configurez votre système afin qu'il utilise tout d'abord les serveurs de noms pour la conversion des noms d'hôte ainsi que des adresses IP. Si l'adresse IP ne peut pas être convertie par l'intermédiaire des serveurs de noms, le système recherche alors l'adresse IP dans le fichier `/etc/hosts`.

12.11. Activation des périphériques

Les périphériques réseau peuvent être configurés pour être activés ou désactivés au démarrage. ou non. Par exemple, un périphérique réseau pour une connexion modem n'est généralement pas configuré pour être lancé au démarrage, contrairement à une connexion Ethernet qui elle, l'est généralement. Si votre périphérique réseau est configuré pour ne pas être lancé au démarrage, vous pouvez utiliser le programme **Red Hat Control Network** afin de l'activer après le démarrage. Pour le lancer, sélectionnez le bouton **Menu principal** (sur le panneau) **=> Outils de système => Contrôle réseau de périphérique** ou tapez la commande `redhat-control-network`.

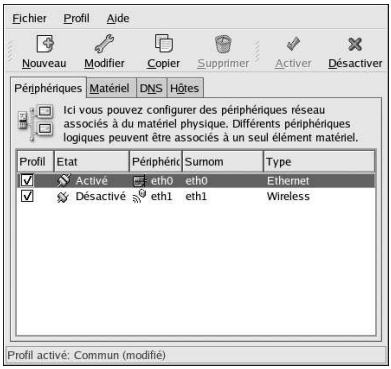

Figure 12-17. Activation des périphériques

Pour activer un périphérique, sélectionnez-le dans la liste des périphériques puis cliquez sur le bouton **Activer**. Pour l'arrêter, sélectionnez-le dans la liste puis cliquez sur **Désactiver**.

Si plusieurs profils réseau sont configurés, ils sont énumérés dans l'interface et peuvent être activés. Reportez-vous à la Section 12.12 pour obtenir de plus amples informations.

12.12. Travail avec des profils

Plusieurs périphériques réseau logiques peuvent être créés pour chaque périphérique matériel physique. Par exemple, si vous avez une carte Ethernet dans votre système (eth0), vous pouvez créer des périphériques réseau logiques avec différents surnoms et différentes options de configuration, tous associés à eth0.

Les périphériques réseau logiques sont différents des alias de périphériques. Les périphériques réseau logiques associés au même périphérique physique doivent exister dans différents profils et ne peuvent pas être activés simultanément. Les alias de périphériques sont également associés au même périphérique matériel, mais les alias de périphériques associés au même matériel peuvent être activés en même temps. Reportez-vous à la Section 12.13 afin d'obtenir de plus amples informations sur la création d'alias de périphériques.

Les *profils* peuvent être utilisés pour créer plusieurs ensembles de configuration pour différents réseaux. Un ensemble de configuration peut inclure des périphériques logiques tels que les hôtes et des paramètres DNS. Après la configuration des profils, vous pouvez utiliser l'**Outil d'administration de réseau** afin de passer de l'un à l'autre.

Par défaut, il existe un profil appelé **Commun**. Pour créer un nouveau profil sélectionnez **Profil** => **Nouveau** dans le menu déroulant puis entrez un nom unique pour le profil.

Vous modifiez maintenant le nouveau profil, comme l'indique la barre de statut en bas de la fenêtre principale.

Cliquez sur le périphérique figurant déjà dans la liste et sélectionnez le bouton **Copier** pour copier le périphérique existant sur un périphérique réseau logique. Si vous utilisez le bouton **Nouveau**, un alias de réseau sera créé, ce qui n'est pas correct. Pour changer les propriétés du périphérique logique, sélectionnez-le parmi la liste puis cliquez sur **Éditer**. Par exemple, le surnom peut être changé en un nom plus parlant, comme **`eth0_office`**, afin qu'il puisse être plus facilement identifiable.

Dans la liste des périphériques figure une colonne de cases de pointage intitulée **Profil**. Vous pouvez cocher ou décocher des périphériques pour chaque profil. Seuls les périphériques cochés sont inclus pour le profil actuellement sélectionné. Par exemple, si vous créez un périphérique logique nommé **`eth0_office`** dans un profil nommé **`Office`** et que vous voulez activer le périphérique logique si

le profil est sélectionné, annulez la sélection du périphérique `eth0` et retenez à la place le périphérique `eth0_office`.

Par exemple, la Figure 12-18 montre un profil appelé **Office** avec le périphérique logique **eth0_office**. Il est configuré pour activer la première carte Ethernet à l'aide de DHCP.

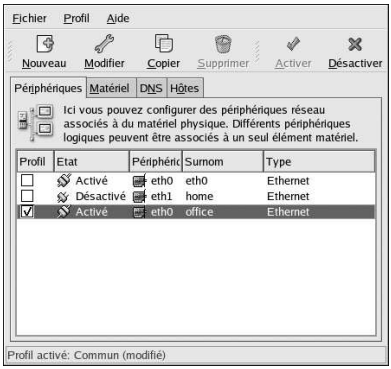

Figure 12-18. Profil Office

Veuillez noter que le profil **Home** figurant dans la Figure 12-19 active le périphérique logique **eth0_home** qui est associé à `eth0`.

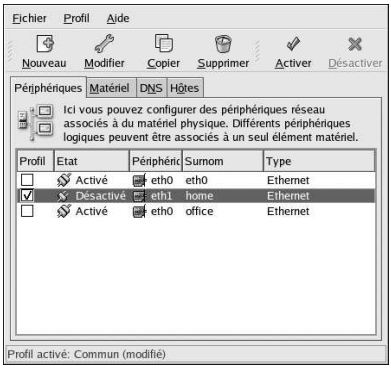

Figure 12-19. Profil Home

Vous pouvez également configurer `eth0` de façon à ce qu'il ne soit activé que dans le profil **Office** et n'activer qu'un périphérique ppp (modem) dans le profil **Home**. Le profil **Commun** peut également activer `eth0` et un profil **Away** activer un périphérique ppp à utiliser en cas de voyage.

Un profil ne peut être activé au démarrage. Seuls les périphériques du profil **Commun** (le profil par défaut) qui sont configurés pour être activés au démarrage, peuvent l'être. Une fois que le système a démarré, allez au bouton **Menu principal** (sur le panneau) **=> Outils de système => Contrôle de périphérique réseau** (Network Device Control) (ou tapez la commande `redhat-control-network`) pour sélectionner un profil et l'activer. La section pour activer le profil n'apparaît dans l'interface du **Contrôle de périphérique réseau** que si l'interface **Commun** par défaut, n'est pas la seule existant.

Sinon, exécutez la commande suivante pour activer un profil (remplacez <*nom-profil*> par le nom du profil):

```
redhat-config-network-cmd --profile
<nom-profil> --activate
```

12.13. Alias de périphériques

Les *alias de périphériques* sont des périphériques virtuels associés au même matériel, mais ils peuvent être activés au même moment afin d'avoir des adresses IP différentes. On les représente généralement avec le nom du périphérique suivi du signe deux-points et d'un nombre (eth0:1, par exemple). Ils sont utiles si vous souhaitez qu'un système ait plusieurs adresses IP, mais que le système n'a qu'une seule carte réseau.

Après avoir configuré un périphérique Ethernet, comme `eth0`, pour qu'il utilise un adresse IP statique (DHCP ne fonctionne pas avec les alias), allez à l'onglet **Périphérique** et cliquez sur **Nouveau**. Sélectionnez la carte Ethernet à configurer avec un alias, configurez l'adresse IP statique pour l'alias et cliquez sur **Appliquer** pour le créer. Étant donné qu'un périphérique existe déjà pour la carte Ethernet, celui nouvellement créé est l'alias comme `eth0:1`.

Attention

Si vous configurez un périphérique Ethernet de façon à ce qu'il ait un alias, ni le périphérique ni le périphérique ne pourront être configurés pour utiliser DHCP. Vous devez configurer manuellement les adresses IP.

La Figure 12-20 montre un exemple d'alias pour le périphérique `eth0`. Veuillez noter le périphérique `eth0:1` — le premier alias pour `eth0`. Le deuxième alias pour `eth0` aurait le nom de périphérique `eth0:2`, et ainsi de suite. Pour modifier les paramètres de l'alias de périphérique, comme par exemple, pour indiquer s'il doit être activé au démarrage et le numéro de l'alias, sélectionnez-le dans la liste et cliquez sur le bouton **Éditer**.

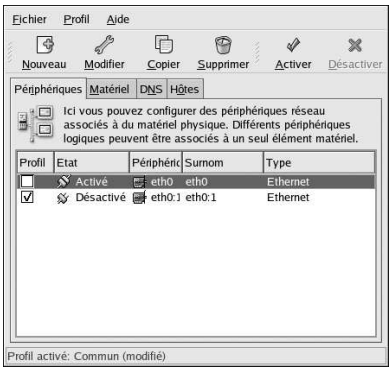

Figure 12-20. Exemple d'alias de périphérique réseau

Sélectionnez l'alias et cliquez sur le bouton **Activer** pour activer l'alias. Si vous avez configuré plusieurs profils, sélectionnez les profils dans lesquels l'inclure.

Afin de vous assurer que l'alias a bien été activé, utilisez la commande `/sbin/ifconfig`. La sortie doit afficher le périphérique ainsi que l'alias de périphérique avec des adresses IP différentes:

```
eth0      Link encap:Ethernet  HWaddr 00:A0:CC:60:B7:G4
          inet addr:192.168.100.5  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:161930 errors:1 dropped:0 overruns:0 frame:0
          TX packets:244570 errors:0 dropped:0 overruns:0 carrier:0
          collisions:475 txqueuelen:100
          RX bytes:55075551 (52.5 Mb)  TX bytes:178108895 (169.8 Mb)
          Interrupt:10 Base address:0x9000

eth0:1    Link encap:Ethernet  HWaddr 00:A0:CC:60:B7:G4
          inet addr:192.168.100.42  Bcast:192.168.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:10 Base address:0x9000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5998 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5998 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1627579 (1.5 Mb)  TX bytes:1627579 (1.5 Mb)
```

Chapitre 13.

Configuration de base du pare-feu

Tout comme un pare-feu évite qu'un incendie ne se propage dans un bâtiment, un pare-feu d'ordinateur empêche que les virus ne se diffusent à l'intérieur du système et évite que des utilisateurs non-autorisés n'accèdent à votre ordinateur. Un pare-feu se trouve entre l'ordinateur et le réseau. Il détermine les services de votre ordinateur auxquels les utilisateurs à distance sur le réseau peuvent accéder. Un pare-feu bien configuré peut augmenter sensiblement la sécurité de votre système. Nous vous conseillons vivement de configurer un pare-feu pour tous les systèmes Red Hat Linux connectés à l'Internet.

13.1. Outil de configuration du niveau de sécurité

Dans l'écran **Configuration du pare-feu** de Red Hat Linux, vous pouvez choisir entre un niveau de sécurité élevé, moyen ou inexistant (aucun) et autoriser des périphériques, des services entrants et des ports spécifiques.

Après l'installation, vous pouvez changer le niveau de sécurité de votre système en utilisant l'**Outil de configuration du niveau de sécurité**. Si vous préférez une application avec assistant, veuillez vous reporter à la Section 13.2.

Pour démarrer l'application, appuyez sur le bouton **Menu principal** (dans le Tableau de bord) => **Outils de système => Niveau de sécurité** ou tapez la commande `redhat-config-securitylevel` à une invite du shell (dans un terminal XTerm ou GNOME, par exemple).

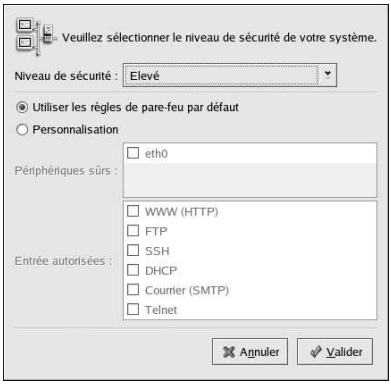

Figure 13-1. Outil de configuration du niveau de sécurité

Choisissez le niveau de sécurité souhaité dans le menu déroulant.

Élevé

Si vous choisissez **Élevé** (High), votre système refusera les connexions (hors paramètres par défaut) que vous n'avez pas explicitement définies. Par défaut, seules les connexions suivantes sont autorisées:

- réponses DNS

- DHCP — afin que toute interface réseau utilisant DHCP puisse être configurée correctement

Si vous choisissez **Élevé**, votre pare-feu n'autorisera pas:

- Le FTP mode actif (le FTP mode passif, utilisé par défaut par la plupart des clients, devrait fonctionner)
- Les transferts de fichiers DCC IRC
- RealAudio™
- Clients système X Window à distance

Si vous connectez votre système à l'Internet, mais ne prévoyez pas d'exécuter un serveur, il s'agit de l'option la plus sûre. Si des services complémentaires sont nécessaires, vous pouvez choisir **Personnaliser** pour autoriser des services spécifiques (pare-feu).

Remarque

Si vous sélectionnez un pare-feu moyen ou élevé, les méthodes d'authentification de réseau (NIS et LDAP) ne fonctionneront pas.

Moyen

Si vous choisissez **Moyen** (Medium), votre pare-feu n'autorisera pas les ordinateurs distants à accéder à certaines ressources de votre système. Par défaut, l'accès aux ressources suivantes est interdit:

- Ports inférieurs à 1023 — les ports réservés standard, utilisés par la plupart des services, comme **FTP**, **SSH**, **telnet**, **HTTP** et **NIS**.
- Le port de serveur NFS (2049) — NFS est désactivé pour les serveurs distants et les clients locaux.
- L'affichage X Window local pour les clients X à distance.
- Le port du serveur X Font (par défaut, **xfs** n'attend pas les requêtes sur le réseau; l'application est désactivée dans le serveur Font).

Si vous voulez autoriser des ressources telles que **RealAudio™** tout en bloquant l'accès aux services normaux, choisissez **Moyen**. Sélectionnez **Personnaliser** pour autoriser des services spécifiques (pare-feu).

Remarque

Si vous sélectionnez un pare-feu moyen ou élevé, les méthodes d'authentification de réseau (NIS et LDAP) ne fonctionneront pas.

Pas de pare-feu

Cette option (None) permet un accès complet à votre système, sans vérification de sécurité. La vérification de sécurité est la désactivation de l'accès à certains services. Ne sélectionnez cette option que si vous utilisez un réseau sûr (pas l'Internet) ou si vous prévoyez de réaliser une configuration de pare-feu plus avancée par la suite.

Choisissez **Personnaliser** pour ajouter des périphériques sécurisés ou pour autoriser des services entrants complémentaires.

Périphériques sûrs

Si vous sélectionnez des périphériques sûrs (**Périphériques sûrs**), tout le trafic à partir de ces périphériques a accès à votre système, et ces périphériques sont exclus des règles de pare-feu. Par exemple, si vous exécutez un réseau local, mais que vous êtes connecté à l'Internet par le biais d'une connexion commutée PPP, vous pouvez cocher **eth0**, et tout le trafic provenant de votre réseau local sera autorisé. Si vous sélectionnez **eth0** comme périphérique sûr, cela signifie que tout le trafic sur l'Ethernet est autorisé, mais que l'interface ppp0 est toujours protégée par le pare-feu. Si vous souhaitez restreindre le trafic sur une interface, ne la cochez pas.

Nous vous déconseillons de configurer comme **Périphériques sûrs**, des périphériques connectés à des réseaux publics, comme l'Internet.

Autoriser l'entrée

Si vous activez ces options, les services spécifiés seront autorisés à traverser le pare-feu. Remarque: lors de l'installation d'un poste de travail, la majorité de ces services n'est *pas* installée sur le système.

DHCP

Si vous autorisez les requêtes et réponses DHCP entrantes, vous autorisez toutes les interfaces réseau utilisant DHCP à déterminer leur adresse IP. DHCP est normalement activé. Si ce n'est pas le cas, votre ordinateur ne peut pas obtenir d'adresse IP.

SSH

*S*ecure *SH*ell (SSH) est un ensemble d'outils vous permettant de vous connecter sur un ordinateur à distance et d'y exécuter des commandes. Si vous voulez utiliser les outils SSH pour accéder à votre machine à travers un pare-feu, activez cette option. Le paquetage `openssh-server` doit être installé si vous voulez accéder à votre machine à distance, à l'aide des outils SSH.

Telnet

Telnet est un protocole permettant de se connecter à des ordinateurs à distance. Les communications Telnet ne sont pas cryptées et ne sont donc pas sécurisées. Nous vous déconseillons d'autoriser l'accès Telnet entrant. Si vous souhaitez toutefois autoriser l'accès Telnet entrant, vous allez devoir installer le pack `telnet-server`.

WWW (HTTP)

Le protocole HTTP est utilisé par Apache (et d'autres serveurs Web) pour servir des pages Web. Si vous prévoyez de rendre votre serveur Web accessible au public, activez cette option. Cette option n'est pas requise pour l'affichage local de pages ou pour le développement de pages Web. Vous devrez installer le paquetage `apache` si vous voulez servir des pages Web.

Le fait d'activer **WWW (HTTP)** n'ouvrira pas de port pour HTTPS. Pour activer HTTPS, spécifiez-le dans le champ **Autres ports**.

Courrier (SMTP)

Si vous voulez autoriser la livraison de messages entrants à travers votre pare-feu, de façon à ce que les hôtes distants puissent se connecter directement à votre machine pour livrer des messages, activez cette option. Vous n'avez pas besoin d'activer cette option si vous récupérez vos messages du serveur de votre ISP par POP3 ou IMAP, ou si vous utilisez un outil tel que **fetchmail**. Remarque: un serveur SMTP configuré de façon incorrecte peut autoriser les ordinateurs à distance à utiliser votre serveur pour envoyer du spam (ou pourriel).

FTP

Le protocole FTP est utilisé pour transférer des fichiers entre ordinateurs sur un réseau. Si vous prévoyez de rendre votre serveur FTP accessible au public, activez cette option. Pour que cette option soit utile, vous devez installer le paquetage `vsftpd`.

Cliquez sur **OK** pour activer le pare-feu. Après avoir cliqué sur **OK**, les options sélectionnées sont converties en commandes `iptables` et écrites dans le fichier `/etc/sysconfig/iptables`. Le service `iptables` est également lancé afin que le pare-feu soit activé immédiatement après l'enregistrement des options sélectionnées.

Avertissement

Si vous avez un pare-feu déjà configuré ou toute règle de pare-feu dans le fichier `/etc/sysconfig/iptables`, ce fichier sera effacé lorsque vous sélectionnerez **Pas de pare-feu** et enregistrerez vos modifications en cliquant sur **OK**.

Les options sélectionnées sont enregistrées dans le fichier `/etc/sysconfig/redhat-config-securitylevel` afin que le paramétrage puisse être utilisé lors de tout démarrage ultérieur. Ne modifiez pas ce fichier manuellement.

Pour activer le service `iptables` de façon à ce qu'il se lance automatiquement au moment du démarrage, reportez-vous à la Section 13.3 pour de plus amples informations.

13.2. GNOME Lokkit

GNOME Lokkit vous permet de configurer les paramètres du pare-feu pour un utilisateur moyen en construisant des règles de réseau `iptables` de base. Vous n'avez pas à écrire les règles; ce programme vous pose une série de questions concernant votre utilisation du système, puis écrit à votre place les règles dans le fichier `/etc/sysconfig/iptables`.

N'essayez pas d'utiliser **GNOME Lokkit** pour générer des règles de pare-feu complexes. Ce programme s'adresse aux utilisateurs moyens souhaitant se protéger lors de l'utilisation d'une connexion Internet modem, câble ou DSL. Pour configurer des règles de pare-feu spécifiques, reportez-vous au chapitre *Techniques de pare-feu avec `iptables`* du *Guide de référence de Red Hat Linux*.

Pour désactiver des services spécifiques et interdire des hôtes et utilisateurs spécifiques, reportez-vous au Chapitre 14.

Pour démarrer une version graphique de **GNOME Lokkit**, sélectionnez le bouton **Menu principal => Outils système => Outils système supplémentaires => Lokkit**, ou tapez la commande `gnome-lokkit` à l'invite du shell, en étant connecté en tant que super-utilisateur (ou root). Si le système X Window n'est pas installé sur votre ordinateur ou si vous préférez un programme de type texte, tapez la commande `lokkit` à une invite du shell afin de démarrer une version en mode texte.

13.2.1. Configuration de base

Figure 13-2. Configuration de base

Une fois que vous avez démarré le programme, choisissez le niveau de sécurité approprié pour votre système:

- **Sécurité élevée** — Cette option permet de désactiver presque toutes les connexions réseau, sauf les réponses DNS et DHCP, pour que les interfaces réseau puissent être activées. IRC, ICQ et les autres services de messagerie instantanés, ainsi que RealAudio™ ne fonctionneront pas sans proxy.
- **Sécurité faible** — Cette option permet d'interdire les connexions distantes au système, y compris les connexions NFS et les sessions X Window à distance. Les services s'exécutant en deçà du port 1023 n'accepteront pas de connexions, y compris FTP, SSH, Telnet et HTTP.
- **Désactiver le pare-feu** — Cette option ne crée aucune règle de sécurité. Nous recommandons de ne choisir cette option que si le système se trouve sur un réseau de confiance (et non sur Internet), si le système se trouve derrière un pare-feu plus grand, ou si vous écrivez vos propres règles de pare-feu personnalisées. Si vous optez pour cette option et cliquez sur **Suivant**, passez à la Section 13.3. La sécurité de votre système ne sera pas modifiée.

13.2.2. Hôtes locaux

Si des dispositifs Ethernet sont installés sur le système, la page **Hôtes locaux** vous permet de configurer l'application ou non des règles de pare-feu aux demandes de connexion envoyées à chaque périphérique. Si le périphérique connecte le système à un réseau LAN derrière un pare-feu et ne se connecte pas directement à l'Internet, sélectionnez **Oui**. Si la carte Ethernet connecte le système à un modem câble ou DSL, nous vous conseillons de choisir **Non**.

Figure 13-3. Hôtes locaux

13.2.3. DHCP

Si vous utilisez DHCP pour l'activation d'interfaces Ethernet sur le système, vous devez répondre **Oui** à la question DHCP. Si vous répondez non, vous ne pourrez pas établir de connexion avec l'interface Ethernet. De nombreux fournisseurs d'accès Internet câble et DSL vous obligent à utiliser DHCP pour établir une connexion Internet.

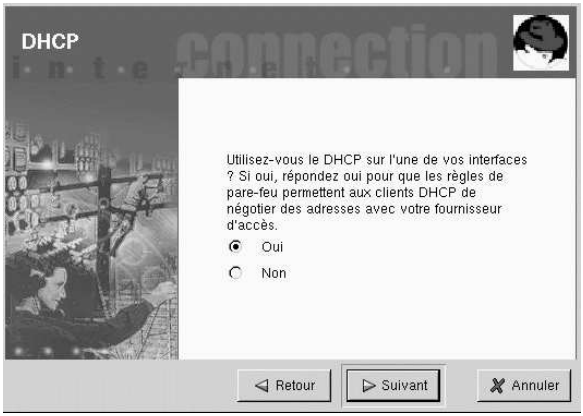

Figure 13-4. DHCP

13.2.4. Configuration des services

GNOME Lokkit vous permet également d'activer et de désactiver des services courants. Si vous répondez **Oui** à la configuration de services, le programme vous propose les services suivants:

- **Serveur Web** — Choisissez cette option si vous voulez que les utilisateurs se connectent à un serveur Web comme Apache s'exécutant sur votre système. Vous n'avez pas besoin de sélectionner cette option si vous voulez voir des pages de votre propre système ou sur d'autres serveurs du réseau.
- **Courrier entrant** — Choisissez cette option si votre système doit accepter les messages entrants. Vous n'avez pas besoin de cette option si vous récupérez vos messages par le biais de IMAP, POP3 ou fetchmail.
- **Shell sécurisé** — Secure Shell, ou SSH, est un ensemble d'outils vous permettant de vous connecter sur un ordinateur à distance et d'y exécuter des commandes par l'intermédiaire d'une connexion cryptée. Si vous voulez accéder à votre ordinateur à distance par ssh, sélectionnez cette option.
- **Telnet** — Telnet vous permet de vous connecter à votre ordinateur à distance; cette option n'est, cependant, pas sécurisée. Elle envoie du texte simple (mots de passe compris) sur le réseau. Nous vous recommandons d'utiliser SSH pour vous connecter à distance à votre ordinateur. Si vous avez besoin d'un accès telnet à votre système, sélectionnez cette option.

Pour désactiver d'autres services dont vous n'avez pas besoin, vous pouvez utiliser **Serviceconf** (voir la Section 14.3) ou **ntsysv** (voir la Section 14.4), ou `chkconfig` (voir la Section 14.5).

13.2.5. Activation du pare-feu

Si vous cliquez sur **Finir**, les règles de pare-feu seront inscrites dans `/etc/sysconfig/iptables` et le pare-feu sera lancé par le service `iptables`.

Avertissement

Si vous avez un pare-feu déjà configuré ou toute règle de pare-feu dans le fichier `/etc/sysconfig/iptables` ce fichier sera effacé lorsque vous sélectionnerez **Désactiver le pare-feu** et enregistrerez vos modifications en cliquant sur **Finir**.

Nous vous recommandons d'exécuter **GNOME Lokkit** à partir de l'ordinateur, et non à partir d'une session X à distance. Si vous désactivez l'accès à distance à votre système, vous ne pourrez plus y accéder ou désactiver les règles de pare-feu.

Cliquez sur **Annuler** si vous ne souhaitez pas écrire les règles de pare-feu.

13.2.5.1. Relais des messages

Un relais des messages est un système permettant à d'autres systèmes d'envoyer des messages par son intermédiaire. Si votre système est un relais des messages, quelqu'un pourrait l'utiliser pour envoyer des messages indésirables à partir de votre ordinateur.

Si vous choisissez d'activer les services de messagerie, une fois que vous aurez cliqué sur **Finir** à la page **Activer le pare-feu**, on vous demandera de vérifier s'il existe un relais des messages. Si vous sélectionnez **Oui**, **GNOME Lokkit** tentera de se connecter au site Web *Mail Abuse Prevention System* à l'adresse http://www.mail-abuse.org/ et exécutera un programme de test de relais des messages. Les résultats du test seront affichés une fois qu'il sera terminé. Si votre système est ouvert aux relais des messages, nous vous recommandons fortement de configurer Sendmail de façon à l'empêcher.

13.3. Activation du service `iptables`

Les règles de pare-feu ne seront actives que si le service `iptables` est en cours d'exécution. Pour lancer manuellement le service, utilisez la commande:

```
/sbin/serviceiptablesrestart
```

Pour vous assurer qu'il sera lancé au démarrage du système, tapez la commande:

```
/sbin/chkconfig--level345iptableson
```

Le service `ipchains` ne peut pas être exécuté parallèlement au service `iptables`. Pour vous assurez que le service `ipchains` est bien désactivé, exécutez la commande:

```
/sbin/chkconfig--level345ipchainsoff
```

Pour configurer les services `iptables` et `ipchains`, vous pouvez employer l'utilitaire **Outil de configuration des services** Reportez-vous à la Section 14.3 pour de plus amples informations.

Chapitre 14.

Contrôle de l'accès aux services

Il est extrêmement important de maintenir la sécurité de votre système Red Hat Linux. Une des manières de garantir la sécurité de votre système est de gérer méticuleusement l'accès aux services. Il se peut que votre système doive fournir un accès ouvert à des services particuliers (comme `httpd` par exemple, si vous utilisez un serveur Web). Cependant, si vous ne devez pas absolument fournir de service, vous devriez le désactiver. Vous diminuerez ainsi votre exposition à d'éventuels bogues.

Plusieurs méthodes de gestion d'accès aux services du système vous sont proposées. Vous devrez choisir celle que vous voulez utiliser, d'après le service, la configuration de votre système et votre niveau de connaissance de Linux.

La façon la plus simple de refuser l'accès à un service est de tout simplement le désactiver. Les services gérés par `xinetd` (dont nous parlerons plus loin) et les services contenus dans la hiérarchie `/etc/rc.d` peuvent tous les deux être configurés pour démarrer ou s'arrêter en utilisant trois applications différentes:

- **Outil de configuration des services** — une application graphique qui affiche une description de chaque service, indique si un service est activé au démarrage du système (pour les niveaux d'exécution 3, 4 et 5) et permet à l'utilisateur de démarrer, d'arrêter et de redémarrer les services.
- **ntsysv** — une application en mode texte qui permet de configurer les services qui seront activés au démarrage du système pour chaque niveau d'exécution. Les changements ne sont appliqués immédiatement dans le cas de services non-`xinetd`. Ces service non-`xinetd` ne peuvent pas être démarrés, arrêtés ou redémarrés à l'aide de ce programme.
- `chkconfig` — un utilitaire en ligne de commande qui permet d'activer et de désactiver des services pour les différents niveaux d'exécution. Les changements ne sont appliqués immédiatement dans le cas de services non-`xinetd`. Ces service non-`xinetd` ne peuvent pas être démarrés, arrêtés ou redémarrés à l'aide de cet utilitaire.

Vous trouverez peut-être que ces outils sont plus faciles à utiliser que d'autres — comme la modification manuelle des nombreux liens symboliques contenus dans les répertoires sous `/etc/rc.d` ou celle des fichiers de configuration `xinetd` contenus dans `/etc/xinetd.d`.

Vous pouvez également gérer l'accès aux services du système en utilisant `iptables` pour configurer un pare-feu IP. Si vous êtes un nouvel utilisateur de Linux, `iptables` n'est pas forcément la meilleure solution pour vous car la configuration de `iptables` peut être compliquée. Pour cette raison, cette option est plutôt recommandée aux administrateurs de système UNIX/Linux expérimentés.

Ceci étant, `iptables` a l'avantage d'être très flexible. Si vous avez par exemple besoin d'une solution personnalisée pour donner à certains hôtes l'accès à certains services, `iptables` est l'outil qu'il vous faut. Pour plus d'informations au sujet d'`iptables`, consultez le *Guide de référence de Red Hat Linux* et le *Guide de sécurité de Red Hat Linux*.

Autrement, si vous cherchez un utilitaire permettant d'instaurer des règles générales d'accès pour votre ordinateur personnel et/ou si vous êtes un nouvel utilisateur de Linux, essayez **GNOME Lokkit**. Cet utilitaire **GNOME Lokkit** est une application avec une interface graphique (GUI) qui vous posera des questions sur la manière dont vous souhaitez utiliser votre ordinateur. D'après vos réponses, l'application configurera un pare-feu de base pour votre système. Vous pouvez également utiliser l'application **Outil de configuration du niveau de sécurité** (`redhat-config-securitylevel`), vous permet de sélectionner le niveau de sécurité pour votre système, d'une façon similaire à celle utilisée dans l'écran **Configuration Pare-feu** dans le programme d'installation de Red Hat Linux. Pour plus d'informations sur ces outils, reportez-vous au Chapitre 13.

14.1. Niveaux d'exécution

Avant de pouvoir configurer l'accès aux services, vous devez comprendre les niveaux d'exécutions de Linux. Un niveau d'exécution est un *mode* défini par les services contenus dans le répertoire `/etc/rc.d/rc<x>.d` où `<x>` correspond au numéro du niveau d'exécution.

Red Hat Linux utilise les niveaux d'exécution suivants:

- 0 — Arrêt
- 1 — Mode mono-utilisateur
- 2 — Pas utilisé (peut être défini par l'utilisateur
- 3 — Mode multi-utilisateurs complet
- 4 — Pas utilisé (peut être défini par l'utilisateur)
- 5 — Mode multi-utilisateur complet (avec un écran de connexion graphique)
- 6 — Redémarrage

Si vous utilisez un écran de connexion texte, vous activez le niveau d'exécution 3. Si vous utilisez un écran de connexion graphique, vous activez le niveau d'exécution 5.

Le niveau d'exécution par défaut peut être changé en modifiant le fichier `/etc/inittab`, qui, au tout début, contient une ligne qui ressemble à celle figurant ci-dessous:

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

Remplacez le numéro de cette ligne par le numéro du niveau d'exécution désiré. Le changement ne sera pas mis en oeuvre tant que vous ne redémarrerez pas le système.

Pour changer immédiatement de niveau d'exécution, connectez-vous en tant que root et utilisez la commande `telinit` suivie du numéro de niveau d'exécution.

14.2. Enveloppeurs TCP

De nombreux administrateurs système UNIX ont l'habitude d'utiliser les enveloppeurs TCP (aussi appelés 'TCP wrappers') pour gérer l'accès à certains services de réseau. Tout service de réseau géré par `xinetd` (ainsi que tous les programmes contenant un support intégré pour libwrap) peuvent utiliser les enveloppeurs TCP pour gérer l'accès. Le démon `xinetd` peut utiliser les fichiers `/etc/hosts.allow` et `/etc/hosts.deny` pour configurer l'accès aux services du système. Comme son nom l'indique, le fichier `hosts.allow` contient une liste des clients autorisés à accéder aux services de réseau contrôlés par `xinetd` et le fichier `hosts.deny` contient lui des règles qui empêchent l'accès. Le fichier `hosts.allow` est prioritaire par rapport au fichier `hosts.deny`. Les autorisations pour permettre ou empêcher l'accès peuvent être basées sur des adresses IP individuelles (ou noms d'hôtes) ou sur un modèle de clients. Pour plus d'informations, consultez le *Guide de référence de Red Hat Linux* et la page de manuel relative à `hosts_access` dans la section 5 des pages de manuel (`man 5 hosts_access`).

14.2.1. `xinetd`

Pour contrôler l'accès aux services Internet, vous pouvez utiliser `xinetd`, un remplaçant plus sûr d'`inetd`. Le démon `xinetd` conserve les ressources système, fournit contrôle d'accès et connexion et peut être utilisé pour lancer des serveurs à buts spéciaux. Ce démon `xinetd` peut être utilisé entre autres pour fournir l'accès à certains hôtes seulement, pour refuser l'accès à d'autres, pour ne fournir l'accès à un service qu'à un moment donné, pour limiter le nombre de connexions et/ou la charge des connexions

Le démon `xinetd` fonctionne en permanence et surveille tous les ports des services qu'il gère. Lorsqu'une requête de connexion est reçue à destination de l'un d'eux, `xinetd` démarre le serveur adapté à ce service.

Le fichier de configuration de `xinetd` est `/etc/xinetd.conf`, mais si vous examinez ce fichier vous verrez qu'il contient seulement quelques valeurs par défaut et une instruction pour inclure le répertoire `/etc/xinetd.d`. Pour activer ou désactiver un service `xinetd`, éditez son fichier de configuration dans le répertoire `/etc/xinetd.d`. Si l'attribut `disable` (désactiver) a la valeur **`yes`**, le service est désactivé. Si au contraire l'attribut `disable` a la valeur **`no`**, le service est dans ce cas activé. Vous pouvez éditer tout fichier de configuration `xinetd` ou changer le statut d'activation à l'aide de **Outil de configuration des services**, **ntsysv**, ou `chkconfig`. Pour une liste des services de réseau contrôlés par `xinetd`, passez en revue le contenu du répertoire `/etc/xinetd.d` à l'aide de la commande `ls /etc/xinetd.d`.

14.3. Outil de configuration des services

L'application graphique **Outil de configuration des services** a été développée par Red Hat pour permettre de configurer les services SysV contenus dans `/etc/rc.d/init.d` qui seront lancés au démarrage (pour les niveaux d'exécution 3, 4 et 5) et les services `xinetd` qui seront activés. L'application permet également d'une part, de démarrer, arrêter et redémarrer les services SysV et d'autre part, de redémarrer `xinetd`.

Pour démarrer l'**Outil de configuration des services** à partir du bureau, allez au bouton **Menu principal** (sur le panneau) **=> Paramètres serveur => Services** ou tapez la commande `redhat-config-services` à l'invite du shell (par exemple, dans une application comme **XTerm** ou **GNOME terminal**).

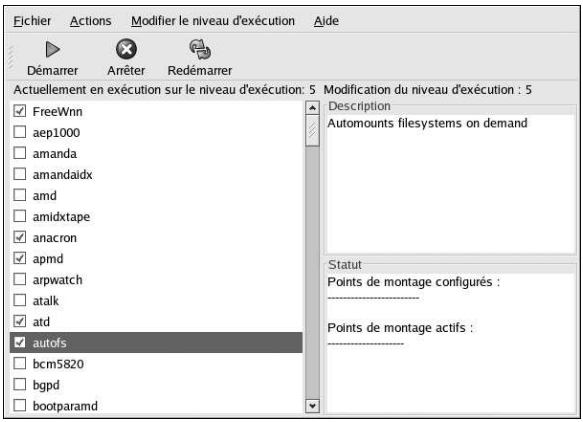

Figure 14-1. Outil de configuration des services

L'**Outil de configuration des services** affiche le niveau d'exécution en cours d'utilisation ainsi que le niveau d'exécution en cours de modification. Pour éditer un autre niveau d'exécution, sélectionnez **Éditer niveau d'exécution** dans le menu déroulant et sélectionnez le niveau d'exécution 3, 4 ou 5. Pour une description des niveaux d'exécution, consultez la Section 14.1.

L'**Outil de configuration des services** énumère les services de `/etc/rc.d/init.d` ainsi que les services contrôlés par `xinetd`. En cliquant sur le nom du service figurant dans la liste à gauche de

l'application, vous en afficherez une brève description de ce service ainsi que son statut. Si le service n'est pas un service `xinetd`, la fenêtre de statut indiquera si le service est actuellement en cours. Si le service est contrôlé par `xinetd`, la fenêtre de statut affiche la phrase **xinetd service**.

Pour démarrer, arrêter ou redémarrer immédiatement un service, sélectionnez le service à partir de la liste et choisissez le bouton approprié dans la barre d'outils (ou sélectionnez l'action désirée dans le menu déroulant d'**Actions**). Si le service est un service `xinetd`, les boutons d'action ne fonctionneront pas car il ne peuvent pas être démarrés ou arrêtés individuellement.

Si vous activez/désactivez un service `xinetd` en sélectionnant ou dé-sélectionnant la case de pointage à coté du nom du service, vous devez choisir **Fichier => Enregistrer les changements** dans le menu déroulant dans le menu déroulant afin de redémarrer `xinetd` et d'activer/désactiver immédiatement le service `xinetd` que vous avez modifié. Le service `xinetd` est également configuré de manière à conserver le paramétrage. Vous pouvez activer/désactiver plus d'un service `xinetd` à un moment donné et enregistrer les changements lorsque vous avez terminé.

Supposons par exemple que vous contrôliez `rsync` pour l'activer à un niveau d'exécution 3 et que vous sauvegardiez ensuite vos changements. Le service `rsync` sera immédiatement activé. Lors du prochain lancement de `xinetd` le service `rsync` sera toujours activé.

Avertissement

Lorsque vous sauvegardez des modifications apportées aux services `xinetd`, le démon `xinetd` est redémarré et les changements sont mis en oeuvre immédiatement. Lorsque vous enregistrez des changements apportés à d'autres services, le niveau d'exécution est reconfiguré mais les changements ne sont pas mis en oeuvre immédiatement.

Pour activer un service non-`xinetd` afin qu'il démarre au moment de l'amorçage au niveau d'exécution actuellement sélectionné, cochez la case de pointage à côté du nom du service figurant dans la liste. Après avoir configuré le niveau d'exécution, mettez les changements en oeuvre en choisissant **Fichier => Enregistrer les changements** dans le menu déroulant. La configuration du niveau d'exécution est certes changée, mais le niveau d'exécution n'est pas redémarré; dans de telles conditions, les changements ne sont pas mis en oeuvre immédiatement.

Supposons par exemple que vous configuriez le niveau d'exécution 3. Si vous changez la valeur pour le service `anacron` en dé-sélectionnant la case appropriée et que vous choisissiez ensuite **Enregistrer les changements**, la configuration du niveau d'exécution 3 changera afin que `anacron` ne soit pas démarré lors de l'amorçage. Le niveau d'exécution 3 n'est toutefois pas réinitialisé et `anacron` tourne donc toujours. À ce stade, choisissez l'une des options suivantes:

1. Arrêt du service `anacron` — Arrêtez le service en le sélectionnant de la liste et en cliquant sur le bouton **Stop**. Un message s'affiche indiquant que le service a été arrêté.
2. Ré-initialisation du niveau d'exécution — Pour réinitialiser le niveau d'exécution, à l'invite du shell, tapez la commande `telinit 3` (où 3 représente le niveau d'exécution choisi). Cette option est conseillée si vous changez la valeur relative à **Démarrer à l'amorçage** pour plus d'un service et si vous souhaitez que ces changements soient mis en oeuvre immédiatement.
3. Terminé! — Vous n'avez pas besoin d'arrêter le service `anacron`. Pour que le service s'arrête vous pouvez attendre que le système redémarre. Au prochain démarrage, le niveau d'exécution sera initialisé sans que le service `anacron` ne tourne.

14.4. ntsysv

L'utilitaire **ntsysv** fournit une interface simple pour activer et désactiver les services. Vous pouvez utiliser **ntsysv**pour activer ou désactiver un service géré par `xinetd`. Vous pouvez également utili-

ser Y **ntsysv** pour configurer des niveaux d'exécution. Par défaut, seul le niveau d'exécution courant est configuré. Pour configurer à un niveau d'exécution différent, spécifiez un ou plusieurs niveau(x) d'exécution à l'aide de l'option `--level`. La commande `ntsysv --level 345` par exemple, configure les niveau d'exécutions 3, 4 et 5.

L'interface **ntsysv** fonctionne comme le programme d'installation en mode texte. Utilisez les flèches vers le haut et vers le bas pour faire défiler la liste. La barre espace sélectionne/dé-sélectionne les services et sert également à appuyer sur les boutons **OK** et **Annuler** (Cancel). Pour passer de la liste des services aux boutons **OK** et **Annuler**, utilisez la touche [Tab]. Un astérisque (*) signifie que le service est activé. Appuyez sur la touche [F1] pour afficher une brève description de chaque service.

Avertissement

Les changements apportés aux services gérés par `xinetd` au moyen de **ntsysv** sont mis en oeuvre immédiatement. Pour tous les autres services, les changements ne sont pas mis en oeuvre immédiatement. Vous devez arrêter et démarrer le service spécifique à l'aide de la commande `service`*`démon`* `stop`. Dans l'exemple précédent, remplacez *`démon`* par le nom du service que vous désirez arrêter; par exemple, `httpd`. Remplacez `stop` par `start` ou `restart` pour démarrer ou redémarrer le service.

14.5. `chkconfig`

La commande `chkconfig` peut également être utilisée pour activer et désactiver les services. Si vous utilisez la commande `chkconfig --list` une liste des services du système apparaîtra et indiquera si les services sont activés (`on`) ou arrêtés (`off`) dans les niveaux d'exécution 0-6. À la fin de la liste, vous verrez une section pour les services gérés par `xinetd`.

Si vous utilisez `chkconfig --list` pour envoyer une requête à un service géré par `xinetd`, vous verrez si le service `xinetd` est activé (`on`) ou désactivé (`off`). La commande `chkconfig --list finger` par exemple, renverra la sortie suivante:

```
finger          on
```

L'exemple ci-dessus montre que `finger` est activé comme un service `xinetd`. Si `xinetd` est en cours d'exécution, `finger` est activé.

Si vous utilisez `chkconfig --list` pour envoyer une requête à un service dans `/etc/rc.d`, vous verrez les paramètres du service pour chaque niveau d'exécution. La commande `chkconfig --list anacron` renverra par exemple, la sortie suivante:

```
anacron         0:off   1:off   2:on    3:on    4:on    5:on
6:off
```

La commande `chkconfig` peut également servir à configurer un service de façon à ce qu'il démarre (ou pas) dans un niveau d'exécution spécifique. Par exemple, pour désactiver `nscd` dans les niveaux d'exécution 3, 4 et 5, utilisez la commande suivante:

```
chkconfig --level 345 nscd off
```

Avertissement

Les services gérés par `xinetd` sont immédiatement mis en oeuvre par `chkconfig`. Si par exemple, `xinetd` est en cours d'exécution, `finger` est désactivé, la commande `chkconfig finger on` est exécutée, `finger` est immédiatement activé et vous n'avez pas besoin de redémarrer `xinetd` manuellement. Les modifications concernant les autres services ne prennent pas effet immédiatement

après l'utilisation de `chkconfig`. Vous devez arrêter ou démarrer le service spécifique à l'aide de la commande `service` *`démon`* `stop`. Dans l'exemple précédent, remplacez *`démon`* par le nom du service que vous voulez arrêter, comme `httpd` par exemple. Pour démarrer ou redémarrer le service, remplacez `stop` par `start` ou `restart` pour démarrer ou redémarrer le service.

14.6. Ressources supplémentaires

Pour obtenir plus d'informations, consultez les ressources énumérées ci-dessous.

14.6.1. Documentation installée

- Les pages de manuel relatives à `ntsysv`, `chkconfig`, `xinetd` et `xinetd.conf`
- `man 5 hosts_access` — La page de manuel pour le format des fichiers de contrôle de l'accès des hôtes (dans la section 5 des pages de manuel).

14.6.2. Sites Web utiles

- http://www.xinetd.org — Page Web relative à `xinetd`. Elle contient une liste plus détaillée des fonctionnalités et des exemples de fichiers de configuration.

Chapitre 15.

OpenSSH

OpenSSH est une mise en application libre et OpenSource des protocoles SSH (*S*ecure *SH*ell). Elle remplace `telnet`, `ftp`, `rlogin`, `rsh` et `rcp` en offrant des outils de connexion sécurisée au réseau par cryptage. OpenSSH prend en charge les versions 1.3, 1.5 et 2 du protocole SSH. Depuis la version 2.9, le protocole par défaut est la version 2, qui utilise les clés RSA par défaut.

15.1. Pourquoi utiliser OpenSSH?

En utilisant les outils OpenSSH, vous augmentez la sécurité de votre ordinateur. En effet, toutes les formes de communication utilisant des outils OpenSSH, y compris les mots de passe, sont cryptées. Aussi bien `Telnet` que `ftp` utilisent des mots de passe en texte standard et transmettent les informations sous forme non cryptée. Les informations peuvent donc être interceptées et les mots de passe découverts; dans de telles conditions, la sécurité de votre système risque d'être compromise par des personnes non-authorisées se connectant à l'aide d'un des mots de passe interceptés. Dans la mesure du possible, utilisez l'ensemble des programmes utilitaires OpenSSH pour éviter tout problème de sécurité.

OpenSSH est aussi très utile car il redirige automatiquement la variable `DISPLAY` vers l'ordinateur client. En d'autres termes, si vous exécutez le système X Window sur votre ordinateur local et que vous vous connectez à un ordinateur distant au moyen de la commande `ssh`, lorsque vous exécutez un programme sur l'ordinateur distant qui nécessite X Window, celui-ci s'affichera sur votre ordinateur local. Cette fonctionnalité est très pratique si vous préférez utiliser des outils d'administration système graphiques, mais n'avez pas toujours physiquement accès à votre serveur.

15.2. Configuration d'un serveur OpenSSH

Avant de pouvoir exécuter un serveur OpenSSH, vous devez vous assurer que les paquetages RPM appropriés sont bien installés. Le paquetage `openssh-server` est nécessaire et dépend du paquetage `openssh`.

Le démon OpenSSH utilise le fichier de configuration `/etc/ssh/sshd_config`. Le fichier de configuration par défaut installé avec Red Hat Linux devrait suffire dans la plupart des cas. Toutefois, si vous souhaitez une configuration du démon différente de celle fournie dans le fichier par défaut `sshd_config`, consultez la page de manuel relative à `sshd` afin d'obtenir une liste des mots clés pouvant être définis dans le fichier de configuration.

Pour démarrer le service OpenSSH, utilisez la commande `/sbin/service sshd start`. Pour arrêter le serveur OpenSSH, utilisez la commande `/sbin/service sshd stop`. Si vous souhaitez que le démon se lance automatiquement au moment du démarrage, reportez-vous au Chapitre 14 dans lequel vous trouverez des informations sur la façon de gérer les services.

