SUSE LINUX

GUIDE DE L'ADMINISTRATEUR

10. Édition 2004

Pour toute remarque ou commentaire, veuillez contacter `documentation@suse.de`.

Auteurs:	Stefan Behlert, Frank Bodammer, Stefan Dirsch, Olaf Donjak, Roman Drahtmüller, Torsten Duwe, Thorsten Dubiel, Thomas Fehr, Stefan Fent, Werner Fink, Kurt Garloff, Carsten Groß, Joachim Gleißner, Andreas Grünbacher, Franz Hassels, Andreas Jaeger, Klaus Kämpf, Hubert Mantel, Lars Marowsky-Bree, Johannes Meixner, Lars Müller, Matthias Nagorni, Anas Nashif, Siegfried Olschner, Peter Pöml, Thomas Renninger, Heiko Rommel, Marcus Schäfer, Nicolaus Schüler, Klaus Singvogel, Hendrik Vogelsang, Klaus G. Wagner, Rebecca Walter, Christian Zoz
Traduction:	Bureau Cornavin, Marlies Kierstaedter, Patricia Vaz
Rédaction:	Jörg Arndt, Antje Faber, Karl Eichwalder, Berthold Gunreben, Roland Haidl, Jana Jaeger, Edith Parzefall, Ines Pozo, Thomas Rölz, Thomas Schraitle
Mis en page:	Manuela Piotrowski, Thomas Schraitle
Typographie:	DocBook-XML, LaTeX

Ce livre a été imprimé sur papier blanchi sans aucune addition de chlore.

Table des matières

Bienvenue

Félicitations pour votre nouveau système d'exploitation LINUX et merci beaucoup d'avoir choisi SUSE LINUX 9.2.

L'achat de cette version vous donne droit à l'assistance technique à l'installation par téléphone et courrier électronique. Sur le portail SUSE LINUX (`http://portal.suse.com`), activez votre compte assistance à l'aide du code imprimé sur l'emballage de vos CD-ROM.

Afin que votre système reste toujours à la pointe de la technologie, nous vous conseillons de procéder à une mise à jour régulière à l'aide du confortable *YaST Online Update*. En addition, nous vous proposons eNewsletter, un service gratuit qui vous envoie des insformations relatives à la sécurité ainsi que des trucs et astuces pour l'utilisation de SUSE LINUX. Il vous suffit d'entrer votre adresse de courrier électronique sur `http://www.suse.com/us/private/newsletter.html`

Le *Guide de l'administrateur* SUSE LINUX vous apporte des informations générales sur le fonctionnement de votre système SUSE LINUX. Depuis les principes de base des systèmes de fichiers, la configuration du noyau et les processus d'amorçage jusqu'à l'installation d'un serveur Web Apache et à la mise en place d'une authentification sécurisée, cet ouvrage a pour objectif de vous initier à l'administration système Linux. Ce *Guide de l'administrateur* SUSE LINUX se divise en cinq parties principales :

Installation L'installation et la configuration d'un système avec YaST, des détails relatifs à des variantes d'installation spéciales, au gestionnaire de volumes logiques (LVM) et à la configuration RAID, aux mises à jour et à la réparation du système.

Système Caractéristiques principales d'un système SUSE LINUX, détails relatifs au noyau, à l'amorçage et au processus init, configuration du gestionnaire d'amorçage et du système X Window, utilisation d'une imprimante et travail mobile sous Linux.

Services Intégration dans un réseau (hétérogène), installation d'un serveur Web Apache, synchronisation des fichiers et aspects liés à la sécurité.

Administration Systèmes de fichiers ACL (listes de contrôle d'accès) et outils importants pour la surveillance du système.

Apendices Sources d'information importantes relatives à Linux et glossaire.

Vous trouverez les versions numériques des manuels SUSE LINUX dans le répertoire `file:///usr/share/doc/manual/`.

Nouveautés dans le manuel de l'administrateur

Voici les modifications qui ont été apportées à la version précédente de ce manuel (SUSE LINUX 9.1) :

- Toute le processus d'installation et de configuration avec YaST décrit auparavant dans le *Guide de l'utilisateur* est maintenant expliqué dans les deux premiers chapitres de ce manuel (voir chapitres *Installation avec YaST* page 7 et *Configuration du système avec YaST* page 45).
- Le chapitre *Réparation du système YaST* a également été transféré du *Guide de l'utilisateur* dans ce manuel (voir chapitre *Réparation du système* page 187).
- Le chapitre *Amorçage et chargeur d'amorçage* a été retravaillé et la description du module YaST a été augmentée (voir chapitre *Amorçage et chargeur d'amorçage* page 205).
- Le chapitre sur l'impression a été actualisé et restructuré (voir chapitre *Imprimante (utilisation)* page 291).
- Le chapitre *Travail mobile sous Linux* a été totalement réécrit (voir chapitre *Travail nomade sous Linux* page 315). *SCPM*, *PCMCIA* et *Communication sans fil* sont maintenant des chapitres à part entière et ont été révisés (voir chapitres *SCPM — System Configuration Profile Management* page 339, *PCMCIA* page 329 et *Communications sans fil* page 375).
- Le chapitre *Le système Hotplug* a été complètement réécrit (voir chapitre *Le système Hotplug* page 399).

- Le chapitre *Noeuds de périphériques dynamiques avec udev* a été ajouté (voir chapitre *Noeuds de périphériques dynamiques avec udev* page 409).
- Le chapitre *PAM – Pluggable Authentication Modules* est également nouveau (voir chapitre *PAM – Pluggable Authentication Modules* page 427).
- Le chapitre relatif au réseau contient une nouvelle section traitant de *SLP — Transmission de services dans le réseau* (voir chapitre *SLP — Transmission de services dans le réseau* page 484).

Conventions typographiques

Ce livre utilise les conventions typographiques suivantes :

- YaST : un nom de programme.
- `/etc/passwd` : un fichier ou un répertoire.
- ⟨*joker*⟩ : le symbole ⟨*joker*⟩ est à remplacer par sa valeur réelle.
- `PATH` : une variable d'environnement nommée PATH
- `ls` : une commande.
- `--help` : des options et paramètres.
- `utilisateur` : un utilisateur.
- Alt : une touche sur laquelle il faut appuyer.
- 'Fichier' : des éléments de menu, des boutons.
- "Processus tué" : des messages du système.

Remerciement

Les développeurs de Linux font avancer le devenir de Linux dans le cadre d'une collaboration mondiale axée sur le bénévolat. Nous les remercions pour leur engagement – cette distribution n'aurait pu voir le jour sans eux. Nous souhaitons aussi tout spécialement remercier Frank Zappa et Pawar.

Et bien entendu, un grand merci à LINUS TORVALDS !

Have a lot of fun !

Votre équipe SUSE

Première partie

Installation

Installation avec YaST

Ce chapitre vous décrit, étape par étape, l'installation de votre système SUSE LINUX avec YaST, l'assistant du système SUSE LINUX. Vous apprendrez comment préparer le processus d'installation et vous obtiendrez des informations relatives aux différentes étapes de l'installation qui vous faciliteront vos prises de décisions lors de la configuration.

1.1 Amorçage du système pour l'installation

Insérez le premier CD-ROM ou le DVD de SUSE LINUX dans le lecteur et redémarrez votre machine. Le programme d'installation de SUSE LINUX sera alors chargé depuis le CD/DVD et l'installation commencera.

1.1.1 Possibles problèmes lors de l'amorçage depuis le CD/DVD

Les possibilités d'amorcer votre ordinateur dont vous disposez dépendent du matériel utilisé. Si votre ordinateur n'amorce pas depuis le CD 1, cela peut être dû à différentes causes :

Votre lecteur de CD ROM ne peut pas lire l'image d'amorçage (*bootimage*) du premier CD. Dans ce cas, utilisez le CD 2 pour amorcer le système. Dans ce deuxième CD, vous trouverez une image d'amorçage conventionnelle de 2,88 Mo, que même les lecteurs obsolètes peuvent lire.

Votre lecteur de CD-ROM n'est pas supporté parce qu'il s'agit d'un lecteur relativement ancien. Dans ce cas, il devrait tout de même être possible d'amorcer depuis le CD et de procéder à l'installation en réseau.

La séquence d'amorçage de l'ordinateur n'est pas configurée correctement dans le BIOS (*Basic Input Output System*). Vous trouverez les informations nécessaires à la modification de la configuration du BIOS dans la documentation de votre carte mère ou dans la section ci-après.

Le BIOS est un programme avec lequel il est possible d'amorcer les fonctions de base de l'ordinateur. Les constructeurs de cartes mères mettent à votre disposition un BIOS spécialement adapté à votre système.

L'accès au setup du BIOS ne peut se produire qu'à un moment bien précis : lors de l'amorçage de l'ordinateur, certains diagnostiques du matériel sont effectués comme, par exemple, le contrôle de la mémoire de travail. À ce moment, la touche à presser pour entrer dans le setup du BIOS apparaîtra dans la partie inférieure de l'écran ou dans la dernière ligne affichée. Généralement, il s'agit des touches Del, F1 ou Esc. Pressez la touche correspondante jusqu'à ce que le setup du BIOS apparaisse.

Une fois le setup du BIOS démarré, modifiez la séquence d'amorçage comme suit : s'il s'agit d'un AWARD BIOS, cherchez l'entrée 'BIOS FEATURES SETUP'.

D'autres constructeurs emploient des entrées similaires comme, par exemple, 'ADVANCED CMOS SETUP'. Sélectionnez l'entrée correspondante et confirmez en pressant (Return).

Pour procéder à la modification de la séquence d'amorçage, c'est la sous-option 'BOOT SEQUENCE' qui est importante. La séquence par défaut est souvent 'C, A' ou 'A, C'. Dans le premier cas, lors de l'amorçage, l'ordinateur recherche tout d'abord le système d'exploitation sur le disque dur (C) et ensuite dans le lecteur de disquettes (A). Pressez la touche (Page précédente) ou (Page suivante) aussi longtemps que nécessaire pour voir apparaître la séquence 'A,CDROM,C'.

Quittez la configuration en pressant la touche (Esc). Sélectionnez 'SAVE & EXIT SETUP' ou pressez la touche (F10) pour enregistrer vos modifications. Confirmez vos modifications en pressant la touche (Y).

Si vous possédez un lecteur de CD-ROM SCSI et que celui-ci est connecté, par exemple, à un adaptateur hôte Adaptec, vous devrez faire appel au BIOS de l'adaptateur par la combinaison de touches (Strg)-(A). Sélectionnez 'Disk Utilities' pour que le système affiche une liste du matériel. Prenez note de l'ID SCSI de votre lecteur de CD-ROM. Quittez le menu en pressant la touche (Esc) pour ouvrir ensuite 'Configure Adapter Settings'. Sous 'Additional Options', vous trouverez le sous-menu 'Boot Device Options'. Sélectionnez ce menu et pressez la touche (Return). Tapez maintenant l'ID de votre lecteur de CD-ROM et pressez de nouveau la touche (Return). En pressant deux fois la touche (Esc), vous reviendrez à l'écran de démarrage du BIOS SCSI que vous quitterez après avoir confirmé avec 'Yes' pour ☞*amorcer* votre ordinateur à nouveau.

1.1.2 Autres possibilités d'amorçage

Outre l'amorçage à partir du CD ou du DVD, vous disposez d'autres possibilités d'amorçage. Celles-ci sont surtout intéressantes lorsque des difficultés apparaissent lors de l'amorçage depuis le CD ou le DVD.

TAB. *1.1:* *Options d'amorçage*

Option d'amorçage	Application
CD-ROM	Ceci est la possibilité d'amorçage la plus simple. Dans ce cas, le système a besoin d'un lecteur de CD-ROM disponible pris en charge par Linux.

Disquette	Vous trouverez sur le premier CD, dans le répertoire `/boot/`, les images nécessaires pour créer une disquette d'amorçage. Consultez le `README` dans ce même répertoire.
PXE ou bootp	Cela doit supporté par le BIOS ou par le microprogramme (firmware) du système utilisé et un serveur d'amorçage doit être disponible dans le réseau. Cette tâche peut également être prise en charge par un autre système SUSE LINUX.
Disque dur	SUSE LINUX peut également amorcer depuis le disque dur. À cette fin, vous devez copier sur le disque dur le noyau (`linux`) et le système d'installation (`initrd`) du répertoire `/boot/loader` du premier CD et ajouter l'entrée correspondante dans le chargeur d'amorçage.

1.2 Écran d'accueil

L'écran d'accueil affiche les différentes possibilités d'installation avant de continuer l'exécution du programme. Dans la partie supérieure se trouve l'option 'Amorcer depuis le disque dur' qui amorce le système déjà installé. Étant donné qu'après l'installation, le CD est introduit pour installer d'autres logiciels, cette option est présélectionnée. Cependant, pour l'installation, sélectionnez 'Installation' à l'aide des touches de direction (flèches). YaST est alors chargé et l'installation commence. Les différentes options de l'écran d'accueil sont :

Amorcer depuis le disque dur Amorce le système déjà installé. Cette option est prédéfinie.

Installation L'installation normale dans laquelle toutes fonctions modernes du matériel sont activées.

Installation - ACPI désactivé Lorsque l'installation normale échoue, il est possible que l'ordinateur ne soit pas capable d'assurer correctement le support ACPI (*Advanced Configuration and Power Interface*). Dans ce cas, vous pouvez procéder à une installation sans support ACPI.

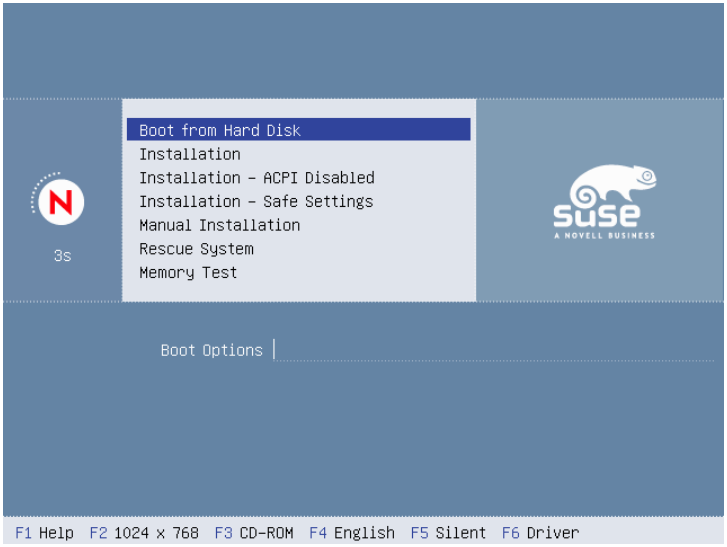


FIG. 1.1: *L'écran d'accueil*

Installation - Mode secure La fonction DMA (pour le lecteur CD-ROM) et les gestionnaires d'énergie problématiques sont désactivés. Les experts peuvent également entrer ou modifier des paramètres du noyau dans la ligne de saisie.

Installation manuelle Lorsque certains pilotes qui ont été chargés automatiquement lors du démarrage de l'installation posent des problèmes, vous pouvez effectuer l'installation manuellement, c'est à dire que les pilotes ne seront pas chargés automatiquement. Cependant, cette option ne fonctionne pas si vous utilisez un clavier USB avec votre ordinateur.

Système de secours Si vous n'avez plus accès au système Linux déjà installé, amorcez l'ordinateur depuis le DVD/CD1 et sélectionnez cette option. Ceci démarre un système de secours qui est en fait un système Linux minimal sans interface graphique mais avec un accès au disque dur pour experts qui vous permettra de réparer d'éventuelles erreurs dans le système installé. Si vous n'êtes pas encore très expérimenté, vous pouvez également utiliser l'outil de réparation du système de YaST. Vous trouverez des détails à ce sujet dans le chapitre *Réparation du système* page 187.

Test de mémoire Cette option vérifie la mémoire RAM de votre système au moyen de cycles répétés d'écriture et de lecture. Ce test est effectué sans fin, étant donné que les erreurs de mémoire se produisent de façon sporadique et ne peuvent être décelées qu'au travers de nombreux cycles d'écriture et de lecture. Si vous pensez que votre mémoire vive est défectueuse, effectuez ce test pendant plusieurs heures. Si aucune erreur n'a alors été signalée, vous pouvez être assuré que la mémoire est intacte. Mettez fin au test en réamorçant l'ordinateur.

Comme l'indique la barre de touches de fonction en bas de l'écran, vous pouvez, à l'aide de ces touches de fonction, procéder aux réglages de plusieurs paramètres pour l'installation.

(F1) Vous obtenez une aide contextuelle relative à l'élément activé de l'écran de démarrage.

(F2) Sélection de différents modes graphiques pour l'installation. Si des problèmes surviennent lors de l'installation graphique, vous pouvez sélectionner ici le mode textuel.

(F3) Normalement, l'installation est faite depuis le support de données inséré. Cependant, vous pouvez sélectionner ici d'autres sources d'installation telles que, par exemple, FTP ou NFS. *SLP* (Service Location Protocol) mérite une mention spéciale. Avec cette option, lors de l'installation dans un réseau avec un serveur SLP, l'un des différents supports d'installation disponibles sur ce serveur peut être sélectionné avant l'installation proprement dite. Vous trouverez plus d'informations relatives au protocole *SLP* à la section *SLP — Transmission de services dans le réseau* page 484.

(F4) Vous pouvez ici définir la langue pour l'écran de démarrage.

(F5) Normalement, lors du démarrage du système, vous ne voyez pas les messages de progression du noyau Linux mais une barre de progression. Si vous souhaitez voir ces messages, sélectionnez ici l'option 'Native' et si vous désirez des informations plus détaillées, sélectionnez 'Verbose'.

(F6) Si vous disposez d'une disquette de mise à jour des pilotes pour SUSE LINUX, vous pouvez l'utiliser ici. Lors de l'installation, il vous sera demandé d'insérer le support de mise à jour.

Lors de l'installation, quelques secondes après l'écran de démarrage, SUSE LINUX charge un ☞*système Linux* minimal qui contrôlera la suite du processus d'installation. Si vous avez sélectionné les modes d'affichage 'Native' ou 'Verbose', l'écran affiche maintenant de nombreux messages et mentions de copyright.

Le programme YaST est lancé à la fin du processus de chargement. Quelques secondes plus tard, vous voyez apparaître l'interface graphique.

C'est maintenant que commence l'installation proprement dite de SUSE LINUX. Tous les écrans de YaST suivent un schéma unifié. Les champs de saisie, les listes de sélection et les boutons des écrans de YaST sont tous accessibles à l'aide de la souris ou du clavier. Si le pointeur ne bouge pas, cela signifie que votre souris n'a pas été reconnue automatiquement. Utilisez dans ce cas le clavier.

1.3 Sélection de la langue

SUSE LINUX et YaST s'adressent à vous dans la langue que vous désirez. La langue que vous sélectionnerez ici s'appliquera aussi à votre disposition de clavier. En outre, YaST détermine une zone horaire par défaut en fonction de la langue que vous avez choisie. Vous pouvez modifier ces paramètres plus tard. Si, contre toute attente, votre souris ne fonctionnait pas, déplacez-vous, à l'aide des touches de direction (flèches), jusqu'à la langue que vous désirez puis pressez la touche (Tab) aussi longtemps qu'il sera nécessaire pour préactiver le bouton 'Suivant' et pressez ensuite la touche (Return).

1.4 Mode d'installation

Si vous avez déjà une version de SUSE LINUX installée sur votre machine, vous avez le choix entre une 'Nouvelle Installation' et une 'Mise à jour d'un système déjà existant'. Vous pouvez aussi décider de démarrer votre système existant avec 'Démarrer le système installé'. Si votre système installé ne démarrait pas, au cas où, par exemple, d'importants paramètres de configuration du système ont été détruits, vous pouvez utiliser l'option 'Réparation du système installé' pour tenter de régler le problème. Si vous n'avez encore installé aucun système SUSE LINUX, vous ne pourrez procéder, bien entendu, qu'à une nouvelle installation (fig. 1.3 page 15).

Le présent chapitre traite uniquement de la 'Nouvelle Installation'. Vous pourrez trouver plus d'informations au sujet de la mise à jour du système dans le chapitre *Mise à jour du système* page 60. Vous trouverez une description des possibilités de réparation du système dans le chapitre *Réparation du système* page 187.

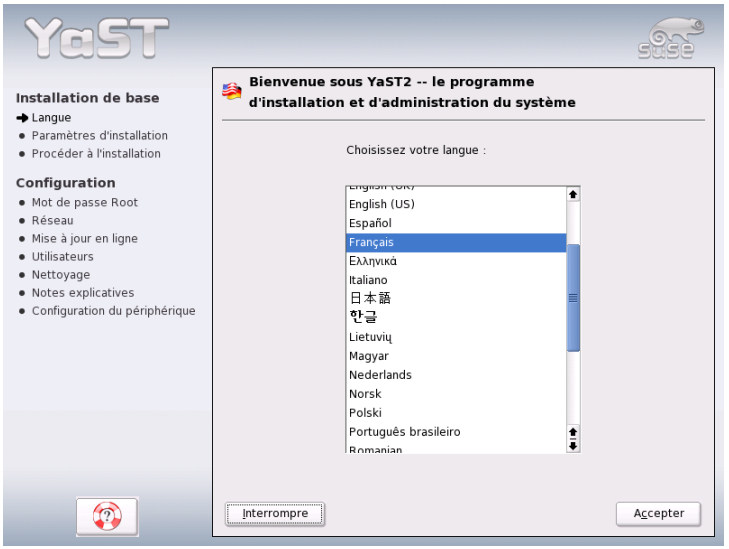


FIG. *1.2:* *Sélection de la langue*

1.5 Suggestions pour l'installation

À la fin du processus de détection du matériel, vous voyez s'afficher dans le dialogue de suggestions (voir figure 1.4 page 16) des informations sur le matériel détecté ainsi que des suggestions pour l'installation et le partitionnement. Si vous cliquez sur une option et effectuez ensuite une configuration, vous reviendrez toujours à cette fenêtre qui affichera les suggestions ainsi que les valeurs qui ont été modifiées. Les réglages que vous pouvez effectuer pour la configuration vont être décrits dans les paragraphes suivants.

1.5.1 Mode d'installation

Ici, vous avez encore la possibilité de changer le mode d'installation. Les choix possibles sont les mêmes que ceux décrits dans la section *Mode d'installation* page précédente.

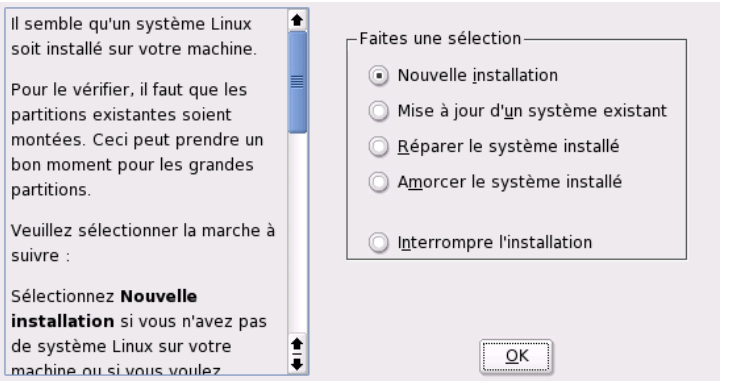


FIG. *1.3:* *Sélection du mode d'installation*

1.5.2 Disposition du clavier

Sélectionnez, dans ce masque, la disposition du clavier que vous désirez utiliser. Elle correspond en général à la langue que vous avez choisie. Tapez ensuite quelques touches, par exemple la lettre É ou la lettre À dans le champ de test afin de vérifier que les caractères accentués sont bien affichés. Cliquez sur 'Suivant', pour revenir au dialogue de propositions.

1.5.3 Souris

Si YaST n'a pas détecté automatiquement la souris, déplacez-vous tout d'abord à l'aide de la touche (Tab) jusqu'à ce que l'option 'Souris' soit marquée. Avec la touche d'espacement, vous obtiendrez l'affichage du masque de sélection du type de souris qui vous est présenté dans la figure 1.5 page 17.

Sélectionnez le type de la souris à l'aide des touches ↑ et ↓. Si vous possédez une documentation relative à votre souris, vous y trouverez une description de son type. Utilisez la combinaison de touches (Alt) + (T) pour sélectionner un type de souris temporairement pour procéder à un test. Si la souris ne réagit pas comme vous le souhaitez, sélectionnez un autre type à l'aide du clavier et procédez à un nouveau test. Utilisez les touches (Tab) et (Return) pour sélectionner la souris.

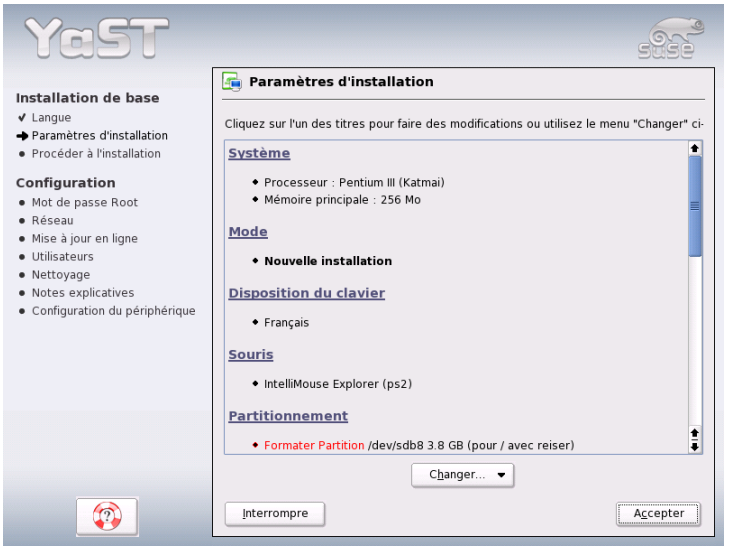


FIG. *1.4:* *Fenêtre de dialogue de suggestions*

1.5.4 Partitionnement

Dans la majorité des cas la proposition de partitionnement faite par YaST est judicieuse et vous pouvez l'accepter sans la modifier. Cependant, si vous souhaitez une distribution spéciale du disque dur, nous vous décrivons ci-après comment procéder.

Types de partition

Chaque disque dur contient une table des partitions qui a de la place pour quatre entrées. Chaque entrée dans la table des partitions peut être soit une partition primaire, soit une partition étendue. Cependant, il est impossible d'avoir plus d'*une* partition étendue.

Les partitions primaires sont très simples à considérer : elles sont constituées d'un domaine continu de cylindres (zones physiques du disque) auquel un système d'exploition est attribué. Cependant, vous ne pouvez créer que jusqu'à quatre partitions primaires par disque dur ; on ne peut pas en entrer plus sur la table des partitions.

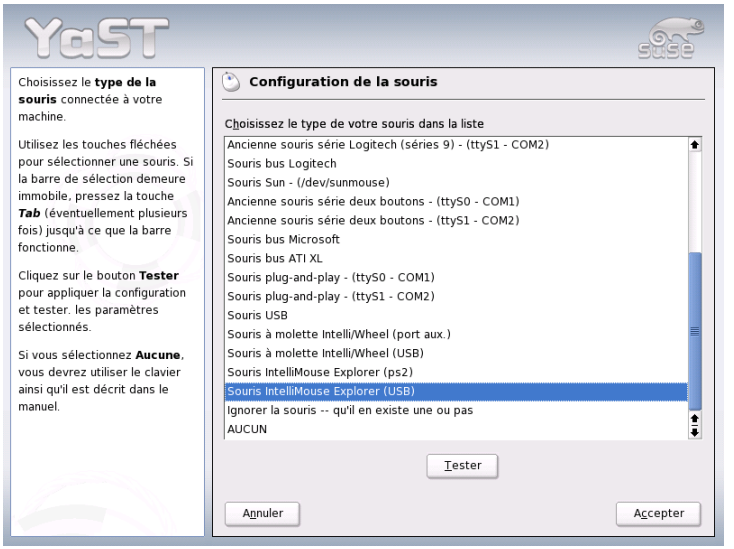


FIG. *1.5:* *Sélection de la souris*

Si vous avez besoin de plus de partitions, vous devrez créer une partition étendue. Une partition étendue est également constituée d'un domaine continu de cylindres du disque dur. Cependant, on peut encore diviser une partition étendue en plusieurs *partitions logiques*, qui, elles ne nécessitent aucune entrée dans la table des partitions. La partition étendue est, en quelque sorte, un container qui comprend les partitions logiques.

Si vous avez besoin de plus de quatre partitions, vous devez vous assurer, lors du partitionnement, qu'une des partitions, la quatrième en dernier lieu, est bien prédéfinie comme partition étendue afin de pouvoir lui attribuer l'ensemble des domaines de cylindres libres. Vous pourrez ensuite y définir autant de partitions logiques que vous le désirez (dans la limite de 15 partitions pour les disques SCSI, SATA et Firewire et de 63 partitions pour les disques (E)IDE).

Le type de partition (primaire ou logique) sur laquelle l'installation de SUSE LINUX est effectuée n'est pas important.

Conseils relatifs à l'espace mémoire

Si vous laissez YaST procéder au partitionnement du disque dur, vous n'aurez (pratiquement) pas à vous préoccuper des besoins en espace disque et du partitionnement du disque dur. Au cas où vous procèderiez vous-même au partitionnement de votre disque dur, nous vous donnons ici quelques conseils quant à l'espace nécessaire aux différents types de système.

Système minimal : 500 Mo Ce système n'a pas d'interface graphique (X11), c'est à dire que vous ne pouvez travailler que depuis la console. En outre, vous ne pouvez procéder qu'à l'installation des logiciels les plus élémentaires.

Système minimal avec interface graphique : 700 Mo
Ici, vous pouvez installer X11 et quelques applications.

Système standard : 2,5 Go Vous pouvez ici installer des interfaces graphiques modernes telles que KDEou GNOME ainsi que de "grandes" applications comme, par exemple, OpenOffice, Netscape ou Mozilla.

La distribution de l'espace disque dépend surtout de la façon dont vous souhaitez utiliser l'ordinateur, mais on peut définir quelques règles simples :

Jusqu'à environ 4 Go : une partition swap et une partition root (`/`). La partition root contient alors également les répertoires pour lesquels des partitions propres sont créées dans le cas de disques durs plus grands.

Plus de 4 Go : Swap, Root (1 Go) et une partition pour `/usr` (4 Go ou plus), une pour `/opt` (4 Go ou plus) et une pour `/var` (1 Go). Le reste de l'espace peut être utilisé pour `/home`.

Selon votre matériel, il peut être nécessaire de configurer une partition d'amorçage (boot) pour les fichiers d'amorçage et le noyau Linux au début du disque dur (`/boot`). Cette partition doit faire au moins 8 Mo ou un cylindre. En principe, si YaST suggère la configuration d'une telle partition, il est plutôt judicieux de créer une lors du partitionnement manuel. En cas de doute, il est plus sûr de créer une partion d'amorçage.

Vous devez songer que certaines applications, pour la plupart des programmes commerciaux, installeront leurs données sous `/opt`. Si nécessaire, pensez soit à prévoir une partition propre à `/opt`, soit à redimensionner la partition root pour qu'elle ait une taille suffisante. KDE et GNOME sont également situés dans le répertoire `/opt` !

Partitionnement avec YaST

Si vous avez sélectionné pour la première fois le partitionnement dans la fenêtre de dialogue de suggestions, le dialogue de partitionnement de YaST apparaît avec les réglages actuels. Vous avez la possibilité d'accepter, de modifier ou de rejeter complètement la suggestion qui vous est faite pour procéder à une nouvelle distribution de l'espace disque.

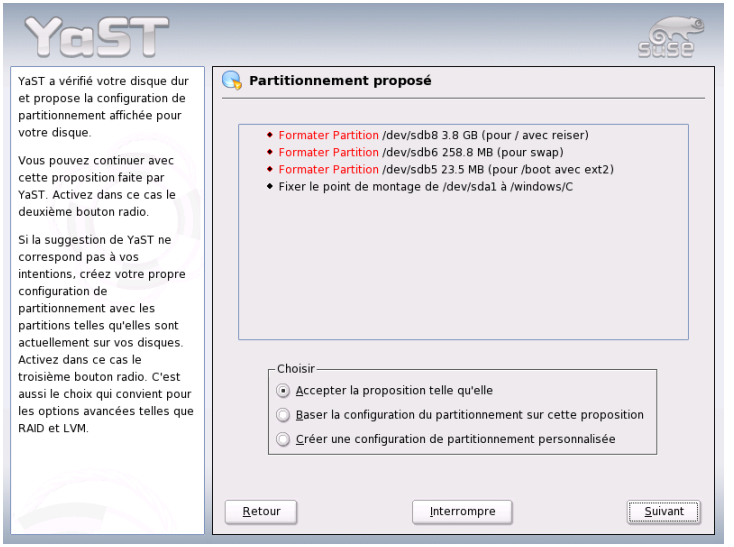


FIG. *1.6:* *Modifier la proposition de partitionnement*

Si vous sélectionnez 'Accepter la proposition de partitionnement', aucune modification ne sera effectuée et le dialogue de propositions restera tel quel. Si vous sélectionnez 'Changer la proposition de partitionnement', le dialogue pour experts apparaît directement et vous permet de procéder à des réglages très fins (voir section *Partitionnement pour experts avec YaST* page 21). La proposition de partitionnement de YaST est affichée dans ce dialogue et vous pouvez procéder à vos modifications.

Si vous sélectionnez 'Créer partitions personnalisées', un dialogue apparaît dans lequel vous pouvez sélectionner le disque dur (figure 1.7 page suivante). Tous les disques durs présents dans votre systèmes sont listés ici. Choisissez celui sur lequel vous désirez installer SUSE LINUX.

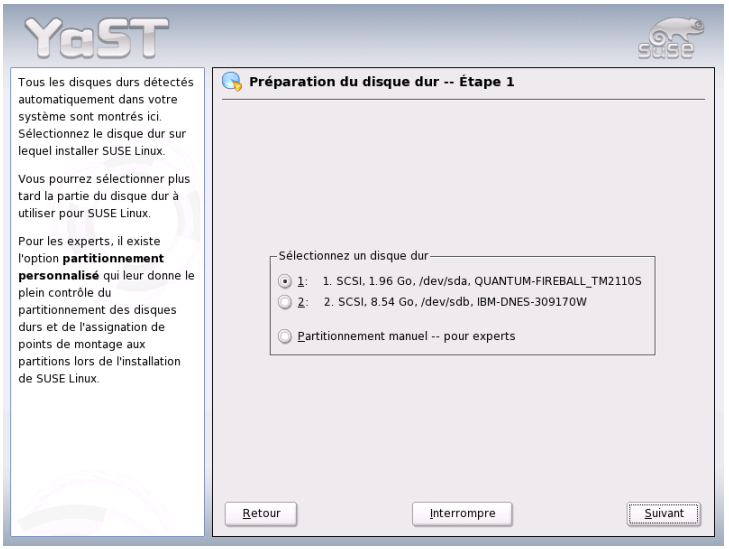


FIG. *1.7:* *Sélection du disque dur*

Après avoir sélectionné un disque dur, vous pouvez spécifier si 'Tout le disque' doit être utilisé ou si l'installation ne doit se faire que sur une des partitions (si une partition est disponible). Si le disque dur sélectionné contient déjà un système d'exploitation Windows, il vous sera demandé si vous voulez effacer votre système Windows ou réduire sa taille. Dans ce cas, lisez la section *Redimensionner une partition Windows* page 24. Dans le cas contraire, vous passerez également au dialogue pour experts dans lequel vous pourrez procéder au partitionnement que vous désirez (voir section *Partitionnement pour experts avec YaST* page ci-contre).

Attention

Définir tout le disque dur pour l'installation

Si vous sélectionnez 'Tout le disque' vous perdrez toutes les données présentes sur ce disque dur avant l'installation.

Attention

Au cours des prochaines étapes de l'installation, YaST vérifiera si l'espace disque est suffisant pour la sélection de logiciels actuelle. Si ce n'est pas le cas, la sélection de logiciels sera automatiquement modifiée et le dialogue de propositions vous en informera. Si vous disposez de suffisamment d'espace mémoire, YaST acceptera vos paramètres de configuration et partitionnera le disque dur en conséquence.

1.5.5 Partitionnement pour experts avec YaST

Dans le dialogue pour experts (figure 1.8), vous pouvez modifier manuellement le partitionnement d'un ou plusieurs disques durs. Vous avez la possibilité d'ajouter, de supprimer ou de modifier des partitions.

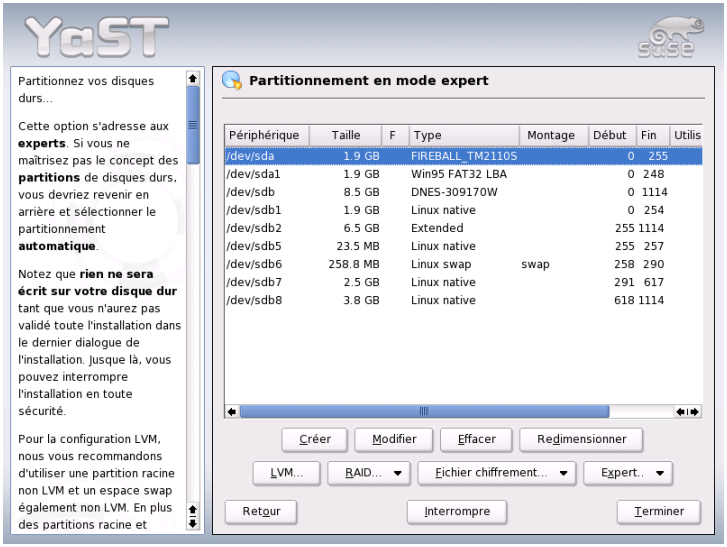


FIG. 1.8: *Le partitionneur de YaST en mode expert*

Le partitionneur établira une liste des disques durs et de toutes les partitions existantes ou proposées. Les disques dans leur intégralité sont représentés comme périphériques sans numéros (par exemple `/dev/hda` ou bien `/dev/sda`) alors que les partitions, en tant que parties de ces périphériques, sont numérotées (par exemple `/dev/hda1` ou bien `/dev/sda1`). La taille, le type, le système de fichiers et le point de montage de chaque disque et partition sont affichés.

Le point de montage indique l'emplacement de l'arborescence Linux où la partition a été rattachée.

De la même façon, l'espace libre sur le disque dur est affiché et sélectionné automatiquement. Si vous voulez attribuer plus d'espace de mémoire pour ☞*Linux* , vous pouvez, dans la liste, libérer des partitions en allant de bas en haut (c'est à dire de la dernière à la première ☞*Partition* d'un disque dur). Ainsi, il n'est pas possible de choisir, par exemple, la deuxième de trois partitions pour Linux et de laisser la première et la troisième pour un autre système d'exploitation.

Créer une partition

Sélectionnez 'Nouveau'. Si vous avez plusieurs disques durs, une fenêtre de dialogue dans laquelle vous pouvez marquer le disque dur sur lequel vous voulez créer la nouvelle partition. Ensuite, spécifiez le type de la partition (primaire ou étendue). Vous pouvez créer jusqu'à quatre partitions primaires ou trois partitions primaires et une partition étendue dans laquelle il vous est possible de créer plusieurs partitions logiques (à ce sujet, consultez le chapitre *Types de partition* page 16).

Sélectionnez maintenant le système de fichiers avec lequel la partition doit être formatée et, si nécessaire, un point de montage. YaST vous propose un point de montage pour chaque partition que vous créez. Vous trouverez des détails relatifs aux paramètres dans la section suivante.

Cliquez sur 'OK' pour que les modifications deviennent effectives. La nouvelle partition est alors ajoutée à la table des partitions. Si vous cliquez sur 'Suivant', les valeurs actuelles seront appliquées et la fenêtre de dialogue apparaîta à nouveau.

Paramètres de partitionnement

Lorsque vous créez une nouvelle partition dans l'arborescence des fichiers ou que vous modifiez une partition existante, vous pouvez définir différents paramètres. Dans le cas de nouvelles partitions, YaST se charge de fixer ces paramètres et normalement, vous n'aurez pas à faire de changement. Cependant, si vous souhaitez réaliser une configuration manuelle, procédez comme suit :

1. Selection de la partition
2. 'Modification' de la partition et réglage des paramètres :

Detection du système de fichiers Même si vous ne voulez pas formater la partition, vous devez ici indiquer au moins l'identificateur du système de fichiers. Les valeurs possibles sont, par exemple, 'Linux', 'Linux swap', 'Linux LVM' et 'Linux RAID'. Vous trouverez plus dans les sections *Configuration du gestionnaire de volumes logiques (LVM)* page 142 et *RAID logiciel* page 152.

Système de fichiers Si vous souhaitez formater la partition durant l'installation, vous pouvez indiquer ici le système de fichiers que doit avoir la partition. Les valeurs possibles sont, par exemple, 'Swap', 'Ext2', 'Ext3', 'ReiserFS' et 'JFS'. Vous trouverez des détails relatifs aux différents systèmes de fichiers à la section *Systèmes de fichiers sous Linux* page 415.

Swap est un format spécial qui convertit la partition en mémoire virtuelle. Chaque système doit avoir une partition swap d'au moins 128 Mo. ReiserFS est le système de fichiers par défaut pour les partitions Linux. ReiserFS, tout comme JFS et Ext3, est un système de fichiers avec journalisation (Journaling Filesystem). Un tel système de fichiers rétablit votre système très rapidement après un plantage éventuel, car la journalisation se fait durant le fonctionnement du système. En outre, ReiserFS est très efficace dans la gestion de grandes quantités de petits fichiers. Ext2 n'est pas un système de fichiers avec journalisation, mais il est très stable et particulièrement approprié pour les petites partitions, car il ne nécessite que peu d'espace disque pour sa propre gestion.

Options du système de fichiers Ici, vous pouvez configurer divers paramètres du système de fichiers sélectionné. Selon le système de fichiers utilisé, vous trouverez ici quelques propositions de configuration des paramètres pour experts.

Chiffrement d'un système de fichiers
Si vous activez le chiffrement, toutes les données de votre disque dur seront chiffrées. Ceci augmente le niveau de sécurité des données importantes, mais le système s'en trouve ralenti car ce processus de chiffrement requiert du temps. Vous trouverez plus d'informations relatives au chiffrement de systèmes de fichiers dans la section *Chiffrer les partitions et les fichiers* page 672.

Options fstab Ici, vous pouvez spécifier différents paramètres pour le fichier d'administration du système de fichiers (`/etc/fstab`).

Point de montage Ici est indiqué le répertoire de l'arborescence du système de fichiers dans lequel la partition doit être montée. Dans le champ de saisie correspondant, YaST vous fait plusieurs suggestions qui implémentent la structure par défaut lors de l'utilisation du système de fichiers sélectionné. Néanmoins, vous pouvez également entrer d'autres noms.

3. Cliquez sur 'Suivant' pour activer la partition.

Lorsque vous procédez manuellement à un partitionnement, vous devez créer une partition swap. La partition swap sert à libérer temporairement le disque dur des données non nécessaires en cet instant afin de toujours conserver la mémoire vive disponible pour les données les plus importantes et les plus utilisées.

Redimensionner une partition Windows

Si lors du partitionnement, vous avez sélectionné un disque dur avec une partition Windows FAT ou une partition Windows NTFS comme emplacement de l'installation, YaST vous offre la possibilité d'éliminer ou de réduire cette partition. De cette façon, vous pourrez installer aussi SUSE LINUX bien qu'il n'y ait pas suffisamment d'espace libre sur le disque dur. Ceci est particulièrement recommandable lorsqu'il n'existe, sur le disque dur, qu'une ☞*partition* contenant Windows, ce qui est souvent le cas sur les ordinateurs préinstallés.

Si YaST remarque que l'espace disponible sur le disque dur sélectionné est trop petit pour l'installation et que ce problème peut être solutionné en éliminant ou en réduisant une partition Windows, une fenêtre de dialogue apparaîtra dans laquelle vous pourrez sélectionner l'option souhaitée.

Si vous sélectionnez 'Supprimer Windows complètement', la partition Windows sera éliminée et l'espace libre ainsi gagné sera utilisée pour installer SUSE LINUX.

Attention

Effacer Windows

Si vous décidez d'éliminer Windows, notez que vous perdrez irrémédiablement toutes les données Windows lors du formatage.

Attention

Si vous décidez de réduire la partition Windows, interrompez d'abord l'installation puis amorcez Windows pour y procéder à certaines étapes préliminaires. Ceci n'est pas absolument nécessaire pour les partitions FAT, mais cela accélère

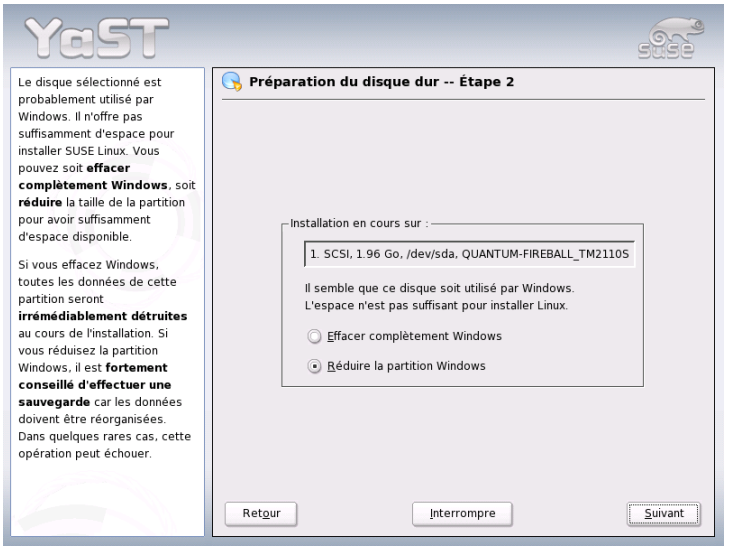


FIG. *1.9:* *Options possibles pour les partitions Windows*

le processus de réduction de la partition FAT et le rend plus sûr. Par contre, ces étapes sont nécessaires dans le cas des partitions NTFS.

Système de fichiers FAT Lancez, sous Windows, le programme scandisk pour vous assurez que le système de fichiers FAT est libre d'erreurs. Puis, déplacez les fichiers au début de la partition avec defrag. Ceci permet d'accélérer le processus de réduction de la partition sous Linux.

Si vous avez auparavant optimisé le fichier d'échange (swap) sous Windows en fixant la même limite supérieure et inférieure pour le fichier, vous devriez procéder à une étape supplémentaire. Dans ce cas, il se peut que, durant le processus de réduction, le fichier swap soit morcelé et dispersé sur l'ensemble de la partition Windows. En outre, le fichier swap devrait également être déplacé lors de ce processus ce qui le ralentirait encore plus. Ainsi, il est préférable d'annuler une telle optimisation avant la réduction pour la réaliser à nouveau par la suite.

Système de fichiers NTFS Ici aussi, exécutez scandisk puis defrag pour déplacer les fichiers au début de la partition. Contrairement au cas du système de fichiers FAT, avec le système NTFS, cette action *doit* être réalisée pour que la partition puisse être réduite.

Remarque

Réduire le fichier d'échange (swap) de Windows

Si vous utilisez votre système avec un fichier d'échange (swap) permanent sur un système de fichiers NTFS, il est possible que ce fichier soit situé à la fin du disque dur et y reste malgré l'exécution de defrag. Ceci peut avoir pour conséquence que la partition ne puisse pas être réduite suffisamment. Pour résoudre ce problème, désactivez temporairement le fichier swap (la mémoire virtuelle) dans Windows. Vous pourrez le réactiver après avoir réduit la partition.

Remarque

Une fois que vous aurez effectué ces préparatifs, sélectionnez l'option 'Redimensionner la partition Windows' dans le dialogue de partition. Après une rapide vérification, YaST ouvre une nouvelle fenêtre de dialogue et vous fait une suggestion pour une réduction raisonnable de votre partition Windows.

Dans le premier diagramme à barres, YaST montre l'espace occupé actuellement par Windows ainsi que l'espace encore disponible sur le disque dur. Le second diagramme vous fait une proposition pour le nouveau partitionnement du disque dur (figure 1.10 page suivante). Vous pouvez accepter ce nouveau partitionnement ou en modifier assez librement les limites avec le curseur.

Si vous quittez ce dialogue avec 'Suivant', la configuration actuelle sera enregistrée et vous retournerez au dialogue précédent. La réduction ne sera pas effectuée immédiatement, mais plus tard, juste avant le formatage du disque dur.

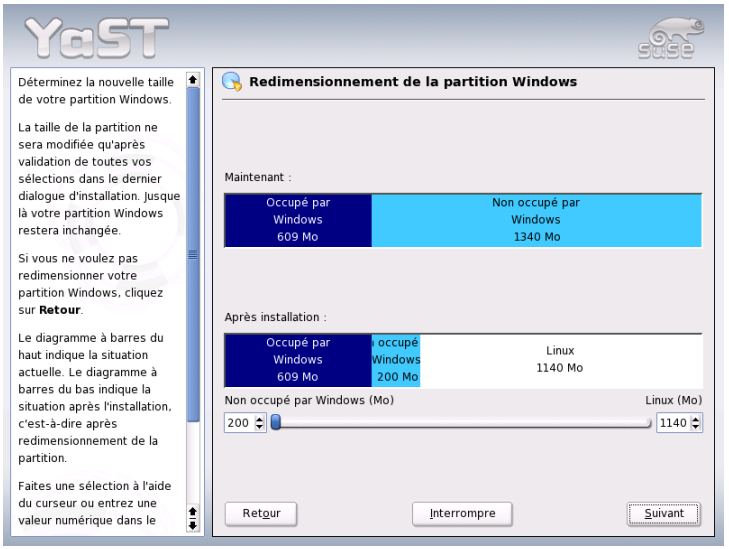


FIG. *1.10:* *Redimensionner une partition Windows*

Remarque

Windows avec système de fichiers NTFS

Par défaut, les versions NT, 2000 et XP de Windows utilisent le système de fichiers NTFS. À l'heure actuelle, Linux ne peut que lire un système de fichiers NTFS mais ne peut pas l'écrire comme c'est le cas pour les systèmes de fichiers FAT. Pour cette raison, avec NTFS, vous pourrez, sous Linux, lire vos fichiers Windows mais vous ne pourrez pas les modifier et les enregistrer. Si vous souhaitez un accès en écriture à vos données Windows et ne tenez pas absolument à utiliser un système de fichiers NTFS, réinstallez Windows sur un système de fichiers FAT32. Dans ce cas, vous aurez un accès complet à vos données de Windows depuis SUSE LINUX.

Remarque

Informations complémentaires sur le partitionnement

Si YaST effectue automatiquement le partitionnement et constate que d'autres partitions sont présentes dans votre système, celles-ci seront également inscrites dans le fichier `/etc/fstab` , afin qu'il soit possible d'accéder simplement à ces données. Dans ce fichier, toutes les partitions présentes sur votre système sont répertoriées avec les propriétés qui leur correspondent, telles que système de fichiers, point de montage et droits d'utilisateur.

Exemple 1.1: */etc/fstab : partitions de données*

```
/dev/sda1       /data1  auto    noauto,user 0 0
/dev/sda8       /data2  auto    noauto,user 0 0
/dev/dasda1     /data3  auto    noauto,user 0 0
```

Les partitions, qu'il s'agisse de partitions Linux ou de partitions FAT, sont enregistrées avec les options `noauto` et `user`. Chaque utilisateur peut ainsi monter ou démonter ces partitions en cas de besoin. Pour des raisons de sécurité, YaST n'entre pas ici l'option `exec` qui est néanmoins nécessaire pour exécuter d'ici des programmes. Si vous désirez cependant exécuter des programmes ou des scripts, saisissez vous-même cette option. Cette option sera nécessaire, au plus tard, lorsque vous verrez apparaître des messages tels que `bad interpreter` ou `Permission denied`.

Vous trouverez de nombreuses autres informations ainsi que des astuces concernant le partitionnement dans la section*Partitionnement pour les experts* page 138.

1.5.6 Logiciels

SUSE LINUX contient un grand nombre de logiciels utilisables dans divers domaines d'application et que vous pouvez installer selon vos préférences. Étant donné qu'il serait très pénible de sélectionner un à un les logiciels parmi la quantité de paquetages disponibles, SUSE LINUX offre trois types de système avec chacun une présélection de logiciels. Selon l'espace disque disponible, YaST sélectionne automatiquement un de ces types de système et affiche cette proposition.

Système minimal (conseillé uniquement pour des utilisations spécifiques)
: Ici, seul le système d'exploitation sera installé ainsi que différents services. Aucune interface graphique n'est installée, l'ordinateur n'est contrôlé que par l'intermédiaire de consoles ASCII. Ce type de système est particulièrement indiqué pour des serveurs qui ne nécessitent que peu ou pas d'interactions avec l'utilisateur.

Système graphique minimal (sans KDE)
: Si vous ne souhaitez pas utiliser le confortable bureau KDE ou si vous n'avez pas assez d'espace, installez ce type de système. Le système installé dispose d'un environnement graphique élémentaire avec un gestionnaire de fenêtres. Vous pouvez utiliser tous les programmes avec une interface graphique propre. Les programmes bureautiques ne sont pas installés.

Système standard (avec KDE et le paquetage Office)
: Ici, vous disposez du plus grand système standard disponible. Il contient le bureau KDE ainsi que la majorité de ses programmes et les applications bureautiques. Ce type de système est le plus approprié pour les stations de travail utilisées dans un cadre normal. YaST le sélectionne si les conditions le permettent.

Si vous cliquez sur 'Logiciels' dans la fenêtre de propositions, vous ouvrez un dialogue dans lequel vous pouvez sélectionner un des types de système. En outre, vous pouvez, en cliquant sur 'Sélection détaillée', démarrer le module de sélection de logiciels (c'est à dire le gestionnaire de paquetages) pour modifier individuellement l'amplitude de l'installation (voir figure 1.11).

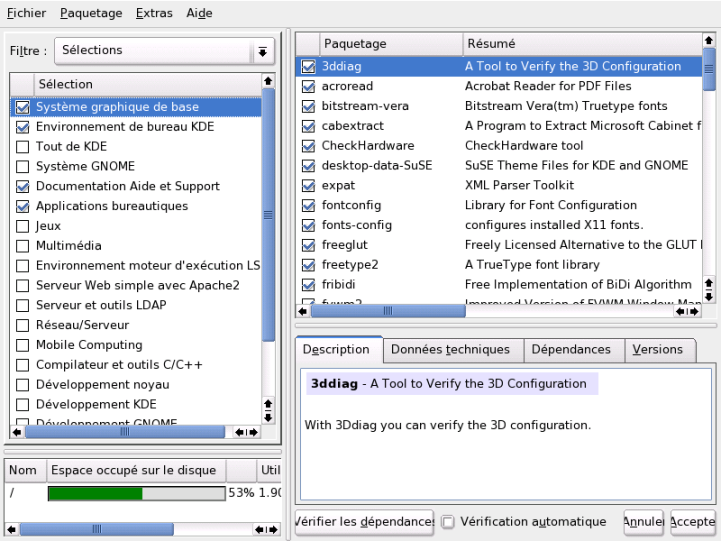


FIG. 1.11: *YaST : Installer et éliminer des logiciels (gestionnaire de paquetages)*

Modifier la sélection de logiciels prédéfinie

Lors de l'installation du "Système standard", il n'est normalement pas utile de modifier la sélection de paquetages, étant donné que le système définit un ensemble de logiciels cohérent qui devraient répondre aux besoins les plus courants sans modification. Cependant, il existe la possibilité de procéder à des modifications manuelles à l'aide du gestionnaire de paquetages. Ce gestionnaire vous offre des filtres qui vous permettent de sélectionner certains logiciels parmi les nombreux paquetages que contient SUSE LINUX en utilisant des différents critères.

La boîte de sélection des filtres se trouve en haut à gauche sous la barre de menus. Lors du démarrage, le filtre de sélections est activé. Les sélections groupent les programmes selon leur domaine d'application, comme par exemple Multimédia et Bureautique. Sous ce panneau, vous voyez les différents groupes du filtre de sélections, dont certains qui sont déjà présélectionnés étant donné qu'ils font partie de l'installation standard de ce type de système. D'un clic de souris sur la case à cocher correspondante, vous pouvez sélectionner des groupes de paquetages dans leur intégralité, soit pour l'installation, soit pour la désinstallation.

Dans la fenêtre de droite, vous voyez la liste des différents paquetages appartenant à chaque sélection. À tous les paquetages correspond un état symbolisé dans une petite boîte d'état au début de la ligne. Lors de l'installation, ce sont surtout les états installer et ne pas installer, qui vous intéressent, c'est à dire, respectivement une croix à droite du nom du paquetage ou un espace libre. Vous pouvez ici, sélectionner ou désélectionner chaque paquetage séparément. À cette fin, cliquez aussi souvent qu'il le faut sur le symbole d'état en début de ligne jusqu'à avoir atteint l'état désiré (installer ou ne pas installer).

Vous pouvez également, d'un clic du bouton de droite de la souris sur la ligne correspondant au paquetage, ouvrir un menu déroulant qui affiche tous les états. Les autres états seront expliqués en détails dans la section *Installer/supprimer des logiciels* page 50 relative à ce module.

Autres filtres

Si vous déroulez la boîte de sélection de filtres, vous verrez une sélection de filtres supplémentaires qui vous aideront à ordonner les paquetages. Pour l'installation, la sélection par 'Groupes de paquetages' est particulièrement intéressante. Avec ce filtre, les paquetages sont affichés sur le côté gauche et sont ordonnés par thème dans une structure en arborescence. Plus vous vous déplacez vers les extrémités des ramifications de l'arborescence dans les sous-groupes (thèmes), plus la sélection se précise, et par conséquent, plus le nombre de paquetages affichés à droite qui correspondent à cette sélection diminue.

La fonction de 'Recherche' vous sert à retrouver un paquetage déterminé. L'utilisation de cette fonction est décrite dans la section *Installer/supprimer des logiciels* page 50.

Dépendances de paquetages et conflits

Il n'est pas possible d'installer n'importe quelle combinaison de logiciels. Les paquetages installés doivent être compatibles entre eux. Si cette règle n'est pas respecté, il peut se produire des incohérences qui mettent en danger le bon fonctionnement du système installé. Si vous sélectionnez ou désélectionnez des paquetages dans ce dialogue, des avertissements relatifs aux dépendances et conflits entre paquetages peuvent apparaître dans cette fenêtre de dialogue. Si vous installez SUSE LINUX pour la première fois ou si vous ne comprenez pas la signification de ces avertissements, veuillez lire la section *Installer/supprimer des logiciels* page 50. Vous y trouverez des informations détaillées quant à l'utilisation du gestionnaire de paquetage ainsi que quelques explications sur l'"organisation des logiciels sous Linux".