Si vous réinstallez un système Red Hat Linux et que des clients s'y connectent avant la réinstallation avec des outils OpenSSH, les utilisateurs clients verront, après la réinstallation, le message suivant:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
```

Le système réinstallé crée un nouvel ensemble de clés d'identification du système, d'où l'avertissement relatif à la modification des clés d'hôtes RSA. Si vous souhaitez conserver les

clés d'hôtes générées pour le système, sauvegardez les fichiers `/etc/ssh/ssh_host*key*` et restaurez-les après la réinstallation. Ce processus permet de conserver l'identité du système si bien que lorsque les clients essaieront de se connecter au système après la réinstallation, ils recevront pas le message d'avertissement.

15.3. Configuration d'un client OpenSSH

Pour vous connecter à un serveur OpenSSH depuis un ordinateur client, les paquetages `openssh-clients` et `openssh` doivent être préalablement installés sur cet ordinateur client.

15.3.1. Utilisation de la commande `ssh`

La commande `ssh` est un substitut sécurisé des commandes `rlogin`, `rsh` et `telnet`. Elle vous permet de vous connecter à un ordinateur distant et d'y exécuter des commandes.

La connexion à un ordinateur distant au moyen de `ssh` est semblable à la connexion en utilisant `telnet`. Par exemple, pour vous connecter à un ordinateur distant appelé pingouin.exemple.net, entrez la commande suivante à l'invite du shell:

```
ssh penguin.example.net
```

La première fois que vous effectuez la connexion à un ordinateur distant à l'aide de `ssh` le système affiche un message semblable à celui-ci:

```
The authenticity of host 'penguin.example.net' can't be established.
DSA key fingerprint is 94:68:3a:3a:bc:f3:9a:9b:01:5d:b3:07:38:e2:11:0c.
Are you sure you want to continue connecting (yes/no)?
```

Tapez **`yes`** pour poursuivre. Ce faisant, le serveur sera ajouté à votre liste d'hôtes connus, comme le montre le message suivant:

```
Warning: Permanently added 'penguin.example.net' (RSA) to the list of known hosts.
```

Une invite vous demandera ensuite d'entrer votre mot de passe pour l'ordinateur distant. Après l'avoir entré, l'invite du shell apparaîtra sur l'ordinateur distant. Si vous n'indiquez pas de nom d'utilisateur, celui sous lequel vous êtes connecté sur l'ordinateur client local sera transmis à l'ordinateur distant. Si en revanche, vous souhaitez spécifier un nom d'utilisateur différent, utilisez la commande suivante:

```
ssh username@penguin.example.net
```

Vous pouvez aussi avoir recours à la syntaxe `ssh -l nom d'utilisateur penguin.example.net`.

La commande `ssh` peut être utilisée pour exécuter une commande sur l'ordinateur distant sans vous connecter à une invite du shell. La syntaxe est alors `ssh nom d'hôte command`. Si vous souhaitez, par exemple, exécuter la commande `ls /usr/share/doc` sur l'ordinateur distant pingouin.exemple.net, entrez la commande suivante à l'invite du shell:

```
ssh penguin.example.net ls /usr/share/doc
```

Une fois le bon mot de passe saisi, le contenu du répertoire distant `/usr/share/doc` sera affiché et vous reviendrez ensuite à l'invite du shell.

15.3.2. Utilisation de la commande `scp`

La commande `scp` peut être utilisée pour transférer des fichiers entre des ordinateurs au moyen d'une connexion cryptée sécurisée. Cette commande est semblable à `rcp`.

La syntaxe générale correspondant au transfert d'un fichier local vers un système distant est la suivante:

```
scp localfile username@tohostname/newfilename
```

Le fichier local (*`localfile`*) spécifie la source et *`username@tohostname:/newfilename`* la destination.

Pour transférer le fichier local `shadowman` vers votre compte dans penguin.example.net, entrez la commande suivante à l'invite du shell (remplacez *`nom-utilisateur`* par votre propre nom-d'utilisateur):

```
scp shadowman username@penguin.example.net:/home/username
```

Cette opération entraînera le transfert du fichier local `shadowman` vers `/home/`*`nom-utilisateur`*`/shadowman` sur penguin.example.net.

La syntaxe générale correspondant au transfert d'un fichier distant vers un système est la suivante:

```
scp username@tohostname:/remotefile /newlocalfile
```

Le fichier distant, *`fichier-distant`*, spécifie la source et nouveau fichier local spécifie *`newlocalfile`* la destination.

Il est également possible de spécifier plusieurs fichiers en tant que fichiers source. Par exemple, pour transférer le contenu du répertoire `/downloads` vers un répertoire existant nommé `uploads` sur l'ordinateur distant pingouin.exemple.net, entrez les éléments ci-dessous à l'invite du shell:

```
scp /downloads/* username@penguin.example.net:/uploads/
```

15.3.3. Utilisation de la commande `sftp`

L'utilitaire `sftp` peut être utilisé pour ouvrir une session FTP interactive sécurisée. Il est semblable à `ftp` mais, contrairement à ce dernier, utilise une connexion cryptée sécurisée. La syntaxe générale de cet utilitaire est *`sftp username@hostname.com`*. Une fois authentifié, vous pouvez utiliser un ensemble de commandes semblables à celles de FTP. Reportez-vous à la page de manuel relative à `sftp` afin de consulter une liste de ces commandes. Pour consulter cette page de manuel, exécutez la commande `man sftp` à l'invite du shell. L'utilitaire `sftp` n'est disponible que dans les versions 2.5.0p1 ou supérieures d'OpenSSH.

15.3.4. Création de paires de clés

Si vous ne voulez pas avoir à entrer votre mot de passe à chaque fois que vous utilisez `ssh`, `scp` ou `sftp` pour vous connecter à un ordinateur distant, vous pouvez créer une paire de clés d'autorisation.

Des clés doivent être créés pour chacun des utilisateurs. Afin de créer une paire de clés pour un utilisateur donné, suivez les étapes suivantes en tant qu'utilisateur souhaitant se connecter à des ordinateurs distants. Si vous le faites en tant que super-utilisateur, seul l'utilisateur root pourra utiliser les clés.

Depuis la version 3.0 de OpenSSH, `~/.ssh/authorized_keys2`, `~/.ssh/known_hosts2` et `/etc/ssh_known_hosts2` sont obsolètes. Les protocles SSH 1 et 2 partagent les fichiers `~/.ssh/authorized_keys`, `~/.ssh/known_hosts` et `/etc/ssh/ssh_known_hosts`.

Red Hat Linux 9 utilise par défaut le protocole 2 de SSH et les clés RSA.

Astuce

Si vous réinstallez Red Hat Linux mais souhaitez conserver votre paire de clés, sauvegardez le répertoire `.ssh` de votre répertoire personnel. Une fois la réinstallation terminée, copiez-le dans votre répertoire personnel (home). Ce processus peut être exécuté pour tous les utilisateurs de votre système, y compris le root.

15.3.4.1. Création d'une paire de clés RSA pour la version 2

Suivez les étapes indiquées ci-dessous afin de créer une paire de clés RSA pour la version 2 du protocole SSH. Il s'agit du démarrage par défaut avec OpenSSH 2.9

1. Pour créer une paire de clés RSA que vous utiliserez avec la version 2 du protocole, entrez la commande suivante à l'invite du shell:
   ```
   ssh-keygen -t rsa
   ```
   Acceptez l'emplacement par défaut du fichier, à savoir `~/.ssh/id_rsa`. Entrez ensuite une phrase d'accès différente du mot de passe de votre compte et confirmez-la en la tapant de nouveau.

   La clé publique est enregistrée dans `~/.ssh/id_rsa.pub`. La clé privée quant à elle, est enregistrée dans `~/.ssh/id_rsa`. Ne divulguez jamais votre clé privée.
2. Changez les autorisations de votre répertoire `.ssh` à l'aide de la commande `chmod 755 ~/.ssh`.
3. Copiez le contenu de `~/.ssh/id_rsa.pub` dans `~/.ssh/authorized_keys` sur l'ordinateur auquel vous désirez vous connecter. Si le fichier `~/.ssh/authorized_keys` n'existe pas, vous pouvez copier le fichier `~/.ssh/id_rsa.pub` dans le fichier `~/.ssh/authorized_keys` sur l'autre ordinateur.
4. Si vous utilisez GNOME, passez à la Section 15.3.4.4. Si vous n'utilisez pas le système X Window, passez à la Section 15.3.4.5.

15.3.4.2. Création d'une paire de clés DSA pour la version 2

Suivez les étapes indiquées ci-dessous afin de créer une paire de clés DSA pour la version 2 du protocole SSH.

1. Pour créer une paire de clés DSA que vous utiliserez avec la version 2 du protocole, entrez la commande suivante à l'invite du shell:
   ```
   ssh-keygen -t dsa
   ```
   Acceptez l'emplacement par défaut du fichier, à savoir `~/.ssh/id_dsa`. Entrez ensuite une phrase d'accès différente du mot de passe de votre compte et confirmez-la en la tapant de nouveau.

   

   Astuce

   Une phrase d'accès est une chaîne de mots et de caractères utilisée pour authentifier un utilisateur. Les phrases d'accès différent des mots de passe dans le sens où les phrases d'accès peuvent inclure des espaces et des tabulations, contrairement aux mots de passe. De plus, elles sont généralement plus longues que les mots de passe car elles constituent de véritables phrases et non pas de simples mots.

La clé publique est enregistrée dans `~/.ssh/id_dsa.pub`. La clé privée quant à elle est enregistrée dans `~/.ssh/id_dsa`. Il est important de ne jamais communiquer votre clé privée à qui que ce soit.

2. Changement d'autorisation pour votre répertoire `.ssh` à l'aide de la commande `chmod 755 ~/.ssh`.
3. Copiez le contenu de `~/.ssh/id_dsa.pub` dans `~/.ssh/authorized_keys` sur l'ordinateur auquel vous souhaitez vous connecter. Si le fichier `~/.ssh/authorized_keys` n'existe pas, vous pouvez copier le fichier `~/.ssh/id_dsa.pub` dans le fichier `~/.ssh/authorized_keys` sur l'autre ordinateur.
4. Si vous utilisez GNOME, passez à la Section 15.3.4.4. Si vous n'utilisez pas le système X Window, passez à la Section 15.3.4.5.

15.3.4.3. Création d'une paire de clés RSA pour les versions 1.3 et 1.5

Suivez les étapes indiquées ci-dessous afin de créer une paire de clés RSA pour la version 1 du protocole SSH. Si vos connexions ne se font qu'entre des systèmes utilisant DSA, vous n'avez pas besoin d'une paire de clés RSA version 1.3 ou RSA version 1.5.

1. Pour générer une paire de clés RSA (pour les versions 1.3 et 1.5 du protocole), entrez la commande suivante à l'invite du shell:
   ```
   ssh-keygen -t rsa1
   ```
   Acceptez l'emplacement par défaut du fichier (`~/.ssh/identity`). Entrez une phrase d'accès différente du mot de passe de votre compte. Confirmez-la en l'entrant de nouveau.

   La clé publique est enregistrée dans `~/.ssh/identity.pub`. La clé privée quant à elle, est enregistrée dans `~/.ssh/identity`. Ne divulguez votre clé privée à quiconque.
2. Modifiez les autorisations de votre répertoire `.ssh` et de votre clé à l'aide des commandes `chmod 755 ~/.ssh` et `chmod 644 ~/.ssh/identity.pub`.
3. Copiez le contenu de `~/.ssh/identity.pub` dans le fichier `~/.ssh/authorized_keys` sur l'ordinateur auquel vous souhaitez vous connecter. Si le fichier `~/.ssh/authorized_keys` n'existe pas, vous pouvez copier le fichier `~/.ssh/identity.pub` dans le fichier `~/.ssh/authorized_keys` sur l'ordinateur distant.
4. Si vous utilisez GNOME, passez à la Section 15.3.4.4. Si vous n'utilisez pas GNOME, passez à la Section 15.3.4.5.

15.3.4.4. Configuration de `ssh-agent` avec GNOME

Vous pouvez vous servir de l'utilitaire `ssh-agent` pour enregistrer votre phrase d'accès afin de ne pas avoir à l'entrer à chaque fois que vous effectuez une connexion `ssh` ou `scp`. Si vous utilisez GNOME, l'utilitaire `openssh-askpass-gnome` peut être utilisé pour obtenir votre phrase d'accès à chaque fois que vous vous connectez à GNOME et pour la garder en mémoire jusqu'à ce que vous quittiez GNOME. Ainsi, vous ne devrez pas entrer votre mot de passe ou votre phrase d'accès lorsque vous effectuerez toute connexion `ssh` ou `scp` au cours d'une session GNOME. Si vous n'utilisez pas GNOME, reportez-vous à la Section 15.3.4.5.

Afin d'enregistrer votre phrase d'accès lors d'une session GNOME, suivez les étapes suivantes:

1. Le paquetage `openssh-askpass-gnome` doit être préalablement installé. Utilisez la commande `rpm -q openssh-askpass-gnome` afin de déterminer si ce dernier est bien installé. Si ce n'est pas le cas, procédez à son installation à l'aide de votre kit CD-ROM Red Hat Linux à partir d'un site miroir FTP Red Hat ou au moyen de Red Hat Network.

2. Sélectionnez le bouton **Menu principal** (sur le panneau) => **Extras** => **Préférences** => **Sessions**, et cliquez sur l'onglet **Programmes de démarrage**. Cliquez sur **Ajouter** et entrez **`/usr/bin/ssh-add`** dans la zone texte de **Commande de démarrage**. Indiquez un numéro de priorité supérieur à toute autre commande existante afin de vous assurer qu'elle sera exécutée en dernier. Le nombre 70 par exemple (ou tout autre nombre plus élevé) est un bon choix de priorité pour `ssh-add`. Plus le numéro de priorité est élevé, plus la priorité est basse. Par conséquent, si vous avez d'autres programmes répertoriés, leur numéro de priorité doit être le plus bas. Cliquez sur **Sortir** pour sortir du programme.
3. Quittez GNOME et connectez-vous à nouveau; en d'autres termes, redémarrez X Window. Une fois GNOME lancé, une boîte de dialogue apparaîtra et vous invitera à saisir votre ou vos phrases d'accès. Entrez la phrase demandée. Si vous avez configuré une paire de clés DSA et une paire de clés RSA, le système vous demandera d'entrer les deux phrases d'accès. À partir de ce moment, `ssh`, `scp` ou `sftp` ne devraient plus vous demander votre mot de passe.

15.3.4.5. Configuration de `ssh-agent`

Vous pouvez vous servir de l'utilitaire `ssh-agent` pour enregistrer votre phrase d'accès afin de ne pas avoir à l'entrer à chaque fois que vous effectuez une connexion `ssh` ou `scp`. Si vous n'utilisez pas le système X Window, suivez les étapes indiquées ci-dessous depuis l'invite du shell. En revanche, si vous utilisez GNOME, mais si vous ne voulez pas qu'il vous demande votre phrase d'accès lorsque vous vous connectez (voir la Section 15.3.4.4), vous pouvez appliquer cette procédure dans une fenêtre de terminal de type Xterm. Si vous utilisez X Window mais pas GNOME, vous pourrez appliquer cette procédure dans une fenêtre de terminal. Votre phrase d'accès ne sera cependant gardée en mémoire que pour cette fenêtre de terminal; il ne s'agit pas d'un paramètre global.

1. À l'invite du shell, tapez la commande suivante:
   ```
   exec /usr/bin/ssh-agent $SHELL
   ```
2. Tapez ensuite la commande:
   ```
   ssh-add
   ```
   et entrez votre ou vos phrases d'accès. Si vous avez plusieurs paires de clés configurées, le système vous invitera à entrer les phrases d'accès correspondantes.
3. Dès que vous vous déconnectez, vos phrases d'accès sont effacées de mémoire dans le système. Vous devez exécuter ces deux commandes à chaque fois que vous vous connectez à une console virtuelle ou que vous ouvrez une fenêtre de terminal.

15.4. Ressources supplémentaires

Les projets OpenSSH et OpenSSL faisant l'objet d'un développement continu, leur site Web respectif constitue la meilleure source d'informations mises à jour. Les pages de manuel relatives aux outils OpenSSH et OpenSSL sont également très utiles et offrent de nombreuses informations détaillées.

15.4.1. Documentation installée

- Les pages de manuel relatives à `ssh`, `scp`, `sftp`, `sshd` et `ssh-keygen` — Ces pages contiennent des informations sur la façon d'utiliser ces commandes, ainsi que sur les paramètres qui s'y rapportent.

15.4.2. Sites Web utiles

- http://www.openssh.com — contient un Forum Aux Questions (FAQ) portant sur OpenSSH, des rapports de bogues, des listes de distribution, les objectifs du projet ainsi que des explications plus techniques sur ses fonctions de sécurité.
- http://www.openssl.org — contient un Forum Aux Questions (FAQ) portant sur OpenSSL, des listes de distribution et une description de l'objectif du projet.
- http://www.freessh.org — contient le logiciel client SSH pour d'autres plates-formes.

Chapitre 16. Système de fichiers réseau (NFS - 'Network File System')

Le système de fichiers réseau (ou NFS de l'anglais 'Network File System') est un moyen de partager des fichiers entre plusieurs machines sur un même réseau comme si les fichiers se trouvaient sur votre disque dur local. Red Hat Linux peut être à la fois un serveur NFS et un client NFS, ce qui signifie qu'il peut exporter des systèmes de fichiers vers d'autres systèmes et monter des systèmes de fichiers exportés à partir d'autres machines.

16.1. Pourquoi utiliser NFS?

NFS peut être utilisé pour partager des répertoires de fichiers entre plusieurs utilisateurs sur un même réseau. Par exemple, un groupe d'utilisateurs qui travaillent sur un même projet peut accéder aux fichiers de ce projet en utilisant un répertoire partagé du système de fichiers NFS (généralement appelée partage NFS) monté dans le répertoire `/myproject`. Pour accéder aux fichiers partagés, l'utilisateur entre dans le répertoire `/myproject` de son ordinateur sans taper de mot de passe ni de commande particulière. L'utilisateur travaille comme si le répertoire se trouvait sur son ordinateur local.

16.2. Montage de systèmes de fichiers NFS

Utilisez la commande `mount` pour monter un système de fichiers NFS partagé d'un autre ordinateur:

```
mount shadowman.example.com:/misc/export/misc/local
```

Avertissement

Le répertoire du point de montage de l'ordinateur local (`/misc/local` dans l'exemple ci-dessus) doit exister.

Dans cette commande, `shadowman.example.com` est le nom d'hôte du serveur de fichiers NFS, `/misc/export` est le répertoire que `shadowman` exporte et `/misc/local` est l'emplacement de l'ordinateur local où vous voulez monter le système de fichiers. Une fois que vous avez exécuté la commande `mount` (et si vous avez les autorisations appropriées du serveur NFS `shadowman.example.com`), l'utilisateur peut exécuter la commande `ls /misc/local` pour afficher une liste des fichiers de `/misc/export` sur `shadowman.example.com`.

16.2.1. Montage des systèmes de fichiers NFS au moyen de `/etc/fstab`

Pour monter un partage NFS à partir d'une autre machine, vous pouvez également ajouter une ligne au fichier `/etc/fstab`. La ligne doit contenir le nom d'hôte du serveur NFS, le répertoire du serveur qui est exporté et le répertoire de l'ordinateur local où vous désirez monter le partage NFS. Vous devez être connecté en tant que super-utilisateur (ou root) pour pouvoir modifier le fichier `/etc/fstab`.

La syntaxe générale de la ligne contenue dans `/etc/fstab` est la suivante:

```
server:/usr/local/pub/pubnfsrsize=8192,wsize=8192,timeo=14,intr
```

Le point de montage `/pub` doit exister sur l'ordinateur client. Après avoir ajouté cette ligne à `/etc/fstab` sur le système client, entrez la commande `mount /pub` à l'invite de shell; le point de montage `/pub` sera monté à partir du serveur.

16.2.2. Montage de systèmes de fichiers NFS au moyen d'autofs

La troisième technique de montage d'un partage NFS concerne l'utilisation d'autofs. Autofs utilise le démon automount pour gérer vos points de montage en ne les montant de façon dynamique que lorsqu'on y accède.

Autofs consulte le fichier de configuration maître `/etc/auto.master` pour déterminer quels points de montage sont définis. Il amorce ensuite un processus de montage automatique avec les paramètres adéquats pour chaque point de montage. Chaque ligne du fichier de configuration maître définit un point de montage et un fichier de configuration séparé qui définit les systèmes de fichiers devant être montés sur ce point de montage. Par exemple, si le fichier `/etc/auto.misc` définit des points de montage dans le répertoire `/misc`, cette relation est définie dans le fichier `/etc/auto.master`.

Chaque entrée dans `auto.master` comporte trois champs. Le premier fournit le point de montage. Le deuxième correspond à l'emplacement du fichier de configuration et le troisième champ est en option. Ce dernier peut contenir des informations telles qu'une valeur de dépassement du délai d'attente.

Par exemple, pour monter le répertoire `/proj52` de l'ordinateur distant penguin.host.net sur le point de montage `/misc/myproject` de votre ordinateur, ajoutez au fichier `auto.master` la ligne suivante:

```
/misc/etc/auto.misc--timeout60
```

Ajoutez la ligne suivante au fichier `/etc/auto.misc`:

```
myproject-rw,soft,intr,rsize=8192,wsize=8192penguin.example.net:/proj52
```

Le premier champ de `/etc/auto.misc` affiche le nom du sous-répertoire `/misc`. Ce répertoire est créé de façon dynamique par automount. Il ne devrait en réalité pas exister sur l'ordinateur client. Le deuxième champ contient les options de montage, telles que `rw` pour l'accès en lecture (r: read) et en écriture (w: write). Le troisième champ indique l'adresse du serveur NFS d'exportation, comprenant le nom d'hôte et le répertoire.

Remarque

Le répertoire `/misc` doit exister sur le système de fichiers local. Celui-ci ne devrait pas contenir de sous-répertoires de `/misc`.

Autofs est un service. Pour le démarrer, entrez à l'invite du shell les commandes suivantes:

```
/sbin/serviceautofsrestart
```

Pour afficher les points de montage actifs, entrez la commande suivante à l'invite du shell:

```
/sbin/serviceautofsstatus
```

Si vous modifiez le fichier de configuration `/etc/auto.master` pendant qu'autofs s'exécute, vous devez dire au démon automount de recharger le fichier en entrant la commande suivante à l'invite du shell:

```
/sbin/serviceautofsreload
```

Pour savoir comment configurer autofs pour qu'il se lance au démarrage, consultez les informations relatives à la gestion des services contenues dans le Chapitre 14.

16.3. Exportation de systèmes de fichiers NFS

Le partage de fichiers d'un serveur NFS s'appelle l'exportation de répertoires. L'**Outil de configuration du serveur NFS** peut être utilisé pour configurer un système en tant que serveur NFS.

Pour utiliser l'**Outil de configuration du serveur NFS**, le système X Window doit être en cours d'exécution, vous devez être connecté en tant que super-utilisateur (ou root) et le paquetage RPM `redhat-config-nfs` doit être installé sur votre système. Pour lancer l'application, sélectionnez le bouton **Menu principal** (sur le tableau de bord) => **Paramètres de système** => **Paramètres de serveur** => **Serveur NFS**, ou vous pouvez taper la commande `redhat-config-nfs` à l'invite du shell.

Figure 16-1. Outil de configuration du serveur NFS

Pour créer un partage NFS, cliquez sur le bouton **Ajouter**. La boîte de dialogue reproduite dans la Figure 16-2 s'affiche.

L'onglet **Informations de base** requiert les informations suivantes:

- **Répertoire** — Indiquez le répertoire à partager, comme par exemple `/tmp`.
- **Hôte(s)** — Indiquez le ou les hôtes qui partageront le répertoire. Reportez-vous à la Section 16.3.2 pour une explication relative aux différents formats possibles
- **Autorisations de base** — Indiquez si le répertoire doit avoir des autorisations en lecture-seule ou en lecture-écriture.

Figure 16-2. Ajout d'un partage

L'onglet **Options générales** permet de configurer les options suivantes:

- **Autoriser les connexions des ports 1024 et supérieurs** — Les services lancés sur les numéros de ports inférieurs à 1024 doivent être lancés en tant que super-utilisateur (ou root). Sélectionnez cette option pour permettre au service NFS d'être lancé par un utilisateur autre qu'un super-utilisateur. Cette option correspond à `insecure`.
- **Activer le verrouillage des fichiers non-sûrs** — Une requête de verrouillage n'est pas nécessaire. Cette option correspond à `insecure_locks`.
- **Désactiver le contrôle de la sous-arborescence** — Si un sous-répertoire d'un système de fichiers est exporté, mais pas la totalité de ce système, le serveur vérifie que le fichier requis se trouve bien dans le sous-répertoire exporté. Cette vérification s'appelle *vérification de la sous-arborescence*. Sélectionnez cette option pour désactiver la vérification de la sous-arborescence. Si tout le système de fichiers est exporté et que cette option est sélectionnée, le taux de transfert sera plus rapide. Cette option correspond à `no_subtree_check`.
- **Synchroniser les operations d'écriture sur demande** — Activée par défaut, cette option ne permet pas au serveur de répondre à des requêtes avant que les modifications effectuées par la requête ne soient enregistrées sur le disque. Cette option correspond à `sync`. Si elle n'est pas sélectionnée, l'option `async` est utilisée.
  - **Forcer la synchronisation immédiate des operations d'écriture** — Ne pas retarder l'enregistrement sur disque. Cette option correspond à `no_wdelay`.

L'onglet **Accès utilisateur** permet de configurer les options suivantes:

- **Considérer l'utilisateur root distant comme root local** — Par défaut, les ID d'utilisateur et de groupe de l'utilisateur root sont tous deux égaux à 0. L'écrasement de l'utilisateur root lie l'ID d'utilisateur 0 et l'ID de groupe 0 aux ID d'utilisateur et de groupe d'anonymes afin que le root du client n'ait pas de privilèges super-utilisateur (ou root) sur le serveur NFS. Si cette option est sélectionnée, l'utilisateur root n'est pas lié à l'utilisateur anonyme et le super-utilisateur d'un client dispose de privilèges root sur les répertoires exportés. Cette option peut réduire de façon importante le niveau de sécurité du système. Ne la sélectionnez que si cela s'avère absolument nécessaire. Cette option correspond à `no_root_squash`.
- **Considérer tous les utilisateurs clients comme des utilisateurs anonymes** — Si cette option est sélectionnée, tous les ID d'utilisateur et de groupe sont liés à l'utilisateur anonyme. Cette option correspond à `all_squash`.
  - **Spécifier l'ID de l'utilisateur local pour les utilisateurs anonymes** — Si l'option **Considérer tous les utilisateurs clients comme des utilisateurs anonymes** est sélectionnée, vous pouvez spécifier un ID d'utilisateur pour l'utilisateur anonyme. Cette option correspond à `anonuid`.
  - **Spécifier l'ID de groupe local pour les utilisateurs anonymes** — Si l'option **Considérer tous les utilisateurs clients comme des utilisateurs anonymes** est sélectionnée, vous pouvez spécifier un ID de groupe pour l'utilisateur anonyme. Cette option correspond à `anongid`.

Pour modifier un partage NFS existant, sélectionnez-le dans la liste et cliquez sur le bouton **Propriétés**. Pour supprimer un partage NFS existant, sélectionnez-le dans la liste et cliquez sur le bouton **Supprimer**.

Après avoir cliqué sur **OK** pour valider l'ajout, la modification ou la suppression d'un partage NFS de la liste, les modifications prennent effet immédiatement — Le démon serveur est relancé et l'ancien fichier de configuration est enregistré en tant que `/etc/exports.bak`. Le nouveau fichier de configuration quant à lui, est enregistré dans `/etc/exports`.

L'utilitaire **Outil de configuration du serveur NFS** lit et enregistre (ou écrit) directement dans le fichier de configuration `/etc/exports`. Le fichier peut donc être modifié manuellement après avoir utilisé cet outil qui peut également être utilisé après avoir modifié manuellement le fichier (si toutefois celui-ci a été modifié en respectant la syntaxe).

16.3.1. Configuration en ligne de commande

Si vous préférez modifier des fichiers de configuration à l'aide d'un éditeur de texte ou si le système X Window n'est pas installé, vous pouvez le faire directement.

Le fichier `/etc/exports` contrôle les répertoires que le serveur NFS exporte. Le format du fichier est le suivant:

```
répertoirenom-d'hôte(options)
```

Seule une des deux options suivantes peut être modifiée: `sync` ou `async` (`sync` est recommandée). Si l'option `sync` est spécifiée, le serveur répond aux requêtes seulement après que les changements effectués par la requête aient été enregistrés sur le disque.

Par exemple:

```
/misc/exportspeedy.example.com(sync)
```

permettrait aux utilisateurs de `speedy.example.com` de monter `/misc/export` avec des autorisations par défaut en lecture-seule, mais:

```
/misc/exportspeedy.example.com(rw,sync)
```

permettrait aux utilisateurs de `speedy.example.com` de monter `/misc/export` avec des privilèges en lecture-écriture.

Reportez-vous à la Section 16.3.2 pour une explication relative aux différents formats possibles de noms d'hôtes.

Pour une liste des options qui peuvent être spécifiées, reportez-vous au *Guide de référence de Red Hat Linux*.

Attention

Faites attention aux espaces dans le fichier `/etc/exports`. Si le nom d'hôte et les options entre parenthèses ne sont pas séparés par un espace, les options sont appliquées uniquement au nom d'hôte. Si le nom d'hôte et les options sont séparés par un espace, les options s'appliquent au reste du monde. Examinons par exemple les lignes ci-dessous:

```
/misc/exportspeedy.example.com(rw,sync)
/misc/exportspeedy.example.com(rw,sync)
```

La première ligne accorde aux utilisateurs de `speedy.example.com` un accès en lecture-écriture et refuse tous les autres utilisateurs. La seconde ligne accorde aux utilisateurs de `speedy.example.com` un accès seulement en lecture (la valeur par défaut) et accorde à tous les autres utilisateurs un accès en lecture-écriture.

Chaque fois que vous modifiez le fichier `/etc/exports`, vous devez informer le démon NFS de la modification ou recharger le fichier de configuration à l'aide des commandes suivantes:

```
/sbin/servicenfsreload
```

16.3.2. Formats des noms d'hôtes

Les hôtes peuvent avoir les formats suivants:

- Ordinateur seul — Un nom de domaine pleinement qualifié (qui peut être résolu par le serveur), un nom d'hôte (qui peut être résolu par le serveur) ou une adresse IP
- Série d'ordinateurs spécifiés avec des caractères génériques — Utilisez les caractères * ou ? pour indiquer une correspondance de chaîne. Par exemple, `192.168.100.*` spécifie toute adresse IP commençant par 192.168.100. Lorsque vous ajoutez des caractères génériques dans les noms de domaines pleinement qualifiés, les points (.) ne sont pas inclus dans le caractère générique. Par exemple, `*.example.com` inclut one.example.com mais n'inclut pas one.two.example.com.
- Réseaux IP — Utilisez *`a.b.c.d/z`*, où *`a.b.c.d`* représente le réseau et *`z`* le nombre de bits dans le masque réseau (192.168.0.0/24, par exemple). *`a.b.c.d/masque-réseau`* est également acceptable; *`a.b.c.d`* représente le réseau et *`masque-réseau`* le masque réseau (192.168.100.8/255.255.255.0, par exemple).
- Groupes réseau — Au format *`@nom-du-groupe`*, où *`nom-du-groupe`* représente le nom du groupe réseau NIS.

16.3.3. Démarrage et arrêt du serveur

Le service `nfs` doit être actif sur le serveur qui exporte les systèmes de fichiers NFS.

Pour afficher l'état du démon NFS, utilisez la commande suivante:

```
/sbin/servicenfsstatus
```

Pour redémarrer le démon NFS, utilisez la commande suivante:

```
/sbin/servicenfsstart
```

Pour arrêter le démon NFS, utilisez la commande suivante:

```
/sbin/servicenfsstop
```

Pour lancer le service `nfs` au démarrage, utilisez la commande:

```
/sbin/chkconfig--level345nfson
```

Vous pouvez également utiliser `chkconfig`, **ntsysv** ou l'**Outil de configuration des services** pour configurer les services qui se lanceront au démarrage. Consultez le Chapitre 14 pour de plus amples informations.

16.4. Ressources supplémentaires

Ce chapitre explique les bases de l'utilisation de NFS. Pour plus de détails, reportez-vous aux ressources ci-dessous.

16.4.1. Documentation installée

- Les pages de manuel relatives à `nfsd`, `mountd`, `exports`, `auto.master` et `autofs` (dans les sections de manuel 5 et 8) — Ces pages montrent la syntaxe correcte des fichiers de configuration NFS et autofs.

16.4.2. Sites Web utiles

- http://www.tldp.org/HOWTO/NFS-HOWTO/index.html — Le *Linux NFS-HOWTO* du projet de documentation Linux.

16.4.3. Livres sur le sujet

- *Managing NFS and NIS Services* de Hal Stern; O'Reilly & Associates, Inc.

Chapitre 17.

Samba

Samba utilise le protocole SMB pour partager les fichiers et les imprimantes sur une connexion réseau. Les systèmes d'exploitation qui prennent en charge ce protocole incluent Microsoft Windows (à travers son voisinage **Voisinage Réseau**), OS/2 et Linux.

17.1. Pourquoi utiliser Samba?

Samba est utile si vous avez un réseau d'ordinateurs à la fois Windows et Linux. Samba fait en sorte que vos fichiers et vos imprimantes soient partagés par tous les systèmes de votre réseau. Si vous voulez que vos fichiers soient partagés uniquement par des ordinateurs Red Hat Linux, utilisez NFS comme l'explique le Chapitre 16. Si vous voulez que vos imprimantes soient partagées uniquement par des ordinateurs Red Hat Linux, vous devez utiliser Samba; reportez-vous au Chapitre 27.

17.2. Configuration d'un serveur Samba

Le fichier de configuration par défaut (`/etc/samba/smb.conf`) permet aux utilisateurs d'afficher leurs répertoires personnels (ou home) Red Hat Linux en tant que partage Samba. Il offre en partage également toute imprimante configurée pour le système Red Hat Linux en tant qu'imprimantes partagées Samba. En d'autres termes, vous pouvez brancher une imprimante à votre système Red Hat Linux et imprimer à partir des ordinateurs Windows de votre réseau.

17.2.1. Configuration graphique

Pour configurer Samba à l'aide d'une interface graphique, utilisez l'utilitaire **Outil de configuration du serveur Samba**. Pour une configuration en ligne de commande, passez à la Section 17.2.2.

L'utilitaire **Outil de configuration du serveur Samba** est une interface graphique permettant de gérer les partages Samba, les utilisateurs et les paramètres de base du serveur. Il modifie les fichiers de configuration dans le répertoire `/etc/samba/`. Toutes les modifications apportées à ces fichiers sans l'utilisation de l'application sont conservées.

Afin de pouvoir utiliser cette application, le système X Window doit être en cours d'exécution, vous devez être connecté en tant que super-utilisateur et le paquetage RPM `redhat-config-samba` doit être installé sur votre système. Pour lancer l'utilitaire **Outil de configuration du serveur Samba** à partir du bureau, allez au bouton **Menu principal** (sur le panneau) => **Paramètres de système** => **Paramètres de serveur** => **Serveur Samba** ou tapez la commande `redhat-config-samba` à une invite du shell (par exemple, dans un terminal XTerm ou GNOME).

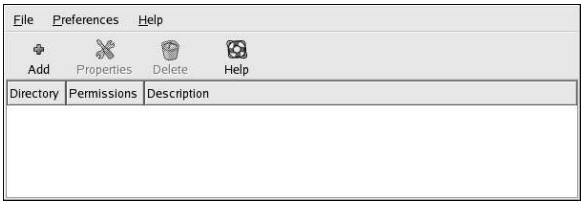

Figure 17-1. Outil de configuration du serveur Samba

Remarque

L'utilitaire **Outil de configuration du serveur Samba** n'affiche pas les imprimantes partagées ou la strophe par défaut permettant aux utilisateurs de consulter leurs propres répertoires personnels sur le serveur Samba.

17.2.1.1. Configuration des paramètres du serveur

La première étape dans la configuration d'un serveur Samba consiste à déterminer d'une part, les paramètres de base pour le serveur et d'autre part, un certains nombres d'options de sécurité. Après le démarrage de l'application, sélectionnez **Préférences => Paramètres du serveur** dans le menu déroulant. L'onglet **Basic** (pour les paramètres de base) apparaît à l'écran comme le montre la Figure 17-2.

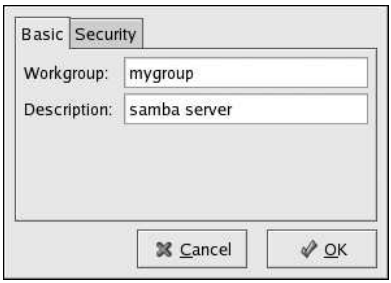

Figure 17-2. Configuration des paramètres de base du serveur

Sous l'onglet **Basic**, spécifiez le groupe de travail auquel l'ordinateur devrait appartenir ainsi qu'une brève description de l'ordinateur. Ces éléments correspondent aux options `workgroup` et `server string` de `smb.conf`.

Figure 17-3. Configuration des paramètres de sécurité du serveur

L'onglet **Sécurité** (Security) contient les options suivantes:

- **Mode d'authentification** — Cet élément correspond à l'option de `sécurité`. Sélectionnez l'un des types d'authentification suivant:
  - **Domaine** — Le serveur Samba dépend d'un contrôleur primaire de domaine Windows NT ou d'un contrôleur secondaire de domaine pour vérifier l'identité de l'utilisateur. Le serveur transmet

le nom d'utilisateur et le mot de passe au contrôleur et attend sa réponse. Spécifiez le nom du BIOS dédié au réseau (NetBIOS) du contrôleur primaire ou secondaire de domaine dans le champ **Authentification du serveur**.

La valeur de l'option **Mots de passe cryptés** doit être **Oui** si cette dernière est sélectionnée.

- **Serveur** — Le serveur Samba essaie de vérifier la combinaison nom d'utilisateur/le mot de passe en les transmettant à un autre serveur Samba. S'il ne peut le faire, le serveur essaie de vérifier ces informations en utilisant le mode d'authentification d'utilisateur. Spécifiez le nom du BIOS dédié au réseau (NetBIOS) de l'autre serveur Samba dans le champ **Authentification du serveur**.
- **Partage** — Les utilisateurs de Samba n'ont pas à saisir une combinaison nom d'utilisateur/mot de passe sur la base d'un serveur Samba individuel. Le système leur demande leur nom d'utilisateur et mot de passe jusqu'à ce qu'ils essaient de se connecter à un répertoire partagé spécifique d'un serveur Samba.
- **Utilisateur** — (Défaut) Les utilisateurs Samba doivent fournir un nom d'utilisateur et mot de passe valides sur la base d'un serveur Samba individuel. Sélectionnez cette option si vous souhaitez que l'option **Utilisateur Windows** fonctionne. Reportez-vous à la Section 17.2.1.2 pour de plus amples informations.

- **Crypter les mots de passe** — (La valeur par défaut est **Yes**) Cette option doit être activée si les clients se connectent à partir de machines équipées de Windows 98, Windows NT 4.0 avec Service Pack 3 ou d'autres versions plus récentes de Microsoft Windows. Les mots de passe sont transmis entre le serveur et le client dans un format crypté au lieu d'un format texte-simple qui peut être intercepté. Ceci correspond à l'option `encrypted passwords` (mots de passe cryptés). Reportez-vous à la Section 17.2.3 pour obtenir de plus amples informations sur les mots de passe Samba cryptés.
- **Compte invité** — Lorsque des utilisateurs normaux ou des utilisateurs invités se connectent à un serveur Samba, ils doivent être mappés à un utilisateur valide du serveur. Sélectionnez un des noms d'utilisateurs existant sur votre système pour créer un compte invité de Samba. Lorsque les invités se connectent au serveur Samba, ils possèdent les mêmes privilèges que ceux accordés à l'utilisateur ayant servi à la création du compte invité. Ceci correspond à l'option `guest account`.

Après avoir cliqué sur **OK**, les modifications sont enregistrées dans le fichier de configuration et le démon est redémarré; les modifications prennent donc effet immédiatement.

17.2.1.2. Gestion des utilisateurs Samba

Avant de pouvoir ajouter un utilisateur Samba, l'utilitaire **Outil de configuration du serveur Samba** nécessite qu'un compte utilisateur existant soit actif sur le système Red Hat Linux agissant en tant que serveur Samba. L'utilisateur Samba est associé au compte utilisateur Red Hat Linux existant.

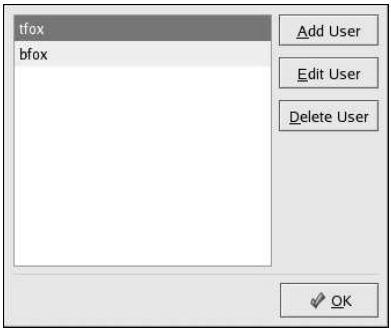

Figure 17-4. Gestion des utilisateurs Samba

Pour ajouter un utilisateur Samba, sélectionnez **Préférences => Utilisateurs Samba** dans le menu déroulant et cliquez sur le bouton **Ajouter utilisateur**. Dans la fenêtre **Créer un nouvel utilisateur Samba** sélectionnez **Nom d'utilisateur Unix** parmi la liste des utilisateurs existant sur le système local.

Si l'utilisateur disposant d'un nom d'utilisateur différent sur un ordinateur Windows souhaite se connecter au serveur Samba à partir de son système Windows, spécifiez ce nom d'utilisateur Windows dans le champ **Nom d'utilisateur Windows**. Le **Mode d'authentification** de l'onglet **Sécurité** dans les préférences relatives aux **Paramètres du serveur** doit être réglé sur **Utilisateur** pour que cette option fonctionne.

Configurez également un **Mot de passe Samba** pour l'utilisateur Samba et confirmez ce mot de passe en le saisissant une deuxième fois. Même si vous choisissez d'utiliser des mots de passe cryptés pour Samba, il est fortement recommandé que les mots de passe Samba pour tous les utilisateurs soient différents des mots de passe système de Red Hat Linux.

Pour modifier un utilisateur existant, sélectionnez ce dernier parmi la liste et cliquez sur **Éditer un utilisateur**. Pour effacer un utilisateur Samba existant, sélectionnez cet utilisateur et cliquez sur le bouton **Supprimer un utilisateur**. La suppression d'un utilisateur Samba ne supprime pas le compte utilisateur Red Hat Linux auquel il est associé.

Les utilisateurs sont modifiés immédiatement après avoir cliqué sur le bouton **OK**.

17.2.1.3. Ajout d'un partage

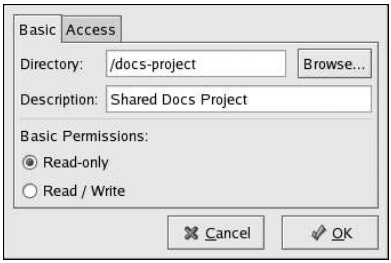

Figure 17-5. Ajout d'un partage

Pour ajouter un partage, cliquez sur le bouton **Ajouter**. L'onglet **Basic** configure les options suivantes:

- **Répertoire** — Spécifie le répertoire à partager via Samba. Ce répertoire doit exister.
- **Descriptions** — Une brève description du partage.
- **Autorisations de base** — Spécifie si les utilisateurs devraient avoir accès aux fichiers du répertoire partagé en lecture-seule ou si au contraire il devraient avoir accès au répertoire partagé en lecture et écriture.

Sur l'onglet **Accès**, sélectionnez entre l'autorisation d'accès au partage réservée seulement à certains utilisateurs spécifiques ou l'autorisation d'accès au partage attribuée à tous les utilisateurs Samba. Si vous choisissez de permettre l'accès seulement à un des utilisateurs spécifiques, sélectionnez ces derniers parmi la liste des utilisateurs Samba disponibles.

Le partage est ajouté immédiatement après avoir appuyé sur **OK**.

17.2.2. Configuration en ligne de commande

Le fichier de configuration de Samba est `/etc/samba/smb.conf`. Si vous modifiez ce dernier, les changements ne prennent effet qu'une fois le démon Samba redémarré à l'aide de la commande `service smb restart`.

Pour spécifier le groupe de travail Windows et une brève description du serveur Samba, modifiez les lignes suivantes dans votre fichier `smb.conf` file:

```
workgroup=NOM-DU-GROUPE-DE-TRAVAIL
serverstring=BREF-COMMENTAIRE-SUR-LE-SERVEUR
```

Remplacez *NOM-DU-GROUPE-DE-TRAVAIL* par le nom du groupe de travail Windows auquel cet ordinateur devrait appartenir. Le champ facultatif *BREF-COMMENTAIRE-SUR-LE-SERVEUR* est utilisé comme commentaire de Windows sur le système Samba.

Pour créer un répertoire de partage Samba sur votre système Linux, ajoutez la section suivante à votre fichier `smb.conf` (après l'avoir modifié en fonction de vos besoins et de votre système):

```
[Nom-du-partage]
comment=Insérez-un-commentaire-ici
path=/home/share/
validusers=tfoxcarole
public=no
writable=yes
printable=no
createmask=0765
```

Dans l'exemple ci-dessus, les utilisateurs tfox et carole peuvent lire et écrire dans le répertoire `/home/share` sur le serveur Samba, à partir d'un client Samba.

17.2.3. Mots de passes cryptés

Dans Red Hat Linux 9, les mots de passe cryptés sont activés par défaut pour des raisons de sécurité. Si les mots de passe cryptés ne sont pas utilisés, ils sont remplacés par des mots de passe en clair; ces derniers peuvent toutefois être interceptés par quelqu'un utilisant un programme renifleur de paquets. Nous vous recommandons donc d'utiliser des mots de passe cryptés.

Le protocole SMB de Microsoft utilisait à l'origine des mots de passe en clair. Cependant, Windows 2000 et Windows NT 4.0 avec le Service Pack 3 ou supérieur, Windows 98, Windows 2000, Windows ME et Windows XP requièrent des mots de passe Samba cryptés. Pour utiliser Samba entre un système Red Hat Linux et un systèmes exécutant une des systèmes d'exploitation Windows mentionnés ci-dessus, vous pouvez modifier le registre Windows afin qu'il utilise des mots de passe en texte clair ou

vous pouvez configurer Samba sur votre système Linux pour qu'il utilise des mots de passe cryptés. Si vous choisissez de modifier le registre, vous devez le faire sur tous vos ordinateurs Windows — il s'agit d'une procédure risquée pouvant générer des conflits. Il est fortement recommandé d'utiliser des mots de passe cryptés afin d'accroître la sécurité de votre système.

Pour configurer Samba sur votre système Red Hat Linux pour l'utilisation de mots de passe cryptés, suivez la procédure ci-dessous:

1. Créez un fichier de mots de passe séparé pour Samba. Pour en créer un sur la base de votre fichier `/etc/passwd` existant, tapez la commande suivante à l'invite du shell:
   ```
   cat/etc/passwd|mksmbpasswd.sh>/etc/samba/smbpasswd
   ```
   Si le système utilise NIS, tapez la commande suivante:
   ```
   ypcatpasswd|mksmbpasswd.sh>/etc/samba/smbpasswd
   ```
   Le script `mksmbpasswd.sh` est placé dans votre répertoire `/usr/bin` avec le paquetage `samba`.
2. Modifiez les autorisations du fichier de mots de passe Samba afin que seul le super-utilisateur (ou root) ait des autorisations en lecture et en écriture:
   ```
   chmod600/etc/samba/smbpasswd
   ```
3. Le script ne copie pas les mots de passe utilisateur dans le nouveau fichier. De plus, un compte utilisateur Samba n'est pas actif tant qu'un mot de passe ne lui a pas été attribué. Pour une sécurité accrue, il est recommandé d'utiliser un mot de passe utilisateur différent pour Samba et pour Red Hat Linux. Pour établir le mot de passe de chacun des utilisateurs Samba, utilisez la commande suivante (remplacez *nom-d'utilisateur* par le nom d'utilisateur de chacun des utilisateurs):
   ```
   smbpasswd nom-d'utilisateur
   ```
4. Les mots de passe cryptés doivent être activés dans le fichier de configuration Samba. Dans le fichier `smb.conf`, vérifiez que les lignes suivantes ne sont pas désactivées:
   ```
   encryptpasswords=yes
   smbpasswdfile=/etc/samba/smbpasswd
   ```
5. Assurez-vous que le service `smb` est bien lancé en tapant la commande `service smb restart` à l'invite du shell.
6. Si vous voulez que le service `smb` démarre automatiquement, utilisez **ntsysv**, `chkconfig` ou l'**Outil de configuration des services** pour l'activer lors de l'exécution. Consultez le Chapitre 14 pour plus d'informations.

Astuce

Pour en savoir plus sur les mots de passe cryptés, consultez `/usr/share/doc/samba-<version>/docs/htmldocs/ENCRYPTION.html` (remplacez *<version>* par le numéro de la version de Samba que vous avez installée).

Le module PAM `pam_smbpass` peut être utilisé pour synchroniser les mots de passe Samba des utilisateurs avec leurs mots de passe système lorsque la commande `passwd` est utilisée. Si un utilisateur invoque la commande `passwd`, le mot de passe qu'il utilise pour se connecter au système Red Hat Linux et le mot de passe qu'il doit fournir pour se connecter à un fichier partagé Samba sont modifiés.

Pour activer cette fonction, ajoutez la ligne suivante à `/etc/pam.d/system-auth` sous l'invocation `pam_cracklib.so`:

```
passwordrequired/lib/security/pam_smbpass.sonullokuse_authtoktry_first_pass
```

17.2.4. Démarrage et arrêt du serveur

Le service `smb` doit être en cours d'exécution sur le serveur partageant les répertoires via Samba.

Affichez le statut du démon Samba à l'aide de la commande suivante:

```
/sbin/servicesmbstatus
```

Démarrez le démon à l'aide de la commande suivante:

```
/sbin/servicesmbstart
```

Arrêtez le démon à l'aide de la commande suivante:

```
/sbin/servicesmbstop
```

Pour lancer le service `smb` au démarrage, utilisez la commande:

```
/sbin/chkconfig--level345smbon
```

Vous pouvez également utiliser `chkconfig`, **ntsysv** ou l'utilitaire **Outil de configuration des services** pour configurer les services spécifiques qui seront lancés lors du démarrage. Reportez-vous au Chapitre 14 pour de plus amples informations.

17.3. Connexion à un fichier partagé Samba

Pour vous connecter à un partage Linux Samba à partir d'un système Microsoft Windows, utilisez le **Voisinage réseau** ou le gestionnaire de fichiers graphique.

Pour vous connecter à un fichier partagé Samba à partir d'un système Linux, entrez la commande suivante à l'invite du shell:

```
smbclient//nom-d'hôte/nom-de-partage-Unom-d'utilisateur
```

Remplacez *`nom-d'hôte`* par le nom d'hôte ou l'adresse IP du serveur samba auquel vous voulez vous connecter, *`nom-du-partage`* par le nom du répertoire partagé que vous voulez parcourir et *`nom-d'utilisateur`* par le nom d'utilisateur Samba pour le système. Saisissez le mot de passe correct ou appuyez sur [Entrée] si aucun mot de passe n'est nécessaire pour l'utilisateur.

Si vous voyez l'invite `smb:\>`, vous avez réussi à vous connecter. Une fois que vous vous êtes connecté, entrez **`help`** pour afficher la liste des commandes. Si vous désirez parcourir le contenu de votre répertoire personnel, remplacez *`nom-du-partage`* par votre nom d'utilisateur. Si le commutateur `-U` n'est pas utilisé, le nom de l'utilisateur actuel est transmis au serveur Samba.

Pour quitter `smbclient`, entrez **`exit`** à l'invite `smb:\>`.

Vous pouvez également utiliser **Nautilus** pour afficher les partages Samba disponibles sur votre réseau. Sélectionnez **Bouton menu principal** (sur le panneau) => **Serveurs réseau** pour afficher une liste des groupes de travail Samba sur votre réseau. Vous pouvez également taper **`smb:`** dans la barre **Emplacement:** de Nautilus afin d'afficher les groupes de travail.

Comme le montre la Figure 17-6, une icône apparaît pour chaque groupe de travail SMB disponible sur le réseau.

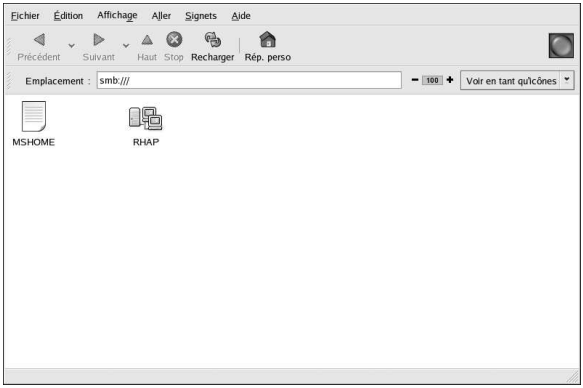

Figure 17-6. Groupes de travail SMB dans Nautilus

Cliquez deux fois sur l'icône d'un des groupes de travail pour afficher une liste des ordinateurs appartenant au groupe de travail donné.

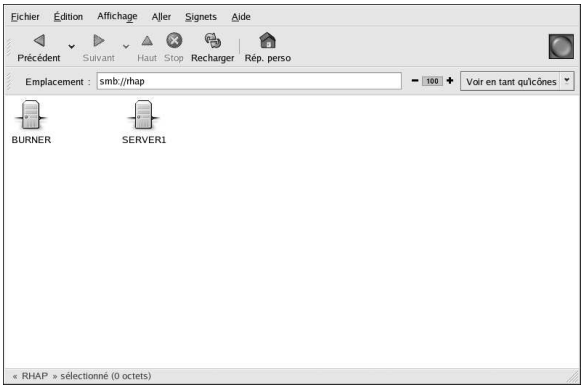

Figure 17-7. Ordinateurs SMB dans Nautilus

Comme le montre la Figure 17-7, il y a une icône pour chaque ordinateur appartenant au groupe de travail. Cliquez deux fois sur une icône pour afficher le partage Samba sur l'ordinateur donné. Si une combinaison nom d'utilisateur/mot de passe est nécessaire, le système vous invitera à la spécifier.

Vous pouvez également spécifier une combinaison nom d'utilisateur/mot de passe dans la barre **Emplacement:** en suivant la syntaxe suivante (remplacez *utilisateur*, *mot-de-passe*, *nom-du-serveur* et *nom-du-partage*par les valeurs appropriées):

```
smb://utilisateur:mot-de-passe@nom-du-serveur/nom-du-partage
```

17.4. Ressources supplémentaires

Pour les options de configuration non-traitées ici, veuillez vous reporter aux ressources suivantes.

17.4.1. Documentation installée

- page de manuel relative à `smb.conf` — explique comment configurer le fichier de configuration Samba
- page de manuel relative à `smbd` — décrit le fonctionnement du démon Samba
- `/usr/share/doc/samba-<numéro-de-versionr>/docs/` — les fichiers d'aide en format HTML et texte inclus dans le paquetage `samba`

17.4.2. Sites Web utiles

- http://www.samba.org — La page Web Samba contient de la documentation utile, des informations sur les listes de diffusion et une liste d'interfaces graphiques.

Chapitre 18. Dynamic Host Configuration Protocol (DHCP)

Le protocole DHCP ('Dynamic Host Configuration Protol') est un protocole réseau permettant d'assigner automatiquement des informations TCP/IP aux ordinateurs clients. Chaque client DHCP se connecte au serveur central DHCP, lequel renvoie la configuration réseau du client, y compris l'adresse IP, la passerelle et les serveurs DNS.

18.1. Pourquoi utiliser DHCP?

DHCP permet de livrer rapidement la configuration réseau des clients. Lors de la configuration du système client, l'administrateur peut choisir DHCP et ne pas avoir à entrer d'adresse IP, de masque de réseau, de passerelle ou de serveur DNS. Le client récupère ces informations à partir du serveur DHCP. DHCP est également utile lorsqu'un administrateur souhaite modifier l'adresse IP d'un nombre important de systèmes. Au lieu de reconfigurer tous les systèmes, il peut se contenter d'éditer un fichier de configuration DHCP sur le serveur pour le nouvel ensemble d'adresses IP. Si les serveurs DNS d'une organisation changent, les modifications sont réalisées sur le serveur DHCP, et non pas sur tous les clients DHCP. Une fois que le réseau est redémarré sur les clients (ou que les clients sont redémarrés), les changements prennent effet.

En outre, si un ordinateur portable ou mobile, quel qu'il soit, est configuré pour DHCP, il peut être déplacé de bureau en bureau sans qu'il soit nécessaire de le reconfigurer, à partir du moment où chacun des bureaux dispose d'un serveur DHCP permettant sa connexion au réseau.

18.2. Configuration d'un serveur DHCP

Vous pouvez configurer un serveur DHCP en utilisant le fichier de configuration `/etc/dhcpd.conf`.

DHCP utilise également le fichier `/var/lib/dhcp/dhcpd.leases` pour stocker la base de données d'attribution client. Reportez-vous à la Section 18.2.2 pour plus d'informations.

18.2.1. Fichier de configuration

La première étape lors de la configuration d'un serveur DHCP consiste à créer le fichier de configuration stockant les informations réseau pour les clients. Des options globales peuvent être choisies pour tous les clients, ou des options spécifiques pour chaque système client.

Le fichier de configuration peut contenir des tabulations ou lignes vierges complémentaires pour faciliter le formatage. Les mots clés ne sont pas sensibles à la casse, et les lignes commençant par un signe dièse (#) correspondent à des commentaires.

Deux schémas de mise à jour DNS sont actuellement mis en place — le mode de mise à jour DNS ad-hoc et le mode de mise à jour rapide interaction DHCP-DNS par intérim. Si ces deux modes sont acceptés comme faisant partie du processus IETF standard, il y a aura un troisième mode — la méthode de mise à jour DNS standard. Le serveur DHCP doit être configuré de façon à utiliser l'un de ces deux schémas. La version 3.0b2pl11 et la version précédente utilisaient le mode ad-hoc, qui a cependant été abandonné. Si vous souhaitez conserver le même comportement, ajoutez la ligne suivante en haut du fichier de configuration:

```
ddns-update-style ad-hoc;
```

Pour utiliser le deuxième mode, ajoutez la ligne suivante en haut du fichier de configuration:

```
ddns-update-style interim;
```

Consultez la page de manuel relative à `dhcpd.conf` pour obtenir de plus détails sur les différents modes.

Il y a deux types de déclarations dans le fichier de configuration:

- Paramètres — les paramètres règlent l'exécution d'une tâche, la façon dont une tâche est exécutée ou les options de configuration réseau à envoyer au client.
- Déclarations — les déclarations décrivent la topologie du réseau, les clients; elles fournissent des adresses pour les clients ou appliquent un groupe de paramètres à un groupe de déclarations.

Certains paramètres doivent commencer par le mot-clé `option` et sont considérés comme des options. Les options configurent les options DHCP alors que les paramètres eux, configurent des valeurs qui ne sont pas facultatives ou contrôlent le comportement du serveur DHCP.

Les paramètres (y compris les options) déclarés avant une section entre parenthèses ({ }) sont considérés comme des paramètres globaux. Ceux-ci s'appliquent à toutes les sections se trouvant en dessous.

Important

Si vous modifiez le fichier de configuration, les modifications ne prendront pas effet tant que vous n'aurez pas redémarré le démon DHCP à l'aide de la commande `service dhcpd restart`.

Dans l'Exemple 18-1, les options `routers`, `subnet-mask`, `domain-name`, `domain-name-servers` et `time-offset` sont utilisées pour les déclarations `host` déclarées en dessous.

Comme l'Exemple 18-1 le montre, vous pouvez déclarer un `subnet` (ou sous-réseau). Pour ce faire, vous devez inclure une déclaration `subnet` pour chaque sous-réseau de votre réseau. Sinon, le serveur DHCP ne démarrera pas.

Dans cet exemple, il y a des options globales pour tous les clients DHCP dans le sous-réseau et une plage, `range`, est déclarée. Les clients reçoivent une adresse IP au sein de `range`.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
option routers                  192.168.1.254;
option subnet-mask              255.255.255.0;

option domain-name              "example.com";
option domain-name-servers       192.168.1.1;

option time-offset              -18000;     # Eastern Standard Time

range 192.168.1.10 192.168.1.100;
}
```

Exemple 18-1. Déclaration de sous-réseau

Tous les sous-réseaux partageant le même réseau physique doivent être déclarés dans une déclaration `shared-network` comme le montre l'Exemple 18-2. Les paramètres se trouvant au sein du fichier `shared-network` mais en dehors des déclarations `subnet` sont considérés comme des paramètres globaux. Le nom du fichier `shared-network` doit correspondre à un titre descriptif du réseau, comme test-lab pour décrire tous les réseaux dans un environnement de labo de tests.

```
shared-network name {
option domain-name              "test.redhat.com";
option domain-name-servers      ns1.redhat.com, ns2.redhat.com;
option routers                  192.168.1.254;
more parameters for EXAMPLE shared-network
subnet 192.168.1.0 netmask 255.255.255.0 {
parameters for subnet
range 192.168.1.1 192.168.1.31;
}
subnet 192.168.1.32 netmask 255.255.255.0 {
parameters for subnet
range 192.168.1.33 192.168.1.63;
}
}
```

Exemple 18-2. Déclaration de réseau partagé

Comme l'illustre l'Exemple 18-3, la déclaration `group` peut être utilisée pour appliquer des paramètres globaux à un groupe de déclarations. Vous pouvez regrouper des réseaux partagés, des sous-réseaux, des hôtes ou autres.

```
group {
option routers                  192.168.1.254;
option subnet-mask              255.255.255.0;

option domain-name              "example.com";
option domain-name-servers       192.168.1.1;

option time-offset              -18000;     # Eastern Standard Time

host apex {
option host-name "apex.example.com";
hardware ethernet 00:A0:78:8E:9E:AA;
fixed-address 192.168.1.4;
}

host raleigh {
option host-name "raleigh.example.com";
hardware ethernet 00:A1:DD:74:C3:F2;
fixed-address 192.168.1.6;
}
}
```

Exemple 18-3. Déclaration de groupe

Pour configurer un serveur DHCP qui attribue une adresse IP dynamique à un système dans un sous-réseau, modifiez l'Exemple 18-4 avec vos valeurs spécifiques. Un temps d'attribution par défaut, un temps d'attribution maximum et des valeurs de configuration réseau pour les clients sont déclarés. Cet exemple assigne aux systèmes clients, des adresses IP dans la gamme `range` 192.168.1.10 et 192.168.1.100.

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "example.com";

subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.10 192.168.1.100;
}
```

Exemple 18-4. Paramètre 'range'

Pour attribuer une adresse IP à un client sur la base de l'adresse MAC de la carte d'interface réseau, utilisez le paramètre `hardware ethernet` dans une déclaration `host`. Comme le montre l'Exemple 18-5, la déclaration `host apex` indique que la carte d'interface réseau avec l'adresse MAC 00:A0:78:8E:9E:AA doit toujours recevoir l'adresse IP 192.168.1.4.

Notez que vous pouvez également utiliser le paramètre facultatif `host-name` pour attribuer un nom d'hôte au client.