Attention

La sélection standard qui vous est proposée, fruit d'une longue expérience, est d'une manière générale très judicieuse pour une utilisation privée, que ce soit pour le débutant comme pour l'utilisateur plus averti. Normalement, il n'est pas nécessaire de procéder à des modifications. N'installez pas et surtout ne désinstallez pas de paquetages sans savoir exactement quelles en seront les conséquences. En tout état de cause, et surtout lorsque vous supprimez des paquetages, veillez à tenir compte des avertissements et ne supprimez surtout pas de paquetages du système de base Linux.

Attention

Quitter la sélection de logiciels

Lorsque vous êtes satisfait de votre sélection de logiciels et une fois qu'il n'existe plus de dépendances non résolues ou de conflits entre paquetages, cliquez sur 'Accepter' pour quitter le programme. Les changements ne seront pas effectués immédiatement contrairement à ce qui se produit lors de l'utilisation de ce module sous un système installé. Ici, la sélecion de logiciels à installer sera enregistrée en attendant que la procédure d'installation soit démarrée.

1.5.7 Démarrer le système (installation du gestionnaire d'amorçage)

Lors de l'installation, YaST propose un mode d'amorçage approprié à votre système. Normalement, vous n'avez pas besoin de modifier ces paramètres. Cependant, modifiez la proposition du système en cas de besoins spéciaux de votre environnement système.

Vous pouvez, par exemple, configurer le mécanisme d'amorçage de façon à ce qu'il soit nécessaire d'insérer une disquette d'amorçage spéciale lors du démarrage de SUSE LINUX. Ceci peut être utile si vous avez l'habitude de travailler avec un autre système d'exploitation dont le mécanisme d'amorçage ne doit pas être modifié. En général, ceci n'est pas nécessaire étant donné que YaST configure le chargeur d'amorçage de telle façon que vous puissiez amorcer le système d'exploitation de votre choix. Plus tard, vous pourrez également changer l'emplacement où le chargeur d'amorçage de SUSE LINUX est enregistré sur le disque dur.

Si vous voulez modifier la proposition de YaST sélectionnez 'Amorçage du système'. Un dialogue apparaît dans lequel vous pouvez accéder au mecanisme d'amorçage. Vous trouverez plus d'informations à ce sujet dans le chapitre *Configuration du chargeur d'amorçage avec YaST* page 219.

Remarque

La modification du mode d'amorçage est à réserver à des utilisateurs expérimentés.

Remarque

1.5.8 Zone horaire

Dans ce masque (figure 1.12 page ci-contre), vous pouvez, dans le champ 'Horloge interne réglée sur', choisir entre les options `Heure locale` et `UTC` (*Universal Time Coordinated*). Votre sélection depend de la configuration de l'horloge BIOS de votre ordinateur. Si elle est réglée sur l'heure `UTC`, SUSE LINUX se charge de passer automatiquement entre l'horaire d'été et l'horaire d'hiver.

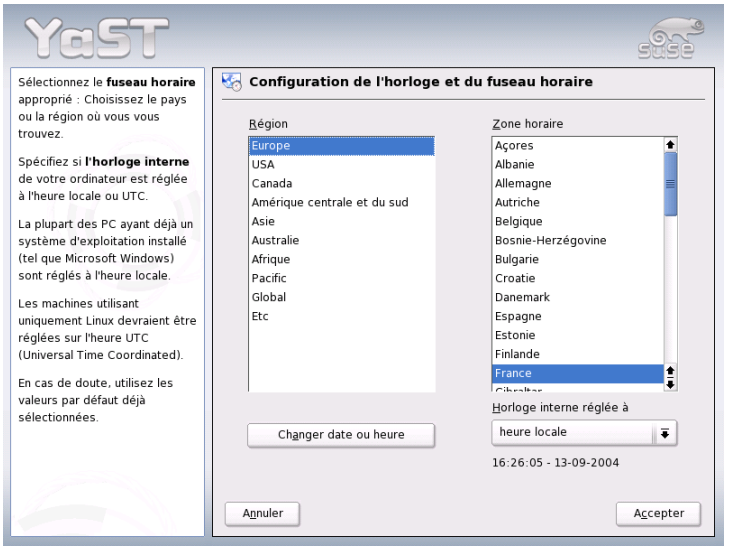


FIG. *1.12:* *Selection de la zone horaire*

1.5.9 Langue

La langue a déjà été sélectionnée au début de l'installation (voir section *Sélection de la langue* page 13). Cependant, si vous souhaitez procéder à des modifications ultérieures, vous pouvez le faire ici. En outre, vous avez ici la possibilité de configurer la langue pour l'utilisateur `root` en cliquant sur le bouton 'Détails'. Le menu déroulant offre trois options :

ctype La variable `LC_CTYPE` pour l'utilisateur `root` est enregistrée dans le fichier `/etc/sysconfig/language`. Ceci définit la localisation pour les appels de fonctions spécifiques à chaque langue.

oui L'utilisateur `root` a exactement la même configuration de la langue que l'utilisateur local.

non La configuration de la langue de l'utilisateur `root` est indépendante de la sélection générale de la langue.

Cliquez sur 'OK' pour terminer la configuration ou sur 'Défausser' pour annuler vos modifications.

1.5.10 Procéder à l'installation

En cliquant sur 'Suivant', vous acceptez la suggestion avec toutes les modifications que vous avez effectuées et vous arrivez à un masque de confirmation de couleur verte. Si vous cliquez ici sur 'Oui', l'installation peut commencer avec les paramètres que vous avez sélectionnés. Le processus d'installation dure généralement de 15 à 30 minutes, selon la performance de votre machine et la sélection de logiciels à installer. Après l'installation des paquetages, YaST amorce le système installé et vous pouvez ensuite passer à la configuration du matériel et des services.

1.6 Terminer l'installation

Une fois que le système et les logiciels sélectionnés ont été installés, vous devrez spécifier un mot de passe pour l'administrateur du système (utilisateur `root`). Vous aurez ensuite la possibilité de configurer l'accès à Internet et une connexion au réseau. De cette façon, il est possible, durant l'installation de procéder à la mise à jour de logiciels pour SUSE LINUX et de configurer les services DNS pour la gestion centralisée des utilisateurs dans un réseau local. Finalement, vous pouvez également configurer le matériel connecté.

1.6.1 Mode de passe root

☞*Root* est le nom du superutilisateur ou administrateur du système ; `root` a des droits que les autres utilisateurs n'ont pas. Il peut modifier le système, installer de nouveaux programmes ou configurer de nouveaux composants matériels. Si un utilisateur a oublié son mot de passe ou si les programmes ne tournent plus, `root` a la possibilité de venir en aide. En règle générale, on ne devrait se connecter sous le compte `root` que pour exécuter des tâches d'administration ou des travaux de maintenance ou de réparation. Pour le travail quotidien, ceci est très risqué car `root` peut, par exemple, effacer irrémédiablement tous les fichiers système.

Lors de l'attribution du mot de passe `root`, celui-ci doit, pour raison de sécurité, être saisi une deuxième fois pour vérification (figure 1.13 page ci-contre). Mémorisez bien le mot de passe de l'utilisateur `root`. Il ne vous sera plus possible de le voir ultérieurement.

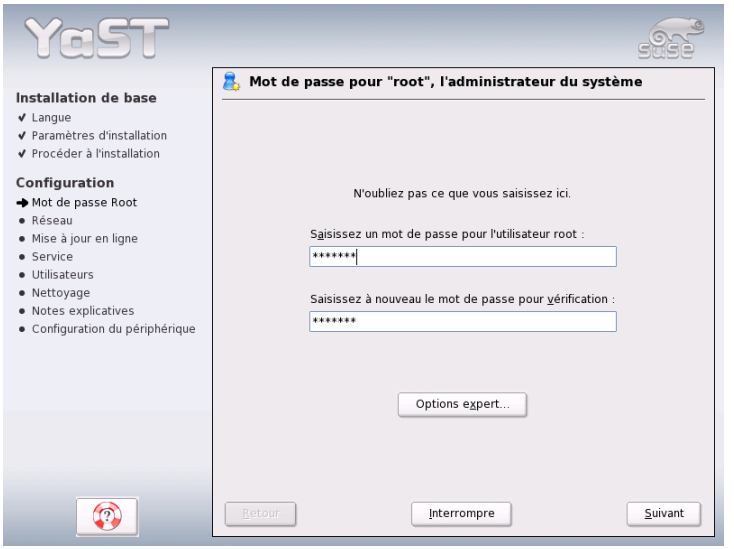


FIG. *1.13:* *Définir le mot de passe de l'utilisateur root*

Attention

L'utilisateur `root` a tous les droits et peut apporter toute sorte de modifications au système. Si vous voulez vous charger de tâches impliquant des modifications, il vous faut un mot de passe attribué spécialement à `root`. Sans ce mot de passe, il ne vous sera pas possible d'exécuter des tâches d'administration.

Attention

1.6.2 Configuration réseau

Dans l'étape suivante, vous avez la possibilité de connecter votre système au reste du monde. Vous pouvez configurer carte réseau, RNIS, modem et DSL. Si votre système dispose de ce type de matériel, profitez de cette opportunité. Ainsi, YaST pourra plus tard procéder sur Internet à des téléchargements de mises à jour pour SUSE LINUX qui seront prises en compte lors de l'installation.

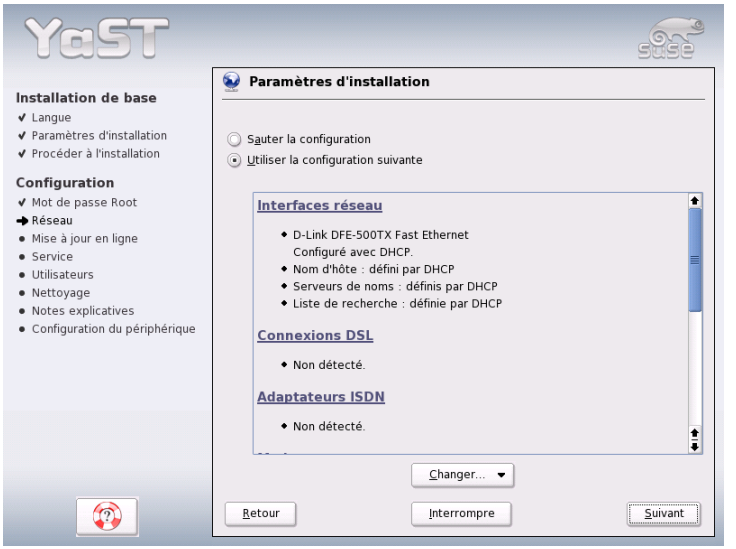


FIG. *1.14:* *Configuration des périphériques réseau*

Si vous souhaitez configurer ici votre matériel réseau, reportez-vous aux sections correspondantes dans le chapitre *L'intégration dans le réseau* page 468. Sinon, sélectionnez l'option 'Ignorer la configuration réseau' et cliquez sur 'Suivant'. Vous pourrez configurer vos composants réseau ultérieurement dans le système déjà installé.

Configuration du pare-feu

Dès que vous mettez en réseau votre système, un pare-feu est démarré automatiquement sur l'interface configurée. La configuration du pare-feu est alors faite sur mesure pour cette interface. Les paramètres de configuration du pare-feu sont affichés aussi dans le dialogue de configuration du réseau. À chaque modification de la configuration des interfaces ou des services, la proposition de configuration pour le pare-feu est actualisée automatiquement. Si vous souhaitez modifier les paramètres générés automatiquement, cliquez sur 'Modifier' → 'Pare-feu'.

Dans le dialogue qui s'ouvre, déterminez si le pare-feu doit être démarré ou non. Si vous ne souhaitez pas démarrer le pare-feu, activez le bouton radio correspondant et quittez le dialogue. Lorsque vous démarrez le pare-feu et souhaitez en modifier la configuration, vous ouvrez, en cliquant sur 'Suivant', des dialogues semblables à ceux décrits dans la section *Configuration avec YaST* page 661.

1.6.3 Tester la connexion Internet

Si vous avez configuré une connexion Internet, vous pouvez maintenant vérifier que celle-ci fonctionne correctement. À cette fin, YaST établit une connexion avec le serveur de SUSE et vérifie par la même occasion si des mises à jour sont disponibles pour SUSE LINUX. Si la connexion fonctionne correctement, vous pouvez télécharger ces mises à jour dans l'étape suivante. En outre, les notes relatives à la dernière version disponible sur le serveur SUSE seront également téléchargées et elles seront affichées à l'écran à la fin du processus d'installation.

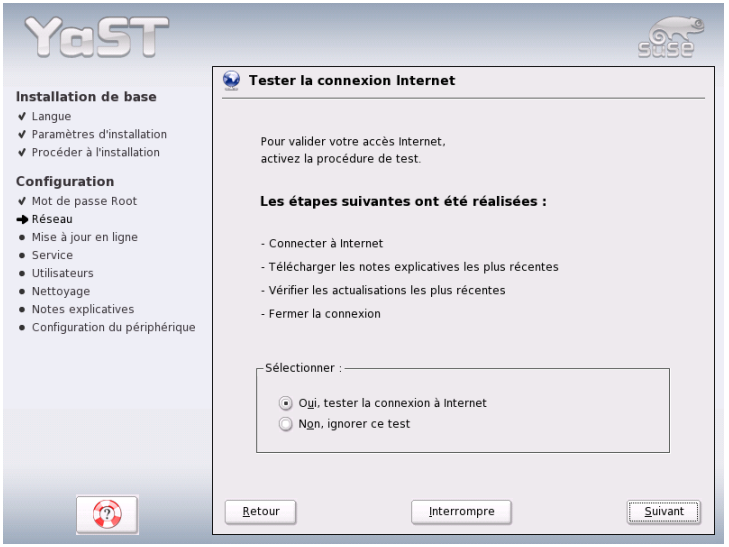


FIG. *1.15:* *Tester la connexion Internet*

Si vous ne souhaitez pas procéder ici au test de la connexion Internet, sélectionnez 'Ignorer ce test' et cliquez sur 'Suivant'. Le téléchargement des mises à jour et des notes les plus récentes ne se fera pas non plus.

1.6.4 Télécharger des mises à jour des logiciels

Si YaST a pu établir une connexion Internet avec le serveur de SUSE dans l'étape précédente, vous aurez la possibilité de procéder à une mise à jour en ligne avec YaST. De cette façon, les éventuels patches de correction d'erreurs et de problèmes de sécurité connus seront installés.

Remarque

Télécharger des mises à jour des logiciels

La durée du processus de mise à jour dépend des performances de votre connexion Internet et de la taille des paquetages de la mise à jour.

Remarque

Si vous souhaitez procéder immédiatement à une mise à jour des logiciels, sélectionnez 'Procéder maintenant à la mise à jour' et cliquez sur 'OK'. Vous entrez dans le dialogue de mise à jour en ligne de YaST où vous pouvez voir les patches disponibles, les sélectionner et les appliquer. Dans ce cas, reportez-vous à la section *YaST OnlineUpdate, Mise à jour en ligne YaST* page 48. Vous pouvez évidemment procéder à la mise à jour plus tard. Dans ce cas, sélectionnez 'Ignorer la mise à jour' et cliquez sur 'OK'.

1.6.5 Authentification des utilisateurs

Si vous avez configuré une connexion Internet dans le cadre de l'installation, vous avez maintenant deux possibilités pour l'administration des utilisateurs du système installé.

Administration local des utilisateurs Les utilisateurs sont administrés localement sur l'ordinateur installé. Ceci est la méthode conseillée pour les ordinateurs utilisés par une seule personne (standalone). Dans ce cas, les données utilisateur sont administrés via le fichier local `/etc/passwd`.

LDAP Les utilisateurs de tous les systèmes sont administrés en réseau, de façon centrale, sur un serveur LDAP.

NIS Les utilisateurs de tous les systèmes sont administrés en réseau, de façon centrale, sur un serveur NIS.

Samba Avec cette option, il est procédé à une authentification SMB dans les réseaux hétérogènes Linux/Windows.

Si toutes les conditions sont remplies, YaST ouvre un dialogue pour sélectionner la méthode appropriée (figure 1.16). Si vous n'êtes connecté à aucun réseau, sélectionnez le mode utilisateur local.

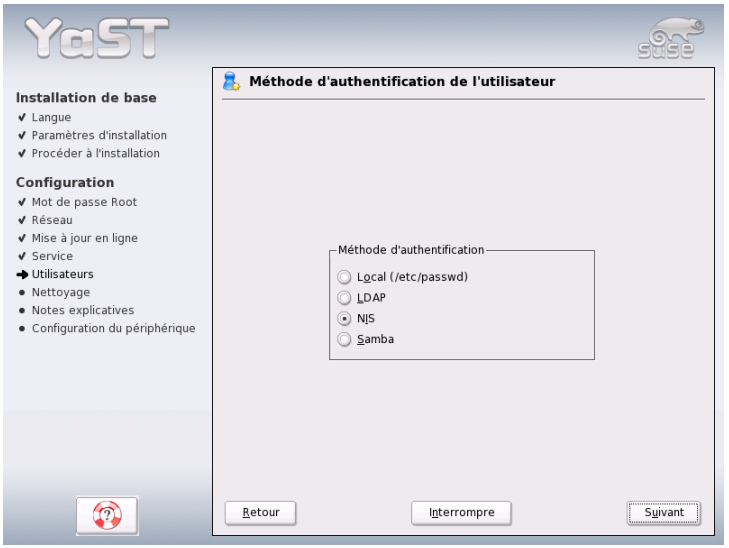


FIG. *1.16:* *Authentification des utilisateurs*

1.6.6 Configuration en tant que client NIS

Si vous avez décidé de procéder à l'administration des utilisateurs via NIS, l'étape suivante consiste à configurer un client NIS. Nous ne décrivons ici que la configuration d'un client ; vous trouverez des informations relatives à la configuration d'un serveur NIS avec YaST à la section *NIS – Network Information Service* page 509.

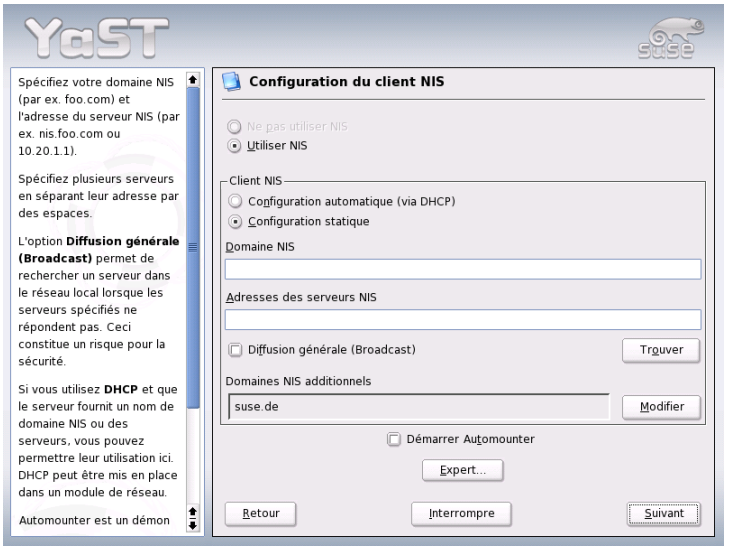


FIG. *1.17:* *Configuration d'un client NIS*

Dans le dialogue (voir figure 1.17), précisez tout d'abord si le client NIS dispose d'une adresse IP statique ou d'une adresse IP dynamique assignée via DHCP. Dans ce cas, vous ne pouvez pas spécifier de domaine DHCP ou d'adresse IP du serveur étant donné que ces données seront également assignées par DHCP. Vous trouverez plus d'informations relatives au protocole DHCP dans la section *DHCP* page 546. Si le client dispose d'une adresse IP statique, saisissez le domaine NIS et le serveur manuellement.

Activez l'option de diffusion générale dans la case à cocher correspondante pour permettre la recherche d'un serveur NIS dans le réseau dans le cas où le serveur indiqué ne répondrait pas. Vous avez également la possibilité de spécifier différents domaines avec un domaine par défaut. Avec l'option 'Ajouter', vous pouvez également spécifier plusieurs serveurs avec fonction de diffusion générale pour chaque domaine.

La configuration pour experts vous permet de sélectionner l'option 'Répondre uniquement à l'hôte local' afin d'éviter que d'autres ordinateurs du réseau puissent savoir quel serveur utilise son client. Si vous activez 'Serveur défectueux', les réponses d'un serveur seront également acceptées sur un port non privilégié. Vous pourrez trouver plus d'informations à ce sujet dans la page de man de `ypbind`.

1.6.7 Créer des utilisateurs locaux

Si vous n'avez configuré aucune authentification d'utilisateurs basée sur un service de noms, vous avez ici l'opportunité de créer des utilisateurs locaux. Les données de ces utilisateurs (nom, login, mot de passe, etc.) sont enregistrées et administrées sur le système installé.

Linux permet à plusieurs utilisateurs de travailler simultanément sur un seul et même système. Pour chaque utilisateur, il doit être créé un compte utilisateur sous lequel il se connectera au système. Les données de chaque utilisateur sont à l'abri de tout accès de la part d'autres utilisateurs qui ne peuvent donc ni les modifier ni les effacer. Chaque utilisateur peut en outre configurer son propre environnement de travail qu'il retrouvera inchangé chaque fois qu'il se connectera au système Linux.

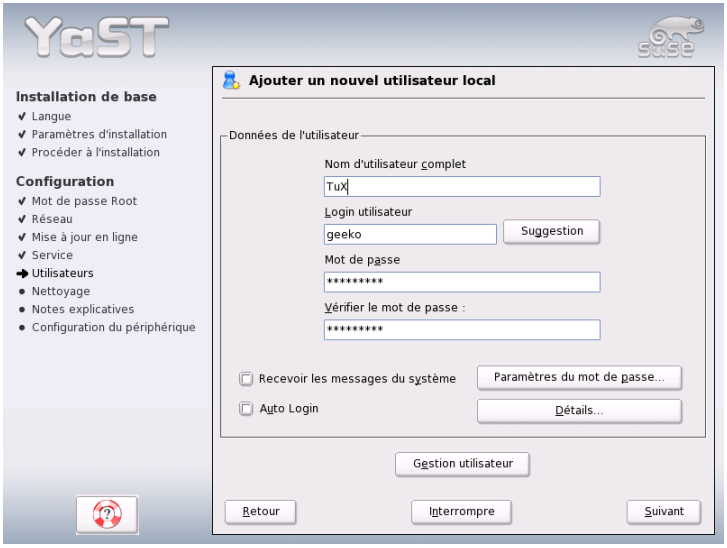


FIG. *1.18:* *Définir le nom d'utilisateur et le mot de passe*

Créer pour vous-même un tel compte d'utilisateur dans la boîte de dialogue qui vous est présentée dans la figure 1.18. Entrez votre prénom et votre nom et choisissez un nom d'utilisateur (login). Si aucun nom approprié ne vous vient à l'idée, vous pouvez cliquer sur 'Suggestion' et il vous sera proposé un nom d'utilisateur.

Il vous faut encore spécifier un mot de passe utilisateur que vous devrez entrer une deuxième fois pour vérification. Le nom d'utilisateur fait savoir au système *qui* vous êtes et le mot de passe lui *garantit* que c'est bien de vous qu'il s'agit.

Attention

Nom d'utilisateur et mot de passe

Notez soigneusement votre nom d'utilisateur et votre mot de passe. Vous en aurez besoin lors de chaque connexon au système.

Attention

Pour constituer une protection efficace, un mot de passe devrait avoir une longueur comprise entre cinq et huit caractères. La longueur maximale d'un mot de passe est de 128 caractères cependant, un module spécial est alors nécessaire. Si ce module n'a pas été chargé, seuls les huit premiers caractères sont utilisés pour l'identification. Il est tenu compte de la casse des lettres et il convient donc de différencier majuscules et minuscules. Les caractères accentués ne sont pas admis mais les caractères spéciaux ainsi que les chiffres de 0 à 9 peuvent être utilisés.

Pour les utilisateurs locaux, il existe encore deux options qui peuvent être activées au choix.

'Recevoir des messages du système' SI vous activez cette case à cocher, vous recevrez les messages de services du système. Normalement, ces messages ne sont envoyés qu'à l'administrateur `root`. Cependant, étant donné que vous n'êtes connecté qu'exceptionnellement en tant que `root`, cette option est surtout intéressante pour l'utilisateur qui travaille le plus souvent sur ce système

'Connexion automatique' Cette option n'est disponible que si vous utilisez le bureau KDE. Avec elle, l'utilisateur actuel est connecté automatiquement lors du démarrage du système. Ceci est surtout intéressant lorsque l'ordinateur n'est utilisé que par une personne.

Attention

Connexion automatique

Lors de la connexion automatique, aucune authentification n'a lieu lors du démarrage du système. N'utilisez *pas* cette option pour des ordinateurs accessibles à d'autre personnes et qui contiennent des données confidentielles.

Attention

1.6.8 Notes de version

Après avoir configuré l'authentification des utilisateurs, vous verrez apparaître les notes de version. Prenez le temps de les lire car elles contiennent des informations actuelles qui n'étaient pas encore disponibles lors de l'impression de ce manuel. Si vous avez configuré une connexion Internet et avez vérifié son fonctionnement avec le serveur de SUSE, vous avez obtenu la dernière version de SUSE ainsi que les informations de dernière minute.

1.7 Configuration du matériel

Après l'installation, YaST vous présente encore un dialogue dans lequel vous pouvez configurer votre carte graphique ainsi que différents composants matériels du système (tels que imprimante ou carte son). En cliquant sur le nom des différents composants, vous démarrez la configuration du matériel. YaST détecte et configure alors automatiquement les composants matériels.

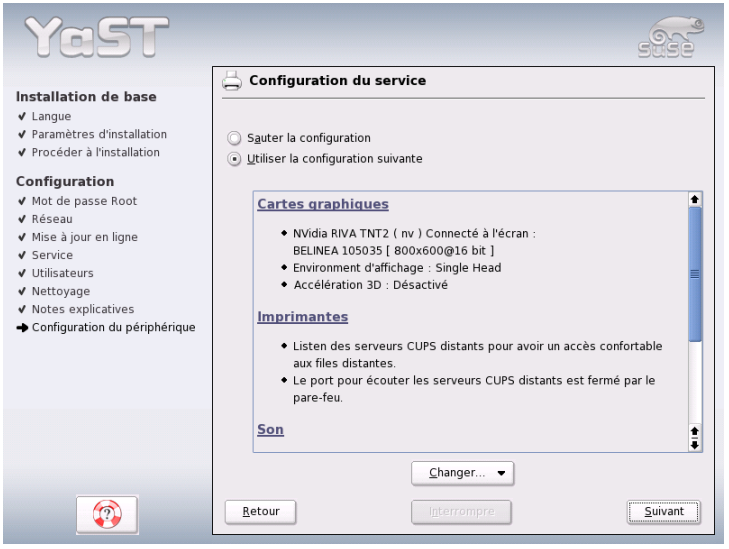


FIG. *1.19:* *Configuration des composants du système*

Vous pourrez procéder à la configuration des périphériques externes plus tard, mais nous vous recommandons de configurer au moins la carte graphique avec les valeurs que vous souhaitez. La proposition standard de YaST est généralement satisfaisante, cependant les préférences pour l'affichage de l'image à l'écran (résolution et profondeur de couleur) varient beaucoup d'un utilisateur à un autre. Si vous souhaitez changer les paramètres, sélectionnez l'option 'Cartes graphiques'. Les fenêtres de dialogue correspondantes sont décrites dans la section *Carte graphique et moniteur (SaX2)* page 70.

Une fois que YaST a terminé d'écrire les fichiers de configuration, cliquez sur 'Terminer' pour finaliser l'installation de SUSE LINUX.

1.8 Login graphique

SUSE LINUX est maintenant installé et vous pouvez vous connecter pour la première fois à votre système. Si, dans le cadre de l'administration locale des utilisateurs, vous avez activé la connexion automatique, vous pouvez commencer sans procédure de login. Sinon, vous verrez apparaître sur votre écran le ☞*login* graphique que vous pouvez voir dans la figure 1.20. Entrez votre nom d'utilisateur ainsi que le mot de passe qui lui correspond afin de vous connecter à votre système.

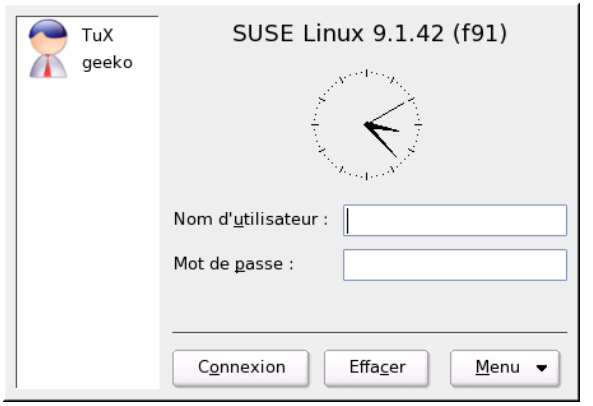


FIG. *1.20:* *Connexion au système (KDE)*

Configuration du système avec YaST

YaST (Yet another Setup Tool), dont vous avez déjà fait connaissance lors de l'installation, est également *l'outil* de configuration de SUSE LINUX. Ce chapitre décrit la configuration de votre système à l'aide de YaST. Vous pourrez configurer confortablement les composants du système les plus importants, c'est à dire, la plus grande partie du matériel, l'interface graphique, l'accès à Internet, les paramètres de sécurité, l'administration des utilisateurs, l'installation de logiciels ainsi que les mises à jour du système et les informations relatives à celui-ci. En outre, vous trouverez des instructions nécessaires à l'utilisation de YaST en mode texte.

2.1 Le démarrage de YaST

La configuration du système avec YaST s'effectue à travers différents modules de YaST. Selon la plateforme matérielle utilisée et la sélection de logiciels installés, vous avez le choix entre différentes façons d'accéder à YaST dans le système installé.

2.1.1 Démarrer depuis une interface graphique

Si vous utilisez une des deux interfaces graphiques KDE ou GNOME, démarrez le centre de contrôle de YaST avec le menu de SUSE ('Système' → 'YaST'). KDE intègre également les différents modules de configuration de YaST dans le centre de contrôle de KDE. Vous serez appelé à saisir le mot de passe root avant que YaST ne démarre car celui-ci nécessite les droits de l'administrateur du système pour pouvoir modifier les fichiers système.

Depuis la ligne de commande, démarrez YaST avec les commandes `sux` (pour vous connecter en tant qu'utilisateur `root`) puis `yast2`. Si vous souhaitez démarrer YaST en mode textuel, saisissez `yast` au lieu de `yast2`. En tant que `root`, utilisez également `yast` afin de démarrer le programme depuis une console virtuelle.

Remarque

Si vous désirez changer la langue de YaST, cliquez sur 'Système' dans le centre de contrôle de YaST puis sélectionnez la langue souhaitée dans le menu 'Sélectionner une langue'. Sélectionnez la langue, fermez le centre de contrôle de YaST, déconnectez-vous de votre système puis reconnectez-vous. Lorsque vous redémarrerez YaST, la nouvelle langue sera activée.

Remarque

2.1.2 Démarrer depuis un terminal distant

Cette méthode s'adresse aux plateformes matérielles qui n'ont pas d'écran ou pour la maintenance à distance de systèmes depuis un autre ordinateur.

Ouvrez tout d'abord une console localement et saisissez, à l'invite, la commande `ssh -X root@<nom du système>`, afin de vous connecter en tant qu'utilisateur `root` sur le système distant et d'obtenir l'affichage de sorties du serveur X sur votre terminal.

Dès que la connexion ssh a été établie, saisissez `yast2` à l'invite du système distant afin de démarrer le mode graphique de YaST et de l'afficher sur le terminal local. Pour démarrer YaST en mode textuel, utilisez `ssh` sans l'option `-X` et démarrez YaST avec la commande `yast`.

2.2 Le centre de contrôle de YaST

Lorsque vous démarrez YaST en mode graphique, vous voyez tout d'abord apparaître le centre de contrôle de YaST (fig. 2.1 page suivante). Dans la partie gauche de l'écran, vous trouvez les sous-divisions 'Logiciels', 'Matériel', 'Périphériques réseau', 'Services réseau', 'Sécurité & Utilisateurs', 'Système' et 'Divers'. En cliquant sur les icônes, vous obtiendrez, dans la partie de droite, l'affichage du contenu de la catégorie sélectionnée. Cliquez, par exemple, sur 'Matériel' puis, à droite sur 'Son', une fenêtre s'ouvrira dans laquelle vous pouvez procéder à la configuration de la carte son. La configuration est généralement effectuée en plusieurs étapes. YaST vous conduira à travers tous les dialogues au moyen d'un clic sur 'Suivant'.

La partie gauche de l'écran affiche un texte d'aide qui vous explique les entrées que vous devez faire. Après avoir fait les spécifications nécessaires, vous terminerez chaque étape de la configuration en cliquant, dans le dernier dialogue, sur le bouton 'Terminer'. La configuration sera alors enregistrée.

2.3 Logiciels

2.3.1 Changer le support d'installation

YaST peut gérer toute une série de sources d'installation et vous permet de sélectionner celle à utiliser pour une installation ou une mise à jour.

Après le démarrage du module, une liste de tous les supports d'installation enregistrés jusque là est affichée. Après une installation normale depuis un CD, cette liste ne contient que le CD comme support. Avec 'Ajouter', vous pouvez introduire, outre des supports d'installation comme des CD et des DVD, des connexions de réseau telles que NFS et FTP. Même des répertoires sur votre disque local peuvent également être utilisés comme supports d'installation (voir le texte d'aide au sujet de YaST).

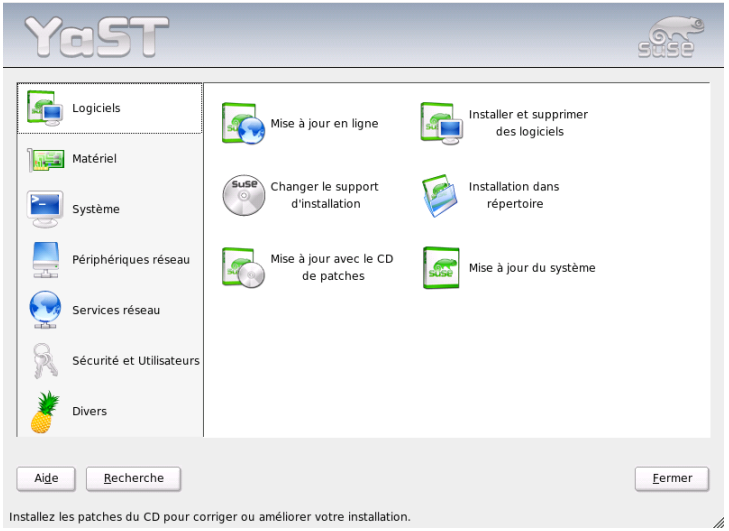


FIG. 2.1: *Le centre de contrôle de YaST*

Les différents supports d'installation enregistrés peuvent être activés ou désactivés et leur état d'activation est indiqué dans la première colonne de la liste. En cliquant sur 'Activer ou Désactiver' pour changer l'état dans la liste. Lors de l'installation de paquetages logiciels ou d'une mise à jour, YaST choisit l'entrée adéquate parmi toutes les sources d'installations activées.

Lorsque vous quittez le module en cliquant sur 'Fermer', la configuration actuelle est enregistrée et sera donc utilisée pour les modules de configuration 'Installer ou supprimer les logiciels' et 'Mise à jour du système'.

2.3.2 YaST OnlineUpdate, Mise à jour en ligne YaST

La mise à jour en ligne de YaST (YOU) permet l'installation de mises à jour importantes et autres améliorations. Les patches correspondants sont mis à votre disposition pour téléchargement sur le serveur FTP de SUSE ainsi que sur différents serveurs miroirs.

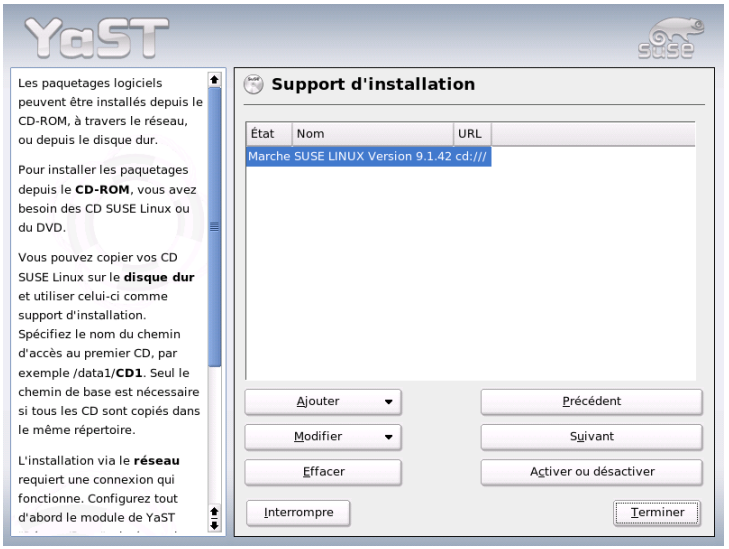


FIG. 2.2: *Changer le support d'installation*

Dans le champ 'Source d'installation', vous pouvez choisir parmi différents serveurs. Lorsque vous sélectionnez un serveur, l'URL correspondant apparaît dans le champ de texte en dessous et peut y être modifié. Vous avez également la possibilité d'introduire un URL local tel que, par exemple, "file:/mon/chemin" (ou tout simplement "/mon/chemin"). Cliquez sur 'Nouveau serveur' pour ajouter des nouveaux serveurs à la liste. En cliquant sur 'Modifier le serveur', vous pouvez modifier la configuration du serveur actuellement sélectionné.

Lors du démarrage du module, l'option 'Sélection manuelle des patches' est activée afin de pouvoir définir individuellement le chargement de chaque patch. Si vous souhaitez installer tous les paquetages de mises à jour sans distinction, désactivez cette option. Selon la largeur de bande de la connexion et la quantité de données à télécharger, le temps de chargement peut être très long.

Si vous activez la case à cocher 'Charger à nouveau tous les patches', *tous* les patches, paquetages installables et descriptions disponibles sur le serveur seront téléchargés. Si elle n'est pas activée (configuration par défaut), vous ne téléchargerez que les paquetages qui ne sont pas encore installés sur votre système.

En outre, vous avez la possibilité de maintenir le système actualisé en permanence automatiquement. Avec l'option 'Configurer la mise à jour totalement automatique', vous définissez un processus qui recherche régulièrement les nouvelles mises à jour et les applique. Ce processus est totalement automatisé. Bien évidemment, il est nécessaire qu'une connexion au serveur de mises à jour soit établie au moment prévu pour la mise à jour.

La mise à jour manuelle (configuration par défaut) permet, après avoir cliqué sur 'Suivant', d'établir une liste de tous les patches disponibles puis démarre le gestionnaire de paquetages (voir section *Installer/supprimer des logiciels* de la présente page). Le filtre pour les patches YOU est alors automatiquement activé et il vous est possible de déterminer les mises à jour que vous souhaitez installer. Les patches de sécurité et les patches recommandés sont déjà présélectionnés lors du démarrage si les paquetages correspondants sont installés dans le système. Il est préférable d'accepter cette présélection.

Une fois que vous avez sélectionné les patches, cliquez, dans le gestionnaire de paquetages, sur 'Accepter'. Tous les patches sélectionnés sont alors téléchargés depuis le serveur puis sont installés sur l'ordinateur. Selon la qualité de la connexion et les performances de votre ordinateur, ce processus peut durer. Les erreurs possibles sont affichées dans une fenêtre et vous pourrez ignorer le paquetage qui pose problème. Certains patches ouvrent une fenêtre avant l'installation pour afficher des informations détaillées.

Lors du téléchargement et de l'installation des mises à jour, vous pouvez suivre le processus dans la fenêtre de protocole. Quittez le dialogue de YOU avec 'Terminer', une fois que vous aurez terminé l'installation de tous les patches. Si vous ne voulez pas conserver les patches une fois la mise à jour effectuée, cliquez sur 'Effacer les sources après la mise à jour'. Le programme SuSEconfig sera alors exécuté afin d'adapter la configuration de votre système aux nouvelles conditions.

2.3.3 Installer/supprimer des logiciels

Ce module vous permet d'installer des applications supplémentaires, de les mettre à jour ou de les désinstaller. Sous Linux, les logiciels se présentent sous forme de paquetages. Un paquetage contient tout ce qui fait un programme complet, c'est à dire le programme lui-même, les fichiers de configuration et la documentation qui lui correspondent. Étant donné que, sous Linux, le code source d'un programme est généralement disponible, il existe normalement un paquetage correspondant avec les sources du programme. Ces sources ne sont pas nécessaires pour travailler avec le programme mais il peut être intéressant, dans certains cas, de les installer. Ainsi, vous pourrez générer une version du programme à votre mesure, chose possible et autorisée sous Linux.

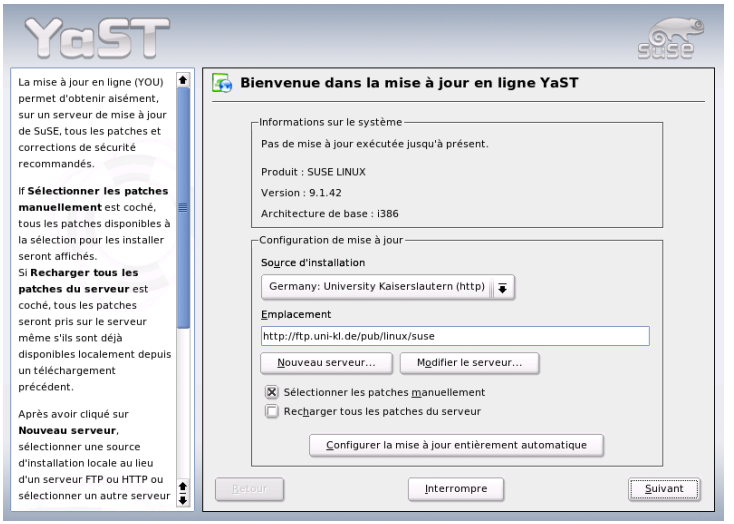


FIG. 2.3: *YaST : Mise à jour en ligne*

Certains paquetages dépendent de façon fonctionnelle d'autres paquetages. Dans ce cas, le programme d'un paquetage ne peut fonctionner correctement que lorsque l'autre paquetage est également installé. En outre, il existe aussi des paquetages qui exigent l'existence d'autres paquetages pour pouvoir être installés, parce que, par exemple, leur routine d'installation nécessite certains outils apportés par ce(s) autre(s) paquetage(s). Lorsque de tels paquetages doivent être installés, il faut prendre garde à observer un certain ordre lors de l'installation. En outre, il existe parfois plusieurs paquetages pouvant remplir la même fonction. Lorsque ces différents paquetages utilisent les mêmes ressources système, ils ne doivent pas être installés simultanément (conflit de paquetages). Ainsi, les dépendances et conflits peuvent non seulement exister entre deux paquetages mais peuvent aussi former de longues chaînes qui, dans les cas les plus complexes, sont très difficilement analysables. Les choses se compliquent encore si la bonne harmonie des programmes dépend aussi de leur version.

Toutes ces conditions doivent être vérifiées lors de l'installation, de la désinstallation ou de la mise à jour de logiciels. Heureusement, YaST dispose du module d'installation de logiciels ou gestionnaire de paquetages, un outil très performant pour la vérification des dépendances et conflits. Le gestionnaire de paquetages procède à une reconnaissance du système et affiche tous les paquetages installés dans celui-ci. Lorsque vous sélectionnez des paquetages additionnels pour les installer, le gestionnaire de paquetages vérifie automatiquement (ou sur demande) les dépendances et les résout en ajoutant automatiquement les éventuels paquetages nécessaires. Si vous sélectionnez par erreur des paquetages qui entrent en conflit, le gestionnaire de paquetages vous en informe et vous propose une solution pour la résolution du conflit. Si vous sélectionnez pour le supprimer un paquetage nécessaire à d'autres paquetages, vous serez, de la même façon, informé par le gestionnaire de paquetages qui vous proposera aussi des informations détaillées ainsi que des propositions de solution.

Outre ces aspects purement techniques, le gestionnaire de paquetages est un bon outil pour obtenir un résumé de tous les paquetages disponibles dans SUSE LINUX. Ce résumé se réalise à l'aide de filtres qui procèdent à des regroupements thématiques et réduisent le nombre de paquetages affichés.

Le gestionnaire de paquetages

Pour modifier à l'aide du gestionnaire de paquetages les logiciels de votre système, sélectionnez 'Installer ou supprimer des logiciels' dans le centre de contrôle de YaST. La fenêtre de dialogue du gestionnaire de paquetages (voir figure 2.4 page suivante).

La fenêtre est divisée en différentes zones thématiques. La taille de ces fenêtres a été optimisée, vous pouvez cependant les modifier en cliquant sur les lignes de séparation et en les déplaçant à l'aide de la souris. Nous allons vous décrire ici le contenu et l'utilisation de ces différentes zones.

La fenêtre de filtres

La sélection individuelle des paquetages lors d'une installation représente une tâche très importante qui demanderait beaucoup de temps. Le gestionnaire de paquetages vous propose donc différentes méthodes de filtrage qui regroupent les paquetages par catégories, affichant un nombre raisonnable de paquetages. La fenêtre de filtres est la zone à gauche sous la ligne de menu. Elle contrôle et affiche différentes méthodes de filtrage. Le contenu de la boîte de sélection de filtres située en haut détermine ce qui sera affiché dans la partie inférieure de la fenêtre de filtres. Cliquez sur la boîte de sélection de filtres pour afficher une liste des filtres disponibles et en sélectionner un.

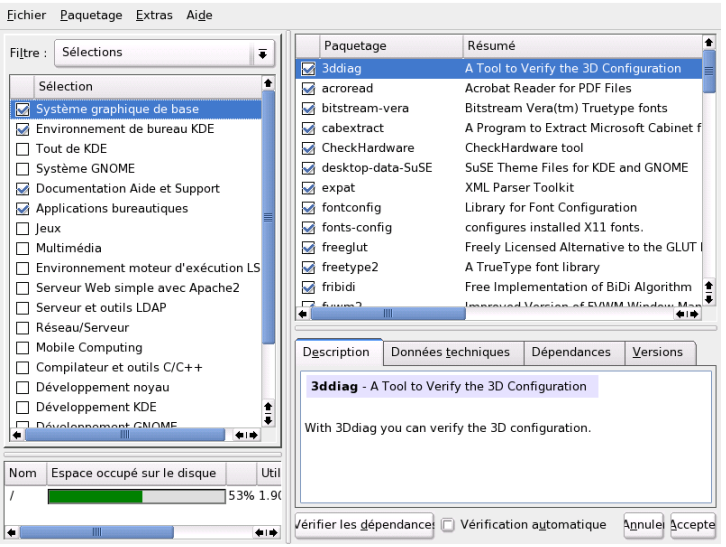


FIG. 2.4: *YaST : le gestionnaire de paquetages*

Le filtre de sélections Lors du démarrage du gestionnaire de paquetages, le filtre de 'Sélections' est activé. Les sélections permettent de grouper les programmes selon leur utilité, par exemple "Multimédia" ou "Bureautique". Sous la boîte de sélection des filtres, vous pouvez voir les différents groupes du filtre sélectionné dont ceux déjà installés sur votre système sont marqués. En cliquant sur la boîte d'état au début de la ligne, vous pouvez sélectionner tous les état possibles successivement. L'état peut également être sélectionné directement en cliquant sur la ligne d'une sélection avec le bouton de droite de la souris pour faire apparaître le menu contextuel. La fenêtre de paquetages individuels à droite affiche tous les paquetages qui appartiennent à la sélection actuelle. Vous pouvez y sélectionner ou désélectionner individuellement les paquetages.

Le filtre de groupes de paquetages Une autre façon de filtrer est la sélection par 'Groupes de paquetages'. Ce filtre offre une gestion plutôt technique des paquetages et est destiné à des utilisateurs qui connaissent déjà un peu les paquetages de SUSE LINUX. Les paquetages sont affichés à gauche dans une arborescence et regroupés selon des thèmes tels que "Applications", "Développement", "Matériel", etc. Plus vous avancez dans l'arborescence , plus le thème se précise et plus la liste correspondante de paquetages diminue, offrant ainsi une meilleure visibilité.

Une autre possibilité de ce filtre est l'affichage de *tous* les paquetages par ordre alphabétique. Pour cela, sélectionnez en haut l'option 'zzz tous'. Étant donné que SUSE LINUX contient énormément de paquetages, il est possible, selon les performances de votre matériel, que la création de cette liste prenne un certain temps.

La fonction de recherche La fonction de 'Recherche' est la méthode la plus simple pour retrouver un paquetage bien déterminé. À l'aide de critères de recherche adéquats, il est possible de définir votre recherche de façon si précise que vous pouvez réussir à ne faire afficher qu'un seul paquetage dans la liste des résultats. Pour cela, introduisez une chaîne de caractères et sélectionnez, à l'aide des cases à cocher, ou cette chaîne doit être recherchée (dans le nom uniquement, dans le nom et dans la description ou dans les dépendances entre paquetages). Pour leurs recherches, les experts peuvent même introduire des caractères jokers ou des expressions régulières et à l'aide des champs "Fournit" et "Nécessite" faire des recherches en fonction des dépendances de paquetages. Par exemple, les développeurs de logiciels qui téléchargent des paquetages sources sur Internet, peuvent ainsi vérifier quel paquetage contient une bibliothèque spécifique nécessaire à la compilation de ce paquetage.

Remarque

Recherche avancée dans le gestionnaire de paquetages

Outre le filtre 'Recherche', il existe une fonction de recherche rapide dans chaque liste du gestionnaire de paquetages. Il suffit d'introduire l'initiale du nom d'un paquetage et le pointeur se positionne directement sur le premier paquetage de la liste dont le nom commence par ce caractère. Pour que cela fonctionne, la liste de paquetages doit être sélectionnée (d'un clic de souris).

Remarque

Résumé de l'installation Après avoir sélectionné des paquetages pour les installer, les supprimer ou les mettre à jour, vous pouvez utiliser la boîte de sélection de filtres pour voir un résumé de l'installation et savoir ainsi précisément ce qui arrivera à chaque paquetage en cliquant sur 'Accepter'. Utilisez les cases à cocher à gauche pour filtrer les paquetages à voir dans la fenêtre d'affichage individuel des paquetages. Si, par exemple, vous souhaitez uniquement vérifier quels paquetages sont déjà installés, désactivez toutes les cases à cocher dès le démarrage à l'exception de 'Conserver'.

L'état des paquetages dans la fenêtre d'affichage individuel peut être modifié comme à votre habitude. Cependant un paquetage peut alors ne plus remplir les conditions du filtre de recherche. Si vous souhaitez également éliminer ces paquetages de la liste, actualisez celle-ci en cliquant sur 'Actualiser la liste'.

La fenêtre de paquetage

Selon le filtre sélectionné, la liste des paquetages affichés dans la fenêtre d'affichage individuel des paquetages diffère. Par exemple, si le filtre 'Sélections' est actif, les paquetages affichés sont ceux appartenant à la sélection faite.

Dans le gestionnaire de paquetages, chaque paquetage à un état logique qui définit ce qui doit arriver au paquetage, par exemple "Installer" ou "Supprimer". Comme dans le filtre de sélections, cet état est symbolisé dans une boîte d'état au début de la ligne. Ici aussi, vous pouvez modifier l'état du paquetage en les faisant défiler avec la souris ou à l'aide du menu contextuel que vous ouvrez avec le bouton de droite de la souris. Il existe toute une série d'états, qui sont sélectionnables ou non, selon la situation globale actuelle. Par exemple, il n'est pas possible de sélectionner l'état "Supprimer" pour un paquetage qui n'est pas encore installé. Pour savoir quels sont les différents états et les symboles correspondants, sélectionnez 'Symboles' dans le menu 'Aide'.

Le gestionnaire de paquetages contient les états suivants pour les paquetages :

Ne pas installer Ce paquetage n'est pas installé et ne sera pas installé.

Installer Ce paquetage n'est pas encore installé mais va être installé.

Conserver Ce paquetage est déjà installé et ne sera pas modifié.

Actualiser Ce paquetage est déjà installé et sera remplacé par la version disponible sur le support d'installation.

Supprimer Ce paquetage est déjà installé et sera supprimé.

Tabou – ne jamais installer Ce paquetage n'est pas installé et ne sera jamais installé, quelques soient les circonstances. Il sera traité comme s'il n'existait sur aucun support d'installation. Par exemple, si un paquetage doit être ajouté automatiquement pour résoudre les dépendances, avec "Tabou", vous vous assurez qu'il ne sera pas installé. Les inconsistances qui en résultent devront alors être résolues manuellement. Pour cette raison, "Tabou" est une option destinée principalement aux experts.

Protégé Ce paquetage est installé et ne doit pas être modifié car cela pourrait provoquer des dépendances non résolues avec d'autres paquetages. Les paquetages de tiers (sans signature SUSE) se voient attribuer cet état de façon automatique pour ne pas être remplacés par des paquetages plus récents présents sur le support d'installation. Ceci pourrait provoquer des conflits entre paquetages qui devraient être résolus manuellement (pour experts).

Installation automatique Le gestionnaire de paquetages a automatiquement sélectionné ce paquetage pour l'installer parce qu'il est nécessaire à un autre paquetage (résolution des dépendances entre paquetages).

Remarque

Pour désélectionner un de ces paquetages, il est possible que vous ayez à utiliser l'état "Tabou".

Remarque

Actualisation automatique Ce paquetage est déjà installé. Il est nécessaire, dans une version plus récente, à un autre paquetage. La version installée sera donc mise à jour de façon automatique.

Suppression automatique Ce paquetage est déjà installé mais il existe un conflit entre paquetages qui rendent obligatoire la suppression de ce paquetage. Cela peut être le cas, par exemple, lorsqu'un autre paquetage remplace l'actuel.

Installation automatique (après sélection)
Ce paquetage a été sélectionné automatiquement pour être installé parce qu'il fait partie d'une sélection prédéfinie (par exemple "Multimédia" ou "Développement").

Mise à jour automatique (après sélection)
Ce paquetage est déjà installé mais il existe une version plus récente sur le support d'installation. Il fait partie d'une sélection prédéfinie (par exemple "Multimédia" ou "Développement") et est donc sélectionné et actualisé automatiquement.

Suppression automatique (après sélection)
Ce paquetage est déjà installé mais une sélection prédéfinie (par exemple "Multimédia" ou "Développement") rend sa suppression nécessaire.

En outre, il est possible de spécifier si vous souhaitez installer les sources d'un programme avec celui-ci. Cette information complète l'état du paquetage et ne peut donc être sélectionnée manuellement. À la place, une case à cocher à la fin de la ligne de description du paquetage permet la sélection des paquetages sources. Vous pouvez également trouver cette option dans le menu 'Paquetage'.

Installer les sources Le code source sera installé.

Ne pas installer les sources Le code source ne sera pas installé.

Les couleurs de caractères utilisées dans la fenêtre d'affichage individuel des paquetages apportent des informations supplémentaires. Les paquetages déjà installés qui sont disponibles dans une nouvelle version sur le support d'installation, sont affichés en bleu. Inversement, les paquetages dont la version installée est plus récente que celle présente sur le support d'installation, sont affichés en rouge. Cependant, étant donné que la numérotation des paquetages n'est pas toujours linéaire, il peut être difficile de déterminer quelle version est la plus récente. Les informations fournies ne sont donc pas absolument certaines mais suffisent généralement à indiquer les paquetages problématiques. Pour voir le numéro exact de la version, utilisez la fenêtre d'informations.

La fenêtre d'informations

En bas, à droite, vous pouvez voir la fenêtre dans laquelle sont affichées, au moyen d'onglets, différentes informations relatives au paquetage sélectionné, telles que la description détaillée qui est affichée au démarrage, les données techniques (taille, groupe, etc.), une liste des dépendances et la version du paquetage.

La fenêtre de ressources

La fenêtre de ressources qui se trouve en bas à gauche affiche l'espace disque nécessaire à l'installation de votre sélection de paquetages courante sur les systèmes de fichiers montés pendant le processus de sélection de paquetages. L'occupation de l'espace dans chaque système de fichiers est indiqué sous forme de diagramme à barres de couleur. Le vert signifie qu'il a encore "beaucoup d'espace". Plus l'espace disque "diminue", plus la couleur des barres passe au rouge. Les valeurs affichées sont virtuelles et ne représentent que l'occupation d'espace qui aurait lieu si la sélection actuelle était installée. Si vous avez sélectionné trop de paquetages pour l'espace disque disponible, une fenêtre d'alerte apparaît.

La barre de menus

La barre de menus dans la partie supérieure de la fenêtre permet également d'accéder à la majorité des fonctions déjà décrites et contient quatre menus :

Fichier L'option 'Exporter' sous 'Fichier' permet de créer une liste de tous les paquetages installés et de les enregistrer dans un fichier texte. Ceci est pratique si vous souhaitez reproduire exactement la même installation à un autre moment ou sur un autre système. Avec la fonction 'Importer', vous pouvez charger un fichier créé de cette façon et générer ainsi exactement la même sélection de paquetages que celle qui a été enregistrée. Dans les deux cas, vous pouvez décider librement où enregistrer le fichier ou bien accepter la proposition du système.

L'option 'Sortir – défausser les modifications' sert à sortir du gestionnaire de paquetages en défaussant toutes les modifications qui ont été réalisées dans la sélection de paquetages depuis le démarrage du gestionnaire. Si par contre, vous sélectionnez 'Sortir – enregistrer les modifications'. Dans ce cas, les modifications sont prises en compte et le programme est fermé ensuite.

Paquetage Les options du menu 'Paquetage' s'appliquent toujours au paquetage actuellement affiché dans la fenêtre d'affichage individuel de paquetages. Bien que tous les états qu'un paquetage peut avoir soient indiqués, vous ne pourrez sélectionner que ceux qui sont possibles et relevants pour ce paquetage. Les cases à cocher vous permettent également d'installer les sources avec le programme. L'option 'Tous ceux de la liste' ouvre un sous-menu qui contient encore tous les états du paquetage. Cependant, un choix dans cette liste ne s'appliquera pas seulement au paquetage courant, mais à *tous* les paquetages de la liste.

Extras Le menu 'Extras' contient des options de gestion des dépendances et conflits entre paquetages. Après avoir sélectionné manuellement les paquetages pour votre installation, cliquez sur 'Afficher les changements automatiques de paquetages'. Une liste des paquetages sélectionnés automatiquement par le gestionnaire de paquetages pour résoudre les dépendances est affichée. S'il existe encore des conflits entre paquetages non résolus, une fenêtre contenant des propositions de solutions apparaît.

Lorsque vous activez l'option "Ignorer" pour les conflits entre paquetages, cette option est enregistrée de façon permanente dans le système. Sinon, vous devriez activer l'option "Ignorer" pour les mêmes paquetages lors de chaque démarrage du gestionnaire de paquetages. Pour désactiver cette option, utilisez 'Réinitialiser les conflits de dépendances ignorés'.