```
host apex {
option host-name "apex.example.com";
hardware ethernet 00:A0:78:8E:9E:AA;
fixed-address 192.168.1.4;
}
```

Exemple 18-5. Adresse IP statique utilisant DHCP

Astuce

Vous pouvez utiliser le fichier de configuration d'exemple figurant dans Red Hat Linux 9 comme point de départ, puis y ajouter vos propres options de configuration personnalisées. Copiez-le à l'emplacement approprié à l'aide de la commande:

```
cp
/usr/share/doc/dhcp-<numéro-de-version>/dhcpd.conf.sample /etc/dhcpd.conf
```

(où <*numéro-de-version*> correspond à la version DHCP que vous utilisez).

Pour obtenir une liste complète des options et de leur fonction, reportez-vous à la page de manuel relative à dhcp-options.

18.2.2. Base de données d'attribution

Sur le serveur DHCP, le fichier `/var/lib/dhcp/dhcpd.leases` stocke la base de données d'attribution client DHCP. Ce fichier ne doit pas être modifié manuellement. Les informations d'attribution DHCP pour toutes les adresses IP récemment attribuées sont automatiquement stockées dans cette base de données. Ces informations comprennent la durée de l'attribution, le destinataire de l'attribution d'adresse IP, les dates de début et de fin pour l'attribution et l'adresse MAC de la carte d'interface réseau qui a été utilisée pour l'attribution.

Toutes les heures de la base de données d'attribution sont des heures 'Greenwich Mean Time' (GMT), et non pas des heures locales.

La base de données d'attribution est recréée de temps en temps de façon à ce que sa taille ne soit pas trop grande. Tout d'abord, toutes les attributions connues sont sauvegardées dans une base de données d'attribution temporaire. Le fichier `dhcpd.leases` est renommé `dhcpd.leases~`, et la base de données d'attribution temporaire est copiée dans `dhcpd.leases`.

Le démon DHCP peut être anéanti et le système peut se bloquer après le changement de nom de la base de données d'attribution, avant la création du nouveau fichier. Si tel est le cas, aucun fichier `dhcpd.leases` n'est nécessaire pour lancer le service. Dans ce cas, ne créez pas de nouveau fichier d'attribution. Si vous le faites, toutes les anciennes attributions seront perdues, et cela entraînera de nombreux problèmes. Vous devez dans ce cas changer le mon du fichier de sauvegarde `dhcpd.leases~` `dhcpd.leases` puis lancer le démon.

18.2.3. Lancement et interruption du serveur

Important

La première fois que vous lancez le serveur DHCP, celui-ci ne fonctionnera pas si le fichier `dhcpd.leases` n'existe pas préalablement. Si le fichier n'existe pas, utilisez la commande `touch /var/lib/dhcp/dhcpd.leases` pour le créer.

Pour lancer le service DHCP, utilisez la commande `/sbin/service dhcpd start`. Pour interrompre le serveur DHCP, utilisez la commande `/sbin/service dhcpd stop`. Si vous voulez que le démon démarre automatiquement à l'amorçage du système, reportez-vous au Chapitre 14 pour en savoir plus sur la gestion des services.

Si vous avez plusieurs interfaces réseau attachées au système, mais que vous voulez le démarrage du serveur DHCP seulement sur l'une d'elles, vous pouvez configurer le serveur DHCP afin qu'il démarre uniquement sur ce périphérique. Dans `/etc/sysconfig/dhcpd`, ajoutez le nom de l'interface à la liste de `DHCPDARGS`:

```
# Command line options here
DHCPDARGS=eth0
```

Il s'agit de quelque chose d'utile si vous avez un ordinateur protégé par un pare-feu et doté de deux cartes réseau. L'une d'elles peut être configurée comme client DHCP pour récupérer une adresse IP d'Internet. L'autre peut servir de serveur DHCP pour le réseau interne se trouvant derrière le pare-feu. En ne spécifiant que la carte réseau connectée au réseau interne, votre système sera plus sûr puisque les utilisateurs ne pourront pas se connecter au démon par le biais de l'Internet.

Options de la ligne de commande pouvant être spécifiées dans `/etc/sysconfig/dhcpd`:

- `-p <numport>` — Spécifie le numéro de port udp sur lequel dhcp est en attente. Le port par défaut est le 67. Le serveur DHCP transmet les réponses aux clients DHCP à un numéro de port supérieur au port udp spécifié. Par exemple, si vous acceptez le port 67 (port par défaut), le serveur attend sur le port 67 les requêtes et sur le port 68 les réponses au client. Si vous spécifiez un port et que vous utilisez l'agent de relais DHCP, vous devez spécifier le même port d'attente pour l'agent de relais DHCP. Pour obtenir de plus amples informations sur le sujet, reportez-vous à la Section 18.2.4.
- `-f` — Exécute le démon comme processus de front. Cette option est principalement utilisée pour le débogage.
- `-d` — Inscrit le démon du serveur DHCP dans le descripteur d'erreurs standard. Cette option est principalement utilisée pour le débogage. Si elle n'est pas spécifiée, l'inscription est faite dans `/var/log/messages`.

- `-cf` *`nomfichier`* — Spécifie l'emplacement du fichier de configuration, par défaut `/etc/dhcpd.conf`.
- `-lf` *`nom-fichier`* Spécifie l'emplacement du fichier de la base de données d'attribution. Si ce fichier existe déjà, il est très important que le même fichier soit utilisé chaque fois que le serveur DHCP est démarré. Il est fortement recommandé de n'utiliser cette option qu'à des fins de débogage sur des machines non productives. L'emplacement par défaut est `/var/lib/dhcp/dhcpd.leases`.
- `-q` — N'imprime pas l'intégralité du message de copyright au démarrage du démon.

18.2.4. Agent de relais DHCP

L'agent de relais DHCP (`dhcrelay`) vous permet de relayer les requêtes DHCP et BOOTP d'un sous-réseau ne disposant pas de serveur DHCP vers un ou plusieurs serveurs DHCP sur d'autres sous-réseaux.

Lorsqu'un client DHCP demande des informations, l'agent de relais DHCP transfère la requête à la liste de serveurs DHCP spécifiés lors du démarrage de l'agent de relais DHCP. Lorsqu'un serveur DHCP renvoie une réponse, la réponse est diffusée sur le réseau ayant envoyé la requête d'origine.

L'agent de relais DHCP attend les requêtes DHCP sur toutes les interfaces à moins que les interfaces ne soient spécifiées dans `/etc/sysconfig/dhcrelay` avec la directive `INTERFACES`.

Pour démarrer l'agent de relais DHCP, utilisez la commande `service dhcrelay start`.

18.3. Configuration d'un client DHCP

La première étape de la configuration d'un client DHCP consiste à vérifier que le noyau reconnaît bien la carte d'interface réseau. La plupart des cartes sont reconnues lors du processus d'installation et le système est configuré pour utiliser le module de noyau correspondant à la carte. Si vous installez une carte après l'installation, **Kudzu** [1] devrait la reconnaître et vous demander de configurer le module de noyau correspondant. Consultez la liste de compatibilité de matériel Red Hat Linux disponible à l'adresse http://hardware.redhat.com/hcl/. Si la carte réseau n'est pas configurée par le programme d'installation ou **Kudzu** et que vous savez quel module de noyau vous devez charger pour cette carte, reportez-vous au Chapitre 31 pour en savoir plus sur le chargement de modules de noyau.

Pour configurer manuellement un client DHCP, vous devez modifier le fichier `/etc/sysconfig/network` afin d'activer la mise en réseau et le fichier de configuration pour chacun des périphériques réseau dans le répertoire `/etc/sysconfig/network-scripts`. Dans ce répertoire, chaque périphérique doit disposer d'un fichier de configuration nommé `ifcfg-eth0`, `eth0` correspondant au nom du périphérique réseau.

Le fichier `/etc/sysconfig/network` doit contenir la ligne suivante:

```
NETWORKING=yes
```

Vous pourriez avoir plus d'informations dans ce fichier, mais la variable `NETWORKING` doit être configurée sur `yes` pour que la mise en réseau s'active au démarrage.

Le fichier `/etc/sysconfig/network-scripts/ifcfg-eth0` doit contenir les lignes ci-dessous:

```
DEVICE=eth0
BOOTPROTO=dhcp
```

1. **Kudzu** est un outil d'analyse du matériel exécuté au démarrage pour déterminer quel matériel a été ajouté ou enlevé du système.

```
ONBOOT=yes
```

Il vous faut un fichier de configuration pour chacun des périphériques que vous souhaitez configurer afin d'utiliser DHCP.

Si vous préférez une interface graphique pour la configuration d'un client DHCP, reportez-vous au Chapitre 12 pour en savoir plus sur l'utilisation de l'**Outil d'administration de réseau** pour configurer une interface réseau qui utilisera DHCP.

18.4. Ressources supplémentaires

Pour les options de configuration qui n'ont pas été couvertes ici, veuillez vous reporter aux ressources suivantes.

18.4.1. Documentation installée

- La page de manuel relative à `dhcpd` — décrit le fonctionnement du démon DHCP.
- La page de manuel relative à `dhcpd.conf` — explique comment configurer le fichier de configuration DHCP et fournit des exemples.
- La page de manuel relative à `dhcpd.leases` — explique comment configurer le fichier d'attribution DHCP et fournit des exemples.
- La page de manuel relative à `dhcp-options` — explique la syntaxe de déclaration des options DHCP dans `dhcpd.conf` et fournit des exemples.
- La page de manuel relative à `dhcrelay` — explique le fonctionnement de l'agent de relais DHCP et les options de configuration correspondantes.

Chapitre 19.

Configuration du Serveur HTTP Apache

Dans Red Hat Linux 8.0, le paquetage du Serveur HTTP Apache a été mis à jour à la version 2.0, qui utilise différentes options de configuration. En outre, depuis la version Red Hat Linux 8.0, le paquetage RPM a été rebaptisé `httpd`. Si vous souhaitez effectuer manuellement la migration d'un fichier de configuration existant, reportez-vous au guide de migration à l'adresse suivante: `/usr/share/doc/httpd-<vers>/migration.html` ou au *Guide de référence de Red Hat Linux* pour obtenir de plus amples informations.

Si vous avez configuré le Serveur HTTP Apache à l'aide de l'**Outil de configuration HTTP** dans une version précédente de Red Hat Linux puis effectué une mise à niveau, il est possible d'utiliser cette application afin de migrer le fichier de configuration vers le nouveau format correspondant à la version 2.0. Lancez l'**Outil de configuration HTTP**, apportez tous les changements nécessaires à la configuration, puis enregistrez-la. Le fichier de configuration enregistré sera compatible avec la version 2.

L'**Outil de configuration HTTP** vous permet de configurer le fichier de configuration `/etc/httpd/conf/httpd.conf` pour le Serveur HTTP Apache. Il n'utilise pas les anciens fichiers de configuration `srm.conf` ou `access.conf`; vous pouvez donc les laisser vides. Il est possible, à partir de l'interface graphique, de configurer des directives telles que des hôtes virtuels, des attributs de journalisation ou encore un nombre maximal de connexions.

Seuls les modules livrés avec Red Hat Linux peuvent être configurés avec l'**Outil de configuration HTTP**. Si vous installez des modules supplémentaires, il ne vous sera pas possible de les configurer à l'aide de cet outil.

Les paquetage RPM `httpd` et `redhat-config-httpd` doivent être préalablement installés si vous souhaitez utiliser l'**Outil de configuration HTTP**. Pour son fonctionnement, il a également besoin du système X Window et des privilèges de super-utilisateur (ou root). Pour démarrer l'application, rendez-vous au bouton **Menu principal => Paramètres de système => Paramètres de serveur => Serveur HTTP** ou tapez la commande `redhat-config-httpd` à l'invite du shell (par exemple, dans un terminal XTerm ou GNOME).

Attention

N'éditez pas manuellement le fichier de configuration `/etc/httpd/conf/httpd.conf` si vous désirez utiliser cet outil. L'**Outil de configuration HTTP** génère automatiquement ce fichier une fois que vous avez enregistré vos changements et quitté le programme. Si vous souhaitez ajouter des modules supplémentaires ou des options de configuration qui ne sont pas disponibles dans l'**Outil de configuration HTTP**, vous ne pouvez pas utiliser cet outil.

Ci-dessous figurent les étapes principales de la configuration du Serveur HTTP Apache à l'aide de l'**Outil de configuration HTTP**:

1. Configurez les paramètres de base dans l'onglet **Main** (Principal).
2. Cliquez sur l'onglet **Virtual Hosts** (Hôtes virtuels) et configurez les paramètres par défaut.
3. Dans l'onglet **Virtual Hosts** (Hôtes virtuels), configurez l'hôte virtuel par défaut.
4. Si vous souhaitez servir plusieurs URL ou hôtes virtuels, ajoutez les hôtes virtuels supplémentaires.
5. Configurez les paramètres du serveur dans l'onglet **Server** (serveur).

6. Configurez les paramètres de connexion dans l'onglet **Performance Tuning** (Réglage des performances).
7. Copiez tous les fichiers nécessaires dans les répertoires `DocumentRoot` et `cgi-bin`.
8. Quittez l'application et choisissez d'enregistrer vos paramètres.

19.1. Paramètres de base

Utilisez l'onglet **Main** (Principal) pour configurer les paramètres de base du serveur.

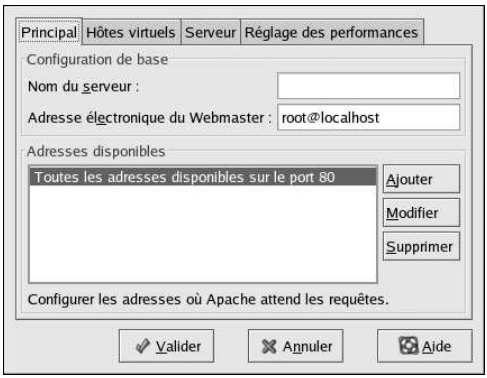

Figure 19-1. Paramètres de base

Entrez un nom de domaine pleinement qualifié pour lequel vous avez des autorisations d'accès dans la zone de texte **Server Name** (Nom de serveur). Cette option correspond à la directive `ServerName` dans `httpd.conf`. Cette directive `ServerName` définit le nom d'hôte du serveur Web. Elle est utilisée lors de la création d'URL de retransmission. Si vous ne définissez pas de nom de serveur, le serveur Web essaie de le résoudre à partir de l'adresse IP du système. Le nom de serveur ne doit pas forcément être identique au nom de domaine résolu à partir de l'adresse IP du serveur. Il se peut par exemple que vous souhaitiez donner au serveur le nom www.your_domain.com alors que son véritable nom DNS est en fait foo.example.com.

Entrez l'adresse électronique de la personne qui met à jour le serveur Web dans la zone de texte **Adresse électronique du Webmaster**. Cette option correspond à la directive `ServerAdmin` dans `httpd.conf`. Si vous configurez les pages d'erreur du serveur de façon à ce qu'elles contiennent une adresse électronique, celle-ci sera alors utilisée pour transmettre tout problème à l'administrateur du serveur. La valeur par défaut est root@localhost.

Utilisez la zone **Available Addresses** (Adresses disponibles) pour définir les ports sur lesquels le serveur acceptera les requêtes entrantes. Cette option correspond à la directive `Listen` dans `httpd.conf`. Par défaut, Red Hat configure le Serveur HTTP Apache de manière à ce qu'il écoute le port 80 pour des communications Web non-sécurisées.

Cliquez sur le bouton **Add** pour définir des ports supplémentaires pour la réception de requêtes. Une fenêtre semblable à celle reproduite dans la Figure 19-2 apparaîtra. Vous pouvez choisir, soit l'option **Listen to all addresses** pour écouter toutes les adresses IP sur le port défini, ou vous pouvez spécifier une adresse IP spécifique à laquelle le serveur acceptera des connexions dans le champ d'adresse, **Address**. Ne spécifiez qu'une seule adresse IP par numéro de port. Si vous souhaitez préciser plus d'une adresse IP pour le même numéro de port, saisissez une entrée pour chacune des adresses IP. Dans la mesure du possible, utilisez une adresse IP au lieu d'un nom de domaine afin d'éviter l'échec

de la recherche de DNS. Reportez-vous à l'adresse: http://httpd.apache.org/docs-2.0/dns-caveats.html pour de plus amples informations sur les *Problèmes en relation avec DNS et Apache*.

L'entrée d'un astérisque (*) dans le champ **Address** revient à choisir **Listen to all addresses**. En cliquant sur le bouton **Edit** dans le cadre **Available Addresses** vous obtiendrez la même fenêtre que celle apparaissant en pressant sur le bouton **Add** mais les champs seront remplis pour les entrées sélectionnées. Pour effacer une entrée, sélectionnez-la et appuyez sur le bouton **Delete**.

Astuce

Si vous configurez le serveur pour qu'il soit en mode réception sur un port inférieur à 1024, vous devrez être connecté en tant que super-utilisateur (ou root) pour pouvoir le lancer. Par contre, pour le port 1024 ou les ports supérieurs, il suffit d'être connecté en tant que simple utilisateur pour lancer `httpd`.

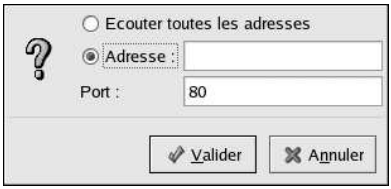

Figure 19-2. Adresses disponibles

19.2. Paramètres par défaut

Après avoir défini **Nom du serveur**, **l'adresse électronique du Webmaster** et **Addresses disponibles**, cliquez sur l'onglet **Hôtes virtuels** puis sur le bouton **Modifier les paramètres par défaut**. La fenêtre reproduite dans la Figure 19-3 s'ouvre alors. Configurez les paramètres par défaut pour votre serveur Web dans cette fenêtre. Si vous ajoutez un hôte virtuel, les paramètres que vous indiquerez auront la priorité pour cet hôte virtuel. Si une directive n'est pas définie dans les paramètres de l'hôte virtuel, la valeur par défaut est utilisée.

19.2.1. Configuration du site

Les valeurs par défaut de **Liste de recherche page répertoire** et **Pages d'erreur** fonctionnent pour la plupart des serveurs. Dans le doute, ne les modifiez pas.

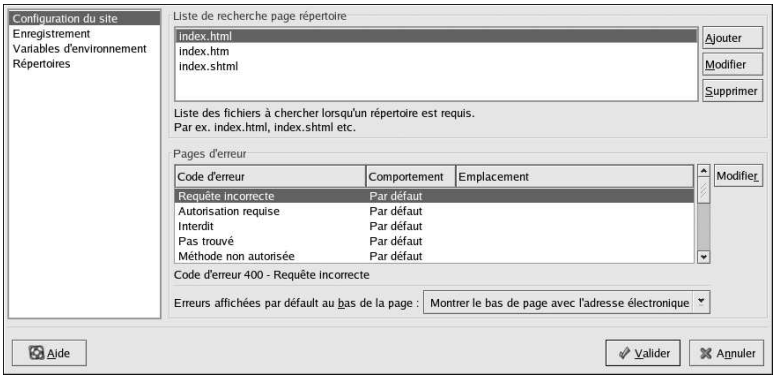

Figure 19-3. Configuration du site

Les entrées énumérées dans **Liste de recherche de pages répertoires** définissent la directive `DirectoryIndex`. `DirectoryIndex` est la page par défaut renvoyée par le serveur lorsqu'un utilisateur demande l'index d'un répertoire en ajoutant une barre oblique (/) à la fin du nom de ce répertoire.

Par exemple, lorsque des utilisateurs demandent la page http://*`www.example.com/this_directory/`*, ils recevront soit la page `DirectoryIndex`, si elle existe, soit une liste de répertoires générée par le serveur. Ce dernier essaiera de trouver un des fichiers listés dans la directive `DirectoryIndex` et renverra le premier qu'il trouvera. S'il ne trouve aucun de ces fichiers et que `Options Indexes` a ce répertoire comme valeur, le serveur générera une liste des sous-répertoires et fichiers contenus dans ce répertoire et la renverra, dans un format HTML.

Utilisez la section **Code d'erreur** pour configurer le Serveur HTTP Apache afin qu'il redirige le client vers une URL locale ou externe en cas de problème ou d'erreur. Cette option correspond à la directive `ErrorDocument`. Si un problème ou une erreur survient lorsqu'un client essaie de se connecter au Serveur HTTP Apache, le bref message d'erreur indiqué dans la colonne **Code d'erreur** s'affiche par défaut. Pour remplacer cette configuration par défaut, sélectionnez le code d'erreur et cliquez sur le bouton **Modifier**. Choisissez **Défaut** afin d'afficher le message d'erreur par défaut. Sélectionnez **URL** pour rediriger le client vers une URL externe et entrez une URL complète, y compris http:// dans le champ **Emplacement**. Sélectionnez **Fichier** pour rediriger le client vers une URL interne et entrez un emplacement de fichier sous le document root du serveur Web. L'emplacement doit commencer par une barre oblique (/) et être relatif au document root.

Par exemple, pour rediriger un code d'erreur "404 Not Found" (impossible de trouver la page) vers une page Web que vous avez créée dans un fichier nommé `404.html`, copiez `404.html` dans *`DocumentRoot`*`/errors/404.html`. Dans ce cas, *`DocumentRoot`* correspond au répertoire Document Root que vous avez défini (la valeur par défaut est `/var/www/html`). Sélectionnez ensuite **Fichier** comme comportement pour le code d'erreur **404 - Not Found** et entrez `/errors/404.html` dans le champ **Emplacement**.

Vous pouvez choisir l'une des options suivantes dans le menu **Erreurs affichées par défaut au bas de la page**:

- **Montrer la bas de page avec adresse électronique** — affiche le bas de page par défaut sur chacune des pages d'erreur ainsi que l'adresse électronique de l'administrateur du site Web spécifiés par la directive `ServerAdmin`. Reportez-vous à la Section 19.3.1.1 pour plus d'informations sur la configuration de la directive `ServerAdmin`.
- **Montrer le bas de page** — n'affiche que le bas de page par défaut sur les pages d'erreur.
- **Aucun bas de page** — n'affiche aucun bas de page sur les pages d'erreur.

19.2.2. Journalisation

Par défaut, le serveur enregistre le journal des transferts dans le fichier `/var/log/httpd/access_log` et le journal des erreurs dans le fichier `/var/log/httpd/error_log`.

Le journal des transferts contient la liste de toutes les tentatives d'accès au serveur Web. Il enregistre l'adresse IP des clients qui essaient de se connecter, la date ainsi que l'heure de leurs tentatives et les fichiers du serveur Web auxquels ils veulent accéder. Entrez le chemin d'accès et le nom du fichier où enregistrer ces informations. Si le chemin d'accès et le nom de fichier ne commencent pas par une barre oblique (/), le chemin est alors relatif au répertoire root du serveur, tel que vous l'avez configuré. Cette option correspond à la directive `TransferLog`.

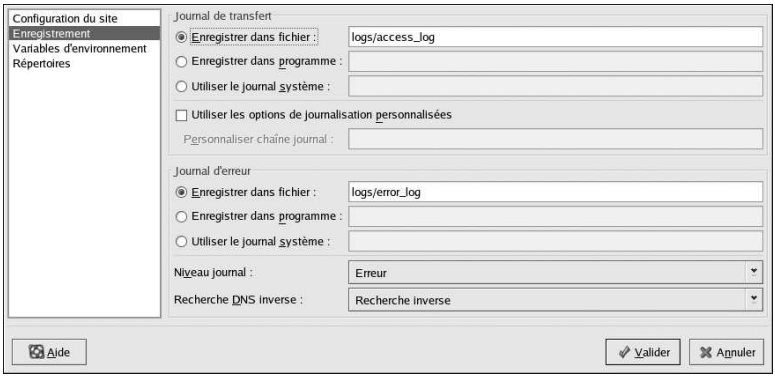

Figure 19-4. Journalisation

Vous pouvez configurer un format de journal personnalisé en cochant l'option **Utiliser les options de journalisation personnalisées** et en entrant une chaîne de journal personnalisée dans le champ **Personnaliser chaîne journal**. Cela permet de configurer la directive `LogFormat`. Reportez-vous à l'adresse suivante:http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#formats pour obtenir de plus amples informations sur le format de cette directive.

Le journal des erreurs contient une liste des erreurs de serveur. Entrez le chemin d'accès et le nom du fichier où enregistrer ces informations. Si le chemin d'accès et le nom de fichier ne commencent pas par une barre oblique (/), le chemin est alors relatif au répertoire root du serveur, tel que vous l'avez configuré. Cette option correspond à la directive `ErrorLog`.

Utilisez le menu **Niveau journal** afin de définir le degré de prolixité des messages dans le journal des erreurs. Vous avez le choix (du moins prolixe au plus prolixe) entre emerg, alert, crit, error, warn, notice, info et debug. Cette option correspond à la directive `LogLevel`.

La valeur choisie dans le menu **Recherche DNS inverse** définit la directive `HostnameLookups`. Choisir **Aucune recherche inverse** (No Reverse Lookup) configure la valeur sur "off". Choisir **Recherche inverse** (Reverse Lookup) configure la valeur sur "on". Choisir **Double recherche inverse** (Double Reverse Lookup) configure la valeur sur "double".

Si vous sélectionnez **Recherche inverse**, votre serveur résout automatiquement l'adresse IP de chaque connexion qui demande un document au serveur Web. Cela signifie que votre serveur effectue une ou plusieurs connexions au DNS afin de trouver le nom d'hôte correspondant à une adresse IP donnée.

Si vous sélectionnez **Double recherche inverse**, votre serveur effectue une double recherche DNS. Autrement dit, après avoir effectué une recherche inverse, le serveur en effectue une deuxième sur le

résultat obtenu. Au moins une des adresses IP de la seconde recherche doit correspondre à l'une des adresses de la première.

En règle générale, vous devriez conserver la valeur **Aucune recherche inverse** pour cette option car les requêtes DNS ajoutent une charge à votre serveur et risquent de le ralentir. Si votre serveur est très occupé, ces recherches, qu'elles soient simples ou doubles, peuvent avoir un effet assez perceptible.

De plus, les recherches inverses et doubles recherches inverses affectent l'activité Internet en général. Toutes les connexions individuelles effectuées pour vérifier les noms d'hôte s'additionnent. Aussi, pour le bien de votre propre serveur Web et de l'Internet, vous devriez conserver la valeur **Aucune recherche inverse**.

19.2.3. Variables d'environnement

Il est parfois nécessaire de modifier des variables d'environnement pour les scripts CGI et les pages à inclure (SSI) au niveau du serveur. Le Serveur HTTP Apache peut utiliser le module `mod_env` pour configurer les variables d'environnement transmises aux scripts CGI et aux pages SSI. Utilisez la page **Variables d'environment** pour configurer les directives de ce module.

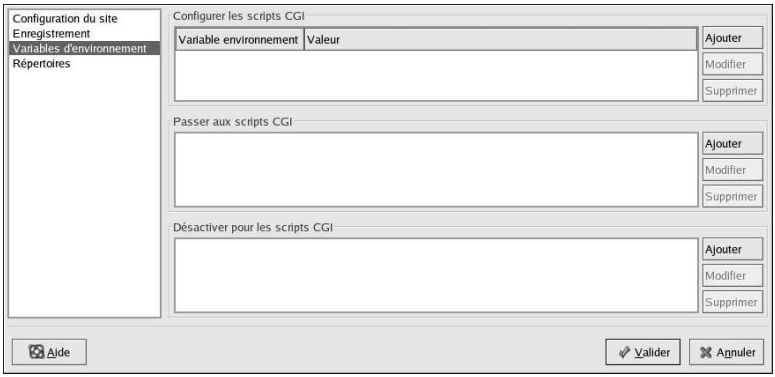

Figure 19-5. Variables d'environnement

Utilisez la section **Définir pour les scripts CGI** pour définir une variable d'environnement transmise aux scripts CGI et aux pages SSI. Par exemple, pour donner à la variable d'environnement `MAXNUM` la valeur `50`, cliquez sur le bouton **Ajouter** dans la section **Définir pour les scripts CGI** comme le montre la Figure 19-5 et tapez **`MAXNUM`** dans le champ de texte **Variable d'environment** et **`50`** dans le champ de texte **Valeur à définir**. Cliquez ensuite sur **OK** pour l'ajouter à la liste. La section **Définir pour les scripts CGI** sert à configurer la directive `SetEnv`.

Utilisez la section **Transmettre aux scripts CGI** pour transmettre la valeur d'une variable d'environnement aux scripts CGI lorsque le serveur est lancé pour la première fois. Pour visualiser cette variable d'environnement, entrez la commande `env` à l'invite du shell. Cliquez sur le bouton **Ajouter** dans la section **Transmettre aux scripts CGI** et entrez le nom de la variable dans la boîte de dialogue. Cliquez ensuite sur **OK** pour l'ajouter à la liste. La section **Transmettre aux scripts CGI** configure la directive `PassEnv` .

Si vous voulez supprimer une variable d'environnement afin que sa valeur ne soit pas transmise aux scripts CGI et aux pages SSI, utilisez la section **Dé-sélectionner pour les scripts CGI**. Cliquez sur **Ajouter** dans la section **Dé-sélectionner pour les scripts CGI** et entrez le nom de la variable d'environnement à désélectionner. Cliquez sur **OK** pour l'ajouter à la liste. Cela correspond à la directive `UnsetEnv` directive.

Pour modifier une de ces valeurs d'environnement, sélectionnez-la parmi la liste et cliquez sur le bouton **Éditer** correspondant. Pour supprimer toute entrée de la liste, sélectionnez-la puis cliquez sur le bouton **Supprimer** correspondant.

Pour en savoir plus sur les variables d'environnement du Serveur HTTP Apache, reportez-vous aux sources suivantes:

```
http://httpd.apache.org/docs-2.0/env.html
```

19.2.4. Répertoires

Utilisez la page **Répertoires** pour configurer des options de répertoires spécifiques. Cela correspond à la directive `<Répertoires>`.

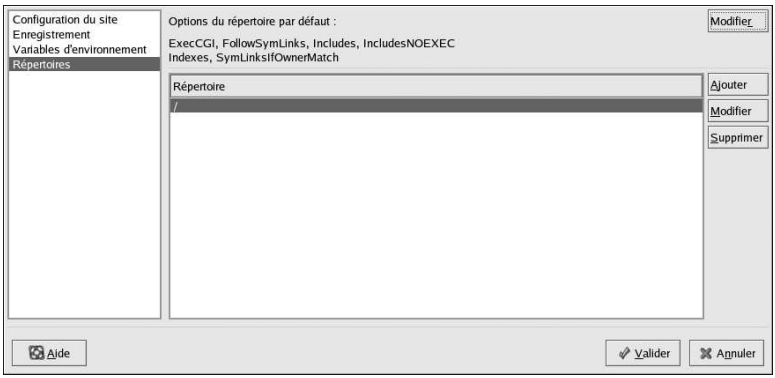

Figure 19-6. Répertoires

Cliquez sur le bouton **Modifier** dans le coin supérieur droit afin de configurer les **Options par défaut des répertoires** pour tous les répertoires non-spécifiés dans la liste **Répertoire** ci-dessous. Les options que vous sélectionnez sont énumérées en tant que directive d'options dans la directive `<Directory>`. Vous pouvez configurer les options suivantes:

- **ExecCGI** — permet l'exécution de scripts CGI. Les scripts CGI ne sont pas exécutés si cette option n'est pas sélectionnée.
- **FollowSymLinks** — permet aux liens symboliques d'être suivis.
- **Includes** — permet les inclusions sur le serveur.
- **IncludesNOEXEC** — permet les inclusions sur le serveur, mais désactive les commandes `#exec` et `#include` dans les scripts CGI.
- **Indexes** — affiche une liste formatée du contenu d'un répertoire, si aucun `DirectoryIndex` (tel que `index.html`) n'existe dans le répertoire demandé.
- **Multiview** — prend en charge la multivue à contenu variable; cette option est désactivée par défaut.
- **SymLinksIfOwnerMatch** — suit les liens symboliques uniquement si le propriétaire du fichier ou du répertoire cible est le même que celui du lien.

Si vous désirez spécifier des options pour des répertoires particuliers, cliquez sur le bouton **Ajouter** situé près de la zone de liste **Répertoire**. La fenêtre présentée dans la Figure 19-7 s'ouvre alors.

Entrez le répertoire à configurer dans le champ **Répertoire** situé au bas de la fenêtre. Sélectionnez les options dans la liste située à droite et configurez la directive `Order` au moyen des options situées à gauche. La directive `Order` contrôle l'ordre dans lequel les directives d'autorisation et de refus sont évaluées. Dans les champs de texte **Autoriser les hôtes à partir de** et **Refuser les hôtes à partir de**, vous pouvez spécifier l'un des éléments suivants:

- Autoriser tous les hôtes — entrez **`all`** pour autoriser l'accès à tous les hôtes.
- Nom de domaine partiel — autorise tous les hôtes dont le nom correspond à, ou se termine par, une chaîne spécifique.
- Adresse IP complète — accorde l'accès à une adresse IP spécifique.
- Un sous-réseau — par exemple **`192.168.1.0/255.255.255.0`**
- Une spécification CIDR de réseau — par exemple **`10.3.0.0/16`**

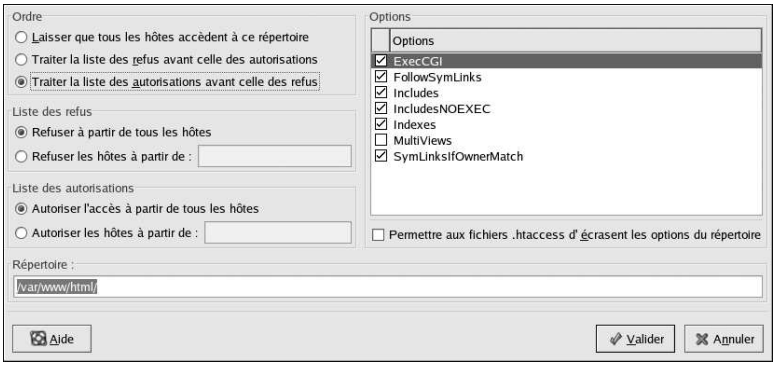

Figure 19-7. Paramètres des répertoires

Si vous cochez la case **Permettre aux fichiers .htaccess d'écraser les options du répertoire**, les directives de configuration du fichier `.htaccess` ont la priorité.

19.3. Paramètres des hôtes virtuels

Vous pouvez utiliser l'**Outil de configuration HTTP** pour configurer des hôtes virtuels. Les hôtes virtuels vous permettent d'exécuter différents serveurs pour différentes adresses IP, différents noms d'hôte ou différents ports sur un même ordinateur. Par exemple, vous pouvez exécuter les sites Web http://www.votre_domaine.com et http://www.votre_second_domaine.com sur le même serveur Web à l'aide d'hôtes virtuels. Cette option correspond à la directive <VirtualHost> pour l'hôte virtuel par défaut ainsi que pour les hôtes virtuels basés sur l'adresse IP. Cela correspond à la directive <NameVirtualHost> pour un hôte virtuel basé sur le nom.

Les directives définies pour un hôte virtuel ne s'appliquent qu'à cet hôte virtuel. Si une directive est définie pour l'ensemble du serveur au moyen du bouton **Modifier paramètres par défaut** et n'est pas définie dans les paramètres de l'hôte virtuel, le paramètre par défaut est alors utilisé. Par exemple, vous pourriez définir **Adresse électronique du Webmaster** dans l'onglet **Main** et ne pas indiquer d'adresse électronique individuelle pour chacun des hôtes virtuels.

L'**Outil de configuration HTTP** inclut un hôte virtuel par défaut (reportez-vous à la Figure 19-8).

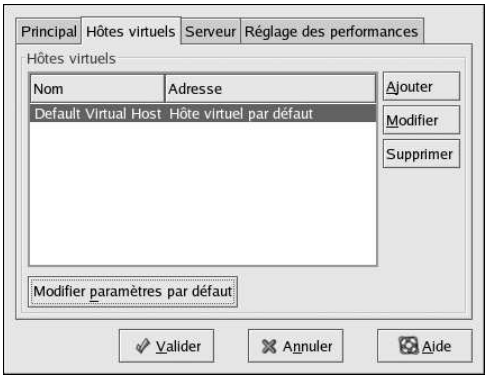

Figure 19-8. Hôtes virtuels

Vous trouverez plus d'informations sur les hôtes virtuels dans la documentation du Serveur HTTP Apache fournie sur votre ordinateur ou sur le site Web suivant: http://httpd.apache.org/docs-2.0/vhosts/.

19.3.1. Ajout et modification d'un hôte virtuel

Pour ajouter un hôte virtuel, cliquez sur l'onglet **Hôtes virtuels** puis sur le bouton **Ajouter**. Vous pouvez également modifier un hôte virtuel en le sélectionnant dans la liste, puis en cliquant sur le bouton **Modifier**.

19.3.1.1. Options générales

Les paramètres de **Options générales** ne s'appliquent qu'à l'hôte virtuel que vous configurez. Définissez le nom de l'hôte virtuel dans la zone de texte **Nom de l'hôte virtuel**. Ce nom est utilisé par l'**Outil de configuration HTTP** pour établir une distinction entre les hôtes virtuels.

Définissez la valeur de **Répertoire racine du document** en indiquant le répertoire qui contient le document racine (ou root) (index.html, par exemple) de l'hôte virtuel. Cette option correspond à la directive `DocumentRoot` dans la directive `<VirtualHost>`. Avant Red Hat Linux 7, la version du Serveur HTTP Apache fournie avec Red Hat Linux utilisait `/home/httpd/html` comme `DocumentRoot`. Toutefois, dans Red Hat Linux 9, le `DocumentRoot` par défaut est `/var/www/html`.

Adresse électronique du Webmaster correspond à la directive `ServerAdmin` dans la directive `VirtualHost`. Cette adresse électronique est utilisée dans le bas de page des pages d'erreur si vous choisissez d'y afficher un bas de page contenant une adresse électronique.

Dans la section **Informations sur l'hôte**, sélectionnez **Hôte virtuel par défaut**, **Hôte virtuel basé sur IP** ou **Hôte virtuel basé sur le nom**.

Hôte virtuel par défaut

Un seul hôte virtuel par défaut doit être configuré (n'oubliez pas qu'il n'existe qu'une seule configuration par défaut). Les paramètres par défaut de l'hôte virtuel sont utilisés lorsque l'adresse IP demandée n'est pas explicitement indiquée dans un autre hôte virtuel. Si aucun hôte virtuel par défaut n'est défini, les paramètres du serveur principal sont utilisés.

Hôte virtuel basé sur IP

Si vous choisissez **Hôte virtuel basé sur IP**, une fenêtre s'ouvre pour configurer la directive <VirtualHost> en fonction de l'adresse IP du serveur. Spécifiez cette adresse IP dans le champ

Adresse IP. Si vous spécifiez plusieurs adresses IP, séparez-les par un espace. Pour spécifier un port, utilisez la syntaxe *Adresse IP:Port*. Utilisez:* pour configurer tous les ports de l'adresse IP. Spécifiez le nom de l'hôte virtuel dans le champ **Nom d'hôte du serveur**.

Hôte virtuel basé sur le nom

Si vous sélectionnez **Hôte virtuel basé sur le nom**, une fenêtre s'ouvre pour configurer la directive `NameVirtualHost` en fonction du nom d'hôte du serveur. Spécifiez l'adresse IP dans le champ **Adresse IP**. Si vous spécifiez plusieurs adresses IP, séparez-les par un espace. Pour spécifier un port, utilisez la syntaxe *Adresse IP:Port*. Utilisez:* pour configurer tous les ports de l'adresse IP. Spécifiez le nom de l'hôte virtuel dans le champ **Nom d'hôte du serveur**. Dans la section **Alias**, cliquez sur **Ajouter** pour attribuer un surnom à l'hôte. Ajouter un surnom à cet hôte équivaut à ajouter une directive `ServerAlias` dans la directive `NameVirtualHost`.

19.3.1.2. SSL

Remarque

Vous ne pouvez pas utiliser un hôte virtuel basé sur un nom avec SSL car l'établissement d'une liaison SSL (lorsque le navigateur accepte le certificat du serveur Web sécurisé) s'effectue avant la requête HTTP qui identifie l'hôte virtuel basé sur le nom approprié. Par conséquent, si vous souhaitez utiliser un hôte virtuel basé sur un nom, vous devez utiliser votre serveur Web non-sécurisé.

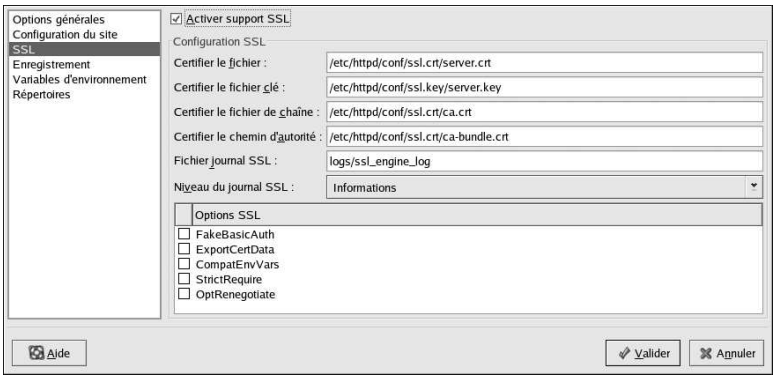

Figure 19-9. Prise en charge SSL

Si le Serveur HTTP Apache n'est pas configuré pour la prise en charge SSL, les communications entre le Serveur HTTP Apache et ses clients ne sont pas cryptées. Cela convient aux sites Web ne contenant aucune information personnelle ou confidentielle. Par exemple, un site Web Open Source qui distribue de la documentation et des logiciels Open Source n'a nullement besoin de communications sécurisées. En revanche, un site Web de commerce électronique qui traite des informations telles que des numéros de cartes de crédit devrait utiliser la prise en charge SSL Apache pour crypter ses communications. L'activation de la prise en charge SSL Apache permet d'utiliser le module de sécurité `mod_ssl`. Pour l'activer à partir de l'**Outil de configuration HTTP**, vous devez accorder l'accès par le port 443 sous l'onglet **Principal => Adresses disponibles**. Reportez-vous à la Section 19.1

pour avoir plus de détails. Sélectionnez ensuite le nom d'hôte virtuel dans l'onglet **Hôtes virtuels**, cliquez sur le bouton **Modifier**, sélectionnez **SSL** dans le menu de gauche et cochez l'option **Activer support SSL**, comme le montre la Figure 19-9. La section **Configuration SSL** est déjà configurée et contient un certificat numérique fictif. Ces certificats fournissent l'authentification au serveur Web sécurisé et identifient ce dernier auprès des navigateurs Web clients. Vous devez acheter votre propre certificat numérique. N'utilisez pas le certificat fictif fourni dans Red Hat Linux pour votre propre site Web. Pour obtenir davantage d'informations sur l'achat d'un certificat numérique approuvé par un fournisseur de certificats, reportez-vous au Chapitre 20.

19.3.1.3. Options supplémentaires pour les hôtes virtuels

Les options **Configuration du site**, **Variables d'environment** et **Répertoires** pour les hôtes virtuels correspondent aux mêmes directives que celles définies à l'aide du bouton **Modifier les paramètres par défaut**, à une différence près que les options définies ici s'appliquent aux hôtes virtuels individuels que vous configurez. Reportez-vous à la Section 19.2 afin d'avoir plus de détails sur ces options.

19.4. Paramètres du serveur

L'onglet **Serveur** vous permet de configurer les paramètres de base du serveur. Les paramètres par défaut attribués aux différentes options conviennent à la plupart des situations.

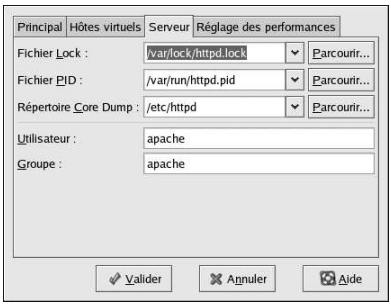

Figure 19-10. Configuration du serveur

La valeur **Lock File** correspond à la directive `LockFile`. Cette dernière définit le chemin d'accès au fichier de verrouillage utilisé lorsque le serveur est compilé avec USE_FCNTL_SERIALIZED_ACCEPT ou USE_FLOCK_SERIALIZED_ACCEPT. Il doit être enregistré sur le disque local. Nous vous conseillons de laisser la valeur par défaut, sauf si le répertoire `logs` est situé sur un partage NFS. Dans ce cas, changez la valeur par défaut par un emplacement sur le disque local, dans un répertoire qui ne peut être lu que par l'utilisateur root.

La valeur **Fichier PID** correspond à la directive `PidFile`. Cette directive définit le fichier dans lequel le serveur enregistre son ID de processus (pid). L'accès en lecture de ce fichier doit être réservé à l'utilisateur root. Il est préférable de laisser, dans la plupart des cas, la valeur par défaut.

La valeur **Répertoire Core Dump** correspond à la directive `CoreDumpDirectory`. Le Serveur HTTP Apache essaie de passer à ce répertoire avant de vider le noyau. La valeur par défaut est `ServerRoot`. Toutefois, si l'utilisateur sous lequel est exécuté le serveur ne peut écrire dans ce répertoire, le vidage du noyau ne peut être enregistré. Modifiez cette valeur en spécifiant un répertoire pour lequel cet

utilisateur a un droit d'écriture, si vous souhaitez enregistrer le vidage du noyau sur le disque à des fins de débogage.

La valeur **Utilisateur** (Utilisateur) correspond à la directive `User`. Elle définit l'ID utilisateur utilisé par le serveur pour répondre aux requêtes. Les paramètres de cet utilisateur déterminent les droits d'accès au serveur. Tout fichier inaccessible pour cet utilisateur le sera également pour les visiteurs de votre site Web. La valeur par défaut de `User` est apache.

L'utilisateur ne doit avoir que les autorisations nécessaires pour accéder aux fichiers qui doivent être visibles aux yeux du monde externe. Il sera aussi le propriétaire de tout processus CGI engendré par le serveur. De plus, il ne devrait pas être autorisé à exécuter du code si ce n'est pour répondre à des requêtes HTTP.

Avertissement

Si vous avez des doutes, ne donnez pas à la directive utilisateur, `User`, la valeur super-utilisateur (ou root). Cela provoquerait d'importantes brèches de sécurité au niveau de votre serveur Web.

Le processus `httpd` parent se lance tout d'abord en tant que root lors d'une exécution normale, mais est ensuite immédiatement transmis à l'utilisateur Apache. Le serveur doit être lancé en tant que super-utilisateur (ou root) car il a besoin de se rattacher à un port dont le numéro est inférieur à 1024 (et qui est donc par définition réservé au système), afin que ce port ne puisse être utilisé que par le super-utilisateur. Cependant, une fois que le serveur s'est attaché à son port, il transmet le processus à l'utilisateur apache avant d'accepter les demandes de connexion.

La valeur **Groupe** correspond à la directive `Group`. La directive `Group` est semblable à la directive `User`. `Group` définit le groupe sous lequel le serveur répond aux requêtes. Sa valeur par défaut est également apache.

19.5. Réglage des performances

Cliquez sur l'onglet **Réglage des performances** pour configurer le nombre maximal de processus serveur enfants souhaités ainsi que les options du Serveur HTTP Apache pour les connexions client. Les paramètres par défaut attribués à ces options conviennent à la plupart des situations. La modification de ces paramètres risque d'affecter les performances générales de votre serveur Web.

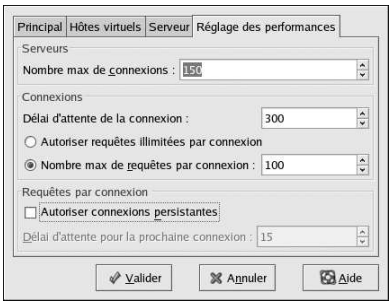

Figure 19-11. Réglage des performances

Configurez l'option **Nombre max de connexions** sur le nombre maximal de requêtes client simultanées que peut gérer le serveur. Pour chaque connexion, un processus `httpd` enfant est créé. Une fois

que le nombre maximal de processus est atteint, personne ne peut se connecter au serveur Web tant qu'un processus enfant n'est pas libéré. Vous ne pouvez pas donner à cette option une valeur supérieure à 256 sans effectuer une recompilation. Cette option correspond à la directive `MaxClients`.

Délai d'attente pour la connexion définit, en secondes, le temps pendant lequel le serveur doit attendre la réception et la transmission d'informations lors de communications. Plus spécifiquement, cette option définit le temps pendant lequel votre serveur attend pour recevoir une requête GET, des paquets TCP sur une requête POST ou PUT et le temps pendant lequel il attend les accusés de réception en réponse aux paquets TCP. Cette valeur est par défaut de 300 secondes, ce qui convient à la plupart des situations. Cette option correspond à la directive `TimeOut`.

Configurez **Nombre max de requêtes par connexion** sur le nombre maximal de requêtes autorisées par connexion persistante. La valeur par défaut est 100, ce qui doit convenir à la plupart des situations. Cette option correspond à la directive `MaxRequestsPerChild`.

Si vous cochez l'option **Autoriser requêtes illimitées par connexion**, la directive `MaxKeepAlive-Requests` prend la valeur 0 et un nombre illimité de requêtes est alors autorisé.

Si vous dé-sélectionnez l'option **Autoriser connexions persistantes**, la directive `KeepAlive` prend la valeur "false" (Faux). Si vous la cochez, la directive `KeepAlive` prend la valeur "true" (Vrai) et la directive `KeepAliveTimeout` prend alors comme valeur le nombre indiqué dans l'option **Délai d'attente pour la prochaine connexion**. Cette directive établit le nombre de secondes pendant lequel votre serveur attendra une requête ultérieure, après qu'une requête ait été servie, avant de fermer la connexion. Cependant, la valeur **Délai d'attente de connexion** s'applique une fois qu'une requête a été reçue.

Si vous indiquez une valeur élevée pour l'option **Connexions persistantes**, cela risque de de ralentir votre serveur, en fonction du nombre d'utilisateurs qui essaient de s'y connecter. Plus ils sont nombreux, plus le nombre de processus serveur qui attendent une autre connexion du dernier client à s'y être connecté est important.

19.6. Enregistrement des paramètres

Si vous ne souhaitez pas enregistrer vos paramètres de configuration du Serveur HTTP Apache, cliquez sur le bouton **Annuler** dans le coin inférieur droit de la fenêtre de l'**Outil de configuration HTTP**. Le système vous demande alors de confirmer cette décision. Si vous cliquez sur **Oui** pour confirmer ce choix, vos paramètres ne sont pas enregistrés.

Si vous souhaitez enregistrer vos paramètres de configuration du Serveur HTTP Apache, cliquez sur le bouton **OK** dans le coin inférieur droit de la fenêtre de l'**Outil de configuration HTTP**. Une fenêtre de dialogue s'affiche. Si vous cliquez sur **Oui**, vos paramètres sont enregistrés dans le fichier `/etc/httpd/conf/httpd.conf`. N'oubliez pas que le fichier de configuration d'origine est alors écrasé.

Si vous utilisez l'**Outil de configuration HTTP** pour la première fois, une boîte de dialogue vous avertit que le fichier de configuration a été modifié manuellement. Si l'**Outil de configuration HTTP** s'aperçoit que le fichier de configuration `httpd.conf` a été modifié manuellement, il enregistre le fichier modifié sous `/etc/httpd/conf/httpd.conf.bak`.

Important

Après avoir enregistré vos paramètres, vous devez redémarrer le démon `httpd` au moyen de la commande `service httpd restart`. Pour ce faire, vous devez être connecté en tant que super-utilisateur (ou root).

19.7. Ressources supplémentaires

Pour en apprendre davantage sur le Serveur HTTP Apache, reportez-vous aux sources d'informations indiquées ci-dessous.

19.7.1. Documentation installée

- Documentation du Serveur HTTP Apache — si le paquetage `httpd-manual` est installé et le démon du Serveur HTTP Apache (`httpd`) est en cours d'exécution, vous pouvez consulter la documentation du Serveur HTTP Apache. Ouvrez un navigateur Web et allez à l'adresse http://localhost du serveur qui exécute le Serveur HTTP Apache. Cliquez ensuite sur le lien **Documentation**.
- `/usr/share/docs/httpd-`*<version>* — Le document *Apache Migration HOWTO* contient une liste des changements apportés entre la version 1.3 et la version 2.0 ainsi que des informations relatives à la migration manuelle du fichier de configuration.

19.7.2. Sites Web utiles

- http://www.apache.org — *La Fondation Logicielle Apache (The Apache Software Foundation)*.
- http://httpd.apache.org/docs-2.0/ — La documentation de la Fondation Logicielle Apache (The Apache Software Foundation) sur le Serveur HTTP Apache version 2.0, y compris le *Guide de l'utilisateur du Serveur HTTP Apache Version 2.0*.
- http://localhost/manual/index.html — Après avoir lancé le Serveur HTTP Apache sur votre système local, vous pouvez consulter le document sur le Serveur HTTP Apache Version 2.0 à partir de l'URL.
- http://www.redhat.com/support/resources/web_ftp/apache.html — Le support de Red Hat maintient une liste de liens utiles au Serveur HTTP Apache.
- http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html — La base de connaissances centralisées Apache de Red Hat Linux compilée par Red Hat.

19.7.3. Livres sur le sujet

- *Apache: The Definitive Guide* de Ben Laurie et Peter Laurie, édité par O'Reilly & Associates, Inc.
- *Guide de référence de Red Hat Linux*; Red Hat, Inc. — Ce manuel inclut entre autres, des instructions sur la migration manuelle du Serveur HTTP Apache version 1.3 vers le Serveur HTTP Apache version 2.0, des informations détaillées sur les directives du Serveur HTTP Apache et des instructions pour l'ajout de modules au Serveur HTTP Apache.

redhat.

Chapitre 20.

Configuration du serveur sécurisé HTTP Apache

20.1. Introduction

Ce chapitre fournit des informations élémentaires sur Serveur HTTP Apache avec le module de sécurité `mod_ssl` activé pour utiliser la bibliothèque et le kit de programmes OpenSSL. La combinaison de ces 3 composants, fournis avec Red Hat Linux, sera appelée serveur Web sécurisé dans ce chapitre ou, tout simplement, serveur sécurisé.

Le module `mod_ssl` est un module de sécurité pour Serveur HTTP Apache. Il utilise les outils fournis par le projet OpenSSL pour ajouter une fonction très importante à Serveur HTTP Apache: la possibilité de crypter les communications. En effet, en cas d'utilisation d'un protocole HTTP normal, les communications entre un navigateur et un serveur Web se font en texte en clair et peuvent donc être interceptées et lues par toute personne se trouvant entre le navigateur et le serveur.

Ce chapitre ne prétend pas fournir une documentation exhaustive et exclusive pour l'un ou l'autre de ces programmes. En revanche, lorsque ce sera possible, ce guide vous indiquera d'autres sources d'informations où vous pourrez trouver des renseignements plus détaillés sur certains sujets.

Ce chapitre vous montrera comment installer ces programmes. Vous y apprendrez également les étapes nécessaires pour générer une clé privée ainsi qu'une demande de certificat, comment générer votre propre certificat auto-signé et installer un certificat à utiliser avec votre serveur sécurisé.

Le fichier de configuration `mod_ssl` se trouve dans `/etc/httpd/conf.d/ssl.conf`. Pour charger ce fichier et donc pour que `mod_ssl` fonctionne, vous devez avoir l'instruction `Include conf.d/*.conf` dans `/etc/httpd/conf/httpd.conf`. Cette instruction est incluse par défaut dans le fichier de configuration par défaut de Serveur HTTP Apache dans Red Hat Linux 9.

20.2. Présentation des paquetages relatifs à la sécurité

Pour activer le serveur sécurisé, vous devez au minimum avoir installé les paquetages suivants:

`httpd`

Le paquetage `httpd` contient le démon `httpd` et quelques utilitaires connexes, fichiers de configuration, icônes, modules Serveur HTTP Apache, pages de manuel et autres fichiers utilisés par Serveur HTTP Apache.

`mod_ssl`

Le paquetage `mod_ssl` contient le module `mod_ssl`, qui fournit un cryptage puissant pour Serveur HTTP Apache via les protocoles SSL ('Secure Sockets Layer') et TLS ('Transport Layer Security').

`openssl`

Le paquetage `openssl` contient le kit de programmes OpenSSL. Celui-ci met en oeuvre les protocoles SSL et TSL et inclut aussi une bibliothèque de cryptage à usage général.

En outre, d'autres paquetages logiciels fournis avec Red Hat Linux peuvent offrir certaines fonctionnalités de sécurité (mais ils ne sont pas nécessaires pour que le serveur sécurisé fonctionne):

`httpd-devel`

Le paquetage `httpd-devel` contient les fichiers Serveur HTTP Apache à inclure, des en-têtes et l'utilitaire APXS. Vous aurez besoin de tout cela si vous souhaitez charger des modules supplémentaires, autres que les modules fournis avec ce produit. Reportez-vous au *Guide de référence de Red Hat Linux* pour avoir plus d'informations sur le chargement de modules dans votre serveur sécurisé à l'aide de la fonctionnalité DSO d'Apache.

Si vous n'avez pas l'intention de charger d'autres modules dans votre Serveur HTTP Apache, vous n'avez pas besoin de ce paquetage.

`httpd-manual`

Le paquetage `httpd-manual` contient *Apache 1.3 User's Guide* du projet Apache au format HTML. Ce manuel est aussi disponible sur le Web à l'adresse suivante: http://httpd.apache.org/docs-2.0/.

Paquetages OpenSSH

Les paquetages OpenSSH fournissent l'ensemble OpenSSH d'outils de connexion réseau pour se connecter à un ordinateur distant et y exécuter des commandes. Les outils OpenSSH cryptent tout trafic (y compris les mots de passe); vous pouvez donc empêcher l'écoute électronique, le détournement de connexion et d'autres attaques au niveau de la communication entre votre ordinateur et l'ordinateur distant.

Le paquetage `openssh` contient des fichiers clé requis aussi bien par les programmes client OpenSSH que le serveur OpenSSH. Le paquetage `openssh` contient également `scp`, un substitut sécurisé de `rcp` (pour la copie de fichiers entre des ordinateurs).

Le paquetage `openssh-askpass` prend en charge l'affichage d'une boîte de dialogue qui vous invite à entrer un mot de passe lors de l'utilisation de l'agent OpenSSH.

Le paquetage `openssh-askpass-gnome` contient une boîte de dialogue de l'environnement de bureau graphique GNOME qui s'affiche lorsque les programmes OpenSSH demandent un mot de passe. Si vous utilisez GNOME et des utilitaires OpenSSH, vous devriez installer ce paquetage.

Le paquetage `openssh-server` contient le démon du shell sécurisé `sshd` et des fichiers connexes. Ce démon est le côté serveur de la suite OpenSSH et doit être installé sur votre ordinateur hôte si vous désirez autoriser la connexion de clients SSH à votre hôte.

Le paquetage `openssh-clients` contient les programmes client nécessaires à l'établissement de connexions cryptées vers des serveurs SSH, y compris les programmes suivants: `ssh`, un substitut sécurisé de `rsh`; `sftp`, un substitut sécurisé de `ftp` (pour le transfert de fichiers entre machines); et `slogin`, un substitut sécurisé de `rlogin` ((pour les connexions à distance) et `telnet` (pour les communications avec un autre hôte via le protocole TELNET).

Pour en savoir plus sur OpenSSH, reportez-vous au Chapitre 15 de ce manuel, au *Guide de référence de Red Hat Linux* et au site Web de OpenSSH à l'adresse suivante: http://www.openssh.com.

`openssl-devel`

Le paquetage `openssl-devel` contient les bibliothèques statiques et les fichiers à inclure nécessaires pour compiler des applications qui prennent en charge divers algorithmes de cryptographie et protocoles. Installez ce paquetage uniquement si vous développez des applications qui incluent la prise en charge SSL — vous n'en avez pas besoin pour utiliser SSL.

`stunnel`

Le paquetage `stunnel` fournit le l'enveloppeur SSL Stunnel. Stunnel prend en charge le cryptage SSL des connexions TCP, il peut donc offrir le cryptage aux démons et protocoles qui ne reconnaissent pas SSL (tels que POP, IMAP et LDAP) sans avoir à apporter de changements au code du démon.

Le Tableau 20-1 affiche un résumé des paquetages du serveur sécurisé et des informations indiquant si chacun des paquetages est facultatif ou non pour l'installation d'un serveur sécurisé.

Nom des paquetages	Facultatif
`httpd`	non
`mod_ssl`	non
`openssl`	non
`httpd-devel`	oui
`httpd-manual`	oui
`openssh`	oui
`openssh-askpass`	oui
`openssh-askpass-gnome`	oui
`openssh-clients`	oui
`openssh-server`	oui
`openssl-devel`	oui
`stunnel`	oui

Tableau 20-1. Paquetages de sécurité

20.3. Présentation des certificats et de la sécurité

Votre serveur sécurisé offre la sécurité à l'aide d'une combinaison du protocole 'Secure Sockets Layer' (ou SSL) et (dans la plupart des cas) d'un certificat numérique attribué par un fournisseur de certificats (CA). SSL traite les communications cryptées et l'authentification mutuelle entre les navigateurs et votre serveur sécurisé. Le certificat numérique approuvé par le CA fournit l'authentification pour votre serveur sécurisé (la réputation du CA est à la base du certificat d'identité de votre organisation). Lorsque votre navigateur communique à l'aide de cryptage SSL, le préfixe `https://` est employé au début de l'adresse URL ('Uniform Resource Locator') dans la barre de navigation.

Le cryptage dépend de l'utilisation de clés (imaginez ces clés comme étant des codeurs/décodeurs de chaînes de données secrètes). Le cryptage dépend de l'utilisation de clés (imaginez ces clés comme étant des codeurs/décodeurs de chaînes de données secrètes). Dans le cas de la cryptographie conventionnelle ou symétrique, les deux extrémités de la transaction ont la même clé, qu'elles utilisent pour décoder leurs transmissions mutuelles. Dans le cas du cryptage public ou asymétrique, il existe deux clés: une clé publique et une clé privée. Les personnes ou les organisations gardent leur clé privée secrète et publie leur clé publique. Les données codées à l'aide de la clé publique ne peuvent être décodées qu'avec la clé privée; les données codées avec la clé privée ne peuvent être décodées qu'avec la clé publique

Pour configurer votre serveur sécurisé, utilisez le cryptage public pour créer une paire de clés publique et privée. Dans la plupart des cas, vous envoyez une demande de certificat (ainsi que votre clé publique), une preuve de l'identité de votre société et un paiement à un fournisseur de certificats. Ce dernier vérifiera votre demande et votre identité, puis vous enverra un certificat pour votre serveur sécurisé.

Un serveur sécurisé utilise un certificat pour s'identifier auprès des navigateurs Web. Vous pouvez générer votre propre certificat (appelé certificat 'auto-signé') ou en obtenir un d'un fournisseur de certificats (CA). Un certificat provenant d'un CA de bonne réputation garantit qu'un site Web est bel et bien associé à une société ou organisation spécifique.

Vous pouvez également créer votre propre certificat auto-signé. Notez toutefois que les certificats auto-signés ne devraient généralement pas être utilisés pour les environnements de production. En effet, ils ne sont pas automatiquement acceptés par les navigateurs Web des utilisateurs — les navigateurs demandent d'abord aux utilisateurs s'ils acceptent le certificat et la création d'une connexion sécurisée. Reportez-vous à la Section 20.5 pour plus d'informations sur les différences entre les certificats auto-signés et ceux signés par un fournisseur de certificats.

Une fois que vous avez votre certificat, auto-signé ou signé par le fournisseur de certificats de votre choix, vous devez l'installer sur votre serveur sécurisé.

20.4. Utilisation de clés et de certificats existants

Si vous avez déjà une clé et un certificat (par exemple, si vous installez le serveur sécurisé pour remplacer le produit du serveur sécurisé d'une autre société), vous pourrez probablement vous servir de votre clé et de votre certificat actuels avec le serveur sécurisé. Dans les deux cas suivants, vous ne pourrez toutefois pas utiliser votre clé et votre certificat existants:

- *Si vous changez votre adresse IP ou votre nom de domaine* — Les certificats sont attribués pour un couple adresse IP et nom de domaine spécifiques. Ainsi, si vous modifiez l'un des deux éléments, vous devez obtenir un nouveau certificat.
- *Si vous avez un certificat de VeriSign et changez de logiciel serveur* — VeriSign est un fournisseur de certificats (CA) très utilisé. Si vous avez déjà un certificat VeriSign pour une autre utilisation, vous avez probablement songé à l'utiliser pour votre nouveau serveur sécurisé. Malheureusement, vous ne serez pas autorisé à le faire car VeriSign attribue ses certificats en fonction d'un logiciel serveur et d'une combinaison adresse IP/nom de domaine spécifique.

  Si vous changez l'un de ces paramètres (par exemple, si vous avez précédemment utilisé un autre produit du serveur sécurisé), le certificat VeriSign en votre possession, utilisé pour l'ancienne configuration, ne fonctionnera plus avec la nouvelle. Vous devrez donc obtenir un nouveau certificat.

Si vous avez déjà une clé et un certificat pouvant être utilisés, vous n'avez pas à générer une nouvelle clé ou à obtenir un nouveau certificat. Par contre, vous devrez peut-être déplacer et renommer les fichiers qui contiennent votre clé et votre certificat.

Déplacez le fichier clé existant vers:

```
/etc/httpd/conf/ssl.key/server.key
```

Déplacez le fichier certificat existant vers:

```
/etc/httpd/conf/ssl.crt/server.crt
```

Après avoir déplacé la clé et le certificat, passez à la Section 20.9.

Si vous effectuez une mise à jour à partir du serveur sécurisé Red Hat, votre ancienne clé (`httpsd.key`) et votre ancien certificat (`httpsd.crt`) se trouvent dans `/etc/httpd/conf/`. Déplacez et rebaptisez votre clé et votre certificat afin que le serveur sécurisé puisse les utiliser. Utilisez les deux commandes suivantes pour déplacer et rebaptiser les fichiers de vos clé et certificat:

```
mv/etc/httpd/conf/httpsd.key/etc/httpd/conf/ssl.key/server.key
mv/etc/httpd/conf/httpsd.crt/etc/httpd/conf/ssl.crt/server.crt
```

Démarrez ensuite votre serveur sécurisé à l'aide de la commande:

```
/sbin/servicehttpdstart
```

Pour un serveur sécurisé, vous devez saisir une phrase-mot de passe. Une fois saisie, appuyez sur [Entrée] et le serveur démarrera.

20.5. Types de certificats

Si vous avez installé votre serveur sécurisé à partir du paquetage RPM inclus dans Red Hat Linux, une clé aléatoire et un certificat de test ont été générés et placés dans les répertoires appropriés. Avant de commencer à utiliser votre serveur sécurisé, vous devez toutefois générer votre propre clé et obtenir un certificat qui identifie correctement votre serveur.

Vous avez besoin d'une clé et d'un certificat pour faire fonctionner votre serveur sécurisé — ce qui signifie que vous avez le choix entre la création d'un certificat auto-signé ou l'achat d'un certificat signé auprès d'un fournisseur de certificats. Quelle différence existe-t-il entre les deux?

Les certificats signés par un fournisseur offrent deux avantages importants pour votre serveur:

- Les navigateurs reconnaissent (généralement) automatiquement ces certificats et autorisent la connexion sécurisée, sans demander à l'utilisateur.
- Lorsqu'un fournisseur de certificats attribue un certificat signé, il garantit l'identité de l'organisation qui fournit les pages Web au navigateur.

Si votre serveur sécurisé est utilisé par le grand public, votre serveur sécurisé doit avoir un certificat signé par un fournisseur de certificats de façon à ce que les internautes sachent que le site est bien la propriété le l'organisation qui prétend en être propriétaire. Avant de signer un certificat, le fournisseur vérifie l'identité de l'organisation qui en fait la demande.

La plupart des navigateurs prenant en charge SSL ont une liste de fournisseurs de certificats qu'ils acceptent automatiquement. Lorsqu'un navigateur tombe sur un certificat d'un fournisseur ne faisant pas partie de cette liste, il demande à l'utilisateur s'il souhaite accepter ou refuser la connexion.

Vous pouvez générer un certificat auto-signé pour le serveur sécurisé, mais sachez que celui-ci n'offrira pas les mêmes fonctionnalités qu'un certificat signé par un fournisseur. Un certificat auto-signé n'est pas reconnu automatiquement par les navigateurs et n'offre aucune garantie quant à l'identité de l'organisation qui fournit le site Web. Un certificat signé par un fournisseur offre quant à lui ces deux avantages importants pour un serveur sécurisé. Si votre serveur sécurisé est destiné à être utilisé dans un environnement de production, vous devriez alors vous munir d'un certificat signé par un fournisseur de certificats.

La procédure pour obtenir un certificat d'un fournisseur est assez simple. Ci-après figure un bref aperçu de cette dernière:

1. Création d'une paire de clés privée et publique de cryptage.
2. Création d'une demande de certificat basée sur la clé publique. La demande de certificat contient des informations sur votre serveur et la société qui l'héberge.
3. Envoi de la demande de certificat, accompagnée des documents qui prouvent votre identité, à un fournisseur. Nous ne pouvons vous dire quel fournisseur choisir. Votre décision peut dépendre de vos propres expériences, de celles de vos amis, de vos collègues ou tout simplement de facteurs économiques.

   Une fois que vous avez choisi un fournisseur de certificats, vous devrez suivre les instructions fournies par ce dernier afin de vous voir délivrer un certificat.
4. Renvoi d'un certificat numérique par le fournisseur de certificats, après satisfaction et validation de votre identité.
5. Installation de ce certificat sur votre serveur sécurisé et commencez à effectuer des transactions sécurisées.

Que votre certificat provienne d'un fournisseur de certificats ou qu'il soit auto-signé, la première étape est la même: il faut générer une clé. Reportez-vous à la Section 20.6 pour avoir des instructions sur la façon de générer une clé.

20.6. Création d'une clé

Pour générer une clé, vous devez être connecté en tant que super-utilisateur (ou root).

D'abord, utilisez la commande `cd` pour vous rendre au répertoire `/etc/httpd/conf`. Supprimez la fausse clé et le faux certificat qui ont été créés lors de l'installation à l'aide de la commande suivante:

```
rmssl.key/server.key
rmssl.crt/server.crt
```

Ensuite, vous devez créer votre propre clé aléatoire. Passez dans le répertoire `/usr/share/ssl/certs` et tapez la commande suivante:

```
makegenkey
```

Votre système affiche alors un message qui ressemble à l'extrait suivant:

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.......++++++
.....................................................................++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

Vous devez maintenant entrer une phrase-mot de passe. Pour une sécurité maximale, votre mot de passe devrait être composé d'au moins huit caractères, contenir des lettres, des chiffres et/ou des signes de ponctuation et ne devrait pas être un mot du dictionnaire. De plus, n'oubliez pas que votre phrase-mot de passe est sensible à la casse.

Remarque

Vous devez vous rappeler cette phrase-mot de passe et l'entrer à chaque fois que vous lancez votre serveur sécurisé; efforcez-vous donc de ne pas l'oublier.

Entrez de nouveau la phrase-mot de passe, pour vous assurer qu'elle est correctement écrite. La réussite de cette opération entraînera la création du fichier `/etc/httpd/conf/ssl.key/server.key` contenant votre clé.

Notez que si vous ne voulez pas entrer votre phrase-mot de passe chaque fois que vous lancez votre serveur sécurisé, vous devez utiliser les deux commandes suivantes à la place de `make genkey` pour créer la clé.

Utilisez la commande suivante pour créer la clé:

```
/usr/bin/opensslgenrsa1024>/etc/httpd/conf/ssl.key/server.key
```

Puis utilisez la commande ci-dessous pour vous assurer que les autorisations sont correctement définies sur votre clé:

```
chmodgo-rwx/etc/httpd/conf/ssl.key/server.key
```

Après avoir utilisé les commandes ci-dessus pour créer votre clé, vous ne devrez plus utiliser de phrase-mot de passe pour lancer votre serveur sécurisé.

Attention

La désactivation de la fonction de mot de passe sur votre serveur sécurisé est un risque de sécurité potentiel. Nous vous recommandons de ne PAS désactiver cette fonction relative à la saisie de la phrase-mot de passe pour votre serveur sécurisé.

Les problèmes associés au fait de ne pas utiliser de phrase-mot de passe sont directement liés à la sécurité gérée sur l'ordinateur hôte. Par exemple, si un individu peu scrupuleux compromet la sécurité UNIX normale de l'ordinateur hôte, cette personne pourrait alors obtenir votre clé privée (le contenu du fichier `server.key`). Cette clé pourrait ensuite être utilisée pour servir des pages Web comme si elles provenaient de votre serveur sécurisé.

Si la sécurité UNIX est maintenue de façon rigoureuse sur l'ordinateur hôte (tous les correctifs et les mises à jour du système d'exploitation sont installés dès qu'ils sont disponibles, aucun service risqué ou inutile n'est exécuté, etc.), la phrase-mot de passe de votre serveur sécurisé peut alors sembler superflue. Toutefois, comme votre serveur sécurisé ne devrait pas avoir besoin d'être redémarré très souvent, la sécurité supplémentaire offerte par l'entrée d'une phrase-mot de passe est appréciable dans la plupart des cas.

Le fichier `server.key` devrait être la propriété du super-utilisateur (ou root) de votre système et aucun autre utilisateur ne devrait pouvoir y accéder. Faites une copie de sauvegarde de ce fichier et gardez-la en lieu sûr. Vous aurez besoin de cette copie de sauvegarde car si vous perdez votre fichier `server.key` après l'avoir utilisé pour créer votre demande de certificat, votre certificat ne fonctionnera plus et le fournisseur de certificats ne pourra rien faire pour vous aider. La seule solution qui s'offrirait alors à vous serait de demander (et de payer pour) un nouveau certificat.

Si vous prévoyez d'acheter un certificat d'un fournisseur de certificats, passez à la Section 20.7. Si vous désirez générer votre propre certificat auto-signé, passez à la Section 20.8.

20.7. Génération d'une demande de certificat à envoyer à un fournisseur de certificats (CA)

L'étape suivant la création de votre clé, consiste à générer une demande de certificat que vous enverrez ensuite au fournisseur de certificats de votre choix. Après vous être assuré que vous vous trouvez bien dans le répertoire `/usr/share/ssl/certs`, tapez la commande suivante:

```
makecertreq
```

Votre système affichera la sortie suivante et vous demandera votre phrse-mot de passe (à moins bien sûr que vous n'ayez désactivé cette fonction):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

Entrez la phrase-mot de passe choisie lors de la création de votre clé. Votre système affichera des instructions et vous demandera de fournir une série de réponses. Les informations que vous fournirez sont ajoutées à la demande de certificat. Un écran de demande ressemble à l'extrait reproduit ci-dessous:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.example.com
Email Address []:admin@example.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Les réponses par défaut sont mises entre parenthèses (`[]`) immédiatement après chaque demande d'entrée. Par exemple, la première information demandée est le nom du pays où le certificat sera utilisé, comme ci-dessous:

```
Country Name (2 letter code) [GB]:
```

L'entrée par défaut, entre parenthèses, est `GB`. Pour accepter cette valeur par défaut, appuyez simplement sur la touche [Entrée] ou entrez le code de deux lettres de votre pays.

Vous devrez tapez le reste des valeurs. Ces dernières devraient être évidentes, mais suivez tout de même les lignes directrices suivantes:

- N'abrégez pas les localités ou les états. Écrivez-les en entier (ex.: Saint-Malo et non St-Malo).
- Si vous envoyez cette demande de certificat à un fournisseur de certificats, veillez à bien indiquer toutes les informations demandées, particulièrement les champs `Nom de l'organisation` et `Nom commun`. Les fournisseurs de certificats vérifient les informations contenues dans les demandes pour déterminer si les organisations sont bel et bien associées au nom fourni dans le champ `Nom commun`. S'ils ont des doutes quant aux informations fournies, ils rejettent les demandes.
- Pour le champ `Nom commun`, assurez-vous d'entrer le *véritable* nom de votre serveur sécurisé (un nom DNS valide) et non pas l'alias que le serveur peut avoir.
- L'`adresse électronique` doit être celle du webmestre (Webmaster) ou de l'administrateur système.
- Évitez tout caractère spécial du type @, #, &, !, etc. Certains fournisseurs de certificats refusent les demandes contenant de tels caractères. Par conséquent, si le nom de votre société contient une esperluette (&), écrivez plutôt 'et'.
- N'utilisez aucun des attributs supplémentaires (`A challenge password` et `An optional company name`). Pour continuer sans remplir ces champs, appuyez simplement sur la touche [Entrée] pour accepter la valeur par défaut (vide) des deux éléments.

Lorsque vous avez terminé d'entrer les informations, le fichier `/etc/httpd/conf/ssl.csr/server.csr` est créé. Ce fichier est votre demande de certificat, prête à être envoyée au fournisseur de certificats.

Après avoir choisi un fournisseur de certificats, suivez les instructions fournies par celui-ci sur son site Web. Ces instructions vous expliquent comment envoyer votre demande de certificat, vous indique si vous devez fournir d'autres informations et vous précise les modes de paiement.

Si vous répondez à toutes ses exigences, le fournisseur vous enverra un certificat (généralement par courrier électronique). Enregistrez-le (ou copiez-le et collez-le) sous `/etc/httpd/conf/ssl.crt/server.crt`. Assurez-vous de bien conserver une copie de sauvegarde de ce fichier.

20.8. Création d'un certificat auto-signé

Vous pouvez créer votre propre certificat auto-signé. Sachez cependant qu'il n'offre pas les mêmes garanties de sécurité qu'un certificat signé par un fournisseur de certificats. Reportez-vous à la Section 20.5 pour de plus amples informations sur les certificats.

Si vous souhaitez créer votre propre certificat auto-signé, vous devez d'abord créer une clé aléatoire en suivant les instructions fournies dans la Section 20.6. Une fois que vous avez une clé, assurez-vous que vous vous trouvez dans le répertoire `/usr/share/ssl/certs` et tapez la commande suivante:

```
maketestcert
```

La sortie ci-dessous s'affichera et vous serez alors invité à entrer votre phrase-mot de passe (à moins que vous n'ayez créé une clé sans phrase-mot de passe):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
```

Après avoir entré votre phrase-mot de passe (ou sans invite si vous avez créé une clé sans phrase-mot de passe), le système vous demandera d'autres informations. La sortie de l'ordinateur ainsi qu'un ensemble de demandes d'informations qui s'affichant à l'écran, ressemblent à l'extrait ci-dessous (vous devez fournir les informations appropriées sur votre organisation et sur votre hôte):

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:My Company, Inc.
Organizational Unit Name (eg, section) []:Documentation
Common Name (your name or server's hostname) []:myhost.example.com
Email Address []:myemail@example.com
```

Une fois les informations données, un certificat auto-signé est créé dans `/etc/httpd/conf/ssl.crt/server.crt`. Vous devez redémarrer votre serveur sécurisé après avoir créé le certificat, à l'aide de la commande suivante:

```
/sbin/servicehttpdrestart
```

20.9. Test du certificat

Afin de tester le certificat de test installé par défaut, un certificat signé par un fournisseur de certificats et un certificat auto-signé, pointez votre navigateur Web vers la page d'accueil suivante (en remplaçant *server.example.com* par votre nom de domaine):

```
https://server.example.com
```

Remarque

Notez bien la lettre `s` après `http`. Le préfixe `https:` est utilisé pour les transactions HTTP sécurisées.

Si vous utilisez un certificat signé par un fournisseur de certificats très connu, votre navigateur l'acceptera probablement de façon automatique (sans vous demander votre approbation) et créera la connexion sécurisée. En revanche, si vous utilisez un certificat de test ou auto-signé, votre navigateur ne le reconnaîtra pas automatiquement car il n'est pas signé par un fournisseur de certificats. Si vous n'utilisez pas un certificat signé par un fournisseur, suivez les instructions fournies par votre navigateur pour accepter le certificat.

Une fois que votre navigateur accepte le certificat, votre serveur sécurisé affichera une page d'accueil par défaut.

20.10. Accès au serveur

Pour accéder à votre serveur sécurisé, utilisez une adresse URL comme celle figurant ci-dessous:

```
https://server.example.com
```

Il est possible d'accéder à un serveur autre qu'un serveur sécurisé (en d'autres termes, un serveur non-sécurisé) en utilisant une adresse URL comme celle figurant ci-dessous:

```
http://server.example.com
```

Le port standard pour les communications Web sécurisées est le 443. Le port standard pour les communications Web non-sécurisées est le 80. La configuration par défaut de votre serveur sécurisé est en mode de réception aussi bien sur l'un que sur l'autre. Il n'est par conséquent pas nécessaire de spécifier le numéro de port dans une URL (le numéro de port est supposé).

Toutefois, si vous configurez votre serveur de façon à ce qu'il soit en mode réception sur un port non-standard (autre que les ports 80 et 443), vous devez spécifier le numéro de port dans toutes les adresses URL permettant une connexion au serveur sur le port non-standard.

Par exemple, vous avez peut-être configuré votre serveur de façon à avoir un hôte virtuel en exécution non-sécurisée sur le port 12331. Toute URL prévue pour la connexion à cet hôte virtuel doit contenir le numéro de port. L'exemple suivant d'URL essaie d'établir une connexion avec un serveur autre qu'un serveur sécurisé (c'est-à-dire une serveur non-sécurisé) en mode de réception sur le port 12331:

```
http://server.example.com:12331
```

20.11. Ressources supplémentaires

Reportez-vous à la Section 19.7 pour obtenir de plus amples renseignements sur Serveur HTTP Apache.

20.11.1. Documentation installée

- `mod_ssl documentation` — Ouvrez un navigateur Web et allez à l'URL http://localhost/manual/mod/mod_ssl.html du serveur qui exécute Serveur HTTP Apache et qui est équipé du paquetage `httpd-manual`.

20.11.2. Sites Web utiles

- http://www.redhat.com/mailing-lists/ — Vous pouvez vous inscrire à la liste de diffusion redhat-secure-server à cette adresse URL.

  Vous pouvez également le faire en envoyant un courrier électronique à l'adresse `<redhat-secure-server-request@redhat.com>` et en indiquant le mot *subscribe* dans l'objet.

- http://www.modssl.org — Le site Web `mod_ssl` est la meilleure source d'informations sur `mod_ssl`. Ce site est une mine de renseignements et comprend notamment un *User Manual* (Guide utilisateur) à l'adresse http://www.modssl.org/docs.

20.11.3. Livres sur le sujet

- *Apache: The Definitive Guide*, 2ème édition, de Ben Laurie et Peter Laurie, O'Reilly & Associates, Inc.

Chapitre 21.

Configuration de BIND

Pour bien conprendre ce chapitre, vous devez connaître les principes de base de BIND et de DNS car son but n'est pas d'en expliquer les concepts. Ce chapitre explique en effet la façon d'utiliser l'**Outil de configuration Bind** (`redhat-config-bind`) pour configurer des zones de serveur BIND de base. Cet outil crée le fichier de configuration `/etc/named.conf` ainsi que les fichiers de configuration de zones dans le répertoire `/var/named` à chaque fois que vous appliquez vos changements.

Important

Ne modifiez pas le fichier de configuration `/etc/named.conf`. L'utilitaire **Outil de configuration Bind** le génère une fois que vous avez appliqué vos changements. Si vous souhaitez configurer des paramètres que l'**Outil de configuration Bind** ne permet pas de configurer, ajoutez-les à `/etc/named.custom`.

L'utilitaire **Outil de configuration Bind** requiert le système X Window et l'accès super-utilisateur (ou root). Pour lancer l'**Outil de configuration Bind**, cliquez sur le bouton **Menu principal** (sur le panneau) => **Paramètres de système => Paramètres serveur => Service de résolution d'adresse IP** (Domain Name Service) ou tapez la commande `redhat-config-bind` à l'invite du shell (dans un terminal XTerm ou GNOME, par exemple).

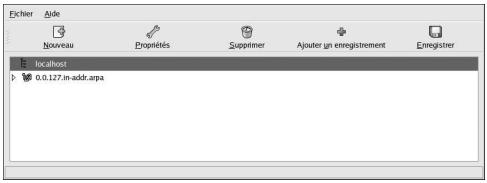

Figure 21-1. Outil de configuration Bind

L'utilitaire **Outil de configuration Bind** configure le répertoire de zone par défaut sur `/var/named`. Tous les fichiers de zone spécifiés sont placés sous ce répertoire. L'**Outil de configuration Bind** inclut également un contrôle de base de la syntaxe lors de la saisie de valeurs. Par exemple, dans le cadre de la saisie d'une adresse IP valide, vous ne pouvez entrer que des numéros et des points (.) dans la zone texte.

L'**Outil de configuration Bind** vous permet d'ajouter une zone maître de retransmission, une zone maître inverse et une zone esclave. Une fois les zones ajoutées, vous pouvez les modifier ou les supprimer de la fenêtre principale comme cela est expliqué dans la Figure 21-1.

Après avoir ajouté, modifié ou supprimé une zone, cliquez sur le bouton **Enregistrer** ou sélectionnez **Fichier => Enregistrer** pour écrire le fichier de configuration `/etc/named.conf` et tous les fichiers de zone individuels dans le répertoire `/var/named`. En enregistrant vos changements, le service `named` procède au rechargement des fichiers de configuration. Vous pouvez également sélectionner **Fichier => Quitter** pour enregistrer vos modifications avant de quitter l'application.

21.1. Ajout d'une zone maître de retransmission

Pour ajouter une zone maître de retransmission (également appelée maître primaire), cliquez sur le bouton **Nouvelle**, sélectionnez **Zone maître de retransmission** et entrez le nom de domaine de la zone maître dans la zone texte, **Nom de domaine**.

Une nouvelle fenêtre similaire à celle présentée dans la Figure 21-2 apparaît avec les options suivantes:

- **Nom** — Nom de domaine qui a été saisi dans la fenêtre précédente.
- **Nom de fichier** — Nom du fichier de la base de données DNS, relatif à `/var/named`. Il est préétabli au nom de domaine suivi de `.zone`.
- **Contact** — Adresse électronique du contact principal de la zone maître.
- **Serveur de noms primaire (SOA)** — Enregistrement SOA ('state of authority'). Cette entrée spécifie le serveur de noms qui représente la meilleure source d'informations pour ce domaine.
- **Numéro de série** — Numéro de série du fichier de la base de données DNS. Ce numéro doit être incrémenté chaque fois que vous modifiez le fichier, afin que les serveurs de noms esclaves de la zone récupèrent les dernières données. L'**Outil de configuration Bind** incrément ce numéro d'une unité lorsque la configuration change. Ce numéro peut également être modifié manuellement en cliquant sur le bouton **Établir** situé près de la valeur **Numéro de série**.
- **Paramètres de temps** — les valeurs **Rafraîchir**, **Ré-essayer**, **Expirer** et **Minimum** TTL ('Time to Live', litteralement Temps de vie) qui sont conservées dans le fichier de base de données DNS. Toutes les valeurs sont exprimées en secondes.
- **Enregistrements** — Ajout, modification et suppression de ressources enregistrées de type **Hôte**, **Alias** et **Serveur de noms**.

Figure 21-2. Ajout d'une zone maître de retransmission

Un **Serveur de noms primaire (SOA)** doit être spécifié ainsi qu'au moins un enregistrement de serveur de noms en cliquant sur le bouton **Ajouter** dans la section **Enregistrements** section.

Après avoir configuré une zone maître de retransmission, cliquez sur **OK** pour revenir à la fenêtre principale, comme le montre la Figure 21-1. À partir du menu déroulant, cliquez sur **Enregistrer** pour d'une part, écrire le fichier de configuration `/etc/named.conf` et tous les fichiers de zone in-

dividuels dans le répertoire `/var/named` et d'autre part, demander au démon de recharger les fichiers de configuration.

Suite à la configuration, une entrée semblable à l'extrait ci-dessous est enregistrée dans `/etc/named.conf`:

```
zone"forward.example.com"{
typemaster;
file"forward.example.com.zone";
};
```

Elle crée également le fichier `/var/named/forward.example.com.zone` en y indiquant les informations ci-dessous:

```
$TTL86400
@INSOAns.example.com.root.localhost(
2;serial
28800;refresh
7200;retry
604800;expire
86400;ttl
)


INNS192.168.1.1.
```

21.2. Ajout d'une zone maître inverse

Pour ajouter une zone maître inverse, cliquez sur le bouton **Ajouter** et sélectionnez **Zone maître inverse**. Entrez les trois premiers octets de la plage d'adresses IP que vous souhaitez configurer. Par exemple, si vous configurez la plage d'adresses IP 192.168.10.0/255.255.255.0, entrez 192.168.10 dans la zone texte d'**Adresse IP (3 premiers Octets)**.

Une nouvelle fenêtre s'affiche à l'écran, comme le montre la Figure 21-3, avec les options ci-dessous:

1. **Adresse IP** — Les trois premiers octets que vous avez entrés dans la fenêtre précédente.
2. **Adresse IP inverse** — Non-modifiable. Pré-configurée en fonction de l'adresse IP entrée.
3. **Contact** — Adresse électronique du contact principal de la zone maître.
4. **Nom de fichier** — Nom du fichier de la base de données DNS dans le répertoire `/var/named`.
5. **Serveur de noms primaire (SOA)** — Enregistrement SOA ('state of authority)'. Ceci spécifie le serveur de noms qui représente la meilleure source d'informations pour ce domaine.
6. **Numéro de série** — Numéro de série du fichier de la base de données DNS. Ce numéro doit être incrémenté chaque fois que vous modifiez le fichier, afin que les serveurs de noms esclaves de la zone récupèrent les dernières données. L'**Outil de configuration Bind** incrémente ce numéro d'une unité lorsque la configuration change. Il peut également être incrémenté manuellement en cliquant sur le bouton **Établir** situé près de la valeur **Numéro de série**.
7. **Paramètres de temps** — Valeurs **Rafraîchir**, **Ré-essayer**, **Expirer** et **Minimum** TTL (Time to Live, littéralement Temps de vie) qui sont conservées dans le fichier de la base de données DNS.
8. **Serveurs de noms** — Ajout, modification et suppression de serveurs de noms pour la zone maître inverse. Un nom de serveur est au minimum requis.

9. **Table d'adresses inverses** — Liste des adresses IP de la zone maître inverse ainsi que des noms d'hôtes correspondants. Par exemple, pour la zone maître inverse 192.168.10, vous pouvez ajouter 192.168.10.1 dans **Table d'adresses inverses** avec le nom d'hôte one.example.com. Le nom d'hôte doit se terminer par un point (.) pour indiquer qu'il s'agit d'un nom d'hôte complet.

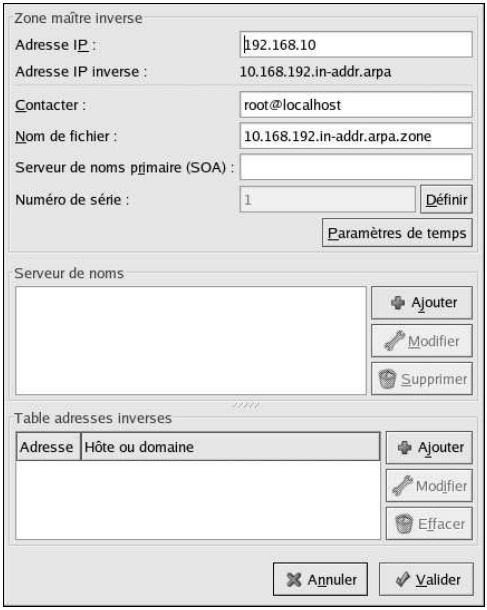

Figure 21-3. Ajout d'une zone maître inverse

Un **Serveur de noms primaire (SOA)** doit être spécifié ainsi qu'au moins un enregistrement de serveur de noms en cliquant sur le bouton **Ajouter** dans la section **Serveurs de noms**.

Après avoir configuré une zone maître inverse, cliquez sur **OK** pour revenir à la fenêtre principale, comme le montre la Figure 21-1. À partir du menu déroulant, cliquez sur **Enregistrer** pour d'une part, écrire le fichier de configuration `/etc/named.conf` et tous les fichiers de zone individuels dans le répertoire `/var/named` et d'autre part, demander au démon de recharger les fichiers de configuration.

Suite à la configuration, une entrée semblable à l'extrait ci-dessous est enregistrée dans `/etc/named.conf`:

```
zone"10.168.192.in-addr.arpa"{
typemaster;
file"10.168.192.in-addr.arpa.zone";
};
```

Elle crée également le fichier `/var/named/10.168.192.in-addr.arpa.zone`, qui contient les informations suivantes:

```
$TTL86400
@INSOAns.example.com.root.localhost(
2;serial
28800;refresh
```

```
7200;retry
604800;expire
86400;ttk
)


@INNSns2.example.com.

1INPTRone.example.com.
2INPTRtwo.example.com.
```

21.3. Ajout d'une zone esclave

Pour ajouter une zone esclave (également appelée maître secondaire), cliquez sur le bouton **Ajouter** et sélectionnez **Zone esclave**. Entrez le nom de domaine de la zone esclave dans la zone texte **Nom de domaine**.

Une nouvelle fenêtre s'affiche à l'écran, comme le montre la Figure 21-4, avec les options ci-dessous:

- **Nom** — Le nom de domaine qui a été entré dans la fenêtre précédente.
- **Liste des maîtres** — Les serveurs de noms à partir desquels la zone esclave récupère ses données. Chaque valeur doit être une adresse IP valide. La zone de texte ne peut contenir que des numéros et des points (.)
- **Nom de fichier** — Nom du fichier de la base de données DNS contenu dans `/var/named`.

Figure 21-4. Ajout d'une zone esclave

Après avoir configuré la zone esclave, cliquez sur **OK** pour revenir à la fenêtre principale, comme le montre la Figure 21-1. Cliquez sur **Enregistrer** pour écrire le fichier de configuration `/etc/named.conf` et demander au démon de recharger les fichiers de configuration.

Suite à la configuration, une entrée semblable à l'extrait ci-dessous est enregistrée dans `/etc/named.conf`:

```
zone"slave.example.com"{
typeslave;
file"slave.example.com.zone";
masters{
```

```
1.2.3.4;
};
};
```

Le fichier de configuration `/var/named/slave.example.com.zone` est créé par le service `named` lorsqu'il télécharge les données de zone du ou des serveurs maîtres.

Chapitre 22. Configuration de l'authentification

Lorsqu'un utilisateur se connecte à un système Red Hat Linux, la combinaison nom d'utilisateur/mot de passe doit être vérifiée, ou *authentifiée*, comme un utilisateur valide et actif. Dans certaines situations, les informations nécessaires à la vérification de l'utilisateur se trouvent sur le système local et dans d'autres situations, le système demande à une base de données utilisateur se trouvant sur un système distant d'effectuer l'authentification.

L'**Outil de configuration d'authentification** fournit une interface graphique permettant non seulement de configurer NIS, LDAP et Hesiod de manière à ce qu'ils extraient les informations d'utilisateur mais permettant également la configuration de LDAP, Kerberos et SMB en tant que protocoles d'authentification.

Remarque

Si vous avez choisi un niveau de sécurité moyen ou élevé lors de l'installation ou avec l'**Outil de configuration du niveau de sécurité** (ou si vous avez choisi un niveau de sécurité moyen ou élevé avec le programme **GNOME Lokkit**), les méthodes d'authentification réseau, y compris NIS et LDAP, ne seront pas autorisées à passer à travers le pare-feu.

Ce chapitre ne se concentre pas en détail sur chacun des différents types d'authentification. Il explique plutôt la manière d'utiliser l'**Outil de configuration d'authentification** afin de les configurer.

Pour démarrer la version graphique de l'**Outil de configuration d'authentification** à partir du bureau, sélectionnez le bouton **Menu principal** (sur le panneau) => **Paramètres du système** => **Authentification** ou tapez la commande `authconfig-gtk` à une invite du shell (par exemple, dans **XTerm** **GNOME terminal**). Afin de démarrer la version texte, tapez la commande `authconfig` à une invite du shell.

Important

Les changements apportés prendront effet aussitôt que vous sortirez du programme d'authentification.

22.1. Informations utilisateur

L'onglet **Informations utilisateur** offre plusieurs options. Pour activer une option, cochez la case de pointage située à côté d'elle. Pour désactiver une option, cliquez sur la case de pointage située à côté d'elle et tout choix précédent sera annulé. Cliquez sur **OK** afin de sortir du programme et mettre en oeuvre les modifications apportées.

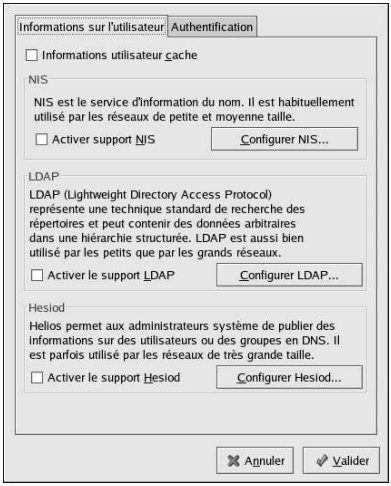

Figure 22-1. Informations utilisateur

La liste ci-dessous explique l'élément que chaque option configure:

- **Cache d'informations utilisateur** — Sélectionnez cette option pour activer le démon de cache de service de noms (`nscd`) et le configurer de manière à ce qu'il se lance au démarrage.

  Le paquetage `nscd` doit être installé pour que cette option puisse fonctionner.

- **Activer support NIS** — Sélectionnez cette option pour configurer le système en tant que client NIS qui se connecte à un serveur NIS pour l'authentification de l'utilisateur et du mot de passe. Cliquez sur le bouton **Configurer NIS** pour spécifier le domaine NIS et le serveur NIS. Si le serveur NIS n'est pas spécifié, le démon essaiera de le trouver par le biais de la diffusion.

  Le paquetage `ypbind` doit être installé pour que cette option puisse fonctionner. Si la prise en charge NIS est activée, les services `portmap` et `ypbind` sont non seulement lancés mais sont également activés de manière à s'amorcer au démarrage.

- **Activer support LDAP** — Sélectionnez cette option pour configurer le système de manière à ce qu'il extraie les informations utilisateur par le biais de LDAP. Cliquez sur le bouton **Configurer LDAP** pour spécifier le **DN de la base de recherche de LDAP** et le **Serveur LDAP**. En sélectionnant **Utiliser TLS pour crypter les mots de passe**, Transport Layer Security deviendra la méthode de cryptage des mots de passe envoyés au serveur LDAP.

  Le paquetage `openldap-clients` doit être installé pour que cette option puisse fonctionner.

  Pour de plus amples informations sur LDAP, reportez-vous au *Guide de référence de Red Hat Linux*.

- **Activer support Hesiod** — Sélectionnez cette option pour configurer le système de manière à ce qu'il extraie ses informations d'une base de données Hesiod distante, y compris les informations utilisateurs.

  Le paquetage `hesiod` doit être installé pour que cette option puisse fonctionner.

22.2. Authentification

L'onglet **Authentification** permet la configuration des méthodes d'authentification réseau. Pour activer une option, cliquez sur la case de pointage vierge placée à côté d'elle. Pour désactiver une option, cliquez sur la case de pointage située à côté d'elle et tout choix précédent sera annulé.

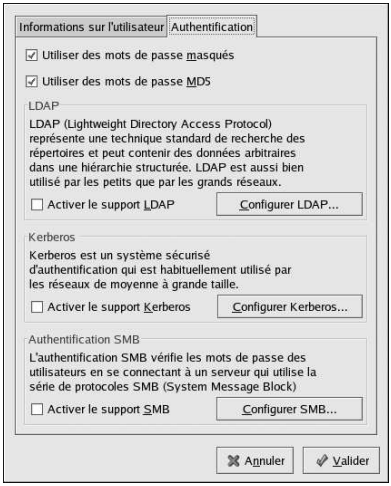

Figure 22-2. Authentification

Les informations suivantes expliquent l'élément que chaque option configure:

- **Utiliser des mots de passe masqués** — Sélectionnez cette option pour conserver les mots de passe dans un format de mots de passe masqués dans le fichier `/etc/shadow` plutôt que dans le fichier `/etc/passwd`. Les mots de passe masqués sont sont activés par défaut lors de l'installaiton et leur utilisation est fortement recommandée afin d'augmenter la sécurité du système.

  Le paquetage `shadow-utils` doit être installé pour que cette option puisse fonctionner. Pour de plus amples informations sur les mots de passe masqués, reportez-vous au chapitre *Utilisateurs et groupes* du *Guide de référence de Red Hat Linux*.
- **Utiliser des mots de passe MD5** — Sélectionnez cette option pour activer les mots de passe MD5, qui peuvent avoir une longueurallant jusqu'à 256 caractères au lieu de huit ou moins. Cette option est sélectionnée par défaut lors de l'installation et leur utilisation est fortement recommandée afin d'augmenter la sécurité du système.
- **Activer support LDAP** — Sélectionnez cette option afin de permettre à des applications supportant PAM d'utiliser LDAP pour l'authentification. Cliquez sur le bouton **Configurer LDAP** pour spécifier les éléments suivants:
  - **Utiliser TLS pour crypter les mots de passe** — Cette option permet d'utiliser Transport Layer Security pour crypter des mots de passe envoyés su serveur LDAP.
  - **DN de la base de recherche LDAP** — Cette option permet d'extraire les informations utilisateur d'après son Nom Distinct (ou DN de l'anglais 'Distinguished Name').
  - **Serveur LDAP** — Cette option permet de spécifier l'adresse IP du serveur LDAP.

  Le paquetage `openldap-clients` doit être installé pour que cette option puisse fonctionner. Reportez-vous au *Guide de référence de Red Hat Linux* pour de plus amples informations sur LDAP.
- **Activer le support Kerberos** — Sélectionnez cette option pour activer l'authentification Kerberos. Cliquez sur le bouton **Configurer Kerberos** pour effectuer la configuration:
  - **Zone** — Cette option permet de configurer la zone (ou 'Realm') du serveur Kerberos. La zone correspond au réseau utilisant Kerberos, composée d'un ou plusieurs KDC et potentiellement, d'un nombre important de clients.

- **KDC** — Cette option permet de définir le centre de distributeur de tickets (ou KDC, de l'anglais 'Key Distribution Center'), le serveur émettant les tickets de Kerberos.
- **Serveurs Admin** — Cette option permet de spécifier les serveurs d'administration exécutant `kadmind`.

Les paquetages `krb5-libs` et `krb5-workstation` doivent être installés pour que cette option puisse fonctionner. Reportez-vous au *Guide de référence de Red Hat Linux* pour de plus amples informations sur Kerberos.

- **Activer support SMB** — Cette option permet de configurer les PAM (les modules d'authentification enfichables) de manière à ce qu'ils utilisent un serveur SMB pour authentifier les utilisateurs. Cliquez sur le bouton **Configurer SMB** pour spécifier les élément suivants:
  - **Groupe de travail** — Cette option permet de spécifier le groupe de travail SMB à utiliser.
  - **Contrôleurs de domaine** — Cette option permet de spécifier les contrôleurs de domaine SMB à utiliser.

22.3. Version en ligne de commande

L'**Outil de configuration d'authentification** peut également être exécuté comme un outil en ligne de commande et donc, sans interface. La version en ligne de commande peut être utilisée dans un script de configuration ou dans un script kickstart. Les options d'authentification sont résumées dans le Tableau 22-1.

Option	Description
`--enableshadow`	Activer les mots de passe masqués
`--disableshadow`	Désactiver les mots de passe masqués
`--enablemd5`	Activer les mots de passe MD5
`--disablemd5`	Désactiver es mots de passe MD5
`--enablenis`	Activer NIS
`--disablenis`	Désactiver NIS
`--nisdomain=<`*`domaine`*`>`	Spécifier un domaine NIS
`--nisserver=<`*`serveur`*`>`	Spécifier un serveur NIS
`--enableldap`	Activer LDAP pour les informations utilisateur
`--disableldap`	Désactiver LDAP pour les informations utilisateur
`--enableldaptls`	Activer l'utilisation de TLS avec LDAP
`--disableldaptls`	Désactiver l'utilisation de TLS avec LDAP
`--enableldapauth`	Activer LDAP pour l'authentification
`--disableldapauth`	Désactiver LDAP pour l'authentification
`--ldapserver=<`*`serveur`*`>`	Spécifier un serveur LDAP
`--ldapbasedn=<`*`dn`*`>`	Spécifier le DN de la base LDAP
`--enablekrb5`	Activer Kerberos
`--disablekrb5`	Désactiver Kerberos

Option	Description
`--krb5kdc=<kdc>`	Spécifier le centre distributeur de tickets (ou KDC) de Kerberos
`--krb5adminserver=<serveur>`	Spécifier le serveur d'administration de Kerberos
`--krb5realm=<zone>`	Spécifier la zone (ou 'realm') de Kerberos
`--enablesmbauth`	Activer SMB
`--disablesmbauth`	Désactiver SMB
`--smbworkgroup=<groupe-de-travail>`	Spécifier le groupe de travail SMB
`--smbservers=<serveur>`	Spécifier les serveurs SMB
`--enablehesiod`	Activer Hesiod
`--disablehesiod`	Désactiver Hesiod
`--hesiodlhs=<lhs>`	Spécifier Hesiod LHS ('left-hand side', côté gauche)
`--hesiodrhs=<rhs>`	Spécifier Hesiod RHS ('right-hand side', côté droit)
`--enablecache`	Activer `nscd`
`--disablecache`	Disable `nscd`
`--nostart`	Ne pas démarrer ou arrêter les services `portmap`, `ypbind` ou `nscd`, même s'ils sont configurés
`--kickstart`	Ne pas afficher l'interface utilisateur
`--probe`	Détecter et afficher les valeurs par défaut du réseau

Tableau 22-1. Options de la ligne de commande

Astuce

Il est possible de trouver ces options dans la page de manuel relative à `authconfig` ou en tapant `authconfig --help` à une invite du shell.

Chapitre 23.

Configuration de l'Agent de Transport de Courrier (ATC)

Il est essentiel d'avoir un *Agent de Transport de Courrier* (ATC ou MTA de l'anglais 'Mail Transport Agent') pour pouvoir envoyer des courriers électroniques depuis un système Red Hat Linux. Un *Agent de Gestion de Courrier* (AGC ou MUA de l'anglais 'Mail User Agent') comme **Evolution**, **Mozilla Mail** et **Mutt**, est utilisé pour lire et composer des courriers électroniques. Lorsqu'un utilisateur envoie un courrier depuis un agent de gestion du courrier, le message est transmis à l'ATC qui le fait suivre à une série d'ATC, jusqu'à ce qu'il arrive à destination.

Même si un utilisateur n'a pas l'intention d'envoyer de courrier depuis le système, des tâches automatiques ou des programmes système peuvent utiliser la commande `/bin/mail` pour envoyer un courrier électronique contenant les messages de journal à l'utilisateur root du système local.

Red Hat Linux 9 fournit deux ATC: Sendmail et Postfix. S'ils sont tous les deux installés, `sendmail` est l'ATC par défaut. Le programme **Commutateur d'agent de transport de courrier** permet à un utilisateur de choisir `sendmail` ou `postfix` comme MTA par défaut pour le système.

Le paquetage RPM `redhat-switch-mail` doit être installé de manière à utiliser la version texte du programme **Commutateur d'agent de transport de courrier**. Si vous souhaitez utiliser la version graphique, le paquetage `redhat-switch-mail-gnome` doit également être installé. Pour obtenir de plus amples informations sur l'installation de paquetages RPM, reportez-vous à la Partie V.

Pour lancer le programme **Commutateur d'agent de transport de courrier**, sélectionnez le bouton **Menu principal** (sur le panneau) => **Extras** => **Outils de système** => **Commutateur d'agent de transport de courrier**, ou tapez la commande `redhat-switch-mail` à l'invite du shell (dans un terminal XTerm ou GNOME, par exemple).

Le programme détecte automatiquement si X Window est en cours d'exécution. Si c'est le cas, le programme démarre en mode graphique comme le montre la Figure 23-1. Si X Window n'est pas détecté, il démarre en mode texte. Vous pouvez forcer le **Commutateur d'agent de transport de courrier** à fonctionner en mode texte en utilisant la commande `redhat-switch-mail-nox`.

Figure 23-1. Commutateur d'agent de transport de courrier

Si vous sélectionner **OK** pour changer le MTA, le démon mail sera activé de manière à être lancé lors du démarrage alors que le démon mail dé-sélectionné sera lui désactivé afin de ne par être lancé lors du démarrage. Comme le démon mail sélectionné est lancé alors que l'autre démon est arrêté, les changements prennent effet immédiatement.

Pour de plus amples informations sur les protocoles email et sur les MTA, reportez-vous au *Guide de référence de Red Hat Linux*. Pour des informations supplémentaires sur les agents de gestion de courrier (AGC), reportez-vous au *Guide de démarrage de Red Hat Linux*.

IV. Configuration du système

Cette section examine non seulement l'accès à la console et la manière permettant de rassembler des informations matérielles et logicielles à partir d'un système Red Hat Linux mais fournit également des explications sur des tâches de configuration courantes du système.

Table des matières

redhat.

Chapitre 24.

Accès console

Lorsque les utilisateurs normaux (c'est-à-dire les utilisateurs qui ne sont pas des super-utilisateurs) se connectent localement à un ordinateur, ils ont deux types de permissions spéciales:

1. Ils peuvent exécuter certains programmes qu'ils n'auraient pas le droit d'exécuter autrement.
2. Ils peuvent accéder à certains fichiers (des fichiers de périphériques spéciaux permettant d'accéder aux disquettes, CD-ROM, etc.) auxquels ils ne pourraient pas accéder autrement.

Étant donné qu'il y a plusieurs consoles sur un ordinateur et que plusieurs utilisateurs peuvent être simultanément connectés à l'ordinateur localement, l'un des utilisateurs doit 'gagner' la course pour l'accès aux fichiers. Le premier utilisateur à se connecter à la console est propriétaire de ces fichiers. Une fois que le premier utilisateur se déconnecte, l'utilisateur qui se connecte ensuite devient propriétaire des fichiers.

Par contraste, *tous* les utilisateurs se connectant à la console seront autorisés à exécuter des programmes accomplissant des tâches normalement réservées au super-utilisateur. Si X est en cours d'exécution, ces actions peuvent être incluses en tant qu'éléments de menu dans une interface utilisateur graphique. Les programmes accessibles de la console comprennent `halt`, `poweroff` et `reboot`.

24.1. Désactivation de l'arrêt via Ctrl-Alt-Suppr

Par défaut, `/etc/inittab` spécifie que votre système est configuré pour arrêter et redémarrer le système en réponse à la combinaison de touches [Ctrl]-[Alt]-[Suppr] à la console. Si vous voulez désactiver cette fonction, désactivez la ligne suivante de `/etc/inittab` en la faisant précéder d'un signe dièse (`#`):

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Ceci étant, vous préférez peut-être autoriser certains utilisateurs normaux à arrêter le système de la console à l'aide de la combinaison [Ctrl]-[Alt]-[Suppr]. Pour réserver ce privilège à certains utilisateurs, suivez les étapes ci-dessous:

1. Ajoutez une option `-a` à la ligne `/etc/inittab` indiquée ci-dessus, afin qu'elle devienne:
   ```
   ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
   ```
   L'option `-a` signale à la commande `shutdown` qu'elle doit rechercher le fichier `/etc/shutdown.allow`, que vous créerez à l'étape suivante.
2. Créez un fichier appelé `shutdown.allow` dans `/etc`. Le fichier `shutdown.allow` doit répertorier les noms d'utilisateurs des personnes qui auront le droit d'arrêter le système à l'aide de la combinaison [Ctrl]-[Alt]-[Suppr]. Le fichier `/etc/shutdown.allow` est une liste d'utilisateurs énumérés un par un, ligne par ligne, ressemblant à l'extrait suivant:
   ```
   stephen
   jack
   sophie
   ```

Selon cet exemple de fichier `shutdown.allow`, Stephen, Jack et Sophie ont le droit d'arrêter le système à partir de la console en utilisant la combinaison de touches [Ctrl]-[Alt]-[Suppr]. Lorsque cette combinaison de touches est utilisée, le fichier `shutdown -a` de `/etc/inittab` vérifie si des utilisateurs mentionnés dans `/etc/shutdown.allow` (ou le super-utilisateur) sont connectés sur une console virtuelle. Si c'est le cas, la procédure d'arrêt du système continuera; sinon, un message d'erreur apparaîtra sur la console du système.

Pour obtenir de plus amples informations sur `shutdown.allow`, reportez-vous à la page de manuel relative à `shutdown`.

24.2. Désactivation de l'accès aux programmes de la console

Pour désactiver l'accès des utilisateurs aux programmes de la console, exécutez la commande ci-dessous en étant connecté en tant que super-utilisateur:

```
rm -f /etc/security/console.apps/*
```

Dans les environnements où la console est sécurisée (mots de passe BIOS et chargeur de démarrage configurés, combinaison [Ctrl]-[Alt]-[Suppr] désactivée, commutateurs d'alimentation et de réinitialisation désactivés, etc.), vous préférez peut-être qu'aucun utilisateur ne puisse exécuter les commandes `poweroff`, `halt` et `reboot`, accessibles à partir de la console par défaut.

Pour empêcher l'exécution de ces dernières, exécutez les commandes suivantes en tant que super-utilisateur:

```
rm -f /etc/security/console.apps/poweroff
rm -f /etc/security/console.apps/halt
rm -f /etc/security/console.apps/reboot
```

24.3. Désactivation de tout accès console

Le module PAM `pam_console.so` gère les permissions et l'authentification pour les fichiers de console. (Consulter le *Guide de référence de Red Hat Linux* pour plus d'informations sur la configuration de PAM). Si vous souhaitez désactiver tout accès console, y compris l'accès aux programmes et aux fichiers, désactivez toutes les lignes se rapportant à `pam_console.so` dans le répertoire `/etc/pam.d`. En tant que super-utilisateur, utilisez le script suivant:

```
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo
$i
done
```

24.4. Définition de la console

Le module `pam_console.so` utilise le fichier `/etc/security/console.perms` pour déterminer les permissions des utilisateurs à la console du système. La syntaxe du fichier est très flexible; vous pouvez éditer le fichier de façon à ce que ces instructions ne s'appliquent plus. Cependant, le fichier par défaut possède une ligne ressemblant à celle qui suit:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

Lorsque les utilisateurs se connectent, ils sont attachés à un genre de terminal nommé, soit un serveur X avec un nom comme `:0` ou `mymachine.example.com:1.0`, soit un dispositif comme `/dev/ttyS0` ou `/dev/pts/2`. Par défaut, les consoles virtuelles locales et les serveurs X locaux sont considérés comme locaux, mais si vous souhaitez considérer le terminal série se trouvant près de vous sur le port `/dev/ttyS1` comme lui aussi local, changez cette ligne de façon à ce qu'elle devienne:

```
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
```

```
/dev/ttyS1
```

24.5. Accessibilité des fichiers depuis la console

Dans `/etc/security/console.perms` se trouve une section comportant des lignes comme:

```
<floppy>=/dev/fd[0-1]* \
/dev/floppy/* /mnt/floppy*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
/dev/mixer* /dev/sequencer \
/dev/sound/* /dev/beep
<cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter* /mnt/cdrom*
```

Vous pouvez ajouter vos propres lignes à cette section, si nécessaire. Assurez-vous que les lignes ajoutées se rapportent bien au périphérique approprié. Vous pourriez par exemple, ajouter la ligne suivante:

```
<scanner>=/dev/scanner /dev/usb/scanner*
```

(Évidemment, vérifiez par exemple que `/dev/scanner` est bien votre scanner et non votre disque dur.)

Telle est la première étape. La deuxième étape consiste à définir ce à quoi ces fichiers serviront. Dans la dernière section du fichier `/etc/security/console.perms` essayez de trouver des lignes semblables à celles figurant ci-dessous:

```
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <sound>  0640 root
<console> 0600 <cdrom>  0600 root.disk
```

et ajoutez une ligne similaire à celle qui suit:

```
<console> 0600 <scanner> 0600 root
```

Ensuite, lorsque vous vous connecterez à la console, vous deviendrez propriétaire du périphérique `/dev/scanner` et les permissions seront 0600 (lecture et écriture par vous uniquement). Lorsque vous vous déconnecterez, le périphérique sera détenu par le super-utilisateur et les permissions 0600 seront maintenues (lecture et écriture par le super-utilisateur).

24.6. Activation de l'accès depuis la console pour d'autres applications

Si vous souhaitez que les utilisateurs de la console aient accès à d'autres applications, suivez les étapes ci-dessous.

Tout d'abord, l'accès console fonctionne *uniquement* pour les applications résidant dans `/sbin` ou `/usr/sbin`; l'application souhaitée doit donc s'y trouver. Une fois que vous avez vérifié sa présence, suivez la procédure ci-dessous:

1. Créez un lien à partir du nom de votre application, comme le programme *`foo`* de notre exemple, vers l'application `/usr/bin/consolehelper`:
   ```
   cd /usr/bin
   ln -s consolehelper
   foo
   ```

2. Créez le fichier `/etc/security/console.apps/foo`:
   ```
   touch
   /etc/security/console.apps/foo
   ```
3. Créez un fichier de configuration PAM pour le service `foo` dans `/etc/pam.d/`. Vous pouvez le faire facilement en démarrant avec une copie du fichier de configuration PAM du service, puis en modifiant le fichier pour en changer le comportement:
   ```
   cp /etc/pam.d/halt
   /etc/pam.d/foo
   ```

Désormais, lorsque vous exécuterez `/usr/bin/foo`, le programme appellera `consolehelper`, qui authentifiera l'utilisateur à l'aide de `/usr/sbin/userhelper`. Pour l'authentification, `consolehelper` demandera le mot de passe de l'utilisateur, si `/etc/pam.d/foo` est une copie de `/etc/pam.d/halt` (sinon, la commande fera ce qui est spécifié dans `/etc/pam.d/foo`) et exécutera `/usr/sbin/foo` avec les permissions du super-utilisateur.

Dans le fichier de configuration de PAM, une application peut être configurée pour utiliser le module *pam_timestamp* afin de mémoriser (en cache) une tentative d'authentification réussie. Lorsqu'une application est démarrée et que l'application correcte est fournie (le mot de passe root), un fichier de référence temporelle (timestamp) est créé. Par défaut, une authentification réussie est mémorisée pendant cinq minutes. Pendant ce temps, toute autre application configurée pour utiliser `pam_timestamp` et être lancée à partir de la même session, est authentifiée automatiquement pour l'utilisateur — l'utilisateur n'a donc plus besoin de ressaisir le mot de passe root.

Ce module est inclus dans le paquetage `pam`. Pour activer cette fonctionnalité, le fichier de configuration PAM présent dans `etc/pam.d/` doit comprendre les lignes suivantes:

```
auth sufficient /lib/security/pam_timestamp.so
session optional /lib/security/pam_timestamp.so
```

La première ligne commençant par `auth` devrait figurer après tout autre ligne `auth sufficient`, et la ligne commençant par `session` devrait figurer après tout autre ligne `session optional`.

Si une application configurée pour utiliser `pam_timestamp` est authentifiée avec succès depuis le bouton **Menu Principal** (sur le tableau de bord), l'icône  est affichée dans la zone de notification du tableau de bord (si vous utilisez l'environnement de bureau GNOME). Lorsque l'authentification arrive à expiration (la valeur par défaut est de cinq minutes), l'icône disparaît.

L'utilisateur peut choisir d'oublier l'authentification mémorisée en cliquant sur l'icône et en sélectionnant l'option d'oubli de l'authentification.

24.7. Le groupe `floppy`

Si, pour une raison quelconque, l'accès console ne vous convient pas et que vous souhaitez octroyer aux utilisateurs autres que le super-utilisateur, l'accès au lecteur de disquettes de votre système, vous pouvez le faire en utilisant le groupe `floppy`. Il vous suffit d'ajouter l'utilisateur ou les utilisateurs au groupe `floppy` en vous servant de l'outil de votre choix. Ci-dessous figure un exemple illustrant l'utilisation de `gpasswd` pour l'ajout de l'utilisateur Fred au groupe `floppy`:

```
[root@bigdog root]# gpasswd -a fred
floppy
Adding user fred to group floppy
[root@bigdog root]#
```

L'utilisateur Fred pourra à présent accéder au lecteur de disquettes du système à partir de la console.

Chapitre 25.

Configuration des utilisateurs et des groupes

L'outil **Gestionnaire d'utilisateurs** vous permet d'afficher, de modifier, d'ajouter et de supprimer des utilisateurs et groupes locaux.

Pour utiliser le **Gestionnaire d'utilisateurs**, vous devez exécuter le système X Window et avoir les privilèges du super-utilisateur. Le paquetage RPM `redhat-config-users` doit également être installé. Pour démarrer le **Gestionnaire d'utilisateurs** à partir du bureau, allez au bouton **Menu principal** (sur le panneau) => **Paramètres Système => Utilisateurs et groupes** ou tapez la commande `redhat-config-users` à l'invite du shell (par exemple, dans un terminal XTerm ou GNOME).

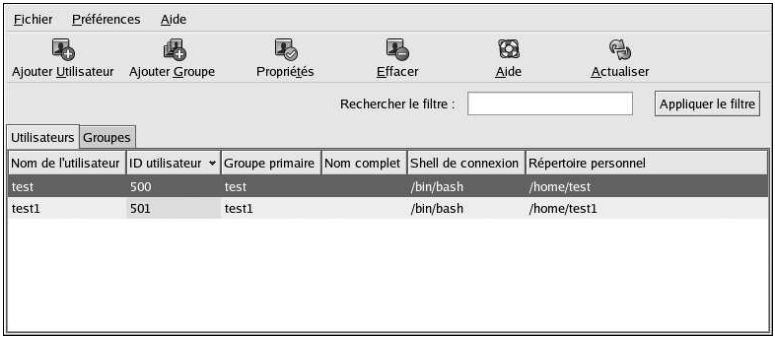

Figure 25-1. Gestionnaire d'utilisateurs

Pour afficher une liste de tous les utilisateurs locaux du système, cliquez sur l'onglet **Utilisateurs** (Users). Pour afficher une liste de tous les groupes locaux du système, cliquez sur l'onglet **Groupes**.

Si vous devez trouver un groupe ou un utilisateur spécifique, tapez les premières lettres de son nom dans le champ **Filtrer par** (Filter by). Appuyez sur [Entrée] ou cliquez sur **Appliquer le filtre** (Apply filter). La liste filtrée s'affichera alors à l'écran.

Pour trier les utilisateurs ou les groupes, cliquez sur le nom de la colonne. Les utilisateurs ou groupes seront triés selon la valeur de cette colonne.

Red Hat Linux réserve les ID utilisateur au-dessous de 500 aux utilisateurs du système. Par défaut, **Gestionnaire d'utilisateurs** n'affiche pas les utilisateurs du système. Pour afficher tous les utilisateurs, y compris les utilisateurs du système, désélectionnez **Préférences => Filtrer les utilisateurs et groupes du système** (Filter system users and groups) dans le menu déroulant.

Pour de plus amples informations sur les utilisateurs et les groupes, consultez le *Guide de référence de Red Hat Linux* et le *Guide d'administration système de Red Hat Linux*.

25.1. Ajout d'un nouvel utilisateur

Pour ajouter un nouvel utilisateur, cliquez sur le bouton **Ajouter utilisateur** (Add User). Une fenêtre apparaît, comme le montre la Figure 25-2. Tapez le nom d'utilisateur et le nom complet pour le nouvel utilisateur dans les champs appropriés. Tapez le mot de passe correspondant dans les champs **Mot de passe** (Password) et **Confirmer le mot de passe**. Le mot de passe doit comporter au moins six caractères.

Astuce

Plus le mot de passe de l'utilisateur sera long, plus il sera difficile pour quelqu'un d'autre de le deviner et de se connecter sans permission sous ce compte. Il est aussi recommandé de ne pas baser le mot de passe sur un nom et de choisir une combinaison de lettres, chiffres et caractères spéciaux.

Sélectionnez un shell de connexion. Si vous hésitez sur le shell à sélectionner, acceptez la valeur par défaut `/bin/bash`. Le répertoire d'enregistrement par défaut est `/home/`*`nom d'utilisateur`* (Username). Vous pouvez changer le répertoire d'enregistrement qui est créé pour l'utilisateur, ou choisir de ne pas créer de répertoire en dé-sélectionnant **Créer un répertoire home** (Create home directory).

Si vous décidez de créer un répertoire personnel (home), sachez que les fichiers de configuration par défaut seront copiés du répertoire `/etc/skel` dans le nouveau répertoire home.

Red Hat Linux utilise un système dit *groupe privé d'utilisateurs* (UPG de l'anglais 'User Private Group'). Le système UPG n'ajoute et ne change rien dans la manière UNIX standard de traiter les groupes; il offre seulement une nouvelle convention. Chaque fois que vous créez un nouvel utilisateur, un groupe unique avec le même nom que l'utilisateur est aussi créé par défaut. Si vous ne souhaitez pas créer ce groupe, désélectionnez **Créer un groupe privé pour l'utilisateur** (Create a private group for the user).

Pour spécifier un ID utilisateur pour l'utilisateur, sélectionnez **Spécifier un ID utilisateur manuellement** (Specify user ID manually). Si l'option n'est pas sélectionnée, le prochain ID utilisateur libre après le numéro 500 sera assigné au nouvel utilisateur. Red Hat Linux réserve les ID utilisateur au-dessous de 500 aux utilisateurs du système.

Cliquez sur **OK** pour créer l'utilisateur.

Figure 25-2. Nouvel utilisateur

Pour configurer des propriétés d'utilisateur plus avancées, comme l'expiration des mots de passe, modifiez les propriétés de l'utilisateur après l'avoir ajouté. Consultez la Section 25.2 pour plus d'informations.

Pour ajouter l'utilisateur à des groupes supplémentaires, cliquez sur l'onglet **Utilisateur** (User), sélectionnez l'utilisateur, puis cliquez sur **Propriétés** (Properties). Dans la fenêtre **Propriétés de l'utilisateur** (User Properties), sélectionnez l'onglet **Groupes**. Sélectionnez les groupes auxquels vous voulez que l'utilisateur fasse partie, sélectionnez le groupe principal pour l'utilisateur puis cliquez sur **OK**.

25.2. Modification des propriétés de l'utilisateur

Pour afficher les propriétés d'un utilisateur existant, cliquez sur l'onglet **Utilisateurs** (Users), sélectionnez l'utilisateur dans la liste des utilisateurs et cliquez sur **Propriétés** (Properties)(ou sélectionnez **Fichier => Propriétés** dans le menu déroulant). Une fenêtre semblable à celle reproduite dans la Figure 25-3 apparaîtra alors.

Figure 25-3. Propriétés de l'utilisateur

La fenêtre **Propriétés de l'utilisateur** (User Properties) est divisée en pages contenant des onglets:

- **Informations utilisateur** (User Data) — Des informations de base sur l'utilisateur sont configurées lorsque vous ajoutez l'utilisateur. Utilisez cet onglet pour changer le nom complet, le mot de passe, le répertoire personnel ou le shell pour la connexion.
- **Information du compte** (Account Info) — Sélectionnez **Activer l'expiration du compte** (Enable account expiration) si vous souhaitez que le compte expire à une certaine date. Entrez la date dans les champs affichés. Sélectionnez **Compte utilisateur verrouillé** (User account is locked) pour verrouiller le compte utilisateur afin que l'utilisateur ne puisse plus se connecter au système.
- **Informations mot de passe** (Password Info) — Cet onglet montre la date à laquelle l'utilisateur a changé son mot de passe pour la dernière fois. Pour forcer l'utilisateur à changer son mot de passe après un certain nombre de jours, sélectionnez **Activer l'expiration du mot de passe** (Enable password expiration). Vous pouvez aussi sélectionner le nombre de jours avant que l'utilisateur ne soit autorisé à changer son mot de passe, le nombre de jours avant que l'utilisateur ne reçoive un message lui demandant de changer de mot de passe et le nombre de jours avant que le compte ne devienne inactif.
- **Groupes** — Sélectionnez les groupes auxquels vous souhaitez que l'utilisateur fasse partie ainsi que le groupe primaire de l'utilisateur.

25.3. Ajout d'un nouveau groupe

Pour ajouter un nouveau groupe utilisateur, cliquez sur le bouton **Ajouter groupe** (Add Group). Une fenêtre semblable à celle reproduite à la Figure 25-4 s'affichera à l'écran. Entrez le nom du nouveau groupe. Pour spécifier un ID groupe pour le nouveau groupe, sélectionnez **Spécifier l'ID groupe manuellement** (Specify group ID manually) et sélectionnez le GID. Red Hat Linux réserve les ID groupe inférieurs à 500 aux groupes du système.

Cliquez sur **OK** pour créer le groupe. Le nouveau groupe apparaîtra dans la liste des groupes.

Figure 25-4. Nouveau groupe

Pour ajouter des utilisateurs au groupe, consultez la Section 25.4.

25.4. Modification des propriétés du groupe

Pour afficher les propriétés d'un groupe existant, choisissez le groupe voulu dans la liste et cliquez sur **Propriétés** (Properties) à partir du bouton de menu (ou choisissez **Fichier => Propriétés** dans le menu déroulant). Une fenêtre semblable à celle reproduite dans la Figure 25-5 apparaîtra.

Figure 25-5. Propriétés des groupes

L'onglet **Utilisateurs du groupe** (Group Users) affiche les utilisateurs qui sont membres du groupe. Sélectionnez des utilisateurs supplémentaires pour les ajouter au groupe et désélectionnez des utilisateurs pour les retirer du groupe. Cliquez sur **OK** ou **Appliquer** (Apply) pour changer les utilisateurs du groupe.

25.5. Configuration de la ligne de commande

Si vous préférez des outils de la ligne de commande ou si ne disposez pas d'un système X Window installé, utilisez ce chapitre pour configurer les utilisateurs et les groupes.

25.5.1. Ajout d'un nouvel utilisateur

Pour ajouter un nouvel utilisateur au système:

1. Exécutez la commande `useradd` pour créer un compte utilisateur verrouillé:
   `useradd <username>`
2. Déverrouillez le compte en utilisant la commande `passwd` pour attribuer un mot de passe et établir des directive quant à l'expiration de ce dernier:
   `passwd <username>`

Les options en ligne de commande pour `useradd` se trouvent dans le Tableau 25-1.

Option	Description
`-c` *commentaire*	Commentaire pour l'utilisateur
`-d` *home-dir*	Répertoire home à utiliser au lieu du répertoire par défaut `/home/`*nom d'utilisateur*
`-e` *date*	Date à laquelle le compte deviendra inactif dans le format AAAA--MM-JJ
`-f` *jours*	Nombre de jours pouvant s'écouler après l'expiration du mot de passe, avant que le compte ne devienne inactif (Si **0** est la valeur choisie, le compte deviendra inactif aussitôt après l'expiration du mot de passe. Si le choix est **-1** le compte de deviendra pas inactif après l'expiration du mot de passe.)
`-g` *nom-groupe*	Nom ou numéro du groupe pour le groupe par défaut de l'utilisateur (Le groupe doit préalablement exister).
`-G` *liste-groupe*	Liste des noms ou numéros de groupes supplémentaires (autres que ceux par défaut), séparés par des virgules, auxquels le membre appartient (Les groupes doivent préalablement exister).
`-m`	Entraîne la création du répertoire home s'il n'existe pas.
`-M`	Évite la création du répertoire home.
`-n`	Évite la création d'un groupe privé d'utilisateur pour l'utilisateur.
`-r`	Entraîne la création d'un compte système avec un ID utilisateur (UID) inférieur à 500 et sans un répertoire home.
`-p` *mot-de-passe*	Le mot de passe crypté avec `crypt`
`-s`	Shell de connexion de l'utilisateur, qui est par défaut `/bin/bash`
`-u` *uid*	ID utilisateur pour l'utilisateur, qui doit être unique et supérieur à 499.

Tableau 25-1. Options en ligne de commande pour `useradd`

25.5.2. Ajout d'un groupe

Pour ajouter un groupe au système, utilisez la commande `groupadd`:

```
groupadd <group-name>
```

Les options de la ligne de commande pour `groupadd` se trouvent dans le Tableau 25-2.

Option	Description
`-g` *gid*	ID groupe pour le groupe, qui doit être unique et supérieur à 499.
`-r`	Entraîne la création d'un groupe système avec un ID groupe (GID) inférieur à 500.
`-f`	Quitte avec un message d'erreur si le groupe existe déjà. (Le groupe groupe n'est pas modifié). Si les options `-g` et `-f` sont précisées mais que le groupe existe déjà, l'option `-g` n'est pas prise en compte.

Tableau 25-2. Options de la ligne de commande pour `groupadd`

25.5.3. Expiration du mot de passe

Pour des raisons de sécurité, il est recommandé aux utilisateurs de changer leurs mots de passe régulièrement. Ceci peut être réaliser lors de l'ajout ou de la modification de l'utilisateur sous l'onglet **Informations-mot-de-passe** de l'outil **Gestionnaire d'utilisateurs**.

Pour configurer l'expiration du mot de passe d'un utilisateur à partir de l'invite du shell, utilisez la commande `chage` suivi d'une des options figurant dans le Tableau 25-3 et du nom d'utilisateur de l'utilisateur de mot de passe.

Important

Les mots de passe ombre doivent être activés afin de pouvoir utiliser la commande `chage`.

Option	Description
`-m` *jours*	Précise la période, en jours, pendant laquelle l'utilisateur doit changer son mot de passe. Si la valeur choisie est 0, le mot de passe n'expire pas.
`-M` *jours*	Précise durée maximale, en jours, pendant laquelle le mot de passe est valide. Lorsque le nombre de jours spécifié par cette option ajouté au nombre de jours précisé avec l'option `-d` est inférieur au jour actuel, l'utilisateur doit changer son mot de passe avant d'utiliser son compte.
`-d` *jours*	Précise le nombre de jours écoulés entre le 1er janvier 1970 et le jour où le mot de passe a été changé.
`-I` *jours*	Spécifie le nombre de jours inactifs après l'expiration du mot de passe, avant que le compte ne soit verrouillé. Si la valeur est 0, le compte ne sera pas verrouillé après l'expiration du mot de passe.
`-E` *date*	Spécifie la date à laquelle le compte sera verrouillé, selon le format AAAA-MM-JJ. Au lieu de la date, il est possible d'utiliser le nombre de jours écoulés depuis le 1er janvier 1970.
`-W` *jours*	Spécifie le nombre de jours devant s'écouler avant la date expiration du mot de passe, avant d'avertir l'utilisateur.

Tableau 25-3. Option de la ligne de commande pour `chage`

Astuce

Si la commande `chage` est suivie directement d'un nom d'utilisateur (sans option), les valeurs courantes de l'expiration du mot de passe s'afficheront et il sera alors possible de les modifier.

Si un administrateur système souhaite qu'un utilisateur détermine un mot de passe lors de sa première connexion, il suffit de choisir une expiration immédiate du mot de passe, forçant ainsi l'utilisateur à le changer aussitôt après s'être connecté pour la première fois.

Pour forcer un utilisateur à configurer son mot de passe lors de la première connexion à la console, suivez les étapes ci-dessous. Notez que cette procédure ne fonctionnera pas si l'utilisateur se connecte

en utilisant le protocole SSH.

1. *Verrouillez le mot de passe de l'utilisateur* — Si l'utilisateur n'existe pas, utilisez la commande `useradd` afin de créer le compte utilisateur mais n'attribuez aucun mot de passe afin qu'il reste verrouillé.

   Si le mot de passe est déjà activé, verrouillez-le à l'aide de la commande suivante:
   `usermod -L nom-d'utilisateur`

2. *Forcez l'expiration immédiate du mot de passe* — Pour ce faire, tapez la commande suivante:
   `chage -d 0 nom-d'utilisateur`

   Cette commande détermine la valeur correspondant à la date à laquelle le mot de passe a été changé la dernière fois, à partir de la référence, 1er janvier 1970. Cette valeur entraîne une expiration immédiate forcée du mot de passe, indépendemment de la politique d'expiration en place (s'il y en a une).

3. *Déverrouillez le compte* — Pour ce faire, il existe deux approches courantes: l'administrateur peut soit assigner un mot de passe initial, soit assigner un mot de passe blanc.

   
   Avertissement

   N'utilisez pas la commande `passwd` pour établir le mot de passe car cette commande désactivera l'expiration immédiate du mot de passe que vous venez juste de configurer.

   Pour attribuer une mot de passe initial, suivez les étapes ci-dessous:

   - Lancez l'interpréteur de la ligne de commande `python` à l'aide de la commande `python`. La sortie suivante s'affichera:
     ```
     Python 2.2.2 (#1, Dec 10 2002, 09:57:09)
     [GCC 3.2.1 20021207 (Red Hat Linux 8.0 3.2.1-2)] on linux2
     Type "help", "copyright", "credits" or "license" for more information.
     >>>
     ```
   - À l'invite, tapez les éléments suivants (en remplaçant *`mot-de-passe`* par le mot de passe à crypter et *`salt`* par une combinaison bien précise de deux lettres de l'alphabet en majuscule ou minuscule, chiffres, le point (.) ou la barre oblique en avant (/)):
     ```
     import crypt; print
     crypt.crypt("mot-de-passe","salt")
     ```
     La sortie produite sera un mot de passe crypté semblable à l'exemple suivant: `12CsGd8FRcMSM`.
   - Tapez [Ctrl]-[D] pour quitter l'interpréteur Python.
   - Coupez et collez la sortie exacte du mot de passe crypté, sans aucun espace blanc ni au début, ni à la fin, dans la commande suivante:
     ```
     usermod -p "mot-de-passe-crypté"
     nom-d'utilisateur
     ```

   Au lieu d'attribuer un mot de passe initial, un mot de passe blanc peut-être établi à l'aide de la commande:
   `usermod -p "" nom-d'utilisateur`

   
   Attention

   L'utilisation d'un mot de passe blanc est certes très pratique aussi bien pour l'utilisateur que pour l'administrateur, mais il y a toujours le risque qu'une tierce personne ne se connecte en premier et n'accède au système. Afin de minimiser une telle menace, il est recommandé à l'administrateur de s'assurer que l'utilisateur est prêt à se connecter dès que le compte est déverrouillé.

Dans les deux cas, l'utilisateur devra saisir un nouveau mot de passe lors de la première connexion.

25.6. Explication du processus

Les étapes suivantes illustrent le processus engendré par l'exécution de la commande `useradd juan` sur un système disposant d'un mot de passe ombre activé:

1. Une nouvelle ligne pour `juan` est créée dans `/etc/passwd`. Cette dernière affiche les caractéristiques suivantes:
   - Elle commence par le nom d'utilisateur, `juan`.
   - Le champ du mot de passe contient un `x` indiquant que le système utilise des mots de passe masqué.
   - Un UID égal ou supérieur à 500 est créé. (Sous Red Hat Linux les UID et GID inférieurs à 500 sont réservés pour aux opérations du système.)
   - Un GID égal ou supérieur à 500 est créé.
   - Les informations GECOS facultatives demeurent vierges.
   - Le répertoire home de l'utilisateur est établi, `/home/juan/`.
   - Le shell par défaut est établi à `/bin/bash`.

2. Une nouvelle ligne pour `juan` est créée dans `/etc/shadow`. Cette dernière affiche les caractéristiques suivantes:
   - Elle commence par le nom d'utilisateur, `juan`.
   - Deux points d'exclamation (`!!`) apparaissent dans le champ mot de passe du fichier `/etc/shadow`, verrouillant le compte.

     

     Remarque

     Si un mot de passe crypté est passé à l'aide de l'indicateur (ou 'flag') `-p`, il est placé dans le fichier `/etc/shadow` sur la nouvelle ligne relative à l'utilisateur.

   - Le mot de passe est ainsi établi de manière à ne jamais expirer.

3. Une nouvelle ligne pour un groupe nommé `juan` est créé dans `/etc/group`. Un groupe portant le même nom qu'un utilisateur est appelé un *groupe privé d'utilisateurs*. Pour obtenir de plus amples informations sur les groupes privés d'utilisateurs, reportez-vous à la Section 25.1.

   La ligne créée dans `/etc/group` affiche les caractéristiques suivantes:
   - Elle commence par le nom de groupe, `juan`.
   - Un `x` apparaît dans le champ du mot de passe, indiquant que le système utilise des mot de passe ombre pour les groupes.
   - Le GID correspond à celui qui est établi pour l'utilisateur `juan` dans `/etc/passwd`.

4. Une nouvelle ligne pour un groupe nommé `juan` est créée dans `/etc/gshadow`. Cette dernière affiche les caractéristiques suivantes:

- Elle commence par le nom du groupe, `juan`.
- Un point d'exclamation (`!`) apparaît dans le champs mot de passe du fichier `/etc/gshadow`, verrouillant le groupe.
- Tous les autres champs sont vierges.

5. Un répertoire pour l'utilisateur `juan` est créé dans le répertoire `/home/`. Ce dernier est la propriété de l'utilisateur `juan` et du groupe `juan`. Toutefois, *seul* l'utilisateur `juan` dispose des privilèges d'écriture, lecture et exécution. Toute autre permission est refusée.
6. Les fichiers placés à l'intérieur de `/etc/skel/` (qui contient les paramètres par défaut de l'utilisateur) sont copiés dans le nouveau répertoire `/home/juan/`.

À ce stade, un compte verrouillé portant le nom `juan` existe sur le système. Afin de l'activer, l'administrateur doit tout d'abord attribuer un mot de passe au compte à l'aide de la commande `passwd` et doit ensuite, s'il le désire, établir des directives quant à l'expiration de ce dernier.

Chapitre 26.

Collecte d'informations sur le système

Avant d'apprendre à configurer votre système, vous devriez apprendre comment recueillir des informations essentielles sur celui-ci. Par exemple, vous devriez être en mesure de déterminer la quantité de mémoire ou d'espace libre, la façon dont est partitionné votre disque dur et les processus en cours d'exécution. Ce chapitre vous explique comment recueillir ce type d'informations sur votre système Red Hat Linux à l'aide de commandes et de programmes simples. Avant d'apprendre à configurer votre système, vous devriez apprendre comment recueillir des informations essentielles sur celui-ci. Par exemple, vous devriez être en mesure de déterminer la quantité de mémoire libre, la façon dont est partitionné votre disque dur et les processus en cours d'exécution. Ce chapitre vous explique comment recueillir ce type d'informations sur votre système Red Hat Linux à l'aide de commandes et de quelques programmes simples.

26.1. Processus système

La commande `ps ax` affiche une liste des processus système en cours, y compris les processus appartenant à d'autres utilisateurs. Pour afficher également le propriétaire de ces processus, utilisez la commande `ps aux`. Cette liste est statique ; il s'agit d'une copie des processus en cours d'exécution. Pour obtenir une liste des processus en cours mise à jour constamment, utilisez la commande `top` décrite ci-dessous.

Les résultats de la commande `ps` peuvent être longs. Pour les empêcher d'être trop importants, vous pouvez les restreindre grâce à la commande suivante:

```
ps aux | less
```

Vous pouvez utiliser la commande `ps` combinée à la commande `grep` pour savoir si une commande est en cours d'exécution. Par exemple, pour déterminer si **emacs** est en cours d'exécution, utilisez la commande suivante:

```
ps ax | grep emacs
```

La commande `top` affiche les processus en cours d'exécution et d'importantes informations sur ceux-ci, telles que l'utilisation de la mémoire et de l'unité centrale. La liste est interactive et en temps réel. Ci-dessous figure un exemple de liste produite par la commande `top`:

```
 00:53:01  up 6 days, 14:05,  3 users,  load average: 0.92, 0.87, 0.71
71 processes: 68 sleeping, 2 running, 1 zombie, 0 stopped
CPU states:  18.0% user   0.1% system   16.0% nice   0.0% iowait  80.1% idle
Mem:  1030244k av,  985656k used,   44588k free,       0k shrd,  138692k buff
                    424252k actv,   23220k in_d,  252356k in_c
Swap: 2040212k av,  330132k used, 1710080k free                  521796k cached

  PID USER     PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME COMMAND
15775 joe      5    0 11028  10M  3192 S     1.5  4.2   0:46 emacs
14429 root     15   0 63620  62M  3284 R     0.5 24.7  63:33 X
17372 joe      11   0  1056 1056   840 R     0.5  0.4   0:00 top
17356 joe      2    0  4104 4104  3244 S     0.3  1.5   0:00 gnome-terminal
    1 root     0    0   544  544   476 S     0.0  0.2   0:06 init
    2 root     0    0     0    0     0 SW    0.0  0.0   0:00 kflushd
    3 root     1    0     0    0     0 SW    0.0  0.0   0:24 kupdate
    4 root     0    0     0    0     0 SW    0.0  0.0   0:00 kpiod
    5 root     0    0     0    0     0 SW    0.0  0.0   0:29 kswapd
  347 root     0    0   556  556   460 S     0.0  0.2   0:00 syslogd
```

```
357 root       0   0   712  712   360 S     0.0  0.2   0:00 klogd
372 bin        0   0   692  692   584 S     0.0  0.2   0:00 portmap
388 root       0   0     0    0     0 SW    0.0  0.0   0:00 lockd
389 root       0   0     0    0     0 SW    0.0  0.0   0:00 rpciod
414 root       0   0   436  432   372 S     0.0  0.1   0:00 apmd
476 root       0   0   592  592   496 S     0.0  0.2   0:00 automount
```

Pour quitter `top`, appuyez sur la touche [q].

Il existe de nombreuses commandes interactives utiles que vous pouvez utiliser avec la commande `top`. Ci-après figure un tableau contenant certaines d'entre elles:

Commande	Description
[Barre espace]	Réactualise immédiatement l'affichage des données
[h]	Affiche un écran d'aide
[k]	Arrête un processus. Le système vous demande l'ID du processus et le signal à lui envoyer.
[n]	Change le nombre de processus affichés. Le système vous demande d'entrer le nombre désiré.
[u]	Trie les processus par utilisateurs.
[M]	Trie les processus par utilisation de la mémoire.
[P]	Trie les processus par utilisation de l'unité centrale.

Tableau 26-1. Commandes `top` interactives

Astuce

Des applications telles que **Mozilla** et **Nautilus** sont dotées une *prise en charge des fils* — plusieurs fils (ou threads) sont créés pour traiter de multiples utilisateurs ou requêtes, et chaque thread reçoit un ID processus. Par défaut, `ps` et `top` n'affichent que le thread principal (initial). Pour afficher tous les threads, utilisez la commande `ps -m` ou tapez [Maj]-[H] dans `top`.

Si vous désirez utiliser une interface graphique pour accomplir les tâches de la commande `top`, vous pouvez utiliser **GNOME System Monitor**. Pour lancer cette application à partir du bureau, sélectionnez le bouton **Menu principal** (sur le Tableau de bord) => **Outils de système** => **Moniteur système** ou tapez `gnome-system-monitor` à une invite de shell prompt depuis le système X Window. Sélectionnez ensuite l'onglet **Liste des processus**.

L'application **GNOME System Monitor** vous permet de rechercher des processus dans la liste des processus en cours et d'afficher tous les processus, vos processus ou les processus actifs.

Pour en savoir plus sur un processus, sélectionnez-le et cliquez sur le bouton **Plus d'informations**. Des détails concernant le processus s'afficheront en bas de la fenêtre.

Pour arrêter un processus, sélectionnez-le et cliquez sur **Arrêter les processus**. Cette fonction est très utile pour les processus ne répondant plus aux saisies de l'utilisateur.

Pour trier les processus selon les informations d'une colonne spécifique, cliquez sur len om de la colonne. La colonne d'après laquelle les informations sont triées devient gris foncé.

Par défaut, **GNOME System Monitor** n'affiche pas les threads. Pour changer cette préférence, sélectionnez **Éditer => Préférences**, cliquez sur l'onglet **Listage des processus** (Process Listing) et sélectionnez **Afficher les fils** (Show Threads). Les préférences vous permettent également de configurer l'intervalle de mise à jour, le type d'informations à afficher par défaut sur chaque processus et les couleurs des graphes système.

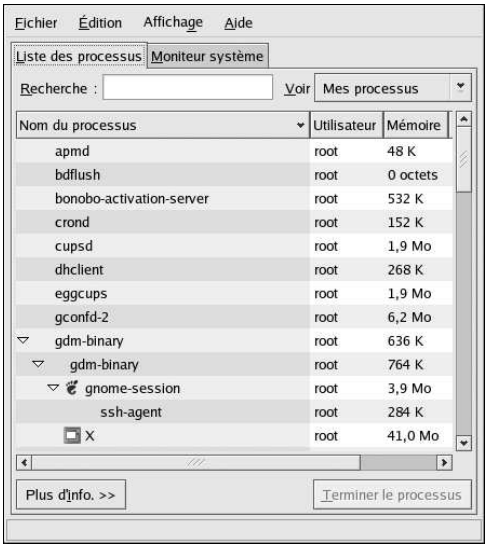

Figure 26-1. Listage des processus de 'GNOME System Monitor'

26.2. Utilisation de la mémoire

La commande `free` affiche la quantité totale de mémoire physique et d'espace swap du système, de même que la quantité de mémoire utilisée, libre, partagée, tampon dans le noyau et cache.

```
             total       used       free     shared    buffers     cached
Mem:        256812     240668      16144     105176      50520      81848
-/+ buffers/cache:     108300     148512
Swap:       265032        780     264252
```

La commande `free -m` permet d'obtenir les mêmes informations mais en méga-octets, ce qui rend leur lecture plus facile.

```
             total       used       free     shared    buffers     cached
Mem:           250        235         15        102         49         79
-/+ buffers/cache:        105        145
Swap:          258          0        258
```

Si vous préférez utiliser une interface graphique pour `free`, vous pouvez utiliser **GNOME System Monitor**. Pour lancer cette application à partir du bureau, sélectionnez le bouton **Menu principal** (sur le tableau de bord) **=> System Tools => Moniteur système** ou tapez `gnome-system-monitor` à une invite de shell dans X Window. Sélectionnez ensuite l'onglet **Moniteur système**.

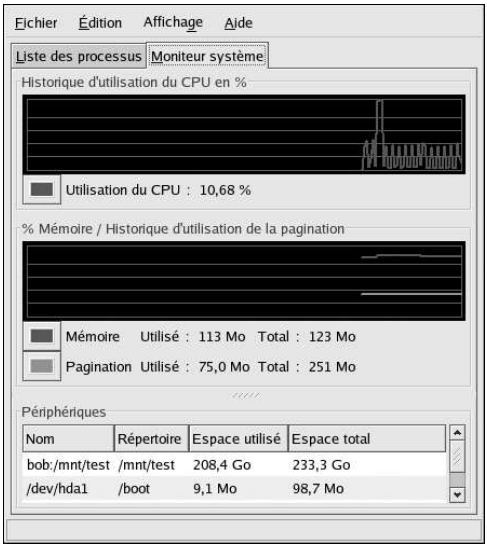

Figure 26-2. Moniteur système de GNOME ('GNOME System Monitor')

26.3. Systèmes de fichiers

La commande `df` affiche l'utilisation de l'espace disque du système. Si vous entrez la commande `df` à l'invite du shell, le résultat ressemblera à l'extrait suivant:

```
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/hda2             10325716   2902060   6899140  30% /
/dev/hda1                15554      8656      6095  59% /boot
/dev/hda3             20722644   2664256  17005732  14% /home
none                    256796         0    256796   0% /dev/shm
```

Par défaut, cet utilitaire affiche la taille de partition en blocs de 1 kilo-octet et la quantité d'espace disque libre et utilisé en kilo-octets. Pour visualiser les informations en méga-octets et giga-octets, utilisez la commande `df -h`. L'argument `-h` signifie format humainement lisible. La sortie ressemble alors plus ou moins à l'extrait suivant:

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda2             9.8G  2.8G  6.5G  30% /
/dev/hda1              15M  8.5M  5.9M  59% /boot
/dev/hda3              20G  2.6G   16G  14% /home
none                  251M     0  250M   0% /dev/shm
```

Dans la liste de partitions, il y a une entrée pour `/dev/shm`. Cette entrée représente le système de fichiers mémoire virtuelle du système.

La commande `du` affiche une estimation de la quantité d'espace utilisée par des fichiers dans un répertoire. Si vous entrez `du` depuis l'invite du shell, l'utilisation d'espace disque de chaque sous-répertoire sera également affichée. De plus, le total du répertoire courant et de ses sous-répertoires est indiqué à la dernière ligne de la liste. Si vous ne voulez pas voir tous les sous-répertoires, utilisez la commande

`du -hs` pour ne visualiser que le grand total du répertoire et ce, dans un format humainement lisible. Utilisez la commande `du --help` pour afficher d'autres options.

Pour visualiser les partitions du système et l'utilisation de l'espace disque en format graphique, utilisez l'onglet **Moniteur système** comme le montre la Figure 26-2.

Astuce

Pour des informations sur l'implémentation des quotas de disque, reportez-vous au Chapitre 6.

26.3.1. Contrôle des systèmes de fichiers

Red Hat Linux fournit un utilitaire nommé `diskcheck` qui contrôle la quantité d'espace disque libre sur le système. Il se base sur le fichier de configuration et envoie un email à l'administrateur de système lorsqu'un ou plusieurs disques ont atteint une certaine capacité (spécifiée). Pour utiliser cet utilitaire, le paquetage RPM `diskcheck` doit être installé.

Cet utilitaire est exécuté comme une tâche cron [1] effectuée toutes les heures.

Les variables suivantes peuvent être définies dans `/etc/diskcheck.conf`:

- `defaultCutoff` — Lorsque le disque atteint ce pourcentage, cela sera rapporté. Par exemple, si `defaultCutoff = 90`, un message sera envoyé lorsque le disque contrôlé aura atteint 90% de sa capacité.
- `cutoff[`*`/dev/partition`*`]` — Remplace la commande `defaultCutoff` pour la partition. Par exemple, si `cutoff['/dev/hda3'] = 50` est spécifié, `diskcheck` avertira l'administrateur de système lorsque la partition aura atteint `/dev/hda3` 50% de sa capacité.
- `cutoff[`*`/mountpoint`*`]` — Remplace la commande `defaultCutoff` pour le point de montage. Par exemple, si `cutoff['/home'] = 50` est spécifié, `diskcheck` avertira l'administrateur de système lorsque le point de montage aura atteint `/home` 50% de sa capacité.
- `exclude` — Spécifie une ou plusieurs partitions que `diskcheck` doit ignorer. Par exemple, si `exclude = "/dev/sda2 /dev/sda4"` est spécifié, `diskcheck` n'avertira pas l'administrateur de système si `/dev/sda2` ou `/dev/sda4` atteint le pourcentage de coupure spécifié.
- `ignore` — Spécifie un ou plusieurs types de système de fichiers à ignorer au format `-x`*`type-système de fichiers`*. Par exemple, si `ignore = "-x nfs -x iso9660"` est spécifié, l'administrateur de système ne sera pas averti si les systèmes de fichiers nfs ou iso9660 atteignent leur capacité.
- `mailTo` — L'adresse email de l'administrateur de système où le message devra être envoyé lorsque les partitions et points de montage atteindront la capacité spécifiée. Par exemple, si `mailTo = "webmaster@example.com"` est spécifié, webmaster@example.com recevra les messages d'avertissement.
- `mailFrom` — Spécifie l'identité de l'expéditeur du message. Cette option s'avère utile si l'administrateur de système veut filtrer le message de `diskcheck`. Par exemple, si `mailFrom = "Disk Usage Monitor"` est spécifié, le message sera envoyé à l'administrateur de système par l'intermédiaire du contrôle d'utilisation du disque (expéditeur).
- `mailProg` — Spécifie le programme de courrier à utiliser pour envoyer les messages d'avertissement. Par exemple, si `mailProg = "/usr/sbin/sendmail"` est spécifié, Sendmail sera utilisé comme programme de courrier.

1. Pour obtenir de plus amples informations concernant cron, consultez le Chapitre 28.

Il n'est pas nécessaire de redémarrer un service si vous avez modifié le fichier de configuration, car il est lu chaque fois que la tâche cron est exécutée. Pour que les tâches cron puissent être exécutées, le service `crond` doit être en cours d'exécution. Pour déterminer si le démon s'exécute, utilisez la commande `/sbin/service crond status`. Nous vous recommandons de démarrer le service au moment du démarrage. Reportez-vous au Chapitre 14 pour obtenir plus de détails sur le lancement automatique du service cron au démarrage.

26.4. Matériel

Si vous avez des problèmes lors de la configuration de votre matériel ou voulez simplement savoir quel matériel se trouve sur votre système, utilisez l'application **Navigateur matériel** (Hardware Browser). Pour démarrer le programme à partir du bureau, sélectionnez le bouton **Menu principal => Outils de système => Navigateur matériel** ou tapez `hwbrowser` à une invite du shell. Comme le montre la Figure 26-3, le programme affiche le lecteurs de CD-ROM, de disquettes, les disques durs et leurs partitions, les périphériques réseau, les dispositifs de pointage, les périphériques système et les cartes vidéo. Pour afficher des informations sur l'un de ces éléments, cliquez sur le nom de catégorie désiré dans le menu de gauche.

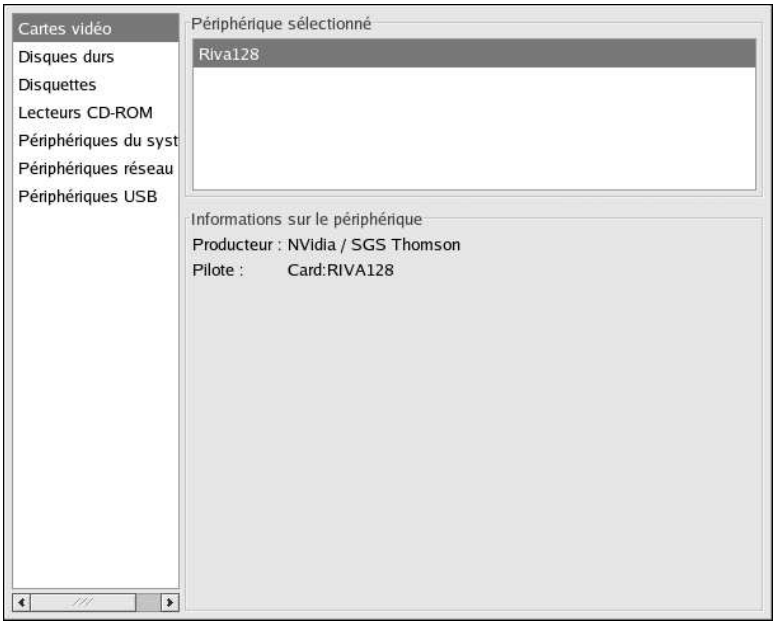

Figure 26-3. Navigateur matériel

La commande `lspci` permet d'afficher tous les dispositifs PCI. Utilisez la commande `lspci -v` pour obtenir plus d'informations, ou `lspci -vv` pour en obtenir encore plus.

Par exemple, `lspci` peut être utilisé pour déterminer le fabricant, le modèle et la taille de la mémoire d'une carte vidéo du système:

```
01:00.0 VGA compatible controller: Matrox Graphics, Inc. MGA G400 AGP (rev 04)
```

```
(prog-if 00 [VGA])
Subsystem: Matrox Graphics, Inc. Millennium G400 Dual Head Max
Flags: medium devsel, IRQ 16
Memory at f4000000 (32-bit, prefetchable) [size=32M]
Memory at fcffc000 (32-bit, non-prefetchable) [size=16K]
Memory at fc000000 (32-bit, non-prefetchable) [size=8M]
Expansion ROM at 80000000 [disabled] [size=64K]
Capabilities: [dc] Power Management version 2
Capabilities: [f0] AGP version 2.0
```

`lspci` permet également d'en savoir plus sur la carte réseau de votre système si vous n'en connaissez pas le fabricant ou le numéro de modèle.

26.5. Ressources supplémentaires

Pour en savoir plus sur la collecte d'informations du système, consultez les sources d'informations suivantes.

26.5.1. Documentation installée

- `ps --help` — Affiche une liste d'options qui peuvent être utilisées avec `ps`.
- Page de manuel relative à `top` — Tapez `man top` pour en savoir plus sur `top` et ses nombreuses options.
- Page de manuel relative à `free` — Tapez `man free` pour en savoir plus sur `free` et ses nombreuses options.
- Page de manuel relative à `df` — Tapez `man df` pour en savoir plus sur `df` et ses nombreuses options.
- Page de manuel relative à `du` — Tapez `man du` pour en savoir plus sur `du` et ses nombreuses options.
- Page de manuel relative à `lspci` — Tapez `man lspci` pour en savoir plus sur la commande `lspci` et ses nombreuses options.
- `/proc` — Le contenu du répertoire `/proc` peut également être utilisé pour recueillir des informations système plus détaillées. Reportez-vous au *Guide de référence de Red Hat Linux* pour en savoir plus sur le répertoire `/proc`.

26.5.2. Livres sur le sujet

- *Guide d'administration système de Red Hat Linux*; Red Hat, Inc. — Inclut un chapitre sur le contrôle des ressources.

Chapitre 27.
Configuration de l'imprimante

L'**Outil de configuration de l'imprimante** permet aux utilisateurs de configurer une imprimante dans Red Hat Linux. Il permet de mettre à jour le fichier de configuration de l'imprimante, d'imprimer des répertoires de spoule ainsi que des filtres.

À partir de la version 9, Red Hat Linux adopte par défaut le système d'impression CUPS. Le système d'impression par défaut des versions précédentes, LPRng, est toujours fourni. Si le système a été mis à niveau à partir d'une version Red Hat Linux précédente, LPRng n'a pas été remplacé par CUPS; lors du processus de mise à niveau et le système continuera donc à utiliser LPRng.

Si le système a été mis à niveau à partir d'une version Red Hat Linux précédente qui utilisait CUPS, les files d'attente configurées ont été conservées lors du processus de mise à niveau et le système continuera donc à utiliser CUPS.

L'**Outil de configuration de l'imprimante** configure aussi bien le système d'impression CUPS que LPRng, selon la configuration choisie pour le système. Lorsque les modifications sont appliquées, l'utilitaire configure le système d'impression actif.

Afin de pouvoir utiliser l'**Outil de configuration de l'imprimante** vous devez avoir les privilèges du super-utilisateur (ou root). Pour lancer l'application, sélectionnez le bouton **Menu principal** (sur le panneau) => **Paramètres du système** => **Impression** ou vous pouvez également tapez la commande `redhat-config-printer`. Cette dernière détermine automatiquement si une version graphique ou texte doit être lancée selon que la commande a été exécutée à partir d'un environnement graphique X Window ou d'une console en mode texte.

Vous pouvez également forcer l'**Outil de configuration de l'imprimante** à démarrer en tant qu'application en mode texte en entrant la commande `redhat-config-printer-tui` à une invite de shell.

Important

Ne modifiez ni le fichier `/etc/printcap` ni les fichiers du répertoire `/etc/cups/`. Chaque fois que le démon d'impression (que ce soit `lpd` ou `cups`) est lancé ou relancé, de nouveaux fichiers de configuration sont créés de façon dynamique. Ces fichiers sont également créés dynamiquement lorsque les modifications sont appliquées avec l'**Outil de configuration de l'imprimante**.

Si vous utilisez LPRng et souhaitez ajouter une imprimante sans l'aide de l'**Outil de configuration de l'imprimante**, modifiez le fichier `/etc/printcap.local`. Les entrées dans `/etc/printcap.local` ne sont pas affichées dans l'**Outil de configuration de l'imprimante** mais sont lues par le démon d'impression. Si vous avez effectué une mise à niveau de votre système à partir d'une version précédente de Red Hat Linux, votre fichier de configuration existant a été converti au nouveau format utilisé par cette application. Chaque fois qu'un nouveau fichier de configuration est créé, l'ancien fichier est enregistré en tant que `/etc/printcap.old`.

Si vous utilisez CUPS, l'**Outil de configuration de l'imprimante** n'applique ni les files d'attente, ni les partages qui n'ont pas été configurés à l'aide de l'**Outil de configuration de l'imprimante**; toutefois, il ne les supprimera pas des fichiers de configuration.

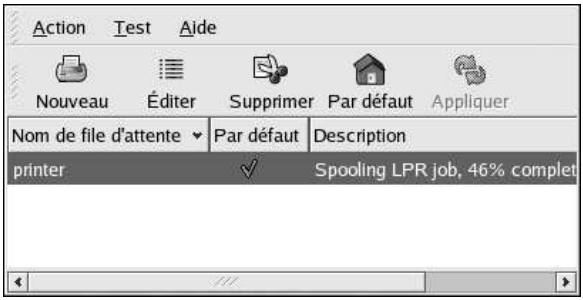

Figure 27-1. Outil de configuration de l'imprimante

Il est possible de configurer les types de files d'attente d'impression suivants:

- **Connectée-localement** — une imprimante directement reliée à votre ordinateur via un port parallèle ou USB.
- **CUPS (IPP) mis en réseau** — une imprimante à laquelle l'accès est possible par un réseau TCP/IP via le protocole d'impression Internet, également connu sous le nom IPP ('Internet Printing Protocol') (par exemple, une imprimante reliée à un autre système Red Hat Linux exécutant CUPS sur le réseau).
- **UNIX (LPD) mis en réseau** — une imprimante reliée à un autre système d'impression UNIX auquel l'accès est possible par un réseau TCP/IP (par exemple, une imprimante reliée à un autre système Red Hat Linux exécutant LPD sur le réseau).
- **Windows (SMB) mis en réseau** — une imprimante reliée à un autre système qui partage une imprimante sur un réseau SMB (par exemple, une imprimante reliée à un ordinateur Microsoft Windows™).
- **Novell (NCP) mis en réseau** — une imprimante reliée à un autre système qui utilise la technologie de réseau Novell NetWare.
- **JetDirect mis en réseau** — une imprimante directement connectée au réseau par HP JetDirect au lieu d'être reliée à un ordinateur.

Important

Si vous ajoutez une nouvelle file d'attente d'impression ou si vous en modifiez une existante, vous devez appliquer les modifications afin qu'elles prennent effet.

Cliquez sur le bouton **Appliquer** afin d'enregistrer tous les changements effectués et de relancer le démon d'impression. Les changements ne sont enregistrés dans le fichier de configuration qu'après le redémarrage du démon d'impression. Vous pouvez également sélectionner **Action => Appliquer**.

27.1. Ajout d'une imprimante locale

Pour ajouter une imprimante locale, comme par exemple une imprimante reliée au port parallèle ou USB de votre ordinateur, cliquez sur le bouton **Nouveau** dans le fenêtre principale de l'**Outil de configuration de l'imprimante**; la fenêtre reproduite dans la Figure 27-2 apparaîtra alors. Cliquez sur **Suivant** pour continuer.

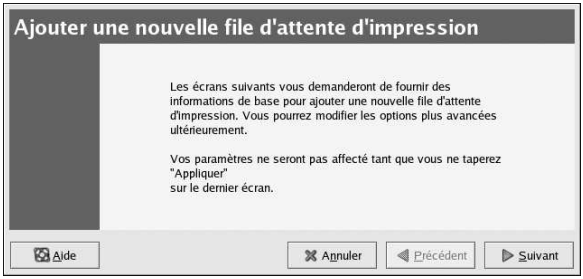

Figure 27-2. Ajout d'une imprimante

Comme l'illustre la fenêtre reproduite dans la Figure 27-3, entrez un nom unique pour l'imprimante dans le champ de texte **Nom**. Le nom de l'imprimante ne doit pas contenir d'espaces et doit commencer par une lettre. Le nom de l'imprimante peut contenir des lettres, des nombres, des tirets (-) et des soulignages (_). Vous pouvez de manière facultative entrez une brève description de l'imprimante, qui elle en revanche, peut contenir des espaces.

Figure 27-3. Choix d'un nom de file d'attente

Après avoir cliqué sur **Suivant**, la fenêtre reproduite dans la Figure 27-4 apparaît. Sélectionnez **Connectée-localement** dans le menu **Sélectionner un type de file d'attente** et choisissez le périphérique. Ce dernier est généralement `/dev/lp0` pour une imprimante parallèle ou `/dev/usb/lp0` pour de imprimante USB. Si aucun périphérique n'apparaît dans la liste, cliquez sur **Reparcourir les périphériques** pour effectuer une nouvelle recherche ou cliquez sur **Personnaliser le périphérique** pour le spécifier manuellement. Cliquez ensuite sur **Suivant** pour continuer.

Figure 27-4. Ajout d'une imprimante locale

L'étape suivante consiste à sélectionner le type d'imprimante. Passez à la Section 27.7 pour continuer.

27.2. Ajout d'une imprimante IPP

Une imprimante IPP est une imprimante reliée à un autre système Linux sur le même réseau exécutant CUPS ou une imprimante configurée sur un autre système d'exploitation pour utiliser IPP. Par défaut, l'**Outil de configuration de l'imprimante** parcours le réseau à la recherche de toute imprimante IPP partagée. (Il est possible de changer cette option en sélectionnant **Action => Partage** dans le menu déroulant.) Toute imprimante IPP réseau apparaît dans la fenêtre principale en tant que file d'attente parcourue.

Si vous disposez d'un pare-feu configuré sur le serveur d'impression, il doit être à même d'envoyer et de recevoir des connexions sur le port UDP entrant, 631. Si vous disposez d'un pare-feu configuré sur le client (l'ordinateur envoyant la requête d'impression), il doit être autorisé à envoyer et accepter des connexions sur le port 631.

Même si vous désactivez la fonction de navigation automatique, il est toujours possible d'ajouter une imprimante IPP réseau en cliquant sur le bouton **Nouveau** dans la fenêtre principale de l'**Outil de configuration de l'imprimante** afin d'obtenir la fenêtre reproduite dans la Figure 27-2. Cliquez sur **Suivant** pour continuer.

Comme l'illustre la fenêtre reproduite dans la Figure 27-3, entrez un nom unique pour l'imprimante dans le champ de texte **Nom**. Le nom de l'imprimante ne doit pas contenir d'espaces et doit commencer par une lettre. Le nom de l'imprimante peut contenir des lettres, des nombres, des tirets (-) et des soulignages (_). Vous pouvez de manière facultative entrez une brève description de l'imprimante, qui elle en revanche, peut contenir des espaces.

Après avoir cliqué sur **Suivant**, la fenêtre reproduite dans la Figure 27-5 apparaît. Sélectionnez **CUPS (IPP) réseau** dans le menu **Sélectionner un type de file d'attente**.