Aide L'option 'Aperçu' du menu 'Aide' affiche un résumé du fonctionnement du gestionnaire de paquetages. Vous trouverez une explication détaillée des états des paquetages et de leurs symboles en sélectionnant l'option 'Symboles'. Si vous souhaitez utiliser le programme sans faire appel à la souris, vous pouvez obtenir une description des combinaisons de touches à l'aide du point de menu 'Touches'.

Vérification des dépendances

Sous la fenêtre d'informations, se trouvent le bouton 'Vérifier les dépendances' et la case à cocher 'Vérification automatique'. Si vous cliquez sur le bouton 'Vérifier les dépendances', le gestionnaire de paquetages contrôle l'existence de dépendances non résolues ou de conflits dans la sélection de paquetages actuelle. En cas de dépendances non résolues, les paquetages nécessaires à la résolution des dépendances seront automatiquement sélectionnés. En cas de conflits entre paquetages, le gestionnaire de paquetages ouvre une fenêtre pour les visualiser et vous propose des possibilités de solution.

Si vous activez 'Vérification automatique', le processus de vérification décrit ci-dessus est effectué à chaque fois que l'état d'un paquetage est modifié. Ceci est pratique parce qu'ainsi les dépendances entre paquetages sont vérifiées en permanence. Cependant cela consomme des ressources et peut ralentir considérablement le fonctionnement du gestionnaire de paquetages. Pour cette raison, la vérification automatique n'est pas activée au démarrage du gestionnaire de paquetages. Vous pouvez choisir l'option qui vous semble la plus pratique. Néanmoins, la vérification des dépendances est toujours faite lorsque vous validez votre sélection en cliquant sur 'Accepter'.

Dans l'exemple suivant, les paquetages `sendmail` et `postfix` ne peuvent pas être installés simultanément. Dans la figure 2.5 page suivante, vous pouvez voir le message de conflit qui vous appelle à prendre une décision. `postfix` est déjà installé, vous pouvez donc renoncer à l'installation de `sendmail`, éliminer `postfix` ou prendre le risque d'ignorer le conflit.

Attention

Traitement des conflits de paquetages

Suivez les conseils de YaST pour le traitement des conflits de paquetages car cela peut affecter la stabilité et la fonctionnalité de votre système.

Attention

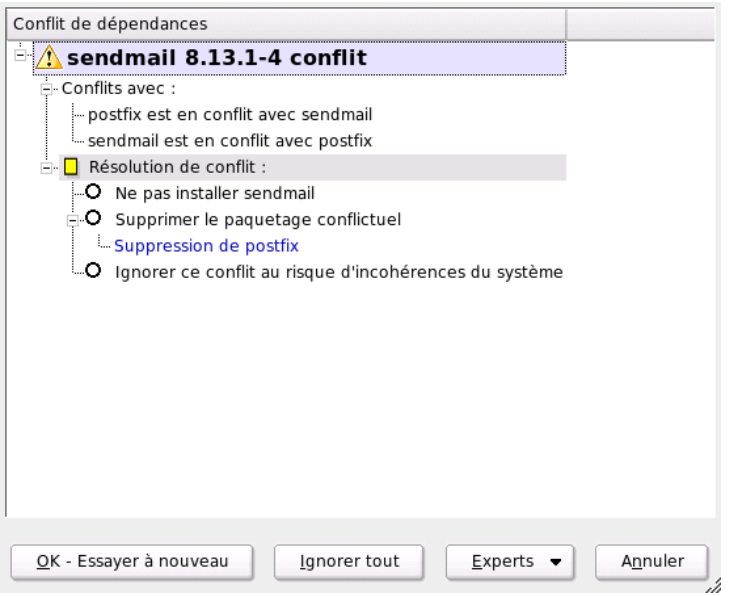


FIG. 2.5: *Gestion de conflits par le gestionnaire de paquetages*

2.3.4 Mise à jour du système

Ce module vous permet d'actualiser votre système. Si votre système est en fonctionnement, vous ne pourrez mettre à jour que les logiciels d'applications mais pas le système de base SUSE LINUX. À cette fin, vous devez amorcer depuis le support d'installation, par exemple à partir du CD. Lors de la sélection du mode d'installation dans YaST, sélectionnez 'Mise à jour du système installé' au lieu de 'Nouvelle installation'.

Le processus de mise à jour ressemble beaucoup à une nouvelle installation du système. YaST vérifie tout d'abord l'état actuel de votre système, détermine une stratégie de mise à jour appropriée et présente les résultats dans un dialogue de propositions. Comme pendant l'installation, vous pouvez également sélectionner les différentes options à l'aide de la souris pour procéder à des modifications individuelles. La majorité des options telles que 'Langue' et 'Disposition du clavier' ont déjà été expliquées dans la section (*Sélection de la langue* page 13) relative à l'installation. En conséquence, nous nous en tiendrons ici à vous expliquer les éléments spécifiques à la mise à jour.

Sélectionné pour la mise à jour

Si différentes versions de SUSE LINUX sont installées sur votre système, vous pouvez sélectionner ici la partition que vous souhaitez mettre à jour. La liste affiche toutes les partitions qui peuvent être actualisés.

Options de mise à jour

Sélectionnez la méthode de mise à jour de votre système. Vous disposez de deux possibilités différentes.

Mise à jour avec installation de nouveaux logiciels
: Si vous souhaitez mettre à jour tout le système, vous pouvez choisir l'une des sélections prédéfinis. Ces sélections sont les mêmes que celles offertes lors de l'installation et permettent également l'installation de nouveaux paquetages.

Mise à jour des paquetages installés uniquement
: Avec cette option, uniquement les paquetages déjà installés sur le système seront mis à jour. Aucun nouveau logiciel ne sera installé.

Vous pouvez également, avec l'option 'Supprimer les paquetages obsolètes', spécifier si les paquetages qui ne sont pas disponibles dans la nouvelle version doivent être effacés. Cette option est sélectionnée par défaut pour éviter que les paquetages obsolètes n'occupent de l'espace disque inutilement.

Paquetages

En cliquant sur 'Paquetages', vous démarrez le gestionnaire de paquetages et vous pourrez y sélectionner ou désélectionner individuellement les paquetages pour la mise à jour. Les conflits entre paquetages qui peuvent apparaître pourront y être résolus à l'aide de la vérification des dépendances. L'utilisation du gestionnaire de paquetages a été expliquée en détails dans la section *Installer/supprimer des logiciels* page 50.

Sauvegarde

Lors de la mise à jour du système, il est possible que les fichiers de configuration de certains paquetages soient remplacés par ceux de la nouvelle version. Vous pouvez avoir modifié ces fichiers dans votre système actuel (avant mise à jour), par conséquent, ceux-ci sont sauvegardés avant la mise à jour. Ce dialogue vous permet de déterminer si ces sauvegardes doivent être effectuées et quelle doit être leur importance.

Remarque

Contenu de la sauvegarde

Veuillez noter que ces sauvegardes ne concernent pas le logiciel mais les fichiers de configuration correspondants.

Remarque

Conseils importants au sujet de la mise à jour

La mise à jour d'un système est, d'un point de vue technique, une opération extrêmement complexe. À cette occasion, YaST doit, pour chaque paquetage logiciel, vérifier quelle version est installée puis définir ce qui doit être fait afin que la nouvelle version remplace correctement l'ancienne. YaST s'assure de reprendre, dans la mesure du possible, pour chaque paquetage installé concerné, les configurations personnelles existantes afin de vous éviter de reconfigurer vos paramètres à chaque fois. Dans certains cas, certains problèmes de configuration peuvent se présenter après la mise à jour si l'ancienne configuration n'est pas compatible avec la nouvelle version du programme ou parce qu'il y a une inconsistance imprévisible entre différentes configurations.

En outre, une mise à jour pose d'autant plus de problèmes que la version à actualiser est ancienne. Des difficultés sont aussi à prévoir si la configuration des paquetages à actualiser s'éloigne du standard. Il est parfois impossible de reprendre correctement une ancienne configuration et il est alors nécessaire d'en créer une nouvelle. Une configuration existante devrait toujours être sauvegardée avant le début de la mise à jour.

2.4 Matériel

Les nouveaux composants matériels doivent tout d'abord être intégrés ou connectés selon les instructions fournies par le constructeur. Activez les périphériques externes tels que l'imprimante ou le modem et lancez le module YaST correspondant. Les composants matériels que l'on trouve habituellement dans le commerce sont, pour la plupart, reconnus automatiquement par YaST qui affiche ensuite leurs données techniques. Si la détection automatique se solde par un échec, YaST vous présentera une liste (par exemple, noms de modèles/constructeurs) dans laquelle vous pourrez sélectionner le périphérique adéquat. Consultez la documentation relative à votre matériel si les informations inscrites sur votre périphérique ne sont pas suffisantes.

Remarque

Noms de modèles

Attention aux noms de modèles : si votre modèle ne figure pas dans la liste, vous pouvez toujours faire un essai en sélectionnant un nom similaire. Dans certains cas, il est cependant indispensable de spécifier le nom exact en tenant compte de chaque lettre ou numéro car un nom similaire ne permet pas toujours de conclure qu'il s'agit d'un périphérique compatible.

Remarque

2.4.1 Lecteurs CD et DVD

Lors de l'installation, tous les lecteurs de CD ROM détectés sont intégrés au système, c'est à dire que les entrées correspondantes seront faites dans le fichier `/etc/fstab` et les sous-répertoires `/media` seront créés. Avec ce module de YaST, vous pouvez également intégrer au système des unités montées ultérieurement.

Une fois que le module est démarré, une liste contenant toutes les unités détectées est affichée. Sélectionnez le nouveau lecteur en cochant la case au début de la ligne, puis cliquez sur 'Terminer'. Le nouveau lecteur est maintenant intégré au système et peut être utilisé.

2.4.2 Imprimante

Sous Linux, les imprimantes sont pilotées par des files d'attente d'impression (en anglais *queues*). Les données à imprimer sont stockées temporairement dans la file d'attente d'impression et envoyées les unes après les autres à l'imprimante par le spouleur d'impression.

La plupart du temps, ces données se présentent sous une forme qui ne permet pas de les envoyer directement à l'imprimante. Un graphique, par exemple, doit d'abord être converti dans un format que l'imprimante peut directement traiter. La conversion dans le langage de l'imprimante est faite par le filtre d'impression.

Exemples de langages d'impression usuels

Pour simplifier, on peut répartir les langages d'impression usuels dans les trois groupes qui suivent :

Texte ASCII Toute imprimante normale peut directement imprimer du texte ASCII. Par ailleurs, il existe des imprimantes qui n'impriment pas de texte ASCII directement, mais que l'on peut piloter grâce à l'un des langages d'impression usuels suivants.

PostScript PostScript est le langage par défaut de l'impression sous Unix/Linux. De tels travaux d'impression peuvent être rendus directement sur les imprimantes PostScript.

PCL3, PCL4, PCL5e, PCL6, ESC/P, ESC/P2, ESC/P Raster
Si ce n'est pas une imprimante PostScript qui est connectée, le filtre d'impression utilise Ghostscript pour convertir les données dans l'un de ces autres langages d'impression usuels. Dans ce cas, le pilote qui s'adapte le mieux possible au modèle d'imprimante est utilisé, afin de pouvoir respecter les particularités du modèle (par exemple le réglage des couleurs).

Déroulement du travail d'impression sous Linux

1. L'utilisateur ou un programme d'application génère un nouveau travail d'impression.
2. Les données à imprimer sont stockées temporairement dans la file d'attente d'impression, d'où elles sont transmises au filtre d'impression par le spouleur d'impression.
3. Le filtre d'impression se charge alors des tâches suivantes :
   (a) Le type des données à imprimer est déterminé.
   (b) Si les données ne sont pas en PostScript, elles sont d'abord converties dans le langage standard PostScript.
   (c) Si nécessaire, les données en PostScript sont converties dans un autre langage d'impression.
   - Si une imprimante PostScript est connectée, les données en PostScript sont envoyées directement à l'imprimante.
   - Si ce n'est pas une imprimante PostScript qui est connectée, le programme Ghostscript intervient avec un pilote Ghostscript adapté au langage d'impression du modèle d'imprimante utilisé, afin de générer les données adaptées à l'imprimante, lesquelles sont ensuite envoyées à l'imprimante.
4. Dès que le travail d'impression a été envoyé en totalité à l'imprimante, le spouleur d'impression retire le travail de la file d'attente.

Imprimantes prises en charge

Étant donné que les pilotes d'impression pour Linux ne sont souvent pas développés par le fabricant du matériel, il est nécessaire que l'imprimante puisse être pilotée au moyen d'un langage d'impression bien connu. Les imprimantes normales comprennent au moins un des langages d'impression connus. Si en revanche le fabricant y renonce et construit une imprimante qui ne peut être pilotée qu'avec des séquences de commande spéciales, il s'agit alors d'une imprimante GDI (comme par exemple un grand nombre d'imprimantes à jet d'encre bon marché) qui, à l'origine, ne fonctionne que sous la version de système d'exploitation pour lequel le fabricant a fourni un pilote. Comme la manière de piloter ce type d'imprimante ne correspond à aucune norme courante, leur utilisation sous Linux est souvent source de difficultés.

SUSE LINUX prend tout de même en charge quelques-unes de ces imprimantes. Toutefois, elles sont souvent problématiques et, pour certains modèles, on peut être soumis à des restrictions comme par exemple ne pouvoir imprimer qu'en noir et blanc et à faible résolution. Pour plus d'informations sur l'utilisation de ces périphériques, reportez-vous également aux sections *Imprimantes propriétaires, le plus souvent des imprimantes GDI* page 293 et *Imprimante sans langage d'impression standard* page 306. 2004-07-29 10:21:47 CEST

Configuration avec YaST

Pour installer l'imprimante, choisissez 'Matériel' dans le Centre de Contrôle YaST, puis 'Imprimante'. La fenêtre principale de configuration des imprimantes s'ouvre. Dans la partie supérieure, la liste des imprimantes reconnues et, dans la partie inférieure, les files d'attente déclarées s'affichent. Lorsqu'une imprimante n'a pas été reconnue automatiquement, vous pouvez l'installer manuellement.

Configuration automatique

YaST permet de configurer automatiquement l'imprimante lorsque la connexion parallèle ou USB a été configurée automatiquement de façon correcte et que l'imprimante qui y est connectée a été reconnue automatiquement. La base de données des imprimantes contient l'identification du modèle d'imprimante que YaST a obtenu lors de la reconnaissance automatique du matériel. Pour certaines imprimantes, ce matériel identifié peut différer du nom du modèle. Dans ce cas, il se peut que le modèle ne puisse être choisi que manuellement.

Chaque configuration devrait faire l'objet d'un test d'impression avec YaST pour vérifier qu'elle fonctionne réellement. De plus, la page de test de YaST vous fournit des informations importantes sur la configuration en question.

Configuration manuelle

Lorsqu'une des conditions requises pour la configuration automatique n'est pas remplie ou que l'on souhaite une configuration particulière donnée, celle-ci doit se faire manuellement. Dans la mesure où YaST reconnaît automatiquement le matériel et où la base de données des imprimantes dispose d'informations sur le modèle d'imprimante en choisi, YaST peut transmettre automatiquement les données nécessaires ou proposer une présélection rationnelle.

En tout, les valeurs suivantes doivent être configurées :

Connexion matérielle (interface) La configuration de la connexion matérielle dépend de si YaST a pu détecter l'imprimante lors de la reconnaissance du matériel. Si YaST peut reconnaître automatiquement le modèle de l'imprimante, on peut partir du principe que la connexion matérielle avec l'imprimante fonctionne et qu'il n'y a donc rien à régler. Si YaST n'est pas en mesure de reconnaître automatiquement le modèle de l'imprimante, il est fort probable que la connexion de l'imprimante au niveau matériel ne fonctionnera pas que si elle est configurée à la main.

Nom de la file d'attente Lorsque l'on imprime, on doit souvent indiquer le nom de la file d'attente, et il vaut donc mieux n'utiliser que des noms composés de minuscules et éventuellement de chiffres.

Modèle d'imprimante et fichier PPD Les réglages propres à l'imprimante (par exemple le pilote Ghostscript et les paramètres propres au pilote approprié pour le filtre d'impression) sont enregistrés dans un fichier PPD (en anglais, *PostScript Printer Description* "description d'imprimante PostScript"). Pour plus d'informations sur les fichiers PPD, reportez-vous également à la section *Installation du logiciel* page 294.

Avec de nombreux modèles d'imprimantes, on dispose de plusieurs fichiers PPD (par exemple lorsque plusieurs pilotes Ghostscript fonctionnent). Le choix du fabricant et du modèle permet de ne devoir choisir ensuite que parmi les fichiers PPD appropriés. Si l'on dispose de plusieurs fichiers PPD, YaST en choisit un (normalement celui qui est mis en évidence par la mention "recommended"). On peut au besoin choisir un autre fichier PPD au moyen de 'Modifier'.

Etant donné que pour les imprimantes non PostScript, le filtre d'impression génère les données adaptées à l'imprimante par l'intermédiaire d'un pilote Ghostscript, c'est la configuration du pilote Ghostscript qui va être décisif pour déterminer le type d'impression. C'est la configuration du pilote Ghostscript (via fichier PPD) et les réglages propres au pilote qui déterminent les caractéristiques de l'impression. Si nécessaire, il est possible via 'modifier' de choisir dans le fichier PPD d'autres réglages dépendants de l'imprimante pour le filtre d'impression.

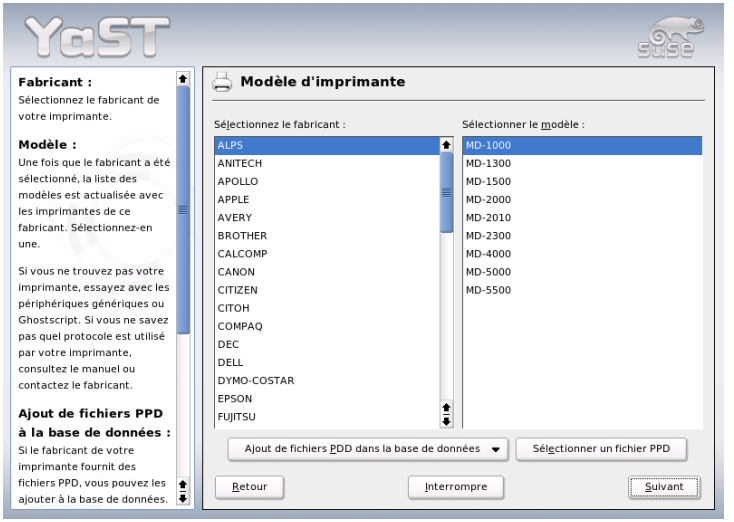


FIG. 2.6: *Configuration de l'imprimante via YaST2 : choix de l'imprimante*

L'impression de la page de test de YaST est indispensable. Si, lors de cette opération, la page de test ne contient que des caractères incompréhensibles (par exemple beaucoup de pages vides), vous pouvez arrêter immédiatement l'impression au niveau de l'imprimante, en retirant tout le papier puis en interrompant le test d'impression.

Si le modèle de l'imprimante ne figure pas dans la base de données des imprimantes, il existe un certain nombre de fichiers PPD génériques pour les langages d'impression usuels, prenez comme "fabricant" UNKNOWN MANUFACTURER.

Autres réglages Vous n'avez normalement rien d'autre à régler.

Configuration des logiciels applicatifs

Les logiciels applicatifs emploient les files d'attente disponibles de la même manière que pour l'impression depuis la ligne de commande. Par conséquent, avec les logiciels applicatifs, ne configurez pas à nouveau l'imprimante, mais utilisez les files d'attente existantes.

Impression depuis la ligne de commande
: En mode la ligne de commande, on imprime avec la commande `lp -d` ⟨*`file_d_attente`*⟩ ⟨*`nom_du_fichier`*⟩ , en remplaçant ⟨*file_d_attente*⟩ et ⟨*nom_du_fichier*⟩ comme il convient.

Impression en mode ligne de commande avec les logiciels applicatifs
: Certains logiciels applicatifs emploient la commande `lp` pour imprimer. Dans le formulaire d'impression du logiciel applicatif, saisissez la commande d'impression appropriée (sans le ⟨*nom_du_fichier*⟩). Par exemple : `lp -d` ⟨*`file_d'attente`*⟩ . Pour cela, il faut modifier la liste déroulante au bas de la boîte de dialogue d'impression des programmes KDE en choisissant 'Impression via un programme externe (générique)', sinon on ne peut pas saisir de commande d'impression.

Impression avec le système d'impression CUPS
: Les programmes de dialogue d'impression comme xpp ou le programme kprinter de KDE permettent non seulement de choisir la file d'attente, mais aussi d'ajuster les options par défaut de CUPS et celles qui sont propres à l'imprimante dans le fichier PPD, au moyen de menus graphiques de sélection. Pour que kprinter soit la boîte de dialogue d'impression uniforme dans différents logiciels applicatifs, saisissez les commandes d'impression `kprinter` ou `kprinter --stdin` dans le formulaire d'impression de ces logiciels applicatifs. La commande d'impression à choisir dépend de ces logiciels. Ainsi, après le formulaire d'impression du logiciel applicatif, la boîte de dialogue d'impression kprinter apparaît, vous permettant d'ajuster la file d'attente ainsi que d'autres options. Avec cette méthode, il faut cependant veiller à ce que les réglages effectués dans le formulaire d'impression du logiciel applicatif et dans kprinter ne se contredisent pas. Il est donc judicieux de n'entreprendre des réglages que dans kprinter.

Problèmes possibles

Lorsque la communication entre l'ordinateur et l'imprimante est défaillante, l'imprimante ne peut pas interpréter correctement les données envoyées, ce qui provoquera l'impression de caractères "aberrants" sur d'énormes quantités de papier. Dans ce cas, reportez-vous à la section *Travaux d'impression erronés ou transfert de données perturbé* page 312.

Informations complémentaires

Pour plus de détails concernant l'impression sous Linux, consultez le chapitre *Imprimante (utilisation)* page 291, des questions d'ordre général ainsi que leurs réponses y sont abordées. De nombreux cas particuliers ont leurs solutions dans la base de données d'assistance. Pour les problèmes d'imprimante, les articles *Drucker einrichten* (en allemand) et *Printer configuration in SUSE LINUX 9.1 on* (en anglais) qu'elle contient vous seront certainement très utiles ; vous les trouverez sous le mot-clé "einrichten" ou "configuration".

`http://portal.suse.com/sdb/en/2004/08/jsmeix_print-einrichten-92.html`

2.4.3 Contrôleur de disques durs

Normalement, YaST configure le contrôleur de disques durs de votre système durant l'installation. Si vous montez des contrôleurs supplémentaires, vous pouvez procéder à leur intégration dans le système avec ce module de YaST. Vous pouvez également modifier la configuration existante, ce qui, cependant, ne devrait pas être nécessaire.

La fenêtre de dialogue offre une liste de tous les contrôleurs de disques durs détectés et permet d'ordonner les modules de noyau adéquats avec des paramètres spécifiques. Utilisez 'Tester le chargement du module' pour vérifier si les configurations actuelles fonctionnent avant de les enregistrer définitivement dans le système.

Attention

Configuration du contrôleur de disques durs

Ceci est un outil pour experts. Si vous procédez ici à une mauvaise configuration, il se peut que le système ne puisse plus amorcer. Quoiqu'il arrive, utilisez toujours l'option de test.

Attention

2.4.4 Carte graphique et moniteur (SaX2)

L'interface graphique, le serveur X, rend possible la communication entre le matériel et les logiciels. Les bureaux comme KDE et GNOME peuvent afficher des informations à l'écran avec lesquelles l'utilisateur peut travailler. Les bureaux et autres applications similaires sont souvent qualifés de *gestionnaire de fenêtres* (*Windowmanager*). Sous Linux il existe de nombreux gestionnaires de fenêtres qui peuvent se différencier énormément les uns des autres tant par leur aspect que par leur fonctionnalité.

L'interface graphique est configurée lors de l'installation. Si vous voulez améliorer les valeurs des paramètres de configuration ou, par exemple, connecter un autre moniteur au système en fonctionnement, utilisez ce module de YaST. Avant toute modification, la configuration actuelle sera enregistrée. Ensuite, la même fenêtre de dialogue que lors de l'installation de SUSE LINUX apparaît. Vous pouvez choisir entre 'Mode texte uniquement' et l'interface graphique. Pour celle-ci, les valeurs actuelles seront affichées : résolution de l'écran, profondeur de couleur, fréquence de rafraîchissement, fabricant et modèle du moniteur si ces données ont été reconnues automatiquement. Si vous venez d'installer votre système ou de connecter une nouvelle carte graphique et voulez l'initialiser pour la première fois, une petite fenêtre apparaît dans laquelle vous devrez préciser si vous voulez activer l'accélération 3D pour votre carte graphique.

Cliquez sur 'Modifier'. Maintenant, SaX2, l'outil de configuration des périphériques d'entrée et de sortie, démarre dans une fenêtre séparée (figure 2.7 page ci-contre).

SaX2 – La fenêtre principale

Dans la barre de navigation à gauche se trouvent quatre options principales : 'Périphériques graphiques', 'Périphériques d'entrée', 'Multihead' et 'AccessX'. Dans 'Périphériques graphiques', vous pouvez configurer le moniteur, la carte graphique, la profondeur de couleur et la résolution ainsi que la taille de l'image. Dans 'Périphériques d'entrée' vous pouvez configurer le clavier et la souris ainsi que, si nécessaire, un écran tactil (*touchscreen*) et une tablette graphique. Dans le menu 'Multihead', vous pouvez configurer une station avec écrans multiples (voir *Multihead* page 76). Vous pouvez définir le mode d'affichage multihead, ainsi que l'ordre des écrans sur votre bureau. 'AccessX' est un outil très pratique pour contrôler le pointeur de la souris avec le pavé numérique du clavier si vous travaillez sur un ordinateur sans souris ou si celle-ci ne fonctionne pas. Vous pouvez ici modifier la vitesse du pointeur de la souris qui est contrôlé à travers la pavé numérique.

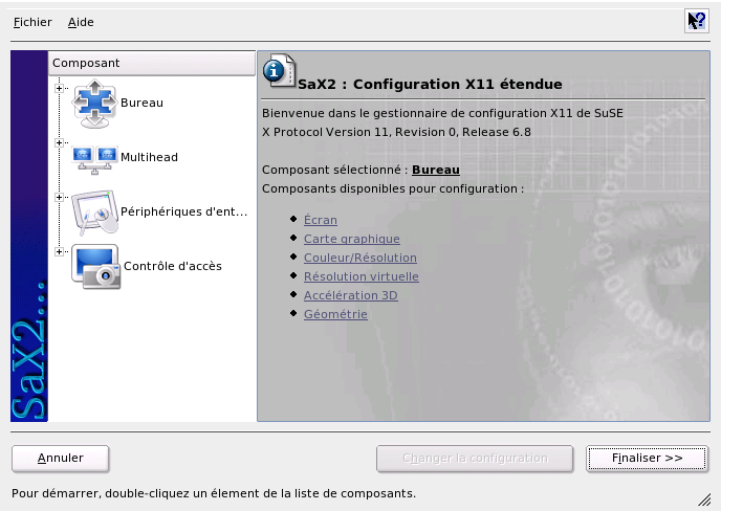


FIG. 2.7: *La fenêtre principale du nouveau SaX2*

Entrez le modèle approprié pour le moniteur et la carte graphique. En général, le système reconnaît automatiquement l'écran et la carte graphique.

Si votre système ne reconnaît pas votre moniteur, le dialogue de selection de moniteurs apparaît avec une liste importante de fabricants et modèles, dans laquelle vous trouverez très probablement le votre. Si ce n'est pas le cas, entrez manuellement les valeurs qui correspondent à votre moniteur ou choisissez la configuration standard, le mode Vesa.

Si vous cliquez, dans la fenêtre principale, sur 'Terminer' une fois que la configuration du moniteur et de la carte graphique est achevée, vous avez la possibilité de procéder à un test de la configuration. De cette façon, vous pouvez vous assurer que la configuration choisie fonctionne sans problème. Si l'image qui est affichée est trouble, interrompez le test en pressant la touche Esc et réduisez la valeur de la fréquence de rafraîchissement de l'image ou bien la résolution ou la profondeur de couleur. Toutes les modifications réalisées – que vous les ayez testées ou non – sont activées lors du redémarrage du système graphique ou du serveur X. Si vous utilisez KDE, il suffit que vous vous déconnectiez puis que vous vous reconnectiez.

Affichage

Sélectionnez ‘Modifier la configuration’ → ‘Propriétés’, une fenêtre contenant les trois onglets‘Moniteur’, ‘Fréquences’ et ‘Avancé’ apparaît.

‘Moniteur’ Sélectionnez ici le fabricant dans la partie gauche de la fenêtre et le modèle dans la partie droite. Si vous avez une disquette de pilotes Linux pour votre moniteur, utilisez-la après avoir cliqué sur ‘Disquette de pilotes’.

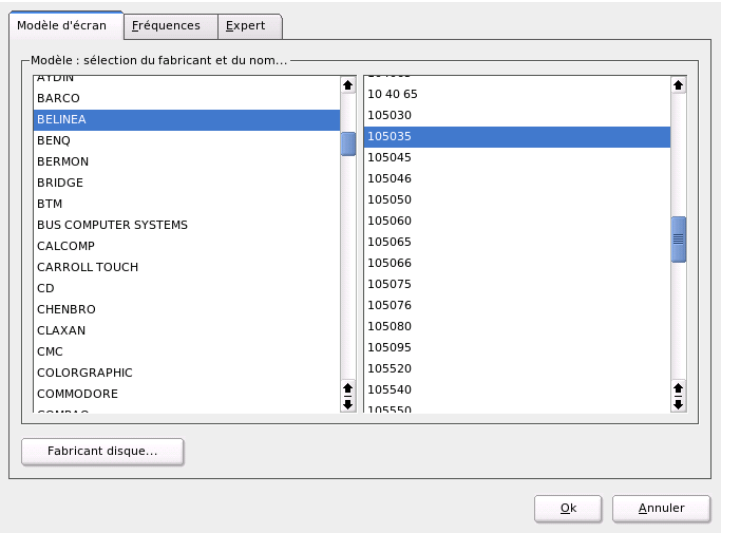


FIG. 2.8: *SaX2 : sélection du moniteur*

‘Fréquences’ Entrez ici les fréquences horizontales et verticales appropriées pour votre moniteur. La fréquence verticale est une autre dénomination de la fréquence de rafraîchissement de l’image. Normalement, ces valeurs sont déterminées automatiquement en fonction du modèle de moniteur et vous n’avez besoin de procéder à aucun changement.

‘Avancé’ Vous pouvez ici configurer encore quelques options pour votre moniteur. Dans le champ de saisie, vous pouvez spécifier la méthode à utiliser pour le calcul de la résolution et de la géométrie de l’écran. Ne procédez ici à des modifications que dans le cas où votre écran a posé des problèmes. Vous pourrez, plus tard changer la taille de l’image et activer le mode de gestion d’énergie DPMS que vous souhaitez.

Attention

Configuration des fréquences du moniteur

Malgré les mécanismes de protection implementés, prenez garde à ce que vous faites lors de l'entrée manuelle des fréquences. Les valeurs erronées peuvent endommager votre moniteur. Consultez le manuel accompagnant votre moniteur avant d'entrer des valeurs manuellement.

Attention

Carte graphique

Dans le dialogue de la carte graphique, vous verrez deux onglets : 'Général' et 'Avancé' :

'Général' – ici, tout comme dans le cas de la configuration du moniteur, vous pouvez entrer le fabricant à gauche et le modèle de la carte graphique à droite.

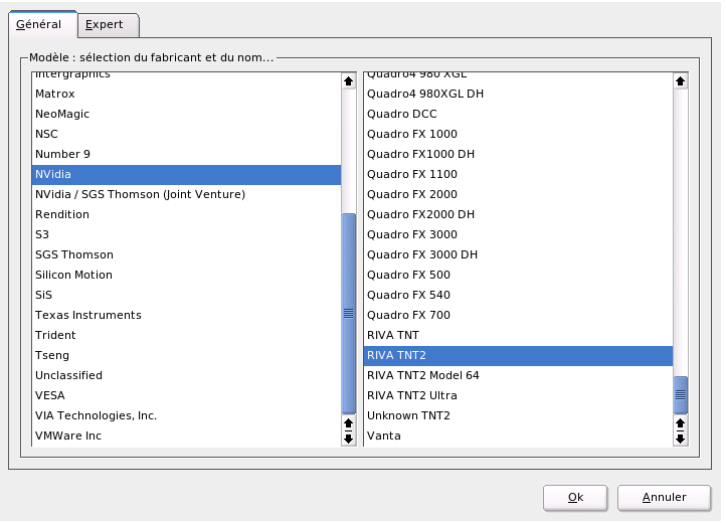


FIG. 2.9: *SaX2 : sélection de la carte graphique*

'Avancé' – vous pouvez ici, à droite, spécifier si vous voulez orienter votre écran verticalement ou horizontalement (ceci ne concerne que certains écrans TFT orientables). Les entrées pour le BusID ne présentent d'intérêt que si vous travaillez avec plus d'un écran. En général, vous n'avez rien à changer ici. Surtout, ne procédez à aucune modification si vous ne connaissez pas la signification des différentes options. Si nécessaire, consultez la documentation qui accompagne votre carte graphique pour connaître la signification des différentes options.

Couleurs et résolution(s)

Ici, vous trouverez trois onglets : 'Couleurs', 'Résolution' et 'Avancé'.

'Couleurs' Selon le matériel utilisé, vous pouvez choisir entre les options de profondeurs de couleur 16, 256, 32768, 65536 et 16,7 millions de couleurs (4, 8, 15, 16 ou 24 bits). Pour une qualité d'affichage raisonnable, sélectionnez au moins 256 couleurs.

'Résolution' Toutes les combinaisons de résolution et profondeur de couleur supportées sans problème par votre matériel vous seront proposées. Ainsi le danger d'endommager votre matériel en utilisant de mauvais paramètres est très réduit avec SUSE LINUX. Si vous souhaitez tout de même modifier manuellement les valeurs de résolution, consultez absolument la documentation de votre matériel pour savoir si les valeurs que vous souhaitez utiliser ne poseront pas de problème.

'Avancé' Ici, vous pouvez ajouter des résolutions à celles offertes dans l'onglet précédent. Celles-ci seront alors ajoutées à la sélection.

Résolution virtuelle

Chaque interface possède une résolution propre, visible sur tout l'écran. Outre cette résolution, vous pouvez configurer une autre résolution plus importante que la zone visible de l'écran. Si vous sortez de l'écran avec le curseur de la souris, vous déplacerez la zone virtuelle dans la zone visible. La taille des pixels ne change pas, mais la surface d'utilisation est plus grande. C'est ce que l'on appelle la résolution virtuelle.

La configuration de la résolution virtuelle peut se faire de deux façons :

'Par glissé-déposé' – si la souris se trouve dans la zone visible de l'écran, le pointeur de la souris se convertit en un réticule. Cliquez sur le bouton de gauche de la souris et maintenez-le enfoncé pendant que vous déplacez la souris, vous modifiez ainsi la taille de la surface marquée. Cette surface affiche la résolution virtuelle correspondant à la résolution réelle représentée sur l'écran. Cette méthode

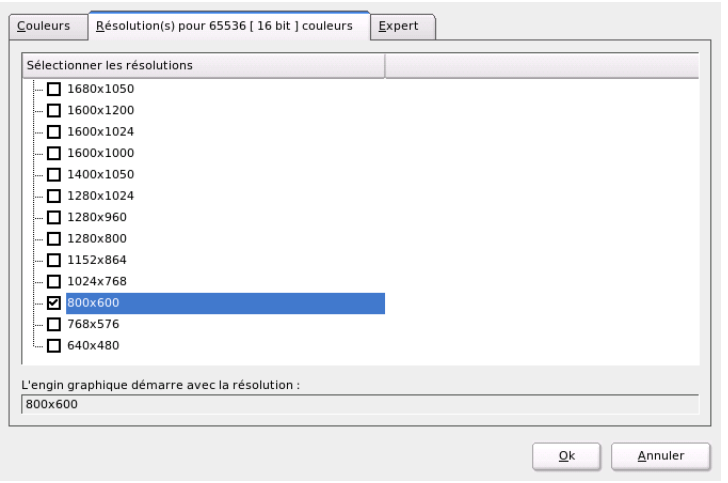


FIG. 2.10: *SaX2 : configuration de la résolution*

de configuration est conseillée lorsque vous ne souhaitez employer comme zone virtuelle qu'une zone déterminée dont vous ne connaissez pas encore exactement la taille.

'À l'aide d'une sélection dans le menu déroulant' – avec le menu déroulant qui se trouve toujours au milieu de la surface marquée, vous pourrez voir la résolution virtuelle configurée actuellement. Si vous savez déjà quelle résolution standard vous souhaitez définir comme résolution virtuelle, sélectionnez-la dans le menu.

Accélération 3D

Si dans la première installation ou lors de la connexion d'une nouvelle carte graphique et de sa configuration, vous n'avez pas activé l'accélération 3D, vous pouvez le faire ici.

Taille et position de l'image

Ici, vous pouvez ajuster, à l'aide des flèches, la taille et la position de l'image (voir figure 2.12 page 77). Si vous travaillez dans un environnement multi-écran *multi-head*, vous pouvez passer sur le moniteur suivant avec le bouton 'Écran suivant' et fixer alors la taille et la position correspondantes. Avec 'Enregistrer', vous enregistrez votre configuration.

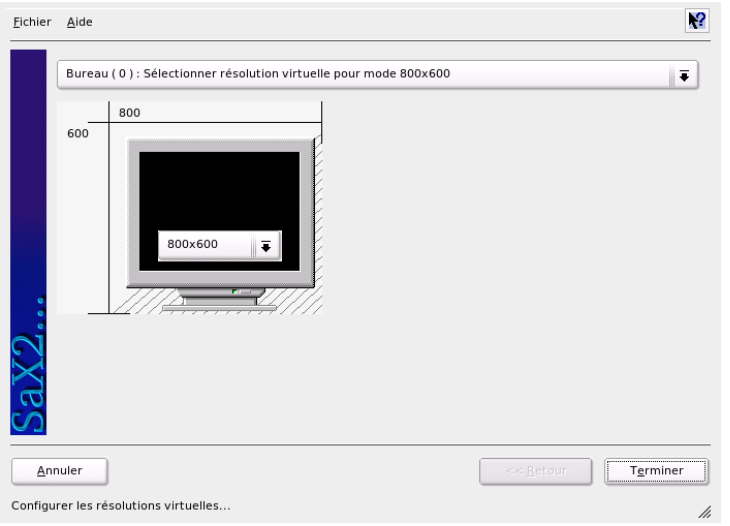


FIG. 2.11: *SaX2 : configuration de la résolution virtuelle*

Attention

Malgré les mécanismes de protection implementés, prenez garde à ce que vous faites lors de l'entrée manuelle des fréquences. Les valeurs erronées peuvent endommager votre moniteur. Consultez le manuel accompagnant votre moniteur avant d'entrer des valeurs manuellement.

Attention

Multihead

Si votre ordinateur est équipé de plus d'une carte graphique ou d'une carte graphique à plusieurs sorties, vous pourrez travailler avec plus d'un écran. Si vous utilisez deux écrans, il s'agit de Dualhead, si vous travaillez avec plus de deux écrans, il s'agit de Multihead. SaX2 détermine automatiquement le nombre de cartes graphiques dans votre système et prépare alors la configuration appropriée. Dans le dialogue multihead de SaX, vous pouvez définir le mode multihead et l'ordre des écrans. Vous pouvez choisir entre trois modes : 'Traditionnel' (par défaut), 'Xinerama' et 'Cloné' :

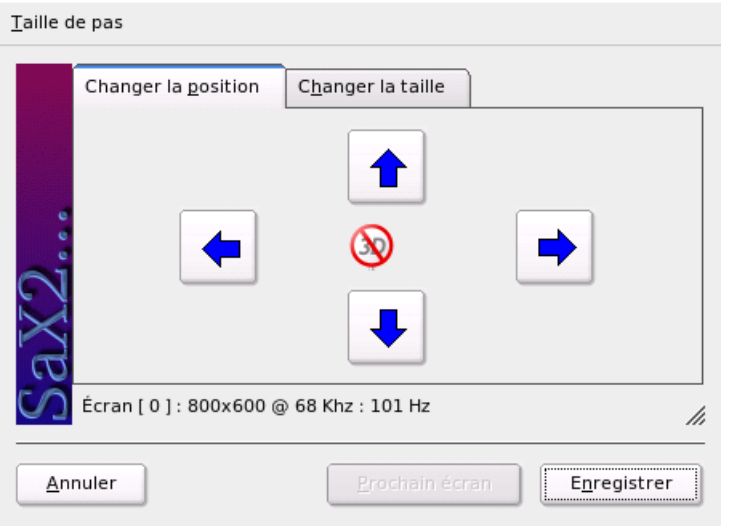


FIG. 2.12: *SaX2 : adaptation de la géométrie de l'image*

'Multihead traditionnel' Chaque moniteur est une unité en soi. Seul le pointeur de la souris peut passer d'un écran à un autre.

'Multihead cloné' Ce mode est utilisé lors de présentations et salons lorsque tout un mur d'écrans est installé. Dans ce mode, tous les moniteurs ont le même contenu. La souris n'apparaît que dans l'écran primaire.

'Multihead Xinerama' Tous les écrans fusionnent en un seul grand écran, c'est à dire que les fenêtres des programmes peuvent être placés sur tous les moniteurs ou avoir une taille supérieure à celle d'un écran.

La disposition d'un environnement multihead décrit la distribution et les relations de comportement entre les différents écrans. Par défaut, SaX2 réalise une disposition en ligne de gauche à droite selon l'ordre des cartes graphiques reconnues. Dans le dialogue 'Disposition' des outils multihead, vous pouvez déterminer l'ordre de vos moniteurs. Pour cela, il vous suffit de déplacer les symboles des écrans avec la souris et de les ordonner comme vous le souhaitez.

Après avoir fermé le dialogue de la disposition, vous pouvez tester la nouvelle configuration en cliquant sur le bouton 'Test'.

Veuillez noter que, pour le moment, Linux n'offre pas l'accélération 3D pour un environnement multihead Xinerama. Dans ce cas, SaX2 désactivera le support 3D.

Périphériques d'entrée

Souris Si le processus de reconnaissance automatique ne reconnaît pas la souris, vous devrez configurer votre souris manuellement. Vous pouvez trouver le type de la souris dans sa documentation. Choisissez la valeur correspondante dans la liste de modèles des souris supportées. Après avoir marqué le modèle adéquat, confirmez la sélection en pressant la touche (5) du pavé numérique.

Clavier Dans le champ de sélection de ce dialogue, vous pouvez déterminer le type de clavier que vous utilisez. En-dessous, vous pouvez choisir la langue pour la disposition du clavier. Finalement, vous pouvez vérifier si cette disposition du clavier fonctionne en saisissant quelques caractères spéciaux dans le champ de test. Saisissez, par exemple, "à", "ç", "é" ou "è".

L'état de la case à cocher qui vous permet d'activer ou de désactiver l'entrée de lettres accentuées dépend de la langue sélectionnée et ne devrait pas être changé. Cliquez sur 'Terminer' pour appliquer les nouveaux paramètres de configuration.

Écran tactil À l'heure actuelle, les écrans tactils des marques Microtouch et Elographics sont supportés par X.Org. SaX2 ne peut reconnaître que le moniteur automatiquement, mais pas le crayon (toucher). Le crayon peut être considéré comme un périphérique d'entrée. Pour le configurer correctement, réalisez les étapes suivantes :

1. Démarrez SaX2 et sélectionnez 'Périphériques d'entrée' → 'Écran tactil'.
2. Cliquez sur 'Ajouter' et ajoutez un écran tactil.
3. Enregistrez la configuration en cliquant sur 'Appliquer'. Il n'est pas absolument nécessaire de tester la configuration.

Les écrans tactils disposent d'une grande variété d'options qui, généralement, doivent tout d'abord être qualibrées. Malheureusement, il n'existe pas d'outil global sous Linux pour cela. La configuration de la taille des écrans tactils étant déjà intégrée dans les valeurs par défaut de la configuration standard, vous n'aurez pas à procéder à une configuration additionnelle.

Tablettes graphiques À l'heure actuelle, X.Org ne supportent que quelques tablettes graphiques. SaX2 permet la configuration des tablettes connectées au port USB comme au port série. Pour la configuration, une tablette graphique peut être considérée comme une souris ou, plus généralement, comme un périphérique d'entrée. Nous vous recommandons de procéder de la manière :

1. Démarrez SaX2 et sélectionnez 'Périphériques d'entrée' → 'Tablette graphique'.
2. Cliquez sur 'Ajouter', sélectionnez le fabricant dans le dialogue suivant et choisissez une tablette graphique dans la liste.
3. Utilisez les cases à cocher à droite pour spécifier si vous utilisez également un crayon et/ou une gomme.
4. Dans le cas d'une tablette connectée à un port série ainsi que pour tous les périphériques d'entrée, vérifiez si la connexion est correcte. `/dev/ttyS0` indique le premier port série, `/dev/ttyS1` le deuxième, etc.
5. Cliquez sur 'Terminer' pour enregistrer la configuration.

AccessX

Si vous voulez travailler sans souris, activez AccessX au démarrage de SaX2. Ainsi, vous pouvez contrôler les mouvements du pointeur sur l'écran à l'aide du pavé numérique de votre clavier (voir tableau 2.1).

TAB. 2.1: *AccessX – contrôle de la souris à l'aide du pavé numérique*

Touche	Description
⊘	Active le bouton de gauche de la souris
⊗	Active le bouton central de la souris
⊖	Active le bouton de droite de la souris
5	Cette touche vous permet de cliquer avec le bouton de la souris que vous activé auparavant. Si vous n'avez activé aucun bouton, c'est le bouton de gauche qui sera utilisé. Une fois que le clic aura été émulé, l'activation de la touche correspondante reviendra à sa configuration standard.
⊕	Cette touche fonctionne comme la touche 5, à la différence qu'elle émule un double-clic.

(0)	Cette touche fonctionne comme la touche (5), à la différence qu'elle émule une pression maintenue sur le bouton de la souris.
(Supr)	Cette touche émule le relâchement du bouton de souris maintenu enfoncé par l'action de la touche (0).
(7)	Déplace la souris vers le coin en haut à gauche
(8)	Déplace la souris en ligne droite vers le haut
(9)	Déplace la souris vers le coin en haut à droite
(4)	Déplace la souris vers la gauche
(6)	Déplace la souris vers la droite
(1)	Déplace la souris vers le coin en bas à gauche
(2)	Déplace la souris en ligne droite vers le bas
(3)	Déplace la souris vers le coin en bas à droite

Vous pouvez, à l'aide du curseur, déterminer la vitesse de déplacement du pointeur de la souris lors de la pression des touches correspondantes.

Informations supplémentaires

Vous pourrez trouver plus d'informations au sujet du système X Windows, son histoire et les propriétés au chapitre *Le système X Window* page 273.

2.4.5 Informations sur le matériel

Pour la configuration des composants matériels, YaST procède à une reconnaissance du matériel. Les données techniques détectées sont affichées dans une fenêtre propre. Ceci est particulièrement utile lorsque vous souhaitez soumettre une requête à notre service d'assistance technique. Pour cela, vous nécessitez des informations sur votre matériel.

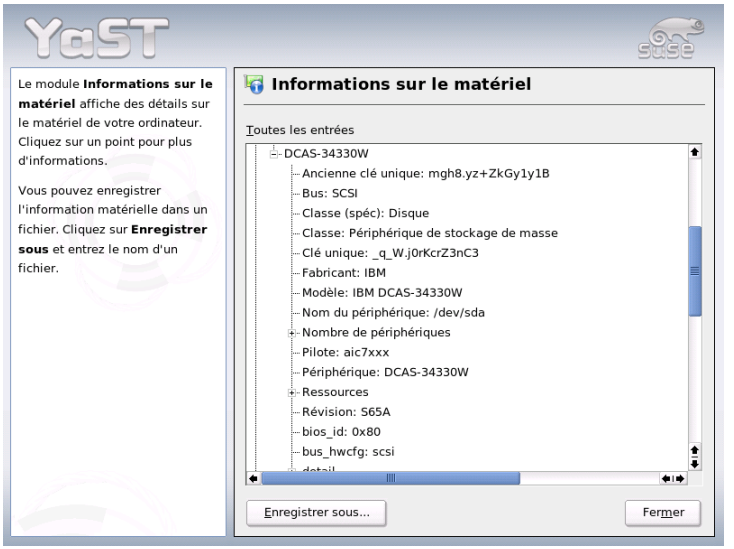


FIG. 2.13: *Affichage des informations sur le matériel*

2.4.6 Mode IDE DMA

Ce module vous permet d'activer ou de désactiver le mode DMA pour le(s) disque(s) dur(s) (IDE) et le(s) lecteur(s) de CD/DVD (IDE) dans le système installé. Ce module ne fonctionne pas pour les périphériques SCSI. Les modes DMA peuvent accroître sensiblement la performance ou la vitesse de transfert de données de votre système.

Lors de l'installation du système, le noyau actuel de SUSE LINUX active automatiquement DMA pour les disques durs et le désactive pour les lecteurs de CD car ceux-ci ont très souvent créé des problèmes lorsque DMA est activé pour tous les lecteurs. Vous pourrez ensuite décider, avec le module DMA, d'activer ou non ce mode pour vos lecteurs. En cas de problèmes, par exemple, dans le fonctionnement de votre disque dur, il peut être utile de désactiver DMA. Inversement, vous pouvez améliorer le taux de transfert de données de votre lecteur de CD en activant DMA si le lecteur supporte ce mode sans problème.

Remarque

DMA (=**D**irect **M**emory **A**ccess) signifie qu'il y a un accès direct à la memoire, c'est à dire que les lecteurs peuvent transférer vos données directement dans la mémoire de travail sans qu'il soit nécessaire de faire un détour par le processeur.

Remarque

2.4.7 Joystick

Avec ce module, vous pouvez configurer votre joystick en sélectionnant le fabricant et le modèle adéquats dans la liste affichée. Avec 'Test', vous pouvez vérifier si le joystick fonctionne correctement. Le dialogue de test affiche trois diagrammes à barres pour les axes analogiques du joystick et des marques pour les quatre boutons standards. Si vous bougez le joystick ou appuyez sur les boutons, la réaction correspondante doit apparaître dans le dialogue de test. Étant donné que la majorité des joysticks sont connectés à la carte son, vous pouvez également accéder à ce module depuis la configuration de la carte son (voir ci-après).

2.4.8 Sélectionner le modèle de souris

Ce module de YaST vous donne la possibilité de configurer le modèle de la souris que vous utilisez. Le processus de sélection de la souris a déjà été expliqué dans le cadre de l'installation personnalisée. Veuillez donc vous reporter à la section *Souris* page 15.

2.4.9 Scanneur

Si vous avez connecté et activé votre scanneur, celui-ci devrait être reconnu automatiquement au lancement de ce module de YaST. Vous verrez alors apparaître le dialogue d'installation du scanneur. Si aucun scanneur n'a été détecté, la procédure se poursuivra avec la configuration manuelle. Si vous avez déjà installé un ou plusieurs scanneurs, vous verrez s'afficher un tableau synoptique avec une liste des scanneurs présents que vous pourrez modifier ou supprimer. Avec 'Ajouter', vous pourrez intégrer un nouveau scanneur.

Il sera ensuite effectué une installation avec des paramètres standards. Si le processus d'installation a abouti, vous en serez informé par un message. Vous aurez alors la possibilité de tester votre scanneur en plaçant un document sur celui-ci et en cliquant sur 'Tester'.

Le scanneur n'a pas été détecté

Tenez présent à l'esprit que seuls les scanneurs supportés peuvent être détectés automatiquement. Les scanneurs utilisés sur une autre machine connectée au réseau ne sont pas reconnus non plus. Il convient, lors de la configuration manuelle, de faire une distinction entre les scanneurs USB, les scanneurs SCSI et les scanneurs réseau.

Scanneur USB Vous devez ici spécifier le nom du constructeur ou du modèle. YaST tente de charger des modules USB. Si vous possédez un scanneur très récent, il est possible que les modules ne puissent pas être chargés automatiquement. Dans ce cas, vous arriverez à un dialogue qui vous donne la possibilité de charger à la main le module USB. Lisez à ce sujet le texte d'aide de YaST.

Scanneur SCSI Spécifiez le nom du périphérique (par exemple, `/dev/sg0`). Remarque : un scanneur SCSI ne doit pas être connecté ou déconnecté lorsque le système est en fonctionnement. Arrêtez tout d'abord votre système.

Scanneur réseau Il vous faut ici l'adresse IP ou le nom d'hôte. Pour la configuration d'un scanneur en réseau, lisez l'article de la base de données support *Scanner under Linux* (`http://sdb.suse.de/`, mot clé `Scanner`).

Si votre scanneur n'a pas été détecté, il est probable qu'il ne soit pas supporté. Il peut cependant arriver que même des scanneurs supportés ne soient pas détectés. Dans un tel cas, vous pourrez aussi avoir recours à la sélection manuelle du scanneur. Si vous pouvez identifier votre scanneur dans la liste des constructeurs et des modèles, sélectionnez-le tout simplement. Sinon, cliquez sur 'Annuler'. Vous trouverez des informations sur les scanneurs fonctionnant avec Linux sous `http://cdb.suse.de` ou `http://www.mostang.com/sane`.

Attention

Assignation manuelle du scanneur

Ne procédez à l'assignation manuelle du scanneur que si vous êtes sûr de ne commettre aucune erreur. Une sélection inappropriée risque d'endommager votre matériel.

Attention

Dépannage

Si votre scanneur n'a pas été détecté, ceci peut être dû aux causes suivantes :

- Le scanneur n'est pas supporté. Sous `http://cdb.suse.de/`, vous trouverez une liste des périphériques compatibles avec Linux.
- Le contrôleur SCSI n'est pas correctement installé.
- Il y a des problèmes de terminaison avec votre port SCSI.
- La longueur du câble SCSI dépasse la limite admise.
- Le scanneur est doté d'un contrôleur Light SCSI qui n'est pas supporté par Linux.
- Le scanneur est éventuellement défectueux.

Attention

Un scanneur SCSI ne doit en aucun cas être connecté ou déconnecté pendant le fonctionnement du système. Arrêtez d'abord votre système.

Attention

Vous trouverez des informations plus détaillées sur les scanneurs dans le *Guide de l'utilisateur* au chapitre `kooka`.

2.4.10 Son

Au lancement du module de configuration du son, YaST tente de détecter automatiquement votre carte son. Si vous le souhaitez, vous pouvez configurer une ou plusieurs cartes son. Si vous souhaitez configurer plusieurs cartes, sélectionnez tout d'abord l'une des cartes que vous voulez utiliser. Avec le bouton 'Configurer', vous arriverez au menu 'Configuration'. Avec le bouton 'Modifier', vous pourrez, sous 'Configuration du son', modifier les paramètres d'une carte déjà configurée. Un clic sur le bouton 'Terminer' enregistre votre configuration actuelle et achève le processus de configuration du son. Dans le cas où YaST ne reconnaîtrait pas automatiquement votre carte son, vous pouvez, dans le menu 'Configuration du son', passer à 'Sélection manuelle de la carte son' en cliquant sur le bouton 'Ajouter une carte son'. Vous avez alors la possibilité de choisir une carte son ainsi que le module adéquat.

Configuration

Avec 'Configuration automatique rapide', vous n'aurez pas à parcourir d'autres étapes de configuration et il ne sera pas effectué de test sonore. La configuration de votre carte son sera achevée ici. Avec 'Configuration normale', vous avez la possibilité de régler le volume de sortie dans le menu 'Volume de la carte son' et de lire un échantillon sonore.

Avec 'Configuration avancée' et la possibilité de changer les options, vous arriverez au menu 'Options avancées pour la carte son' qui vous permet de modifier manuellement les options des modules son.

En outre, vous pouvez ici configurer votre joystick, en cliquant sur la case à cocher du même nom. Un dialogue apparaît dans lequel vous devez sélectionner le modèle de votre joystick puis cliquer sur 'Suivant'. Le même dialogue apparaît également si vous cliquez sur 'Joystick' dans le centre de contrôle de YaST.

Volume de la carte son

Dans ce masque, vous pouvez tester la configuration de votre carte son. Avec les boutons '+' et '-', vous pouvez régler le volume sonore. Nous vous conseillons de commencer à environ 10% pour ne pas endommager vos haut-parleurs et ne faire courir aucun risque à vos oreilles. Après avoir cliqué sur le bouton 'Tester', vous devriez entendre un échantillon sonore. Si vous n'entendez rien, ajustez le volume. En cliquant sur 'Suivant', vous terminez la configuration du son et enregistrez les paramètres du volume.

Configuration du son

Avec l'option 'Supprimer', vous pouvez éliminer une carte son. Les entrées concernant les cartes son déjà configurées seront désactivées dans le fichier `/etc/modprobe.d/sound`. Sous 'Options', vous pouvez accéder au menu 'Options avancées pour la carte son'. Vous avez ici la possibilité d'adapter manuellement les options des modules son. Dans le menu 'Mixer', vous pouvez régler le niveau d'entrée et de sortie des différentes cartes son. Avec 'Suivant', vous enregistrez les nouveaux paramètres et avec 'Retour', vous restaurez les valeurs initiales. Avec 'Ajouter la carte son...', vous pouvez intégrer des cartes son supplémentaires. Si YaST détecte automatiquement une autre carte son, vous arriverez au menu 'Configurer une carte son'. Si YaST ne trouve pas de carte son, vous passerez directement à l'option 'Sélection manuelle de la carte son'.

Si vous utilisez une carte `Creative Soundblaster Live` ou `AWE`, vous pouvez, à l'aide de l'option 'Installer des fontes sonores', copier automatiquement sur votre disque dur des fontes sonores SF2 provenant du CD-ROM pilote Soundblaster original. Ces fontes seront enregistrées dans le répertoire `/usr/share/sfbank/creative/`.

Pour lire des fichiers Midi, vous devez avoir activé la case à cocher 'Démarrer le séquenceur'. Les modules pour le support du séquenceur seront alors chargés en même temps que les modules son.

En activant 'Terminer', vous enregistrez les paramètres pour le volume et la configuration de toutes les cartes installées jusqu'à présent. Les paramètres concernant le mixer sont insérés dans le fichier `/etc/asound.conf` et les données de configuration ALSA sont ajoutées à la fin du fichier `/etc/modprobe.conf` .

Configurer une carte son

Si plusieurs cartes son ont été trouvées, choisissez la carte que vous désirez dans 'Liste des cartes détectées automatiquement...'. Cliquez sur 'Suivant' pour accéder au menu 'Configuration'. Si la carte son n'est pas détectée automatiquement, sélectionnez l'option 'Sélectionner dans la liste' et cliquez sur 'Suivant' pour arriver au menu 'Sélection manuelle de la carte son'.

Sélection manuelle de la carte son

Si votre carte n'est pas détectée automatiquement, il sera affiché une liste de modèles de cartes son et de pilotes dans laquelle vous pourrez faire un choix. Si vous sélectionnez 'Toutes', vous pourrez voir la liste complète des cartes son supportées.

Consultez, si besoin, la documentation de votre carte son qui vous fournira les informations nécessaires. Vous pourrez également trouver une liste des cartes supportées par ALSA avec le module son correspondant à chaque carte sous `/usr/share/doc/packages/alsa/cards.txt` et `http://www.alsa-project.org/~goemon/`. Après avoir fait votre sélection, vous reviendrez au menu 'Configuration' en cliquant sur 'Suivant'.

2.4.11 Sélection de la disposition du clavier

La disposition de clavier à utiliser correspond généralement à la langue sélectionnée mais peut être changée indépendamment de celle-ci. Dans le champ de test, faites un essai afin de vérifier, par exemple si les caractères accentués ainsi que la lettre ç et le symbole de pipe | sont correctement affichés. Vérifez également les lettres z, w qui sont inversées sur un clavier américain.

2.4.12 Cartes TV et radio

Après le démarrage et l'initialisation de ce module de YaST, vous voyez tout d'abord apparaître le dialogue 'Configuration des cartes TV et radio'. Si votre carte a été reconnue automatiquement, elle apparaîtra dans la liste. Sélectionnez la ligne correspondante par un clic de souris et cliquez ensuite sur 'Configurer'.

Dans le cas où votre carte n'aurait pas été reconnue, sélectionnez autre carte non reconnue. Cliquez sur 'Configurer' pour accéder à la sélection manuelle et sélectionner votre carte dans la liste des modèles et fabricants.

Si vous avez déjà configuré des cartes TV ou radio, le bouton 'Modifier' vous donne la possibilité d'apporter des modifications à cette configuration. Vous voyez alors le dialogue 'Vue d'ensemble des cartes TV et radio' qui contient une liste de toutes les cartes déjà configurées. Sélectionnez une carte et démarrez la configuration manuelle avec 'Modifier'.

Lors de la détection automatique du matériel, YaST tente d'assigner le tuner correct à votre carte. Si vous avez un doute, choisissez 'Par défaut (détecté)' et vérifiez si cela fonctionne. Si vous n'avez pas pu sélectionner tous les émetteurs, cela peut être du, par exemple, au fait que la reconnaissance automatique du type de tuner a échoué. Dans ce cas, cliquez sur le bouton 'Sélectionner le tuner' et choisissez le type de tuner approprié dans la liste de sélection.

Si vous êtes familiarisé aux spécifications techniques, vous pouvez procéder à une configuration plus fine de votre carte TV ou radio dans le dialogue pour experts. Vous pouvez y sélectionner spécifiquement un module noyau et ses paramètres. Vous pouvez également contrôler tous les paramètres du pilote de la carte TV. Pour cela, sélectionnez les paramètres à modifier et entrez les nouvelles valeurs dans les lignes correspondantes. Confirmez les nouvelles valeurs en cliquant sur 'Appliquer' ou restaurez les valeurs par défaut avec 'Réinitialiser'.

Dans le dialogue ‘Cartes TV et radio, audio’, vous pouvez connecter la carte TV ou radio avec la carte son installée. Outre dans leur configuration, les cartes doivent également être connectées par un câble qui relie la sortie de la carte TV ou radio avec l’entrée audio externe de la carte son. Pour cela, la carte son doit déjà être configurée et l’entrée externe doit être activée. Si vous n’avez pas encore configuré votre carte son, faites-le dans le dialogue correspondant avec ‘Configurer la carte son’ (voir section *Son* page 84).

Si la carte TV ou radio dispose de fiches pour haut-parleurs, vous pouvez les connecter directement et il ne sera pas nécessaire de configurer la carte son. Il existe également des cartes TV sans fonction audio (par exemple pour caméras CCD) qui ne nécessitent donc pas de configuration du son non plus.

2.5 Périphériques réseau

Vous trouverez la description de la configuration YaST pour tous types de périphériques réseau supportés ainsi que des informations sur la connexion au réseau dans la section *L’intégration dans le réseau* page 468. La configuration de périphériques réseau pour la communication sans fil est décrite au chapitre *Communications sans fil* page 375.

2.6 Services réseau

Vous trouverez dans ce groupe des outils destinés avant tout aux grands réseaux (d’entreprise) pour y prendre en charge des services de résolution de noms, d’authentification des utilisateurs, de fichiers et d’impression.

2.6.1 Administration depuis un ordinateur distant

Si vous souhaitez maintenir votre système à travers une connexion VNC depuis un ordinateur distant, autorisez l’établissement de la connexion avec ce module YaST.

2.6.2 Serveur DHCP

À l'aide de YaST, vous pouvez, en quelques étapes, configurer votre propre serveur DHCP. Vous trouverez des informations à ce sujet ainsi qu'une description des différentes étapes de configuration avec YaST au chapitre *DHCP* page 546.

2.6.3 Nom d'hôte et DNS

Ce module sert à la configuration séparée de nom d'hôte et DNS lorsque celle-ci n'a pas été faite lors de la configuration du périphérique réseau.

Cette option est intéressante pour l'utilisateur privé qui peut, ici, modifier le nom de son ordinateur et de son domaine. Si vous avez configuré correctement l'accès DSL, modem ou RNIS de votre fournisseur, vous verrez ici, dans la liste du serveur de noms, des entrées qui ont été faites automatiquement étant donné qu'elles ont été obtenues à partir des données du fournisseur d'accès. Si vous vous trouvez dans un réseau local, vous obtiendrez probablement le nom d'hôte via DHCP. Dans ce cas, veillez à ne pas changer le nom.

2.6.4 Serveur DNS

Dans le réseaux de grande taille, il est conseillé de configurer un serveur DNS qui prendra en charge la résolution de noms pour ce réseau. Sa configuration à l'aide de yast; est décrite dans la section *Configuration avec YaST* page 500. Le chapitre *DNS – Domain Name System* page 487 contient des informations relatives au service DNS.

2.6.5 Serveur HTTP

Si vous souhaitez avoir votre propre serveur web, configurez Apache à l'aide de YaST. Vous trouverez plus d'informations à ce sujet au chapitre *Le serveur web Apache* page 563.

2.6.6 Client LDAP

Outre NIS, vous disposez également de LDAP pour procéder à l'authentification des utilisateurs dans le réseau. Vous trouverez des informations relatives à LDAP ainsi qu'une description détaillée de la configuration d'un client avec YaST dans la section *LDAP – un service d'annuaire* page 514.

2.6.7 Agent de transfert de message (MTA)

Le module de configuration vous permet de configurer vos options de courrier si vous utilisez les programmes sendmail ou postfix, ou si vous envoyez vos messages à travers le serveur SMTP de votre fournisseur. Vous pouvez télécharger les messages qui vous sont destinés à l'aide de SMTP ou avec le programme fetchmail, dans lequel vous devez spécifier les données des serveurs POP3 ou IMAP de votre fournisseur.

Vous pouvez également spécifier vos données d'accès POP et SMTP au programme de messagerie de votre choix, par exemple KMail

, comme à votre habitude (réception avec POP3, envoi avec SMTP). Dans ce cas, vous n'avez pas besoin de ce module.

Type de connexion

Si vous souhaitez procéder à la configuration de votre courrier électronique avec YaST, le système vous demandera dans la première fenêtre du dialogue, les données du type de connexion désirée pour accéder à Internet. Vous disposez des options suivantes :

'Permanente' Si vous souhaitez une connexion permanente avec Internet, sélectionnez cette option. Votre ordinateur sera en ligne sans interruption et aucune numérotation supplémentaire ne sera nécessaire. Si votre système se trouve dans un réseau local avec un serveur central de messagerie électronique pour l'envoi des messages, sélectionnez également cette option pour garantir un accès permanent à votre courrier.

'Composition' Cette option de menu est utile pour tous les utilisateurs qui ont à la maison un ordinateur connecté à aucun réseau et qui doivent se connecter de temps en temps pour accéder à Internet.

Sans connexion Si vous ne disposez d'aucune connexion à Internet et vous n'appartenez à aucun réseau, vous ne pourrez ni envoyer ni recevoir de courrier électronique.

En outre, vous pouvez lancer l'antivirus pour les messages entrants en activant la case à cocher de AMaViS. Le paquetage correspondant sera installé automatiquement dès que vous activerez le filtre de courrier. Dans le dialogue suivant, spécifiez le serveur de courrier sortant (le serveur SMTP de votre fournisseur) et les paramètres pour le courrier entrant. Si vous utilisez une connexion téléphonique (dial-up), vous pouvez indiquer divers serveurs POP ou IMAP pour

la réception du courrier par différents utilisateurs. Enfin, vous pouvez, de façon optionnelle, ajouter des alias supplémentaires, configurer le masquage ou définir des domaines virtuels dans ce dialogue. Quittez la configuration du courrier en cliquant sur 'Terminer'.

2.6.8 Client NFS et serveur NFS

NFS vous donne la possibilité, sous Linux, de gérer un serveur de fichiers auquel les membres de votre réseau peuvent accéder. Sur ce serveur de fichiers, vous pouvez, par exemple, mettre différents programmes et données ou même de la mémoire à disposition des utilisateurs. Dans le module 'Serveur NFS', vous définissez votre ordinateur en tant que serveur NFS et déterminez quels répertoires doivent être exportés, c'est à dire, quels répertoires peuvent être utilisés par les utilisateurs du réseau. Chaque utilisateur (à qui le droit a été accordé) peut alors monter ces répertoires dans sa propre arborescence. Vous trouverez la description de ce module YaST et des informations relatives à NFS à la section *NFS – Systèmes de fichiers partagés* page 541.

2.6.9 Client NIS et Serveur NIS

Dès que vous utilisez plus d'un système, l'administration des utilisateurs (à l'aide des fichiers `/etc/passwd` et `/etc/shadow`) devient pénible. Dans de tels cas, les données des utilisateurs devraient être administrés sur un serveur central et, à partir de celui-ci, être déployées sur les clients. Outre LDAP et Samba, vous disposez également de NIS. Vous trouverez des informations détaillées sur NIS et sa configuration avec YaST dans la section *NIS – Network Information Service* page 509.

2.6.10 Client NTP

NTP (*Network Time Protocol*) est un protocole utilisé pour la synchronisation de l'horloge d'un ordinateur via un réseau. Vous trouverez des informations relatives à NTP et la description de sa configuration avec YaST à la section *Synchronisation temporelle avec xntp* page 556.

2.6.11 Services réseau (inetd)

Avec cet outil, vous pouvez définir quels services système, par exemple, finger, talk, ftp, etc., doivent être démarrés lors de l'amorçage de SUSE LINUX. Ainsi, d'autres utilisateurs externes peuvent se connecter à votre ordinateur à travers ces services. En outre, vous pouvez définir des paramètres différents pour chaque service. Par défaut, le service de niveau supérieur qui gère les différents services réseaux (inetd ou xinetd) n'est pas démarré.

Au démarrage de ce module, sélectionnez lequel de ces deux services doit être configurés. Dans le dialogue suivant, vous pouvez décider, à l'aide d'un bouton radio, si inetd (ou xinetd) doit être démarré. Le démon (x)inetd peut être démarré avec une sélection standard de services réseau ou avec une sélection personnalisée de services réseau dans laquelle vous pouvez 'Ajouter' de nouveaux services ou 'Supprimer' ou 'Modifier' des services existants.

Attention

Configuration des services réseau (inetd)

La mise en place et l'organisation de services de réseau sur votre système est un processus complexe qui requiert des connaissances très précises du concept Linux des services réseau.

Attention

2.6.12 Routage

Ici aussi, vous n'avez besoin de cet outil que si vous vous trouvez dans un réseau local ou si vous vous connectez à Internet au moyen d'une carte réseau, par exemple avec une connexion DSL. Comme indiqué au chapitre *DSL* page 475, pour une connexion DSL, les valeurs entrées ne sont d'aucune importance pour l'établissement de la connexion et ne sont que des valeurs fictives nécessaires uniquement pour activer la carte réseau. La valeur attribuée à l'entrée passerelle n'est importante que dans le cas où vous vous trouvez dans un réseau local et utilisez un de vos ordinateurs en tant que passerelle vers Internet (gateway). Vous trouverez des informations détaillées relatives au routage dans la section *Le routage sous SUSE LINUX* page 483.

2.6.13 Configuration d'un serveur/client Samba

Si vous souhaitez utiliser un réseau hétérogène avec des machines Linux et des machines Windows, Samba gère la communication entre le deux mondes. Vous trouverez des informations détaillées relatives à Samba et à la configuration des client et serveur à la section *Samba* page 615.

2.7 Sécurité et utilisateurs

L'une des propriétés fondamentales de Linux est sa fonction multi-utilisateur qui permet à plusieurs personnes de travailler simultanément mais de manière indépendante sur un seul et même système Linux. Chacun possède son propre compte utilisateur constitué par un nom d'utilisateur ou nom de login et par un mot de passe personnel qui lui permettent de se connecter au système. Chacun a son répertoire personnel dans lequel il stocke ses fichiers privés et enregistre ses configurations.

2.7.1 Gestion des utilisateurs

Après avoir lancé cet outil de configuration, vous voyez s'ouvrir le masque Gestion des utilisateurs et des groupes. Vous avez maintenant le choix entre les utilisateurs et les groupes.

Pour faciliter la gestion, YaST met à votre disposition une liste de tous les utilisateurs locaux qui ont accès au système. Si vous vous trouvez dans un grand réseau, vous pouvez utiliser l'option 'Créer un filtre' pour générer une liste de tous les utilisateurs du système (par exemple, `root`) ou des utilisateurs NIS. Vous avez aussi la possibilité de créer des filtres personnalisés. Au lieu de passer d'un groupe d'utilisateurs à un autre, combinez-les à votre convenance. Pour ajouter des utilisateurs, cliquez sur 'Ajouter' et remplissez les champs nécessaires dans le masque suivant. Le nouvel utilisateur pourra ensuite se connecter à l'ordinateur avec son nom de login et son mot de passe. L'option 'Détails' vous permet de procéder à une configuration plus détaillée du profil de l'utilisateur. Il est possible de configurer manuellement le shell de connexion et le répertoire personnel. En outre, il est possible d'assigner l'utilisateur à des groupes déterminés. La période de validité du mot de passe se configure dans 'Configuration du mot de passe'. Tous les paramètres peuvent être modifiés en cliquant sur le bouton 'Modifier'. Pour éliminer un utilisateur, sélectionnez-le dans la liste et cliquez sur 'Supprimer'.

Pour l'administration avancée du réseau, vous avez la possibilité de spécifier les options par défaut pour la création de nouveaux utilisateurs dans 'Options pour experts'. Vous définissez le type d'authentification (NIS, LDAP, Kerberos ou Samba) ainsi que l'algorithme utilisé pour le chiffrement du mot de passe. Ces options de configuration sont surtout intéressantes pour les grands réseaux (d'entreprises).

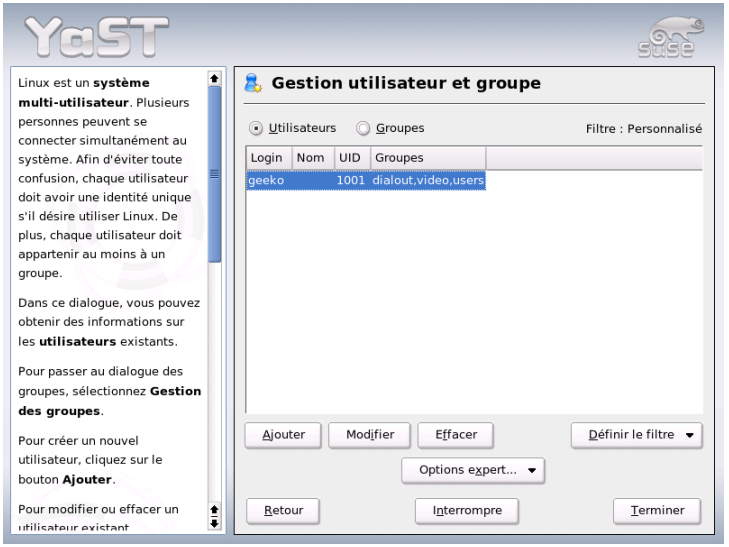


FIG. 2.14: *Gestion des utilisateurs*

2.7.2 Gestion des groupes

Démarrez le module de gestion des groupes du centre de contrôle de YaST ou cliquez sur la case à cocher 'Groupes' dans la gestion des utilisateurs. La fonctionnalité des deux masques est identique, la différence étant qu'il s'agit ici de la création de groupes au lieu d'utilisateurs.

Pour faciliter la gestion des groupes, YaST met à votre disposition une liste de tous les groupes. Pour éliminer un groupe, cliquez dans la liste sur la ligne correspondante afin que celle-ci apparaisse en bleu foncé puis cliquez sur 'Supprimer'. Pour 'Ajouter' et 'Modifier' un groupe, entrez, dans le masque correspondant de YaST, ses nom, ID de groupe (gid) et les utilisateurs de ce groupe. Vous pouvez également attribuer un mot de passe pour l'entrée dans ce groupe (optionnel). Les paramètres pour le filtre sont identiques au dialogue 'Gestion des utilisateurs'.

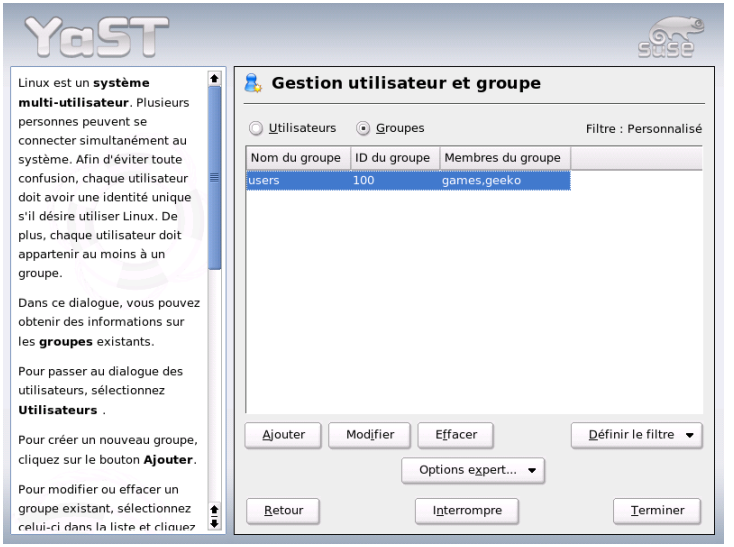


FIG. 2.15: *Gestion des groupes*

2.7.3 Paramètres de sécurité

Le dialogue de démarrage intitulé 'Configuration de la sécurité locale' que vous pouvez invoquer sous 'Sécurité et utilisateurs', vous donne le choix entre quatre options : le 'niveau 1' est pour les machines monopostes (préconfiguré), le 'niveau 2' est pour les stations de travail en réseau (préconfiguré), le 'niveau 3' est pour les serveurs en réseau (préconfiguré) et la configuration 'personnalisée' est pour vos propres paramètres.

Si vous avez sélectionné l'une des trois premières options, vous avez la possibilité d'utiliser, pour la sécurité du système, une configuration déjà prédéfinie. Cliquez simplement sur 'Terminer'. Sous 'Détails', vous avez accès aux différentes configurations que vous pouvez modifier selon vos désirs. Si vous sélectionnez la configuration 'personnalisée', vous accéderez automatiquement aux différents dialogues après avoir cliqué sur 'Suivant'. Vous trouverez ici les valeurs définies lors de l'installation.

'Configuration du mot de passe' Si vous souhaitez que le système vérifie les nouveaux mots de passe avant de les acepter, activez les deux cases à cocher 'Vérification des nouveaux mots de passe' et 'Vérifier la plausibilité des mots de passe'. Spécifiez la longueur minimale et maximale des mots de passe pour les nouveaux utilisateurs ainsi que la période de validité du mot de passe, sa date d'expiration et préciser combien de jours avant l'expiration l'utilisateur devra en être averti par un message (le message est affiché lors de la procédure de login sur la console texte).

'Paramètres d'amorçage' Spécifiez ici de quelle manière la combinaison de touches Ctrl Alt Delete doit être interprétée.

Sur la console texte, combinaison de touches déclenche habituellement un redémarrage du système. Il est en principe préférable de ne rien changer ici. À moins que votre machine ou votre serveur ne soit accessible à d'autres utilisateurs et que vous ayez lieu de craindre que quelqu'un puisse effectuer cette action sans autorisation. Si vous sélectionnez 'Stop', cette combinaison de touches déclenchera un arrêt du système et si vous choisissez 'Ignorer', elle ne provoquera plus rien.

Spécifiez également qui est autorisé à arrêter le système à partir de KDM (KDE Display Manager – le login graphique).

'Seulement root' (l'administrateur du système), 'Tous les utilisateurs', 'Personne' ou 'Utilisateurs locaux' ? Si vous sélectionnez 'Personne', le système ne pourra être arrêté qu'à partir de la console texte.

'Paramètres de login' Après une tentative de connexion qui s'est soldée par un échec, on doit normalement attendre quelques secondes avant de pouvoir recommencer. Cette règle a pour but de rendre la vie dure aux casseurs de mots de passe. Vous avez en outre la possibilité d'activer les options 'Enregistrer les tentatives de login échouées' et 'Enregistrer les tentatives de login réussies'. Si vous soupçonnez que quelqu'un cherche à deviner votre mot de passe, vous pouvez contrôler les entrées dans les fichiers de traces du système sous `/var/log`. Avec l'option 'Permettre le login graphique à distance', les autres utilisateurs pourront accéder à l'écran de login graphique

à travers le réseau. Cependant, cette possibilité d'accès représente un risque potentiel pour votre sécurité et est donc désactivée par défaut.

'Paramètres pour la création de nouveaux utilisateurs'
Chaque utilisateur possède un identificateur numérique et un identificateur alphanumérique. L'association entre ces deux identificateurs se fait dans le fichier `/etc/passwd` et ne devrait présenter aucune ambiguïté.

Les données affichées ici vous permettent de voir les zones de valeurs utilisées pour la partie numérique d'un identificateur lorsqu'un nouveau compte utilisateur est créé. Le minimum fixé à 500 pour un utilisateur est une valeur raisonnable et devrait être considéré comme la limite inférieure à ne pas dépasser. Procédez de la même façon pour la configuration des identificateurs de groupes.

'Paramètres divers' Vous avez trois possibilités de définir la 'Configuration des droits d'accès aux fichiers'. Vous avez le choix entre 'Easy', 'Secure' et 'Paranoid'. Pour la plupart des utilisateurs, la première option est suffisante. Le texte d'aide de YaST vous informe sur ces trois niveaux de sécurité.

L'option 'Paranoid' est extrêmement restrictive et devrait être utilisée par un administrateur système comme base pour une configuration personnalisée. Si vous choisissez 'Paranoid', vous devrez vous attendre à des perturbations ou dysfonctionnements lors de l'exécution de certains programmes car vous n'avez plus les droits nécessaires pour accéder à différents fichiers. Dans ce dialogue, vous pouvez en outre déterminer l'utilisateur qui devra lancer le programme updatedb. Ce programme qui est exécuté automatiquement tous les jours ou après chaque amorçage génère une base de données (locatedb) dans laquelle est enregistré l'emplacement de chaque fichier. Si vous sélectionnez 'Personne', il ne sera possible de trouver dans la base de données que les chemins d'accès que n'importe quel utilisateur (sans privilège) pourrait voir. Si vous sélectionnez `root`, tous les fichiers locaux seront indexés puisque l'utilisateur `root`, en tant que Super-User, est autorisé à lister tous les répertoires.

Enfin, vous pouvez désactivez l'option 'Répertoire courant dans le chemin de l'utilisateur root'.

En cliquant sur 'Terminer', vous achèverez la configuration des paramètres de sécurité de votre système.

FIG. 2.16: *YaST : Configuration des paramètres de sécurité*

2.7.4 Pare-feu

Ce module vous permet de mettre en place et de configurer de façon très simple le pare-feu SuSEfirewall2 pour protéger votre système des intrus venant d'Internet. Vous trouverez des informations détaillées relatives à SuSEfirewall2 dans la section *Mascarade et pare-feu* page 656.

Remarque

Démarrage automatique du pare-feu

Sur chaque interface réseau configurée, YaST démarre automatiquement un pare-feu avec les paramètres appropriés. Vous n'avez donc besoin de ce module que si vous souhaitez procéder à une configuration plus avancée du pare-feu ou si vous souhaitez le désactiver complètement.

Remarque

2.8 Système

2.8.1 Copie de sauvegarde des zones du système

Avec le nouveau module de sauvegarde, vous avez la possibilité d'effectuer une sauvegarde de votre système avec YaST. Ce module n'effectue pas de sauvegarde complète mais enregistre uniquement des informations sur les paquetages modifiés, les zones système critiques et les fichiers de configuration.

Lors de la configuration, vous pouvez décider quels fichiers devront être sauvegardés. Par défaut, les informations concernant les paquetages qui ont été modifiés depuis la dernière installation seront enregistrées. Vous pouvez, en outre, stocker dans votre répertoire `/etc` ou dans votre répertoire `home`, des fichiers qui n'appartiennent à aucun paquetage, par exemple de nombreux fichiers de configuration. Vous pouvez également ajouter les zones système critiques du disque dur telles que les tables des partitions ou le secteur d'amorçage (MBR) qui pourront être utilisées dans le cas d'une éventuelle restauration.

2.8.2 Restauration du système

Avec le module de restauration (figure 2.17 page suivante), vous pouvez restaurer votre système à partir d'une copie de sécurité. Suivez les instructions dans YaST. En cliquant sur 'Suivant', vous ouvrez les différents dialogues. Entrez tout d'abord à quel endroit se trouve(nt) la/les copie(s), c'est à dire soit sur un support amovible, soit sur un disque local ou encore sur un système de fichiers du réseau. Vous obtenez ensuite les descriptions et contenus correspondants à la copie et vous pourrez sélectionner ce que vous voulez récupérer.

En outre, il existe deux dialogues supplémentaires dans lesquels vous pouvez choisir les paquetages qui ont été ajoutés depuis la dernière copie de sauvegarde et qui doivent être désinstallés. De plus, les paquetages supprimés depuis la dernière copie de sauvegarde et qui doivent être réinstallés. À l'aide de ces deux étapes supplémentaires, vous pouvez restaurer votre système exactement dans le même état que lors de la dernière sauvegarde.

Attention

Restaurer le système

Étant donné que ce module permet normalement d'installer, de remplacer ou de désinstaller de nombreux paquetages et fichiers, nous vous conseillons de ne l'utiliser que si vous avez l'habitude de manipuler les copies de sauvegarde. Dans le cas contraire, vous pourriez perdre des données.

Attention

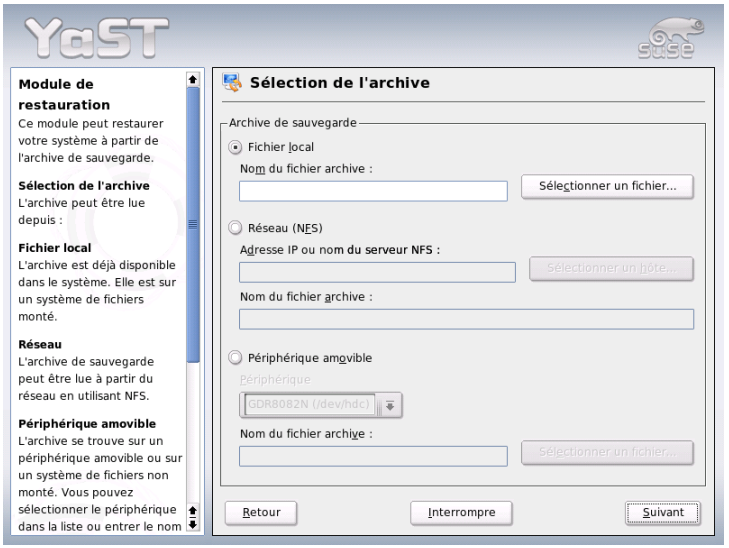


FIG. 2.17: *YaST : Fenêtre de démarrage du module de restauration*

2.8.3 Création d'une disquette d'amorçage, de secours ou de modules

Avec ce module de YaST, vous pouvez créer, d'une manière très simple et aisée, des disquettes d'amorçage, de secours et de modules. Ces disquettes vous seront utiles au cas où la configuration de démarrage de votre système se détériorerait.

La disquette de secours est tout spécialement nécessaire si le système de fichiers de la partition root est abimé. Dans ce cas, vous pouvez également avoir besoin de la disquette de modules contenant divers pilotes pour pouvoir accéder au système (par exemple, pour accéder à un système RAID).

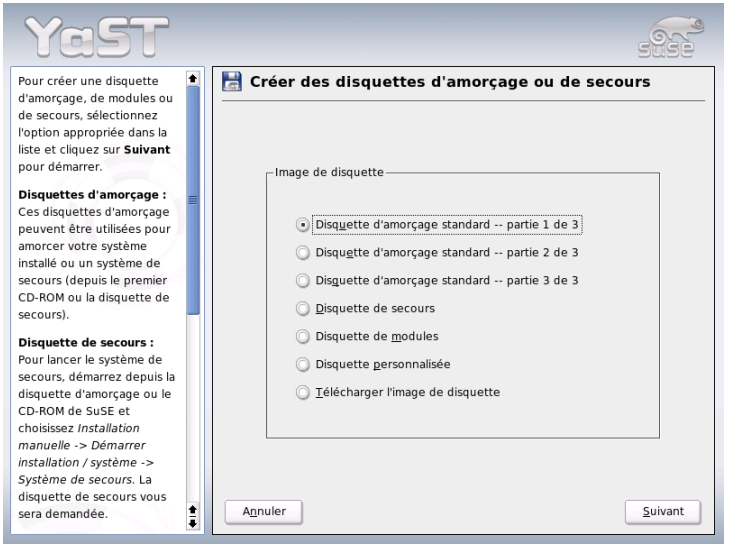


FIG. 2.18: *Création d'une disquette d'amorçage, de secours ou de modules*

'Disquettes d'amorçage standards' Avec cette option, vous pouvez créer une disquette de démarrage standard pour amorcer un système déjà installé. Cette disquette est également nécessaire à l'amorçage du système de sauvegarde.

'Disquettes de secours' Cette disquette contient un environnement spécial qui vous permet d'effectuer des travaux de réparation ou de maintenance dans un système déjà installé, par exemple, vérifier les systèmes de fichiers et actualiser le gestionnaire de démarrage.

Pour démarrer le système de secours, amorcez tout d'abord avec la disquette d'amorçage standard puis sélectionnez 'Installation manuelle', 'Démarrer installation/système' et 'Système de secours'. L'insertion de la disquette de secours vous sera alors demandée. Si vous avez configuré votre système pour l'utilisation de pilotes spéciaux (par exemple, RAID ou USB), chargez les modules correspondants depuis la disquette de modules.

'Disquettes de modules' Les disquettes de modules contiennent des pilotes système supplémentaires. Le noyau standard ne supporte que les unités IDE. Si les unités de votre système sont connectées à des contrôleurs spéciaux (par exemple, SCSI), vous devrez charger les pilotes correspondants depuis une disquette de modules. Si vous sélectionnez cette option et cliquez sur 'Suivant', vous ouvrez un dialogue pour créer différentes disquettes de modules.

Vous disposez des disquettes de modules suivantes

Modules USB Cette disquette contient des modules USB, dont vous aurez besoin, par exemple, si vous connectez des lecteurs USB.

Modules IDE, RAID et SCSI Le noyau standard ne supporte que des lecteurs IDE normaux, vous aurez donc besoin de cette disquette de modules si vous utilisez des contrôleurs IDE spéciaux. En outre, vous y trouverez aussi tous les modules RAID et SCSI.

Modules réseau Si vous nécessitez l'accès à un réseau, vous devrez charger le module pilote correspondant à votre carte réseau.

PCMCIA, CDROM (non ATAPI), FireWire et systèmes de fichiers Cette disquette contient tous les modules PCMCIA que l'on utilise surtout pour les ordinateurs portables. En outre, elle contient aussi les modules pour FireWire et quelques systèmes de fichiers moins courants. Les lecteurs CD-ROM anciens qui ne répondent pas encore aux normes ATAPI, peuvent également être utilisés avec des pilotes qui se trouvent sur cette disquette.

Pour charger des pilotes depuis une disquette de modules dans le système de secours, sélectionnez 'Modules noyau (pilotes matériel)' et le type de modules souhaité (SCSI, Ethernet, etc.). Vous devrez ensuite insérer la disquette de modules correspondantes et les modules qu'elle contient seront affichés. Sélectionnez le module désiré. Tenez compte des messages du système : 'Loading module <nom_du_module> failed!' vous indique que le module n'a pas reconnu le matériel. Certains pilotes anciens nécessitent des paramètres déterminés pour pouvoir contrôler le matériel de façon correcte. Dans ce cas, veuillez consulter la documentation de votre matériel.

'Disquette personnalisée' Cette option vous permet de copier une image disquette quelconque du disque dur vers la disquette. Ce fichier image doit déjà exister sur le disque dur.

'Télécharger une image disquette' Cette option vous permet de télécharger une image disquette depuis Internet après avoir saisi l'URL et les données d'authentification correspondants.

Pour créer les disquettes citées ci-dessus, sélectionnez l'option appropriée et cliquez sur 'Suivant'. Insérez une disquette comme cela vous est demandé. Cliquez encore une fois sur 'Suivant', le contenu correspondant à l'option sera alors écrit sur la disquette.

2.8.4 LVM

Le gestionnaire de volumes logiques (*Logical Volume Manager*, LVM) est un outil permettant le partionnement individuel du disque dur au moyen de disques logiques. Vous trouverez plus d'informations à ce sujet à la section *Configuration du gestionnaire de volumes logiques (LVM)* page 142.

2.8.5 Partitionner

Il est possible de modifier le partitionnement dans un système installé, cependant cela devrait être réservé aux experts. Dans le cas contraire, il existe une grande probabilité de perdre les données qui se trouvent dans le système. Si vous souhaitez utiliser tout de même cet outil, vous en trouverez une description dans la section relative à l'installation dans le chapitre *Partitionnement* page 16 de ce manuel (le même partitionneur est utilisé durant l'installation que dans le système installé).

2.8.6 Gestionnaire de profils (SCPM)

Le module pour le gestionnaire de profils (SCPM, *System Configuration Profile Management*) vous offre la possibilité de créer des configurations du système individuelles complètes, de les gérer et de passer de l'une à l'autre à volonté. Normalement, une telle propriété peut être très utile, surtout dans le cas des ordinateurs portables qui sont utilisés dans des endroits différents (dans des réseaux différents) par des personnes différentes. Cependant, cela peut également être

utile dans le cas d'ordinateurs stationnaires afin de pouvoir utiliser différents matériels ou différentes configurations de test. Si vous souhaitez obtenir des informations complémentaires au sujet du gestionnaire de profils SCPM et de son utilisation, veuillez vous reporter à la section correspondante dans le chapitre *SCPM — System Configuration Profile Management* page 339.

2.8.7 Éditeur de niveau d'exécution

Vous pouvez utiliser SUSE LINUX dans différents niveaux d'exécution (*runlevel*). Par défaut, le système est démarré dans le niveau d'exécution 5. Ceci signifie que la fonctionnalité multi-utilisateurs, l'accès au réseau et l'interface graphique (système X Window) sont activés. Les autres niveaux d'exécution vous proposent la fonctionnalité multi-utilisateurs avec accès au réseau sans X (niveau d'exécution 3), fonctionnalité multi-utilisateurs sans accès au réseau (niveau d'exécution 2), système mono-utilisateur (niveau d'exécution 1 et S), arrêt du système (niveau d'exécution 0) et réamorçage du système (niveau d'exécution 6).

Les différents niveaux d'exécution sont surtout utiles lorsque, dans un niveau d'exécution supérieur, un problème arrive dans le service correspondant (X ou réseau). Le système peut alors être démarré dans un niveau d'exécution inférieur afin de réparer le service en cause. En outre, beaucoup de serveurs fonctionnent sans interface graphique et ces ordinateurs doivent donc être amorcés dans le niveau d'exécution 3, par exemple.

Normalement, vous n'aurez besoin que du niveau d'exécution par défaut (5). Cependant, si l'interface graphique venait à se planter, vous pouvez redémarrer votre système X Window en passant dans une console texte à l'aide de la combinaison de touches Ctrl + Alt + F1, vous y connecter en tant qu'administrateur root puis passer dans le niveau d'exécution 3 à l'aide de la commande `init 3`. De cette façon, votre système X Window sera arrêté. Vous pouvez le redémarrer en saisissant simplement `init 5`.

Vous trouverez plus d'informations au sujet des niveaux d'exécution sous SUSE LINUX et une description de l'éditeur de niveaux d'exécution de YaST dans le chapitre *Processus d'amorçage* page 253.

2.8.8 Éditeur sysconfig

Dans le répertoire `/etc/sysconfig` se trouvent les fichiers qui contiennent les paramètres les plus importants pour SUSE LINUX. L'éditeur sysconfig présente toutes les possibilités de configuration de façon claire. Les valeurs peuvent être modifiées et enregistrées dans les différents fichiers de configuration. Cependant, la modification manuelle de ces valeurs n'est généralement pas nécessaire, étant donné que lors de l'installation d'un paquetage ou lors de la configuration d'un service, etc. les fichiers sont actualisés automatiquement. Vous trouverez plus d'informations relatives à `/etc/sysconfig` sous SUSE LINUX et à l'éditeur sysconfig de YaST dans le chapitre *Processus d'amorçage* page 253.

2.8.9 Sélection de la zone horaire

La zone horaire est déjà déterminée au cours de l'installation – ici, vous avez la possibilité de procéder encore à une modification. Dans la liste des pays, cliquez simplement sur le nom du vôtre et sélectionnez 'Heure locale' ou 'UTC' (*Universal Time Coordinated*). Dans un système Linux, on utilise habituellement 'UTC'. Les machines sur lesquelles sont installés d'autres systèmes d'exploitation, par exemple Microsoft Windows™, utilisent généralement l'heure locale.

2.8.10 Sélection de la langue

Il est possible de changer ultérieurement la langue. La configuration de la langue effectuée avec YaST s'étend à tout le système. Elle est donc valable pour YaST et le bureau.

2.9 Divers

2.9.1 Adresser une requête d'Assistance Technique à l'Installation

L'achat d'une distribution SUSE LINUX vous donne droit à l'assistance gratuite à l'installation. Vous trouverez des informations plus détaillées, (par exemple étendue du service, adresse, numéro de téléphone etc.) sur notre page web `www.suse.de`

YaST vous donne la possibilité d'adresser directement une requête par courrier électronique au service d'Assistance Technique à l'Installation de SUSE. Vous pourrez bénéficier de ce service après enregistrement. Fournissez au début de votre requête les informations nécessaires – Vous trouverez votre code d'enregistrement au dos de la pochette des CD. Sélectionnez dans la fenêtre suivante la catégorie de votre problème et décrivez-le (figure 2.19). Pour la rédaction de votre requête, lisez le texte d'aide de YaST qui vous informe de la meilleure manière de décrire votre problème afin que l'équipe d'assistance puisse vous venir en aide au plus vite.

Remarque

Si vous avez besoin d'une assistance plus avancée (par exemple pour des problèmes particuliers), vous pouvez vous adresser aux Services Professionnels de SUSE. Vous trouverez des informations plus détaillées sous `http://www.suse.de/de/support/`.

Remarque

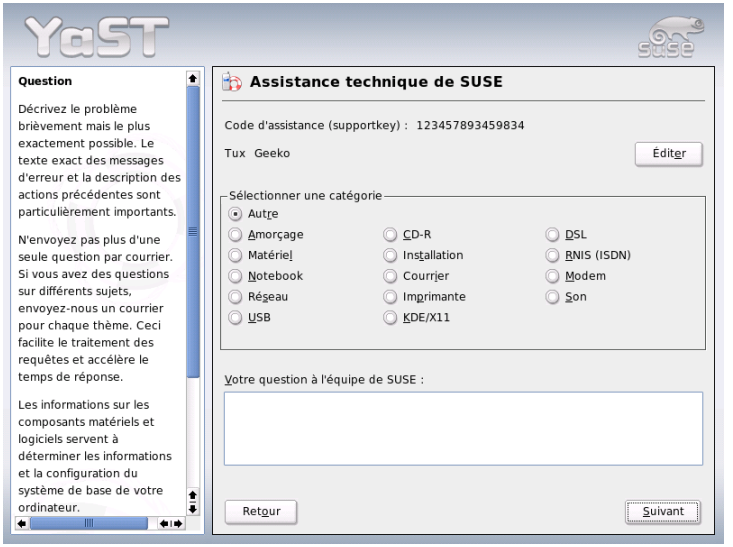


FIG. 2.19: *Adresser une requête d'Assistance Technique à l'Installation*

2.9.2 Fichier de démarrage

Le fichier de démarrage est le fichier qui contient les messages qui apparaissent à l'écran lors du démarrage de la machine. Il s'agit du fichier `/var/log/boot.msg`. Avec ce module de YaST, vous pouvez l'afficher et vérifier, par exemple, si tous les services et fonctions ont été démarrés comme vous l'aviez prévu.

2.9.3 Fichier de traces du système

Le fichier de traces du système enregistre ce qui se passe sur votre machine et se trouve sous `/var/log/messsages`. Vous voyez apparaître ici les messages du noyau classés par date et heure.

2.9.4 Charger le CD de pilotes du fabricant

Avec ce module, vous pouvez installer automatiquement des pilotes de périphériques à partir d'un CD contenant des pilotes pour SUSE LINUX.

Si une nouvelle installation de votre système SUSE LINUX devait s'avérer nécessaire, ce module de YaST vous donne la possibilité, après installation, de charger les pilotes indispensables à partir du CD du fabricant.

2.10 YaST en mode texte (ncurses)

Cette section s'adresse principalement aux administrateurs système et aux experts dont les machines n'exécutent pas de serveur X et qui doivent utiliser l'utilitaire d'installation en mode texte. Vous trouverez dans cette section des informations de base sur l'exécution et l'utilisation de YaST en mode texte (ncurses).

Lorsque vous lancez YaST en mode texte, le centre de contrôle YaST apparaît d'abord (voir l'illustration 2.20 page suivante). On distingue ici trois rubriques : sur le volet gauche, dans un cadre blanc épais, on peut voir les catégories auxquelles sont rattachés les différents modules. La catégorie courante est mise en surbrillance. Le volet droit, pourvu d'un cadre fin, présente les différents modules appartenant à la catégorie active. Le volet inférieur, enfin, comporte les boutons 'Aide' et 'Quitter'.

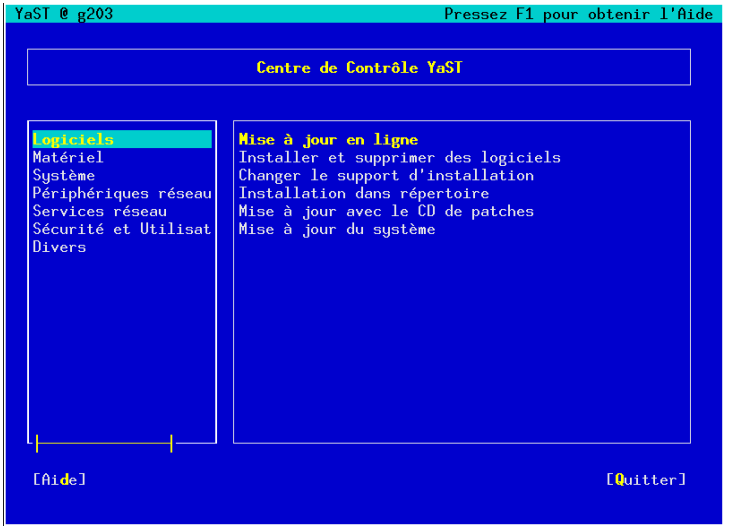


FIG. 2.20: *Écran principal de YaST ncurses*

Après le premier démarrage du centre de contrôle de YaST, la catégorie 'Logiciels' est sélectionnée automatiquement. Pour changer de catégorie, appuyez sur les touches (↓) et (↑). Pour lancer un module depuis la catégorie sélectionnée, utilisez la touche (→). Le module sélectionné apparaît alors avec dans un cadre épais. Sélectionnez le module de votre choix à l'aide des touches (↓) et (↑). Tout en maintenant la touche de direction enfoncée, faites "défiler" les différents modules disponibles . Dès que vous avez sélectionné un module, le titre correspondant apparaît en surbrillance. Parallèlement, une description succincte du module s'affiche sur le volet inférieur.

Appuyez sur la touche (Enter) pour lancer le module choisi. Le module comporte différents boutons ou zones de sélection avec une lettre de couleur différente (jaune, dans la configuration par défaut). La combinaison de touches (Alt)–(lettre jaune) vous permet de sélectionner directement le bouton en question en vous épargnant d'utiliser laborieusement la touche de navigation (Tab).

Pour quitter le centre de contrôle de YaST, vous pouvez soit utiliser le bouton 'Quitter', soit sélectionner le sous-menu 'Quitter' de la liste des catégories, puis appuyer sur la touche (Entrée).

2.10.1 Navigation dans les modules de YaST

Dans la description suivante de l'interface des modules de YaST, nous faisons l'hypothèse que les touches de fonctions et les combinaisons utilisant la touche (Alt) fonctionnent correctement, et n'ont pas été modifiées pour l'ensemble du système. Pour plus d'informations sur les exceptions possibles, reportez vous au chapitre *Restrictions sur les combinaisons de touches* page suivante.

Navigation entre les boutons/listes de sélection
Les touches (Tab) et (Alt)–(Tab) ou (Maj)–(Tab) vous permettent de naviguer librement parmi les boutons et/ou les cadres des listes de sélection.

Navigation dans les listes de sélection
Dans un cadre activé dans lequel se trouve une liste de sélection, c'est à l'aide des flèches ((↑) et (↓)) que vous pouvez naviguer entre les différents éléments, par exemple, entre les différents modules d'un groupe de modules du centre de contrôle. Si certaines lignes ont une longueur supérieure à celle du cadre et que leur texte dépasse de ce cadre, vous pouvez "scroller" c'est-à-dire faire défiler le contenu du cadre horizontalement vers la droite au moyen de (Maj)–(→) ou vers la gauche avec (Maj)–(←) (une solution alternative consiste à utiliser (Ctrl)–(e) ou (Ctrl)–(a)). Cette combinaison fonctionne également là où (→) et (←) provoquent, comme dans le centre de contrôle, un saut du cadre actif vers le cadre suivant ou de la liste de sélection active vers la liste suivante.

Boutons, boutons radio et cases à cocher
Pour actionner les cases à cocher (*Check box*) et les boutons radio (*Radio-button*), appuyez sur la touche (Espace) ou (Entrée). Il est également possible d'activer les boutons radio et cases à cocher comme des boutons normaux au moyen de (Alt)–(lettre jaune). Pour la navigation par tabulation, il est nécessaire d'appuyer encore une fois sur la touche (Entrée) pour exécuter l'action sélectionnée ou activer le menu correspondant (voir l'illustration 2.21 page suivante).

Les touches de fonction Les touches de fonction ((F1) à (F12)) son également liées à des fonctions. Elles permettent d'actionner rapidement les différents boutons disponibles. L'affectation d'une touche de fonction donnée à une fonction dépend du module de YaST dans lequel vous vous trouvez. En effet, les différents modules comportent chacun leurs propres boutons (tels que Détails, Ajouter, Supprimer, etc.). Les utilisateurs habitués à l'ancien YaST1 retrouveront par exemple les boutons 'OK', 'Suivant' et 'Terminer' sur la touche de fonction (F10). L'aide de YaST, à laquelle vous accédez en appuyant sur la touche (F1), vous fournira la table de correspondance entre les fonctions et les touches de fonction associées.

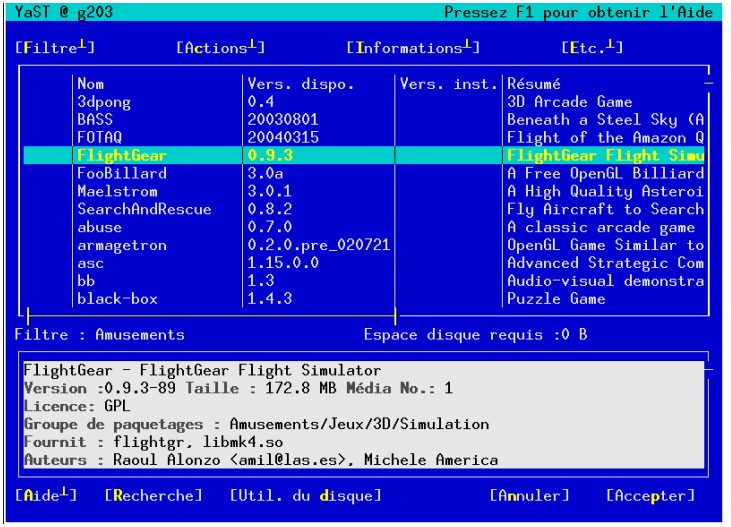


FIG. 2.21: *Le module d'installation de logiciels*

2.10.2 Restrictions sur les combinaisons de touches

Dans le cas où vous avez défini pour l'ensemble de votre système des combinaisons de touches utilisant Alt depuis le serveur X actif, il est possible que les combinaisons de touches utilisant Alt ne fonctionnement pas sous YaST. De même, les touches Alt ou Maj peuvent également avoir été affectées par les paramètres du terminal utilisé.

Substitution de la touche Esc à la touche Alt :
Les raccourcis utilisant la touche Alt peuvent être pris avec Esc au lieu de Alt. Ainsi, Esc–h remplace par exemple la combinaison de touches Alt–h.

Avance et retour au moyen des combinaisons Ctrl–f et Ctrl–b :
Dans le cas où les combinaisons de touches Alt et Maj sont réservées par le gestionnaire de fenêtres ou par le terminal, vous pouvez utiliser à la place les combinaisons Ctrl–f (Suivant) et Ctrl–b (Précédent).

Restriction des touches de fonction : Les touches de fonction sont également réservées. Il est possible que certaines touches de fonctions soient réservées à cause du choix du terminal et qu'elles ne soient donc pas disponibles pour YaST. Toutefois, la console texte devrait continuer à avoir pleinement accès aux combinaisons de touches (Alt) et aux touches de fonction.

2.10.3 Appel des différents modules

Vous pouvez également gagner du temps en appelant séparément chacun des modules de YaST. Les modules sont exécutés simplement à l'aide de la commande : `yast nommodule`

Ainsi, le module réseau est par exemple lancé à l'aide de la commande `yast lan`. Vous pouvez obtenir la liste de tous les noms de modules disponibles sur votre système en exécutant la commande `yast -l` ou `yast --list`.

2.10.4 YaST Online Update

Le module YOU

Le module de mise à jour en ligne de YaST ("YaST Online Update" ou YOU) peut être appelé comme tout autre module de YaST, en tant qu'utilisateur `root`, au moyen de la ligne de commande :

```
yast online_update .url <url>
```

`yast online_update` appelle le module correspondant. Au moyen de l'option `url`, vous indiquez à YOU un serveur (local ou sur Internet) à partir duquel récupérer tous les correctifs et les informations. Si cette information n'est pas fournie au premier appel à YOU, vous pouvez renseigner le serveur/le répertoire dans le formulaire de YaST. Avec le bouton 'Configurer mise à jour automatisée', vous pouvez configurer une tâche Cron pour procéder à automatisation de la mise à jour.

Online Update (Mise à jour en ligne) en ligne de commande

Vous pouvez mettre à jour votre système de façon totalement automatisée, par exemple au moyen de scripts, avec l'outil en ligne de commande online_update.

Dans les cas concrets, vous souhaitez que votre système recherche des correctifs sur un serveur donné, de façon régulière et à des moments précis, télécharge les correctifs et les informations correspondantes, mais n'effectue pas l'installation. Vous voulez vérifier ultérieurement le nombre de correctifs et sélectionner ceux que vous souhaitez installer :

- Mettez en place une tâche Cron qui exécute la commande suivante :

  ```
  online_update -u <URL> -g <typemaj>
  ```

  `-u` permet de transmettre l'URL de l'arborescence de répertoires à partir de laquelle les correctifs doivent être téléchargés. Les protocoles `http`, `ftp`, `smb`, `nfs`, `cd`, `dvd` et `dir` sont pris en charge. L'option `-g` vous permet de télécharger les correctifs dans un répertoire local sans les installer. Vous disposez aussi d'une option permettant de contrôler le nombre de correctifs en fonction de trois types de mises à jour : `security` (mises à jour de sécurité), `recommended` (mises à jour conseillées) et `optional` (mises à jour optionnelles). Si vous ne précisez pas de type de mise à jour, online_update télécharge tous les correctifs disponibles pour les types `security` et `recommended`.
- Vous avez ensuite la possibilité d'installer immédiatement les paquetages téléchargés, sans explorer en détail et individuellement les correctifs. Les correctifs sont stockés par online_update en suivant le chemin `/var/lib/YaST2/you/mnt`. Pour terminer l'installation des correctifs, utilisez la commande suivante :

  ```
  online_update -u /var/lib/YaST2/you/mnt/ -i
  ```

  Le paramètre `-u` transmets l'URL (locale) correspondant aux correctifs à installer. `-i` permet de démarrer la procédure d'installation.
- Si vous souhaitez voir les correctifs téléchargés avant d'effectuer leur installation, et éventuellement en supprimer certains, appelez le formulaire YOU au moyen de :

  ```
  yast online_update .url /var/lib/YaST2/you/mnt/
  ```

  YOU démarre et choisit comme source des correctifs le répertoire local, qui contient les correctifs précédemment téléchargés, plutôt qu'un répertoire distant sur Internet. Vous choisissez ensuite les correctifs que vous souhaitez appliquer, comme pour toute installation habituelle, au moyen du gestionnaire de paquetages.

À partir de la ligne de commande, il est possible de définir le comportement de la mise à jour en ligne YaST à l'aide de paramètres. Dans ce cas, les actions souhaitées sont spécifiées avec des paramètres à la ligne de commande comme suit : `online_update [paramètre ligne de commande]`. Les paramètres possibles et leur signification sont répertoriés dans la liste ci-après.

`-u URL` URL de base de l'arborescence de répertoires depuis laquelle les patches doivent être téléchargés.

`-g` Seulement télécharger les patches, ne pas les installer.

`-i` Installer les patches déjà chargés mais ne rien télécharger.

`-k` Vérifier si de nouveaux patches sont disponibles.

`-c` Afficher la configuration actuelle, sinon ne rien faire.

`-p produit` Produit pour lequel des patches doivent être récupérés.

`-v version` Version du produit pour laquelle des patches doivent être récupérés.

`-a architecture` Architecture de base du produit pour laquelle des patches doivent être récupérés.

`-d` "Essai à vide" (dry run). Télécharger les patches et simuler l'installation (le système demeure intact pour des raisons de test).

`-n` Pas de vérification de la signature des fichiers téléchargés.

`-s` Afficher la liste des patches disponibles.

`-V` Mode prolixe (verbose). Affiche les messages du processus.

`-D` Mode débogage pour les experts et dans le but de la recherche d'erreur.

Plus d'informations sur online_update sont disponibles en tapant la commande `online_update -h`.

Variantes d'installation spéciales

L'installation de SUSE LINUX est très souple. Les variantes vont d'une installation rapide en mode graphique à une installation en mode texte qui permet de nombreux ajustements manuels.

Vous trouverez ci-après les méthodes d'installation spéciales et des indications concernant l'utilisation de différentes sources d'installation (CD-ROM, NFS). Ce chapitre contient également des astuces pour résoudre des problèmes susceptibles de se produire lors de l'installation et, en guise de conclusion, une section sur le partitionnement avancé.

3.1 linuxrc

À chaque ordinateur, correspondent des routines spéciale, souvent appelées BIOS, qui sont exécutées lors du démarrage du sytèmes et initialisent ainsi le matériel de façon à ce qu'un amorçage soit possible. Lors de la procédure d'amorçage en soi, une image qui sera exécutée par l'ordinateur est chargée par ces routines. Cette image peut être in gestionnaire d'amorçage, mais il est théoriquement possible de charger aussi un noyau directement. Lors de l'installation de SUSE LINUX, une image d'amorçage est chargée ; celle-ci contient un noyau et un programme du nom de "linuxrc".

linuxrc est un programme qui s'exécute durant le démarrage du noyau avant l'amorçage à proprement parler. Cette particularité du noyau permet d'amorcer un petit noyau modulaire et de charger ultérieurement sous forme de modules les quelques pilotes dont on a vraiment besoin. Avec SUSE LINUX, linuxrc démarre YaST après l'analyse du système. La reconnaissance automatique du matériel, effectuée avant le démarrage par YaST, est généralement suffisamment fiable. Cependant, si vous voulez charger des pilotes à la main ou entrer de paramètres spéciaux, vous pouvez également utiliser linuxrc de façon interactive. Dans ce cas, démarrez une "installation manuelle".

Vous pouvez utiliser linuxrc non seulement lors de l'installation mais également comme un outil d'amorçage dans un système installé. Il est même possible de lancer un système de secours autonome s'exécutant en mémoire vive. Pour plus de précisions, reportez-vous à la section *Le système de secours SUSE* page 192.

3.1.1 Notions de base : linuxrc

Le programme linuxrc vous permet de faire des réglages concernant l'installation et de charger les pilotes nécessaires sous forme de modules du noyau. linuxrc démarre enfin YaST et l'installation proprement dite des logiciels système et des programme peut commencer.

Déplacez-vous dans le menu avec ↑ et ↓ et choisissez une action, comme 'OK' ou 'Annuler' avec ← et →. La touche Retour chariot validera votre choix.

Paramètres

Le programme linuxrc commence automatiquement avec le choix de la langue et du clavier.

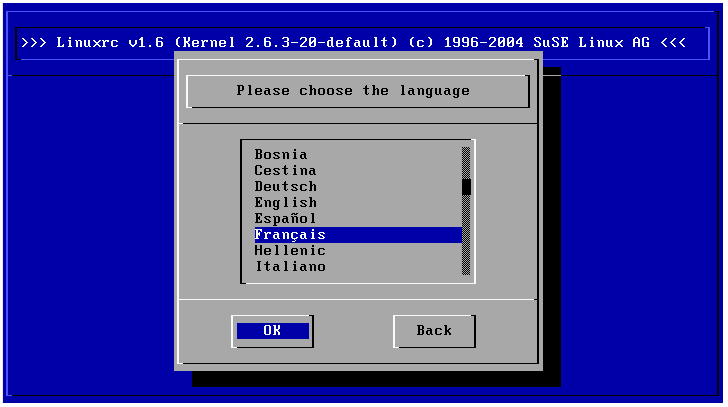


FIG. *3.1:* *Choix de la langue*

- Choisissez la langue d'installation (par exemple 'Français') et confirmez avec (Retour chariot).
- Choisissez ensuite la disposition du clavier (par exemple 'Français').