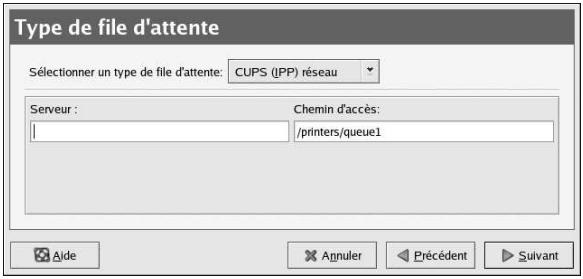

Figure 27-5. Ajout d'une imprimante IPP

Des champs de texte pour les options suivantes apparaissent:

- **Serveur** — Le nom d'hôte ou l'adresse IP de l'ordinateur distant auquel une imprimante est reliée.
- **Chemin d'accès** — Le chemin d'accès à la file d'attente d'impression sur l'ordinateur distant.

Cliquez sur **Suivant** pour continuer.

L'étape suivante consiste à sélectionner le type d'imprimante. Passez à la Section 27.7 pour continuer.

Important

Le serveur d'impression IPP réseau doit autoriser les connexions à partir du système local. Reportez-vous à la Section 27.13 pour de plus amples informations.

27.3. Ajout d'une imprimante UNIX (LPD) distante

Pour ajouter une imprimante UNIX distante, comme par exemple une imprimante reliée à un autre système Linux sur le même réseau, cliquez sur le bouton **Nouveau** dans la fenêtre principale de l'**Outil de configuration de l'imprimante**. La fenêtre reproduite dans la Figure 27-2 apparaîtra alors. Cliquez sur **Suivant** pour continuer.

Comme l'illustre la fenêtre reproduite dans la Figure 27-3, entrez un nom unique pour l'imprimante dans le champ de texte **Nom**. Le nom de l'imprimante ne doit pas contenir d'espaces et doit commencer par une lettre. Le nom de l'imprimante peut contenir des lettres, des nombres, des tirets (-) et des soulignages (_). Vous pouvez de manière facultative entrez une brève description de l'imprimante, qui elle en revanche, peut contenir des espaces.

Sélectionnez **UNIX (LPD) réseau** dans le menu **Sélectionner un type de file d'attente** puis cliquez sur **Suivant**.

Figure 27-6. Ajout d'une imprimante LPD distante

Des champs de texte pour les options suivantes apparaissent:

- **Serveur** — Le nom d'hôte ou l'adresse IP de l'ordinateur distant auquel l'imprimante est reliée.
- **File d'attente** — La file d'attente d'imprimante distante. La file d'attente d'imprimante par défaut est généralement `lp`.

Cliquez sur **Suivant** pour continuer.

L'étape suivante consiste à sélectionner le type d'imprimante. Passez à la Section 27.7 pour continuer.

Important

Le serveur d'impression distant doit accepter des travaux d'impressions du système local. Reportez-vous à la Section 27.13.1 pour obtenir de plus amples informations.

27.4. Ajout d'une imprimante Samba (SMB)

Pour ajouter une imprimante à laquelle on accède à l'aide du protocole SMB (comme une imprimante reliée à un système Microsoft Windows), cliquez sur le bouton **Nouveau** dans la fenêtre principale de l'**Outil de configuration de l'imprimante**. La fenêtre reproduite dans la Figure 27-2 apparaîtra alors. Cliquez sur **Suivant** pour continuer.

Comme l'illustre la fenêtre reproduite dans la Figure 27-3, entrez un nom unique pour l'imprimante dans le champ de texte **Nom**. Le nom de l'imprimante ne doit pas contenir d'espaces et doit commencer par une lettre. Le nom de l'imprimante peut contenir des lettres, des nombres, des tirets (-) et des soulignages (_). Vous pouvez de manière facultative entrez une brève description de l'imprimante, qui elle en revanche, peut contenir des espaces.

Sélectionnez **Windows (SMB) réseau** dans le menu **Sélectionner un type de file d'attente** puis cliquez sur **Suivant**. Si l'imprimante est reliée à un système Microsoft Windows, choisissez ce type de file d'attente.

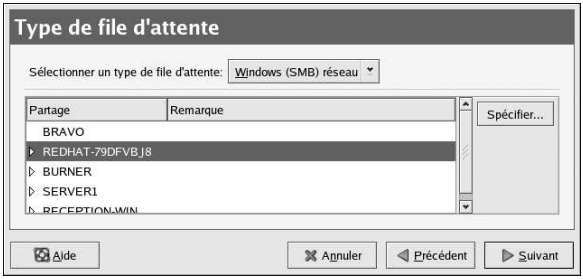

Figure 27-7. Ajout d'une imprimante SMB

Comme le montre la Figure 27-7, les partages SMB sont détectés automatiquement et listés. Cliquez sur la flèche à côté de chaque nom de partage pour obtenir une liste plus détaillée. Dans cette liste, choisissez une imprimante.

Si l'imprimante que vous souhaitez partagée n'apparaît pas dans la liste, cliquez sur le bouton **Spécifier** situé à droite. Les champs de texte relatifs aux options suivantes apparaissent alors:

- **Groupe de travail** — Le nom du groupe de travail associé à l'imprimante partagée.
- **Serveur** — Le nom du serveur partageant l'imprimante.
- **Partage** — Le nom de l'imprimante partagée au moyen de laquelle vous voulez imprimer. Ce nom doit être le même que celui défini comme l'imprimante Samba sur l'ordinateur Windows distant.
- **Nom d'utilisateur** — Le nom d'utilisateur sous lequel vous devez vous connecter pour accéder à l'imprimante. Cet utilisateur doit exister sur le système Windows et doit avoir l'autorisation d'accéder à l'imprimante. Le nom d'utilisateur par défaut est généralement **`invité`** pour les serveurs Windows, ou **`personne`** pour les serveurs Samba.
- **Mot de passe** — Le mot de passe (si nécessaire) de l'utilisateur spécifié dans le champ **Nom d'utilisateur**.

Cliquez sur le bouton **Suivant** pour continuer. L'**Outil de configuration de l'imprimante** essaiera alors de se connecter à l'imprimante partagée. Si cette dernière nécessite un nom d'utilisateur et un mot de passe, une fenêtre de dialogue apparaîtra pour vous inviter à saisir un nom d'utilisateur et un mot de passe valides. Dans le cas où un mauvais nom de partage aurait été spécifié, vous pourrez le modifier ici également. Si le nom d'un groupe de travail est nécessaire pour la connexion au partage, il peut être spécifié dans cette boîte de dialogue. La fenêtre en question est la même que celle apparaissant lorsque vous cliquez sur le bouton **Spécifier**.

L'étape suivante consiste à sélectionner le type d'imprimante. Passez à la Section 27.7 pour continuer.

Avertissement

Si vous avez besoin d'un nom d'utilisateur ou d'un mot de passe, ils sont conservés dans un format non-crypté dans des fichiers lisibles seulement par le super-utilisateur (ou root) et lpd. Ainsi, quiconque ayant les privilèges de super-utilisateur peut obtenir des informations sur le nom d'utilisateur ou le mot de passe. Afin d'éviter cette situation, il est vivement recommandé que le nom d'utilisateur et le mot de passe nécessaires pour accéder à l'imprimante soient différents de ceux utilisés pour le compte utilisateur sur un système Red Hat Linux local. Dans de telles condtions (nom d'utilisateur et mot de passe différents pour l'imprimante et le système), le seul compromis de sécurité possible serait l'utilisation non-autorisé de l'imprimante. S'il y a des partages de fichiers à partir du serveur, il est là encore fortement conseiller d'utiliser un mot de passe différent de celui utilisé pour la file d'attente d'impression.

27.5. Ajout d'une imprimante NetWare de Novell (NCP)

Pour ajouter une imprimante Novell NetWare (NCP), cliquez sur le bouton **Nouveau** dans la fenêtre principale de l'**Outil de configuration de l'imprimante**. La fenêtre reproduite dans Figure 27-1 apparaîtra alors. Cliquez **Suivant** pour continuer.

Comme l'illustre la fenêtre reproduite dans la Figure 27-3, entrez un nom unique pour l'imprimante dans le champ de texte **Nom**. Le nom de l'imprimante ne doit pas contenir d'espaces et doit commencer par une lettre. Le nom de l'imprimante peut contenir des lettres, des nombres, des tirets (-) et des soulignages (_). Vous pouvez de manière facultative entrez une brève description de l'imprimante, qui elle en revanche, peut contenir des espaces.

Sélectionnez **Novell (NCP) réseau** dans le menu **Sélectionnez un type defile d'attente**.

Figure 27-8. Ajout d'une imprimante NCP

Des champs de texte pour les options suivantes apparaissent:

- **Serveur** — Le nom d'hôte ou l'adresse IP du système NCP auquel l'imprimante est reliée.
- **File d'attente** — La file d'attente distante pour l'imprimante sur le système NCP.
- **Utilisateur** — Le nom d'utilisateur sous lequel vous devez vous connecter pour accéder à l'imprimante.
- **Mot de passe** — Le mot de passe pour l'utilisateur spécifié dans le champ **Utilisateur** ci-dessus.

L'étape suivante consiste à sélectionner le type d'imprimante. Passez à la Section 27.7 pour continuer.

Avertissement

Si vous avez besoin d'un nom d'utilisateur ou d'un mot de passe, ils sont conservés dans un format non-crypté dans des fichiers lisibles seulement par le super-utilisateur (ou root) et lpd. Ainsi, quiconque ayant les privilèges de super-utilisateur peut obtenir des informations sur le nom d'utilisateur ou le mot de passe. Afin d'éviter cette situation, il est vivement recommandé que le nom d'utilisateur et le mot de passe nécessaires pour accéder à l'imprimante soient différents de ceux utilisés pour le compte utilisateur sur un système Red Hat Linux local. Dans de telles condtions (nom d'utilisateur et mot de passe différents pour l'imprimante et le système), le seul compromis de sécurité possible serait l'utilisation non-autorisé de l'imprimante. S'il y a des partages de fichiers à partir du serveur, il est là encore fortement conseiller d'utiliser un mot de passe différent de celui utilisé pour la file d'attente d'impression.

27.6. Ajout d'une imprimante JetDirect

Pour ajouter une imprimante JetDirect, cliquez sur le bouton **Nouveau** dans la fenêtre principale de l'**Outil de configuration de l'imprimante**. La fenêtre reproduite dans la Figure 27-1 apparaîtra alors. Cliquez sur **Suivant** pour continuer.

Comme l'illustre la fenêtre reproduite dans la Figure 27-3, entrez un nom unique pour l'imprimante dans le champ de texte **Nom**. Le nom de l'imprimante ne doit pas contenir d'espaces et doit commencer par une lettre. Le nom de l'imprimante peut contenir des lettres, des nombres, des tirets (-) et des soulignages (_). Vous pouvez de manière facultative entrez une brève description de l'imprimante, qui elle en revanche, peut contenir des espaces.

Sélectionnez **JetDirect réseau** dans le menu **Sélectionner un type de file d'attente** et cliquez sur **Suivant**.

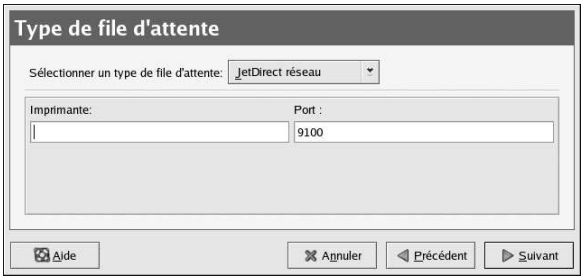

Figure 27-9. Ajout d'une imprimante JetDirect

Les champs de texte pour les options suivantes apparaissent:

- **Imprimante** — Le nom d'hôte ou l'adresse IP de l'imprimante JetDirect.
- **Port** — Le port de l'imprimante JetDirect qui en attente de travaux d'impression. Le port par défaut est 9100.

L'étape suivante consiste à sélectionner le type d'imprimante. Passez à la Section 27.7 pour continuer.

27.7. Sélection d'un modèle d'imprimante et fin du processus

Après avoir sélectionné le type de file d'attente de l'imprimante, l'étape suivante consiste à sélectionner le modèle de cette imprimante.

Une fenêtre semblable à celle reproduite dans la Figure 27-10 apparaît. Si le modèle n'a pas été détecté automatiquement, sélectionnez-le dans la liste fournie. Les imprimantes sont réparties par fabricants. Choisissez le nom du fabricant de votre imprimante dans le menu déroulant. Les modèles d'imprimantes sont mis à jour chaque fois qu'un nouveau fabricant est sélectionné. Choisissez le modèle d'imprimante dans la liste.

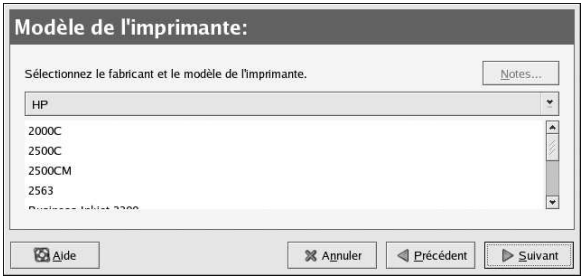

Figure 27-10. Sélection d'un modèle d'imprimante

Le pilote d'impression recommandé est choisi en fonction du modèle d'imprimante retenu. Le pilote d'impression traite les données que vous souhaitez imprimer dans un format que l'imprimante comprend. Étant donné qu'une imprimante locale est reliée directement à votre ordinateur, vous avez besoin d'un pilote d'impression pour traiter les données envoyées à l'imprimante.

Si vous configurez une imprimante distante (IPP, LPD, SMB, or NCP), le serveur d'impression distant dispose généralement de son propre pilote d'impression. Si vous sélectionnez un pilote d'impression supplémentaire sur votre ordinateur local, les données seront filtrées plusieurs fois, et converties dans un format non-reconnu par l'imprimante.

Afin de vous assurer que les données ne seront pas filtrées plusieurs fois, essayez tout d'abord de sélectionner **Générique** pour le fabricant et **File d'attente d'impression de base** ou **Imprimante Postscript** pour le modèle de l'imprimante. Après avoir validé les modifications, imprimez une page test pour vérifier la nouvelle configuration. Si le test échoue, il est possible qu'aucun pilote d'impression ne soit configuré pour le serveur d'impression distant. Essayez de sélectionner un pilote d'impression en fonction du fabricant et du modèle de l'imprimante distante, de valider les modifications et d'imprimer une page test.

Astuce

Après avoir ajouté une imprimante, il est possible de sélectionner un pilote d'impression différent. Pour ce faire, lancez l'**Outil de configuration de l'imprimante**, sélectionnez l'imprimante dans la liste, cliquez sur **Éditer** puis sur l'onglet **Pilote**, sélectionnez enfin un autre pilote et validez les modifications.

27.7.1. Confirmation de la configuration de l'imprimante

La dernière étape consiste à confirmer votre configuration d'imprimante. Cliquez sur **Appliquer** pour ajouter la file d'impression si les paramètres sont corrects. Cliquez sur **Précédent** pour modifier la configuration de l'imprimante.

Cliquez sur le bouton **Appliquer** dans la fenêtre principale pour enregistrer vos modifications et redémarrer le démon d'impression. Après avoir appliqué les modifications, imprimez une page test pour vérifier que la configuration est bien correcte. Reportez-vous à la Section 27.8 pour obtenir de plus amples informations sur le sujet.

Si vous avez besoin d'imprimer des caractères dépassant le jeu ASCII classique (y compris ceux qui sont utilisés dans des langues comme le japonais), vous devez réviser vos options de pilotes et sélectionner **Préparer Postscript**. Reportez-vous à la Section 27.9 pour plus de détails. Vous pouvez également configurer des options comme la taille du papier si vous éditez la file d'impression après l'avoir ajoutée.

27.8. Impression d'une page test

Une fois la configuration de l'imprimante terminée, il est recommandé d'imprimer une page test afin de vous assurer du bon fonctionnement de l'imprimante. Pour ce faire, sélectionnez dans la liste des imprimantes celle que vous souhaitez tester, puis choisissez la page test appropriée dans le menu déroulant **Test**.

Si vous avez changé le pilote d'impression ou modifié les options du pilote, nous vous recommandons d'imprimer une page test pour vérifier le bon fonctionnement de la nouvelle configuration.

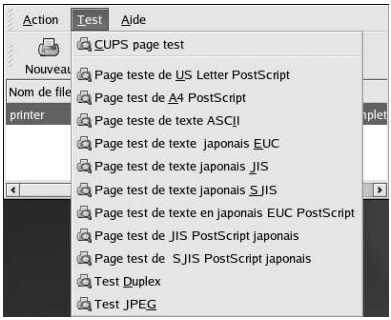

Figure 27-11. Options de la page test

27.9. Modification des imprimantes existantes

Pour supprimer une imprimante existante, sélectionnez l'imprimante et cliquez sur le bouton **Supprimer** dans la barre d'outils. L'imprimante est alors retirée de la liste. Cliquez sur **Appliquer** pour enregistrer les changements et redémarrer le démon d'impression.

Pour définir l'imprimante par défaut, sélectionnez l'imprimante dans la liste et cliquez sur le bouton **Défaut** dans la barre d'outils. L'icône d'imprimante par défaut ✓ apparaît alors dans la colonne **Défaut** de l'imprimante par défaut présente dans la liste.

Après avoir ajouté votre ou vos imprimante(s), vous pouvez modifier les paramètres en sélectionnant l'imprimante dans la liste et en cliquant sur le bouton **Éditer**. La fenêtre à onglets reproduite dans la Figure 27-12 apparaît alors. Elle affiche les valeurs actuelles pour l'imprimante que vous avez sélectionnée. Apportez tous les changements souhaités et cliquez sur **OK**. Cliquez ensuite sur **Appliquer** dans la fenêtre principale de l'**Outil de configuration de l'imprimante** pour enregistrer les changements et redémarrer le démon d'impression.

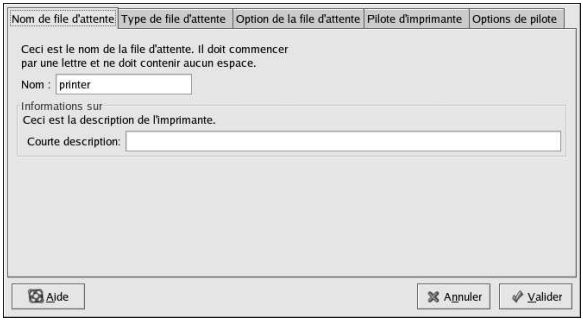

Figure 27-12. Modification d'une imprimante

27.9.1. Nom de la file d'attente

Si vous décidez de renommer une imprimante ou de changer sa courte description, modifiez la valeur dans l'onglet **Nom de la file d'attente**. Cliquez sur **OK** pour retourner à la fenêtre principale. Le nouveau nom de l'imprimante devrait alors apparaître dans la liste des imprimantes. Cliquez sur **Appliquer** pour enregistrer la modification et redémarrer le démon d'impression.

27.9.2. Type de file d'attente

L'onglet **Type de file d'attente** montre le type de file d'attente que vous avez sélectionné lorsque vous avez ajouté l'imprimante ainsi que ses paramètres. Il est possible de changer le type de file d'attente ou simplement les paramètres de l'imprimante. Après avoir effectué les modifications, cliquez sur **OK** pour retourner à la fenêtre principale. Cliquez sur **Appliquer** pour enregistrer la modification et redémarrer le démon d'impression.

Selon le type de file d'attente choisi, différentes options s'afficheront. Consultez la section appropriée traitant de l'ajout d'une imprimante afin d'obtenir une description des options.

27.9.3. Pilote d'imprimante

L'onglet **Pilote d'imprimante** montre le pilote d'imprimante actuellement utilisé. Si vous le changez, cliquez sur **OK** pour retourner à la fenêtre principale. Cliquez ensuite sur **Appliquer** pour enregistrer les changements et redémarrer le démon d'impression.

27.9.4. Options de pilote

L'onglet **Options de pilote** affiche les options avancées de l'imprimante. Celles-ci varient selon le pilote. Parmi les options courantes figurent:

- Sélectionnez **Envoyer saut de page (FF)** (de l'anglais 'Form-Feed') si la dernière page de votre travail d'impression n'est pas éjectée de l'imprimante (par exemple si la lumière d'alimentation clignote). Si cela ne fonctionne pas, essayez de sélectionner **Envoyer Fin-de-transmission (EOT)** (de l'anglais 'End Of Transmission'). Certaines imprimantes nécessitent à la fois **Envoyer saut de page (FF)** et **Envoyer Fin-de-transmission (EOT)** pour éjecter la dernière page. Cette option n'est disponible qu'avec le système d'impression LPRng.

- L'option **Envoyer Fin-de-transmission (EOT)** devrait être utilisée lorsque l'envoi d'un saut de page (FF) ne fonctionne pas. Reportez-vous à **Envoyer saut de page (FF)** ci-dessus. Cette option n'est disponible qu'avec un système d'impression LPRng.
- L'option **Supposer que les données inconnues font partie d'un texte** devrait être sélectionnée si votre pilote d'imprimante ne reconnaît pas certaines des données qui lui sont envoyées. Ne sélectionnez cette option que si vous rencontrez des problèmes d'impression. Lorsque cette option est sélectionnée, le pilote d'imprimante suppose que toute donnée non-reconnue est du texte et il essaie donc de l'imprimer en tant que tel. Si vous sélectionnez cette option en même temps que l'option **Convertir le texte en Postscript**, le pilote d'imprimante suppose que les données inconnues sont du texte et les convertit en PostScript. Cette option n'est disponible qu'avec un système d'impression LPRng.
- L'option **Préparer Postscript** devrait être sélectionnée si vous imprimez des caractères dépassant le jeu ASCII de base et que leur sortie n'est pas correcte (comme pour les caractères japonais). Cette option va retraduire les polices PostScript non-standard afin qu'elles puissent être correctement imprimées.

  Si votre imprimante ne prend pas en charge les polices que vous tentez d'imprimer, essayez de sélectionner cette option. Par exemple vous pouvez la choisir lorsque vous imprimez des polices japonaises sur une imprimante non-japonaise.

  Un temps supplémentaire est nécessaire pour accomplir cette action. Ne la choisissez que si vous rencontrez des problèmes pour imprimer correctement les polices.

  Sélectionnez également cette option si votre imprimante ne peut pas traiter PostScript niveau 3. Cette option permet de le convertir en PostScript niveau 1.
- L'option **Pré-filtrage GhostScript** — permet de sélectionner **Pas de pré-filtrage**, **Convertir en PS niveau 1**, ou **Convertir en PS niveau 2** dans le cas où l'imprimante rencontrerait des problèmes lors du traitement de certains niveaux de PostScript. Cette option est seulement disponible si le pilote PostScript est utilisé avec le système d'impression CUPS.
- L'option **Convertir le texte en Postscript** est sélectionnée par défaut. Si votre imprimante peut imprimer du texte en clair, essayez de dé-sélectionner cette option afin de réduire le temps d'impression. Cette option n'est pas disponible avec le système d'impression CUPS car le texte est toujours converti en PostScript.
- L'option **Format de la page** vous permet de sélectionner le format papier pour votre imprimante, comme par exemple A4, A3, US légal et US lettre.
- L'option **Filtre effectif de locale** est configurée par défaut sur **C**. Si vous imprimez des caractères japonais, sélectionnez **ja_JP**. Sinon, acceptez la valeur **C** par défaut.
- L'option **Source de support** adopte par défaut la valeur **Valeur par défaut de l'imprimante**. Modifiez cette option pour utiliser du papier d'un endroit différent.

Si vous modifiez les options de pilote, cliquez sur **OK** pour retourner à la fenêtre principale. Cliquez sur **Appliquer** pour enregistrer les changements puis redémarrer le démon d'impression.

27.10. Enregistrement du fichier de configuration

Quand vous enregistrez votre configuration d'imprimante à l'aide de l'**Outil de configuration de l'imprimante**, l'application crée son propre fichier de configuration, qui est utilisé pour créer le répertoire `/etc/cups` (ou le fichier `/etc/printcap` que `lpd` lit). Vous pouvez utiliser les options de ligne de commande afin d'enregistrer ou de restaurer le fichier de l'**Outil de configuration de l'imprimante**. Si le répertoire `/etc/cups` ou le fichier `/etc/printcap` est enregistré ou restauré aux mêmes endroits, la configuration de l'imprimante ne sera pas restaurée car chaque fois que le démon d'imprimante est redémarré, il crée un nouveau fichier `/etc/printcap` à partir du fichier de

configuration spécial de l'**Outil de configuration de l'imprimante**. Lors de la création d'une sauvegarde des fichiers de configuration du système, utilisez la méthode suivante pour enregistrer vos fichiers de configuration de l'imprimante. Si le système utilise LPRng et que des paramètres personnalisés ont été ajoutés dans le fichier `/etc/printcap.local`, intégrez-les également dans votre système de sauvegarde.

Pour enregistrer votre configuration d'imprimante, tapez cette commande en étant connecté en tant que super-utilisateur (ou root):

```
/usr/sbin/redhat-config-printer-tui --Xexport > settings.xml
```

Votre configuration est enregistrée dans le fichier `settings.xml`.

Si ce fichier est enregistré, il peut être utilisé pour restaurer les paramètres de l'imprimante. Ceci peut être utile si votre configuration d'imprimante est supprimée, si vous réinstallez Red Hat Linux ou si vous voulez utiliser la même configuration d'imprimante sur plusieurs systèmes. Le fichier devrait être enregistré sur un système différent avant de procéder à l'installation. Pour restaurer la configuration, tapez cette commande en étant connecté en tant que super-utilisateur:

```
/usr/sbin/redhat-config-printer-tui --Ximport < settings.xml
```

Si vous avez déjà un fichier de configuration (vous avez déjà configuré une ou plusieurs imprimantes sur le système) et que vous essayez d'importer un autre fichier de configuration, le fichier existant est écrasé. Si vous voulez conserver vos informations existantes et ajouter la configuration dans le fichier enregistré, vous pouvez fusionner les deux fichiers à l'aide de la commande suivante (en tant que super-utilisateur):

```
/usr/sbin/redhat-config-printer-tui --Ximport --merge < settings.xml
```

Votre liste d'imprimantes comprend alors les imprimantes que vous avez configurées sur le système ainsi que celles que vous aurez importées du fichier de configuration enregistré. Si le fichier de configuration importé possède une file d'attente d'impression ayant le même nom qu'une file déjà présente sur le système, la file du fichier importé va écraser l'imprimante existante.

Après l'importation du fichier de configuration (avec ou sans la commande `merge`), vous devez redémarrer le démon d'impression. Si vous utilisez CUPS, exécutez la commande:

```
/sbin/service cups restart
```

Si vous utilisez LPRng, exécutez la commande:

```
/sbin/service lpd restart
```

27.11. Configuration en ligne de commande

Si X Window n'est pas installé et que vous ne souhaitez pas utiliser une version en mode texte, vous pouvez ajouter une imprimante par le biais de la ligne de commande. Cette méthode est utile si vous souhaitez ajouter une imprimante à partir d'un script ou dans la section %post d'une installation kickstart.

27.11.1. Ajout d'une imprimante locale

Pour ajouter une imprimante:

```
redhat-config-printer-tui --Xadd-local options
```

Options:

--device=*noeud*

(Nécessaire) Le noeud de périphérique à utiliser. Par exemple, `/dev/lp0`.

--make=*marque*

(Nécessaire) La chaîne IEEE 1284 MANUFACTURER ou le nom du fabricant de l'imprimante listé dans la base de données foomatic, si la chaîne du fabricant n'est pas disponible.

--model=*modèle*

(Nécessaire) La chaîne IEEE 1284 MODEL ou le modèle de l'imprimante listé dans la base de données foomatic, si la chaîne du modèle n'est pas disponible.

--name=*nom*

(Facultatif) Le nom à donner à la nouvelle file d'attente. Si aucun nom n'est donné, un nom basé sur le noeud de périphérique (comme « lp0 ») sera utilisé.

--as-default

(Facultatif) Configurer ceci comme file par défaut.

Si vous utilisez CUPS comme système d'impression (le choix par défaut), après avoir ajoutée l'imprimante, utilisez la commande suivante pour démarrer/redémarrer le démon correspondant:

```
service cups restart
```

Si vous utilisez LPRng comme système d'impression, après avoir ajoutée l'imprimante, utilisez la commande suivante pour démarrer/redémarrer le démon correspondant:

```
service lpd restart
```

27.11.2. Suppression d'une imprimante locale

Une file d'attente d'impression peut également être supprimée par le biais de la ligne de commande.

En étant connecté en tant que super-utilisateur (ou root), tapez la commande suivante pour supprimer une file d'attente d'impression:

```
redhat-config-printer-tui --Xremove-local options
```

Options:

--device=*noeud*

(Nécessaire) Le noeud de périphérique utilisé, comme par exemple, `/dev/lp0`.

--make=*marque*

(Nécessaire) La chaîne IEEE 1284 MANUFACTURER ou (si aucune n'est disponible) le nom du fabricant de l'imprimante listé dans la base de données foomatic.

--model=*modèle*

(Nécessaire) La chaîne IEEE 1284 MODEL ou (si aucune n'est disponible) le modèle de l'imprimante listé dans la base de données foomatic.

Si vous utilisez CUPS comme système d'impression (le choix par défaut), après avoir supprimée l'imprimante de la configuration de l'utilitaire **Outil de configuration de l'imprimante**, redémarrez le démon de l'imprimante afin que les changements prennent effet:

```
service cups restart
```

Si vous utilisez LPRng comme système d'impression (le choix par défaut), après avoir supprimée l'imprimante de la configuration de l'utilitaire **Outil de configuration de l'imprimante**, redémarrez le démon de l'imprimante afin que les changements prennent effet:

```
service lpd restart
```

Si vous utilisez CUPS, que vous avez supprimé toutes les imprimantes et que vous ne souhaitez plus exécuter le démon de l'imprimante, entrez la commande suivante:

```
service cups stop
```

Si vous utilisez LPRng, que vous avez supprimé toutes les imprimantes et que vous ne souhaitez plus exécuter le démon de l'imprimante, entrez la commande suivante:

```
service lpd stop
```

27.12. Gestion des travaux d'impression

Lorsque vous envoyez un travail d'impression au démon d'impression, comme par exemple l'impression d'un texte depuis **Emacs** ou d'une image depuis **The GIMP**, ce travail est ajouté à la file de spoule d'impression. Cette dernière est une liste des travaux d'impression qui ont été envoyés à l'imprimante et d'informations sur chaque requête d'impression, comme par exemple, l'état de la requête, le nom d'utilisateur de la personne qui l'a émise, le nom d'hôte du système qui l'a envoyée, le numéro du travail, etc.

Si l'environnement de bureau en cours d'exécution est de type graphique, cliquez sur l'icône **Gestionnaire d'imprimante** dans le panneau afin de lancer le **Gestionnaire d'impression GNOME**, comme l'illustre la Figure 27-13.

Figure 27-13. Gestionnaire d'impression GNOME

Il peut également être lancé en sélectionnant le bouton **Menu principal** (sur le panneau) => **Outils du système => Gestionnaire d'impression**.

Pour changer les paramètres de l'imprimante, cliquez sur l'icône de l'imprimante à l'aide du bouton droit de votre souris et sélectionnez **Propriétés**. L'**Outil de configuration de l'imprimante** sera alors lancé.

Cliquez deux fois sur l'imprimante configurée afin d'afficher la file d'attente du spoule d'impression, comme l'illustre la Figure 27-14.

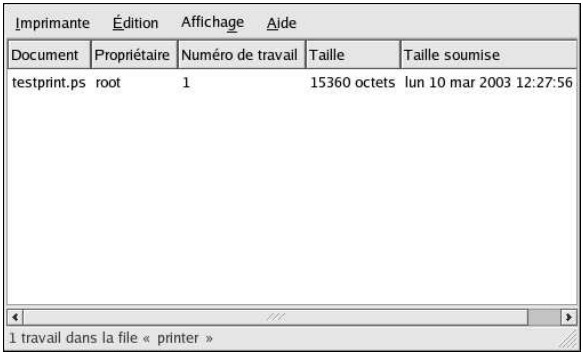

Figure 27-14. Liste des travaux d'impression

Afin d'annuler un travail d'impression spécifique listé dans le **Gestionnaire d'impression GNOME**, choisissez-le dans la liste et sélectionnez **Éditer => Annuler les documents** dans le menu déroulant.

Dans le cas où des travaux d'impression actifs se trouveraient dans le spoule d'impression, une icône de notification pourrait apparaître dans la **Zone de notification du panneau** du bureau, comme l'illustre la Figure 27-15. La détection des travaux d'impression se faisant toutes les cinq secondes, l'icône ne s'affichera peut-être pas pour de courts travaux d'impression.

Figure 27-15. Icône de notification de l'imprimante

Après avoir cliqué sur l'icône de notification de l'imprimante, le **Gestionnaire d'impression GNOME** démarre et affiche une liste des travaux d'impression courants.

L'icône du **Gestionnaire d'impression** se trouve également sur le panneau. Pour imprimer un fichier à partir de **Nautilus**, parcourez l'emplacement du fichier et faites-le glisser jusqu'à ce qu'il soit placé sur l'icône **Gestionnaire d'impression** sur le panneau. La fenêtre reproduite dans la Figure 27-16 apparaît alors. Cliquez sur **OK** pour commencer l'impression du fichier.

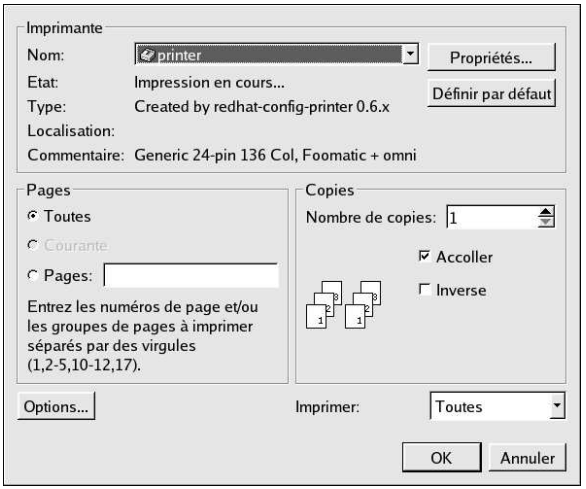

Figure 27-16. Écran de vérification de l'impression

Afin d'afficher la liste des travaux d'impression dans le spoule d'impression à partir d'une invite du shell, tapez la commande `lpq`. Les dernières lignes ressembleront à l'extrait ci-dessous:

```
Rank    Owner/ID            Class  Job Files       Size Time
active user@localhost+902     A    902 sample.txt  2050 01:20:46
```

Exemple 27-1. Exemple de sortie `lpq`

Si vous voulez annuler un travail d'impression, trouvez le numéro de travail de la requête au moyen de la commande `lpq` puis utilisez la commande `lprm` *`numéro de travail`*. Par exemple, `lprm 902` annule le travail d'impression dans l'Exemple 27-1. Vous devez disposer des autorisations adéquates pour annuler un travail d'impression. Vous ne pouvez pas annuler ceux qui ont été lancés par d'autres utilisateurs à moins que vous ne soyez connecté en tant que super-utilisateur (ou root) sur la machine à laquelle l'imprimante est reliée.

Vous pouvez également imprimer un fichier directement depuis l'invite du shell. Par exemple, la commande `lpr sample.txt` imprimera le fichier `sample.txt`. Le filtre d'impression détermine le type de fichier dont il s'agit et le convertit dans un format que l'imprimante pourra interpréter.

27.13. Partage d'une imprimante

La capacité de l'**Outil de configuration de l'imprimante** à partager les options de configuration ne peut être exploitée que si vous utilisez le système d'impression CUPS. Pour configurer un partage en utilisant LPRng, reportez-vous à la Section 27.13.1.

Le *partage* de l'imprimante est le terme utilisé pour faire référence au fait d'autoriser des utilisateurs d'un ordinateur du réseau autre que le votre à envoyer des travaux d'impression à une imprimante configurée pour votre système. Par défaut, les imprimantes configurées avec l'**Outil de configuration de l'imprimante** ne sont pas partagées.

Afin de partager une imprimante configurée, lancez l'**Outil de configuration de l'imprimante** et sélectionnez une imprimante de la liste. Sélectionnez ensuite **Action => Partage** dans le menu déroulant.

Remarque

Si vous ne sélectionnez aucune imprimante et que vous sélectionnez les options **Action** => **Partage** la sortie n'affichera que les options de partage pour tout le système, comme elles apparaissent habituellement sous l'onglet **Général**.

Sous l'onglet **File d'attente**, sélectionnez l'option permettant de mettre la file d'attente à la disposition d'autres utilisateurs.

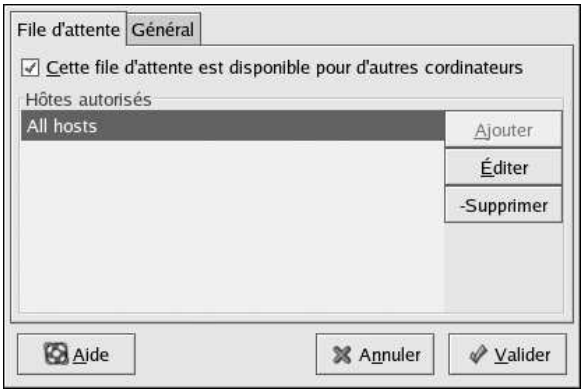

Figure 27-17. Options des files d'attente

Après avoir sélectionné le partage de la file d'attente, par défaut, *tous* les hôtes sont autorisés à envoyer des travaux d'impression à l'imprimante partagée. Le fait d'autoriser tous les systèmes du réseau à imprimer vers la file d'attente peut créer des situations dangereuses, tout particulièrement si le système est directement relié à l'Internet. dans ce cas, il est fortement recommandé de changer cette option en sélectionnant l'entrée **Tous les hôtes** et en cliquant sur le bouton **Éditer** afin de faire apparaître la fenêtre reproduite dans la Figure 27-18.

Si vous avez un pare-feu configuré sur le serveur d'impression, il doit être en mesure d'envoyer et de recevoir des connexions sur le port UDP entrant, 631. Si vous avez un pare-feu configuré sur le client (l'ordinateur envoyant la requête d'impression), il doit être autorisé à envoyer et accepter des connexions sur le port 631.

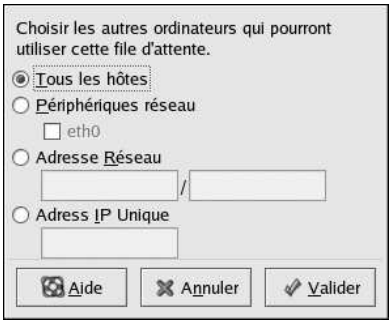

Figure 27-18. Hôtes autorisés

L'onglet **Général** permet de configurer les paramètres de toutes les imprimantes, y compris celles ne s'affichant pas avec l'**Outil de configuration de l'imprimante**. Deux options sont possibles:

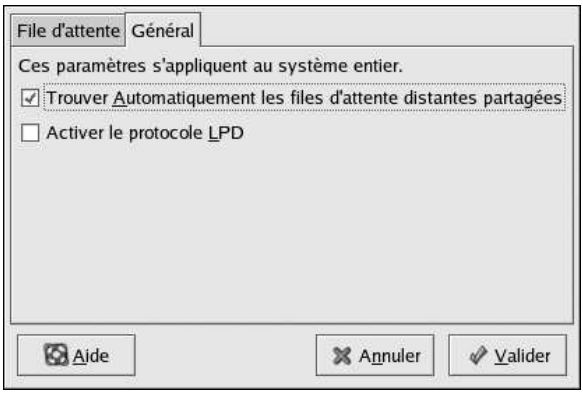

Figure 27-19. Options de partage pour tout le système

- **Trouver automatiquement les files d'attente distantes partagées** — Cette option, électionnée par défaut, active la navigation IPP; ce faisant, lorsque les autres ordinateurs transmettent les files d'attente qu'ils ont, ces dernières sont automatiquement ajoutées à la liste des imprimantes disponibles du système; aucune configuration supplémentaire n'est nécessaire pour une imprimante trouvée par navigation IPP. Cette option ne permet pas le partage automatique des imprimantes configurées sur le système local.
- **Activer le protocole LPD** — Cette option permet à l'imprimante de recevoir des travaux d'impression de la part de clients configurés pour l'utilisation du protocole LPD au moyen du service `cups-lpd`, qui est une service `xinetd`.

Avertissement

Si cette option est activée, tout travail d'impression provenant d'hôtes quelconques est accepté, s'il est reçu d'un client LPD.

27.13.1. Partage d'une imprimante avec LPRng

Si le système d'impression LPRng est en cours d'exécution, le partage doit être configuré manuellement. Afin permettre à des systèmes du réseau d'envoyer des travaux d'impression à une imprimante configurée sur système Red Hat Linux, utilisez les étapes suivantes:

1. Créez le fichier `/etc/accepthost`. Dans ce dernier, ajoutez l'adresse IP ou le nom d'hôte du système pour lequel vous souhaitez autoriser l'accès à l'impression; utilisez une ligne par adresse IP ou nom d'hôte.
2. Décommentez la ligne suivante dans `/etc/lpd.perms`:
   ```
   ACCEPT SERVICE=X REMOTEHOST=</etc/accepthost
   ```
3. Comme ci-dessous, relancez le démon afin que les modifications soient mise en oeuvre:
   ```
   service lpd restart
   ```

27.14. Changement de système d'impression

Pour changer de système d'impression, exécutez l'application **Commutateur du système d'imprimante**. Lancez-la en sélectionnant le bouton **Menu principal** (sur le panneau) => **Paramètres du système** => **Paramètres du système supplémentaires** => **Commutateur du système d'imprimante** ou tout simplement en tapant `redhat-switch-printer` à une invite du shell (par exemple, dans un terminal XTerm ou GNOME).

Le programme détecte automatiquement si le système X Window est en cours d'exécution. Si tel est le cas, le programme démare en mode graphique, comme le montre la Figure 27-20. En revanche, si ce n'est pas le cas, il démarrera en mode texte. Si vous souhaitez le forcer à démarrer en tant qu'une pallication en mode texte, utilisez la commande `redhat-switch-printer-nox`.

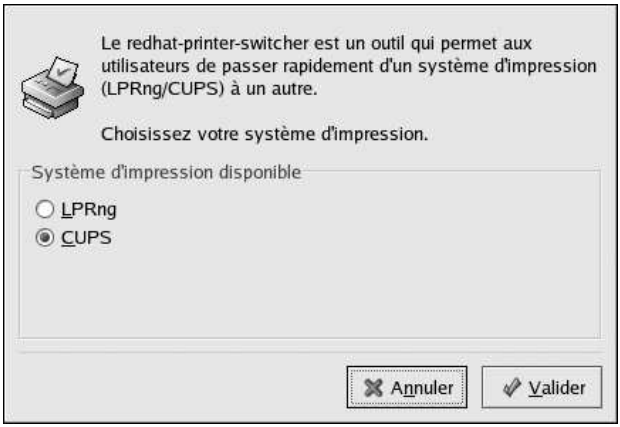

Figure 27-20. Commutateur du système d'imprimante

Sélectionnez l'un des deux systèmes d'impression suivant: **LPRng** ou **CUPS**. Dans Red Hat Linux 9, CUPS est le choix par défaut. Si un seul système d'impression est installé sur votre système, il sera la seule option affichée.

Si vous sélectionnez **OK** pour changer de système d'impression, le démon d'impression sélectionné est activé de manière à se lancer au démarrage et le démon d'impression déselectionné est désactivé

afin de ne pas s'exécuter au démarrage. Le démon d'impression sélectionné est lancé alors que l'autre démon d'impression est arrêté, mettant ainsi les changements en application immédiatement.

27.15. Ressources supplémentaires

Pour en savoir plus sur l'impression avec Red Hat Linux, consultez les ressources mentionnées ci-dessous.

27.15.1. Documentation installée

- `man printcap` — La page de manuel relative au fichier de configuration d'imprimante `/etc/printcap`.
- `map lpr` — La page de manuel relative à la commande `lpr` qui vous permet d'imprimer des fichiers depuis la ligne de commande.
- `man lpd` — La page de manuel relative au démon d'impression du système LPRng.
- `man lprm` — La page de manuel relative à l'utilitaire de ligne de commande afin de supprimer les travaux d'impression de la file de spoule d'impression de système LPRng.
- `man mpage` — La page de manuel relative à l'utilitaire de ligne de commande afin d'imprimer plusieurs pages sur une seule feuille.
- `man cupsd` — La page de manuel relative au démon d'impression du système CUPS.
- `man cupsd.conf` — La page de manuel relative au fichier de configuration du démon d'impression du système CUPS.
- `man classes.conf` — La page de manuel relative au fichier de configuration de classe pour le système d'impression CUPS.

27.15.2. Sites Web utiles

- http://www.linuxprinting.org — *GNU/Linux Printing* contient une grande quantité d'informations sur l'impression sous Linux.
- http://www.cups.org/ — Documentation, Forum Aux Questions (FAQ) et groupes de discussion sur CUPS.

Chapitre 28.

Tâches automatisées

Dans Linux, des tâches peuvent être configurées pour s'exécuter automatiquement pendant une période de temps ou à une date donnée, ou encore lorsque la moyenne de chargement du système se situe en dessous d'un certain niveau. Red Hat Linux est préconfiguré pour l'exécution de certaines tâches système importantes permettant de garder votre système à jour. Par exemple, la banque de données slocate utilisée par la commande `locate` est mise à jour quotidiennement. Un administrateur système peut utiliser des tâches automatisées pour effectuer entre autres des sauvegardes périodiques, contrôler le système, exécuter des scripts personnalisés.

Red Hat Linux est livré avec quatre utilitaires de tâches automatisée: `cron`, `anacron`, `at` et `batch`.

28.1. Cron

Cron est un démon qui peut être utilisé pour programmer l'exécution de tâches récurrentes en fonction d'une combinaison de l'heure, du jour du mois, du mois, du jour de la semaine et de la semaine.

Cron suppose que le système est allumé en permanence. Si le système n'est pas allumé au moment où une tâche doit être exécutée, l'exécution n'a pas lieu. Pour configurer des tâches basées sur des périodes et non sur des dates précises, reportez-vous à la Section 28.2. Pour programmer des tâches uniques, reportez-vous à la Section 28.3.

Afin de pouvoir utiliser le service cron, le paquetage RPM `vixie-cron` doit être installé et le service `crond` doit être en cours d'exécution. Pour savoir si le paquetage est installé, utilisez la commande `rpm -q vixie-cron`. Pour savoir si le service est en cours d'exécution, utilisez la commande `/sbin/service crond status`.

28.1.1. Configuration des tâches Cron

Le fichier de configuration principal de cron, `/etc/crontab`, contient les lignes suivantes:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

Les quatre premières lignes sont des variables servant à configurer l'environnement dans lequel les tâches cron sont exécutées. La valeur de la variable `SHELL` indique au système quel environnement shell utiliser (bash shell dans cet exemple) et la variable `PATH` définit le chemin d'accès utilisé pour l'exécution des commandes. Le résultat des tâches cron est envoyé par courrier électronique au nom d'utilisateur défini par la variable `MAILTO`. Si la variable `MAILTO` est définie comme étant une chaîne vide (`MAILTO=""`), aucun courrier électronique ne sera envoyé. La variable `HOME` peut être utilisée pour définir le répertoire personnel à utiliser pour l'exécution de commandes ou de scripts.

Chacune des lignes du fichier `/etc/crontab` représente une tâche et se présente sous le format:

```
minute   hour   day   month   dayofweek   command
```

- `minute` — tout nombre entier compris entre 0 et 59
- `hour` — tout nombre entier compris entre 0 et 23
- `day` — tout nombre entier compris entre 1 et 31 (si le mois est spécifié, le jour doit être valide)
- `month` — tout nombre entier compris entre 1 et 12 (ou abréviation du nom du mois comme jan, fév, etc.)
- `dayofweek` — tout nombre entier compris entre 0 et 7, 0 ou 7 représentant le dimanche (ou l'abréviation du jour de la semaine: lun, mar, etc.)
- `command` — la commande à exécuter (il peut s'agir d'une commande telle que `ls /proc >> /tmp/proc` ou de la commande d'exécution d'un script personnalisé que vous avez écrit.)

Pour les valeurs ci-dessus, un astérisque (*) peut être utilisé afin d'indiquer toutes les valeurs valides. Par exemple, un astérisque utilisé pour la valeur du mois signifie une exécution mensuelle de la commande, en tenant compte bine sûr des contraintes liées aux autres valeurs.

Un trait d'union (-) placé entre deux nombres entiers indique une fourchette de nombres entiers. Par exemple, **`1-4`** correspond aux nombres entiers 1, 2, 3 et 4.

Une série de valeurs séparées par des virgules (,) correspond à une liste. Par exemple, **`3, 4, 6, 8`** correspond à ces quatre nombres entiers spécifiques.

La barre oblique en avant (/) peut être utilisée pour spécifier des valeurs échelonnées. Pour sauter la valeur d'un nombre entier dans une fourchette, faites suivre la fourchette de **`/`**<***`nombre entier`***>. Par exemple, **`0-59/2`** permet de définir une minute sur deux dans le champ des minutes. Ces valeurs échelonnées peuvent également être utilisées avec un astérisque. Par exemple, la valeur **`*/3`** peut être utilisée dans le champ des mois pour exécuter la tâche tous les trois mois.

Les lignes commençant par le signe dièse (#) correspondent à des commentaires et ne sont pas traitées.

Comme vous pouvez le voir dans le fichier `/etc/crontab`, il utilise le script `run-parts` pour exécuter les scripts des répertoires `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly`, et `/etc/cron.monthly` sur une base respectivement horaire, quotidienne, hebdomadaire ou mensuelle. Les fichiers de ces répertoires doivent être des scripts shell.

Si une tâche cron doit être exécutée sur une base qui n'est ni horaire, ni quotidien, ni hebdomadaire, ni mensuel, elle peut être ajoutée au répertoire `/etc/cron.d`. Tous les fichiers de ce répertoire utilisent la même syntaxe que `/etc/crontab`. Reportez-vous à l'Exemple 28-1 pour obtenir différents exemples.

```
# record the memory usage of the system every monday
# at 3:30AM in the file /tmp/meminfo
30 3 * * mon cat /proc/meminfo >> /tmp/meminfo
# run custom script the first day of every month at 4:10AM
10 4 1 * * /root/scripts/backup.sh
```

Exemple 28-1. Exemples de Crontab

Les utilisateurs autres que le super-utilisateur (root) peuvent configurer des tâches cron à l'aide de l'utilitaire `crontab`. Tous les crontabs définis par l'utilisateur sont stockés dans le répertoire `/var/spool/cron` et exécutés avec les noms des utilisateurs qui les ont créés. Pour créer un crontab en tant qu'utilisateur, connectez-vous sous le nom de cet utilisateur et tapez la commande `crontab -e` pour modifier le crontab de l'utilisateur à l'aide de l'éditeur déterminé par la variable d'environnement the `VISUAL` ou `EDITOR`. Le fichier utilise le même format que `/etc/crontab`. Lorsque les modifications apportées au crontab sont enregistrées, ce dernier est stocké en fonction du nom d'utilisateur et enregistré dans le fichier `/var/spool/cron/`*`nom-utilisateur`*.

Le démon cron vérifie le fichier `/etc/crontab`, le répertoire `/etc/cron.d/` ainsi que le répertoire `/var/spool/cron` toutes les minutes afin de voir si des modifications y ont été apportées. S'il en

trouve, celles-ci sont chargées dans la mémoire. Il n'est par conséquent pas nécessaire de redémarrer le démon si un fichier crontab est modifié.

28.1.2. Contrôle de l'accès à cron

Les fichiers `/etc/cron.allow` e `/etc/cron.deny` sont utilisés pour limiter l'accès à cron. Le format de ces deux fichiers de contrôle d'accès requiert un nom d'utilisateur sur chaque ligne. Les espaces blancs ne sont pas acceptés. Le démon cron (`crond`) n'a pas à être redémarré si les fichiers de contrôle d'accès sont modifiés. Ces derniers sont lus chaque fois qu'un utilisateur essaie d'ajouter ou de supprimer une tâche cron.

L'utilisateur root peut toujours utiliser cron, indépendamment des noms d'utilisateurs répertoriés dans les fichiers de contrôle d'accès.

Si le fichier `cron.allow` existe, seuls les utilisateurs qui y sont répertoriés peuvent utiliser cron et le fichier `cron.deny` n'est pas pris en compte.

En revanche, si le fichier `cron.allow` n'existe pas, les utilisateurs répertoriés dans `cron.deny` ne sont pas autorisés à utiliser cron.

28.1.3. Démarrage et arrêt du service

Pour lancer le service cron, utilisez la commande `/sbin/service crond start`. Pour interrompre le service, utilisez la commande `/sbin/service crond stop`. Nous vous recommandons de lancer le service au démarrage. Reportez-vous au Chapitre 14 pour en savoir plus sur le lancement automatique du service cron lors du démarrage.

28.2. Anacron

Anacron est un planificateur de tâches similaire à cron, sauf qu'il ne requiert pas l'exécution du système en continu. Il peut être utilisé pour l'exécution quotidienne, hebdomadaire et mensuelle de tâches généralement exécutées par cron.

Afin de pouvoir utiliser le service Anacron, le paquetage RPM `anacron` doit être installé et le service `anacron` doit être en cours d'exécution. Pour savoir si le paquetage est installé, utilisez la commande `rpm -q anacron`. Pour savoir si le service est en cours d'exécution, utilisez la commande `/sbin/service anacron status`.

28.2.1. Configuration des tâches Anacron

Les tâches Anacron sont répertoriées dans le fichier de configuration `/etc/anacrontab`. Chaque ligne de ce fichier correspond à une tâche. Elles se présentent sous le format suivant:

```
period   delay   job-identifier  command
```

- `period` — fréquence (en jours) d'exécution de la commande
- `delay` — temps d'attente en minutes
- `job-identifier` — description de la tâche; utilisé dans les messages Anacron et comme nom du fichier de référence temporelle de la tâche; peut contenir tout caractère autre qu'un blanc (à l'exception des barres obliques).
- `command` — commande à exécuter

Pour chaque tâche, Anacron détermine si la tâche a été exécutée au cours de la période spécifiée dans le champ `period` du fichier de configuration. Si ce n'est pas le cas, Anacron exécute la commande spécifiée dans le champ `command` après avoir respecté le délai d'attente spécifié dans le champ `delay`.

Une fois la tâche terminée, Anacron enregistre la date dans un fichier de référence temporelle dans le répertoire `/var/spool/anacron`. Seule la date est utilisée (et pas l'heure). La valeur associée à `job-identifier` est utilisée comme nom de fichier pour le fichier de référence temporelle.

Les variables d'environnement telles que `SHELL` et `PATH` peuvent être définies au début du fichier `/etc/anacrontab` comme pour le fichier de configuration cron.

Le fichier de configuration par défaut ressemble à l'extrait ci-dessous:

```
# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# These entries are useful for a Red Hat Linux system.
1       5       cron.daily              run-parts /etc/cron.daily
7       10      cron.weekly             run-parts /etc/cron.weekly
30      15      cron.monthly            run-parts /etc/cron.monthly
```

Figure 28-1. Fichier de configuration anacrontab par défaut

Comme le montre la Figure 28-1, anacron dans le système Red Hat Linux est configuré pour s'assurer que les tâches cron quotidiennes, hebdomadaires et mensuelles seront bien exécutées.

28.2.2. Démarrage et arrêt du service

Pour lancer le service anacron, utilisez la commande `/sbin/service anacron start`. Pour interrompre le service, utilisez la commande `/sbin/service anacron stop`. Nous vous recommandons de lancer le service au démarrage. Reportez-vous au Chapitre 14 pour de plus amples informations sur le lancement automatique du service anacron au démarrage.

28.3. At et Batch

Tandis que cron et anacron servent à programmer des tâches récurrentes, la commande `at` est utilisée pour programmer une tâche unique à un moment donné. La commande `batch` sert à programmer une tâche qui doit être exécutée une seule fois lorsque la moyenne de chargement du système descend en dessous de 0.8.

Pour utiliser `at` ou `batch` le paquetage RPM `at` doit être installé sur votre système et le service `atd` doit être en cours d'exécution. Pour savoir si le paquetage est installé, utilisez la commande `rpm -q at`. Pour savoir si le service est en cours d'exécution, utilisez la commande `/sbin/service atd status`.

28.3.1. Configuration des tâches At

Pour programmer une tâche qui ne sera exécutée qu'une fois à un moment donnez, entrez la commande `at` *`moment`*, où *`moment`* correspond au moment d'exécution de la commande.