3.1.2 Menu principal

Après avoir configuré la langue et le clavier, vous accédez au menu principal de linuxrc (voir l'illustration 3.2 page suivante). linuxrc est normalement utilisé pour démarrer Linux, on s'intéresse donc au menu 'Installation / Démarrer le système'. Vous pourrez y accéder directement ou indirectement en fonction de la configuration matérielle de la machine ainsi que de vos projets d'installation. Pour plus d'informations, reportez-vous à la section *Installation en mode texte avec YaST* page 127.

3.1.3 Informations sur le système

L'écran 'Informations sur le système' (illustration 3.3 page 119) vous permet de vérifier les messages du noyau ainsi que différents autres points tels que les adresses d'entrée/sortie des cartes PCI ou la taille mémoire détectée par Linux.

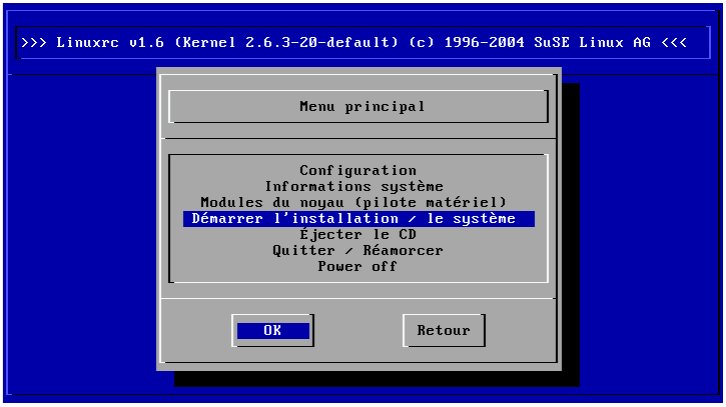


FIG. 3.2: *Menu principal de linuxrc*

Les lignes ci-après montrent comment déclarer un disque dur et un lecteur de cédérom sur un adaptateur EIDE. Dans ce cas, vous n'avez pas à charger de module noyau pour l'installation :

```
hda: IC35L060AVER07-0, ATA DISK drive
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
hdc: DV-516E, ATAPI CD/DVD-ROM drive
ide1 at 0x170-0x177,0x376 on irq 15
hda: max request size: 128KiB
hda: 120103200 sectors (61492 MB) w/1916KiB Cache, CHS=65535/16/63, UDMA(100)
 hda: hda1 hda2 hda3
```

Dans le cas où vous avez lancé un noyau comportant déjà un pilote SCSI statique, il n'est bien entendu plus nécessaire de charger de module SCSI. Si vous souhaitez intégrer un adaptateur SCSI à votre système, vous devrez charger le module SCSI correspondan ; à ce sujet, consultez la section *Chargement de modules* page suivante. Dans les noyaux livrés avec SUSE, ces modules sont déjà pré-compilés lorsque cela est possible. Voici des messages types affichés lors de la reconnaissance d'un adaptateur SCSI et des périphériques attachés :

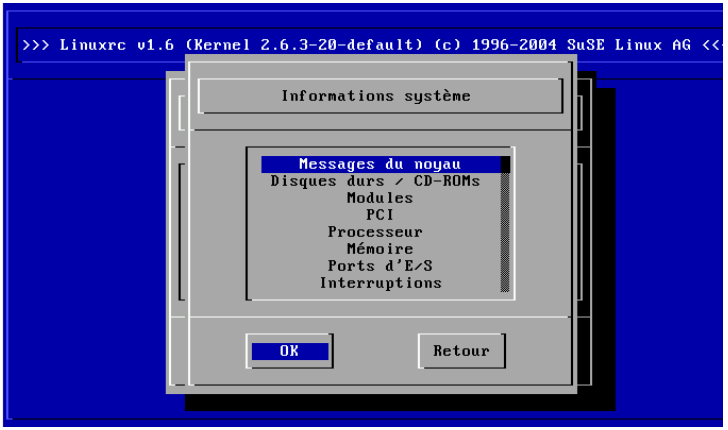


FIG. 3.3: *Informations système*

```
SCSI subsystem initialized
scsi0 : Adaptec AIC7XXX EISA/VLB/PCI SCSI HBA DRIVER, Rev 6.2.36
        <Adaptec aic7890/91 Ultra2 SCSI adapter>
        aic7890/91: Ultra2 Wide Channel A, SCSI Id=7, 32/253 SCBs

(scsi0:A:0): 40.000MB/s transfers (20.000MHz, offset 15, 16bit)
  Vendor: IBM       Model: DCAS-34330W       Rev: S65A
  Type:   Direct-Access                      ANSI SCSI revision: 02
scsi0:A:0:0: Tagged Queuing enabled.  Depth 32
SCSI device sda: 8467200 512-byte hdwr sectors (4335 MB)
SCSI device sda: drive cache: write back
 sda: sda1 sda2
Attached scsi disk sda at scsi0, channel 0, id 0, lun 0
(scsi0:A:6): 20.000MB/s transfers (20.000MHz, offset 16)
  Vendor: TEAC      Model: CD-ROM CD-532S    Rev: 1.0A
  Type:   CD-ROM                             ANSI SCSI revision: 02
```

3.1.4 Chargement de modules

C'est ici que vous indiquez les modules (pilotes) dont vous avez besoin.linuxrc propose les pilotes disponibles dans une liste. Vous voyez à gauche le nom du module concerné et à droite une description succincte du matériel pris en charge par le pilote. Un certain nombre de composants utilisent plusieurs pilotes ou des pilotes récents en version alpha. Ceux-ci sont également proposés.

FIG. *3.4:* *Charger des modules*

3.1.5 Saisie de paramètres

Lorsque vous avez trouvé le pilote prenant en charge votre matériel, appuyez sur la touche (Entrée). Un formulaire s'ouvre alors dans lequel vous pouvez saisir les paramètres du module à charger. Rappelons à cet égard que, contrairement à la saisie de paramètres à l'invite du noyau, il est nécessaire de séparer par des espaces les différents paramètres associés à un même module.

Dans la plupart des cas, il n'est pas nécessaire d'indiquer avec précision le matériel à utiliser, dans la mesure où la plupart des pilotes trouvent eux-mêmes vos composants. Il n'est nécessaire de préciser les paramètres que pour les cartes réseau et pour les anciens modèles de lecteurs de cédérom utilisant leur propre carte contrôleur. Dans tous les cas, faites d'abord un essai en appuyant sur (Entrée).

Pour certains modules, l'identification et l'initialisation du matériel peuvent durer relativement longtemps. Vous pouvez activer la console virtuelle 4 ((Alt)(F4)) pour voir les messages émis par le noyau durant le chargement. Les adaptateurs SCSI en particulier mettent un certain temps à se charger car ils attendent que tous les périphériques connectés se soient déclarés.

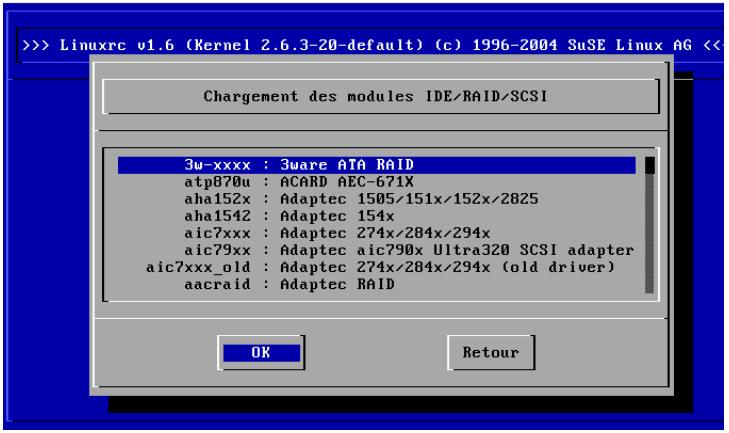


FIG. 3.5: *Choix des pilotes SCSI*

Lorsque le module a été chargé avec succès, les messages du noyau sont affichés par linuxrc, ce qui vous permet de vous assurer que tout s'est déroulé comme prévu. Dans le cas contraire, les messages qui s'affichent peuvent préciser la cause de l'échec.

Remarque

Si les modules par défaut ne prennent pas en charge votre support d'installation (lecteur de CD-ROM propriétaire, lecteur de CD-ROM sur port parallèle, carte réseau, PCMCIA), vous pouvez éventuellement recourir aux pilotes supplémentaires d'une disquette de modules pour générer ce type de disquette, reportez-vous à *Trucs et astuces* page 131. Allez à la fin de la liste et choisissez l'élément de menu 'Davantage de modules' ; dans ce cas, linuxrc exige la disquette de modules.

Remarque

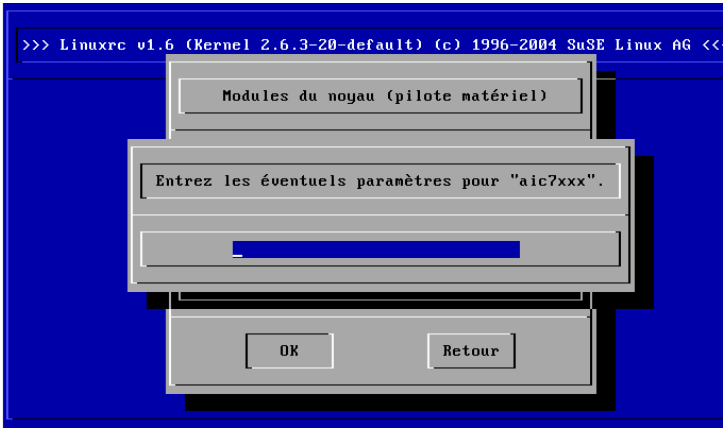


FIG. 3.6: *Saisie des paramètres pour le chargement d'un module*

3.1.6 Démarrer le système / l'installation

Lorsque la prise en charge de votre matériel nécessaire à l'installation à été réalisée par le noyau, vous pouvez passer au point 'Système / Démarrer l'installation'. Là, vous pouvez entreprendre plusieurs actions : 'Installation / Démarrer la mise à jour', 'Démarrer le système installé' (la partition racine doit être connue), 'Démarrer le système de sauvegarde' (voir la section *Le système de secours SUSE* page 192) ou 'Éjecter le CD'.

Appuyez maintenant sur (Retour) pour arriver à l'élément de menu 'Démarrer installation / mise à jour'. Choisissez ensuite le support source ; il suffit généralement de laisser le curseur sur la présélection : 'CD-ROM'.

Appuyez maintenant sur (Retour). L'environnement d'installation est directement démarré depuis le CD 1 ou le DVD. Dès que ce processus est achevé, YaST démarre et l'installation commence.

Pour l'installation (illustration 3.8 page 124) et, de manière analogue pour le système de récupération, vous pouvez choisir différentes sources (illustration 5.3 page 193).

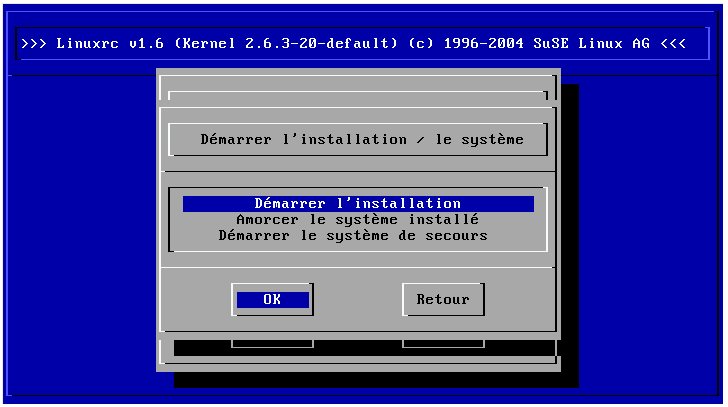


FIG. 3.7: *Menu d'installation de linuxrc*

3.1.7 Problèmes possibles

linuxrc n'offre pas la disposition de clavier souhaitée.
Dans ce cas, choisissez d'abord une autre disposition (en situation d'urgence : 'English (US)') ; après l'installation, on peut ensuite basculer avec YaST sur la bonne disposition.

L'adaptateur SCSI utilisé n'est pas reconnu :

- Essayez de charger le module d'un pilote compatible.
- Vérifiez s'il existe une disquette de mise à jour du pilote pour votre adaptateur.

Le lecteur de CD-ROM ATAPI utilisé reste bloqué lors de la lecture :
Reportez-vous à la section *Le CD-ROM ATAPI reste bloqué lors de la lecture* page 135.

Le système reste bloqué lors du chargement des données sur le disque virtuel :
Dans certains cas, des problèmes peuvent survenir lors du chargement des données sur le disque virtuel (*RAM disk*), de sorte qu'il est impossible de charger YaST. La méthode suivante donne le plus souvent un résultat satisfaisant :

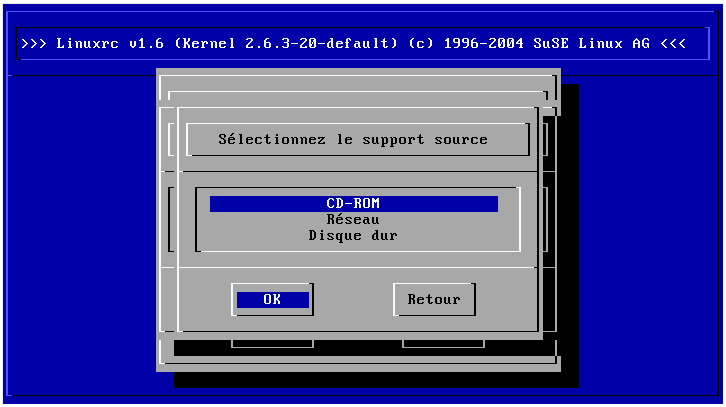


FIG. *3.8:* *Sélectionner le support source dans linuxrc*

Dans le menu principal de linuxrc, choisissez 'Configuration' → 'Débogage (experts)' ; réglez 'Forcer le chargement de l'image de root' (*Force root image*) sur 'non'. Retournez dans le menu principal et recommencez l'installation.

3.1.8 Passer des paramètres à linuxrc

Si linuxrc ne se trouve pas en mode manuel, l'application cherche un fichier Info, soit sur disquette, soit dans le fichier `initrd` du répertoire `/info`. C'est seulement à la suite de cette recherche que linuxrc lit les paramètres de l'invite du noyau. Les valeurs pré-enregistrées peuvent être modifiées dans le fichier `/linuxrc.config` qui est lu en premier lieu. Dans tous les cas, il vaut mieux enregistrer toute modification dans le fichier Info.

Un fichier Info est constitué de mots-clés et des valeurs associées selon le modèle `key: value`. Ces paires de mots-clés/valeur peuvent aussi être transmises à l'invite d'amorçage du support d'installation sous cette forme. Le fichier `/usr/share/doc/packages/linuxrc/linuxrc.html` contient une liste de tous les mots-clés disponibles. Quelques uns des mots-clés les plus importants vous sont donnés ici, à titre d'exemple, avec des valeurs d'exemple :

Install: URL (nfs, ftp, hd, ...) Définir la source d'installation avec un URL. Les protocoles acceptés sont `cd`, `hd`, `nfs`, `smb`, `ftp`, `http` et `tftp`. La syntaxe correspond à la syntaxe habituelle telle qu'elle peut aussi être utilisé dans un navigateur, par exemple :

- `nfs://<serveur>/<répertoire>`
- `ftp://[utilisateur[:motdepasse]@]<serveur>/<répertoire>`

Netdevice: <eth0> Si vous disposez de plusieurs périphériques Ethernet, vous pouvez sélectionner l'interface que doit utiliser linuxrc à l'aide du paramètre `Netdevice:`.

HostIP: <10.10.0.2> Ceci définit l'adresse IP de l'ordinateur.

Gateway: <10.10.0.128> Lorsque le serveur d'installation n'est pas situé dans le même sous-réseau que l'ordinateur, il peut être atteint via la passerelle (*gateway*) par défaut.

Proxy: <10.10.0.1> Pour les connexions de type ftp et http, vous pouvez également utiliser un proxy. Celui-ci doit être défini à l'aide du paramètre `Proxy:`.

ProxyPort: <3128> Si le proxy n'utilise pas le port par défaut, cette option peut définir le port à utiliser.

Textmode: <0|1> Utilisez ce paramètre pour démarrer YaST en mode textuel.

VNC: <0|1> Pour pouvoir installer confortablement des ordinateurs qui ne possèdent pas de console graphique, il est possible d'utiliser VNC pour contrôler le processus d'installation. Le paramètre `VNC` active ce service sur le système d'installation. Voyez aussi le paramètre `VNCPassword`.

VNCPassword: <password> Définit le mot de passe pour définir les droits d'accès lors d'une installation VNC.

UseSSH: <0|1> Prépare un accès SSH à linuxrc. Ceci permet une installation avec YaST en mode textuel.

SSHPassword: <password> Prépare le mot de passe pour l'utilisateur `root` dans linuxrc.

Insmod: <Modul> <Parameter> Charge le module défini dans le noyau. Les paramètres nécessaires au chargement du module sont entrés séparés par des espaces.

AddSwap: <0|3|/dev/hda5> Avec une valeur à 0 pour ce mot-clé, la partition d'échange (`swap`) n'est jamais utilisée. Si la valeur est positive, c'est la partition portant le numéro correspondant qui est activée. Il est également possible de donner directement le nom de la partition.

3.2 Installation via VNC

VNC (*Virtual Network Computing*) est une solution client-serveur qui permet de manipuler un serveur X distant au moyen d'un client léger et facile à manipuler. Ce client est disponible pour différents systèmes d'exploitation tels que diverses versions de Microsoft Windows, Apples MacOS et Linux.

On utilise le client VNC, vncviewer, pour garantir l'affichage graphique et la manipulation de YaST pendant le processus d'installation. Avant le démarrage du système à installer, vous devez d'abord préparer l'ordinateur distant afin qu'il puisse accéder par le biais du réseau au système à installer.

3.2.1 Préparation de l'installation VNC

Pour effectuer une installation VNC, vous devez transmettre quelques paramètres au noyau, ceci devant avoir lieu avant l'amorçage du noyau. Pour ce faire, transmettez à l'invite de commande d'amorçage les options suivantes :

```
vnc=1 vncpassword=<xyz> install=<Quelle>
```

`vnc=1` signalise que le serveur VNC est démarré sur le système d'installation. En entrant `vncpassword`, vous transmettez le mot de passe qui sera utilisé plus tard. La source d'installation (`install`) peut soit être indiquée manuellement (indication du protocole et de la page URL se référant au répertoire correspondant) soit contenir l'instruction `slp:/`. Dans le deuxième cas, la source d'installation est automatiquement recherchée par l'intermédiaire d'une demande SLP. Pour plus de détails sur SLP, consultez la section *SLP — Transmission de services dans le réseau* page 484.

3.2.2 Clients pour l'installation VNC

La connexion à l'ordinateur d'installation et au serveur VNC y étant exploité s'établit au moyen d'un client VNC. Sous SUSE LINUX, on utilise ce vncviewer, faisant partie du paquetage `xorg-x11-Xvnc`. Si vous souhaitez établir une connexion avec le système d'installation à partir d'un client Windows, vous devez installer dans le système Windows le programme tightvnc que vous trouverez sur le premier CD-ROM de SUSE LINUX dans le répertoire`/dosutils/tightvnc`.

Démarrez le client VNC de votre choix et entrez l'adresse IP du système d'installation ainsi que le mot de passe VNC dès que le programme vous invite à entrer ces indications.

Une solution alternative consiste à établir des connexions VNC également au moyen d'un navigateur internet compatible Java en entrant les informations suivantes dans le champ d'adresse internet du navigateur :

```
http://<IP-Adresse des Installationssystems>:5801/
```

Une fois la connexion établie, YaST est amorcé et vous pouvez commencer l'installation.

3.3 Installation en mode texte avec YaST

Au lieu de l'installer avec un assistant graphique, on peut installer le système à l'aide des menus en mode texte de YaST (mode console). Tous les modules de YaST sont eux aussi disponibles dans ce mode texte. On peut s'en servir en particulier lorsque l'on n'a pas besoin d'interface graphique (systèmes serveurs) ou si la carte graphique n'est pas prise en charge par le Système X Window. L'installation dans ce mode d'installation est également possible pour les malvoyants à l'aide des périphériques de sortie adéquats.

Vous devez tout d'abord configurer la séquence d'amorçage dans le BIOS de l'ordinateur afin qu'il s'amorce sur le lecteur de CD-ROM. Insérez le DVD ou le CD 1 dans le lecteur et redémarrez l'ordinateur. L'écran de démarrage apparaîtra au bout de quelques instants.

Avec les touches ↑ et ↓, choisissez 'Installation manuelle' dans un délai de 10 secondes, afin que le système installé *ne* démarre *pas* automatiquement. Saisissez les paramètres d'amorçage dans la ligne `boot options` si votre matériel l'exige. Toutefois, aucun paramètre particulier n'est en principe nécessaire. Si, comme langue d'installation, vous sélectionnez la langue de votre clavier, la disposition du clavier sera configurée correctement. Ceci simplifie la saisie des paramètres.

La touche F2 ('Mode graphique') permet de fixer la résolution d'écran pour l'installation. Choisissez 'Mode texte' pour passer en mode texte pur si la carte graphique pose par ailleurs des problèmes pendant l'installation. Pour terminer, appuyez sur Retour chariot. Une barre de progression indiquant "Loading Linux kernel" apparaît, puis le noyau s'amorce et linuxrc démarre. Le programme linuxrc est piloté par menus et attend une saisie de l'utilisateur.

Diverses difficultés d'amorçage se résolvent généralement à l'aide de paramètres de noyau. En cas de problèmes de DMA, on dispose de l'option de démarrage 'Installation - Safe Settings'.

Si votre lecteur de CD-ROM (ATAPI) reste bloqué lors de l'amorçage du système, lisez la section *Le CD-ROM ATAPI reste bloqué lors de la lecture* page 135.

En cas de difficultés avec ACPI (*Advanced Configuration and Power Interface*) on peut jouer sur les paramètres du noyau suivants :

`acpi=off` Ce paramètre désactive le système ACPI complet. Il se justifie par exemple si votre ordinateur ne dispose pas de prise en charge ACPI ou si vous soupçonnez fortement que l'implémentation ACPI pose des problèmes.

`acpi=oldboot` Désactive presque complètement le sytème ACPI, seuls les éléments nécessaires à l'amorçage sont utilisés.

`acpi=force` Active ACPI même si votre ordinateur a un BIOS antérieur à 2000. Ce paramètre prend le pas sur `acpi=off`.

`pci=noacpi` Ce paramètre désactive le détournement d'IRQ PCI du nouveau système ACPI.

Recherchez également les articles de la base de données support sur `https://portal.suse.com` à l'aide du mot-clé *acpi*.

Choisissez 'Memory Test' dans le menu d'amorçage pour contrôler la mémoire si des difficultés "inexplicables" surviennent lors du chargement du noyau ou au cours de l'installation. Linux impose des exigences élevées en ce qui concerne le matériel. La mémoire et son temps de latence doivent être parfaitement ajustés ! Vous trouverez plus d'informations dans la base de données support à l'aide du mot-clé *memtest86*. Le mieux est d'effectuer le test de mémoire durant la nuit.

3.4 Démarrer SUSE LINUX

Après l'installation, il reste à déterminer comment vous souhaitez démarrer Linux au quotidien. L'aperçu qui suit présente les différentes possibilités de démarrage de Linux. La meilleure méthode pour vous parmi celles-ci dépend surtout de l'utilisation que vous prévoyez.

Chargeur d'amorçage de Linux La solution la plus propre techniquement et la plus universelle consiste à utiliser un gestionnaire d'amorçage de Linux comme GRUB (*GRand Unified Bootloader*) ou LILO (*LInux LOader*), qui permet de choisir entre différents systèmes d'exploitation avant l'amorçage. Le chargeur d'amorçage peut déjà être mis en place lors de l'installation ou être configuré ultérieurement, par exemple, avec YaST.

Disquette d'amorçage Vous démarrez Linux au moyen de la *disquette d'amorçage* (disquette de boot). Cette méthode fonctionne toujours et la disquette d'amorçage peut être générée avec YaST. Consultez la section *Création d'une disquette d'amorçage, de secours ou de modules* page 100

La disquette d'amorçage est aussi une solution provisoire judicieuse si vous ne maîtrisez pas encore les autres possibilités ou si vous souhaitez différer votre décision à propos du mécanisme d'amorçage définitif. De plus, si vous ne voulez pas écraser le chargeur d'amorçage d'un autre système d'exploitation, la disquette d'amorçage est une solution acceptable.

Attention

Certains BIOS vérifient la structure du secteur d'amorçage (MBR) et affichent par erreur une alerte de virus après que l'on ait installé GRUB ou LILO. Cette difficulté se contourne facilement en désactivant la 'protection contre les virus' dans le BIOS, si cette option existe. Vous pourrez réactiver cette option plus tard. Mais cette fonctionnalité est superflue si Linux est votre unique système d'exploitation.

Attention

Vous trouverez une étude détaillée de différentes méthodes d'amorçage, au chapitre *Amorçage et chargeur d'amorçage* page 205.

3.4.1 L'écran graphique SUSE

L'écran graphique SUSE apparaît sur la console 1 lorsque l'option "vga=<valeur>" est passée en tant que paramètre au noyau. Au moment de l'installation avec YaST, cette option est réglée automatiquement en fonction de la résolution choisie et de la carte graphique utilisée.

3.4.2 Désactiver l'écran SUSE

Vous avez en principe trois possibilités :

- Désactiver l'écran SUSE à la demande.
  Saisissez sur la ligne de commande : `echo 0 >/proc/splash`.
  L'écran graphique peut ainsi être désactivé. La commande suivante permet de le réactiver : `echo 0x0f01 >/proc/splash`.
- Désactiver l'écran SUSE par défaut :
  Ajoutez à la configuration du chargeur d'amorçage un paramètre du noyau `splash=0`. Vous trouverez davantage d'informations à ce propos au chapitre *Amorçage et chargeur d'amorçage* page 205. Si toutefois vous préférez le mode texte qui était proposé par défaut sur les versions antérieures, saisissez à la place `vga=normal`.
- Désactiver définitivement l'écran SUSE :
  Compilez un nouveau noyau et désactivez l'option 'Use splash screen instead of boot logo' dans le menu 'frame-buffer support'.

Remarque

L'écran de démarrage est automatiquement désactivé lorsque vous avez désactivé le prise en charge du frame buffer dans le noyau. Si vous compilez votre propre noyau, SUSE ne peut pas garantir de services d'assistance pour le système !

Remarque

3.5 Installations particulières

3.5.1 Installation sans prise en charge du CD-ROM

Que faire lorsqu'une installation par défaut au moyen d'un lecteur de CD-ROM n'est pas possible ? Votre lecteur de CD-ROM peut ne pas être pris en charge du fait qu'il s'agit d'un ancien lecteur propriétaire. Ou bien vous n'avez peut-être pas de lecteur de CD-ROM dans votre second ordinateur (par exemple un portable), mais un adaptateur Ethernet susceptible de convenir.

Sur ce type d'ordinateur sans prise en charge du CD-ROM, SUSE LINUX vous offre la possibilité de procéder à une installation au travers d'une connexion réseau : dans ces cas-là, on fait principalement appel à NFS ou FTP *via* Ethernet.

3.5.2 Installation en réseau

Cette méthode n'est pas couverte par l'assistance à l'installation. Elle est donc réservée aux seuls utilisateurs expérimentés en informatique. Pour installer SUSE LINUX par le biais d'une source réseau, deux étapes sont nécessaires :

1. La mise à disposition des données nécessaires à l'installation (CDs, DVD) sur un ordinateur qui servira plus tard de source d'installation.
2. L'amorçage du système à installer au moyen d'une disquette, d'un CD ou du réseau et la configuration du réseau.

La source d'installation peut être rendue disponible grâce à différents protocoles. Sous Linux, vous disposez de NFS et FTP pour mettre les sources à votre disposition de façon simple. Pour l'installation en soi, veuillez consulter la section *Passer des paramètres à linuxrc* page 124.

3.6 Trucs et astuces

3.6.1 Créer une disquette d'amorçage sous DOS

Il vous faut une disquette HD 3,5 pouces formatée et un lecteur de disquettes 3,5 pouces à partir duquel l'amorçage est possible.

Le répertoire `boot` du CD 1 contient quelques images de disquettes. Une telle image peut être copiée sur une disquette grâce à des programmes utilitaires appropriés ; on parle alors de disquette d'amorçage.

En outre, les images de disquettes renferment aussi le chargeur (*Loader*) Syslinux et le programme linuxrc. Syslinux permet de choisir le noyau souhaité pendant le processus d'amorçage et au besoin de passer des paramètres concernant le matériel utilisé. Le programme linuxrc vous assiste lors du chargement des modules de noyau prenant en charge votre matériel particulier et démarre enfin l'installation.

Créer une disquette d'amorçage avec rawwritewin

Vous pouvez trouver sous Windows le programme graphique rawwritewin. Sous Windows, vous trouverez ce programme sur le CD 1 dans le répertoire `dosutils/rawwritewin`.

Une fois démarré, vous devez lui fournir le fichier image. Les fichiers images se trouvent également sur le CD 1 dans le répertoire boot. Vous avez au minimum besoin des images "bootdisk" et "modules1". Pour voir ces fichiers dans l'explorateur de fichiers, vous devez changer le type de fichier en "all files".

Insérez une disquette dans votre lecteur de disquettes et cliquez sur 'write'.

Pour écrire plusieurs disquettes, répétez simplement cette procédure.

Créer une disquette d'amorçage avec rawrite

Pour créer les disquettes d'amorçage et de modules de SUSE, vous disposez du programme DOS `rawrite.exe` (CD 1, répertoire `dosutils\rawrite`). Un ordinateur équipé d'un DOS (par exemple, FreeDOS) ou de Windows est nécessaire pour cette opération.

Voici la description des étapes si vous travaillez sous Windows :

1. Insérez le CD numéro 1 de SUSE LINUX.
2. Ouvrez une fenêtre DOS (avec le menu Démarrer, dans 'Utilitaires' → 'Invite de commandes MS-DOS').
3. Démarrez le programme rawrite.exe en indiquant le chemin correct vers le lecteur de CD. Dans notre exemple, vous vous trouvez sur le disque dur `C:`, dans le répertoire `Windows` et votre lecteur de CD porte la lettre `D:`

   ```
   C:\Windows: d:\dosutils\rawrite\rawrite
   ```

4. Après avoir démarré, le programme demande la source et la cible (*destination*) des fichiers à copier. Il s'agit de l'emplacement de l'image de la disquette d'amorçage sur le CD numéro 1 du jeu de CDs, qui se trouve dans `boot`. Le nom du fichier est tout simplement `bootdisk`. N'oubliez pas non plus d'indiquer ici le chemin vers votre lecteur de CD.

   ```
   C:\Windows: d:\dosutils\rawrite\rawrite
   RaWrite 1.2 - Write disk file to raw floppy diskette

   Enter source file name: d:\boot\bootdisk
   Enter destination drive: a:
   ```

Dès que vous avez saisi la lettre du lecteur cible `a:`, rawrite vous invite à insérer une disquette formatée et à appuyer sur (Entrée). La progression de la copie s'affiche ensuite au cours de la procédure. Elle peut s'interrompre à l'aide de la combinaison de touches (Ctrl)-(c).

Vous pouvez aussi créer de cette manière les autres images de disquettes `modules1`, `modules2`, `modules3` et `modules4`. Celles-ci sont requises lorsque vous avez des périphériques USB ou SCSI ou une carte réseau ou PCMCIA et que vous souhaitez y accéder dès l'installation. Une disquette de modules peut aussi s'avérer nécessaire pour utiliser un système de fichiers spécial au cours de cette phase.

3.6.2 Créer une disquette d'amorçage sous un système de type Unix

Conditions requises

Vous pouvez recourir à un système de type Unix ou Linux équipé d'un lecteur de CD-ROM opérationnel. Prévoyez une disquette vérifiée (formatée).

Pour créer des disquettes d'amorçage, procédez comme suit :

1. Si vous devez encore formater les disquettes :

   ```
   fdformat /dev/fd0u1440
   ```

   Montez le CD 1, par exemple dans `/media/cdrom`:
2. `mount -tiso9660 /dev/cdrom /media/cdrom`
3. Sur le CD, placez-vous dans le répertoire `boot`:

   ```
   cd /media/cdrom/boot
   ```

4. Créez la disquette d'amorçage avec la commande

   ```
   dd if=/media/cdrom/boot/bootdisk of=/dev/fd0 bs=8k
   ```

Dans le répertoire `boot`, le fichier `README` vous indique les détails concernant les images de disquettes; ces fichiers se lisent avec `more` ou `less`.

Vous pouvez aussi créer de cette manière les autres images de disquettes `modules1`, `modules2`, `modules3` et `modules4`. Celles-ci sont requises lorsque vous avez des périphériques USB ou SCSI ou une carte réseau ou PCMCIA et que vous souhaitez y accéder dès l'installation. Une disquette de modules peut aussi s'avérer nécessaire pour utiliser un système de fichiers spécial au cours de cette phase.

Les choses se compliquent si vous souhaitez par exemple utiliser un noyau compilé par vos soins pendant l'installation. Dans ce cas, écrivez d'abord l'image par défaut (`bootdisk`) sur la disquette et écrasez ensuite le noyau réel (`linux`) avec votre propre noyau (reportez-vous à la section *Compilation du noyau* page 234):

```
dd if=/media/cdrom/boot/bootdisk of=/dev/fd0 bs=8k
mount -t msdos /dev/fd0 /mnt
cp /usr/src/linux/arch/i386/boot/vmlinuz /mnt/linux
umount /mnt
```

3.6.3 Amorcer depuis une disquette (SYSLINUX)

La disquette d'amorçage peut toujours se révéler utile lorsque l'installation se déroule dans des conditions particulières (par exemple, lorsque le lecteur de CD-ROM n'est pas disponible). Pour créer la disquette d'amorçage, reportez-vous à *Créer une disquette d'amorçage sous DOS* page 131 et à *Créer une disquette d'amorçage sous un système de type Unix* page précédente.

Le processus d'amorçage est déclenché par le chargeur d'amorçage SYSLINUX (`syslinux`). SYSLINUX est configuré de manière à effectuer une reconnaissance du matériel limitée lors de l'amorçage. Il s'agit essentiellement des étapes suivantes :

1. Vérifier si le BIOS prend en charge un framebuffer conformément à VESA 2.0 et amorcer le noyau en conséquence.
2. Sélectionner les données des moniteurs (informations DDC).
3. Lire le bloc numéro 1 depuis le premier disque dur (MBR) pour décider plus tard de d'attribuer des identificateurs BIOS aux noms des périphériques (*devices*) lors de la configuration du gestionnaire d'amorçage. Il faut en outre essayer de lire le bloc au moyen des fonctions lba32 du BIOS pour vérifier s'il gère ces fonctions.

Remarque

Pour ignorer toutes ces étapes, il suffit d'appuyer sur les touches (Verrouillage Majuscules) ou (Maj) au démarrage de SYSLINUX. En cas d'erreur, il est possible d'ajouter à `syslinux.cfg` la ligne

```
verbose 1
```

Le gestionnaire d'amorçage annonce alors chaque action en cours dans l'ordre.

Remarque

Si l'ordinateur refuse de s'amorcer depuis la disquette, il est probable qu'il faille auparavant adapter la séquence d'amorçage dans le BIOS de l'ordinateur ainsi : `A,C,CDROM`.

► **x86**
Sur les systèmes x86, outre le CD 1, le deuxième CD est également amorçable. Tandis que le CD 1 fonctionne grâce à une image ISO amorçable, le CD 2 est amorcé au moyen d'une image de disque de 2,88 Mo. N'utilisez le CD 2 que si vous êtes sûr que vous pouvez amorcer depuis un CD, mais que cela ne fonctionne pas avec le CD 1 (c'est une solution de repli). ◄

3.6.4 Mon lecteur de CD-ROM prend-il en charge Linux ?

On peut généralement affirmer que la plupart des lecteurs de CD-ROM sont pris en charge.

- Il ne devrait y avoir aucun problème avec les lecteurs ATAPI.
- La gestion des lecteurs de CD-ROM SCSI ne dépend que de la prise en charge du contrôleur SCSI connecté au lecteur de CD-ROM. Les contrôleurs pris en charge sont indiqués dans la base de données des composants CDB. Lorsque votre contrôleur SCSI n'est pas pris en charge et que le disque dur dépend également du contrôleur SCSI, l'installation n'est malheureusement pas possible. Dans ce cas, vérifiez si le fabricant de votre contrôleur SCSI offre un pilote pour Linux.
- Beaucoup de lecteurs de CD-ROM propres à certains fabricants fonctionnent aussi sous Linux. Les lecteurs dans cette catégorie peuvent néanmoins poser des problèmes. Si votre lecteur n'est pas explicitement mentionné, vous pouvez toujours essayer un type similaire du même fabricant.
- Les lecteurs de CD-ROM USB sont également pris en charge. Si le BIOS de votre ordinateur ne gère pas encore l'amorçage des périphériques USB, commencez l'installation au moyen des disquettes d'amorçage. Vous trouverez plus de détails à ce sujet dans *Amorcer depuis une disquette (SYSLINUX)* page ci-contre. Avant d'amorcer avec une disquette, veillez à ce que tous les périphériques USB nécessaires soient déjà connectés et sous tension.

3.7 Le CD-ROM ATAPI reste bloqué lors de la lecture

Bien souvent, lorsque le lecteur de CD-ROM ATAPI n'est pas reconnu ou reste bloqué lors de la lecture, c'est parce que le matériel est mal configuré. Les différents périphériques devraient normalement être connectés au bus (E)IDE à la

suite l'un de l'autre : c'est-à-dire que le premier périphérique est maître sur le premier contrôleur et le deuxième esclave. Enfin, le troisième périphérique est maître sur le second contrôleur et le quatrième est à nouveau esclave.

On ne trouve souvent dans un ordinateur que le disque dur et le lecteur de CD-ROM, qui se bloque lorsqu'il est maître sur le second contrôleur. Dans certains cas, Linux à lui seul ne s'en sort pas avec ce trou. La plupart du temps, on peut néanmoins aider le noyau à le sauter en indiquant un paramètre approprié (`hdc=cdrom`).

Il suffit parfois de placer un faux cavalier (jumper) pour un lecteur ; en d'autres termes, 'il est configuré comme esclave, bien qu'il soit connecté comme maître sur le second contrôleur, ou inversement. En cas de doute, il faut vérifier ces paramètres et le cas échéant les corriger.

En outre, il existe encore de nombreuses puces EIDE défectueuses. Celles-ci sont pour la plupart connus à ce jour ; le noyau contient du code pour éviter ce type de problèmes. Un noyau spécial existe pour ces cas (reportez-vous au `README` dans le répertoire `/boot` du CD-ROM d'installation).

Si l'amorçage ne devait pas fonctionner du premier coup, essayez les paramètres du noyau suivants :

`hdx=cdrom` `x` vaut ici `a`, `b`, `c`, `d`, etc. et signifie :

- `a` — Maître sur le premier contrôleur IDE
- `b` — Esclave sur le premier contrôleur IDE
- `c` — Maître sur le second contrôleur IDE

`hdb=cdrom` est un exemple de `paramètres à saisir`. Ce paramètre vous permet d'indiquer le lecteur de CD-ROM au noyau lorsque ce dernier ne le trouve pas et que vous avez un lecteur de CD-ROM ATAPI.

`idex=noautotune` `x` vaut `0`, `1`, `2`, `3`, etc. et signifie :

- `0` — Premier contrôleur IDE
- `1` — Second contrôleur IDE

`ide0=noautotune` est un exemple de `paramètre à donner`. Ce paramètre est d'habitude utile pour les disques durs (E)IDE.

3.8 Périphériques SCSI et noms de fichiers des périphériques durables

Les périphériques SCSI, comme par exemple les partitions de disques durs, reçoivent lors de l'amorçage des noms de fichiers qui leur sont attribués de manière plus ou moins dynamique. Cela ne représente aucun problème dans la mesure où ni le nombre ni la configuration des périphériques ne sont modifiés. Mais lorsque l'on ajoute un disque dur SCSI supplémentaire et que celui-ci est reconnu par le noyau avant l'ancien disque dur, ce dernier reçoit un nouveau nom et les éléments dans la table de montage `/etc/fstab` ne correspondent alors plus.

Pour contourner cette difficulté, il est possible d'utiliser le script d'amorçage système `boot.scsidev`. `boot.scsidev` peut être activé à l'aide de la commande `/sbin/insserv` et les paramètres nécessaires sont enregistrés dans `/etc/sysconfig/scsidev`. Le script `/etc/rc.d/boot.scsidev` inscrit des noms de périphériques permanents dans `/dev/scsi/`. Ces noms de périphériques peuvent être utilisés dans le fichier `/etc/fstab`. Si des noms de périphériques persistents doivent être utilisés, il est possible de les définir dans le fichier `/etc/scsi.alias`. Voyez aussi `man scsidev`.

Remarque

Noms de périphériques et udev

boot.scsidev est également supporté sous SUSE LINUX. Cependant, il est conseillé d'utiliser udev pour la génération de noms de périphériques. dans ce cas, les entrées sont faites dans `/dev/by-id/` de udev.

Remarque

Dans le mode expert de l'éditeur de niveaux d'exécution, il faut faire appel à `boot.scsidev` pour l'étape `B`, les liens utiles sont alors placés dans `/etc/init.d/boot.d`, ce qui permet de créer les noms lors de l'amorçage.

3.9 Partitionnement pour les experts

Le chapitre sur l'installation par défaut aborde les différentes possibilités de partitionnement du système (reportez-vous à [1]). Cette section fournit des informations détaillées qui vous permettront de créer un schéma de partitionnement optimal. Elle intéressera en particulier les utilisateurs qui aimeraient configurer au mieux leur système, tant en termes de sécurité que de vitesse, et qui pour cela sont prêts le cas échéant à remettre complètement à neuf le système existant.

Nous supposons que vous comprenez de façon élémentaire le mode de fonctionnement d'un système de fichiers UNIX. Les notions de point de montage, de partition physique, étendue et logique ne devraient pas vous être étrangères.

La première étape consiste à réunir les informations suivantes :

- Comment cet ordinateur sera-t-il utilisé (serveur de fichiers, serveur d'applications, serveur de calcul, ordinateur personnel) ?
- Combien de personnes travailleront-elles sur cet ordinateur (sessions simultanées) ?
- Combien de disques durs l'ordinateur comporte-t-il, quelle est leur taille et de quel système disposez-vous (contrôleur EIDE, SCSI ou RAID) ?

3.9.1 Taille de la partition d'échange (swap)

Vous lirez souvent : "la taille de la partition d'échange doit au moins être le double de celle de la mémoire centrale". Cette formulation vient encore d'une époque où 8 Mo de mémoire vive dans un ordinateur, ce n'était pas rien. L'ordinateur disposait ainsi d'environ 30 à 40 Mo de mémoire virtuelle, c'est-à-dire de mémoire vive plus de mémoire d'échange. Avec les applications modernes, ces valeurs doivent également être revues à la hausse. Un utilisateur moyen ne rencontrera pas de problème s'il table sur 512 Mo de mémoire virtuelle. Vous ne devriez en aucun cas ne pas créer de mémoire d'échange du tout.

Lorsque vous utilisez l'hibernation (suspend to disk), la mémoire principale est enregistrée sur la partition d'échange. Dans ce cas, la partition d'échange doit impérativement être plus importante que la mémoire principale.

3.9.2 Suggestions de partitionnement pour scénarios spéciaux

Utilisation comme serveur de fichiers

Ici, on s'intéresse *vraiment* aux performances du disque dur. Les périphériques SCSI devraient absolument avoir la préférence. Tenez également compte de la performance des disques et du contrôleur utilisé.

Un serveur de fichiers offre la possibilité de gérer des données de manière centralisée. Il peut s'agir dans ce cas de répertoires utilisateur, de bases de données ou d'autres archives. L'avantage est que l'administration est considérablement simplifiée. Si le serveur de fichiers doit servir un réseau plus étendu (à partir de 20 utilisateurs), l'optimisation de l'accès au disque devient essentielle. Admettons que vous souhaitiez développer un serveur de fichiers qui doit mettre à disposition les répertoires personnels (home) de 25 utilisateurs : vous savez que chaque utilisateur prendra au maximum 1000 à 1500 Mo pour ses données personnelles. Si aucun de ces utilisateurs ne fait de compilation dans son répertoire personnel, une partition de 40 Go conviendra à cet effet, une fois montée dans `/home`.

Si vous avez 50 utilisateurs, il faut compter sur une partition de 80 Go. Dans ce cas, il vaut cependant mieux répartir `/home` sur deux disques durs de 40 Go, puisque ceux-ci ne se partagent alors pas la charge (ni le temps d'accès !).

Remarque

Les utilisateurs devraient absolument placer le cache de leur navigateur web sur leurs disques durs locaux !

Remarque

Utilisation comme serveur de calcul

Un serveur de calcul est généralement un ordinateur performant qui se charge des tâches intensives de calcul au sein du réseau. Une telle machine dispose en général d'une mémoire centrale assez étendue (au moins 512 Mo de mémoire vive). Le seul aspect auquel il faut veiller pour obtenir un débit plus rapide des disques concerne les éventuelles partitions d'échange. Ici également, répartissez plusieurs partitions d'échange sur plusieurs disques.

3.9.3 Possibilités d'optimisation

Les disques sont le principal facteur limitant. Pour éviter ce goulot d'étranglement, il y a trois possibilités qu'il est préférable de mettre en œuvre ensemble :

- Répartir la charge de manière égale sur plusieurs disques.
- Mettre en place un système de fichiers optimisé (par exemple `reiserfs`).
- Équiper le serveur de fichiers de suffisamment de mémoire (256 Mo minimum).

Mettre en parallèle plusieurs disques

La méthode citée en premier exige une explication plus approfondie. La totalité du temps qui s'écoule jusqu'à la mise à disposition des données demandées se décompose approximativement ainsi :

1. Temps nécessaire pour que la demande arrive au contrôleur de disque.
2. Temps nécessaire au contrôleur de disque pour envoyer cette requête au disque dur.
3. Temps nécessaire au disque dur pour positionner sa tête.
4. Temps nécessaire au support pour tourner jusqu'au bon secteur.
5. Temps nécessaire pour le transfert.

Le point 1 dépend de la connexion réseau et doit être réglé à ce niveau. Le point 2 est un délai relativement négligeable qui dépend du contrôleur de disque lui-même. Les points 3 et 4 sont les plus importants. Le positionnement est mesuré en ms. Si l'on compare au temps d'accès en mémoire centrale mesuré en ns, on obtient un facteur de l'ordre de 1 million ! Le point 4 dépend du nombre de tours/minute du disque. Ce délai est également de l'ordre de plusieurs ms la plupart du temps. Le point 5 dépend du nombre de tours/minute et du nombre de têtes, ainsi que de la position courante de la tête (au centre ou à la périphérie).

Pour obtenir des performances optimales, il faut donc se pencher sur le point 3. La fonctionnalité disconnect des périphériques SCSI entre en jeu ici. Grâce à elle, voici sommairement ce qui se passe :

Le contrôleur envoie au périphérique connecté (dans ce cas, le disque dur) la commande Aller à la piste x, secteur y. Maintenant, la mécanique inerte du disque doit se mettre en mouvement. Si le disque est intelligent (donc, connaît `disconnect`) et si le pilote du contrôleur gère aussi cette fonctionnalité, le contrôleur envoie directement au disque une commande `disconnect` et le disque se sépare du bus SCSI. À partir de cet instant, d'autres périphériques

peuvent procéder à leurs transferts. Au bout d'un certain temps (selon une stratégie et/ou la charge sur le bus SCSI), la connexion est activée à nouveau sur le disque. Dans l'idéal, ce dernier a déjà atteint la piste demandée.

Dans un système d'exploitation multitâche et multiutilisateur comme Linux, cela permet naturellement de procéder à une bonne optimisation. Examinons un extrait du résultat de la commande `df` (reportez-vous à l'affichage de 3.1).

Exemple 3.1: *Exemple de résultat de la commande df*

```
Système de fichiers Taille Utilisé Disponible % d'utilisation Monté sur
/dev/sda5 1,8 Go 1.6 Go 201 M 89 % /
/dev/sda1 23 Mo 3,9 Mo 17 Mo 18 % /boot
/dev/sdb1 2,9 Go 2,1 Go 677 Mo 76 % /usr
/dev/sdc1 1,9 Go 958 Mo 941 Mo 51 % /usr/lib
shmfs 185 Mo 0 184 Mo 0 % /dev/shm
```

Que nous apporte cette parallélisation ? Supposons que nous saisissions la commande suivante en tant qu'utilisateur `root` dans `/usr/src` :

```
tar xzf paquetage.tar.gz -C /usr/lib
```

Cette commande installe paquetage.tar.gz sous `/usr/lib/paquetage`. Pour ce faire, l'interpréteur de commandes (le *shell*) appelle tar et gzip (il se trouvent dans /bin, lui-même sur `/dev/sda`), puis `paquetage.tar.gz` est lu depuis `/usr/src` (qui se trouve sur le disque `/dev/sdb`). Enfin, les données extraites sont écrites sous `/usr/lib` (se trouvant sur `/dev/sdc`). Le positionnement, aussi bien que la lecture/l'écriture des tampons internes du disque peuvent maintenant s'exécuter pratiquement en parallèle.

C'est un exemple parmi de nombreux autres. En règle générale, lorsque l'on dispose de nombreux disques (de vitesses semblables), `/usr` et `/usr/lib` devraient résider sur des disques différents. Dans ce cadre, `/usr/lib` devrait avoir une capacité d'environ 70 % de `/usr`. Le répertoire racine `/` devrait se trouver au même endroit que `/usr/lib` lorsque l'on répartit sur deux disques, en raison de la fréquence d'accès au disque.

Vitesse et mémoire centrale

Nous attirons l'attention à de nombreux endroits sur le fait que la taille de la mémoire centrale sous Linux est souvent plus importante que la vitesse du processeur. Une raison – même si ce n'est pas la principale – de ce phénomène est est que Linux utilise des tampons dynamiques pour les données des disques durs. Dans ce cadre, Linux emploie toutes sortes de subterfuges comme le read ahead (il charge par précaution des secteurs à l'avance) et le delayed write (les accès en écriture sont mis de côté pour s'effectuer en une seule fois ensuite). Cette dernière fonctionnalité est la raison pour laquelle on ne peut pas simplement mettre un ordinateur sous Linux hors tension. Ces deux techniques sont responsables du fait qu'avec le temps, la mémoire centrale semble toujours se remplir et que Linux est si rapide ; reportez-vous aussi à la section *La commande free* page 242.

3.10 Configuration du gestionnaire de volumes logiques (LVM)

YaST contient un outil de partitionnement professionnel qui vous permet de traiter les partitions existantes, de les supprimer ou d'en ajouter de nouvelles. À partir de ce module de YaST, vous avez accès à la configuration du RAID logiciel et du gestionnaire de volumes logiques (*Logical Volume Manager*, LVM).

Remarque

Vous trouverez des informations sur les tenants et les aboutissants et des conseils sur le partitionnement dans la section *Partitionnement pour les experts* page 138.

Remarque

Normalement, les partitions se définissent pendant l'installation. Si vous souhaitez ajouter un deuxième disque dur, vous pouvez aussi intégrer celui-ci dans le système Linux existant. Vous devez ensuite, pour ce faire, partitionner ce nouveau disque dur, puis monter ces nouvelles partitions et enfin les déclarer dans `/etc/fstab`. Le cas échéant, il est nécessaire de copier quelques données pour déplacer une partition `/opt` trop petite de l'ancien disque dur sur le nouveau.

Faites preuve de précaution si vous souhaitez modifier le partitionnement du disque dur sur lequel vous travaillez actuellement – cela est en principe possible, mais il faut immédiatement après redémarrer le système. Il est impensable d'amorcer à partir du cédérom puis d'entreprendre ensuite la modification du partitionnement. Appuyez sur le bouton 'Experts...' du programme de partitionnement pour faire apparaître un menu avec les commandes suivantes :

Relecture de la table des partitions Sert à lire le partitionnement à nouveau à partir du disque dur. Vous avez besoin de cette option par exemple si vous avez effectué le partitionnement sur la console texte manuellement.

Adaptation des points de montage d'un fichier /etc/fstab existant
N'a un sens que pendant l'installation. La lecture de l'ancien `fstab` n'est nécessaire que si vous ne mettez pas à jour votre système mais que vous le réinstallez. Vous n'avez alors pas besoin d'indiquer manuellement les points de montage.

Effacer la table des partitions et le label du disque
Permet d'écraser complètement l'ancienne table des partitions. Cela peut par exemple être utile si vous rencontrez des problèmes avec des labels de disques durs inhabituels. Avec cette méthode toutefois, toutes les données sur le disque dur sont perdues.

3.10.1 Gestionnaire de volumes logiques (LVM)

À partir de la version 2.6 du noyau, le gestionnaire de volumes logiques est disponible dans sa version 2. Celui-ci offre une compatibilité ascendante avec les gestionnaires de volumes logiques précédents et peut toujours gérer les anciens groupes de volumes. Si vous créez de nouveaux groupes de volumes, vous devez décider si vous souhaitez utiliser le nouveau format ou la celui compatible avec la version précédente. Le gestionnaire de volumes logiques 2 n'a plus besoin d'aucun correctif du noyau et utilise le *device mapper* (mise en correspondance des périphériques), intégré dans la version 2.6. À partir de ce noyau, le gestionnaire de volumes logiques ne peut plus être utilisé que dans la version 2. Dans ce chapitre on entend toujours par gestionnaire de volumes logiques le gestionnaire de volumes logiques dans la version 2.

Le gestionnaire de volumes logiques vous permet de répartir de manière flexible la place sur le disque dur entre les différents systèmes de fichiers. Comme la modification des partitions sur un système en cours d'exploitation nécessite de gros efforts, on a développé le gestionnaire de volumes logiques : il met une réserve virtuelle (Volume Group – abrégé VG) à disposition dans l'espace mémoire dans lequel sont générés les volumes logiques en fonction des besoins. Le système d'exploitation utilise alors ces derniers plutôt que les partitions physiques.

Particularités :

- Vous pouvez rassembler plusieurs disques durs/partitions en une grande partition logique.
- Si l'espace disponible sur un volume logique (par exemple `/usr`) tire à sa fin, vous pouvez l'agrandir en le configurant de manière appropriée.
- Avec le gestionnaire de volumes logiques, vous pouvez même ajouter des disques durs ou des volumes logiques dans un système en cours d'exploitation ; la condition préalable étant qu'il faut utiliser du matériel pouvant être remplacé à chaud approprié pour ce genre d'interventions.
- Vous pouvez utiliser plusieurs disques durs en mode RAID 0 (striping, entrelacement) pour obtenir une amélioration des performances.
- La fonctionnalité "snapshot" (instantané) permet, notamment sur les serveurs, de réaliser des sauvegardes cohérentes alors même que le système est en cours de fonctionnement.

L'utilisation du gestionnaire de volumes logiques est déjà utile pour de nombreux ordinateurs domestiques ou petits serveurs. Si vous avez, par exemple, un volume de données en évolution constante comme par exemple pour les bases de données, les archives MP3 ou les répertoires d'utilisateurs, etc., il faut alors envisager d'utiliser un gestionnaire de volumes logiques. Il est alors par exemple possible d'avoir des systèmes de fichiers qui sont plus gros qu'un disque dur physique. Un autre avantage du gestionnaire de volumes logiques est que vous pouvez créer jusqu'à 256 volumes logiques. Faites attention cependant car le travail avec le gestionnaire de volumes logiques est différent de celui avec des partitions classiques.

Vous trouverez des instructions et des informations complémentaires sur la configuration du "gestionnaire de volumes logiques" (LVM) dans le document officiel LVM-Howto `http://tldp.org/HOWTO/LVM-HOWTO/`.

3.10.2 Configuration du gestionnaire de volumes logiques avec YaST

Pendant l'installation, pendant que vous créez une partition LVM, YaST prépare la configuration du gestionnaire de volumes logiques.Vous devez pour cela cliquer sur 'Partitionnement' dans l'écran des propositions, puis dans la fenêtre suivante sur 'Annuler' ou 'Modifier'. Vous devez ensuite créer une partition pour le gestionnaire de volumes logiques. Pour cela, choisissez 'Créer' → 'Ne pas formater' dans le programme de partitionnement puis le type '0x8e Linux LVM'. Vous pourrez procéder à la suite du partitionnement avec le gestionnaire de volumes logiques directement à la suite ou alors plus tard dans le système installé en sélectionnant la partition LVM dans le programme de partitionnement, puis en cliquant sur 'LVM...'.

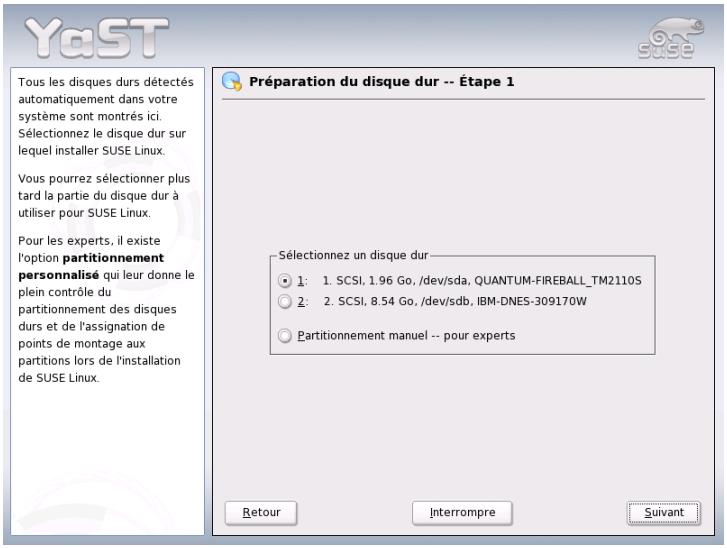


FIG. 3.9: *YaST : activer le gestionnaire de volumes logiques pendant l'installation*

3.10.3 LVM – Programme de partitionnement

Une fois que vous avez choisi 'LVM...' sous partitionner, une boîte de dialogue dans laquelle vous pouvez modifier le partitionnement de vos disques durs s'affiche. Utilisez-la pour supprimer ou modifier des partitions existantes et en créer de nouvelles. Une partition qui doit être utilisée pour le gestionnaire de volumes logiques doit avoir comme type de partition 8E. Ces partitions sont désignées par le texte "Linux LVM" dans la liste des partitions affichée dans la fenêtre (voir la dernière section).