L'argument *`moment`* peut prendre l'une des valeurs suivantes:

- Format HH:MM — Par exemple, 04:00 signifie 4:00 du matin. Si l'heure est déjà passée, le processus sera exécuté le lendemain à la même heure.
- midnight — signifie minuit, soit 12:00AM.
- noon — signifie midi, soit 12:00PM.
- teatime — signifie 16:00 heures ou 4:00PM.
- Format mois jour année — Par exemple, "January 15 2002" signifie le 15ème jour du mois de janvier de l'année 2002. L'année est en option.
- Formats MMJJAA, MM/JJ/AA, ou MM.JJ.AA — Par exemple, 011502 correspond au 15ème jour du mois de janvier de l'année 2002.
- now + temps — le temps est indiqué en minutes, heures, jours ou semaines. Par exemple, now + 5 days indique que la commande sera exécutée à la même heure dans cinq jours.

L'heure doit être spécifiée en premier, suivie de la date en option. Pour plus d'informations sur le format de l'heure, lisez le fichier texte `/usr/share/doc/at-<version>/timespec`.

Après avoir entré la commande `at` avec l'argument de temps, l'invite `at>` s'affiche. Entrez la commande à exécuter, appuyez sur la touche [Entrée] et tapez Ctrl-D. Vous pouvez spécifier plusieurs commandes en entrant chacune d'elles puis en tapant sur la touche [Entrée]. Après avoir tapé toutes les commandes, appuyez sur la touche [Entrée] afin d'afficher une ligne vide, puis tapez Ctrl-D. Un script shell peut également être saisi en appuyant sur la touche [Entrée] après chaque ligne du script et en tapant Ctrl-D sur une ligne vide pour quitter. Si un script est entré, le shell utilisé est celui qui est défini dans l'environnement SHELL de l'utilisateur, le shell de connexion de l'utilisateur ou `/bin/sh` (celui qui est trouvé en premier).

Si l'ensemble de commandes ou de scripts essaie d'afficher des informations dans la sortie standard, ces informations sont envoyées par courrier électronique à l'utilisateur.

Utilisez la commande `atq` pour afficher les tâches en attente. Reportez-vous à la Section 28.3.3 afin d'obtenir davantage d'informations.

L'utilisation de la commande `at` peut être restreinte. Reportez-vous à la Section 28.3.5 pour de plus amples informations.

28.3.2. Configuration des tâches Batch

Pour exécuter une seule fois une tâche spécifique lorsque la moyenne de chargement est inférieure à 0.8, utilisez la commande `batch`.

Une fois la commande `batch` saisie, l'invite `at>` s'affiche. Entrez la commande à exécuter, appuyez sur la touche [Entrée] et tapez Ctrl-D. Vous pouvez spécifier plusieurs commandes en entrant chacune d'elles suivie de [Entrée]. Après avoir tapé toutes les commandes, appuyez sur la touche [Entrée] afin d'afficher une ligne vide, puis tapez Ctrl-D. Un script shell peut également être saisi en appuyant sur la touche [Entrée] après chaque ligne du script et en tapant Ctrl-D sur une ligne vide pour quitter. Si un script est saisi, le shell utilisé est celui défini dans l'environnement SHELL de l'utilisateur, le shell de connexion de l'utilisateur ou `/bin/sh` (celui qui est trouvé en premier). L'ensemble de commandes ou de scripts est exécuté dès que la moyenne de chargement se situe en dessous de 0.8.

Si l'ensemble de commandes ou de scripts essaie d'afficher des informations dans la sortie standard, ces informations sont envoyées par courrier électronique à l'utilisateur.

Utilisez la commande `atq` pour afficher les tâches en attente. Reportez-vous à la Section 28.3.3 afin d'obtenir davantage d'informations.

L'utilisation de la commande `batch` peut être restreinte. Reportez-vous à la Section 28.3.5 pour obtenir des d'informations plus détaillées.

28.3.3. Affichage des tâches en attente

Pour afficher les tâches `at` et `batch` en attente, utilisez la commande `atq`. Elle affiche une liste des tâches en attente, une tâche par ligne. Chaque ligne se présente sous le format suivant: numéro de la tâche, date, heure, classe de la tâche et nom d'utilisateur. Les utilisateurs ne peuvent afficher que leurs propres tâches. Si le super-utilisateur (root) exécute la commande `atq` toutes les tâches de tous les utilisateurs sont affichées.

28.3.4. Options de ligne de commande supplémentaires

Parmi les options de ligne de commande supplémentaires pour `at` et `batch` on trouve:

Option	Description
`-f`	Lit les commandes ou le script shell depuis un fichier au lieu de les spécifier à l'invite.
`-m`	Envoie un courrier électronique à l'utilisateur une fois la tâche accomplie.
`-v`	Affiche l'heure à laquelle la tâche sera exécutée.

Tableau 28-1. Options de ligne de commande `at` et `batch`

28.3.5. Contrôle de l'accès à At et Batch

Les fichiers `/etc/at.allow` et `/etc/at.deny` peuvent servir à limiter l'accès aux commandes `at` et `batch`. Le format de ces deux fichiers de contrôle d'accès requiert un nom d'utilisateur sur chaque ligne. Les espaces blancs n'y sont pas acceptés. Le démon `at` (`atd`) n'a pas à être redémarré si les fichiers de contrôle d'accès sont modifiés. Ces fichiers sont lus chaque fois qu'un utilisateur essaie d'exécuter les commandes `at` ou `batch`.

L'utilisateur root peut toujours exécuter les commandes `at` et `batch` indépendamment des fichiers de contrôle d'accès.

Si le fichier `at.allow` existe, seuls les utilisateurs qui y sont répertoriés peuvent utiliser `at` ou `batch` et le fichier `at.deny` n'est pas pris en considération.

Si le fichier `at.allow` n'existe pas, aucun utilisateur répertorié dans `at.deny` ne sont autorisés à utiliser ni `at` ni `batch`.

28.3.6. Démarrage et arrêt du service

Pour lancer le service `at`, utilisez la commande `/sbin/service atd start`. Pour arrêter le service, utilisez la commande `/sbin/service atd stop`. Nous vous recommandons de lancer le service au démarrage. Reportez-vous au Chapitre 14 pour en savoir plus sur le lancement automatique du service cron lors du démarrage.

28.4. Ressources supplémentaires

Pour en savoir plus sur la configuration de tâches automatisées, reportez-vous aux ressources suivantes.

28.4.1. Documentation installée

- Page de manuel relative à `cron` — offre un aperçu de cron.
- Pages de manuel relatives à `crontab` dans les sections 1 et 5 — La page de manuel dans la section 1 contient un aperçu du fichier `crontab`. La page de manuel de la section 5 contient le format du fichier ainsi que des exemples d'entrées.
- `/usr/share/doc/at-<version>/timespec` contient des informations plus détaillées sur les dates pouvant être spécifiées pour les tâches cron.
- Page de manuel relative à `anacron` — description d'anacron et de ses options de ligne de commande.
- Page de manuel relative à `anacrontab` — un bref aperçu du fichier de configuration anacron.
- `/usr/share/doc/anacron-<version>/README` — décrit Anacron et son utilité.
- Page de manuel relative à `at` — description de `at` et `batch` ainsi que leurs options de ligne de commande.

Chapitre 29.

Fichiers journaux

Les *fichiers journaux* sont des fichiers qui contiennent des messages relatifs au système, y compris au noyau, aux services et aux applications qui s'y rapportent. Les fichiers journaux diffèrent en fonction du type d'information qu'ils contiennent. Il y a par exemple un fichier journal système par défaut, un fichier journal réservé aux messages de sécurité et un fichier journal réservé aux tâches cron.

Les fichiers journaux peuvent s'avérer très utiles si vous essayez de réparer un problème au niveau du système, par exemple si vous essayez de charger un pilote de noyau, ou si vous recherchez des tentatives de connexion non-autorisée au système. Ce chapitre indique où trouver les fichiers journaux, comment les consulter et les éléments à rechercher dans ces derniers.

Certains fichiers journaux sont contrôlés par un démon nommé `syslogd`. Vous pouvez trouver une liste des messages de journaux gérée par `syslogd` dans le fichier de configuration `/etc/syslog.conf`.

29.1. Emplacement des fichiers journaux

La plupart des fichiers journaux sont situés dans le répertoire `/var/log`. Certaines applications telles que `httpd` et `samba` disposent d'un répertoire situé dans `/var/log`, qui contient leurs fichiers journaux.

Vous remarquerez que les fichiers du répertoire contenant les fichiers journaux sont suivis de numéros. Ils sont créés lorsqu'une rotation est opérée sur les fichiers journaux. Cette rotation est effectuée afin que la taille de ces fichiers ne devienne pas trop importante. Le paquetage `logrotate` contient une tâche cron qui effectue automatiquement une rotation des fichiers journaux en fonction du fichier de configuration `/etc/logrotate.conf` ainsi que des fichiers de configuration du répertoire `/etc/logrotate.d`. Par défaut, l'opération de rotation est effectuée toutes les semaines et conserve les fichiers journaux des quatre semaines précédentes.

29.2. Affichage des fichiers journaux

La plupart des fichiers journaux sont en format texte clair. Vous pouvez les visualiser à l'aide de n'importe quel éditeur de texte tel que **Vi** ou **Emacs**. Certains fichiers journaux sont lisibles par tous les utilisateurs du système; vous devez toutefois être connecté en tant que super-utilisateur pour lire la plupart des fichiers journaux.

Pour afficher les fichiers journaux système dans une application interactive en temps réel, utilisez l'**Afficheur de journal**. Pour lancer l'application, cliquez sur le bouton **Menu principal** (sur le panneau) => **Outils de système** => **Journaux système** ou tapez la commande `redhat-logviewer` à l'invite du shell.

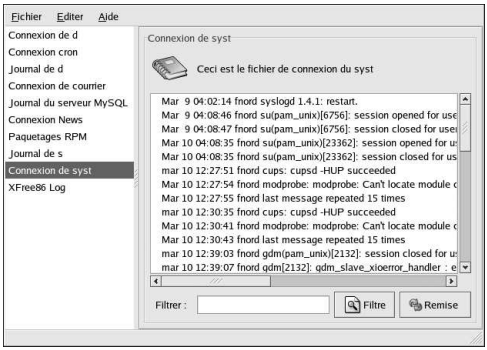

Figure 29-1. Afficheur de journal

L'application n'affiche que les fichiers journaux qui existent; par conséquent, la liste reproduite dans la Figure 29-1 sera peut-être différente de la votre. Pour visualiser la liste complète des fichiers journaux qu'elle peut afficher, reportez-vous au fichier de configuration, `/etc/sysconfig/redhat-logviewer`.

Le fichier journal actuellement affichable est, par défaut, rafraîchi toutes les 30 secondes. Pour modifier le taux de rafraîchissement, sélectionnez **Éditer => Préférences** dans le menu déroulant. La fenêtre reproduite dans la Figure 29-2 apparaîtra alors. Dans l'onglet **Fichiers journaux**, cliquez sur les flèches haut et bas placées à côté du taux de rafraîchissement pour le modifier. Cliquez sur **Fermer** pour revenir à la fenêtre principale. Le taux de rafraîchissement est alors immédiatement modifié. Pour rafraîchir manuellement le fichier affichable, sélectionnez **Fichier => Rafraîchir maintenant** ou pressez [Ctrl]-[R].

Pour filtrer le contenu du fichier journal à la recherche de mots-clés, tapez le mot ou les mots que vous recherchez dans le champ de texte **Filtre pour** et cliquez sur **Filtrer**. Cliquez sur **Réinitialiser** pour réinitialiser le contenu.

Vous pouvez également modifier l'emplacement où l'application recherche les fichiers journaux à partir de l'onglet **Fichiers journaux**. Sélectionnez le fichier journal dans la liste puis cliquez sur le bouton **Changer d'emplacement**. Tapez le nouvel emplacement du fichier journal ou cliquez sur le bouton **Recherche en cours** afin de localiser le fichier à l'aide d'une boîte de dialogue de sélection de fichiers. Cliquez sur **OK** pour retourner aux préférences et sur **Fermer** pour retourner à la fenêtre principale.

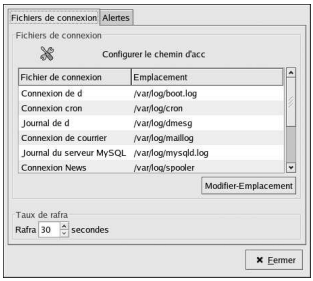

Figure 29-2. Emplacements des fichiers journaux

29.3. Examen des fichiers journaux

L'**Afficheur de journal** peut être configuré pour afficher une icône d'alerte près de la ligne qui contient des mots d'alerte clé. Pour ajouter des mots d'alerte, sélectionnez **Éditer => Préférences** dans le menu déroulant et cliquez sur l'onglet **Alertes**. Cliquez sur le bouton **Ajouter** pour ajouter un mot d'alerte. Pour supprimer un mot d'alerte, sélectionnez-le dans la liste et cliquez sur bouton **Supprimer**.

Figure 29-3. Alertes

Chapitre 30.

Mise à niveau du noyau

Le noyau Red Hat Linux a été construit de façon personnalisée par l'équipe noyau de Red Hat, afin d'assurer son intégrité ainsi que sa compatibilité avec le matériel pris en charge. Avant que Red Hat ne publie un noyau, celui-ci doit subir toute une série de tests d'assurance qualité.

Les noyaux Red Hat Linux sont mis en paquetage au format RPM afin de permettre une mise à niveau et une vérification plus faciles. Par exemple, le paquetage RPM `kernel` distribué par Red Hat, Inc. est installé et une image `initrd` est créée; il n'est pas conséquent pas nécessaire d'utiliser la commande `mkinitrd`après l'installation d'un noyau différent. Dans le cas où GRUB ou LILO est installé, il modifie également le fichier de configuration du chargeur d'amorçage afin d'inclure le nouveau noyau.

Ce chapitre couvre les étapes nécessaires à la mise à niveau du noyau uniquement sur un système x86.

Avertissement

La construction de votre propre noyau personnalisé n'est pas prise en charge par l'équipe d'assistance à l'installation de Red Hat Linux. Pour obtenir de plus amples informations sur la construction d'un noyau personnalisé à partir du code source, reportez-vous à l'Annexe A.

30.1. Noyau 2.4

Red Hat Linux est livré avec un noyau 2.4 personnalisé. Ce dernier propose les fonctions suivantes:

- Le répertoire du noyau source est désormais `/usr/src/linux-2.4/` plutôt que `/usr/src/linux/`.
- Prise en charge du système de fichiers ext3.
- Prise en charge multi-processeurs (SMP).
- Prise en charge USB.
- Prise en charge préliminaire des périphériques IEEE 1394, également appelés FireWire™.

30.2. Préparation en vue de la mise à niveau

Avant de procéder à la mise à niveau, vous devez prendre quelques mesures de précaution. Vous devez tout d'abord vous assurer de bien avoir une disquette de démarrage opérationnelle pour votre système, au cas où un problème surviendrait. En effet, si le chargeur d'amorçage n'est pas correctement configuré pour démarrer le nouveau noyau, vous ne pourrez lancer votre système à moins d'être en possession d'une disquette de démarrage opérationnelle.

Pour créer une disquette d'amorçage, connectez-vous en tant que super-utilisateur (ou root) à une invite du shell et tapez la commande suivante:

```
/sbin/mkbootdisk `uname -r`
```

Astuce

Consultez la page de manuel relative à `mkbootdisk` pour connaître d'autres options.

Redémarrez votre ordinateur avec la disquette de démarrage afin de vous assurer qu'elle fonctionne bien avant de poursuivre.

Vous ne devriez pas avoir à utiliser cette disquette de démarrage, toutefois, rangez-la en lieu sûr, juste au cas où.

Pour déterminer les paquetages installés sur votre système, exécutez la commande suivante à une invite du shell:

```
rpm -qa | grep kernel
```

La sortie résultante contient certains (ou la totalité) des paquetages suivants, en fonction du type d'installation effectuée (les numéros de version et de paquetages pourraient toutefois être différents):

```
kernel-2.4.20-2.47.1
kernel-debug-2.4.20-2.47.1
kernel-source-2.4.20-2.47.1
kernel-doc-2.4.20-2.47.1
kernel-pcmcia-cs-3.1.31-13
kernel-smp-2.4.20-2.47.1
```

À partir de cette sortie, déterminez les paquetages à télécharger pour la mise à niveau du noyau. Pour un système n'utilisant qu'un seul processeur, le seul paquetage `kernel` est nécessaire.

Si votre ordinateur dispose de plusieurs processeurs, le paquetage `kernel-smp`, permettant la prise en charge de processeurs multiple, doit être installé, afin que le système puisse utiliser plus d'un processeur. Il est fortement recommandé d'installer également le paquetage `kernel` au cas où le noyau multiprocesseur ne fonctionnerait pas correctement sur votre système.

Si l'ordinateur dispose de plus de quatre giga-octets de mémoire, le paquetage `kernel-bigmem` doit être installé afin de permettre au système d'utiliser plus de quatre giga-octets de mémoire. Là encore, il est fortement recommandé d'installer le paquetage `kernel` à des fins de débogage. Le paquetage `kernel-bigmem` est destiné uniquement à l'architecture i686.

Si la prise en charge PCMCIA est nécessaire (dans le cas d'un ordinateur portable, par exemple), il faudra installer le paquetage `kernel-pcmcia-cs`.

Le paquetage `kernel-source` n'est pas nécessaire à moins que vous n'envisagiez de recompiler le noyau ou d'effectuer un développement de noyau.

Le paquetage `kernel-doc` contient la documentation relative au développement de noyau et n'est pas requis. Il est néanmoins recommandé si le système est utilisé pour un développement de noyau.

Le paquetage `kernel-util` qui comprend des utilitaires permettant de contrôler le noyau ou le matériel du système, n'est pas requis.

Red Hat construit des noyaux optimisés pour différentes versions x86. Les options sont `athlon` pour les systèmes AMD Athlon™ et AMD Duron™, `i686` pour les systèmes Intel® Pentium® II, Intel® Pentium® III ainsi que Intel® Pentium® 4 et `i586` pour les systèmes Intel® Pentium® et AMD K6™. Si vous ne connaissez pas la version de votre système, utilisez le noyau construit pour la version `i386`; il convient en effet à tous les systèmes de type x86.

La version x86 du paquetage RPM est comprise dans le nom du fichier. Par exemple, `kernel-2.4.20-2.47.1.athlon.rpm` est optimisé pour les systèmes AMD Athlon™ ainsi que AMD Duron™ et `kernel-2.4.20-2.47.1.i686.rpm` est optimisé pour les systèmes Intel® Pentium® II, Intel® Pentium® III ainsi que Intel® Pentium® 4. Une fois que vous avez déterminé les paquetages dont vous avez besoin pour mettre à niveau votre noyau, sélectionnez l'architecture appropriée pour

les paquetages `kernel`, `kernel-smp` et `kernel-bigmem`. Utilisez les versions `i386` des autres paquetages.

30.3. Téléchargement du noyau mis à niveau

Il existe plusieurs façons de déterminer s'il existe une mise à niveau du noyau pour votre système.

- Rendez-vous à l'adresse suivante: http://www.redhat.com/apps/support/errata/, choisissez la version appropriée de Red Hat Linux et consultez les errata s'y rapportant. Les errata relatifs au noyau se trouvent normalement dans la section **Security Advisories**. Dans la liste d'errata, cliquez sur les errata relatifs au noyau afin de parcourir le rapport détaillé s'y rapportant. Dans ce dernier figure une liste de paquetages RPM requis ainsi qu'un lien pour les télécharger depuis le site FTP de Red Hat. Ils peuvent également être téléchargés depuis un site FTP miroir de Red Hat. Une liste de ces sites est fournie à l'adresse http://www.redhat.com/download/mirror.html.
- Utilisez Red Hat Network pour télécharger les paquetages RPM noyau et installer les paquetages. Red Hat Network peut s'occuper du téléchargement du noyau le plus récent, de la mise à niveau du noyau sur le système, de la création d'une image de disque RAM si nécessaire, ainsi que de la configuration du chargeur d'amorçage de façon à ce qu'il démarre le nouveau noyau. Pour plus d'informations, reportez-vous au *Red Hat Network User Reference Guide* (Guide de référence) disponible à l'adresse suivante: http://www.redhat.com/docs/manuals/RHNetwork/.

Si les paquetages RPM ont été téléchargés à partir de la page d'errata de Red Hat Linux ou si Red Hat Network n'a servi qu'à télécharger les paquetages, passez à la Section 30.4. Si Red Hat Network a servi à télécharger et installer le noyau mis à niveau, suivez les instructions contenues dans la Section 30.5 et dans la Section 30.6, mais ne modifiez la configuration du noyau pour qu'il démarre par défaut, car Red Hat Network remplace automatiquement le noyau par défaut par la version la plus récente.

30.4. Exécution de la mise à niveau

Après avoir extrait tous les paquetages nécessaires, il est possible de mettre à niveau le noyau existant. En étant connecté en tant que super-utilisateur, à une invite du shell, changez de répertoire pour vous rendre dans celui contenant les paquetages RPM du noyau puis suivez les étapes suivantes:

Important

Il est fortement recommandé de conserver l'ancien noyau au cas où le nouveau noyau aurait des problèmes de fonctionnement.

Utilisez l'argument `-i` avec la commande `rpm` afin de conserver l'ancien noyau. Si l'option `-U` a été utilisée pour mettre à niveau le paquetage noyau (`kernel`), le noyau actuellement installé sera écrasé (il est possible que la version noyau et la version x86 diffèrent):

```
rpm -ivh kernel-2.4.20-2.47.1.i386.rpm
```

S'il s'agit d'un système multi-processeurs, installez également les paquetages `kernel-smp` (il est possible que la version noyau et la version x86 diffèrent):

```
rpm -ivh kernel-smp-2.4.20-2.47.1.i386.rpm
```

S'il s'agit d'un système de type `i686` comportant plus de 4 giga-octets de RAM, installez le paquetage `kernel-bigmem` conçu également pour l'architecture `i686` (il est possible que la version noyau diffère):

```
rpm -ivh kernel-bigmem-2.4.20-2.47.1.i686.rpm
```

Si les paquetages `kernel-source`, `kernel-docs` ou `kernel-utils` doivent être mis à niveau, il n'est probablement pas nécessaire de conserver les anciennes versions. Utilisez les commandes suivantes pour mettre à niveau ces paquetages (il est possible que les versions diffèrent):

```
rpm -Uvh kernel-source-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-docs-2.4.20-2.47.1.i386.rpm
rpm -Uvh kernel-utils-2.4.20-2.47.1.i386.rpm
```

Si le système nécessite une prise en charge PCMCIA (un portable, par exemple) installez le paquetage `kernel-pcmcia-cs` et conserver l'ancienne version. Si le commutateur `-i` est utilisé, il y aura probablement un conflit car l'ancien noyau a besoin de ce paquetage pour se lancer avec la prise en charge PCMCIA. Pour contourner ce problème, utilisez le commutateur `--force` de la façon suivante (il est possible que la version diffère):

```
rpm -ivh --force kernel-pcmcia-cs-3.1.24-2.i386.rpm
```

L'étape suivante consiste à vérifier que l'image de disque RAM initial à bien été créée. Reportez-vous à la Section 30.5 pour de plus amples informations.

30.5. Vérification de l'image de disque RAM initial

Si le système utilise le système de fichiers ext3 ou un contrôleur SCSI, il est nécessaire d'avoir un disque RAM initial. Le rôle de ce dernier est de permettre à un noyau modulaire d'avoir accès aux modules dont il pourrait avoir besoin pour démarrer avant que le noyau ait accès au périphérique où les modules se trouvent normalement.

Le disque RAM initial peut être créé à l'aide de la commande `mkinitrd`. Toutefois, cette étape se déroule automatiquement si le noyau et les paquetages qui lui sont associés sont installés ou mis à niveau à partir des paquetages RPM distribués par Red Hat, Inc.; il n'est donc pas nécessaire d'effectuer cette étape manuellement. Afin de vous assurer que le disque a bien été créé, utilisez la commande `ls -l /boot` et vérifiez par là-même l'existence du fichier `initrd-2.4.20-2.47.1.img` (la version devrait correspondre à la version du noyau qui vient d'être installé)

Il est maintenant nécessaire de vérifier que le chargeur d'amorçage a bien été configuré de façon à ce qu'il démarre le nouveau noyau. Consultez la Section 30.6 pour plus d'informations.

30.6. Vérification du chargeur d'amorçage

Le paquetage RPM `kernel` configure le chargeur d'amorçage GRUB ou LILO de façon à ce que le noyau nouvellement installé soit démarré si l'un des chargeurs est installé. Il ne configure toutefois pas le chargeur d'amorçage afin qu'il démarre par défaut le nouveau noyau.

Il est vivement recommandé de vérifier que le chargeur d'amorçage a été correctement configuré. Il s'agit en effet d'une étape cruciale. S'il n'est pas correctement configuré, le système ne pourra pas démarrer Red Hat Linux correctement. Dans ce cas, démarrez votre système à l'aide de la disquette de démarrage préalablement créée et essayez de reconfigurer le chargeur d'amorçage.

30.6.1. GRUB

Si vous avez choisi GRUB comme chargeur d'amorçage, vérifiez que le fichier `/boot/grub/grub.conf` contient une section `title` portant la même version que le paquetage `kernel` que vous venez d'installer (si vous avez installé le paquetage `kernel-smp` ou le paquetage `kernel-bigmem`, il y aura également une section correspondante):

```
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=3
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-2.47.1)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-2.47.1 ro root=LABEL=/
        initrd /initrd-2.4.20-2.47.1.img
title Red Hat Linux (2.4.20-2.30)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-2.30 ro root=LABEL=/
        initrd /initrd-2.4.20-2.30.img
```

Si une partition `/boot` séparée a été créée, les chemins d'accès au noyau ainsi qu'à l'image d'initrd sont relatifs à la partition `/boot`.

Notez bien que la valeur par défaut ne correspond pas au nouveau noyau. Pour configurer GRUB de façon à ce qu'il démarre le nouveau noyau par défaut, remplacez la valeur de la variable `default` par le numéro de la section du titre qui contient le nouveau noyau. La numérotation commence à 0. Ainsi, si le nouveau noyau correspond à la deuxième section du titre, donnez à `default` la valeur **`1`**.

Vous pouvez maintenant commencer à tester votre nouveau noyau en redémarrant l'ordinateur et en lisant bien les messages qui apparaîtront pour vous assurer que tout le matériel est correctement détecté.

30.6.2. LILO

Si vous avez choisi LILO comme chargeur d'amorçage, vérifiez que le fichier `/etc/lilo.conf` contient une section `image` portant la même version que le paquetage `kernel` que vous venez d'installer (si vous avez installé le paquetage `kernel-smp` ou le paquetage `kernel-bigmem`, il y aura également une section correspondante):

```
prompt
timeout=50
default=2.4.20-2.30
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
message=/boot/message
linear

image=/boot/vmlinuz-2.4.20-2.47.1
        label=2.4.20-2.47.1
        initrd=/boot/initrd-2.4.20-2.47.1.img
        read-only
        append="root=LABEL=/"

image=/boot/vmlinuz-2.4.20-2.30
        label=2.4.20-2.30
        initrd=/boot/initrd-2.4.20-2.30.img
        read-only
        append="root=LABEL=/"
```

Notez bien que la valeur par défaut ne correspond pas au nouveau noyau. Pour configurer GRUB de façon à ce qu'il démarre le nouveau noyau par défaut, donnez à la variable `default` la valeur de `label` qui se trouve dans la section `image` du nouveau noyau. En étant connecté en tant que super-utilisateur, exécutez la commande `/sbin/lilo` pour activer les modifications. Suite à cette opération, une sortie semblable à l'extrait suivant s'affichera:

```
Added 2.4.20-2.47.1 *
Added linux
```

L'astérisque (`*`) placé après `2.4.20-2.47.1` indique que le noyau de cette section est celui que LILO démarrera par défaut.

Vous pouvez maintenant commencer à tester votre nouveau noyau en redémarrant l'ordinateur et en lisant bien les messages qui apparaîtront pour vous assurer que tout le matériel est correctement détecté.

Chapitre 31.

Modules de noyau

Le noyau Linux est de conception modulaire. Au démarrage, seul un noyau résident minimal est chargé dans la mémoire. Par la suite, chaque fois qu'un utilisateur demande une fonction qui n'est pas présente dans le noyau résident, un *module de noyau*, parfois également appelé *périphérique*, est chargé dynamiquement en mémoire.

Lors de l'installation, le matériel présent sur votre système est détecté. En fonction de cette analyse et des informations fournies par l'utilisateur, le programme détermine modules doivent être chargés au démarrage. Le programme d'installation configure le mécanisme de chargement dynamique afin qu'il fonctionne de façon transparente.

Si du nouveau matériel est ajouté après l'installation et que ce matériel nécessite un module de noyau, le système doit être configuré de manière à ce qu'il charge le module de noyau approprié pour le nouveau matériel. Lorsque le système est amorcé avec le nouveau matériel, le programme **Kudzu** s'exécute, détecte le nouveau matériel s'il est pris en charge et configure le module en conséquence. Le module peut aussi être spécifié manuellement en modifiant le fichier de configuration du module, à savoir `/etc/modules.conf`.

Remarque

Les modules de cartes vidéo utilisés pour afficher l'interface du système X Window font partie du paquetage `XFree86`, pas du noyau; ce chapitre ne s'applique par conséquent pas à ces dernières.

Par exemple, si un système inclut un adaptateur réseau PCI EtherPower 10 SMC, le fichier de configuration des modules contiendra la ligne suivante:

```
alias eth0 tulip
```

Si une deuxième carte réseau est ajoutée au système et qu'elle est identique à la première, insérez la ligne suivante dans `/etc/modules.conf`:

```
alias eth1 tulip
```

Reportez-vous au *Guide de référence de Red Hat Linux* pour obtenir une liste alphabétique des modules de noyau et du matériel pris en charge par les modules.

31.1. Utilitaires des modules de noyau

Un groupe de commandes permettant la gestion des modules de noyau peut également être utilisé si le paquetage `modutils` est installé. Utilisez ces commandes pour déterminer si un module a bien été chargé ou pour essayer différents modules pour un nouveau composant matériel.

La commande `/sbin/lsmod` permet d'afficher une liste des modules actuellement chargés. Par exemple:

```
Module                  Size  Used by    Not tainted
iptable_filter          2412   0 (autoclean) (unused)
ip_tables              15864   1 [iptable_filter]
nfs                    84632   1 (autoclean)
lockd                  59536   1 (autoclean) [nfs]
```

```
sunrpc                  87452   1 (autoclean) [nfs lockd]
soundcore                7044   0 (autoclean)
ide-cd                  35836   0 (autoclean)
cdrom                   34144   0 (autoclean) [ide-cd]
parport_pc              19204   1 (autoclean)
lp                       9188   0 (autoclean)
parport                 39072   1 (autoclean) [parport_pc lp]
autofs                  13692   0 (autoclean) (unused)
e100                    62148   1
microcode                5184   0 (autoclean)
keybdev                  2976   0 (unused)
mousedev                 5656   1
hid                     22308   0 (unused)
input                    6208   0 [keybdev mousedev hid]
usb-uhci                27468   0 (unused)
usbcore                 82752   1 [hid usb-uhci]
ext3                    91464   2
jbd                     56336   2 [ext3]
```

Pour chaque ligne, la première colonne correspond au nom du module, la deuxième colonne affiche la taille du module et la troisième colonne précise l'utilisation par le module.

Les informations figurant après la colonne d'utilisation varie légèrement selon le module. Si la valeur `(unused)` (non-utilisé) apparaît sur la ligne du module, le module en question n'est pas utilisé. Si la valeur `(autoclean)` (nettoyage automatique) apparaît sur la ligne du module, le module en question peut être déchargé à l'aide de la commande `rmmod -a`. Lors de l'exécution de cette commande, tout module portant la mention 'autoclean' et n'ayant pas été utilisé depuis la dernière opération de nettoyage automatique, est déchargé. Red Hat Linux n'effectue pas cette opération de nettoyage automatique par défaut.

Si un module de la liste apparaît entre parenthèses à la fin de la ligne, le module en question a une relation de dépendance avec le module énuméré sur la même ligne, dans la première colonne. Par exemple, dans la ligne

```
usbcore                 82752   1 [hid usb-uhci]
```

les modules de noyau hid et usb-uhci dépendent du module usbcore pour leur fonctionnement.

La sortie de `/sbin/lsmod` est la même que celle obtenue lors de l'affichage de `/proc/modules`.

Pour charger un module de noyau, utilisez la commande `/sbin/modprobe` suivie du nom du noyau. Par défaut, `modprobe` essaie de charger le module à partir des sous-répertoires `/lib/modules/<`*`version-du-noyau`*`>/kernel/drivers/`. Il existe un sous-répertoire pour chaque module, comme par exemple le sous-répertoire `net/` pour les pilotes d'interfaces réseau. Certains modules de noyau sont soumis à des dépendances de modules et nécessitent donc pour leur chargement, que d'autres modules soient préalablement chargés. La commande `/sbin/modprobe` vérifie ces dépendances et charge les dépendances de modules, avant de charger le module spécifié.

Par exemple, la commande

```
/sbin/modprobe hid
```

charge d'abord toute dépendance de module et ensuite effectue le chargement du module `hid`.

Pour afficher à l'écran toutes les commandes au fur et à mesure que `/sbin/modprobe` les exécute, utilisez l'option `-v`. Par exemple:

```
/sbin/modprobe -v hid
```

Une sortie semblable à celle reproduite ci-dessous s'affiche alors:

```
/sbin/insmod /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Using /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Symbol version prefix 'smp_'
```

La commande `/sbin/insmod` permet également de charger des modules de noyau; toutefois, elle ne résout pas les problèmes de dépendances. Dans de telles conditions, il est recommandé d'utiliser la commande `/sbin/modprobe`.

Pour décharger des modules de noyau, utilisez la commande `/sbin/rmmod` suivie du nom du module. L'utilitaire `rmmod` ne décharge que les modules non-utilisés et n'appartenant pas à une relation de dépendance avec d'autre modules en cours d'utilisation.

Par exemple, la commande

```
/sbin/rmmod hid
```

décharge le module de noyau `hid`.

`modinfo` constitue un autre utilitaire de module de noyau utile. Utilisez la commande `/sbin/modinfo` pour afficher des informations concernant un module de noyau. La syntaxe générale est la suivante:

```
/sbin/modinfo [options] <module>
```

Les options comprennent `-d` qui affiche une brève description du module et `-p` qui répertorie les paramètres pris en charge par le module. Pour\ une liste complète des options, reportez-vous à la page de manuel de `modinfo` (`man modinfo`).

31.2. Ressources supplémentaires

Pour de plus amples informations sur les modules de noyau et leurs utilitaires, reportez-vous aux ressources suivantes.

31.2.1. Documentation installée

- Page de manuel relative à `lsmod` — description et explication des sorties correspondantes.
- Page de manuel relative à `insmod` — description et liste d'options de ligne de commande.
- Page de manuel relative à `modprobe` — description et liste d'options de ligne de commande.
- Page de manuel relative à `rmmod` — description et liste d'options de ligne de commande.
- Page de manuel relative à `modinfo` — description et liste d'options de ligne de commande.
- `/usr/src/linux-2.4/Documentation/modules.txt` — comment compiler et utiliser des modules de noyau.

31.2.2. Sites Web utiles

- http://www.redhat.com/mirrors/LDP/HOWTO/Module-HOWTO/index.html — *Linux Loadable Kernel Module HOWTO* (HOWTO Modules de noyau chargeables Linux) du Projet de documentation Linux.

V. Gestions des paquetages

Sur un système Red Hat Linux les logiciels sont divisés en paquetages RPM qui peuvent être installés, mis à niveau ou retirés. Cette section décrit la manière permettant des gérer les paquetages RPM sur un système Red Hat Linux à l'aide d'outils graphiques ou utilisant la ligne de commande.

Table des matières

Chapitre 32.

Gestion des paquetages à l'aide de RPM

Le gestionnaire de paquetages RPM est est un système de gestion des paquetages que tout le monde peut utiliser et qui peut être exécuté aussi bien sur Red Hat Linux que sur d'autres systèmes Linux et UNIX. Red Hat, Inc. encourage d'ailleurs tous les éditeurs à utiliser RPM pour leurs propres produits. RPM peut être distribué aux conditions fixées par la licence publique générale.

RPM facilite la mise à jour du système pour l'utilisateur final. En effet, il suffit de quelques commandes pour effectuer l'installation, la désinstallation et la mise à jour de paquetages RPM. RPM maintient aussi une base de données des paquetages installés et de leurs fichiers, ce qui vous permet de procéder à des recherches et des vérifications approfondies dans votre système. Si vous préférez travailler au moyen d'une interface graphique, utilisez l'**Outil de gestion de paquetages**, vous pourrez ainsi effectuer de nombreuses commandes RPM. Reportez-vous au Chapitre 33 pour obtenir de plus amples informations.

En outre, RPM manipule les fichiers de configuration avec soin durant les mises à jour afin d'éviter que vos personnalisations ne soient perdues — chose que vous ne pourriez faire avec des fichiers `.tar.gz` normaux.

Si vous êtes un développeur, RPM vous permet de prendre le code source du logiciel et de le transformer en paquetage source et binaire pour l'utilisateur final. Ce processus est assez simple et est piloté depuis un unique fichier et des retouches (patches) facultatives que vous créez. Cette démarcation claire entre le code source d'origine et vos retouches, ainsi que les instructions de création facilitent l'entretien du paquetage alors que de nouvelles versions du logiciel sont publiées.

Remarque

Comme RPM apporte des changements au système, il vous est nécessaire d'être connecté comme root pour pouvoir installer, désinstaller ou mettre à jour un paquetage RPM.

32.1. Objectifs de la conception de RPM

Pour bien comprendre comment utiliser RPM, il est utile de comprendre les objectifs qui ont guidé sa conception.

Evolutivité

Grâce à RPM, vous pouvez mettre à jour les composants individuels de votre système sans devoir tout réinstaller. Lorsque vous obtenez une nouvelle version d'un système d'exploitation fondé sur RPM (comme Red Hat Linux), vous n'avez pas à l'installer en entier sur votre ordinateur (contrairement aux systèmes d'exploitation fondés sur des systèmes de paquetages différents). RPM permet de faire une mise à jour 'intelligente', complètement automatisée et sans démontage de votre système. Les fichiers de configuration des paquetages sont préservés durant la mise à jour, ce qui signifie que vous ne perdez pas vos personnalisations. Aucun fichier de mise à jour spécial n'est requis pour mettre à jour un paquetage car le même fichier RPM est utilisé pour installer et mettre à jour le paquetage sur votre système.

Fonctions de recherche performantes

RPM est conçu pour offrir de puissantes options de recherche. Vous pouvez ainsi chercher dans votre base de données des paquetages ou des fichiers spécifiques et trouver facilement à quel

paquetage appartient un fichier et la provenance d'un paquetage. Les fichiers contenus dans les paquetages RPM sont stockés dans des archives compressées et dotées d'un en-tête binaire qui contiennent des informations utiles au sujet des paquetages et de leur contenu; la recherche de paquetages individuels est donc facile et rapide.

Vérification du système

La possibilité de vérifier les paquetages est une autre caractéristique importante. Si vous vous inquiétez à l'idée avoir supprimé un fichier important d'un des paquetages, vous n'avez qu'à vérifier le paquetage en question. Ce faisant, toute anomalie vous sera rapportée. À ce stade, vous pourrez réinstaller le paquetage si cela s'avère nécessaire. Cependant, tous les fichiers de configuration que vous avez modifiés sont préservés lors de la réinstallation.

Sources d'origine

L'un des objectifs principaux de l'application était de permettre l'utilisation de sources logicielles d'origine, c'est-à-dire telles qu'elles ont été écrites par les auteurs originaux du programme. RPM est fourni avec les sources d'origine et les retouches qui y ont été ajoutées ainsi qu'avec les instructions complètes de création. Cela représente un gros avantage et pour bien des raisons. Par exemple, si une nouvelle version est publiée, vous n'avez pas nécessairement à recommencer à zéro pour la compiler. Vous pouvez simplement jeter un coup d'oeil aux retouches pour voir ce que vous *pourriez* avoir à faire. Toutes les valeurs par défaut déjà compilées et les changements apportés pour faire en sorte que le logiciel soit créé correctement peuvent être visualisés au moyen de cette technique.

Le désir de maintenir les sources d'origine ne peut sembler important que pour le développeur, mais en réalité cela assure également des logiciels de qualité supérieure pour l'utilisateur final. Nous aimerions profiter de l'occasion pour remercier nos amis de la distribution BOGUS, à la l'origine du concept des sources d'origine.

32.2. Utilisation de RPM

RPM a cinq modes d'opération de base (sans compter la construction de paquetages): installation, désinstallation, mise à jour, recherche et vérification. Cette section vous donne un aperçu de chacun de ces modes. Pour obtenir plus de détails et connaître les différentes options, consultez `rpm--help` ou reportez-vous à la Section 32.5 qui vous donnera plus d'informations sur RPM.

32.2.1. Recherche de paquetages RPM

Avant d'utiliser un paquetage RPM, vous devez savoir où le trouver. Si vous cherchez sur l'Internet, vous découvrirez sans doute de nombreux référentiels, mais si vous êtes à la recherche de paquetages RPM créés par Red Hat, vous les trouverez aux endroits suivants:

- CD-ROM Red Hat Linux
- Page Web Errata Red Hat, à l'adresse suivante: http://www.redhat.com/apps/support/errata/
- Site FTP miroir de Red Hat, disponible à l'adresse suivante: http://www.redhat.com/download/mirror.html
- Red Hat Network — le Chapitre 34 fournit des informations détaillées sur Red Hat Network

32.2.2. Installation

Les noms de fichier des paquetages RPM ressemblent généralement à ceci : `foo-1.0-1.i386.rpm`. Le nom de fichier comprend le nom du paquetage (`foo`), la version (`1.0`), l'édition (`1`) et l'architecture (`i386`). Rien de plus simple que d'installer un paquetage; vous n'avez qu'à entrer la commande suivante à l'invite du shell (en tant qu'utilisateur root):

```
rpm -Uvh foo-1.0-1.i386.rpm
```

Si l'installation est réussie, vous verrez ce qui suit:

```
Preparing...                ########################################### [100%]
   1:foo                    ########################################### [100%]
```

Comme vous pouvez le constater, RPM affiche le nom du paquetage, puis une succession de symboles dièse pour indiquer la progression de l'installation du paquetage.

À partir de la version 4.1 de RPM, la signature d'un paquetage est vérifiée lors de son installation ou de sa mise à niveau. Si la vérification de la signature échoue, vous verrez un message d'erreur de ce type:

```
error: V3 DSA signature: BAD, key ID 0352860f
```

S'il s'agit d'une nouvelle signature (en-tête uniquement), vous verrez un message d'erreur du type:

```
error: Header V3 DSA signature: BAD, key ID
0352860f
```

Si la clé nécessaire à la vérification de la signature n'est pas installée sur votre système, le message contiendra `NOKEY` :

```
warning: V3 DSA signature: NOKEY, key ID
0352860f
```

Reportez-vous à la Section 32.3 pour plus d'informations sur la vérification de la signature d'un paquetage.

Remarque

Si vous installez un paquetage de noyau, utilisez plutôt la commande `rpm -ivh`. Reportez-vous à Chapitre 30 pour plus de détails.

L'installation des paquetages a été conçue de façon à être simple, mais des erreurs peuvent parfois survenir.

32.2.2.1. Le paquetage est déjà installé

Si vous installez un paquetage dont la version est déjà installée, le système affiche:

```
Preparing...                ########################################### [100%]
package foo-1.0-1 is already installed
```

Si vous désirez poursuivre l'installation malgré le fait que la version du paquetage soit déjà installée, utilisez l'option `--replacepkgs`, qui indique ainsi à RPM d'ignorer le message d'erreur:

```
rpm -ivh --replacepkgs foo-1.0-1.i386.rpm
```

Cette option peut s'avérer utile lorsque des fichiers installés du paquetage RPM ont été éliminés ou lorsque vous voulez les fichiers de configuration originaux du paquetage RPM à installer.

32.2.2.2. Conflits de fichiers

Si vous tentez d'installer un paquetage contenant un fichier déjà installé par un autre paquetage ou une version précédente du même paquetage, le système affiche:

```
Preparing...                ########################################### [100%]
file /usr/bin/foo from install of foo-1.0-1 conflicts with file from package
bar-2.0.20
```

Pour faire en sorte que RPM ignore cette erreur, utilisez l'option `--replacefiles`:

```
rpm -ivh --replacefiles foo-1.0-1.i386.rpm
```

32.2.2.3. Dépendance non-résolue

Les paquetages RPM peuvent 'dépendre' d'autres paquetages, ce qui signifie qu'ils requièrent l'installation d'autres paquetages pour fonctionner correctement. Si vous essayez d'installer un paquetage pour lequel il existe une telle dépendance non-résolue, vous verrez s'afficher:

```
Preparing...                ########################################### [100%]
error: Failed dependencies:
        bar.so.2 is needed by foo-1.0-1
    Suggested resolutions:
        bar-2.0.20-3.i386.rpm
```

Si vous installez un Red Hat officiel, il vous proposera généralement le(s) paquetage(s) nécessaire(s) à la résolution de la dépendance. Localisez le paquetage en question sur les CD-ROM de Red Hat Linux ou sur le site FTP Red Hat (ou miroir), et ajoutez-le à la commande:

```
rpm -ivh foo-1.0-1.i386.rpm bar-2.0.20-3.i386.rpm
```

Si l'installation des deux paquetages est réussie, vous verrez:

```
Preparing...                ########################################### [100%]
   1:foo                    ########################################### [ 50%]
   2:bar                    ########################################### [100%]
```

Si aucun paquetage n'est suggéré pour résoudre la dépendance, vous pouvez essayez d'utiliser l'option `--redhatprovides` pour déterminer le paquetage contenant le fichier requis. Pour utiliser cette option, il faut que le paquetage `rpmdb-redhat` soit installé sur votre système.

```
rpm -q --redhatprovides bar.so.2
```

Si le paquetage contenant `bar.so.2` se trouve dans la base de données installée du paquetage `rpmdb-redhat`, le nom du paquetage sera affiché:

```
bar-2.0.20-3.i386.rpm
```

Si vous voulez néanmoins forcer l'installation (ce qui est une mauvaise idée car le paquetage ne fonctionnera probablement pas correctement), utilisez l'option `--nodeps`.

32.2.3. Désinstallation

La désinstallation d'un paquetage est aussi simple que son installation. Entrez simplement la commande suivante à l'invite du shell:

```
rpm -e foo
```

Remarque

Notez que nous avons utilisé le *nom* de paquetage `foo`, pas celui du *fichier* original du paquetage `foo-1.0-1.i386.rpm`. Pour désinstaller un paquetage, vous devrez remplacer `foo` par le nom du paquetage en question.

Une erreur de dépendance peut se produire lors de la désinstallation d'un paquetage si un autre paquetage installé dépend de celui que vous essayez de supprimer. Par exemple:

```
Preparing...                ########################################### [100%]
error: removing these packages would break dependencies:
        foo is needed by  bar-2.0.20-3.i386.rpm
```

Pour que RPM ignore cette erreur et désinstalle le paquetage malgré tout (ce qui est également une mauvaise idée du fait que le paquetage qui en dépend cessera probablement de fonctionner correctement), utilisez l'option `--nodeps`.

32.2.4. Mise à jour

La mise à jour d'un paquetage est semblable à son installation. Entrez la commande suivante à l'invite du shell:

```
rpm -Uvh foo-2.0-1.i386.rpm
```

Ce que vous ne voyez pas ci-dessus est que RPM désinstalle automatiquement les anciennes versions du paquetage `foo`. En réalité, il pourrait être plus judicieux de toujours utiliser la commande `-U` pour installer des paquetages car elle fonctionne même lorsque aucune version antérieure du paquetage n'est installée.

Comme RPM effectue une mise à jour intelligente des paquetages avec des fichiers de configuration, le message suivant peut apparaître:

```
saving /etc/foo.conf as /etc/foo.conf.rpmsave
```

Ce message signifie que les changements que vous avez apportés au fichier de configuration ne sont peut-être pas 'compatibles' avec le nouveau fichier de configuration du paquetage. Aussi, RPM sauvegarde-t-il le fichier original et installe-t-il le nouveau. Vous devez ensuite déterminer les différences entre les deux fichiers de configuration et trouver une solution le plus rapidement possible, afin d'assurer que votre système continue de fonctionner correctement.

La mise à jour est en fait une combinaison de l'installation et de la désinstallation. Il se pourrait donc que le système affiche des erreurs d'installation ou de désinstallation lors de la mise à jour d'un paquetage RPM. Un autre type d'erreur peut également survenir: lorsque RPM pense que vous essayez de faire la mise à jour d'un paquetage au moyen d'une version plus *ancienne*. Le système affiche alors:

```
package foo-2.0-1 (which is newer than foo-1.0-1) is already installed
```

Pour faire en sorte que le paquetage RPM soit mis à jour malgré tout, utilisez l'option `--oldpackage`:

```
rpm -Uvh --oldpackage foo-1.0-1.i386.rpm
```

32.2.5. Actualisation

L'actualisation d'un paquetage est semblable à sa mise à jour. Entrez la commande suivante à l'invite du shell:

```
rpm -Fvh foo-1.2-1.i386.rpm
```

L'option d'actualisation de RPM vérifie les versions de paquetages spécifiées dans la ligne de commande par rapport aux versions installées sur le système. Lorsqu'une version plus récente d'un paquetage déjà installé est traitée par l'option d'actualisation de RPM, la mise à niveau vers la version plus récente intervient. Toutefois, l'option d'actualisation de RPM n'installe pas un paquetage s'il n'existe pas un paquetage du même nom installé précédemment. Ceci diffère de l'option de mise à jour de RPM, vu que la mise à jour installera *effectivement* les paquetages, qu'une version antérieure soit installée ou non.

L'option d'actualisation de RPM peut fonctionner pour des paquetages pris individuellement ou pour des groupes de paquetages. Exemple: si vous venez tout juste de télécharger un grand nombre de paquetages et désirez seulement mettre à jour les paquetages, parmi ceux-ci, déjà installés sur votre système, utilisez l'option d'actualisation. Ce faisant, vous n'aurez pas à supprimer les paquetages non-voulus du groupe de paquetages téléchargés avant d'utiliser RPM.

Dans ce cas, vous pouvez exécuter la commande suivante:

```
rpm -Fvh *.rpm
```

De cette façon, RPM ne met à jour que les paquetages déjà installés.

32.2.6. Recherche

L'interrogation de la base de données des paquetages installés s'effectue à l'aide de la commande `rpm -q`. La commande `rpm -q foo` imprime le nom du paquetage, la version et l'édition du paquetage foo installé:

```
foo-2.0-1
```

Remarque

Notez que nous avons utilisé le *nom* du paquetage `foo`. Pour procéder à la recherche d'un autre paquetage, vous devrez remplacer`foo` par le nom du paquetage en question.

Au lieu de spécifier le nom du paquetage, vous pouvez utiliser les options suivantes avec `-q` pour spécifier quel(s) paquetage(s) vous voulez rechercher. Elles sont appelées *options de spécification de paquetage*.

- `-a` recherche tous les paquetages actuellement installés.
- `-f` <*fichier*> interroge le paquetage qui possède le <*fichier*>. Lorsque vous spécifiez un fichier, vous devez indiquer son chemin d'accès complet (par exemple, `/usr/bin/ls`).

- `-p <fichier_de_paquetage>` interroge le paquetage <*fichier_de_paquetage*>.

Il y a plusieurs manières de spécifier les informations à afficher sur les paquetages recherchés. Les options suivantes sont utilisées pour sélectionner le type d'informations recherché. Elles sont appelées *options de sélection d'informations*.

- `-i` affiche des informations sur le paquetage, telles que le nom, la description, l'édition, la taille, la date de création, l'éditeur, etc.
- `-l` affiche la liste des fichiers contenus dans le paquetage.
- `-s` affiche l'état de tous les fichiers du paquetage.
- `-d` affiche la liste des fichiers de documentation (pages de manuel, pages d'informations, fichiers README, etc.).
- `-c` affiche la liste des fichiers de configuration. Il s'agit de fichiers que vous modifiez après l'installation pour adapter le paquetage à votre système (comme `sendmail.cf`, `passwd`, `inittab`, etc.).

Pour les options qui affichent des listes de fichiers, vous pouvez ajouter `-v` à la commande pour obtenir les listes dans un format `ls -l` familier.

32.2.7. Vérification

La vérification d'un paquetage permet de comparer les informations sur les fichiers d'un paquetage installé à celles du paquetage original. La vérification compare, entre autres, la taille, la somme MD5, les autorisations, le type, le propriétaire et le groupe de chaque fichier.

La commande `rpm -V` vérifie un paquetage. Vous pouvez utiliser n'importe laquelle des *options de sélection de paquetage* de la liste pour spécifier les paquetages que vous souhaitez vérifier. Une utilisation simple est `rpm -V foo` qui vérifie si tous les fichiers du paquetage foo sont tels qu'ils étaient lors de leur installation initiale. Par exemple:

- Pour vérifier un paquetage contenant un fichier particulier:
  ```
  rpm -Vf /bin/vi
  ```
- Pour vérifier TOUS les paquetages installés:
  ```
  rpm -Va
  ```
- Pour comparer un paquetage installé à un fichier de paquetage RPM:
  ```
  rpm -Vp foo-1.0-1.i386.rpm
  ```
  Cette commande peut être utile si vous pensez que vos bases de données RPM sont corrompues.

Si la vérification est correcte, elle ne fournit aucun résultat. S'il y a des discordances, elles sont affichées. Le format du résultat est une chaîne de huit caractères (un `c` indique un fichier de configuration) et le nom du fichier. Chacun des huit caractères indique le résultat d'une comparaison entre un attribut du fichier et la valeur de cet attribut enregistrée dans la base de données RPM. Un simple point (`.`) signifie que le test a réussi. Les caractères suivants indiquent l'échec de certains tests:

- `5` — somme de contrôle MD5
- `S` — taille de fichier
- `L` — lien symbolique
- `T` — date de modification du fichier
- `D` — périphérique
- `U` — utilisateur

- `G` — groupe
- `M` — mode (comprend les permissions et le type de fichier)
- `?` — fichier pas lisible

Si vous voyez un résultat affiché, essayez de déterminer s'il est préférable de supprimer ou de réinstaller le paquetage, ou de résoudre le problème autrement.

32.3. Vérification de la signature d'un paquetage

Si vous désirez vous assurer qu'un paquetage n'a pas été corrompu ou manipulé, vous n'avez qu'à examiner la somme MD5 en entrant la commande suivante à l'invite du shell (remplacez *<fichier-rpm>* par le nom de fichier du paquetage RPM):

```
rpm -K --nogpg <rpm-file>
```

Le message *<fichier-rpm>*: `md5 OK` s'affiche. Ce petit message signifie que le fichier n'a pas été endommagé par le téléchargement. Pour voir un message plus détaillé, remplacez `-K` par `-Kvv` dans la commande.

Toutefois, quelle est la fiabilité du développeur du paquetage ? Si le paquetage est *signé* à l'aide de la *clé* GnuPG du développeur, vous savez au moins que le développeur est celui qu'il prétend être.

Un paquetage RPM peut être signé à l'aide de Gnu Privacy Guard (ou GnuPG), pour en assurer la fiabilité lors d'un téléchargement.

GnuPG est un outil permettant de sécuriser les communications ; il s'agit d'un outil de remplacement complet et gratuit de la technologie de cryptage de PGP, un programme de protection électronique de l'information. Avec GnuPG, vous pouvez authentifier la validité de documents, crypter et décrypter des données à destination ou en provenance de vos correspondants. Cet outil peut également décrypter et vérifier des fichiers PGP 5.*x*.

Durant l'installation de Red Hat Linux, GnuPG est installé par défaut. Ainsi, vous pouvez commencer immédiatement à utiliser GnuPG pour vérifier les paquetages que vous recevez de Red Hat. Vous devez d'abord importer la clé publique de Red Hat.