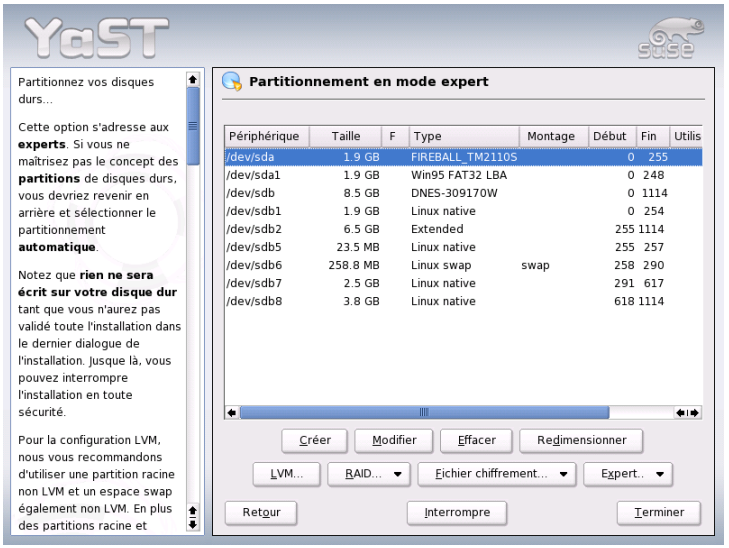


FIG. 3.10: *YaST : programme de partitionnement du gestionnaire de volumes logiques*

Remarque

Modification des partitions de volumes logiques

Au début des volumes physiques, des informations relatives au volume sont toujours inscrites dans la partition. Ainsi, un volume physique "sait" à quel groupe de volumes il appartient. Si vous souhaitez réaliser un nouveau partitionnement, nous vous recommandons de supprimer le début de ce volume. Dans le cas d'un groupe de volumes "system" et d'un volume physique "/dev/sda2", vous pouvez le faire par exemple avec la commande `dd if=/dev/zero of=/dev/sda2 bs=512 count=1`.

Remarque

Il n'est pas nécessaire d'attribuer à toutes les partitions prévues pour le gestionnaire de volumes logiques, une à une, l'identificateur de partition `8E`. YaST règle si nécessaire automatiquement à `8E` le type d'une partition attribuée à un groupe de volumes du gestionnaire de volumes logiques. Si vos disques contiennent des domaines non partitionnés, vous devez créer pour tous ces domaines des partitions LVM. Attribuez-leur alors immédiatement le type de partition `8E`. Vous n'avez pas besoin de les formater et vous ne pouvez enregistrer aucun point de montage pour ces dernières.

Si vous avez déjà sur votre système une configuration de gestionnaire de volumes logiques valide, celle-ci est automatiquement activée lors du début de la configuration du gestionnaire de volumes logiques. Si cette activation est réussie, le partitionnement de tous les disques contenant une partition appartenant à un groupe de volumes activé ne peut plus être modifié. Le noyau refuse de lire le partitionnement modifié d'un disque dur tant qu'une seule partition de ce disque est utilisée.

Vous pouvez naturellement, sans aucun problème, procéder à une modification du partitionnement de disques qui n'appartiennent pas à un groupe de volumes du gestionnaire de volumes logiques. Si vous avez déjà sur votre système une configuration du gestionnaire de volumes logiques valide, une modification du partitionnement n'est normalement pas possible. Vous devez à présent configurer sur ce formulaire tous les points de montage qui ne reposent pas sur des volumes logiques du gestionnaire de volumes logiques. Le système de fichiers racine au moins doit, dans YaST, se trouver sur une partition normale. Sélectionnez cette partition dans la liste et définissez la en tant que système de fichiers racine en cliquant sur le bouton 'Modifier'.

Nous vous conseillons, du fait de la grande flexibilité du gestionnaire de volumes logiques, de placer tous les autres systèmes de fichiers sur des volumes logiques du gestionnaire de volumes logiques. Une fois la partition racine définie, vous pouvez quitter cette boîte de dialogue.

3.10.4 LVM – Organisation des volumes physiques

Utilisez la boîte de dialogue 'LVM' pour gérer les groupes de volumes (souvent abrégés "VG") du gestionnaire de volumes logiques. S'il n'existe encore aucun groupe de volumes sur votre système, une fenêtre vous demandant d'en créer un s'affiche. Nous vous recommandons de choisir `system` comme nom du groupe de volumes sur lequel les fichiers du système SUSE LINUX se trouvent.

La *Physical Extent Size*, taille de l'étendue physique (souvent abrégée par PE-Size), précise la taille maximale d'un volume physique et logique dans ce groupe de volumes. Cette valeur est normalement fixée à 4 mégaoctets. Cela autorise une taille maximale pour un volume physique et logique de 256 gigaoctets. N'augmentez donc cette taille de l'étendue physique (par exemple à 8, 16 ou 32 mégaoctets) que si vous avez besoin de volumes logiques de plus de 256 gigaoctets.

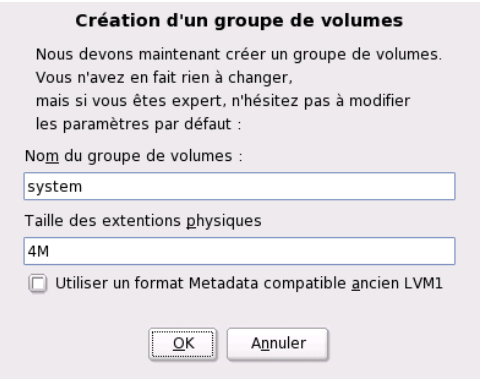


FIG. *3.11:* *YaST : créer un groupe de volumes*

La boîte de dialogue suivante donne la liste de toutes les partitions qui possèdent le type "Linux LVM" ou "Linux native". Aucune partition d'échange ou DOS n'est affichée. Si une partition est déjà attribuée à un groupe de volumes, c'est le nom du groupe de volumes qui est affiché dans la liste. Les partitions non attribuées sont identifiées par "--".

Le groupe de volumes actuellement utilisé peut être modifié dans la zone de sélection en haut à gauche. Utilisez les boutons en haut à droite pour ajouter des groupes de volumes supplémentaires et supprimer des groupes de volumes existants. Vous ne pouvez cependant supprimer que les groupes de volumes auxquels plus aucune partition n'est attribuée. Pour un système SUSE LINUX installé normal, vous n'avez pas besoin de créer plus d'un groupe de volumes. Une partition attribuée à un groupe de volumes est également appelée volume physique (*Physical Volume*, PV).

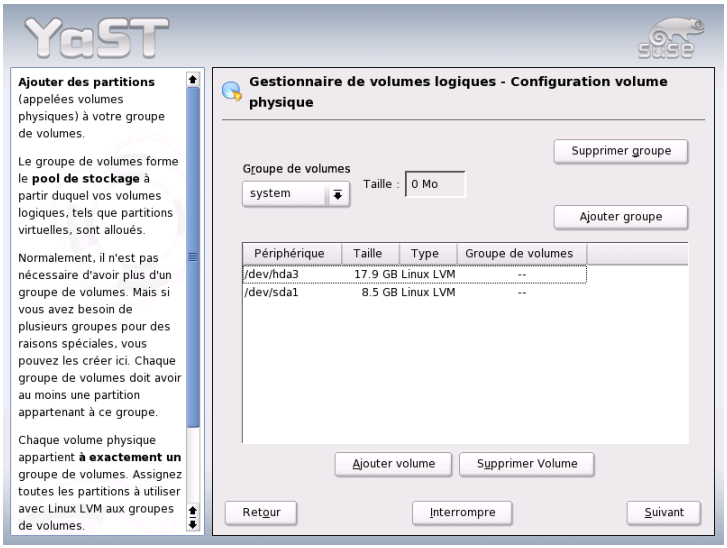


FIG. 3.12: *YaST : vue d'ensemble sur les partitions*

Pour ajouter dans le groupe de volumes de votre choix une partition jusqu'alors non attribuée, sélectionnez d'abord la partition, puis cliquez sur le bouton 'Ajouter volume' sous la liste de sélection. Le nom du groupe de volumes est alors placé à côté de la partition sélectionnée. Nous vous conseillons d'attribuer toutes les partitions que vous envisagez d'utiliser pour le gestionnaire de volumes logiques à un groupe de volumes sans quoi l'espace de la partition reste inutilisé. Avant de pouvoir quitter la boîte de dialogue, un volume physique au moins doit être attribué à chaque groupe de volumes.

3.10.5 Volumes logiques

C'est dans cette boîte de dialogue que sont gérés les volumes logiques (souvent abrégés par "LV").

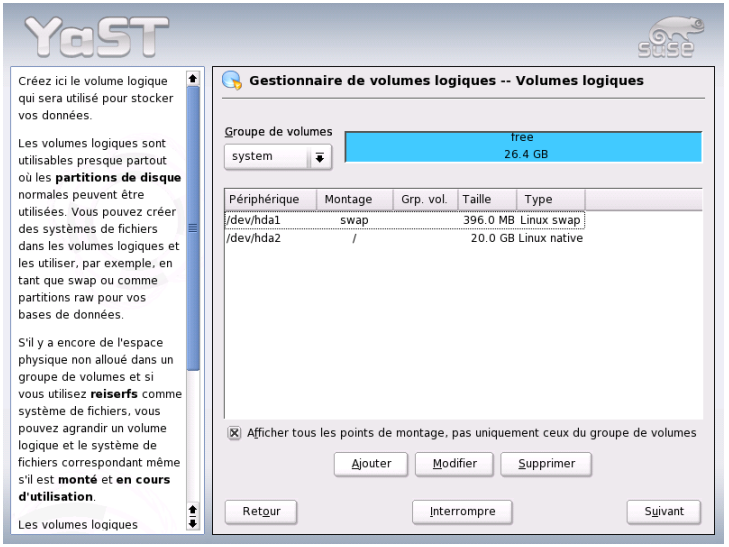


FIG. 3.13: *YaST : gestion des volumes logiques*

Chaque volume logique est attribué à un groupe de volumes et possède une taille donnée. Si, lors de la création des volumes logiques, vous souhaitez créer une matrice entrelacée de disques RAID (*striping array*), vous devez créer le volume logique contenant le plus de lacets (*stripes*) comme étant le premier. Un volume

logique monté en RAID avec n lacets ne peut alors être correctement créé que si l'espace sur le disque utilisé par le volume logique peut encore être réparti de manière uniforme sur n volumes physiques. Si vous ne disposez que de deux volumes physiques, un volume logique avec trois lacets n'est bien entendu pas possible.

Normalement, un système de fichiers (par exemple reiserfs, ext2) est créé sur un volume logique, puis un point de montage lui est attribué. Vous trouvez ensuite sous ce point de montage les fichiers du système installé qui sont enregistrés sur ce volume logique. La liste contient toutes les partitions Linux normales auxquelles un point de montage est attribué, toutes les partitions d'échange et tous les volumes logiques existants.

Attention

L'utilisation du gestionnaire de volumes logiques implique, le cas échéant, une augmentation des risques tels que par exemple la perte de données. Parmi les éventuels dangers, on note les plantages de programmes, les pannes de courant ou les commandes erronées. N'oubliez pas de sauvegarder vos données avant d'installer le gestionnaire de volumes logiques ou de modifier la configuration de volumes – ne travaillez jamais sans sauvegarde !

Attention

Si vous aviez déjà configuré LVM sur votre système, les volumes logiques existants apparaissent ici. Vous devez toutefois encore attribuer à ces volumes logiques le point de montage approprié. Si c'est la première fois que vous configurez le gestionnaire de volumes logiques sur un système, il n'existe dans ce formulaire encore aucun volume logique et vous devez créer pour chaque point de montage un volume logique (avec le bouton 'Ajouter') et définir sa taille, son type de système de fichiers (par exemple reiserfs ou ext2) et le point de montage (par exemple `/var`, `/usr`, `/home`).

Si vous avez créé plusieurs groupes de volumes, vous pouvez changer de groupe de volumes dans la liste de choix en haut à gauche. Les volumes logiques créés se trouvent à chaque fois dans le groupe de volumes affiché en haut à gauche. Si vous avez bien créé tous les volumes logiques tels que vous en aviez besoin, la configuration du gestionnaire de volumes logiques est terminée. Vous pouvez quitter la boîte de dialogue et continuer le choix de logiciels si vous vous trouvez dans le processus d'installation.

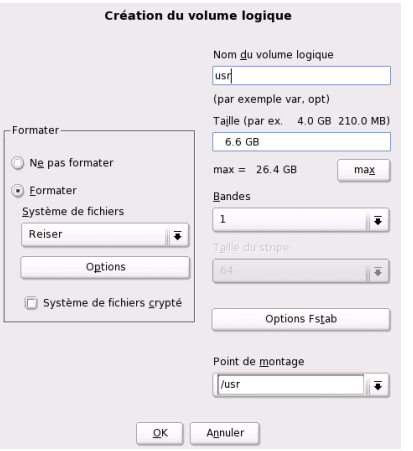


FIG. *3.14:* *YaST : créer des volumes logiques*

3.11 RAID logiciel

La technologie RAID (de l'anglais *Redundant Array of Independent Disks*) repose sur l'idée de rassembler plusieurs partitions de disque dur en un seul gros disque "virtuel" afin d'optimiser les performances et la sûreté des données, chacune de ces exigences étant exclusive de l'autre. Le "niveau RAID" (*RAID-Level*) définit la façon de combiner et de commander ensemble des disques durs offerte par un contrôleur RAID.

Un contrôleur RAID utilise généralement le protocole SCSI, qui permet de mieux contrôler un plus grand nombre de disques durs que le protocole IDE et qui se prête mieux au traitement des commandes en parallèle. Entre-temps, il existe également des contrôleurs RAID qui fonctionnent avec des disques durs IDE ou SATA. À ce sujet, consultez également la base de données matériel sous `http://cdb.suse.de`.

Le contrôleur RAID, qui peut être un équipement très coûteux, peut être avantageusement remplacé par le RAID logiciel, qui est capable de remplir les mêmes fonctions. SUSE LINUX vous offre la possibilité, en utilisant YaST, de combiner plusieurs disques durs en un système RAID logiciel – ce qui constitue une alternative très avantageuse au RAID matériel.

3.11.1 Niveaux RAID courants

RAID 0 Ce niveau améliore les performances de vos accès aux données. Il ne s'agit pas, à proprement parler, de RAID véritable, en raison de l'absence de sécurisation des données. Malgré cela, le terme "RAID 0" est entré dans l'usage. Le "RAID 0" combine au moins deux disques durs. Les performances sont très bonnes – mais il suffit qu'un seul des disques, quel qu'en soit le nombre, soit défaillant pour que le système RAID soit détruit, entraînant la perte de vos données.

RAID 1 Ce niveau offre une sûreté des données satisfaisante, celles-ci étant copiées dans un rapport 1:1 sur une autre disque dur, selon la technique de "mise en miroir de disques durs". Dans le cas où un disque viendrait à être détruit, une copie de son contenu se trouve sur un autre disque. Tous les disques sauf un peuvent donc être défectueux sans risque de perte de données. Les performances en écriture diminuent quelque peu avec l'utilisation du niveau RAID 1 (on constate un ralentissement de l'ordre de 10 à 20 %). En contrepartie, les performances en lecture représentent une nette amélioration par rapport à l'utilisation d'un unique disque dur physique normal. En effet, les données sont dupliquées et peuvent donc être lues en parallèle.

RAID 5 Le niveau RAID 5 est un compromis optimal entre les deux autres niveaux, concernant la redondance et les performances. L'espace disque disponible correspond au nombre de disques utilisés moins un. Comme dans le niveau RAID 0, les données sont réparties entre les disques. La sécurisation des données est dévolue à des "blocs de parité" qui, pour le RAID 5, sont créés sur l'une des partitions. Ceux-ci sont combinés par l'opération XOR – ce qui permet, en cas de défaillance d'une partition, d'utiliser le bloc de parité correspondant pour reconstituer le contenu avec l'aide de l'opération logique XOR. Le RAID 5 ne permet pas d'avoir plus d'un disque dur défaillant à la fois. Dès qu'un disque dur est hors service, il doit être remplacé le plus vite possible afin de ne pas perdre les données.

3.11.2 Configuration du RAID logiciel avec YaST

La configuration du RAID logiciel est accessible soit depuis un module 'RAID' indépendant à la rubrique 'Système' soit depuis le module de partitionnement à la rubrique 'Matériel'.

1ère étape : Partitionnement Le menu 'Partitionnement en mode expert' dans l'outil de Partitionnement énumère vos partitions. Vous voyez ici les partitions RAID logiciel que vous avez créées. Dans le cas contraire, vous devez en créer de nouvelles. Les niveaux RAID 0 et RAID 1 requièrent au moins deux partitions – elles sont normalement au nombre de deux exactement pour le RAID 1. En revanche, le RAID 5 requiert au moins trois partitions. Il est recommandé de n'utiliser que des partitions de taille identique.

Les différentes partitions d'un RAID doivent être installées sur différents disques durs afin de parer au risque de perte de données dû à la défaillance d'un disque dur en RAID 1 et 5 et pour optimiser les performances en RAID 0.

2ème étape : Création d'un disque RAID

Lorsque vous cliquez sur 'RAID', une boîte de dialogue apparaît, à partir de laquelle vous êtes invité à choisir le niveau RAID 0, 1 ou 5. L'écran suivant vous propose d'associer les partitions au nouveau RAID. Les options de paramétrage correspondant à la taille de bloc ("chunk size") sont accessibles depuis les 'Options en mode expert' – vous pouvez procéder à des réglages fins pour les performances. Lorsque la case 'superblock permanent' est cochée, les partitions RAID seront reconnues en tant que telles juste après le démarrage de l'ordinateur.

Lorsque la configuration est achevée, vous voyez sur l'écran "Partitionnement en mode expert" le périphérique `/dev/md0` (etc.) assorti de l'identifiant "RAID".

Dépannage Pour savoir si une partition RAID est abîmée, examinez le contenu du fichier `/proc/mdstats`. La procédure à suivre lorsqu'un dysfonctionnement s'est produit,est d'arrêter votre système Linux et de remplacer le disque défectueux par un nouveau disque partitionné de manière identique. Redémarrez ensuite votre système et exécutez la commande `raidhotadd /dev/mdX /dev/sdX`. Le nouveau disque dur est alors automatiquement intégré au système RAID et est restauré de manière totalement transparente.

Vous trouverez dans le Howto indiqué ci-après la marche à suivre pour configurer le RAID logiciel, ainsi que différents détails supplémentaires :

- `/usr/share/doc/packages/raidtools/Software-RAID-HOWTO.html`
- `http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html`

ou dans la liste de diffusion Linux RAID disponible par exemple à l'adresse

- `http://www.mail-archive.com/linux-raid@vger.rutgers.edu`

Vous y trouverez également de l'aide dans le cas où vous rencontreriez des problèmes complexes inattendus.

Mise à jour du système et gestion des paquetages

SUSE LINUX offre la possibilité d'actualiser un système existant sans nouvelle installation. Cependant, il faut faire une distinction entre l'*actualisation de divers paquetages logiciels* et une *mise à jour de l'ensemble du système*.

Vous pouvez aussi installer divers paquetages à la main avec le gestionnaire de paquetages rpm.

4.1 Actualiser SUSE LINUX

Il est bien connu que les logiciels progressent d'une version à l'autre. Par conséquent, il convient de vérifier avec `df` la capacité maximale des différentes partitions *avant* la mise à jour. Si vous estimez qu'elle risque d'être limitée, faites alors une sauvegarde de vos données avant la mise à jour et partitionnez le système à nouveau. Il n'est pas possible de donner à chacun des informations générales détaillées sur la quantité d'espace nécessaire – l'espace requis dépend du type de partitionnement existant, des logiciels choisis et du numéro de version du système existant sur la distribution SUSE LINUX actuelle.

Remarque

Nous ne saurions trop vous recommander de lire sur le CD le fichier `LISEZMOI` ou `README` ou sous DOS/Windows, le fichier `LISEZMOI.DOS` (`README.DOS`) ; vous y trouverez mentionnées toutes les modifications supplémentaires qui ont eu lieu *après* l'impression de ce manuel.

Remarque

4.1.1 Préparatifs

Avant le début d'une mise à jour, il est plus sûr de copier les anciens fichiers de configuration sur un support séparé (dévideur à bande ou *streamer*, disque amovible, lecteur de disques ZIP, CD-ROM, etc.). Il s'agit principalement des fichiers enregistrés dans `/etc` ; les répertoires et fichiers présents dans `/var` et dans `/opt` sont également à contrôler et éventuellement à sauvegarder. En outre, il n'est pas inutile de sauvegarder les données actuelles des utilisateurs contenues dans `/home` (les répertoires personnels contenus dans `HOME`) sur un support tiers. La sauvegarde des données ne peut se faire qu'en tant qu'administrateur système ; seul dispose des droits permettant de lire tous les fichiers locaux. Avant de commencer la procédure de mise à jour, notez l'emplacement de la partition racine ; la commande `df /` vous permet de connaître le nom du périphérique abritant la partition racine ; dans le cas présenté 4.1 page ci-contre, l'emplacement à noter de partition racine est `/dev/hda2`.

Exemple 4.1: *Aperçu avec df -h*

```
Sys. de fich. Tail. Occ. Disp. %Occ. Monté sur
/dev/hda1     1,9G  189M  1,7G  10% /dos
/dev/hda2     8,9G  7,1G  1,4G  84% /
/dev/hda5     9,5G  8,3G  829M  92% /home
```

L'affichage montre que la partition `/dev/hda2` est rattachée au système de fichiers (montée) à l'emplacement `/`

4.1.2 Problèmes possibles

Contrôler passwd et group dans /etc

Avant la mise à jour, assurez-vous que `/etc/passwd` et `/etc/group` ne comportent pas d'erreur de syntaxe. À cette fin, exécutez les programmes de vérification `pwck` et `grpck` en tant que `root` et corrigez les erreurs qui ont été signalées.

PostgreSQL

Avant une mise à jour de PostgreSQL (`postgres`) , il est généralement recommandé d'exporter (*dump*) les données des bases ; reportez-vous à `pg_dump`. Cette opération n'est bien sûr nécessaire que si vous avez effectivement utilisé PostgreSQL avant la mise à jour.

4.1.3 mise à jour avec YaST

Après les travaux préliminaires décrits dans la section *Préparatifs* page précédente, vous voici arrivé à la procédure d'amorçage.

1. Démarrez le système comme pour une installation (reportez-vous au guide de l'utilisateur) puis dans YaST — après avoir défini la langue — *ne* choisissez *pas* 'Nouvelle installation', mais 'Mise à jour d'un système existant'.
2. YaST déterminera s'il existe plus d'une partition racine ; si ce n'est pas le cas, il continue avec la sauvegarde du système. S'il existe plusieurs partitions, choisissez celle qui convient et confirmez par 'Suivant' (dans l'exemple de la section *Préparatifs* page ci-contre, vous aviez noté `/dev/hda2`).
   YaST lira l'ancien fichier `fstab` présent sur cette partition pour ensuite analyser les systèmes de fichiers qui y sont répertoriés et enfin les monter.

3. Vous avez alors la possibilité de créer une copie de sauvegarde des fichiers système pendant la mise à jour. Cette option ralentit la procédure de mise à jour, mais vous devriez la choisir si vous n'avez actuellement pas de sauvegarde système.
4. La boîte de dialogue suivante permet de définir soit que seuls les logiciels déjà installés seront actualisés, soit que de nouveaux composants logiciels importants seront ajoutés au système (Mode de mise à jour). Il est recommandé d'accepter le choix proposé ('Système par défaut'). Vous pourrez éliminer plus tard d'éventuelles imprécisions avec YaST.

Si vous avez des difficultés avec la reconnaissance automatique du matériel de YaST, vous pouvez également initialiser la mise à jour à l'aide de linuxrc. Consultez, à ce sujet, la section *linuxrc* page 116.

4.1.4 Actualisation de divers paquetages

Indépendamment d'une mise à jour totale, vous pouvez actualiser à tout moment les différents paquetages ; vous devez toutefois veiller *vous-même* à ce que le système reste cohérent : vous trouverez des recommandations de mise à jour répertoriées à l'adresse `http://www.suse.com/us/private/download/updates/` (en anglais).

Dans le menu de sélection de paquetages de YaST, vous pouvez faire ce que bon vous semble. Si vous choisissez de mettre à jour un paquetage qui joue un rôle fondamental dans le fonctionnement du système, YaST vous en avertit. Les paquetages de ce type devraient être actualisés avec le mode spécial de mise à jour. Quelques paquetages contiennent par exemple des bibliothèques partagées, potentiellement utilisées au moment de la mise à jour de processus en cours d'exécution. Une mise à jour dans le système actuel amènerait donc ces programmes à ne plus pouvoir fonctionner correctement.

4.2 Modifications des logiciels d'une version à l'autre

Les sections suivantes dressent la liste des détails qui ont changé d'une version à l'autre. Cet aperçu montre si des configurations ont été modifiées, si des fichiers de configuration ont été déplacés, ou encore si des applications connues ont été

modifiées de façon perceptible. Il ne sera traité que des aspects qui affectent directement l'utilisateur ou l'administrateur dans leur travail quotidien.

Les problèmes et les particularités de chaque version sont publiés sur le serveur Web : reportez-vous aux liens ci-dessous. On peut accéder aux mises à jour importantes des différents paquetages à l'adresse `http://www.suse.com/us/private/download/updates/` (en anglais).

4.2.1 De la version 8.0 à la version 8.1

Problèmes et particularités : `http://portal.suse.com/sdb/en/2002/10/bugs81.html` (en anglais).

- Modifications concernant les noms d'utilisateurs et de groupes du système : pour se mettre en conformité avec UnitedLinux, quelques éléments ont été adaptés dans `/etc/passwd` et/ou `/etc/group`.
  - Utilisateurs modifiés : `ftp` dorénavant dans le groupe `ftp` (et non plus dans `daemon`).
  - Groupes renommés : `www` (il s'agissait de `wwwadmin`) ; `games` (il s'agissait de `game`).
  - Nouveaux groupes : `ftp` (avec le GID `50`) ; `floppy` (avec le GID `19`) ; `cdrom` (avec le GID `20`) ; `console` (avec le GID `21`) ; `utmp` (avec le GID `22`).
- Modifications en rapport avec le FHS (reportez-vous à la section *Standards et spécifications* page 727) :
  - Un exemple d'environnement pour HTTPD (Apache) se trouve dans `/srv/www` (il s'agissait de `/usr/local/httpd`).
  - Un exemple d'environnement pour FTP se trouve dans `/srv/ftp` (il s'agissait de `/usr/local/ftp`). Le paquetage `ftpdir` est nécessaire pour celui-ci.
- Pour permettre un accès ciblé au logiciel recherché , les divers paquetages ne sont plus regroupés en un petit nombre de séries peu claires, mais par groupes RPM portant des noms évocateurs. En conséquence, il n'existe plus sur les CDs de répertoire abscons dans `suse`, mais quelques répertoires nommés d'après des architectures comme `ppc`, `i586` ou `noarch`.
- Lors d'une nouvelle installation, les programmes suivants ne sont désormais plus configurés ou installés automatiquement :
  - Le chargeur d'amorçage GRUB qui offre incontestablement plus de possibilités que LILO. LILO reste toutefois en place lors de la *mise à jour* du système.
  - Le logiciel de messagerie postfix à la place de sendmail.
  - Le logiciel de gestion de listes de discussion mailman est installé à la place de majordomo.

- ▷ Choisissez à la main harden_suse si nécessaire et lisez la documentation actuelle le concernant !

- Paquetages répartis : `rpm` dans `rpm` et `rpm-devel` ; `popt` dans `popt` et `popt-devel` ; `libz` dans `zlib` et `zlib-devel`.
  `yast2-trans-*` est désormais distribué en fonction des langues : `yast2-trans-cs` (tchèque), `yast2-trans-de` (allemand), `yast2-trans-es` (espagnol) ; lors de l'installation, toutes les langues ne sont plus installées pour économiser de l'espace disque. Faites une installation ultérieure des paquetages nécessaires pour que YaST prenne en charge d'autres langues !
- Paquetages renommés : `bzip` en `bzip2`.
- Paquetages obsolètes : `openldap`, utilisez à présent `openldap2` ; `su1`, passez dorénavant à `sudo`.

4.2.2 De la version 8.1 à la version 8.2

Problèmes et particularités : `http://portal.suse.com/sdb/en/2003/04/bugs82.html` (en anglais).

- Prise en charge 3D des cartes graphiques de type nVidia (modifications) : les paquetages `NVIDIA_GLX/NVIDIA_kernel` (y compris le script `switch2nvidia_glx`) ne sont plus fournis. Téléchargez le programme d'installation nVidia pour `Linux IA32` sur la page web de nVidia (`http://www.nvidia.com`), utilisez-le pour installer le pilote, puis faites appel à SaX2 ou à YaST pour activer la prise en charge de la 3D.
- Lors d'une nouvelle installation, le démon xinetd est installé à la place du démon inetd et configuré dans des conditions sûres reportez-vous au répertoire `/etc/xinetd.d`). Le démon inetd reste néanmoins en place lors d'une mise à jour du système.
- PostgreSQL est à présent disponible dans la version 7.3. Un dump/restore (export/import des données) avec `pg_dump` est requis pour une mise à jour depuis une version 7.2.x. Lorsque votre application interroge les catalogues système, d'autres adaptations sont alors nécessaires, puisque la version 7.3 a introduit des schémas. Vous trouverez des informations complémentaires à l'adresse : `http://www.ca.postgresql.org/docs/momjian/upgrade_tips_7.3` (en anglais).

- La version 4 de stunnel ne gère plus aucune option en ligne de commande. Le script `/usr/sbin/stunnel3_wrapper` qui est en mesure de convertir les options de ligne de commande dans un fichier de configuration approprié pour stunnel est néanmoins fourni et doit être utilisé à la demande (à la place d'`OPTIONS`, utilisez les vôtres) :

  ```
  /usr/sbin/stunnel3_wrapper stunnel OPTIONS
  ```

  Le fichier de configuration produit est aussi affiché sur la sortie par défaut, de sorte que vous pouvez utiliser aisément ces indications pour générer un fichier de configuration permanent pour l'avenir.
- openjade (`openjade`) est maintenant le moteur DSSSL qui remplace jade (`jade_dsl`) lorsqu'on appelle db2x.sh (`docbook-toys`). Pour des raisons de compatibilité, les divers programmes sont également mis à disposition sans le préfixe `o`.
  Si des applications particulières dépendent du répertoire `jade_dsl` et des fichiers qui y sont actuellement installés, il faut soit reconfigurer les applications en question pour prendre en compte le nouveau répertoire `/usr/share/sgml/openjade`, soit créer un lien en tant que :

  ```
  cd /usr/share/sgml rm jade_dsl ln -s openjade jade_dsl
  ```

  Pour éviter un conflit avec le `rzsz`, l'outil en ligne de commande `sx` appelle en outre `s2x` et/ou `sgml2xml` ou `osx`.

4.2.3 De la version 8.2 à la version 9.0

Problèmes et particularités : `http://sdb.suse.de/sdb/de/html/bugs90.html`.

- Les services de maintenance périodiques dans `/etc/cron.daily`, `/etc/cron.weekly` et `/etc/cron.monthly` sont exécutés aux environs de 4 heures du matin. Ces horaires ne sont valables que pour les nouvelles installations ; après une mise à jour, il convient d'adapter `/etc/crontab`.
- Le gestionnaire de paquetages RPM est actuellement disponible en version 4. La fonctionnalité prévue pour la compilation des paquetages est désormais transférée dans le programme autonome `rpmbuild` ; il faut toujours utiliser `rpm` pour installer, actualiser et interroger la base de données ; reportez-vous à la section *RPM – Le gestionnaire de paquetages de la distribution* page 174.

- Dans l'espace *Impression*, on trouve le paquetage `footmatic-filters`. Son contenu a été séparé du paquetage `cups-drivers` car il est apparu qu'on peut imprimer avec, même si CUPS n'est pas installé. On peut donc ainsi peaufiner des configurations avec YaST qui sont indépendantes du système d'impression (CUPS, LPRng). En tant que fichier de configuration, ce paquetage contient le fichier `/etc/foomatic/filter.conf`.
- Désormais, les paquetages `footmatic-filters` et `cups-drivers` sont également requis pour la mise en œuvre des programmes LPRng/lpdfilter.
- Les ressources XML des paquetages logiciels fournis sont rendus accessibles grâce à des déclarations contenues dans `/etc/xml/suse-catalog.xml`. Ce fichier ne peut pas être traité avec `xmlcatalog` car sinon, des commentaires d'organisation nécessaires pour garantir une mise à jour en bonne et due forme disparaissent. `/etc/xml/suse-catalog.xml` est rendu accessible au moyen d'une instruction `nextCatalog`, de sorte que des outils XML comme `xmllint` ou `xsltproc` peuvent trouver automatiquement les ressources locales.

4.2.4 De la version 9.0 à la version 9.1

Problèmes et particularités : `http://sdb.suse.de/sdb/de/html/bugs91.html`.

Migration vers le noyau 2.6

SUSE LINUX a été complètement migrée vers le noyau version 2.6 ; vous ne devriez plus utiliser la version précédente 2.4, car les programmes ne fonctionneront probablement plus. Vous trouverez ci-dessous quelques détails à prendre en compte :

- Les modules ne sont chargés et configurés qu'à partir du fichier `/etc/modprobe.conf` ; le fichier `/etc/modules.conf` est obsolète. YaST essaiera de convertir les données (voir aussi le script `/sbin/generate-modprobe.conf`).
- Les modules ont désormais le suffixe `.ko`.
- Le module `ide-scsi` n'est plus nécessaire à la gravure des CD.
- Dans les options du module son ALSA, le préfixe `snd_` a été supprimé.
- `sysfs` complète désormais le système de fichiers `/proc`.
- La gestion de l'énergie (en particulier l'ACPI) a été améliorée et peut désormais être configurée *via* un module de YaST.

Codepage et montage de partitions VFAT

Lors du montage de partitions VFAT, le paramètre `code=` dans `codepage=` doit être modifié. Si le montage d'une partition VFAT pose problème, vérifiez si le fichier `/etc/fstab` contient les anciens noms de paramètres.

Veille/attente (standby/suspend) avec ACPI

Avec le nouveau noyau 2.6 les modes veille/attente de ACPI sont supportés. Veuillez noter que ces fonctions en sont encore au stage expérimental et ne sont pas encore supportés par tous les matériels. Pour bénéficier de cette fonctionnalité, vous nécessitez le paquetage `powersave`. Vous trouverez plus d'informations relatives à ce paquetage sous `/usr/share/doc/packages/powersave`. Vous trouverez un frontal graphique dans le paquetage `kpowersave`.

Périphériques d'entrée (Input Devices)

Concernant les changements des périphériques d'entrée (*Input Devices*), reportez-vous à l'article susnommé du portail (`http://portal.suse.de/sdb/en/2004/02/bugs91.html`).

Native POSIX Thread Library et glibc 2.3.x

Les programmes liés à NGPT (*Next Generation POSIX Threading*) ne fonctionnent pas avec la glibc 2.3.x. Tous les programmes de ce type qui ne fonctionnent pas sous SUSE LINUX doivent être recompilés avec linuxthreads ou avec NPTL (Native POSIX Thread Library). Il est préférable d'utiliser NPTL pour le portage pour plus de pérennité vis-à-vis des standards futurs.

En cas de difficulté avec NPTL, il est possible d'utiliser linuxthreads, plus ancien, si la variable suivante est modifiée (dans laquelle ⟨*kernel-version*⟩ doit être remplacée par le numéro de version du noyau correspondant) :

```
LD_ASSUME_KERNEL=kernel-version
```

Les numéros de version suivants sont possibles :

2.2.5 (i386, i586): linuxthreads sans piles flottantes (*Floating Stacks*)

2.4.1 (AMD64, i586, i686) : linuxthread avec piles flottantes

Remarque à propos du noyau et de linuxthreads *avec* piles flottantes :

Les programmes qui utilisent `errno`, `h_errno` et `_res` doivent inclure les fichiers d'en-têtes correspondant (`errno.h`, `netdb.h` et/ou `resolv.h`) avec `#include`. Les programmes C++ qui mettent en oeuvre plusieurs fils d'exécution (*multithread*) et qui utilisent l'*annulation de fil d'exécution* (*thread cancellation*) doivent accéder à la variable d'environnement `LD_ASSUME_KERNEL=2.4.1` pour utiliser la bibliothèque linuxthreads.

Adaptations pour Native POSIX Thread Library

NPTL (*Native POSIX Thread Library*) est disponible dans SUSE LINUX 9.1 en tant que paquetage de gestion de fils de d'exécution. NPTL a été développé de manière à conserver une compatibilité binaire avec l'ancienne bibliothèque linuxthreads. Cependant, aux endroits auxquels linuxthreads enfreint la norme POSIX, NPTL a nécessité des adaptations ; il faut en particulier nommer : la gestion des signaux ; `getpid` renvoie pour tous les fils d'exécurtion la même valeur ; les gestionnaires de fils d'exécutions qui enregistrent pthread_atfork ne fonctionnent pas lorsque `vfork` est utilisé.

Configuration des interfaces réseau

La configuration des interfaces réseau a changé. Jusqu'à présent, l'initialisation du matériel était démarrée après la configuration de l'interface maintenant, le nouveau matériel sera tout d'abord recherché et initialisé et ensuite l'interface réseau pourra être configurée.

De plus, de nouveaux noms ont été introduits pour les fichiers de configuration. Étant donné que le nom d'une interface réseau est générée dynamiquement et que le nombre de périphériques hotplug augmente sans arrêt, un nom tel que `eth`⟨*X*⟩ n'est plus adapté à la configuration. Pour cette raison, nous n'utilisons que des descriptions sans équivoque telles que l'adresse MAC ou le port PCI pour nommer les configurations des interfaces.

Conseil : vous pouvez, bien entendu, utiliser les noms des interfaces dès qu'ils apparaissent. Des commandes telles que `ifup eth0` ou `ifdown eth0` sont toujours possibles.

Les configurations des périphériques se trouvent dans `/etc/sysconfig/hardware`. Les interfaces mises à disposition par ces périphériques se trouvent comme à l'habitude (simplement avec des noms différents) dans `/etc/sysconfig/network`.

Vous trouverez une description détaillée sous `/usr/share/doc/packages/sysconfig/README`.

Configuration du son

Après une mise à jour, les cartes son doivent être reconfigurées. Cela peut se faire à l'aide du module son de YaST à cette fin, exécutez, en tant que `root`, la commande suivante : `yast2 sound`.

Domaine de premier niveau .local en tant que domaine link-local

La bibliothèque Resolver traite le domaine de premier niveau `.local` en tant que domaine "link-local" et envoie des requêtes DNS multidiffusion à l'adresse de multidiffusion `224.0.0.251` port `5353` au lieu de requêtes DNS normales ; ceci est une modification incompatible. Si le domaine `.local` est déjà utilisé dans la configuration du serveur de noms, il faut utiliser un autre nom de domaine. Vous trouverez plus d'informations relatives au DNS multidiffusion sous `http://www.multicastdns.org`.

Encodage UTF-8 pour tout le système

`UTF-8` est désormais l'encodage par défaut du système. Lors d'une installation standard, une localisation avec l'indication d'encodage (*Encoding*) `.UTF-8` est aussi accessible (`fr_FR.UTF-8`). Vous trouverez plus d'informations sous `http://www.suse.de/~mfabian/suse-cjk/locales.html`.

Noms de fichiers après la conversion UTF-8

Les fichiers dans les systèmes de fichiers qui ont été créés auparavant n'utilisent pas d'encodage UTF-8 (tant que rien d'autre n'est précisé) pour les noms de fichiers. Si ces fichiers contiennent d'autres caractères que les caractères ASCII, ils apparaîtront "bizarrement". Pour éviter cela, le script `convmv` peut être utilisé ; il convertit l'encodage des noms de fichiers en UTF-8.

Outils Shell compatibles avec le standard POSIX de 2001

Les outils en mode interpréteur de commande provenant du paquetage `coreutils` comme `tail`, `chown`, `head`, `sort` suivent dorénavant le réglage par défaut de la norme POSIX de 2001 (*Single UNIX Specification, version 3 == IEEE Std 1003.1-2001 == ISO/IEC 9945:2002*) au détriment de la norme de 1992. Toutefois, l'ancien comportement peut être imposé avec une variable d'environnement :

```
_POSIX2_VERSION=199209
```

La nouvelle valeur est 200112 et est acceptée comme norme pour `_POSIX2_VERSION`. Vous pouvez lire le standard SUS ici (gratuit, mais une inscription est nécessaire) :

`http://www.unix.org`

Un bref comparatif :

TAB. *4.1:* *Comparatif POSIX 1992/POSIX 2001*

POSIX 1992	POSIX 2001
chown tux.users	chown tux:users
tail +3	tail -n +3
head -1	head -n 1
sort +3	sort -k +3
nice -10	nice -n 10
split -10	split -l 10

Remarque

Les logiciels provenant d'une tierce partie ne suivent probablement pas encore le nouveau standard ; dans ce cas il est conseillé de mettre la variable d'environnement comme décrit ci-dessus à la valeur `_POSIX2_VERSION=199209`.

Remarque

/etc/gshadow obsolète

`/etc/gshadow` a été abandonné et supprimé car ses données sont superflues pour les raisons suivantes :

- La glibc ne le prend pas en charge.
- Il n'existe pas d'interface officielle pour ces données, et il n'existe pas non plus d'interface dans la suite shadow.
- La plupart des outils qui vérifient les mots de passe de groupe ne s'appuient pas sur ce fichier et l'ignorent à cause des deux raisons précédemment énoncées.

OpenLDAP

- Étant donné que le format des bases a changé, les bases de données doivent être générées à nouveau. Lors de la mise à jour, cette conversion est effectuée automatiquement ; cependant, dans certains cas particuliers, la conversion échouera.
- Le schéma de vérification a été considérablement amélioré. Ainsi, certaines opérations (non conformes au standard) possibles avec la version précédente du serveur LDAP ne sont maintenant plus possibles.
- La syntaxe des fichiers de configuration a été partiellement modifiée par rapport aux ACL (listes de contrôle d'accès).

Vous trouverez plus d'informations relatives à la mise à jour dans le fichier `/usr/share/doc/packages/openldap2/README.update`

Apache 1.3 remplacé par Apache 2

Le serveur web Apache (version 1.3) a été remplacé par Apache 2. Une mise à jour d'un système avec installation d'un serveur HTTP effacera le paquetage Apache et installera Apache 2. Le système doit alors être modifié manuellement ou à l'aide de YaST. Les fichiers de configuration ne se trouvent plus maintenant sous `/etc/httpd` mais sous `/etc/apache2`.

Pour la façon de gérer simultanément plusieurs requêtes, on a le choix entre les fils d'exécution et les processus. Les processus sont gérés par un seul module appelé module de multi-traitement (*Multi-Processing-Modul* - MPM). Apache 2 utilise aussi un paquetage `apache2-prefork` (préféré pour la stabilité) ou `apache2-worker`. La réaction d'Apache 2 à ces requêtes est différente selon le MPM utilisé. Cela a principalement des conséquences sur les performances et sur l'utilisation des modules. Ces points seront discutés plus en détails dans le chapitre sur Apache *Les fils d'exécution (threads)* page 567.

Apache 2 reconnaît maintenant le protocole Internet IPv6 à venir.

Il existe désormais un mécanisme grâce auquel le développeur du module peut donner des indications sur l'ordre désiré de chargement du module pour que l'utilisateur n'ait plus à s'en préoccuper. L'ordre dans lequel les modules sont démarrés est souvent important et était auparavant déterminé par l'ordre de chargement. Un module qui n'autorise l'accès aux utilisateurs identifiés pour certaines ressources doit ainsi être appelé en premier afin que l'utilisateur qui n'a pas de droit d'accès ne puisse en aucun cas être amené à voir la page.

Les requêtes et réponses d'Apache peuvent passer à travers un filtre.

De samba 2.x à samba 3.x

Avec la mise à jour de samba 2.x par samba 3.x, l'authentification `winbind` n'est plus disponible ; les autres méthodes sont toujours possibles. Pour cette raison, les programmes suivants ont été modifiés :

```
/usr/sbin/wb_auth
/usr/sbin/wb_ntlmauth
/usr/sbin/wb_info_group.pl
```

Voir aussi : `http://www.squid-cache.org/Doc/FAQ/FAQ-23.html#ss23.5`

Mise à jour de OpenSSH (version 3.8p1)

Le support `gssapi` a été remplacé par `gssapi-with-mic` afin d'éviter de possibles attaques MITM. Ces deux versions ne sont pas compatibles. Ceci signifie que vous ne pourrez pas vous authentifier depuis des distributions plus anciennes avec des tiquets Kerberos car d'autres méthodes d'authentification sont maintenant utilisées.

Applications SSH et terminal

Lors de l'accès depuis un ordinateur distant (surtout SSH, telnet et RSH) entre une version 9 (dans la configuration par défaut, avec UTF-8 activé) et un système plus ancien (SUSE LINUX 9.0 et versions précédentes, produits pour lesquels UTF-8 n'étaient pas supportés ou activés par défaut), les applications de terminal peuvent afficher des caractères erronés.

Cela vient du fait que OpenSSH ne transmet pas de paramètres locaux et les paramètres par défaut des systèmes sont donc utilisés alors qu'ils ne correspondent peut-être pas avec les paramètres du terminal distant. Ceci concerne YaST en mode textuel ainsi que des applications qui sont exécutées depuis un ordinateur distant en tant qu'utilisateur normal (pas `root`). Les application exécutées par `root` ne sont concernées que lorsque l'utilisateur a modifié les paramètres locaux pour `root` (uniquement `LC_CTYPE` est défini par défaut).

libiodbc a été rejeté

Les utilisateurs de FreeRADIUS doivent maintenant utiliser unixODBC car libiodbc a été rejeté.

Ressources XML dans /usr/share/xml

Le FHS (voir *Standards et spécifications* page 727) prévoit que les ressources XML (DTDs, feuilles de style, etc) soient installées dans `/usr/share/xml`. Pour cette raison, quelques répertoires ne se situent plus dans `/usr/share/sgml`. En cas de problème, vous devez modifier les scripts ou Makefiles y faisant référence, ou modifier les catalogues officiels (en particulier `/etc/xml/catalog` et/ou `/etc/sgml/catalog`).

Supports de données avec subfs

Les supports de données sont maintenant intégrés à l'aide de subfs. Maintenant, les supports de données amovibles ne doivent plus être montés (`mount`) manuellement. Il suffit de passer dans le répertoire correspondant sous `/media` pour monter le dispositif. Les supports de données ne peuvent pas être démontés tant qu'un programme y accède.

4.2.5 De la version 9.1 à la version 9.2

Reportez vous à l'article "Known Problems and Peculiarities in SuSE 9.2" (en anglais) dans la base de données d'assistance à l'adresse `http://portal.suse.com`, en recherchant le mot clé *Peculiarities*.

Pare-feu actif durant l'installation à partir de la boîte de dialogue de suggestion

SuSEFirewall2, la solution pare-feu fournie, est activée depuis la boîte de dialogue de suggestion vers la fin de l'installation pour accroître la sécurité. Cela veut ainsi dire qu'au début tous les ports sont fermés et qu'ils peuvent être ouverts à la demande à partir du début de la boîte de dialogue de suggestion.

Si lors de l'installation ou la configuration d'un service un accès au réseau est utilisé, le module YaST correspondant ouvre les ports TCP et UDP utilisés sur toutes les inerfaces internes et externes. Si cela n'est pas voulu, l'utilisateur peut fermer les ports dans le module YaST ou entreprendre une configuration détaillée du pare-feu.

TAB. 4.2: *Ports utilisés par les services importants*

Service	Ports
Serveur HTTP	Le pare-feu sera adapté grâce aux instructions "Listen" (uniquement pour TCP).
Courrier électronique (postfix)	smtp 25/TCP
Serveur Samba	netbios-ns 137/TCP; netbios-dgm 138/TCP; netbios-ssn 139/TCP; microsoft-ds 445/TCP
Serveur DHCP	bootpc 68/TCP
Serveur DNS	domain 53/TCP; domain 53/UDP
- " -	auxquels s'ajoute une prise en charge particulière du portmapper dans SuSEFirewall2
portmapper	sunrpc 111/TCP; sunrpc 111/UDP
Serveur NFS	nfs 2049/TCP
- " -	plus portmapper
Serveur NIS	portmap activé
tftp	tftp 69/TCP
CUPS (IPP)	ipp 631/TCP; ipp 631/UDP

Configuration du système d'impression

À la fin de l'installation (Boîte de dialogue de suggestion), il faut veiller à ce que les ports utiles au système d'impression soient ouverts dans la configuration du pare-feu. Les ports 631/TCP et 631/UDP sont nécessaires à CUPS et ne devraient pas être bloqués pour un fonctionnement normal. Si on veut imprimer via LPD ou via SMB, le port 515/TCP (pour l'ancien protocole LPD) ou les ports utilisés par Samba doivent être accessibles.

Passage à X.Org

Le passage de XFree86 à X.Org est facilité par des liens de compatibilité pour que les fichiers et commandes importants puissent rester accessibles par leurs anciens noms.

TAB. 4.3: *Commandes*

XFree86	X.Org
`XFree86`	`Xorg`
`xf86config`	`xorgconfig`
`xf86cfg`	`xorgcfg`

TAB. 4.4: *Fichiers journaux dans /var/log*

XFree86	X.Org
`XFree86.0.log`	`Xorg.0.log`
`XFree86.0.log.old`	`Xorg.0.log.old`

De plus, en raison du passage à X.org, le nom des paquetages est passé de `XFree86*` à `xorg-x11`.

Modifications du paquetage powersave

Les fichiers de configuration `/etc/sysconfig/powersave` ont été modifiés.

TAB. 4.5: *Division des fichiers de configuration dans /etc/sysconfig/powersave*

Ancien	est maintenant divisé en
`/etc/sysconfig/powersave/common`	`common`
	`cpufreq`
	`events`
	`battery`
	`sleep`
	`thermal`

`/etc/powersave.conf` n'existe plus et les variables existantes sont reprises dans les fichiers comme décrit dans le tableau ci-dessus. Si vous aviez fait des modifications à la variable "event" de `/etc/powersave.conf`, celles-ci sont maintenant adaptées en conséquence dans `/etc/sysconfig/powersave/events`

Il faut de plus veillez à ce que la dénomination des "Modes de veille" (en anglais *Sleep Status*) ait été modifiée ; il y avait précédemment :

- suspend (ACPI S4, APM suspend)
- standby (ACPI S3, APM standby)

On a maintenant :

- suspend to disk (ACPI S4, APM suspend)
- suspend to ram (ACPI S3, APM suspend)
- standby (ACPI S1, APM standby)

OpenOffice.org (OOo)

Chemin : OOo est maintenant installé dans `/usr/lib/ooo-1.1` au lieu de `/opt/OpenOffice.org`. Le répertoire par défaut pour les installations utilisateurs est maintenant `~/.ooo-1.1` au lieu de `~/OpenOffice.org1.1`.

Raccourcis : Il existe de nouveaux raccourcis pour le démarrage des composants d'OOo ; voici un tableau de correspondance :

TAB. *4.6:* *Raccourcis*

Ancien	Nouveau
/usr/X11R6/bin/OOo-calc	/usr/bin/oocalc
/usr/X11R6/bin/OOo-draw	/usr/bin/oodraw
/usr/X11R6/bin/OOo-impress	/usr/bin/ooimpress
/usr/X11R6/bin/OOo-math	/usr/bin/oomath
/usr/X11R6/bin/OOo-padmin	/usr/sbin/oopadmin
/usr/X11R6/bin/OOo-setup	-
/usr/X11R6/bin/OOo-template	/usr/bin/oofromtemplate
/usr/X11R6/bin/OOo-web	/usr/bin/ooweb
/usr/X11R6/bin/OOo-writer	/usr/bin/oowriter
/usr/X11R6/bin/OOo	/usr/bin/ooffice
/usr/X11R6/bin/OOo-wrapper	/usr/bin/ooo-wrapper

Les raccourcis comprennent maintenant l'option `--icons-set` pour passer entre les jeux d'icônes KDE et GNOME. Les options suivantes ne sont plus prises en charge :`--default-configuration`, `--gui`, `--java-path`, `--skip-check`, `--lang` (la langue sera configurée à partir des paramètres de langue (en anglais *locales*)), `--messages-in-window` et `--quiet`.

Prise en charge de KDE et GNOME Les extensions à KDE et GNOME sont fournies séparément dans les paquetages `OpenOffice_org-kde` et `OpenOffice_org-gnome`.

Table de mixage "kmix"

La table de mixage kmix est installée par défaut. Pour le matériel haut de gamme, il existe des alternatives pour la tables de mixages comme QAMix/KAMix, envy24control (uniquement ICE1712) ou hdspmixer (uniquement RME Hammerfall).

4.3 RPM – Le gestionnaire de paquetages de la distribution

Sous SUSE LINUX,le gestionnaire de paquetages RPM (*RPM Package Manager*) s'appuie principalement sur les programmes `rpm` et `rpmbuild` chargés d'assurer la gestion des paquetages logiciels. Ainsi, les utilisateurs et les administrateurs, sans oublier bien entendu les créateurs de paquetages ont accès à toute la puissance de la base de données RPM, qu'ils peuvent interroger sans limites afin d'obtenir toutes les informations utiles sur les logiciels installés.

La commande `rpm` fonctionne essentiellement selon cinq modes : l'installation, la désinstallation ou la mise à jour de paquetages logiciels ; la régénération de la base de données RPM ; l'interrogation de la base de données RPM ou d'archives RPM données ; le contrôle d'intégrité des paquetages ; enfin la signature des paquetages. La commande `rpmbuild` est quant-à-elle chargée de générer les paquetages pouvant être installés à partir des sources originelles (*pristine sources*).

Les archives RPM pouvant être installées sont empaquetées dans un format binaire particulier ; elles comprennent les fichiers de programmes à installer ainsi que différentes méta-informations utilisées lors de l'installation par la commande `rpm` afin de configurer le paquetage logiciel concerné. Ces méta-informations sont également enregistrées dans la bases de données RPM dans une optique documentaire. Les archives RPM utilisent l'extension de fichier `.rpm`.

La commande `rpm` permet de gérer des paquetages conformes au standard LSB ; Pour plus de précisions sur LSB, reportez-vous à la section *Standards et spécifications* page 727.

Remarque

Un nombre considérables de paquetages ont besoin de composants (bibliothèques, fichiers d'en-tête à inclure, etc.) indispensables pour le développement logiciel, et constitués en paquetages indépendants. Ces paquetages de développement sont uniquement requis par les utilisateurs désirant compiler *eux-mêmes* leurs propres logiciels – par exemple pour compiler de nouveaux paquetages. Ces paquetages se reconnaissent généralement à leur suffixe `-devel` : `alsa-devel`, `gimp-devel`, `kdelibs-devel`, etc.

Remarque

4.3.1 Vérification de l'authenticité d'un paquetage.

Les paquetages RPM de SUSE LINUX sont signés à l'aide de GnuPG. La clé, fingerprint compris, est :

```
1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>
Key fingerprint = 79C1 79B2 E1C8 20C1 890F  9994 A84E DAE8 9C80 0ACA
```

La commande suivante permet de vérifier la signature d'un paquetage RPM, ce qui permet de s'assurer qu'il provient réellement de SUSE ou d'une autre source de confiance :

```
rpm --checksig apache-1.3.12.rpm
```

Cette mesure de précaution est recommandée tout particulièrement avec les paquetages de mise à jour obtenus sur Internet. Notre clé de signature de paquetage est déposée par défaut dans `/root/.gnupg/`. Depuis la version 8.1, cette clé est également enregistrée dans le répertoire `/usr/lib/rpm/gnupg/`, afin de permettre aux utilisateurs normaux de vérifier par eux-même la signature des paquetages RPM.

4.3.2 Gestion des paquetages : installation, mises à jour et désinstallation

En temps normal, l'opération d'installation d'une archive RPM est rapide :

```
rpm -i <paquetage>.rpm
```

Toutefois, cette commande par défaut installe un paquetage uniquement si les dépendances sont satisfaites et s'il n'y a pas de conflit ; La commande `rpm` affiche, le cas échéant, un message d'erreur indiquant les paquetages requis pour satisfaire les dépendances. De son côté, la base de données s'assure de l'absence de conflit : en règle générale, un fichier ne peut être rattaché qu'à un seul paquetage. Il est possible de contourner cette règle en faisant appel à différentes options. Cette faculté doit toutefois être réservée aux utilisateurs avertis, en raison des conséquences qu'il peut y avoir pour les mises à jour ultérieures du système.

Les options ci-après sont également intéressantes pour actualiser un paquetage : `-U` ou `--upgrade` et `-F` ou `--freshen`.

```
rpm -F <paquetage>.rpm
```

Cette opération supprime une éventuelle version antérieure du paquetage et installe la nouvelle version. La différence entre les deux versions est que l'option `-U` installe également les paquetages qui, jusqu'alors, n'étaient pas disponibles sur le système. Au contraire, l'option `-F` ne remplace un paquetage que s'il avait déjà été installé dans la version antérieure. Dans le même temps, la commande `rpm` essaye d'être respectueuse des *fichiers de configuration*, en utilisant – en simplifiant quelque peu – la stratégie suivante :

- Dans le cas où un fichier de configuration n'a pas été modifié par l'administrateur système, la commande `rpm` installe la nouvelle version du fichier correspondant. L'administrateur n'a pas à intervenir.
- Lorsqu'un fichier de configuration a été modifié par l'administrateur, n'importe quand avant la mise à jour, la commande `rpm` sauvegarde dans ce cas – et dans ce cas seulement – le fichier sous l'extension `.rpmorig` ou `.rpmsave` et installe la nouvelle version à partir du paquetage RPM, dans le cas où une modification serait intervenue entre le fichier initial et le fichier provenant du paquetage de la mise à jour. Il est alors probable que vous soyez obligé d'ajuster le fichier de configuration qui vient d'être installé à l'aide de la copie (`.rpmorig` ou `.rpmsave`), en fonctions de vos paramètres système.
- Les fichiers `.rpmnew` sont créés chaque fois qu'il existe déjà un fichier de configuration *et* et que l'option `noreplace` a été définie dans le fichier `.spec`.

Lorsqu'une mise à jour a été effectuée, tous les fichiers `.rpmorig`-, `.rpmsave`- et `.rpmnew` doivent être effacés après avoir été comparés avec les versions concurrentes, de manière à éviter tout conflit lors des mises à jour ultérieures. L'extension `.rpmorig` est choisie dans le cas où le fichier était inconnu de la base de données RPM. Dans le cas contraire, c'est l'extension `.rpmsave` qui est utilisée ; en d'autres termes : l'extension `.rpmorig` est utilisée pour les mises à jour d'un format tiers vers le format RPM et l'extension `.rpmsave` pour les mises à jour d'un ancien paquetage en un nouveau paquetage. Dans le cas de l'extension `.rpmnew`, il n'est pas possible de déterminer si l'administrateur système a modifié le fichier de configuration ou non. Vous trouverez une liste de ces fichiers à l'emplacement `/var/adm/rpmconfigcheck`.