32.3.1. Importation de clés

Pour vérifier des paquetages Red Hat, vous devez importer la clé Red Hat GPG. Pour ce faire, exécutez la commande suivante à une invite de shell:

```
rpm --import /usr/share/rhn/RPM-GPG-KEY
```

Pour afficher une liste de toutes les clés installées pour une vérification RPM, exécutez la commande:

```
rpm -qa gpg-pubkey*
```

Pour la clé Red Hat, la sortie comprendra:

```
gpg-pubkey-db42a60e-37ea5438
```

Pour afficher des détails sur une clé spécifique, utilisez `rpm -qi` suivie de la sortie de la commande précédente:

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

32.3.2. Vérification de la signature de paquetages

Pour vérifier la signature GnuPG d'un fichier RPM après avoir importé la clé GnuPG du constructeur, utilisez la commande suivante (remplacez *<fichier-rpm>* par le nom de fichier du paquetage RPM):

```
rpm -K <rpm-file>
```

Si tout se passe bien, vous verrez le message: `md5 gpg OK`. Cela signifie que la signature du paquetage a été vérifiée et qu'il n'est pas corrompu.

Astuce

Pour obtenir davantage d'informations sur GnuPG, consultez l'Annexe B.

32.4. Étonnez vos amis avec RPM

RPM est un outil pratique pour gérer votre système ainsi que pour identifier et résoudre des problèmes. Aussi, la meilleure façon de donner un sens à toutes ses options est d'examiner quelques exemples.

- Vous avez peut-être supprimé des fichiers accidentellement, mais ne savez pas exactement lesquels. Pour vérifier le système en entier et trouver ce qui pourrait manquer, entrez la commande suivante:
  ```
  rpm -Va
  ```
  Si certains fichiers ont disparu ou ont été corrompus, vous devriez probablement réinstaller le paquetage ou désinstaller et puis réinstaller le paquetage.
- Il se pourrait qu'un jour vous tombiez sur un fichier que vous ne reconnaissez pas. Pour connaître le paquetage auquel il appartient, entrez simplement:
  ```
  rpm -qf /usr/X11R6/bin/ghostview
  ```
  Le résultat devrait ressembler à ceci:
  ```
  gv-3.5.8-22
  ```
- Nous pourrions combiner les deux exemples précédents et en faire le scénario suivant. Imaginons que vous avez des problèmes avec le programme `/usr/bin/paste`. Vous aimeriez vérifier à quel paquetage il appartient, mais vous ne savez pas à quel paquetage appartient `paste`. Entrez simplement la commande suivante:
  ```
  rpm -Vf /usr/bin/paste
  ```
  et la vérification du paquetage s'effectue.
- Vous aimeriez obtenir plus de détails sur un programme particulier? Vous n'avez qu'à essayer la commande suivante pour localiser la documentation fournie avec le paquetage auquel appartient le programme:
  ```
  rpm -qdf /usr/bin/free
  ```
  Le résultat devrait ressembler à ce qui suit:
  ```
  /usr/share/doc/procps-2.0.11/BUGS
  /usr/share/doc/procps-2.0.11/NEWS
  /usr/share/doc/procps-2.0.11/TODO
  /usr/share/man/man1/free.1.gz
  /usr/share/man/man1/oldps.1.gz
  /usr/share/man/man1/pgrep.1.gz
  /usr/share/man/man1/pkill.1.gz
  /usr/share/man/man1/ps.1.gz
  ```

```
/usr/share/man/man1/skill.1.gz
/usr/share/man/man1/snice.1.gz
/usr/share/man/man1/tload.1.gz
/usr/share/man/man1/top.1.gz
/usr/share/man/man1/uptime.1.gz
/usr/share/man/man1/w.1.gz
/usr/share/man/man1/watch.1.gz
/usr/share/man/man5/sysctl.conf.5.gz
/usr/share/man/man8/sysctl.8.gz
/usr/share/man/man8/vmstat.8.gz
```

- Vous pourriez aussi découvrir un nouveau paquetage RPM sans toutefois savoir à quoi il sert. Pour trouver des informations à son sujet, utilisez la commande suivante:

  ```
  rpm -qip crontabs-1.10-5.noarch.rpm
  ```

  Le résultat devrait ressembler à ceci:

  ```
  Name        : crontabs                      Relocations: (not relocateable)
  Version     : 1.10                               Vendor: Red Hat, Inc.
  Release     : 5                              Build Date: Fri 07 Feb 2003 04:07:32
  PM EST
  Install date: (not installed)                Build Host: porky.devel.redhat.com
  Group       : System Environment/Base        Source RPM: crontabs-1.10-5.src.rpm
  Size        : 1004                              License: Public Domain
  Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
  Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
  Summary     : Root crontab files used to schedule the execution of programs.
  Description :
  The crontabs package contains root crontab files. Crontab is the
  program used to install, uninstall, or list the tables used to drive the
  cron daemon. The cron daemon checks the crontab files to see when
  particular commands are scheduled to be executed. If commands are
  scheduled, then it executes them.
  ```

- Maintenant, vous souhaitez peut-être voir quels fichiers le RPM de `crontabs` installe. Pour ce faire, vous entreriez la commande suivante:

  ```
  rpm -qlp crontabs-1.10-5.noarch.rpm
  ```

  Le résultat devrait ressembler à ce qui suit:

  ```
  Name        : crontabs                      Relocations: (not relocateable)
  Version     : 1.10                               Vendor: Red Hat, Inc.
  Release     : 5                              Build Date: Fri 07 Feb 2003 04:07:32
  PM EST
  Install date: (not installed)                Build Host: porky.devel.redhat.com
  Group       : System Environment/Base        Source RPM: crontabs-1.10-5.src.rpm
  Size        : 1004                              License: Public Domain
  Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
  Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
  Summary     : Root crontab files used to schedule the execution of programs.
  Description :
  The crontabs package contains root crontab files. Crontab is the
  program used to install, uninstall, or list the tables used to drive the
  cron daemon. The cron daemon checks the crontab files to see when
  particular commands are scheduled to be executed. If commands are
  scheduled, then it executes them.
  ```

Ce ne sont que quelques exemples. Vous trouverez de nombreuses autres utilisations de RPM en vous en servant.

32.5. Ressources supplémentaires

RPM est un programme utilitaire très complexe, doté de nombreuses options et méthodes de recherche, d'installation, de mise à jour et de désinstallation de paquetages. Consultez les sources d'informations suivantes pour en savoir plus sur RPM.

32.5.1. Documentation installée

- `rpm --help` — cette commande permet d'afficher une référence rapide des paramètres de RPM.
- `man rpm` — la page de manuel relative à RPM donne plus de détails sur les paramètres de RPM que la commande `rpm --help`.

32.5.2. Sites Web utiles

- http://www.rpm.org/ — le site Web RPM.
- http://www.redhat.com/mailing-lists/rpm-list/ — la liste de distribution RPM est mise en archive à cet endroit. Pour vous y inscrire, envoyez un message électronique à l'adresse <`rpm-list-request@redhat.com`> et écrivez le mot `subscribe` dans la ligne objet.

32.5.3. Livres sur le sujet

- *Maximum RPM* de Ed Bailey ; édité par Red Hat Press — une version en ligne est disponible à l'adresse suivante: http://www.rpm.org/ et http://www.redhat.com/docs/books/.

Chapitre 33.

Outil de gestion de paquetages

Lors de l'installation, les utilisateurs choisissent un type d'installation, tel que **Poste de travail** ou **Serveur**. L'installation des paquetages logiciels est basée sur ce choix. Parce qu'il existe plusieurs types d'utilisateurs différents, il est possible que certains d'entre eux souhaitent installer ou supprimer des paquetages une fois l'installation terminée. L'**Outil de gestion de paquetages** permet aux utilisateurs d'effectuer ces opérations.

Le système X Window est nécessaire pour exécuter le programme **Outil de gestion de paquetages**. Pour lancer l'application, cliquez sur le bouton **Menu principal** (sur le panneau) => **Paramètres de système => Ajouter/Supprimer des applications** ou tapez la commande `redhat-config-packages` à l'invite du shell.

La même interface apparaîtra si vous insérez le CD-ROM 1 de Red Hat Linux dans votre ordinateur.

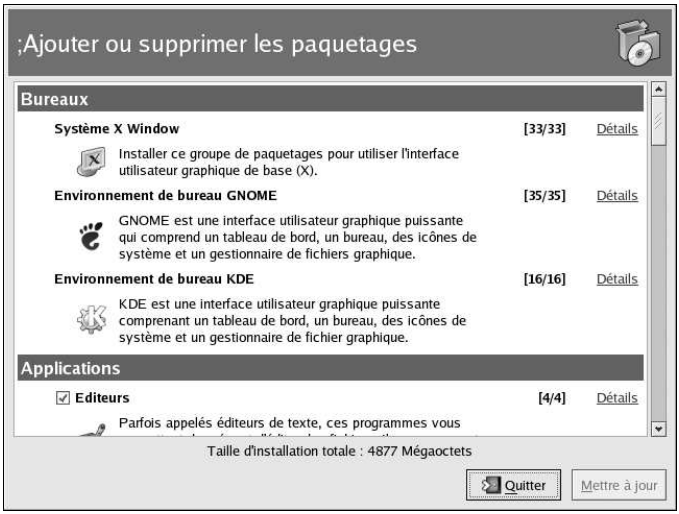

Figure 33-1. Outil de gestion de paquetages

L'interface de cette application est similaire à celle utilisée lors de l'installation. Les paquetages sont divisés en groupes. Ceux-ci contiennent une liste des *paquetages standard* et des *paquetages supplémentaires* partageant des fonctions communes. Le groupe **Internet Graphique** contient par exemple un navigateur Web, un client de messagerie électronique ainsi que d'autres programmes graphiques servant à se connecter à l'Internet. Les paquetages standard ne peuvent pas être supprimés, sauf si la totalité du groupe de paquetages est sélectionnée. Les paquetages supplémentaires sont des paquetages facultatifs que vous pouvez choisir d'installer ou de supprimer, si le groupe est sélectionné.

La fenêtre principale montre une liste des groupes de paquetages. Si la case de pointage située près d'un groupe est cochée, cela signifie que les paquetages de ce groupe sont actuellement installés. Pour afficher la liste des paquetages individuels pour un groupe, cliquez sur le bouton **Détails** situé près de ce dernier. Les paquetages individuels dont la case de pointage correspondante est cochée sont actuellement installés.

33.1. Installation des paquetages

Pour installer les paquetages standard d'un groupe qui n'est pas actuellement installé, cochez la case de pointage située près de ce groupe. Pour personnaliser les paquetages du groupe devant être installés, cliquez sur le bouton **Détails** situé près de ce dernier. La liste des paquetages standard et supplémentaires s'affiche, comme le montre la Figure 33-2. Lorsque vous cliquez sur le nom d'un paquetage, l'espace disque requis pour son installation s'affiche en bas de la fenêtre. En cochant la case de pointage située près du nom du paquetage, vous indiquez que vous souhaitez l'installer.

Vous pouvez également choisir des paquetages individuels appartenant à des groupes déjà installés. Pour ce faire, cliquez sur le bouton **Détails** et cochez la case de pointage correspondant aux paquetages supplémentaires qui ne sont pas encore installés.

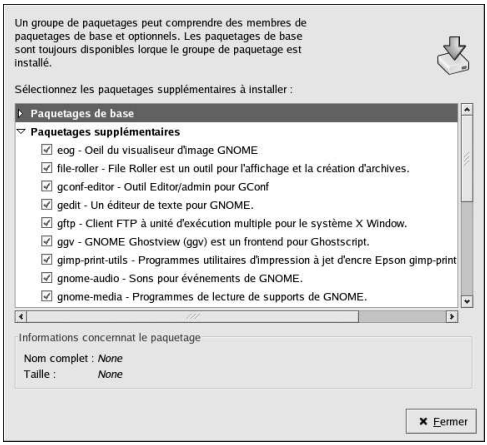

Figure 33-2. Sélection individuelle des paquetages

Après avoir choisi les groupes de paquetages ainsi que les paquetages individuels à installer, cliquez sur le bouton **Mettre à jour** de la fenêtre principale. L'application calculera ensuite la quantité d'espace disque requis pour l'installation des paquetages et recherchera les dépendances éventuelles, puis affichera une fenêtre récapitulative. S'il existe des dépendances, elles seront automatiquement ajoutées à la liste des paquetages à installer. Cliquez sur le bouton **Afficher détails** afin d'afficher la liste complète des paquetages devant être installés.

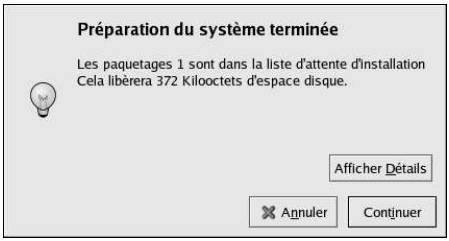

Figure 33-3. Récapitulatif de l'installation des paquetages

Cliquez sur **Continuer** pour lancer le processus d'installation. Une fois ce processus terminé, un message **Mise à jour terminée** s'affiche.

Astuce

Si vous utilisez **Nautilus** pour naviguer dans les fichiers et répertoires de votre ordinateur, vous pouvez également l'utiliser pour installer les paquetages. Dans **Nautilus**, allez dans le répertoire qui contient un paquetage RPM (ceux-ci portent généralement l'extension `.rpm`) et cliquez deux fois sur l'icône RPM.

33.2. Suppression de paquetages

Pour désinstaller tous les paquetages d'un groupe, désélectionnez la case de pointage située près du nom de ce dernier. Pour supprimer des paquetages individuels, cliquez sur le bouton **Détails** situé près du groupe et désélectionnez les paquetages souhaités.

Une fois que vous avez choisi les paquetages à supprimer, cliquez sur le bouton **Mettre à jour** de la fenêtre principale. L'application calcule la quantité d'espace disque qui sera libérée ainsi que les dépendances des paquetages logiciels. Si d'autres paquetages dépendent des paquetages que vous avez choisis de désinstaller, ils seront automatiquement ajoutés à la liste des paquetages à supprimer. Cliquez sur le bouton **Afficher détails** afin d'afficher la liste complète des paquetages devant être supprimés.

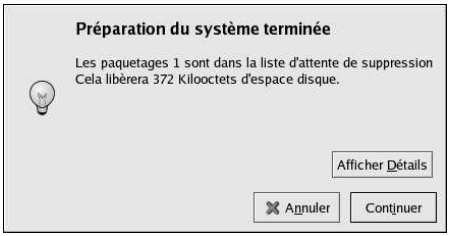

Figure 33-4. Récapitulatif de la suppression des paquetages

Cliquez sur **Continuer** pour lancer le processus de suppression. Une fois ce processus terminé, un message **Mise à jour terminée** s'affiche.

Astuce

Vous pouvez associer l'installation ainsi que la suppression de paquetages en sélectionnant les groupes/paquetages à installer/supprimer puis en cliquant sur **Mettre à jour**. La fenêtre **Préparation du système terminée** affiche le nombre de paquetages devant être installés et supprimés.

Chapitre 34.

Red Hat Network

Red Hat Network est une solution Internet pour la gestion d'un ou plusieurs système(s) Red Hat Linux. Toutes les alertes de sécurité, de correction de bogues et d'amélioration (connues sous le nom d'alertes d'errata) peuvent être directement téléchargées de Red Hat en utilisant l'application indépendante **Agent de mise à jour Red Hat** ou via le site Web de RHN à l'adresse suivante: http://rhn.redhat.com/.

Figure 34-1. Votre RHN

Red Hat Network fait économiser du temps aux utilisateurs de Red Hat Linux car ces derniers reçoivent un courrier électronique lorsque des paquetages sont publiés. Ils n'ont donc pas à rechercher sur le Web les mises à jour de paquetages ou les alertes de sécurité. Par défaut, Red Hat Network installe également les paquetages. Les utilisateurs n'ont donc ni à apprendre comment utiliser RPM, ni à se soucier de résoudre les dépendences des paquetages logiciels. RHN le fait à leur place.

Chaque compte Red Hat Network est accompagné des éléments suivants:

- Alertes d'errata — Vous êtes averti lorsque des alertes de sécurité, de correctifs de bogues et d'amélioration sont publiés pour tous les systèmes de votre réseau à travers l'interface Bases

Figure 34-2. Errata pertinente

- Notifications automatiques par courrier électronique — Recevez un courrier électronique lorsque une alerte d'errata est publiée pour votre système.
- Mises à jour d'errata programmées — Envoi programmé des mises à jour d'errata.
- Installation de paquetages — Programmez l'installation d'un paquetage sur un ou plusieurs systèmes avec un simple clic de souris.
- **Agent de mise à jour Red Hat** — utilisez l'**Agent de mise à jour Red Hat** pour télécharger les derniers logiciels pour votre système (avec une installation de paquetages facultatifs).
- Site Web de Red Hat Network — gérez plusieurs systèmes, téléchargez des paquetages individuels et programmez des actions telles que les mises à jour d'errata à partir de tout ordinateur grâce à un navigateur Web utilisant une connexion sécurisée.

Pour commencer à utiliser Red Hat Network, suivez les trois étapes principales décrites ci-dessous:

1. Créez un profile de système en utilisant l'une des méthodes suivantes:
   - Enregistrement du système avec RHN lors de l'utilisation de l' **Agent de paramétrage** au premier démarrage de votre système après l'installation.
   - Sélectionnez le bouton **Menu principal => Outils de système => Red Hat Network** sur votre bureau.
   - Exécutez la commande `up2date` à partir de l'invite du shell.

2. Connectez-vous à RHN à l'adresse http://rhn.redhat.com/ et enregistrez le système pour bénéficier d'une offre de services. Tous les utilisateurs reçoivent un compte Red Hat Network gratuit pour un système. Des comptes supplémentaires peuvent être achetés.

3. Commencez à programmer les mises à jour de votre système via le site Web de RHN ou téléchargez et installez les mises à jour des errata à l'aide de l'**Agent de mise à jour Red Hat**.

Pour des informations plus détaillées, consultez le Guide de référence de l'utilisateur de Red Hat Network (*Red Hat Network User Reference Guide*) disponible à l'adresse suivante: http://www.redhat.com/docs/manuals/RHNetwork/.

Astuce

Red Hat Linux inclut l'**Outil de notification Red Hat Network**, une icône du paneau très pratique qui affiche des alertes visibles lorsqu'une mise à jour pour votre système Red Hat Linux est publiée. Pour de plus amples informations sur l'applet, rendez-vous à l'URL suivante: http://rhn.redhat.com/help/basic/applet.html

VI. Annexes

Cette section contient des instructions sur la manière de construire un noyau personnalisé à partir de fichiers source fournis par Red Hat, Inc.. Elle inclut également un chapitre sur le Gnu Privacy Guard, un outil pouvant être utilisé afin de securiser les communications.

Table des matières

Annexe A.
Création d'un noyau personnalisé

Les néophytes du système Linux se demandent souvent: "Pourquoi devrais-je construire mon propre noyau?". Étant donné les progrès réalisés en matière d'utilisation des modules de noyau, la meilleure réponse à cette question est sans doute: "Si vous ne savez pas pour quelle raison vous devriez construire votre propre noyau, vous n'avez probablement pas besoin de le faire."

Le noyau fournit avec Red Hat Linux et par le biais du système d'Errata de Red Hat Linux prend en charge la plupart du matériel moderne et des fonctions de noyau. Ainsi, la plupart des utilisateurs ne devrait pas avoir à le recompiler. Cette annexe est fournie à titre de guide pour les utilisateurs qui souhaitent recompiler leur noyau afin par exemple, d'obtenir des connaissances plus approfondies en la matière.

Afin de mettre à niveau le noyau à l'aide des paquetages de noyau distribués par Red Hat, Inc., reportez-vous au Chapitre 30.

Avertissement

La construction d'un noyau personnalisé n'est pas prise en charge par l'équipe d'assistance à l'installation de Red Hat Linux. Pour de plus amples informations sur la mise à niveau du noyau à l'aide du paquetage RPM distribué par Red Hat, Inc., reportez-vous au Chapitre 30.

A.1. Préparation en vue de la construction du noyau

Avant de construire un noyau personnalisé, il est extrêmement important de vous assurer que vous disposez bien d'une disquette de démarrage en mode de secours opérationnelle, juste au cas où une erreur serait commise. Afin de créer une disquette d'amorçage qui démarrera en utilisant le noyau actuellement en fonctionnement, exécutez la commande suivante:

```
/sbin/mkbootdisk `uname -r`
```

Après avoir créé la disquette, testez-la afin de vous assurez qu'elle peut bien amorcer le système.

Afin de recompiler le noyau, le paquetage `kernel-source` doit être installé. Entrez la commande

```
rpm -q kernel-source
```

pour vérifier si ce dernier est installé. Si ce n'est pas le cas, installez-le à partir des CD-ROM Red Hat Linux ou depuis le site FTP Red Hat qui se trouve à l'adresse suivante: ftp://ftp.redhat.com (une liste des sites miroirs est disponible à http://www.redhat.com/mirrors.html), ou Red Hat Network. Pour obtenir de plus amples informations sur l'installation de paquetages RPM, reportez-vous à la Partie V.

A.2. Construction du noyau

Les instructions contenues dans cette section se réfèrent à la création d'un noyau modularisé. Si vous souhaitez construire un noyau monolithique, reportez-vous à la Section A.3 pour obtenir une explication des différents aspects de la construction et de l'installation d'un noyau monolithique.

Remarque

Cet exemple utilise la version de noyau 2.4.20-2.47.1 (la version de noyau peut être différente). Pour identifier la version de votre noyau, entrez la commande `uname -r` et remplacez 2.4.20-2.47.1 par la version de noyau fournie par cette commande.

Pour construire un noyau personnalisé pour une architecture x86 (effectuez toutes les étapes suivantes en étant connecté en tant que super-utilisateur):

1. Ouvrez l'invite du shell et allez dans le répertoire `/usr/src/linux-2.4/`. Dorénavant, toutes les commandes doivent être exécutées à partir de ce répertoire.
2. Il est important d'avoir une arborescence source dont vous connaissez la condition lorsque vous vous lancez dans la construction d'un noyau. Il est par conséquent recommandé de commencer par la commande `make mrproper` afin de supprimer tous les fichiers de configuration et toutes les traces des constructions précédentes qui pourraient se trouver dans l'arborescence source. Si vous avez déjà un fichier de configuration nommé `/usr/src/linux-2.4/.config`, sauvegardez-le dans un répertoire différent avant d'exécuter cette commande et recopiez-le ensuite.
3. Il est recommandé d'utiliser comme point de départ, la configuration du noyau Red Hat Linux par défaut. Pour ce faire, copiez le fichier de configuration de l'architecture du système qui se trouve dans le répertoire `/usr/src/linux-2.4/configs/` dans `/usr/src/linux-2.4/.config`. Si le système a plus de quatre giga-octets de mémoire, copiez le fichier contenant le mot-clé `bigmem`.
4. Personnalisez ensuite les paramètres. Si le système X Window est disponible, la méthode recommandée consiste à utiliser la commande `make xconfig` pour exécuter la **Configuration du noyau Linux**.

Remarque

Pour pouvoir utiliser l'outil graphique avec la commande `make xconfig`, le paquetage `tk` fournissant la commande `wish`, doit être installé. Pour obtenir de plus amples informations sur l'installation de paquetages RPM, reportez-vous à la Partie V.

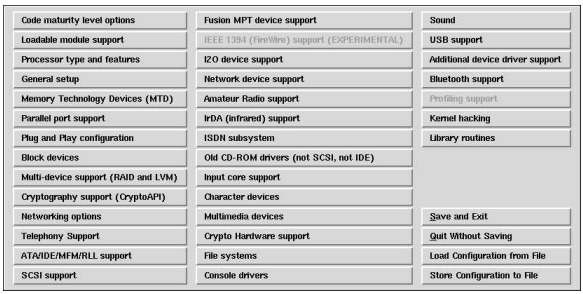

Figure A-1. Configuration des catégories de composants du noyau

Comme le montre la Figure A-1, cliquez sur la catégorie que vous souhaitez configurer. Chaque catégorie contient un certain nombre de composants. Effectuez votre choix en sélectionnant **y** (oui), **m** (module) ou **n** (non) à côté du composant à compiler dans le noyau puis compilez-le

ou non en tant que module du noyau. Pour plus d'informations sur le composant, cliquez sur le bouton **Aide** placé juste à côté.

Cliquez sur le bouton **Menu principal** pour afficher à nouveau la liste de catégories.

Après avoir terminé la configuration, cliquez sur le bouton **Enregistrer et quitter** dans la fenêtre du menu principal afin de créer le fichier de configuration `/usr/src/linux-2.4/.config` et de sortir du programme de **configuration du noyau Linux**.

Même si aucun changement n'a été apporté aux paramètres, il est nécessaire d'exécuter la commande `make xconfig` (ou l'une des autres méthodes utilisées pour la configuration du noyau) avant de continuer.

Parmi les autres méthodes utilisées pour la configuration du noyau figurent:

- `make config` — Un programme interactif en mode texte. Les composants sont présentés de façon linéaire et las résponses aux questions les concernant sont fournies sur une base individuelle. Cette méthode ne nécessite pas l'utilisation du système X Window et ne permet pas de revenir en arrière pour modifier les réponses apportées aux questions précédentes.
- `make menuconfig` — Un programme en mode texte piloté par des menus. Les composants sont présentés dans un menu de catégories spécifiques; sélectionnez les composants souhaités de la même manière que celle utilisée dans le programme d'installation Red Hat Linux en mode texte. Changez simplement l'étiquette correspondant à l'élément que vous souhaitez inclure: **[*]** (incorporé), **[ ]** (exclu), **<M>** (module) ou **< >** (module possible). Cette méthode ne requiert pas le système X Window.
- `make oldconfig` — Un script non-interactif qui modifie le fichier de configuration afin qu'il contienne les paramètres par défaut. Si votre système utilise le noyau Red Hat Linux par défaut, il crée un fichier de configuration pour le noyau livré avec Red Hat Linux pour votre architecture. Cela peut être utile lors de la configuration de votre noyau car vous pouvez ainsi connaître les composants par défaut et désactiver ceux que vous ne souhaitez pas utiliser.

Remarque

Pour utiliser `kmod` et les modules de noyau, répondez **`Yes`** à `kmod support` et `module version (CONFIG_MODVERSIONS) support` lors de la configuration.

5. Après avoir créé un fichier `/usr/src/linux-2.4/.config` utilisez la commande `make dep` pour définir correctement toutes les dépendances.
6. Utilisez la commande `make clean` pour préparer l'arborescence source en vue de la construction.
7. Il est recommandé de donner au noyau personnalisé un numéro de version différent afin d'éviter que le noyau existant ne soit écrasé. La méthode décrite ici est celle dont le dépannage est le plus simple en cas de problèmes. D'autres possibilités sont décrites en détail à l'adresse suivante: http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html ou dans `Makefile` dans `/usr/src/linux-2.4`.

   Par défaut, `/usr/src/linux-2.4/Makefile` comporte le mot `custom` à la fin de la ligne commençant par `EXTRAVERSION`. En ajoutant un élément à la chaîne, il est possible d'avoir simultanément sur le système l'ancien et le nouveau noyau, (version 2.4.20-2.47.1custom).

   Si le système contient plus d'un noyau personnalisé, il est recommandé d'ajouter la date à la fin (ou tout autre identificateur).
8. Construisez le noyau à l'aide de `make bzImage`.
9. Construisez les modules que vous avez configurés à l'aide de `make modules`.

10. Utilisez la commande `make modules_install` pour installer les modules de noyau (même si vous n'en avez construit aucun). Notez le caractère de soulignement (_) dans la commande pour donner l'instruction d'installer les modules de noyau dans le chemin du répertoire `/lib/modules/<KERNELVERSION>/kernel/drivers` (où *KERNELVERSION* correspond à la version spécifiée dans `Makefile`). Dans cet exemple, il s'agirait donc de `/lib/modules/2.4.20-2.47.1custom/kernel/drivers/`.

11. Utilisez `make install` pour copier votre nouveau noyau ainsi que les fichiers qui lui sont associés dans les répertoires appropriés.

    Outre l'installation des fichiers de noyau dans le répertoire `/boot`, cette commande exécute également le script `/sbin/new-kernel-pkg` qui construit une nouvelle image `initrd` et ajoute de nouvelles entrées au fichier de configuration du chargeur d'amorçage.

    Si votre système dispose d'un adaptateur SCSI que le pilote SCSI a été compilé en tant que module ou si le noyau a été construit avec une prise en charge ext3 en tant que module (la valeur par défaut de Red Hat Linux), l'image `initrd` est nécessaire.

12. Même si des modifications sont effectuées au niveau de l'image `initrd` et du chargeur d'amorçage, vérifiez d'une part qu'elles ont été faites correctement et assurez-vous d'autre part de bien utiliser la version personnalisée du noyau au lieu de 2.4.20-2.47.1. Pour obtenir des informations sur la manière de vérifier ces modifications, reportez-vous à la Section 30.5 et à la Section 30.6.

A.3. Construction d'un noyau monolithique

Les étapes relatives à la construction d'un noyau monolithique sont, à quelques exceptions près, les mêmes que celles que vous devez suivre pour la construction d'un noyau modulaire.

- Lors de la configuration du noyau, ne compilez rien en tant que module. Autrement dit, répondez uniquement **`Yes`** ou **`No`** aux questions. Vous devez également répondre **`No`** à `kmod support` et `module version (CONFIG_MODVERSIONS) support`.
- Ignorez les étapes suivantes:
  ```
  make modules
  make modules_install
  ```
- Modifiez la ligne `kernel` du fichier `grub.conf` en ajoutant `nomodules` ou modifiez le fichier `lilo.conf` de manière à ce qu'il inclue la ligne `append=nomodules`.

A.4. Ressources supplémentaires

Pour obtenir de plus amples informations sur le noyau Linux, veuillez vous reporter aux ressources ci-dessous.

A.4.1. Documentation installée

- `/usr/src/linux-2.4/Documentation` — Documentation avancée concernant le noyau Linux et ses modules. Ces documents sont destinés aux personnes souhaitant contribuer à l'élaboration du code source du noyau et comprenant le fonctionnement du noyau.

A.4.2. Sites Web utiles

- http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html — *The Linux Kernel HOWTO* (HOWTO du noyau Linux) du Projet de documentation Linux.
- http://www.kernel.org/pub/linux/docs/lkml/ — Liste de diffusion du noyau Linux.

redhat.

Annexe B.

Démarrer à l'aide de Gnu Privacy Guard

Ne vous êtes-vous jamais demandé si votre courrier électronique pouvait être lu par des personnes autres que vous et le destinataire lors de sa transmission? Malheureusement, il est effectivement possible que des personnes étrangères interceptent, voire manipulent vos messages.

Dans le courrier postal traditionnel, les lettres sont expédiées sous pli fermé et distribuées à leur destinataire après avoir transité par divers services postaux. L'envoi de courrier par Internet lui, est beaucoup moins sûr; le courrier électronique est le plus souvent transmis de serveur à serveur sous forme de texte non-crypté. Aucune mesure de précaution particulière n'est prise pour mettre votre correspondance à l'abri de l'interception ou de la modification par des personnes autres que le destinataire voulu.

Pour vous aider à protéger la confidentialité de vos communications, Red Hat Linux 9 inclut GnuPG ou *GNU Privacy Guard*, qui est installé par défaut au cours d'une installation Red Hat Linux classique. On se réfère souvent à cette application sous l'acronyme *GPG*.

GnuPG est un outil permettant de sécuriser les communications; il s'agit d'un outil de remplacement complet et gratuit de la technologie de cryptage de PGP ('Pretty Good Privacy', une application très utilisée). GnuPG vous permet non seulement de crypter vos données et votre correspondance mais également d'authentifier vos envois en *signant numériquement* votre travail. GnuPG peut également décrypter et vérifier les fichiers PGP.5.*x*.

Du fait que GnuPG est compatible avec d'autres normes de cryptage, votre correspondance sécurisée sera probablement compatible avec des applications de courrier électronique fonctionnant sur d'autres plates-formes, telles que Windows et Macintosh.

GnuPG utilise la technique de *cryptographie à clé publique* pour sécuriser l'échange de données. Ce système génère deux clés: une clé publique et une clé privée. Vous pouvez échanger votre clé publique avec des correspondants ou avec un serveur de clés, mais ne révélez jamais votre clé privée.

Le cryptage dépend de l'utilisation de clés. Dans le cas de la cryptographie conventionnelle ou symétrique, les deux extrémités de la transaction ont la même clé, qu'elles utilisent pour décoder leurs transmissions mutuelles. Dans le système de cryptographie à clé publique, deux clés coexistent: une clé publique et une clé privée. Les personnes ou les organisations gardent leur clé privée secrète et publie leur clé publique. Les données codées à l'aide de la clé publique ne peuvent être décodées qu'avec la clé privée; les données codées avec la clé privée ne peuvent être décodées qu'avec la clé publique.

Important

Rappelez-vous que votre clé publique peut être donnée à tout correspondant avec lequel vous voulez communiquer de façon sécurisée, mais vous ne devez jamais révéler votre clé privée.

Pour l'essentiel, la cryptographie dépasse la portée de cette documentation; des volumes entiers ont déjà été écrits sur le sujet. Nous espérons cependant que ce chapitre vous apportera une compréhension suffisante du fonctionnement de GnuPG pour vous permettre de commencer à utiliser la cryptographie dans votre propre correspondance. Pour plus d'informations sur GnuPG, PGP et la technologie de cryptage, reportez-vous à la Section B.8.

B.1. Fichier de configuration

La première fois que vous exécutez une commande GnuPG, un répertoire `.gnupg` est créé dans votre répertoire personnel (home). Avec la version 1.2, le nom du fichier de configuration a changé de `.gnupg/options` à `.gnupg/gpg.conf`. Si le fichier de configuration `.gnupg/gpg.conf` ne se trouve pas dans votre répertoire personnel, `.gnupg/options` sera utilisé. Si vous utilisez la version 1.2 ou une version supérieure, il est recommandé de changer le nom de votre fichier de configuration à l'aide de la commande suivante:

```
mv ~/.gnupg/options ~/.gnupg/gpg.conf
```

Si vous effectuez une mise à niveau à partir d'une version antérieure à 1.0.7, vous pouvez créer des caches de signatures dans votre porte-clés afin de réduire le temps d'accès de ce dernier. Afin d'effectuer cette tâche, exécutez la commande suivante une seule fois:

```
gpg --rebuild-keydb-caches
```

B.2. Messages d'avertissement

Lorsque vous exécuterez des commandes GnuPG, vous verrez probablement le message suivant:

```
gpg: Warning: using insecure memory!
```

Le fait que les utilisateurs qui ne sont pas root ne puissent pas verrouiller les pages mémoire est à l'origine de cet avertissement. S'ils pouvaient le faire, ils pourraient exécuter un refus d'attaques de service (Dos) sans mémoire; il s'agit donc d'un problème possible de sécurité. Pour plus d'informations, reportez-vous à l'adresse suivante: http://www.gnupg.org/(en)/documentation/faqs.html#q6.1.

Il se peut aussi que le message suivant apparaisse:

```
gpg: WARNING: unsafe permissions on configuration file "/home/username/.gnupg/gpg.conf"
```

Cet avertissement apparaît si les permissions de fichier de votre fichier de configuration autorisent de tierces personnes de le lire. Si cet avertissement s'affiche, il est recommandé d'exécuter la commande suivante afin de changer les permissions de fichier:

```
chmod 600 ~/.gnupg/gpg.conf
```

Le message suivant est un autre message d'avertissement courant:

```
gpg: WARNING: unsafe enclosing directory permissions on configuration file
"/home/username/.gnupg/gpg.conf"
```

Cet avertissement apparaît si les permissions de fichier du répertoire contenant le fichier de configuration autorisent de tierces personnes à lire son contenu. Si cet avertiseement s'affiche, il est recommandé d'exécuter la commande suivante afin de changer les permissions de fichier:

```
chmod 700 ~/.gnupg
```

Si vous avez effectué une mise à niveau à partir d'une ancienne version de GnuPG, il se peut que le message suivant s'affiche:

```
gpg: /home/username/.gnupg/gpg.conf:82: deprecated option "honor-http-proxy"
gpg: please use "keyserver-options honor-http-proxy" instead
```

Cet avertissement apparaît parce que votre fichier `~/.gnupg/gpg.conf` contient la ligne suivante:

```
honor-http-proxy
```

Pour la version 1.0.7 et les versions postérieures, il est préférable d'utiliser une syntaxe différente. Modifiez la ligne en question de la manière suivante:

```
keyserver-options honor-http-proxy
```

B.3. Création d'une paire de clés

Pour commencer à utiliser GnuPG, vous devez d'abord générer une nouvelle paire de clés: une clé publique et une clé privée.

Pour générer une paire de clés, à l'invite du shell, entrez la commande suivante:

```
gpg --gen-key
```

Comme vous travaillez la plupart du temps à partir de votre compte utilisateur, vous devriez exécuter cette action lorsque vous êtes connecté à votre compte utilisateur (et non pas en tant que root).

Le système affiche alors un écran d'introduction, comportant des options clé, y compris une option recommandée (l'option par défaut), semblable à l'exemple présenté ci-dessous:

```
gpg (GnuPG) 1.2.1; Copyright (C) 2002 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Please select what kind of key you want:
   (1) DSA and ElGamal (default)
   (2) DSA (sign only)
   (5) RSA (sign only)
Your selection?
```

La plupart des écrans vous offrant la possibilité de sélectionner des options indiquent l'option par défaut entre parenthèses. Pour l'accepter, appuyez simplement sur la touche [Entrée].

Dans le premier écran, vous devez accepter l'option par défaut: `(1) DSA and ElGamal`. Cette option vous permet de créer une signature numérique et d'utiliser deux techniques pour le cryptage et le décryptage. Entrez **1** puis appuyez sur la touche [Entrée].

Choisissez ensuite la taille de la clé ou sa longueur. Généralement, plus la clé est longue, plus elle protégera vos messages contre d'éventuelles attaques. La taille par défaut, 1024 bits, devrait suffire pour la protection de la plupart des utilisateurs; par conséquent, appuyez sur la touche [Entrée] pour accepter cette valeur.

L'étape suivante consiste à spécifier la durée de validité de votre clé. La valeur par défaut (`0 = key does not expire`) - aucune limite de validité - convient habituellement. Si, toutefois, vous choisissez une date d'expiration, n'oubliez pas d'en avertir les personnes avec qui vous avez échangé votre clé publique et de leur fournir une nouvelle clé. Si vous ne choisissez pas de date d'expiration, on vous demandera de confirmer votre décision. Appuyez sur la touche [y] pour confirmer votre décision.

Vous devez ensuite fournir un identificateur d'utilisateur qui comprend votre nom, votre adresse électronique et un commentaire optionnel. Lorsque vous avez terminé, le système affiche un résumé des informations fournies.

Après avoir accepté vos choix, vous devez entrer une phrase-mot de passe (ou phrse d'accès).

Tip

Tout comme les mots de passe de vos comptes, une bonne phrase-mot de passe est essentielle pour obtenir un niveau de sécurité optimal de GnuPG. Par exemple, alternez des majuscules et des minuscules dans votre phrase-mot de passe et insérez-y des chiffres ou des signes de ponctuation.

Les clés sont créées une fois la phrase-mot de passe entrée et vérifiée. Le système affiche alors un message semblable à celui-ci:

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++.+++++.++++++++....++++++++++..+++++.+++++.+++++++.+++++++
+++.++++++++++++++++++++++++++++++++++++++.........................++++
```

Lorsque le système a terminé, vos clés nouvellement créées sont placées dans le répertoire `.gnupg` de votre répertoire personnel. Pour afficher vos clés, utilisez la commande:

```
gpg --list-keys
```

Le résultat de cette commande ressemblera à l'extrait suivant:

```
/home/username/.gnupg/pubring.gpg
---------------------------------------
pub  1024D/B7085C8A 2000-06-18 Your Name <you@example.com>
sub  1024g/E12AF9C4 2000-06-18
```

Si vous avez utilisez la version 1.0.6 ou une version antérieure, pour créer une clé GnuPG, exporter votre clé privée et importer cette dernière dans la nouvelle clé, vous devez faire confiance à votre propre clé pour signer tout élément avec une version 1.0.7 ou une version postérieure. Pour ce faire, exécutez la commande suivante (remplacez <*user-id*>):

```
gpg --edit-key <user-id>
```

À l'invite `Command>` tapez **`trust`** et choisissez `5 = I trust ultimately` pour faire confiance à votre propre clé.

B.4. Création d'un certificat de révocation

Après avoir créé votre paire de clés, créez un certificat de révocation pour votre clé publique. Si vous oubliez votre phrase-mot de passe ou si quelqu'un la découvre, vous pourrez publier ce certificat afin d'informer d'autres utilisateurs que cette clé publique ne doit plus être utilisée.

Remarque

Générer un certificat de révocation n'équivaut pas à révoquer une clé que vous venez de créer. Vous ne faites que vous munir d'une solution sûre afin de pouvoir révoquer votre clé et la protéger de l'utilisation publique. Imaginons qu'après avoir créé une clé, vous oubliiez votre phrase-mot de passe, changiez de fournisseur d'accès Internet (et donc d'adresse) ou soyez victime d'une panne de disque dur. Ce certificat de révocation peut alors vous permettre de disqualifier votre clé publique.

Votre signature apparaîtra comme valide aux personnes ayant lu votre correspondance avant la révocation de la clé et vous serez en mesure de décrypter les messages reçus avant la révocation. Pour générer un certificat de révocation, utilisez l'option `--gen-revoke`:

```
gpg --output revoke.asc --gen-revoke  <you@example.com>
```

Notez que si vous omettez l'option `--output revoke.asc` ci-dessus, votre certificat de révocation sera retourné à la sortie standard, à savoir votre écran. Même si vous pouvez copier et coller le contenu de la sortie dans un fichier de votre choix à l'aide d'un éditeur de texte, il est probablement plus simple d'envoyer la sortie à un fichier se trouvant dans votre répertoire de connexion. Vous pourrez de la sorte conserver le certificat en vue d'un usage ultérieur ou bien le déplacer vers un lecteur de disquette et le conserver en lieu sûr.

Le résultat ressemblera à l'extrait suivant:

```
sec  1024D/823D25A9 2000-04-26  Votre nom <you@example.com>

Create a revocation certificate for this key?
```

Appuyez sur la touche [Y] afin de créer un certificat de révocation pour la clé répertoriée. On vous demandera ensuite de fournir la raison de la révocation ainsi qu'une description (facultative). Après confirmation de la raison, entrez la phrase-mot de passe utilisée pour générer la clé.

Une fois votre certificat de révocation créé (`revoke.asc`), il est placé dans votre répertoire de connexion. Vous devriez le copier sur une disquette que vous conserverez en lieu sûr (si vous ignorez comment copier un fichier sur une disquette dans Red Hat Linux, reportez-vous au *Guide de démarrage de Red Hat Linux*.)

B.5. Exportation de votre clé publique

Pour que vous puissiez utiliser la cryptographie à clé publique, il faut que vos correspondants disposent d'une copie de votre clé publique. Pour envoyer cette clé à vos correspondants ou à un serveur de clés, vous devez l'*exporter*.

Pour exporter votre clé et l'afficher sur une page Web ou la coller dans un message électronique, entrez la commande suivante:

```
gpg --armor --export <you@example.com> > mykey.asc
```

Rien ne s'affiche parce que, en plus d'avoir exporté votre clé publique, vous avez redirigé la sortie vers un fichier appelé, par exemple, `maclé.asc`. (Sans l'ajout de `> maclé.asc`, la clé aurait été affichée comme sortie standard à l'écran.)

À présent, vous pouvez insérer le fichier `mykey.asc` dans un message électronique ou l'exporter vers un serveur de clés. Pour voir la clé, entrez `less maclé.asc` afin d'ouvrir le fichier dans un pager (tapez [q] pour quitter le pager). Le résultat devrait ressembler à l'extrait ci-dessous:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.1 (GNU/Linux)
Comment: For info see http://www.gnupg.org

mQGiBDkHP3URBACkWGsYh43pkXU9wj/X1G67K8/DSrl85r7dNtHNfLL/ewil10k2
q8saWJn26QZPsDVqdUJMOdHfJ6kQTAt9NzQbgcVrxLYNfgeBsvkHF/POtnYcZRgL
tZ6syBBWs8JB4xt5V09iJSGAMPUQE8Jpdn2aRXPApdoDw179LM8Rq6r+gwCg5ZZa
pGNlkgFu24WM5wC1zg4QTbMD/3MJCSxfL99Ek5HXcB3yhj+o0LmIrGAVBgoWdrRd
BIGjQQFhV1NSwC8YhN/4nGHWpaTxgEtnb4CI1wI/G3DK9olYMyRJinkGJ6XYfP3b
cCQmqATDF5ugIAmdditnw7deXqn/eavaMxRXJM/RQSgJJyVpbAO2OqKe6L6Inb5H
kjcZA/9obTm499dDMRQ/CNR92fA5pr0zriy/ziLUow+cqI59nt+bEb9nY1mfmUN6
```

```
SW0jCH+pIQH5lerV+EookyOyq3ocUdjeRYF/d2jl9xmeSyL2H3tDvnuE6vgqFU/N
sdvby4B2Iku7S/h06W6GPQAe+pzdyX9vS+Pnf8osu7W3j60WprQkUGF1bCBHYWxs
YWdoZXIgPHBhdWxnYWxsQHJlZGhhdC5jb20+iFYEExECABYFAjkHP3UECwoEAwMV
AwIDFgIBAheAAAoJEJECmvGCPSWpMjQAoNF2zvRgdR/8or9pBhu95zeSnkb7AKCm
/uXVS0a5KoN7J61/lvEwxl1poLkBDQQ5Bz+MEAQA8ztcWRJjW8cHCgLaE402jyqQ
37gDT/n4VS66nU+YItzDFScVmgMuFRzhibLblfO9TpZzxEbSF3T6p9hLLnHCQlbD
HRsKfh0eJYMMqB3+HyUpNeqCMEEd9AnWD9P4rQtO7Pes38sV0lX0OSvsTyMG9wEB
vSNZk+Rl+phA55r1s8cAAwUEAJjqazvk0bgFrwlOPG9m7fEeDlvPSV6HSA0fvz4w
c7ckfpuxg/URQNf3TJA00Acprk8Gg8J2CtebAyR/sP5IsrK5l1luGdk+l0M85FpT
/cen2OdJtToAF/6fGnIkeCeP1O5aWTbDgdAUHBRykpdWU3GJ7NS6923fVg5khQWg
uwrAiEYEGBECAAYFAjkHP4wACgkQkQKa8YI9JamliwCfXox/HjlorMKnQRJkeBcZ
iLyPH1QAoI33Ft/0HBqLtqdtP4vWYQRbibjW
=BMEc
-----END PGP PUBLIC KEY BLOCK-----
```

B.5.1. Exportation vers un serveur de clés

Si vous n'avez que quelques correspondants, vous pouvez exporter votre clé publique et la leur envoyer personnellement. En revanche, si vous correspondez avec de nombreuses personnes, la distribution de votre clé risque de prendre du temps. C'est là qu'interviennent les serveurs de clés.

Un serveur de clés est un répositoire Internet où vous pouvez déposer votre clé publique et à partir duquel vous pouvez la distribuer à toute personne qui en fait la demande. Il existe de nombreux serveurs de clés qui, pour la plupart, essaient de coordonner leurs activités; envoyer votre clé à l'un d'eux équivaut à la distribuer à tous. Il ne restera plus à votre correspondant qu'à demander votre clé publique à un serveur de clés, puis à l'importer vers son porte-clés. Il est ainsi prêt à effectuer des connexions sécurisées avec vous.

Astuce

Comme la plupart des serveurs de clés sont synchronisés, l'envoi de votre clé publique à un seul d'entre eux équivaut à l'envoyer à tous. Vous pouvez cependant localiser différents serveurs. Pour un bon endroit pour commencer à rechercher des serveurs de clés et autres informations consultez la section *Keyserver.Net* disponible à l'adresse suivante: http://www.keyserver.net.

Vous pouvez envoyer votre clé publique depuis l'invite du shell ou depuis votre navigateur; vous devez bien sûr être en ligne pour pouvoir envoyer ou recevoir des clés d'un serveur de clés.

- À l'invite du shell, entrez les éléments suivants:
  `gpg --keyserver search.keyserver.net --send-key` *`vous@exemple.com`*
- Dans votre navigateur, connectez-vous à Keyserver.Net (http://www.keyserver.net) puis sélectionnez l'option vous permettant d'ajouter votre propre clé publique PGP.

  Votre tâche suivante consiste à copier et coller votre clé publique dans la zone appropriée de la page Web. Voici quelques indications afin de vous aider à le faire:

  - Ouvrez votre fichier de clé publique exporté (par exemple, *`maclé.asc`*, créé dans la Section B.5) à l'aide d'un pager — utilisez, par exemple, la commande `less maclé.asc`.
  - À l'aide de la souris, copiez le fichier en mettant en surbrillance toutes les lignes depuis `BEGIN PGP` jusqu'à `END PGP` (reportez-vous à la Figure B-1).
  - Collez le contenu du fichier *`maclé.asc`* dans la zone appropriée de la page de Keyserver.Net en cliquant avec le bouton du milieu de votre souris (ou bien avec les deux boutons si vous avez une souris à deux boutons). Cliquez ensuite sur le bouton **Soumettre** de la page du serveur de

clés (si vous commettez une erreur, cliquez sur le bouton **Ré-initialiser** de la page afin d'effacer la clé que vous avez collée).

Figure B-1. Copie de votre clé publique

Veuillez noter que si vous soumettez votre clé à un autre serveur de clés de type Web, la transaction ci-dessus sera sensiblement la même.

Vous n'avez rien d'autre à faire. Que vous utilisiez l'invite du shell ou le Web, vous verrez s'afficher un message vous informant que la soumission de votre clé a réussi — soit à l'invite du shell, soit sur le site Web du serveur de clés. Désormais, tous les utilisateurs qui souhaitent communiquer avec vous en toute sécurité peuvent importer votre clé publique et l'ajouter à leur porte-clés.

B.6. Importation d'une clé publique

L'autre opération impliquée par l'échange de clés est l'importation des clés publiques d'autres utilisateurs dans votre porte-clés —. Lorsque vous importez la clé publique de quelqu'un, vous pouvez décrypter ses messages et vérifier sa signature numérique par rapport à la clé publique correspondante de votre porte-clés.

L'une des manières les plus simples d'importer une clé consiste à la télécharger ou à l'enregistrer à partir d'un site Web.

Après avoir téléchargé une clé et l'avoir sauvegardée dans le fichier *clé.asc*, utilisez la commande suivante pour l'ajouter à votre porte-clés.

```
gpg --import key.asc
```

Une autre façon d'enregistrer une clé consiste à utiliser la fonction **Enregistrer sous**d'un navigateur. Si vous utilisez un navigateur tel que **Mozilla**, et localisez une clé sur un serveur de clés, vous pouvez enregistrer la page comme un fichier texte (sélectionnez **Fichier =>** puis **Enregistrer la page sous**). Dans la zone déroulante située près de **Type de fichier**, choisissez **Fichiers texte (*.txt)**. Vous pouvez ensuite l'importer — mais souvenez-vous du nom du fichier que vous avez enregistré. Par exemple, imaginons que vous ayez enregistré une clé sous forme de fichier texte appelé *nouvelle-clé.txt*. Pour importer le fichier, entrez les éléments suivants à l'invite du shell:

```
gpg --import nouvelle-clé.txt
```

Le résultat ressemblera à l'extrait suivant:

```
gpg: key F78FFE84: public key imported
gpg: Total number processed: 1
gpg:               imported: 1
```

Pour vérifier si cela a fonctionné, utilisez la commande `gpg --list-keys`; la clé que vous venez d'importer devrait être répertoriée dans votre porte-clés.

Lorsque vous importez une clé publique, vous ajoutez cette dernière à votre *porte-clés* (un fichier dans lequel les clés publiques et privés sont gardées). Ensuite, lorsque vous téléchargez un document ou fichier de cette entité, vous pouvez vérifier la validité de ce document par comparaison avec la clé que vous avez ajoutée à votre porte-clés.

B.7. Que sont les signatures numériques?

Les signatures numériques sont similaires aux signatures manuscrites. Toutefois, à la différence du courrier traditionnel, où quelqu'un peut toujours tenter d'imiter votre signature manuscrite, il est impossible de falsifier une signature numérique. Ceci résulte du fait que la signature est générée à l'aide de votre clé secrète unique et peut être vérifiée par le destinataire à l'aide de votre clé publique.

Une signature numérique date un document ; cela signifie essentiellement que l'heure à laquelle vous avez signé le document fait partie de la signature. Ainsi, si quelqu'un tente de modifier le document, la vérification de la signature échoue. Certaines applications de courrier électronique, telles que **Exmh** ou **KMail** de KDE, permettent de signer des documents à l'aide du GnuPG intégré à l'interface de l'application.

Les documents *signés clairement* et *signatures détachées* sont deux types de signatures numériques utiles. Les deux solutions offrent, techniquement, la même sécurité quant à l'authenticité du message, sans que le destinataire ait à décrypter le message tout entier.

Dans le cas d'un message clairement signé, votre signature apparaît comme un bloc de texte dans le cadre de votre lettre; en revanche, une signature détachée est envoyée comme fichier séparé avec votre correspondance.

B.8. Ressources supplémentaires

La technologie du cryptage va bien au-delà de ce nous pouvons couvrir dans cette présentation de GnuPG. Ci-dessous figurent d'autres sources de renseignements qui vous permettront de compléter vos connaissances sur le sujet.

B.8.1. Documentation installée

- `man gpg` et `info gpg` — Petit guide de référence des commandes et options GnuPG.

B.8.2. Sites Web utiles

- http://www.gnupg.org — le site Web de GnuPG contient des liens vers les versions les plus récentes de GnuPG, un manuel utilisateur exhaustif et d'autres ressources en matières de cryptage.

- http://hotwired.lycos.com/webmonkey/backend/security/tutorials/tutorial1.html — Consultez le 'cours de cryptage', *Encryption Tutorial* du site Webmonkey pour en savoir plus sur le cryptage et la manière d'appliquer les techniques de cryptage.
- http://www.eff.org/pub/Privacy — La fondation Electronic Frontier Foundation et ses archives sur la protection de la vie privée, la sécurité, le cryptage et la surveillance, "Privacy, Security, Crypto, & Surveillance".

B.8.3. Livres sur le sujet

- *The Official PGP User's Guide* de Philip R. Zimmerman; MIT Press
- *PGP: Pretty Good Privacy* de Simson Garfinkel; O'Reilly & Associates, Inc.
- *E-Mail Security: How to Keep Your Electronic Messages Private* de Bruce Schneier; John Wiley & Sons

Index

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Colophon

Les guides Red Hat Linux sont écrits sous format DocBook SGML v4. Les formats HTML et PDF sont produits à l'aide de feuilles de style DSSSL personnalisées et de scripts de wrapper jade personnalisés. Les fichiers DocBook SGML sont écrits avec **Emacs** avec l'aide du mode PSGML.

Garrett LeSage a créé les graphiques d'admonition (remarque, astuce, important, attention et avertissement). Ils peuvent être librement redistribués avec la documentation Red Hat.

L'équipe de documentation de produits Red Hat Linux est composée des personnes suivantes:

Sandra A. Moore — Rédaction/Conception du *Guide d'installation de x86 Red Hat Linux*; Contribution à la rédaction du *Guide de démarrage de Red Hat Linux*

Tammy Fox — Rédaction/Conception du *Guide de personnalisation de Red Hat Linux*; Contribution à la rédaction du *Guide de démarrage de Red Hat Linux*; Rédaction/Conception des feuilles de style et des scripts DocBook personnalisés

Edward C. Bailey — Rédaction/Conception du *Guide d'administration système de Red Hat Linux*; Contribution à la rédaction du *Guide d'installation de x86 Red Hat Linux*

Johnray Fuller — Rédaction/Conception du *Guide de référence de Red Hat Linux*; Co-rédaction/Co-conception du *Guide de sécurité de Red Hat Linux*; Contribution à la rédaction du *Guide d'administration système de Red Hat Linux*

John Ha — Rédaction/Conception du *Guide de démarrage de Red Hat Linux*; Co-rédaction/Co-conception du *Guide de sécurité de Red Hat Linux*; Contribution à la rédaction du *Guide d'administration système de Red Hat Linux*

Jean-Paul Aubry — Traduction du *Guide d'installation de x86 Red Hat Linux*. Traduction du *Guide de démarrage de Red Hat Linux*. Traduction du *Guide de personnalisation de Red Hat Linux*. Traduction du *Guide de référence de Red Hat Linux*.