Gardez à l'esprit que certains fichiers de configuration (par exemple `/etc/httpd/httpd.conf`) sont intentionnellement laissés inchangés afin de vous permettre de continuer à travailler avec vos propres paramètres.

L'option `-U` représente donc plus un équivalent de la séquence `-e` (désinstaller/supprimer) et `-i` (installer). Chaque fois que cela est possible, il est préférable de privilégier l'option `-U`.

Remarque

Après chaque mise à jour, vous devez contrôler les copies de sauvegarde créées à l'aide de la commande `rpm` et portant l'extension `.rpmorig` ou `.rpmsave`, correspondant aux anciens fichiers de configuration. Si nécessaire, récupérez votre configuration depuis les copies de sauvegarde et remettez-la dans les nouveaux fichiers de configuration. Supprimez enfin tous les anciens fichiers portant l'extension `.rpmorig` ou `.rpmsave`.

Remarque

YaST accompagné de l'option `-i` est en mesure de résoudre toutes les dépendances entre paquetages et d'effectuer l'installation correspondante :

```
yast -i <paquetage>
```

La procédure à appliquer pour la suppression de paquetage est analogue :

```
rpm -e <paquetage>
```

Toutefois, la commande `rpm` ne supprime un paquetage que s'il ne subsiste plus de dépendances. Ainsi, il est théoriquement impossible de supprimer Tcl/Tk tant qu'un autre programme en a besoin – c'est d'ailleurs le rôle de la base de données RPM de veiller sur ces dépendances. Dans le cas exceptionnel où une opération de suppression s'avérerait impossible, malgré l'absence de dépendances, il peut être utile de recréer la base de données RPM à l'aide de l'option `--rebuilddb` ; voir ci-après les remarques concernant la base de données RPM.

4.3.3 RPM et correctifs

Afin d'assurer la sécurité de fonctionnement d'un système, il est indispensable d'intégrer régulièrement des paquetages dans le système afin de le mettre à jour. Jusqu'à présent, il n'était possible de corriger des bogues présents dans un paquetage qu'en remplaçant ce dernier intégralement. Lorsque l'on a affaire à des paquetages volumineux comportant des bogues peu importants, le volume de données en cause peut devenir rapidement considérable. C'est ainsi que SUSE propose, depuis la version 8.1, une fonctionnalité dans les RPM, permettant d'appliquer des correctifs à des paquetages.

L'exemple de pine illustre les informations les plus intéressantes concernant un correctif-RPM :

- Le correctif RPM convient-il à mon système ?
  Pour vous en assurer, vous devez dans un premier temps demander quelle est la version du paquetage. Dans le cas de l'application pine, la commande est la suivante :

  ```
  rpm -q pine
  pine-4.44-188
  ```

  L'opération suivante consiste à examiner le correctif afin de déterminer s'il correspond précisément à cette version de pine :

  ```
  rpm -qp --basedon pine-4.44-224.i586.patch.rpm
  pine = 4.44-188
  pine = 4.44-195
  pine = 4.44-207
  ```

  Ce correctif correspond à trois versions différentes de pine. La version installée dans notre cas s'y trouve également, ce qui permet d'appliquer le correctif.
- Quels sont les fichiers remplacés par le correctif ?
  Il est facile, à partir du correctif RPM, d'identifier les fichiers affectés par le correctif en question. Le paramètre `-P` de `rpm` sert à accéder à des fonctions propres aux correctifs. Ainsi, la liste des fichiers est obtenue à l'aide la commande suivante :

  ```
  rpm -qpPl pine-4.44-224.i586.patch.rpm
  /etc/pine.conf
  /etc/pine.conf.fixed
  /usr/bin/pine
  ```

  ou, dans le cas où le correctif est déjà installé, avec

  ```
  rpm -qPl pine
  /etc/pine.conf
  /etc/pine.conf.fixed
  /usr/bin/pine
  ```

- Comment appliquer un RPM correctif au système ?
  Les RPM correctifs sont utilisés de la même manière que les RPM normaux. La seule différence est que cela implique qu'un RPM approprié ait déjà été appliqué.
- Quels sont les correctifs qui ont été appliqués dans le système et quelle version de paquetage ont-ils touché ?

Il est possible d'énumérer tous les correctifs ayant été appliqués sur le système en exécutant la commande `rpm -qPa`. La commande se présente alors comme suit si, comme c'est le cas dans notre exemple, nous avons un système auquel un correctif a déjà été appliqué :

```
rpm -qPa
pine-4.44-224
```

Dans le cas où vous souhaiteriez savoir, après quelque temps, quelle version de paquetage a été mise en place dans un premier temps, cette information se trouve également dans la base de données RPM. Ainsi, pour la commande `pine`, cette information est obtenue à l'aide de la commande :

```
rpm -q --basedon pine
pine = 4.44-188
```

Pour de plus amples informations, notamment sur la fonctionnalité des correctifs de RPM, reportez-vous aux pages de manuel de `rpm` et `rpmbuild`.

4.3.4 Interrogation

L'option `-q` (*query*) permet de demander des informations. Ceci vous permet d'examiner vous-même un fichier RPM (option `-p` ⟨*Fichier paquetage*⟩) mais également d'interroger la base de données RPM. Vous pouvez par ailleurs définir le mode d'affichage des informations affichées à l'aide des options supplémentaires suivantes ; voir le tableau 4.7.

TAB. 4.7: *Les principales options d'interrogation sont les suivantes (-q [-p] paquetage)*

`-i`	Affichage des informations relatives à un paquetage
`-l`	Affichage de la liste de fichiers du paquetage
`-f` ⟨*FICHIER*⟩	Demande du paquetage qui posséde le fichier ⟨*FICHIER*⟩ ; ⟨*FICHIER*⟩ doit être indiqué avec son chemin complet !
`-s`	Affichage de l'état des fichiers (implique `-l`)
`-d`	Lister uniquement les fichiers de documentation"| (implique `-l`)

`-c`	Lister uniquement les fichiers de configuration"| (implique `-l`)
`--dump`	Afficher toutes les informations pouvant être consultées associées aux fichier (utiliser avec `-l`, `-c` ou `-d`)
`--provides`	Lister les fonctionnalités proposées par le paquetage qui peuvent être demandées par un autre paquetage à l'aide du paramètre `--requires`
`--requires`, `-R`	Afficher les dépendances du paquetage
`--scripts`	Afficher les différents scripts d'installation/désinstallation

La commande suivante affiche l'information 4.2 :

```
rpm -q -i wget
```

Exemple 4.2: *rpm -q -i wget*

```
Name        : wget                     Relocations: (not relocateable)
Version     : 1.8.2                    Vendor: SuSE Linux AG, Nuernberg, Germany
Release     : 301                      Build Date: Di 23 Sep 2003 20:26:38 CEST
Install date: Mi 08 Okt 2003 11:46:31 CEST      Build Host: levi.suse.de
Group: Productivity/Networking/Web/Utilities Source RPM: wget-1.8.2-301.src.rpm
Size        : 1333235                  License: GPL
Signature   : DSA/SHA1, Di 23 Sep 2003 22:13:12 CEST, Key ID a84edae89c800aca
Packager    : http://www.suse.de/feedback
URL         : http://wget.sunsite.dk/
Summary     : A tool for mirroring FTP and HTTP servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

L'option `-f` fonctionne uniquement si le nom complet, incluant le chemin, est connu. Vous pouvez spécifier un nombre de fichiers à chercher quelconque, par exemple :

```
rpm -q -f /bin/rpm /usr/bin/wget
```

donne le résultat suivant :

```
rpm-3.0.3-3
wget-1.5.3-55
```

Dans le cas où une partie seulement du nom du fichier est connue, il faut utiliser un script shell (par exemple le fichier 4.3) ; le nom de fichier cherché doit être transmis en paramètre lors de l'appel du script.

Exemple 4.3: *Script de recherche de paquetage*

```
#! /bin/sh
for i in $(rpm -q -a -l | grep  $1); do
    echo "\"$i\" est contenu dans le paquetage :"
    rpm -q -f $i
    echo ""
done
```

La commande permet d'afficher précisément les informations (de mise à jour, de configuration, de modification, etc.) correspondant à un paquetage donné ; ici, par exemple avec le paquetage `rpm` :

```
rpm -q --changelog rpm
```

Toutefois, la base de données RPM n'affiche que les 5 derniers éléments ; le paquetage lui-même comprend tous les éléments (des 2 dernières années). La question suivante fonctionne lorsque le CD 1 est monté sous `/cdrom` :

```
rpm -qp --changelog /cdrom/suse/i586/rpm-3*.rpm
```

La base de données installée permet également de procéder à des vérifications. Ces opérations sont effectuées avec l'option `-V` (comparable à l'option `-y` ou `--verify`). Ainsi, la commande `rpm` affiche tous les fichiers qui ont été modifiés par rapport à la version initiale correspondant au paquetage. La commande `rpm` peut être complétée par des paramètres (jusqu'à huit) faisant référence aux modifications suivantes :

TAB. *4.8:* *Les vérifications*

`5`	Somme de contrôle MD5
`S`	Taille du fichier
`L`	Lien symbolique
`T`	Date/heure de modification
`D`	Numéros de périphérique (*device numbers*) majeur et mineur
`U`	Utilisateur (*user*)
`G`	Groupe (*group*)
`M`	Mode (recouvre les droits et le type)

Un `c` s'affiche en plus dans le cas des fichiers de configuration. L'exemple suivant illustre le cas où le fichier `/etc/wgetrc` de `wget` a été modifié :

```
rpm -V wget
S.5....T c /etc/wgetrc
```

Les fichiers de la base de données RPM se trouvent sous le répertoire `/var/lib/rpm`.

Avec une partition `/usr` de 1 Go, la base de données peut très bien occuper 30 Mo d'espace disque ; ceci est particulièrement vrai après une mise à jour complète. Dans l'éventualité où la base de données semblerait excessivement volumineuse, la solution la plus efficace consiste à utiliser l'option `--rebuilddb` pour créer une nouvelle base de données s'appuyant sur la base de données existante. Il est recommandé de réaliser une copie de la base de données existante avant de la reconstituer.

Par ailleurs, le script `cron` `cron.daily` crée des copies quotidiennes de la base de données dans `/var/adm/backup/rpmdb`. Leur nombre est fixé par la variable `MAX_RPMDB_BACKUPS` (option par défaut : `5`) dans `/etc/sysconfig/backup` ; chaque sauvegarde peut utiliser jusqu'à 3 Mo pour un répertoire `/usr` de 1 Go..

4.3.5 Installation et compilation de paquetages sources

Tous les paquetages source ont l'extension `.src.rpm` à la suite du nom du paquetage ; ces fichiers sont les RPM source ("Source-RPMs").

Remarque

Ces paquetages peuvent être installés avec YaST – de la même manière que pour tout autre paquetage –, à ceci près que les paquetages source ne sont jamais marqués comme étant installés (`[i]`), comme c'est le cas pour les autres paquetages classiques. La raison en est que les paquetages source ne sont pas répertoriés dans la base de données RPM, celle-ci s'intéressant uniquement aux applications *installées*.

Remarque

Les répertoires de travail de `rpm` et `rpmbuild` dans `/usr/src/packages` doivent exister (en l'absence de paramétrage personnalisé, tel qu'il peut être réalisé dans `/etc/rpmrc`) :

SOURCES pour les sources originales (fichiers `.tar.gz`, etc.) ainsi que pour les adaptations propres à une distribution (fichiers `.dif`).

SPECS pour les fichiers `.spec` chargés de contrôler la procédure de build à la manière d'une méta-makefile.

BUILD C'est sous ce répertoire que les sources sont décompactées, qu'un correctif leur est appliqué et qu'elles sont compilées.

RPMS Répertoire dans lequel les paquetages binaires sont enregistrés.

SRPMS Emplacement des RPM sources.

Lorsque vous installez un paquetage source avec YaST, les composants requis pour la procédure de build sont installés sous `/usr/src/packages` : les sources et les modifications qui y sont apportées dans `SOURCES` et le fichier `.spec` correspondant dans `SPECS`.

Remarque

itez de faire des expériences sur les RPM avec des composants système importants (`glibc`, `rpm`, `sysvinit` etc.), au risque de mettre en péril le fonctionnement de votre système.

Remarque

Examinons à présent le paquetage `wget.src.rpm`. Après avoir installé le paquetage source `wget.src.rpm` avec YaST, nous avons les fichiers :

```
/usr/src/packages/SPECS/wget.spec
/usr/src/packages/SOURCES/wget-1.4.5.dif
/usr/src/packages/SOURCES/wget-1.4.5.tar.gz
```

La commande `rpmbuild -b X /usr/src/packages/SPECS/wget.spec` lance la procédure de compilation ; On peut remplacer `X` par différents niveaux (voir l'affichage de l'option `--help` ou la documentation de RPM) ; nous nous contenterons de donner un explication succincte :

- **`-bp`** Préparer les sources dans le répertoire `/usr/src/packages/BUILD` : les décompacter et appliquer les correctifs
- **`-bc`** comme `-bp`, l'opération de compilation en plus
- **`-bi`** comme `-bc`, l'opération d'installation en plus. Attention, dans le cas où un paquetage ne prend pas en charge la fonctionnalité BuildRoot, des fichiers de configuration importants risquent d'être remplacés lors des opérations de configuration !
- **`-bb`** comme `-bi`, avec, en outre, la création du RPM binaire ; en cas de succès, ce fichier se trouve dans `/usr/src/packages/RPMS`.
- **`-ba`** comme `-bb`, avec, en outre, la création du RPM source ; en cas de succès, il est enregistré sous `/usr/src/packages/SRPMS`.

L'option `--short-circuit` permet de sauter un certain nombre d'étapes. Le RPM binaire créé doit finalement être installé à l'aide de la commande `rpm -i` ou, de préférence, à l'aide de la commande `rpm -U` .

4.3.6 Création de paquetages avec build

De nombreux paquetages présentent le risque de copier involontairement les fichiers dans le système en cours d'exécution. Pour éviter ce problème, vous pouvez utiliser `build` qui se charge de créer un environnement destiné à la compilation du paquetage. La mise en place de cet environnement où la racine du système est transplantée (chrootée) suppose que l'on réserve une arborescence de paquetages complète pour le script `build`. Cette arborescence peut être créée sur un disque dur, sur un système NFS ou sur DVD Le script obtient l'emplacement correspondant à l'aide de la commande `build --rpms <Chemin>`. Contrairement à la commande `rpm`, la commande `build` demande à ce que le fichier SPEC soit dans le même répertoire que les sources. Dans le cas où vous souhaitez recompiler wget, comme dans l'exemple précédent, et que le DVD est monté sur le système dans le répertoire `/media/dvd`, exécutez les commandes suivantes en tant que `root` :

```
cd /usr/src/packages/SOURCES/
mv ../SPECS/wget.spec .
build --rpms /media/dvd/suse/ wget.spec
```

Un environnement minimal destiné à la création du paquetage SuSe est ensuite mis en place dans `/var/tmp/build-root`. Les paquetages ainsi créés sont ensuite enregistrés dans `/var/tmp/build-root/usr/src/packages/RPMS`

Le script `build` propose un certain nombre d'options supplémentaires. Ainsi, il est possible d'utiliser en priorité vos propres RPM, omettre l'initialisation de l'environnement de build ou restreindre la commande `rpm` à l'un des niveaux précédemment décrits. La commande `build --help` et la page de manuel `man build` permettent d'obtenir de plus amples informations.

4.3.7 Utilitaires pour les archives RPM et pour la base de données RPM.

Midnight Commander (`mc`) peut afficher le contenu d'une archive RPM ou en copier des parties. Il représente ce genre d'archives à la manière d'un système de fichiers virtuel, toutes les commandes des menus de Midnight Commander étant disponibles – en fonction du contexte – : Les informations contenues dans les lignes d'en-tête-tirées du fichier `HEADER` peuvent être affichées à l'aide de la touche (F3) ; Les touches du curseur et (Entrée) permettent de naviguer dans l'arborescence de l'archive. Si nécessaire, la touche de fonction (F5) permet de copier des composants.

KDE comprend l'utilitaire kpackage, tandis que GNOME propose l'application gnorpm.

Le programme Alien (`alien`) permet de convertir les formats de paquetages propres aux différentes distributions. Ainsi, il est possible de convertir en RPM d'anciennes archives TGZ *avant* leur installation, afin de fournir à la base de données RPM, *pendant* l'installation du paquetage, des informations sur ce dernier. Attention toutefois : `alien` est un script Perl qui est selon les auteurs du programme encore en phase alpha, malgré un numéro de version élevé. Par ailleurs,il existe également un fichier `rpm.el` pour l'application Emacs, qui est une interface avec rpm.

Réparation du système

Outre de nombreux modules YaST pour l'installation et la configuration du système, SUSE LINUX offre également des fonctions de réparation du système installé. Ce chapitre décrit les diverses façons et les différents niveaux de réparation du système.

5.1 Démarrer l'outil de réparation du système de YaST

Étant donné qu'il n'est pas certain, en cas de dommages, que le système pourra être amorcé et sachant qu'un système en fonctionnement est difficile à réparer, l'outil de réparation du système de YaST est démarré à partir du CD ou du DVD d'installation de SUSE LINUX. Une fois que vous aurez passé les étapes décrites dans le chapitre *Installation avec YaST* page 7, le dialogue de sélection du mode d'installation s'ouvrira. Sélectionnez alors l'option 'Réparation du système installé' (figure 5.1).

Remarque

Sélection du support d'installation

Pour procéder au test et à la réparation, des pilotes seront chargés du CD/DVD. Vous devez donc vous assurer d'utiliser un support d'installation qui correspond *exactement* à la version installée de SUSE LINUX.

Remarque

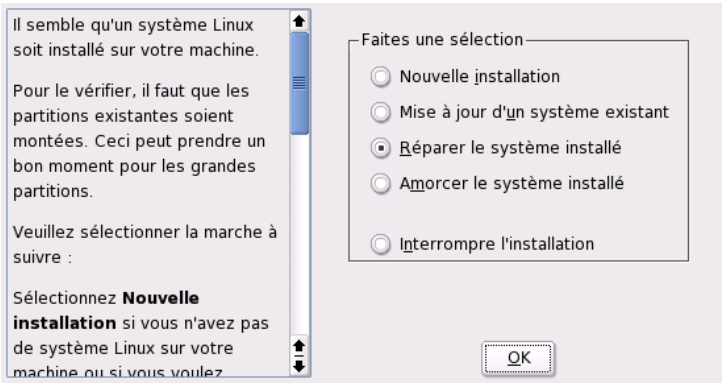


FIG. 5.1: *Sélectionner l'outil de réparation du système de YaST*

Sélectionnez ensuite comment la réparation du système doit être effectuée. Les possibilités dont vous disposez sont 'Réparation automatique', 'Réparation personnalisée' et 'Outils pour experts'. Elles sont décrites ci-après.

5.2 Réparation automatique

Si la cause du dommage n'est pas déterminée, alors cette méthode est la plus appropriée pour restaurer un système détérioré. Une fois la sélection faite, il est procédé à une analyse détaillée du système installé. Étant donné le nombre de tests et vérifications à réaliser, cette analyse peut durer un certain temps. Vous pourrez suivre la progression de cette procédure en bas de l'écran dans deux barres de progression. La barre supérieure affiche le déroulement de la vérification partielle en cours, la barre inférieure affichant quant à elle l'état global de l'analyse. Dans la fenêtre au-dessus, vous pouvez voir quelle action est menée actuellement et quel résultat a eu la vérification (figure 5.2 page suivante). Les groupes de tests suivants seront exécutés, chaque groupe contenant toute une série de vérifications.

Tables de partitions de tous les disques durs
La validité et la cohérence des tables de partitions de tous les disques durs trouvés est vérifiée.

Zones d'échange (swap) Les zones d'échange du système installé sont recherchées, vérifiées et éventuellement proposées pour être activées. Acceptez l'activation ; vous augmenterez ainsi la rapidité de l'outil de réparation du système de YaST.

Systèmes de fichiers Pour chaque système de fichiers trouvé, une vérification spécifique sera effectuée.

Entrées du fichier `/etc/fstab` L'intégrité et la cohérence des entrées du fichier seront vérifiées. Toutes les partitions valides seront rattachées.

Configuration du chargeur d'amorçage
L'intégrité et la cohérence de la configuration du chargeur d'amorçage du système installé (GRUB ou LILO) seront vérifiées. Les périphériques boot et root seront testés et la disponibilité du module initrd sera contrôlée.

Base de données de paquetages Ici, il est vérifié que tous les paquetages nécessaires à une installation minimale sont disponibles. Si vous le souhaitez, les paquetages de base peuvent aussi être analysés, cependant cela peut durer très longtemps.

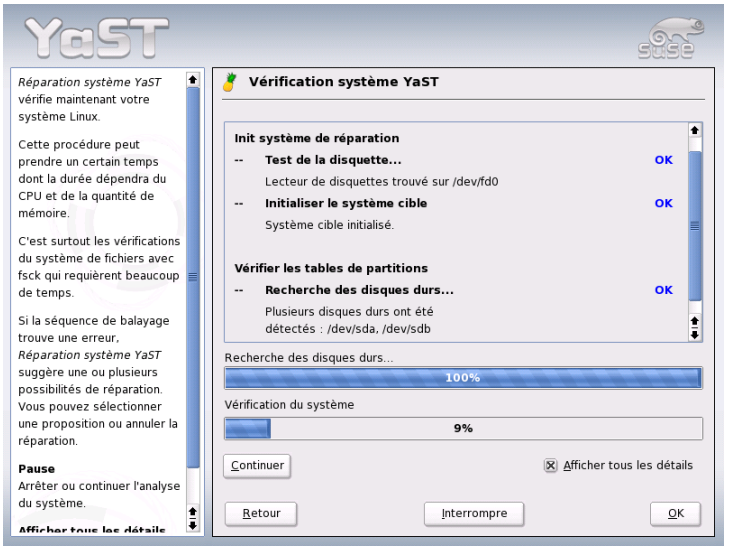


FIG. 5.2: *Le mode de réparation automatique*

Lorsqu'une erreur est trouvée, l'analyse est arrêtée et une fenêtre de dialogue est ouverte. Cette fenêtre affiche des détails et propose des solutions. Étant donné le nombre de vérifications effectuées, il n'est pas possible de décrire ici tous les cas de figure. Veuillez lire les conseils affichés à l'écran, puis sélectionnez l'option désirée. En cas de doute, vous pouvez également refuser la réparation proposée. Le système reste alors inchangé (pour ce point). Aucune réparation ne sera effectuée automatiquement sans demande de confirmation.

5.3 Réparation personnalisée

La réparation automatique décrite dans la section précédente procède à toutes les vérifications. Ceci n'est utile que lorsque l'origine des dommages du système est inconnue. Par contre, si vous savez quel zone du système est touchée, vous pouvez limiter ici le nombre des tests à effectuer. Après avoir sélectionné 'Réparation personnalisée', vous obtenez un choix de groupes de tests qui, dans un premier temps, sont tous sélectionnés. Dans ce cas, la vérification est la même que lors

d'une réparation automatique. Si vous savez où l'erreur *ne* se situe *pas*, vous pouvez désélectionner les groupes correspondants en cliquant sur la case à cocher correspondante. En cliquant sur 'Suivant', vous démarrez alors une procédure de test plus courte et donc plus rapide. Notez cependant que tous les groupes de tests ne peuvent pas être appliqués seuls. La vérification des entrées fstab, par exemple, est toujours associée à la vérification du système de fichiers ainsi que des zones d'échange (swap) associées. Si nécessaire, YaST vérifie ces dépendances en sélectionnant automatiquement le nombre minimum de groupes de tests.

5.4 Outils pour experts

Si vous connaissez bien SUSE LINUX et que vous avez déjà une idée très concrète de ce qui doit être réparé dans votre système, vous pouvez, après avoir sélectionné 'Outils pour experts', utiliser l'outil précis dont vous avez besoin pour la réparation.

Installer un nouveau chargeur d'amorçage
Ici, vous démarrez le module de configuration du chargeur d'amorçage. Vous trouverez plus de détails à ce sujet dans le chapitre *Configuration du chargeur d'amorçage avec YaST* page 219

Démarrer le partitionneur Ici, vous démarrez le partitionneur YaST. Vous trouverez plus de détails à ce sujet dans le chapitre*Installation avec YaST* page 7.*Partitionnement pour experts avec YaST* page 21

Réparation du système de fichiers Vous pouvez vérifier ici les systèmes de fichiers de votre système installé. Vous disposez d'une sélection de toutes les partitions trouvées et vous pouvez y choisir celle que vous souhaitez vérifier.

Restaurer des partitions perdues Lorsque des tables de partitions de votre système sont endommagées, vous pouvez tenter ici une reconstruction. Dans le cas de plusieurs disques durs, vous aurez d'abord la possibilité de choisir l'un d'entre eux. Cliquez sur 'OK' pour lancer la vérification. Cela peut prendre un certain temps, en fonction des performances de votre ordinateur et de la taille du disque dur.

Remarque

Reconstruction d'une table de partitions

La reconstruction d'une table de partitions est complexe. YaST essaie de reconnaître les partitions perdues à travers l'analyse des zones de données du disque dur. En cas de succès, les partitions retrouvées seront intégrées à la table de partitions reconstruite. Cependant, cela ne fonctionne pas à tous les coups.

Remarque

Enregistrer la configuration du système sur une disquette
Avec cette option, vous pouvez enregistrer des données importantes du système sur une disquette. Si une de ces données devait être endommagée plus tard, elle pourrait être restaurée à l'aide de la disquette.

Vérifier les logiciels installés Ici, la cohérence de la base de données de paquetages est testée et la disponibilité des paquetages les plus importants est vérifiée. Si des paquetages installés sont endommagés, vous pouvez ici requérir leur réinstallation.

5.5 Le système de secours SUSE

SUSE LINUX comporte plusieurs systèmes de secours à l'aide desquels vous pouvez accéder de l'extérieur à vos partitions Linux : vous pouvez charger le *système de secours* (*rescue system*) à partir d'un CD, du réseau, ou du serveur FTP de SUSE. Le système de secours contient plusieurs programmes qui pourront vous aider à résoudre des problèmes de disques durs devenus inaccessibles, de fichiers de configuration erronés, etc. Parted (`parted`) fait également partie du système de secours pour modifier les tailles des partitions. Il peut au besoin être lancé à partir du système de secours manuellement, si vous ne voulez pas utiliser le partitionneur intégré à YaST. Vous trouverez des informations sur Parted à l'adresse :

`http://www.gnu.org/software/parted/`

5.5.1 Démarrer le système de secours

On démarre le système de secours à partir d'un CD (ou d'un DVD). Pour cela, il faut que l'ordinateur puisse être amorcé à partir du lecteur de CD-ROM ou de DVD. Le cas échéant, vous devez modifier l'ordre d'amorçage dans la configuration du BIOS.

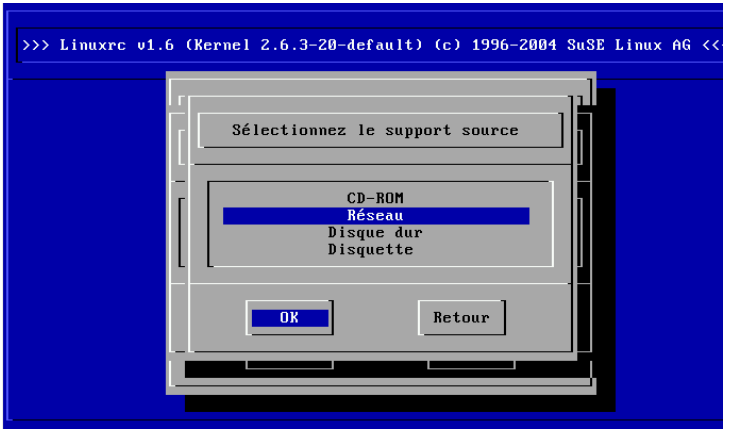


FIG. 5.3: *Média source pour le système de secours*

Vous trouverez ci-après la procédure de démarrage du système de secours :

1. Insérez le premier CD ou le premier DVD de SUSE LINUX dans le lecteur correspondant et mettez votre système sous tension.
2. Vous pouvez laisser démarrer le système automatiquement ou choisir 'Manual Installation' et ensuite – si nécessaire – saisir les paramètres de démmarrage spéciaux dans 'boot option'.
3. Procédez dans linuxrc aux réglages nécessaires pour la langue et le clavier.
4. Les modules du noyau nécessaires à votre système peuvent ensuite être chargés. Veuillez charger à ce moment *tous* les modules dont vous pensez qu'ils seront utilisés dans le système de secours. Le système de secours lui-même n'en comporte presque aucun pour une question de place.
5. Choisissez dans le menu principal le point commande 'Démarrer installation/système'.

6. Choisissez dans le menu 'Démarrer l'installation/le système' le point 'Démarrer le système de secours' (cf. Fig. 3.7 page 123) et saisissez alors le support source souhaité (cf. Fig. 5.3 page précédente).

   'CD-ROM' Le système de secours sur le CD-ROM est utilisé.

   'Réseau' Le système de secours est démarré via une liaison réseau. Pour cela, le module de noyau correct pour la carte réseau doit d'abord avoir été chargé (cf. les indications générales dans la section *Installation en réseau* page 131). Dans un sous-menu se trouvent plusieurs protocoles à disposition (cf. Fig. 5.4) : NFS, FTP, SMB etc.

   'Disque dur' Si vous avez déjà copié auparavant un système de secours sur un disque dur actuellement accessibles, vous pouvez indiquez ici où il se trouve. Ce système de secours est ensuite utilisé.

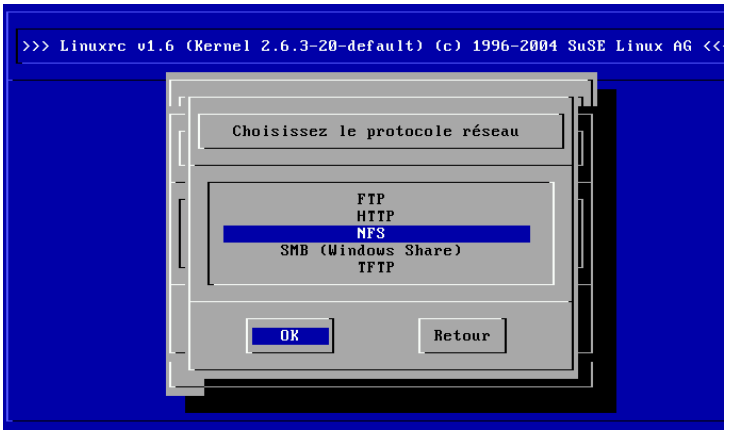


FIG. 5.4: *Protocoles de réseau*

Quel que soit le média choisi, le système de secours est décompressé, chargé comme nouveau système de fichiers racine sur un disque virtuel, monté et démarré. Il est ainsi prêt à fonctionner.

5.5.2 Utiliser le système de secours

Avec les combinaisons (Alt) + (F1) jusqu'à (Alt) + (F3), le système de secours met à votre disposition au moins trois consoles virtuelles, auxquelles vous pouvez vous connecter comme utilisateur `root` sans mot de passe. (Alt) + (F10) vous permet d'accéder à la console système avec les messages du noyau et de syslog.

Vous trouverez dans le répertoire `/bin` l'interpréteur de commande et les utilitaires (par exemple mount). Les utilitaires de fichiers et de réseau, par exemple pour contrôler et réparer des systèmes de fichiers (reiserfsck, e2fsck, etc.) se trouvent dans le répertoire `/sbin`. Vous trouverez aussi dans ce répertoire les fichiers binaires les plus importants pour la gestion du système comme fdisk, mkfs, mkswap, init, shutdown, ainsi que pour le fonctionnement du réseau comme ifconfig, route et netstat. Vous disposez en tant qu'éditeur de vi dans `/usr/bin` ; vous y trouverez aussi d'autres outils (grep, find, less etc.) ainsi que le programme telnet.

Accès au système normal

Le point de montage `/mnt` est destiné à monter votre système SUSE LINUX sur le disque. Vous pouvez, à des fins personnelles, créer d'autres répertoires et les utiliser comme points de montage.

Supposez par exemple que votre système normal est composé d'après `/etc/fstab` comme décrit dans le fichier exemple 5.1.

Exemple 5.1: *Exemple /etc/fstab*

```
/dev/sdb5       swap        swap        defaults   0   0
/dev/sdb3       /           ext2        defaults   1   1
/dev/sdb6       /usr        ext2        defaults   1   2
```

Attention

Considérez dans la section suivante l'ordre dans lequel les périphériques doivent être montés.

Attention

Afin d'avoir accès à tout le système, montez-le pas à pas sous `/mnt` avec les instructions suivantes :

```
mount /dev/sdb3 /mnt
mount /dev/sdb6 /mnt/usr
```

Vous avez désormais accès à tout le système et pouvez par exemple réparer les erreurs dans les fichiers de configuration comme `/etc/fstab`, `/etc/passwd` et `/etc/inittab`. Les fichiers de configuration ne se trouvent alors plus dans le répertoire `/etc` mais dans le répertoire `/mnt/etc`. Pour récupérer les partitions complètement perdues en les recréant simplement avec le programme fdisk, imprimez (copie papier) *auparavant* le répertoire `/etc/fstab` et le résultat de la commande `fdisk -l`.

Réparer les systèmes de fichiers

Des systèmes de fichiers endommagés sont une raison particulièrement valable de recourir au système de secours. Les systèmes de fichiers ne peuvent en principe pas être réparés quand le système est en marche. En cas de dommages importants, le système de fichiers racine ne peut le cas échéant même pas être monté et le démarrage du système se termine par un `kernel panic`. Il ne reste alors que la solution de tenter la réparation par l'extérieur à l'aide d'un système de secours.

Les utilitaires reiserfsck, e2fsck et dumpe2fs (pour le diagnostic) sont inclus dans le système de secours de SUSE LINUX. Vous pouvez résoudre ainsi la plupart des problèmes. Comme en cas de besoin les pages de manuel de reiserfsck et de e2fsck ne sont souvent plus accessibles, elles sont imprimées dans les annexes *Page de manuel de reiserfsck* page 729 et *Page de manuel-de e2fsck* page 735.

Exemple : si un système de fichiers `ext2` ne peut plus être monté à cause d'un *superbloc invalide*, le programme e2fsck échouera sans doute aussi. La solution consiste à utiliser les sauvegardes de superblocs créées et maintenues à jour dans le système de fichiers tous les 8192 blocs (8193, 16385…). C'est ce qu'exécute par exemple la commande :

```
e2fsck -f -b 8193 /dev/<Partition_Défectueuse>
```

L'option `-f` force le contrôle de système de fichiers et prévient ainsi l'erreur possible de `e2fsck`, à condition que – concernant la copie du superbloc intact– tout soit en ordre.

Deuxième partie

Système

Applications 32 bit et 64 bit dans un environnement système de 64 bit

SUSE LINUX est disponible pour plusieurs plateformes 64 bits. Ceci ne signifie pas nécessairement que toutes les applications contenues ont déjà été adaptées sur 64 bits. SUSE LINUX supporte l'utilisation d'applications 32 bits dans un environnement système de 64 bits. Ce chapitre vous donne un petit aperçu de la façon dont ce support est transféré sur des plateformes SUSE LINUX 64 bits.

SUSE LINUX pour les plateformes 64 bits AMD64 et EM64T est étudié de telle façon que les applications 32 bits existantes dans l'environnement 64 bits soient utilisables "dès la sortie du carton". Grâce à ce support, il vous est possible de continuer à utiliser les applications 32 bits que vous préférez sans avoir à attendre qu'un port 64 bits correspondant soit disponible.

Pour comprendre le support 32 bits, vous devez d'abord vous intéresser aux thèmes suivants :

Support de la durée d'exécution Comment les applications 32 bits peuvent-elles être exécutées ?

Support de développement Comment compiler les applications 32 bits pour qu'elles puissent être utilisables autant dans des environnements 32 bits que dans des environnements 64 bits ?

Noyau API Comment des applications 32 bits peuvent-elles fonctionner sous un noyau 64 bits ?

6.1 Support de la durée d'exécution

Remarque

Conflits entre la version 32 bits et 64 bits d'une application

Si une application est disponible autant pour 32 bits que pour 64 bits, une installation parallèle des deux versions posera inévitablemenet des problèmes. Dans de tels cas, vous devez vous décider pour l'une ou l'autre des deux versions, installer et utiliser celle-ci.

Remarque

Chaque application nécessite une série de bibliothèques pour être exécutée correctement. Les désignations pour les versions 32 bits et 64 bits de cette bibliothèque sont malheureusement identiques – elle doivent se différencier l'une de l'autre d'une autre façon.

Pour maintenir la compatibilité avec la version 32 bits, les bibliothèques sont mémorisées dans le système à l'endroit même où elles se trouvent dans l'environnement 32 bits. La version 32 bits de `libc.so.6` se trouve aussi bien dans l'environnement 32 bits que dans l'environnement 64 bits sous `/lib/libc.so.6`.

Toutes les bibliothèques 64 bits et les fichiers objet se trouvent dans des répertoires appelés `lib64`, c'est-à-dire que fichiers objet 64 bits que vous chercheriez normalement sous`/lib`, `/usr/lib` et `/usr/X11R6/lib`, se trouvent maintenant sous `/lib64`, `/usr/lib64` et `/usr/X11R6/lib64`. Il y a ainsi de la place pour les bibliothèques 32 bits sous `/lib`, `/usr/lib` et `/usr/X11R6/lib`, le nom de fichier pour les deux versions pouvant être conservé de façon inchangée.

En principe, les sous-répertoires des répertoires objet dont le contenu des données est indépendant de la taille du mot, *ne sont pas* déplacés. Vous trouverez par exemple toujours les polices X11 comme d'habitude sous `/usr/X11R6/lib/X11/fonts`.

Ce schéma est conforme à la LSB (Linux Standards Base) et au FHS (File System Hierarchy Standard).

6.2 Développement de logiciels

Avec un Biarch-Development-Toolchain, on peut générer aussi bien des objets 32 bits que des objets 64 bits. Sur presque toutes les plateformes, le standard est la compilation d'objets 64 bits. Quand des flags spéciaux sont utilisés, des objets 32 bits peuvent être générés. Pour GCC, ce flag spécial est `-m32`

Notez que tous les fichiers d'en-tête doivent être écrits dans une forme indépendante de l'architectuure et que les bibliothèques installées 32 et 64 bits doivent présenter une API (Application Programming Interface) en accord avec les fichiers d'en-tête installés. L'environnement SUSE normal est conçu selon ce schéma – . Pour les bibliothèques que vous actualisez vous-même, vous devez vous occuper personnellement de ces questions.

6.3 Compilation de logiciels sur des plateformes Biarch

Pour développer sur une architecture Biarch des fichiers binaires pour l'autre architecture, vous devez installer en plus les bibliothques correspondantes pour l'architecture additionnelle. Ces paquetages s'appellent `rpmname-32bit` .

Vous avez en outre besoin des fichiers d'en-tête et bibliothèques adéquates que vous trouverez dans les paquetages `rpmname-devel` ainis que les bibliothèques de développement au sujet de l'architecture additionnelle que vous trouverez sous `rpmname-devel-32bit` .

La plupart des programmes open source utilisent une configuration de programme basée sur autoconf. Pour utiliser autoconf pour la configuration d'un programme pour l'architecture additionnelle, vous devez écraser les réglages normaux du compilateur et de l'éditeur de liens de autoconf en appelant les scripts configure avec des variables d'environnement supplémentaires.

L'exemple suivant se base sur un système AMD64 et EM64T avec x86 comme architecture additionnelle :

- Définissez que autoconf doit utiliser le compileur 32S bits :

  ```
  CC="gcc -m32"
  ```

- Donnez l'ordre à l'éditeur de liens de traiter les objets 32 bits :

  ```
  LD="ld -m elf_i386"
  ```

- Définissez que l'assembleur crée des objets 32 bits :

  ```
  AS="gcc -c -m32"
  ```

- Définissez que les bibliothèques pour libtool etc. proviennent de `/usr/lib` :

  ```
  LDFLAGS="-L/usr/lib"
  ```

- Définissez que les bibliothèques sont classées dans le sous-répertoire `lib` :

  ```
  --libdir=/usr/lib
  ```

- Définissez que les bibliothèques X 32 bits sont utilisées :

  ```
  --x-libraries=/usr/X11R6/lib/
  ```

Ces variables ne sont pas toutes nécessaires pour chaque programme. Adaptez-les aux données du programme.

6.4 Spécifications du noyau

Les noyaux 64 bits pour AMD64 et EM64T offrent un ABI du noyau (Application Binary Interface) aussi bien 64 que 32 bits. Ce dernier est identique à l'ABI pour le noyau 32 bits correspondant. Ceci signifie que l'application 32 bits avec le noyau 64 bits peut communiquer de la même manière qu'avec le noyau 32 bits.

Veuillez noter que l'émulation 32 bits d'appels système d'un noyau 64 bits ne supporte pas un certain nombre d'API utilisés par les programmes système. Ceci dépend de la plateforme. C'est pour cette raison qu'un petit nombre d'applications comme lspci ou les programmes d'administration LVM existent en tant que programmes 64 bits pour qu'ils fonctionnent correctement.

Un noyau 64 bits peut charger exclusivement des modules de noyau 64 bits spécialement compilés pour ce noyau. L'utilisation de modules de noyau 32 bits *n'est pas* possible.

Remarque

Quelques applications ont besoin de leurs propres modules de noyau chargeables. Si vous avez l'intention d'utiliser une telle application 32 bits dans un environnement système 64 bits, contactez le fournisseur de cette application et SUSE pour être sûr que la version 64 bits du module de noyau chargeable et que la conversion 32 bits des noyaux API sont disponibles pour ce module.

Remarque

Amorçage et chargeur d'amorçage

Ce chapitre décrit le processus d'amorçage de votre système Linux. Vous apprendrez comment configurer GRUB, le chargeur d'amorçage utilisé par SUSE LINUX. À cette fin, vous disposez du module YaST avec lequel vous pouvez procéder à la configuration de tous les paramètres nécessaires. Si besoin est, consultez les sections suivantes consacrées à la théorie de la procédure d'amorçage. En conclusion, nous avons rassemblé quelques uns des problèmes les plus fréquents lors de l'amorçage avec GRUB ainsi que leur solution.

7.1 La procédure d'amorçage

Lors de la procédure d'amorçage, le contrôle de votre système passe, dans un processus en trois étapes, de BIOS au noyau de votre système d'exploitation en passant par le chargeur d'amorçage. Juste après la mise sous tension de l'ordinateur, le BIOS (en anglais,*Basic Input Output System*) initialise l'écran et le clavier et teste la mémoire centrale. Jusqu'à cet instant, l'ordinateur ne dispose d'aucune mémoire de masse. Enfin, les informations relatives à la date actuelle, à l'heure et aux périphériques les plus importants sont lues à partir des valeurs CMOS (*CMOS Setup*). À partir du moment où le premier disque dur et sa géométrie sont connus, le BIOS passe le contrôle au chargeur d'amorçage.

D'une taille de 512 octets, le premier secteur physique de données du premier disque dur est chargé dans la mémoire et le programme (le *chargeur d'amorçage*) qui se trouve au début de ce secteur prend le contrôle. La suite d'instructions exécutées avec le chargeur d'amorçage détermine le reste de la procédure d'amorçage. Pour cette raison, les 512 premiers octets sur le premier disque dur sont également appelés *secteur maître d'amorçage* (en anglais, *Master Boot Record*, MBR).

Jusqu'à cet instant (chargement du MBR), le processus d'amorçage s'exécute complètement indépendamment du système installé sur l'ordinateur et celui-ci ne dispose jusque là que des routines (pilotes) enregistrées dans le BIOS pour accéder à ses périphériques.

7.1.1 Secteur maître d'amorçage

La structure de l'enregistrement d'amorçage maître se définit à l'aide d'une convention commune à tous les systèmes d'exploitation. Les 446 premiers octets sont réservés au code programme. Les 64 octets suivants prévoient de la place pour une table des partitions contenant jusqu'à quatre sections ; reportez-vous à la section *Partitionnement pour les experts* page 138. La table des partitions contient des informations sur la partitionnement du disque dur et le type de système de fichiers dont le système d'exploitation a besoin. Sans cette table des partitions, le système d'exploitation ne peut pas utiliser le disque dur. Les 2 derniers octets du MBR doivent contenir un "nombre magique" fixe (AA55) : un MBR qui contient autre chose à cet emplacement est considéré comme incorrect par le BIOS et par tous les systèmes d'exploitation.

7.1.2 Secteurs d'amorçage

Les secteurs d'amorçage sont les premiers secteurs des partitions de disque dur, sauf dans le cas d'une partition étendue qui ne représente qu'un "conteneur" pour les autres partitions. Ces secteurs d'amorçage disposent d'une place de 512 octets et sont prévus pour accueillir le code capable de démarrer un système d'exploitation se trouvant sur cette partition. Cela s'applique aux secteurs d'amorçage de partitions formatées sous DOS, Windows ou OS/2 qui contiennent aussi d'autres données capitales du système de fichiers. Par opposition, les secteurs d'amorçage des partitions Linux sont, même après l'installation d'un système de fichiers, tout d'abord vides. Une partition Linux n'est ainsi pas *amorçable par elle-même*, même si elle contient un noyau et un système de fichiers root correct. Un secteur d'amorçage qui contient un code correct pour le démarrage du système contient dans les 2 derniers octets la même marque "magique" que le MBR (`AA55`).

7.1.3 Amorçage de DOS ou de Windows

Si le MBR contient du code d'amorçage général (générique), le système à démarrer peut être déterminé avec exactement une partition primaire active ou marquée comme amorçable. En général, la validité du secteur d'amorçage de cette partition sera également vérifiée. Depuis le système démarré lors de la prochaine procédure d'amorçage, il est facile de passer à un autre système grâce à `fdisk`.

Si une partition DOS/Windows est active, le secteur d'amorçage charge les pilotes `.sys` nécessaires au démarrage du système. Sous DOS, une seule partition principale peut être identifiée comme étant active. Par conséquent, le système DOS ne peut pas être hébergé sur des lecteurs logiques dans une partition étendue.

Windows 2000/XP peut aussi être installé sur une partition logique ; il est même possible de procéder à plusieurs installations simultanées de Windows. Cependant, les fichiers d'amorçage correspondants sont écrits sur une partition principale. Si un système 2000/XP supplémentaire est installé, celui-ci est ajouté directement au menu d'amorçage. Par conséquent, la limitation due au fait que Windows ne peut pas fonctionner sans partition principale demeure.

7.2 Méthodes d'amorçage

La "méthode d'amorçage" la plus simple concerne un ordinateur avec un seul système d'exploitation. Dès que plus d'un système d'exploitation est installé sur un ordinateur, plusieurs méthodes d'amorçage sont possibles :

Amorcer des systèmes supplémentaires à partir de supports de données externes
: Un système d'exploitation est chargé à partir du disque dur. À l'aide d'un chargeur d'amorçage installé sur un support de données externe (Disquette, CD, support de données USB), vous pouvez démarrer d'autres systèmes d'exploitation. Étant donné que GRUB peut charger tous les autres systèmes d'exploitation, il n'est pas nécessaire de conserver un chargeur d'amorçage externe.

Installation du gestionnaire d'amorçage dans le MBR
: Un gestionnaire d'amorçage permet d'avoir plusieurs systèmes d'exploitation en parallèle sur un seul ordinateur et de les utiliser en alternance. L'utilisateur choisit le système à charger lors du processus d'amorçage ; un changement de système d'exploitation implique le redémarrage de l'ordinateur. La condition préalable est que le gestionnaire d'amorçage choisi "s'accorde" avec tous les systèmes d'exploitation. Le gestionnaire d'amorçage de SUSE LINUX, GRUB, permet de démarrer tous les systèmes d'exploitation courants. Par conséquent, SUSE LINUX installe le gestionnaire d'amorçage souhaité par défaut dans le MBR. Ne modifiez donc pas ce réglage dans la boîte de dialogue d'installation.

7.3 Choix du chargeur d'amorçage

Par défaut, c'est le chargeur d'amorçage GRUB qui est utilisé sous SUSE LINUX. Cependant, pour quelques exceptions et certaines constellations matérielles ou logicielles, il faut avoir recours à LILO.

Lorsque vous effectuez une mise à jour à partir d'une version précédente de SUSE LINUX qui utilisait LILO, LILO est à nouveau installé. Lors d'une première installation au contraire, c'est GRUB qui, outre la partition racine, est installé sur les systèmes Raid suivants :

- Contrôleur Raid dépendant du processeur (comme, par exemple, de nombreux contrôleurs Promise ou Highpoint)

- Raid logiciel
- LVM

Vous trouverez des informations sur l'installation et la configuration de LILO dans la base de données support à l'aide du mot-clé "LILO".

7.4 Amorcer avec GRUB

GRUB (*Grand Unified Bootloader*) comporte deux niveaux. Le premier niveau (stage1) est stocké sur 512 octets dans le MBR ou le secteur d'amorçage d'une partition de disque ou d'une disquette. Le deuxième niveau (stage 2), plus volumineux, est ensuite chargé et contient le véritable code programme. En ce qui concerne GRUB, la seule tâche qu'effectue le premier niveau consiste à charger le deuxième niveau du chargeur d'amorçage.

stage2 peut accéder à des systèmes de fichiers. Actuellement, Ext2, Ext3, ReiserFS, JFS, XFS, Minix et le système de fichiers DOS FAT FS utilisé par Windows sont pris en charge. Bien qu'avec des limitations, JFS XFS ainsi que UFS/FFS, utilisé par les systèmes BSD, sont également pris en charge. Depuis sa version 0.95, GRUB peut également amorcer depuis un CD ou un DVD avec un système de fichiers standard conforme à la norme ISO 9660 selon les spécifications "El Torito". GRUB peut aussi accéder avant le démarrage à des systèmes de fichiers de disques supportés par le BIOS (disquette ou encore disques durs, lecteurs CD ou lecteurs DVD reconnus par le BIOS), c'est pourquoi il n'est plus nécessaire de réinstaller le chargeur d'amorçage après avoir modifié le fichier de configuration de GRUB (`menu.lst`). À l'amorçage, GRUB relit le fichier de menu contenant les chemins actuels et les déclarations de partitions du noyau ou du disque virtuel initial (`initrd`) et trouve lui-même ces fichiers.

Pour la configuration en soi de GRUB, trois fichiers sont nécessaires ; ils sont décrits ci-après :

`/boot/grub/menu.lst` Ce fichier contient toutes les données relatives aux partitions ou aux systèmes d'exploitation qui sont amorçables avec GRUB. Sans ces données, la prise de contrôle du système par le système d'exploitation n'est pas possible.

`/boot/grub/device.map` Ce fichier "traduit" les noms de périphériques utilisés par la notation GRUB/BIOS en noms de périphériques Linux.

`/etc/grub.conf` Dans ce fichier, les paramètres et options que l'interpréteur de commandes (shell) GRUB nécessite afin d'installer correctement le chargeur d'amorçage sont exécutés.

GRUB peut être contrôlé de différentes façons. Les entrées d'amorçage d'une configuration existante sont sélectionnées à l'aide de l'écran de démarrage (splash screen). La configuration est lue sans modification dans le fichier `menu.lst`.

GRUB permet la modification de tous les paramètres d'amorçage *avant* l'amorçage. Par exemple, si une erreur a été faite lors de l'édition du fichier de menu, celui-ci peut être "réparé" par ce biais. De plus, des commandes d'amorçage peuvent être saisies interactivement dans une sorte d'invite de commande (voir section *Modification d'éléments du menu pendant la procédure d'amorçage* page 214). GRUB permet aussi de connaître l'état du noyau et de `initrd` avant l'amorçage. Vous pouvez ainsi amorcer des systèmes d'exploitation qui n'ont pas encore été enregistrés dans le menu d'amorçage.

Enfin, il existe, avec le *shell GRUB*, une émulation de GRUB dans le système installé. Vous pouvez utiliser l'interpréteur de commande (shell) GRUB afin d'installer GRUB ou bien pour tester une nouvelle configuration avant de la mettre en place (voir section *L'interpréteur de commandes (shell) GRUB* page 217).

7.4.1 Le menu de démarrage de GRUB

L'écran de démarrage graphique avec le menu d'amorçage s'appuie sur le fichier de configuration de GRUB `/boot/grub/menu.lst`, qui contient toutes les informations à propos des partitions ou systèmes d'exploitation pouvant être démarrés à l'aide du menu.

GRUB relit à chaque démarrage du système le fichier de menu du système de fichiers. Il n'est donc pas nécessaire de réinstaller GRUB après chaque modification du fichier — utilisez le module chargeur d'amorçage de YaST pour procéder aux modifications de la configuration de GRUB (voir section *Configuration du chargeur d'amorçage avec YaST* page 219).

Le fichier de menu comporte des commandes. La syntaxe est très simple. Chaque ligne comporte une commande, suivie de paramètres optionnels, séparés comme pour l'interpréteur de commandes par des espaces. Quelques instructions admettent pour des raisons historiques un signe égal avant le premier paramètre. Les commentaires sont introduits par un dièse (#).

Pour identifier les éléments de menu dans l'aperçu du menu, vous devez attribuer à chaque choix un nom ou un `titre` (*title*). Le texte se trouvant après le mot-clé `title`, y compris les espaces, est affiché dans le menu comme une option pouvant être choisie. Toutes les instructions jusqu'au prochain `title` sont exécutées si cette sélection est effectuée dans le menu.

Le cas le plus simple est la redirection vers des gestionnaires d'amorçage d'autres systèmes d'exploitation. La commande s'appelle `chainloader` et l'argument est normalement le bloc d'amorçage d'une autre partition dans la notation des blocs (*Block-Notation*) de GRUB, par exemple :

```
chainloader (hd0,3)+1
```

Les noms de périphériques sous GRUB sont expliqués dans la section *Conventions de nom pour disques durs et partitions* page suivante. L'exemple ci-dessus spécifie le premier bloc de la quatrième partition sur le premier disque dur.

La commande `kernel` spécifie une image du noyau. Le premier argument est le chemin vers l'image du noyau sur une partition. Les arguments restants sont transmis au noyau sur la ligne de commande.

Quand le noyau ne dispose pas des pilotes intégrés nécessaires pour l'accès à la partition racine, il faut utiliser `initrd`. Il s'agit là d'une commande GRUB séparée, qui a comme seul argument le chemin vers le fichier `initrd`. Comme l'adresse de démarrage de `initrd` est écrite dans l'image du noyau déjà chargée, la commande `initrd` doit suivre la commande `kernel`.

La commande `root` permet d'indiquer plus facilement l'emplacement des fichiers du noyau et de initrd. `root` prend un unique argument, soit un périphérique de GRUB, soit une partition sur un tel périphérique. Tout chemin de fichiers du noyau, de `initrd`, ou autres, auquel aucun autre périphérique n'a été associé de façon explicite est associé à ce périphérique jusqu'à la commande `root` suivante. Cette commande n'apparaît pas dans un fichier `menu.lst` qui est généré pendant l'installation. Elle sert à la simplification lors d'une modification manuelle.

À la fin de chaque élément de menu, la commande `boot` est toujours implicite, si bien que celle-ci ne doit pas être écrite dans le fichier menu. S'il vous arrivait cependant d'utiliser GRUB de façon interactive pour démarrer, vous devez saisir à la fin la commande `boot`. `boot` n'a pas d'arguments, il n'exécute que l'image du noyau chargée ou le gestionnaire chaîné indiqué.

Lorsque vous avez écrit tous les éléments du menu, vous devez définir un élément par défaut (`default`). En son absence, le premier (élément `0`) sera utilisé. Vous pouvez aussi indiquer un délai en secondes après lequel le lancement doit s'effectuer. `timeout` et `default` apparaissent généralement avant les éléments du menu. Vous trouverez un fichier d'exemple et les explications associées en section *Exemple d'un fichier menu* page 213.

Conventions de nom pour disques durs et partitions

GRUB utilise pour la désignation de disques durs et partitions d'autres conventions que celles dont vous avez l'habitude pour les périphériques Linux normaux (par exemple, `/dev/hda1`). Le premier disque dur est toujours appelé `hd0`, le lecteur de disquettes est appelé `fd0`.

Le comptage de partitions dans GRUB commence par zéro. (`hd0,0`) correspond à la première partition sur le premier disque dur ; sur un ordinateur habituel avec un disque connecté comme Primary Master, le nom du périphérique est `/dev/hda1`.

Les quatre partitions primaires possibles prennent les numéros de partition `0` à `3`. Les partitions logiques sont numérotées à partir de `4` :

```
(hd0,0)   première partition primaire sur le premier disque dur
(hd0,1)   deuxième partition primaire
(hd0,2)   troisième partition primaire
(hd0,3)   quatrième partition primaire (et souvent étendue)
(hd0,4)   première partition logique
(hd0,5)   deuxième partition logique
...
```

GRUB ne différencie pas les périphériques IDE, SCSI ou RAID. Tous les disques durs reconnus par le BIOS ou d'autres contrôleurs sont numérotés conformément à l'ordre d'amorçage préréglé dans le BIOS.

Le fait qu'il n'y ait pas de relation claire entre les noms de périphériques Linux et les noms de périphériques du BIOS est un problème pour GRUB. GRUB utilise un certain algorithme pour générer ce classement et l'enregistre dans le fichier `device.map` qui peut être modifié. Vous trouverez plus d'informations sur `device.map` dans la section *Le fichier device.map* page 215.

Un chemin GRUB complet comprend un nom de périphérique écrit entre parenthèses ainsi que le chemin du fichier dans le système de fichiers sur la partition indiquée. Le chemin commence par un slash. Par exemple, sur un système avec un seul disque dur IDE et Linux sur la première partition, le noyau amorçable pourrait se présenter comme suit :

```
(hd0,0)/boot/vmlinuz
```

Exemple d'un fichier menu

Pour mieux comprendre la structure d'un fichier menu GRUB, nous présentons un court exemple. Cet exemple d'installation comprend une partition d'amorçage Linux sous `/dev/hda5`, une partition root sous `/dev/hda7` et une installation Windows sous `/dev/hda1`.

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8

title linux
   kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
   initrd (hd0,4)/initrd
title windows
   chainloader(hd0,0)+1
title floppy
   chainloader(fd0)+1
title failsafe
   kernel (hd0,4)/vmlinuz.shipped root=/dev/hda7 ide=nodma \
   apm=off acpi=off vga=normal nosmp maxcpus=0 3
   initrd (hd0,4)/initrd.shipped
```

Le premier bloc concerne la configuration de l'écran de démarrage :

`gfxmenu (hd0,4)/message` L'image de fond se trouve dans `/dev/hda5` et porte le nom de `message`

`color white/blue black/light-gray`
Le schéma de couleurs : blanc (premier plan), bleu (fond), noir (sélection) et gris clair (fond de la sélection). Le schéma de couleur n'a aucun effet sur l'écran de démarrage (splash screen), uniquement sur le menu modifiable de GRUB dans lequel vous arrivez lorsque vous quittez le splash screen à l'aide de Esc.

`default 0` Le premier élément du menu avec `title linux` correspond à l'amorçage par défaut.

`timeout 8` Après huit secondes sans réaction de la part de l'utilisateur, GRUB amorce le système automatiquement.

Le deuxième bloc, et le plus grand, énumère les différents systèmes d'exploitation amorçables ; les sections de chaque système d'exploitation sont introduites par `title`.

- Le premier élément (`title linux`) s'occupe de l'amorçage de SUSE LINUX. Le noyau (`vmlinux`) se trouve sur la première partition (ici la partition d'amorçage) du premier disque dur. Les paramètres du noyau comme, par exemple, l'indication de la partition racine ou du mode VGA y sont rattachés. La partition racine est indiquée selon le schéma Linux (`/dev/hda7/`) puisque cette information est destinée au noyau et n'a rien à voir avec GRUB. `initrd` se trouve également sur la première partition du premier disque dur.
- Le deuxième élément s'occupe du chargement de Windows. Windows est démarré à partir de la première partition du premier disque dur (`hd0,0`). `chainloader +1` gère la lecture et l'exécution du premier secteur de la partition indiquée.
- Le paragraphe suivant a pour but de permettre le démarrage depuis une disquette, sans avoir à modifier le BIOS.
- L'option d'amorçage `failsafe` sert à démarrer Linux avec un ensemble donné de paramètres du noyau, qui permettent eux-mêmes un démarrage des systèmes Linux problématiques.

Le fichier de menu peut être modifié à tout moment et est automatiquement repris par GRUB au démarrage suivant. Vous pouvez éditer à tout moment ce fichier avec YaST ou avec l'éditeur de votre choix. Vous pouvez sinon effectuer des modifications temporaires de façon interactive par la fonction Edit de GRUB (voir section *Modification d'éléments du menu pendant la procédure d'amorçage* de la présente page).

Modification d'éléments du menu pendant la procédure d'amorçage

À partir du menu d'amorçage graphique GRUB, vous pouvez choisir à l'aide des flèches lequel des systèmes d'exploitation doit être démarré. Si vous choisissez un système Linux, vous pouvez ajouter, à l'invite d'amorçage, vos propres paramètres de démarrage. Si vous appuyez sur Esc et quittez l'écran de démarrage, vous pouvez, après avoir saisi e (edit), modifier de façon ponctuelle directement et séparément des éléments du menu. Les modifications que vous effectuez de cette manière ne sont valables que pour ce seul processus d'amorçage et ne sont pas conservées de façon durable.

Remarque

Type de clavier pendant le démarrage

Notez que seul le clavier américain est disponible pour le démarrage. Veillez à la permutation des caractères spéciaux.

Remarque

Une fois le mode d'édition activé, choisissez à l'aide des flèches l'élément du menu dont vous voulez modifier la configuration. Afin de rendre la configuration modifiable, tapez à nouveau sur (e). Vous corrigez ainsi les erreurs de désignation de partition ou de chemin, avant qu'ils n'aient une influence négative sur le processus de démarrage. En appuyant sur (Enter), vous quittez le mode d'édition, revenez dans le menu et vous pouvez amorcer cette configuration avec (b). D'autres possibilités d'action sont indiquées dans le texte d'aide en bas.

Si vous voulez enregistrer de façon durable des options de démarrage modifiées et les faire parvenir au noyau, ouvrez en tant qu'utilisateur `root` le fichier `menu.lst` et ajoutez à la ligne existante les paramètres de noyau supplémentaires, séparés par un espace :

```
title linux
kernel (hd0,0)/vmlinuz root=/dev/hda3 <paramètre supplémentaire>
initrd (hd0,0)/initrd
```

GRUB prend en compte automatiquement le nouveau paramètre lors du prochain démarrage. Sinon, il est aussi possible de faire appel au module gestionnaire d'amorçage de YaST pour cette modification. Ici aussi, le nouveau paramètre est seulement rajouté à la ligne existante, séparé par un espace.

7.4.2 Le fichier device.map

Le fichier déjà mentionné `device.map` contientles correspondances entre les noms de périphériques de GRUB et de Linux. Si vous travaillez sur un système mixte avec des disques durs IDE et SCSI, GRUB doit essayer, à l'aide d'un processus défini, de déterminer la séquence d'amorçage. GRUB n'a pas accès aux informations du BIOS à ce sujet. GRUB enregistre le résultat de ce contrôle dans `/boot/grub/device.map`. Un exemple de fichier `device.map` pour un système exemple – en supposant que la séquence d'amorçage configurée dans le BIOS soit IDE avant SCSI – se présente ainsi :

```
(fd0)  /dev/fd0
(hd0)  /dev/hda
(hd1)  /dev/sda
```

Comme la séquence des disques IDE, SCSI et autres dépend de différents facteurs et que Linux ne peut reconnaître cet ordonnancement, il est possible de configurer la séquence manuellement dans `device.map`. Si vous avez des problèmes à l'amorçage, vérifiez que l'ordre dans ce fichier correspond à celui du BIOS et, si nécessaire, modifiez-le temporairement avec l'interpréteur de commandes de GRUB (voir la section *L'interpréteur de commandes (shell) GRUB* page suivante). Si le système Linux est amorcé, vous pouvez modifier de façon durable le fichier `device.map` avec le module du chargeur d'amorçage de YaST ou un éditeur de votre choix.

Après des modifications manuelles du fichier `device.map`, exécutez la commande suivante pour réinstaller GRUB. Le fichier `device.map` sera lu à nouveau et les commandes contenues dans `grub.conf` seront exécutées :

```
grub --batch < /etc/grub.conf
```

7.4.3 Le fichier /etc/grub.conf

Le troisième fichier de configuration important de GRUB outre `menu.lst` et `device.map` est `/etc/grub.conf`. Les paramètres et les options dont la commande `grub` a besoin pour installer correctement le chargeur d'amorçage y sont énumérés :

```
root (hd0,4)
install /grub/stage1 d (hd0) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
quit
```

La signification des différentes choix en détails :

root (hd0,4) Cette commande indique à GRUB de se référer pour les commandes suivantes à la première partition logique du premier disque dur sur lequel il trouve ses fichiers de démarrage.

install `parameter` La commande `grub` doit être démarrée avec le paramètre `install`. `stage1` en tant que premier niveau du gestionnaire d'amorçage doit être installé dans le MBR du premier disque dur (`/grub/stage1 d (hd0)`). `stage2` doit être chargé à l'adresse mémoire 0x8000 (`/grub/stage2 0x8000`). Le dernier élément `(hd0,4)/grub/menu.lst` indique à `grub` où se trouve le fichier menu.

7.4.4 L'interpréteur de commandes (shell) GRUB

GRUB existe en deux versions : en tant que gestionnaire d'amorçage, et en tant que programme Linux normal dans `/usr/sbin/grub`. Ce programme sera désigné par le terme *interpréteur de commandes (shell) GRUB*. Cette fonctionnalité permettant d'installer GRUB comme chargeur d'amorçage sur un disque dur ou sur une disquette est directement intégrée dans GRUB par le biais des commandes `install` ou `setup`. Elle est donc disponible dans l'interpréteur de commandes GRUB lorsque Linux est chargé.

Les commandes `install` et `setup` sont également disponibles *pendant* la procédure d'amorçage, sans que Linux ne soit nécessairement lancé. Ceci facilite le sauvetage d'un système défectueux (plus amorçable), étant donné que le fichier de configuration défectueux du chargeur d'amorçage peut être évité grâce à la saisie manuelle des paramètres. La saisie manuelle des paramètres au moment de l'amorçage est également intéressante pour tester les nouvelles configurations lorsque le système original ne doit pas être affecté. Entrez simplement les commandes de configuration expérimentales avec la même syntaxe que dans `menu.lst` ; testez la fonctionnalité de cette entrée sans modifier le fichier de configuration existant et donc sans affecter la capacité d'amorçage du système. Si vous souhaitez, par exemple, tester un nouveau noyau, saisissez la commande `kernel` avec le chemin d'accès au nouveau noyau. Si la procédure d'amorçage échoue, vous reprendrez la prochaine procédure d'amorçage avec le fichier `menu.lst` intact. De la même façon, l'interface ligne de commande peut servir à amorcer le système dans le cas inverse d'un fichier `menu.lst` défectueux en saisissant le paramètre corrigé à la ligne de commande. Une fois que le système fonctionne, corrigez ce paramètre dans `menu.lst`. Ainsi, le système est à nouveau amorçable.

L'algorithme d'association entre les périphériques de GRUB et les noms de périphériques de Linux n'entre en jeu que lorsque l'interpréteur de commandes GRUB est utilisé en tant que programme Linux (lancé avec la commande `grub` comme décrit, par exemple, dans la section *Le fichier device.map* page 215). Le programme lit alors le fichier `device.map`. Vous trouverez plus d'informations à ce sujet dans la section *Le fichier device.map* page 215.

7.4.5 Créer un mot de passe d'amorçage

GRUB prend déjà en charge au moment du démarrage l'accès au système de fichiers, c'est-à-dire que des utilisateurs sans droit de super-utilisateur peuvent accéder à des fichiers de votre système Linux auxquels ils n'auraient pas accès une fois le système démarré. Vous protégez de tels accès par un mot de passe. Vous pouvez soit interdire l'accès de personnes non autorisées au système de fichiers au moment du démarrage soit interdire aux utilisateurs le démarrage de certains systèmes d'exploitation.

Pour l'attribution d'un mot de passe de démarrage, procédez ainsi en tant qu'utilisateur `root` :

- Tapez la commande `grub` à l'invite root.
- Chiffrez le mot de passe dans l'interpréteur de commandes de GRUB :

```
grub> md5crypt
Password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

- Ajoutez la valeur chiffrée dans la section globale du fichier `menu.lst` :

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

  L'exécution de commandes de GRUB depuis l'invite d'amorçage est protégée. Cette possibilité n'est à nouveau autorisée qu'après avoir saisi (p) ainsi que le mot de passe. Le démarrage d'un système d'exploitation à partir du menu de démarrage reste possible pour tous les utilisateurs.
- Pour empêcher le démarrage d'un ou de plusieurs systèmes d'exploitation à partir du menu d'amorçage, ajoutez la ligne `lock` dans le fichier `menu.lst` pour chaque section ne devant pas être démarrée sans mot de passe. Ceci donnerait dans l'exemple :

```
title linux
kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
initrd (hd0,4)/initrd
lock
```

  Après un redémarrage du système et le chois de Linux dans le menu d'amorçage, le message d'erreur suivant apparaît tout d'abord :

```
Error 32: Must be authenticated
```

Appuyez sur (Enter) pour arriver au menu, puis sur (p) pour accéder à l'invite de mot de passe. Après avoir saisi le mot de passe et appuyé sur (Enter), le système d'exploitation désiré (dans ce cas Linux) est amorcé automatiquement.

Remarque

Mot de passe d'amorçage et écran de démarrage (splash screen)

Si vous utilisez un mot de passe d'amorçage pour GRUB, vous ne disposez pas de l'écran de démarrage habituel.

Remarque

7.5 Configuration du chargeur d'amorçage avec YaST

Avant de réaliser des changements dans la configuration du chargeur d'amorçage, familiarisez-vous à la théorie relative au processus d'amorçage. Le module YaST facilite en grande partie la configuration du chargeur d'amorçage.

Dans le centre de contrôle de YaST, sélectionnez le module 'Configuration du chargeur d'amorçage' sous 'Système'. Vous voyez alors apparaître la configuration actuelle du chargeur d'amorçage dans votre système et vous pouvez procéder à vos modifications (voir fig. 7.1 page suivante).

7.5.1 La fenêtre principale

Le champ de configuration (fond blanc) se divise en trois colonnes : la colonne de gauche ('Changé') sert au marquage des options modifiées qui apparaissent dans la colonne du milieu. Les valeurs actuelles se trouvent dans la colonne de la droite. Pour ajouter une nouvelle option, cliquez sur le bouton 'Ajouter'. Par contre, si vous souhaitez uniquement changer la valeur d'une option, sélectionnez celle-ci avec la souris puis cliquez sur 'Modifier'. Si vous ne voulez pas utiliser une option existante, sélectionnez-la puis cliquez sur 'Supprimer'.

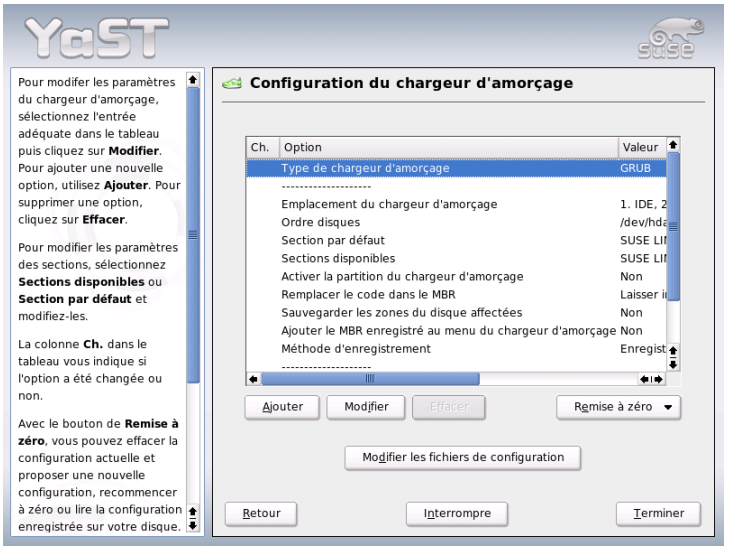


FIG. 7.1: *Configuration du chargeur d'amorçage avec YaST*

Sous la fenêtre de configuration, se trouve à droite la boîte combinée intitulée 'Réinitialisation' contenant les options suivantes :

Proposer une nouvelle configuration Le système crée une nouvelle proposition de configuration. Si pendant ce processus, des versions plus anciennes de Linux ou si d'autres systèmes sont trouvés sur d'autres partitions, ceux-ci seront intégrés au menu d'amorçage. Il est alors possible de sélectionner entre l'amorçage directe de Linux ou l'amorçage à travers le chargeur d'amorçage existant déjà. Dans ce cas, vous aurez un deuxième menu d'amorçage lors du démarrage.

Démarrer de zéro Cette option vous permet de créer votre propre configuration depuis le début sans aucune intervention ou suggestions.

Recharger la configuration depuis le disque
Si vous avez déjà procédé à quelques modifications et que celles-ci ne vous conviennent pas, cette option vous permet de revenir à la configuration actuellement enregistrée par votre système.

Proposer et fusionner avec des menus GRUB existants
Si un autre système d'exploitation et une version de Linux plus ancienne sont installés sur d'autres partitions, le menu sera composé d'une entrée pour le nouveau SUSE LINUX, une entrée pour l'autre système d'exploitation ainsi que toutes les entrées de l'ancien menu d'amorçage. Ce processus peut prendre un certain temps. Si vous utilisez LILO, cette option n'existe pas.

Restaurer le MBR depuis le disque dur
Avec cette option, vous reprenez le MBR enregistré sur le disque dur.

Sous cette boîte combinée, vous trouverez le bouton 'Modifier les fichiers de configuration' qui vous permet de modifier directement dans un éditeur les fichiers de configuration. Sélectionnez le fichier dans le champ de sélection pour l'éditer directement. Cliquez sur 'OK' et les changements seront enregistrés. Utilisez 'Annuler' pour sortir de la configuration du chargeur d'amorçage sans l'enregistrer et 'Retour' pour revenir à la fenêtre principale.

7.5.2 Options de la configuration du chargeur d'amorçage

La configuration avec YaST est beaucoup plus simple que la modification directe des fichiers. Sélectionnez une option avec la souris et cliquez sur 'Modifier'. Une fenêtre de dialogue apparaît dans laquelle vous pouvez procéder à des réglages individuels. Cliquez sur 'OK' pour confirmer les modifications et retourner à la fenêtre de dialogue principale dans laquelle vous pourrez modifier d'autres options. Ces options sont différentes selon le chargeur d'amorçage. Nous vous présentons ici quelques options importantes de GRUB :

Type de chargeur d'amorçage Avec cette option, vous pouvez passer de GRUB à LILO et réciproquement. Vous ouvrez ainsi un autre dialogue dans lequel vous pouvez spécifier le type de changement. Vous pouvez transformer la configuration de GRUB en une configuration LILO similaire, en risquant toutefois de perdre quelques informations au cas où il n'existerait pas d'options équivalentes. En outre, vous pouvez créer une configuration totalement nouvelle ou accepter une proposition que vous pourrez bien entendu modifier si vous le désirez.

Si vous démarrez la configuration du chargeur d'amorçage dans le système en fonctionnement, vous pouvez charger la configuration sur le disque dur. Néanmoins, si vous décidez de revenir au chargeur d'amorçage précédemment configuré, vous pouvez le charger à nouveau en utilisant la dernière option de cette configuration. Cependant, tout ceci n'est possible que tant que vous n'avez pas quitté le module du chargeur d'amorçage.

Emplacement du chargeur d'amorçage
Specifiez, dans cette fenêtre de dialogue, où le chargeur d'amorçage doit être installé : dans le secteur maître d'amorçage (MBR), dans le secteur d'amorçage de la partition d'amorçage (si elle existe déjà), dans le secteur d'amorçage de la partition root ou sur la disquette. Avec l'option 'Autres', vous pouvez choisir le lieu d'installation librement.

Ordre des disques durs Si vous disposez de deux ou plusieurs disques durs, indiquez ici l'ordre correspondant à celui de la configuration du BIOS.

Section par défaut Avec cette option, vous spécifiez le noyau ou système d'exploitation qui doit démarrer par défaut si vous ne faites aucune sélection dans le menu du chargeur d'amorçage. Une fois que le délai d'attente est passé, ce système sera amorcé automatiquement. En cliquant, dans ce menu, sur le bouton 'Modifier', vous verrez une liste de toutes les entrées du menu d'amorçage. Sélectionnez l'entrée souhaitée et activez-la en cliquant sur le bouton 'Definir comme standard'. Ici, vous avez aussi la possibilité de modifier une entrée en cliquant sur 'Changer'.

Sections disponibles Dans la fenêtre principale, cette option vous permet de voir quelles entrées de menu existent. Si vous sélectionnez cette option et cliquez sur 'Changer', vous ouvrirez le même dialogue qu'avec 'Section par défaut'.

Activer la partition du chargeur d'amorçage
Utilisez cette option pour activer la partition dont le secteur d'amorçage contient le chargeur d'amorçage, indépendamment de la partition dans laquelle se trouve le répertoire `/boot` ou `/` (root) contenant les fichiers du chargeur d'amorçage.

Remplacer le code dans le MBR Si vous aviez installé GRUB directement dans le secteur maître d'amorçage (MBR) ou si vous procédez à une installation sur un disque dur tout neuf et que vous ne souhaitiez plus installer GRUB dans le secteur maître d'amorçage, remettez en place le code d'amorçage générique à l'aide de cette option.

Sauvegarde des fichiers et zones du disque dur
Les zones du disque dur qui ont été modifiées sont sauvegardées.

Ajouter le MBR enregistré dans le menu du chargeur d'amorçage
Ajoute le MBR enregistré dans le menu du chargeur d'amorçage.

Dans la section inférieure, vous trouverez une option intéressante, le 'Timeout', qui définit le délai d'attente du chargeur d'amorçage (temps pendant lequel il attend que vous fassiez une sélection) avant le démarrage du système. Le bouton 'Ajouter' permet de spécifier toute une série d'autres options. Pour obtenir plus de détails quant aux options possibles, lisez les pages de manuel correspondantes (`man grub`, `man lilo`) et la documentation (en ligne) sur le site web `http://www.gnu.org/software/grub/manual/`.

7.6 Désinstallation du chargeur d'amorçage Linux

YaST procède pour vous à la désinstallation du chargeur d'amorçage Linux et à la restauration du MBR dans l'état antérieur l'installation de Linux. Lors de l'installation, YaST génère automatiquement une copie de sauvegarde du MBR original et, si vous le souhaitez, l'applique à nouveau écrasant ainsi GRUB.

Pour désinstaller GRUB, démarrez le module chargeur d'amorçage de YaST ('Système' → 'Configuration du chargeur d'amorçage'). Dans le premier dialogue, sélectionnez 'Remise à zéro' → 'Restaurer le MBR du disque dur' puis quittez le dialogue avec 'Terminer'. Dans le MBR, GRUB est maintenant écrasé avec les données du MBR d'origine.

7.7 Créer un CD-ROM d'amorçage

Si vous rencontrez des problèmes pour démarrer votre système installé avec un gestionnaire d'amorçage ou si vous ne souhaitez ou ne pouvez pas installer le chargeur d'amorçage dans le secteur maître d'amorçage (MBR) de votre disque dur ni sur une disquette, vous pouvez aussi préparer un CD-ROM amorçable sur lequel sont gravés les fichiers de démarrage de Linux. Votre ordinateur doit, bien entendu, disposer d'un graveur de CD-ROM correctement installé.

Pour créer un CD-ROM d'amorçage avec GRUB, vous n'avez besoin que de `stage2_eltorito`, une forme spéciale de *stage2* et éventuellement d'un `menu.lst` adapté à vos besoins qui n'est cependant pas nécessaire. Les fichiers classiques `stage1` et `stage2` ne sont pas nécessaires.

Créez un répertoire dans lequel l'image ISO doit être faite :

```
cd /tmp
mkdir iso
```

Créez un sous-répertoire pour GRUB dans `/tmp` :

```
mkdir -p iso/boot/grub
```

Copiez le fichier `stage2_eltorito` dans le répertoire `grub` :

```
cp /usr/lib/grub/i386-pc/stage2_eltorito iso/boot/grub
```

Copiez également le noyau (`/boot/vmlinuz`), `initrd` (`/boot/initrd`) et `/boot/message` dans `iso/boot/` :

```
cp /boot/message iso/boot/
cp /boot/vmlinuz iso/boot/
cp /boot/initrd iso/boot/
```

Pour que GRUB puisse trouver ces fichiers, copiez `menu.lst` dans `iso/boot/` et modifiez le chemin d'accès spécifié de façon à ce que les fichiers soient lus sur le CD. Pour cela, remplacez les noms de périphériques des disques durs (par exemple `(hd*)`) dans le chemin d'accès spécifié par le nom de périphérique du lecteur CD-ROM (`(cd)`) :

```
gfxmenu (cd)/boot/message
timeout 8
default 0

title Linux
    kernel (cd)/boot/vmlinuz root=/dev/hda5 vga=794 resume=/dev/hda1
splash=verbose showopts
    initrd (cd)/boot/initrd
```

Enfin, créez une image ISO9660 à l'aide de la commande suivante :

```
mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -o grub.iso iso
```

Gravez le fichier `grub.iso` résultant sur un CD avec le programme de votre choix.

7.8 Problèmes possibles et solutions

Cette section répertorie quelques uns de problèmes principaux qui peuvent surgir lors de l'amorçage avec GRUB. Les solutions possibles sont abordées. Pour certaines, vous trouverez un article dans la base de données support (`http://portal.suse.de/sdb/de/index.html`). Si votre problème n'est pas contenu dans cette liste, nous vous conseillons de faire une recherche dans la base de données support (`https://portal.suse.com/PM/page/search.pm`) avec les mots-clés "GRUB", "Amorcer", "Chargeur d'amorçage".

GRUB et XFS XFS ne laisse aucune place dans le bloc d'amorçage des partitions pour `stage1`. Il est donc important de ne pas choisir comme emplacement pour un chargeur d'amorçage une partition sur laquelle se trouve un XFS. Dans ce cas, il est bon de créer une partition d'amorçage séparée qui ne soit pas formatée avec XFS (voir ci-dessous).

GRUB et JFS Bien que techniquement possible, une combinaison de GRUB avec JFS est problématique. Dans ce cas, créez une partition d'amorçage séparée `/boot` et formatez-la avec Ext2. Installez GRUB dans cette partition.

GRUB indique une erreur "GRUB Geom Error"
GRUB ne contrôle la géométrie des disques durs rattachés qu'au moment de l'amorçage. Dans de rares cas, le BIOS donne ici des indications incohérentes, si bien que GRUB indique une erreur GRUB Geom Error. Dans de tels cas, utilisez LILO ou actualisez au besoin le BIOS. Vous trouverez des informations détaillées sur l'installation, la configuration et la maintenance de LILO dans la base de données support à l'aide du mot-clé LILO.

GRUB donne ce message d'erreur également lorsque Linux est installé dans le système sur un disque dur supplémentaire qui n'est pas enregistré dans le BIOS. La première partie du chargeur d'amorçage (*stage1*) est trouvée et chargée correctement mais la deuxième partie (*stage2*) n'est pas trouvée. La solution est alors d'enregistrer le nouveau disque dur dans le BIOS.

Le système mixte IDE-SCSI n'amorce pas
Il peut arriver que, lors de l'installation, YaST ait mal reconnu l'odre d'amorçage des disques durs (et que vous ne l'ayez pas corrigé). Ainsi, GRUB prendra, par exemple, `/dev/hda` comme `hd0` et `/dev/sda` comme `hd1` alors que dans le BIOS, c'est l'ordre inverse (SCSI *avant* IDE) qui est entré.

Dans ce cas, corrigez, lors de l'amorçage, les disques durs utilisés à la ligne de commande GRUB puis modifiez le fichier `device.map` dans le système amorcé afin de corriger l'attribution une bonne fois. Ensuite, vérifiez également les noms de périphériques GRUB dans les fichiers `/boot/grub/menu.lst` et `/boot/grub/device.map` et installer avec le chargeur d'amorçage à nouveau avec la commande suivante :

```
grub --batch < /etc/grub.conf
```

Amorcer Windows depuis le deuxième disque dur
Certains systèmes d'exploitation (par exemple, Windows) ne peuvent démarrer qu'à partir du premier disque dur. Lorsque vous avez installé un tel système d'exploitation sur un disque dur autre que le premier, vous pouvez exécuter un échange logique dans l'élément de menu correspondant.

```
...
title windows
   map (hd0) (hd1)
   map (hd1) (hd0)
   chainloader(hd1,0)+1
...
```

Ici, il faut démarrer Windows à partir du deuxième disque dur. Pour cela, la séquence logique des disques durs est modifiée avec `map`. Notez bien que durant cet échange, la logique du fichier du menu de GRUB n'est *pas* modifiée. Comme précédemment, vous devrez entrer le deuxième disque dur dans `chainloader`.

7.9 Informations complémentaires

Sur la page Web `http://www.gnu.org/software/grub/`, vous trouverez des informations détaillées sur GRUB en anglais.

Quand texinfo est installé sur l'ordinateur, vous pouvez afficher dans l'interpréteur de commandes avec `info grub` les pages Info relatives à GRUB. Recherchez aussi dans la base de données d'assistance `http://portal.suse.com/sdb/en/index.html` le mot-clé GRUB afin de trouver des informations sur des thèmes particuliers.

Le noyau Linux

Le noyau exploite le matériel du système Linux et le met à la disposition des différents processus. Dans les pages qui suivent, vous n'apprendrez pas à devenir un "bidouilleur" (*hacker*) du noyau, mais à mettre à jour le noyau et à compiler puis installer un noyau configuré par vos soins. Si vous procédez comme le décrit ce chapitre, le noyau précédent reste opérationnel et peut être amorcé à tout moment à la demande.

Le noyau placé lors de l'installation dans le répertoire `/boot` est configuré de manière à prendre en charge une gamme de matériel aussi étendue que possible. Il n'est généralement *pas nécessaire* de fabriquer votre propre noyau, sauf si vous voulez essayer des fonctionnalités ou des pilotes "expérimentaux".

Il est souvent possible de modifier le comportement du noyau installé à l'aide de paramètres de noyau. Par exemple, le paramètre `desktop` diminue les tranches de temps de l'ordonnanceur ce qui fait que le système est subjectivement plus rapide. Vous trouverez plus d'informations dans la documentation relative au noyau dans le répertoire `/usr/src/linux/Documentation` si le paquetage `kernel-source` est installé.

Pour produire un nouveau noyau, il existe déjà des `Makefiles` permettant d'automatiser l'opération presque complètement. Seul le choix du matériel et des fonctionnalités que le noyau gérera doit être effectué de manière interactive. Puisque vous devez connaître votre système informatique suffisamment bien pour faire un choix viable, nous recommandons – au moins pour les premiers essais – de modifier un fichier de configuration existant et opérationnel et diminuer ainsi le risque de réglages incorrects.

8.1 Mise à jour du noyau

Pour installer une mise à jour du noyau SUSE, téléchargez le paquetage de mise à jour depuis le serveur FTP de SUSE ou sur un miroir comme par exemple `ftp://ftp.gwdg.de/pub/linux/suse/`. Si vous ne savez pas quel noyau vous avez actuellement, vous pouvez par exemple regarder la chaîne du numéro de version : `cat /proc/version`.

Vous pouvez aussi vérifier à quel paquetage appartient le noyau `/boot/vmlinuz` : `rpm -qf /boot/vmlinuz`.

Avant l'installation, vous devriez sauvegarder le noyau d'origine et le fichier `initrd` correspondant. Lancez pour ce faire les deux commandes suivantes en tant que `root` :

```
cp /boot/vmlinuz-$(uname -r) /boot/vmlinuz.old
cp /boot/initrd-$(uname -r) /boot/initrd.old
```

Installez alors le nouveau paquetage avec la commande `rpm -Uvh <NomDuPaquetage>`. Veillez à utiliser le bon numéro de version.

Depuis la version 7.3 de SUSE LINUX, reiserfs est le système de fichiers par défaut, ce qui suppose de mettre en œuvre un "disque virtuel initial". Celui-ci est créé avec la commande `mk_initrd`. Les versions actuelles de SUSE LINUX permettent de réaliser cette opération automatiquement lors de l'installation du noyau.

Pour pouvoir amorcer l'ancien noyau le cas échéant, il faut configurer en conséquence le chargeur d'amorçage. Vous trouvez des informations précises à ce sujet dans le chapitre *Amorçage et chargeur d'amorçage* page 205.

Si vous souhaitez installer le noyau original à partir des CD de SUSE, procédez de façon analogue. Sur le CD 1 ou le DVD, vous trouverez le noyau par défaut dans le répertoire `boot` sous la forme d'un paquetage rpm. Installez-le comme décrit précédemment. Si vous obtenez un message d'erreur indiquant qu'un paquetage plus récent est déjà installé, ajoutez l'option `--force` à la commande rpm.

8.2 Les sources du noyau

La compilation d'un noyau exige l'installation de ses sources (paquetage `kernel-source`). D'autres paquetages nécessaires comme le compilateur C (paquetage `gcc`), les utilitaires binaires GNU (paquetage `binutils`) et les fichiers à inclure du compilateur C (paquetage `glibc-devel`) sont de plus choisis automatiquement.

Une fois l'installation terminée, les sources du noyau se trouvent dans le répertoire `/usr/src/linux-<version-noyau>`. Si vous projetez de faire des tests avec le noyau et d'en maintenir différentes versions en même temps sur votre disque, il est proposé de décompacter les diverses versions dans différents répertoires et d'accéder immédiatement aux sources pertinentes au moyen d'un lien, puisqu'il existe des paquetages logiciels qui s'attendent à trouver les sources du noyau dans le répertoire `/usr/src/linux`. YaST s'occupe automatiquement de ce type d'installation.

8.3 Configuration du noyau

La configuration du noyau en cours d'exécution est enregistrée dans le fichier `/proc/config.gz`. Pour adapter cette configuration à vos souhaits, allez en tant qu'utilisateur `root` dans le répertoire `/usr/src/linux` et lancez les commandes suivantes :

```
zcat /proc/config.gz > .config
make oldconfig
```

La commande `make oldconfig` utilise le fichier `/usr/src/linux/.config` comme base de la configuration du noyau actuelle. Lorsque de nouvelles options apparaissent dans le noyau courant, elles peuvent alors être choisies ou non.

Lorsque le fichier `.config` est absent, une configuration par défaut contenue dans les sources du noyau est utilisée.

8.3.1 Configuration depuis la ligne de commande

Pour configurer le noyau, allez dans le répertoire `/usr/src/linux` et saisissez la commande `make config`.

Vous devrez alors répondre à une série de questions sur les fonctionnalités système que le noyau doit assurer. Deux ou trois possibilités s'offrent normalement à vous lorsque vous répondez aux questions : soit simplement (y) et (n), soit une des trois possibilités (y) (*yes* - oui), (n) (*no* - non) et (m) (module). `m` signifie dans ce cas que le pilote correspondant n'est pas lié physiquement au noyau, mais plutôt compilé sous forme de module qui peut être chargé dans le noyau pour la durée de son exécution. Tous les pilotes qui sont absolument nécessaires à l'amorçage du système doivent être liés physiquement au noyau ; vous choisirez donc dans ce cas (y). Avec (Entrée), confirmez la présélection présente dans le fichier `.config`. Si vous appuyez sur une autre touche lors d'une question, vous obtenez l'affichage d'un court texte d'aide sur l'option concernée.

8.3.2 Configuration en mode texte

La configuration du noyau peut se faire de manière plus attrayante avec "menuconfig" ; pour ce faire, vous devrez éventuellement installer avec YaST le paquetage `ncurses-devel`. Démarrez la configuration du noyau avec la commande `make menuconfig`.

Lors d'une légère modification de la configuration, vous ne devez pas "essayer" toutes les questions, mais le menu vous permet de choisir directement certaines zones.Les préréglages sont tirés du fichier `.config`. Pour charger une autre configuration, choisissez dans le menu 'Charger un autre fichier de configuration' et indiquez le nom du fichier.

8.3.3 Configuration avec le système X Window

Si vous avez installé le Système X Window (paquetage `xorg-x11`) ainsi que les paquetages de développement QT (`qt3-devel`), vous pouvez aussi choisir de lancer la configuration au moyen de la commande `make xconfig`.

Vous obtenez alors une interface graphique qui rend la configuration plus confortable. Pour ce faire, vous devrez toutefois démarrer le Système X Window en tant que `root` ou saisir d'abord `xhost +` dans l'interpréteur de commandes en tant qu'utilisateur normal, pour que `root` puisse l'accéder à l'affichage. Les préréglages sont lus dans le fichier `.config`. Tenez compte du fait que la configuration au moyen de `make xconfig` n'est pas aussi bien maintenue que les autres possibilités de configuration. Vous devrez donc toujours exécuter un `make oldconfig` supplémentaire après cette l'utilisation de cette méthode.

8.4 Modules du noyau

Les composants matériels des PCs sont variés. Pour pouvoir les utiliser correctement, vous aurez besoin d'un "pilote" qui permettra au système d'exploitation (grâce au "noyau" Linux) de communiquer correctement avec le matériel. Il y a généralement deux mécanismes pour intégrer des pilotes au noyau :

- Les pilotes peuvent être compilés physiquement dans le noyau. Dans ce guide, de tels noyaux "d'un seul bloc" sont qualifiés de noyaux *monolithiques*. Certains pilotes ne peuvent être utilisés que sous cette forme.
- Les pilotes peuvent n'être chargés qu'en fonction des besoins dans le noyau que l'on qualifie dans ce cas de noyau *modulaire*. L'avantage est que seuls les pilotes nécessaires sont chargés et que le noyau ne contient aucun élément inutile.

Lors de la configuration du noyau, on établit quels pilotes sont liés physiquement au noyau et lesquels sont placés dans des modules. Tous les composants du noyau qui ne sont pas impérativement nécessaires au cours du processus d'amorçage devraient être mis sous forme de modules. On s'assure ainsi que le noyau n'est pas trop volumineux et qu'il peut être chargé sans difficulté à partir du BIOS et de n'importe quel gestionnaire d'amorçage. Le pilote du disque dur, la gestion d'`ext2` et d'autres fonctionnalités similaires doivent donc en principe être directement compilés au sein du noyau. La prise en charge d'`isofs`, de `msdos` ou du son (`sound`) devraient toujours être compilées sous forme de modules.

Les modules du noyau se trouvent dans le répertoire `/lib/modules/<Version>`, où `Version` correspond à la version actuelle du noyau.

8.4.1 Reconnaissance du matériel actuel avec hwinfo

Le programme hwinfo à votre disposition sous SUSE LINUX permet de reconnaître le matériel actuellement présent sur l'ordinateur et d'y affecter les pilotes disponibles. La commande `hwinfo --help` vous offre un court paragraphe d'aide. Par exemple, pour obtenir des informations sur les périphériques SCSI installés, saisissez la commande suivante :

```
hwinfo --scsi
```

L'affichage de cet utilitaire est également à votre disposition dans YaST dans le module Informations sur le matériel.

8.4.2 Manipulation des modules

Les commandes suivantes permettent de manipuler les modules :

`insmod` Le module indiqué est chargé à l'aide de la commande `insmod`. Puis il est cherché dans un sous-répertoire de `/lib/modules/<Version>`. `insmod` *ne* devrait *plus* être utilisé, au profit de `modprobe` (voir ci-dessous).

`rmmod` Le module indiqué est déchargé. Cela n'est bien sûr possible que si la fonctionnalité correspondante du noyau n'est plus utilisée. Par conséquent, il n'est pas possible de décharger le module `isofs` lorsqu'un un CD est encore monté.

depmod Cette commande crée un fichier portant le nom `modules.dep` dans le répertoire `/lib/modules/<Version>`, dans lequel sont enregistrées les dépendances mutuelles des divers modules. On s'assure ainsi que lors du chargement d'un module, tous les modules qui en dépendent sont également chargés automatiquement. S'il n'existe pas encore, le fichier contenant les dépendances des modules est généré au démarrage du système.

modprobe Chargement et/ou déchargement d'un module avec prise en compte des dépendances d'autres modules. Cette commande est très puissante et permet d'atteindre de nombreux autres objectifs (par exemple, pour essayer tous les modules d'un certain type, jusqu'à pouvoir réussir à charger l'un d'entre eux). Contrairement au chargement au moyen d'insmod, modprobe analyse le fichier `/etc/modprobe.conf` et on devrait donc en principe l'employer pour charger des modules. Pour obtenir une explication détaillée de toutes les possibilités, consultez les pages de manuel appropriées.

lsmod Cette commande indique quels sont les modules actuellement chargés et par combien d'autres modules ils sont utilisés. Les modules qui ont été chargés par le démon du noyau sont identifiés par le `autoclean` qui le suit alors. `autoclean` attire l'attention sur le fait que ces modules seront automatiquement retirés s'ils restent inutilisés pendant un certain temps et si l'on a pris des mesures en conséquence ; reportez-vous à la section *Kmod – le chargeur de modules du noyau* page suivante.

modinfo Affiche des informations sur un module. Étant donné que ces informations sont extraites du module, seules les informations qui ont été intégrées par les développeurs du pilote pourront être affichées. Les informations contenues sont l'auteur, une description, la licence, les paramètres de module, les dépendances et les alias.

8.4.3 /etc/modprobe.conf

Le chargement des modules est influencé par les fichiers `/etc/modprobe.conf` et `/etc/modprobe.conf.local`, ainsi que par le répertoire `/etc/modprobe.d` ; reportez-vous à la page de manuel `man modprobe.conf`. On trouve également dans ce fichier les paramètres des modules qui accèdent directement au matériel et doivent donc être ajustés en fonction d'un système particulier (par exemple le pilote du lecteur CD-ROM ou le pilote réseau). Les paramètres enregistrés à cet endroit sont décrits dans les sources du noyau. Installez le paquetage `kernel-source` et lisez la documentation contenue dans le répertoire `/usr/src/linux/Documentation`.

8.4.4 Kmod – le chargeur de modules du noyau

Lorsqu'on utilise des modules du noyau, la méthode la plus élégante consiste à mettre en œuvre le "chargeur de modules du noyau". Kmod veille en arrière-plan à ce que les modules nécessaires soient automatiquement chargés au moyen d'appels à modprobe dès que l'on accède à la fonctionnalité correspondante du noyau.

Pour pouvoir utiliser Kmod, cochez l'option 'Chargeur de modules du noyau' (`CONFIG_KMOD`) lors de la configuration du noyau. L'application Kmod n'est pas conçue pour décharger automatiquement des modules ; grâce à l'équipement actuel en mémoire vive (RAM) des ordinateurs, le gain de mémoire centrale ne serait qu'accessoire. Les serveurs qui ont des tâches spéciales à accomplir et ne nécessitent que peu de pilotes préféreront un noyau "monolithique" pour des raisons de performances.

8.5 Réglages lors de la configuration du noyau

Il n'est pas possible de représenter ici en détail les diverses possibilités de configuration du noyau. Faites appel à la pléthore de fichiers d'aide qui existent sur le sujet. La version la plus récente de la documentation se trouve toujours dans le répertoire `/usr/src/linux/Documentation`, pour autant que le paquetage `kernel-source` soit installé.

8.6 Compilation du noyau

Nous recommandons de générer une "bzImage". Ainsi, on peut en général éviter que le noyau ne devienne "trop volumineux", comme cela peut facilement se produire lorsqu'on choisit trop de fonctionnalités et qu'on crée une "zImage" (les messages typiques sont alors "kernel too big" ou "System is too big").

Après avoir configuré le noyau en fonction de vos besoins, démarrez la compilation (dans le répertoire `/usr/src/linux/` :

```
make clean
make bzImage
```

Vous pouvez également saisir ces deux commandes sur une seule ligne de commande :

```
make clean bzImage
```

Après une compilation réussie, vous trouverez le noyau comprimé dans `/usr/src/linux/arch/<arch>/boot`. L'image du noyau – le fichier qui contient le noyau – s'appelle `bzImage`.

Si vous ne trouvez pas ce fichier, il est très probable qu'une erreur est apparue au cours de la compilation du noyau. Si vous êtes sous Bash, vous pouvez avec :

```
make bzImage 2> &1 | tee kernel.out
```

démarrer à nouveau le processus de compilation et en obtenir un "enregistrement simultané" dans le fichier `kernel.out`.

Si vous avez configuré des parties du noyau sous forme de modules pouvant être chargés, vous devez ensuite passer à la compilation de ces modules. Utilisez pour ce faire la commande `make modules`.

8.7 Installer un noyau

Après avoir compilé le noyau, vous devez installer ce nouveau noyau de façon à pouvoir l'amorcer à l'avenir.

Le noyau doit maintenant être installé dans `/boot`. Vous y parvenez à l'aide de la commande suivante :

```
INSTALL_PATH=/boot make install
```

Les modules compilés doivent encore être installés ; vous pouvez en faire une copie dans les répertoires cibles appropriés dans le répertoire `/lib/modules/<Version>` grâce à la commande `make modules_install`. Les anciens modules de la même version de noyau sont écrasés, mais vous pouvez réinstaller les modules et le noyau d'origine à partir des CD.

Remarque

Veillez à ce que les modules éventuels correspondants à des fonctionnalités que vous venez de compiler directement dans le noyau aient été retirés du répertoire `/lib/modules/<Version>`. Sinon, des effets imprévisibles peuvent se produire ! C'est une des raisons pour lesquelles il est *formellement* déconseillé aux utilisateurs inexpérimentés de compiler le noyau.

Remarque

Afin queGRUB puisse amorcer l'ancien noyau (désormais `/boot/vmlinuz.old`), ajoutez dans le fichier `/boot/grub/menu.lst` une nouvelle image d'amorçage intitulée `Linux.old`. Cette procédure est décrite en détail dans le chapitre *Amorçage et chargeur d'amorçage* page 205. GRUB ne nécessite pas de nouvelle installation.

Ce paragraphe mérite toute votre attention : le fichier `/boot/System.map` contient les symboles du noyau dont les modules ont besoin pour pouvoir appeler correctement les fonctions du noyau. Ce fichier est dépendant du noyau actuel. C'est pourquoi, après la compilation et l'installation du noyau, vous devriez copier le nouveau fichier `/usr/src/linux/System.map` dans le répertoire `/boot`. Ce fichier sera à nouveau généré à chaque compilation du noyau.

Si lors de l'amorçage, vous deviez recevoir un message d'erreur comme "System.map does not match actual kernel", il est alors probable que le fichier `System.map` n'a pas été copié dans `/boot` après la compilation du noyau.

8.8 Faire le ménage sur le disque dur après la compilation

Si vous avez des problèmes d'espace disque, vous pouvez supprimer les fichiers objets produits pendant la compilation du noyau :

```
cd /usr/src/linux
make clean
```

Si toutefois vous disposez de l'espace disque suffisant et prévoyez de configurer à nouveau le noyau à maintes reprises, ignorez cette dernière étape. Une nouvelle compilation du noyau est alors beaucoup plus rapide, puisque seules les parties concernées par les modifications correspondantes.sont à nouveau compilées.

Particularités du système

Vous trouverez dans ce chapitre des informations sur les différents paquetages logiciels ainsi que sur les consoles virtuelles et l'assignation des touches. En conclusion, vous trouverez une section consacrée aux adaptations locales et linguistiques (I18N/L10N).

9.1 Remarques sur certains paquetages logiciels

9.1.1 Les paquetages bash et /etc/profile

Le programme bash évalue dans cet ordre les fichiers d'initialisation lorsqu'il est appelé comme interpréteur de commandes à la connexion (shell de login) :

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Les utilisateurs peuvent ajouter leurs propres lignes dans `~/.profile` ou dans `~/.bashrc`. Pour modifier ces fichiers comme il se doit, il est indispensable de recopier les paramètres de base de `/etc/skel/.profile` et de `/etc/skel/.bashrc` dans le répertoire utilisateur. Il est donc recommandé, après avoir effectué une mise à jour, de copier la configuration à partir de `/etc/skel`. Exécutez les commandes suivantes depuis un terminal afin de conserver une copie des modifications que vous avez réalisées :

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Vous reporterez ensuite à partir des fichiers `*.old` les modifications que vous avez apportées.

9.1.2 Le paquetage cron

Les tables `cron` se trouvent dans `/var/spool/cron/tabs`. Le fichier `/etc/crontab` sert de planificateur horaire pour tout le système. Ce fichier indique à quelle heure une commande s'exécute ainsi que sous quel utilisateur (voir le listing 9.1 page ci-contre, dans lequel l'utilisateur en question est `root`). Des tables organisées sur le même modèle et se rattachant à un paquetage en particulier se trouvent dans le répertoire `/etc/cron.d` – voir la page de manuel `man cron`.

Exemple 9.1: *Exemple de déclaration dans /etc/crontab*

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Le fichier `/etc/crontab` *ne peut pas* être édité à l'aide de la commande `crontab -e` mais il doit être chargé directement dans un éditeur pour y recevoir les modifications prévues et y être enregistré.

Un certain nombre de paquetages installent dans les répertoires `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` et `/etc/cron.monthly` des scripts shell gérés par `/usr/lib/cron/run-crons`. Toutes les 15 minutes, la table principale (`/etc/crontab`) appelle `/usr/lib/cron/run-crons`, ce qui permet de rattraper éventuellement les étapes qui n'ont pas pu être traitées à temps.

Pour plus de clarté, les travaux de maintenance exécutés quotidiennement sur le système sont répartis sur plusieurs scripts (paquetage `aaa_base`). Ainsi, le répertoire `/etc/cron.daily` comporte à côté de `aaa_base` par exemple les composants `backup-rpmdb`, `clean-tmp` ou `clean-vi`.

9.1.3 Fichiers journaux — le paquetage logrotate

De nombreux services système ("démons") ainsi que le noyau lui-même enregistrent régulièrement l'état du système et d'éventuels incidents dans des fichiers journaux (*logfiles*). L'administrateur peut ainsi déterminer de façon fiable dans quel état le système se trouvait à un instant donné, identifier les erreurs ou les dysfonctionnements et réagir de façon appropriée. Ces fichiers journaux se trouvent, conformément au standard FHS, dans le répertoire `/var/log` et grossissent de jour en jour. On peut contrôler la croissance de ces fichiers à l'aide de `logrotate`.

Configuration

Le fichier de configuration `/etc/logrotate.conf` définit le comportement d'ensemble. La directive `include` permet de nommer les fichiers supplémentaires devant être chargés. Il est prévu que les différents paquetages de SUSE LINUX installent des fichiers dans `/etc/logrotate.d`. (par exemple `syslog` et YaST procèdent ainsi).

Exemple 9.2: *Exemple de fichier /etc/logrotate.conf*

```
# see "man logrotate" for details
# rotate log files weekly weekly
# keep 4 weeks worth of backlogs rotate 4
# create new (empty) log files after rotating old ones create
# uncomment this if you want your log files compressed
#compress
# RPM packages drop log rotation information into this directory
include /etc/logrotate.d
# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}
# system-specific logs may be also be configured here.
```

logrotate lui-même est contrôlé par cron et déclenché quotidiennement par `/etc/cron.daily/logrotate`.

Remarque

L'option `create` lit les préférences éventuelles de l'administrateur dans les fichiers `/etc/permissions*`. Assurez-vous que cela n'entre pas en conflit avec vos réglages.

Remarque

9.1.4 Les pages de manuel

Un certain nombre de programmes GNU (par exemple tar) ne tiennent plus à jour de pages de manuel. Celles-ci ont été remplacées par une présentation rapide appelée par l'option `--help` ainsi que par des fichiers Info détaillés. Le programme info constitue le système hypertexte du système GNU. La commande `info info` donne accès à une première aide à l'utilisation ; la commande info peut être appelée depuis Emacs en exécutant `emacs -f info` ou bien directement à l'aide de la commande `info`. Les applications tkinfo, xinfo ou l'accès au système d'aide en ligne sont des alternatives conviviales.

9.1.5 La commande locate

locate, qui permet de trouver rapidement des fichiers, ne fait pas partie des logiciels installés par défaut. Si vous souhaitez l'utiliser, vous devrez l'installer (`find-locate`) — le processus updatedb sera alors démarré quotidiennement de façon automatique, la nuit ou environ 15 minutes après le démarrage.

9.1.6 La commande ulimit

La commande `ulimit` (*user limits*) permet de fixer des limites à l'utilisation des ressources système ou d'afficher ces dernières. ulimit est utilisé notamment pour limiter la mémoire allouée aux applications. Ainsi, on peut éviter qu'une application ne monopolise la majeure partie ou la totalité de la mémoire et ne gèle le système.

Le programme ulimit peut être appelé avec différentes options. C'est ainsi que les options présentées dans la table 9.1 permettent par exemple de restreindre l'utilisation de la mémoire.

TAB. *9.1:* *ulimit : configuration des ressources de l'utilisateur*

`-m`	Taille maximale de la mémoire physique
`-v`	Taille maximale de la mémoire virtuelle
`-s`	Taille maximale de la pile
`-c`	Taille maximale des fichiers Core (de vidage mémoire)
`-a`	Affichage des limites fixées

La configuration peut être définie pour tous les utilisateurs dans le fichier `/etc/profile`. Il est nécessaire par exemple d'y activer la création de fichiers Core dont les programmeurs ont besoin pour le "débogage". Les utilisateurs ne sont pas autorisés à augmenter les valeurs fixées par l'administrateur système dans `/etc/profile`. Ils peuvent toutefois saisir des paramètres particuliers dans leur propre fichier `~/.bashrc`.

Exemple 9.3: *Paramètres ulimit dans /.bashrc*

```
# Limitation de la mémoire réelle
ulimit -m 98304

# Limitation de la mémoire virtuelle
ulimit -v 98304
```

La mémoire doit être exprimée en Ko. Pour plus de précisions, reportez-vous à la page de manuel `man bash`.

Remarque

Tous les interpréteurs de commandes (shells) ne prennent pas en charge les valeurs `ulimit`. Dans le cas où vous auriez besoin de définir des paramètres globaux fixant ces limitations, vous pouvez utiliser PAM (par exemple `pam_limits`) qui offre des possibilités de configuration avancées.

Remarque

9.1.7 La commande free

La commande `free` prête quelque peu à confusion lorsqu'il s'agit de déterminer comment la mémoire vive est utilisée à un moment donné… on trouve ces informations dans `/proc/meminfo`. De nos jours, cela ne devrait préoccuper aucun utilisateur d'un système d'exploitation moderne comme Linux. Le concept de "mémoire vive disponible" remonte à l'époque où la gestion unifiée de la mémoire (*unified memory management*) n'existait pas encore – Le slogan "La mémoire disponible est de la mauvaise mémoire" (*Free memory is bad memory*) s'applique bien à Linux. Par la suite, Linux s'est toujours efforcé de trouver un équilibre entre les caches sans jamais accepter la présence de mémoire réellement libre (c'est-à-dire inutilisée).

Le noyau n'a aucune idée des programmes ou des données utilisateurs. Il gère les programmes et les données utilisateurs dans la "mémoire cache". Lorsque la mémoire commence à être saturée, une partie est écrite dans la zone de mémoire d'échange (swap) ou dans des fichiers à partir desquels ils ont été initialement lus à l'aide de l'appel système `mmap` ; voir à ce sujet la page de manuel `mmap`.

À côté de cela, le noyau utilise également des zones de mémoire caches supplémentaires, comme le *slab cache*, qui contient par exemple les caches utilisés pour l'accès réseau. C'est ce qui permet d'expliquer les éventuelles différences entre les valeurs dans `/proc/meminfo`. Pratiquement tous ces caches sont référencés dans `/proc/slabinfo`.

9.1.8 Le fichier /etc/resolv.conf

La résolution de noms est gérée par l'intermédiaire du fichier `/etc/resolv.conf` ; voir la section *DNS – Domain Name System* page 487 . Ce fichier est actualisé par le script `/sbin/modify_resolvconf` exclusivement. Aucun autre programme n'est autorisé à manipuler directement le fichier `/etc/resolv.conf`. Cette règle doit être respectée pour assurer la cohérence entre la configuration réseau et les données associées.

9.1.9 Configuration de GNU Emacs

GNU Emacs est un environnement complexe. Pour de plus amples informations, consultez le lien `http://www.gnu.org/software/emacs/`.

Dans les paragraphes suivants, on passe en revue les fichiers de configuration sur lesquels GNU Emacs se base au démarrage. Au démarrage, Emacs lit plusieurs fichiers contenant les réglages de l'utilisateur, de l'administrateur système et du distributeur pour s'adapter et se préconfigurer en fonction de leurs besoins respectifs.

Le fichier d'initialisation `~/.emacs` est installé, pour chaque utilisateur, à partir de `/etc/skel` dans le répertoire personnel ; Le fichier `.emacs` charge à son tour le fichier `/etc/skel/.gnu-emacs`. Si l'utilisateur souhaite lui même apporter des modifications, il est conseillé de copier ce fichier `.gnu-emacs` dans son répertoire personnel puis de procéder aux réglages souhaités :

```
cp /etc/skel/.gnu-emacs ~/.gnu-emacs
```

Dans `.gnu-emacs`, le fichier `~/.gnu-emacs-custom` est répertorié comme `custom-file`. Si l'utilisateur ayant les privilèges `customize` modifie la configuration, ses modifications seront enregistrées sous `~/.gnu-emacs-custom`.

Sous SUSE LINUX, avec le paquetage `emacs`;le fichier `site-start.el` est installé dans le répertoire `/usr/share/emacs/site-lisp`. Le fichier `site-start.el` est chargé *avant* le fichier d'initialisation `~/.emacs`. Le fichier `site-start.el` permet entre autres de charger certains fichiers de configuration installés avec des paquetages Emacs additionnels de la distribution (par exemple le paquetage `psgml`). De tels fichiers de configuration se trouvent également dans le répertoire`/usr/share/emacs/site-lisp` et commencent toujours par `suse-start-`.

L'administrateur système local peut enregistrer des réglages s'appliquant à tousles utilisateurs dans le fichier `default.el`. Pour plus d'informations, consultez le fichier info d'Emacs à la section `Init File` : `info:/emacs/InitFile`. Il y est notamment décrit comment empêcher le chargement de ce fichier — si besoin est.

Les composants d'Emacs sont répartis dans plusieurs paquetages :

- Paquetage de base `emacs`
- On installe en général en plus le paquetage `emacs-x11` dans lequel figure le programme *avec* la prise en charge de X11.
- Le paquetage `emacs-nox` contient le programme *sans* la prise en charge de X11.
- Le paquetage `emacs-info` contient de la documentation en ligne au format Info.
- Le paquetage `emacs-el` contient les fichiers de bibliothèque non compilés en Lisp Emacs — ce paquetage n'est pas nécessaire à l'exécution !
- De nombreux paquetages supplémentaires peuvent être installés si besoin est : le paquetage `emacs-auctex` (pour LaTeX) ; `psgml` (pour SGML/XML) ; `gnuserv` (pour l'utilisation en mode client/serveur), etc.

9.1.10 Brève initiation au vi

Pour beaucoup de travaux sur le système, mais également pour des travaux de programmation, on utilise encore aujourd'hui des éditeurs de texte. Dans le domaine Unix, le vi s'est au fil du temps imposé comme étant l'éditeur qui, en plus des fonctions confortables d'édition, laisse en outre question ergonomie beaucoup d'éditeurs dans l'ombre, et est utilisé avec la souris.

Commutation entre les modes : Insert, Command, et Extended Mode

On différencie en principe dans le vi trois différents modes de fonctionnement ; le mode *Insert*, le mode *Command* et le mode *Extended*.

Ce qui est le plus déconcertant pour les débutants est le fait que les touches ont des effets très différents selon le mode. Nous vous présentons tout d'abord une méthode courante de commutation entre les modes. Après le démarrage, le vi est normalement en mode *Command*.

Du mode Command vers le mode Insert
Il existe ici une grand nombre de possibilités. L'utilisation courante est : a comme append, i comme insert, ou o pour une nouvelle ligne sous la ligne actuelle.

Du mode Insert vers le mode Command
Pour quitter le mode *Insert*, vous avez besoin de la touche (ESC).
Dans le mode *Insert*, il n'est pas possible d'arrêter le vi. C'est pourquoi il est important de garder (ESC) en mémoire.

Du mode Command vers le mode Extended
Le mode *Extended* du vi peut être atteint via les deux-points placés devant. Le mode Extended, appelé aussi mode *ex* correspond à un propre éditeur fonctionnant ligne par ligne. Vous pouvez, à l'aide de ce mode, effectuer des tâches multiples et compliquées.

Du mode Extended vers le mode Command
Après l'exécution d'une commande dans le mode *Extended*, on se trouve en principe à nouveau dans le mode *Command*. Si on ne veut finalement exécuter aucune commande dans le mode *Extended*, on peut, à l'aide de la touche de retour en arrière, à nouveau effacer les deux-points, et on revient alors également au mode *Command*.

Notez qu'une commutation du mode *Insert* vers le mode *Extended* nécessite toujours le passage intermédiaire dans le mode *Command*. Il n'est pas prévu de commutation directe.

Il est souvent difficile pour les débutants de quitter à nouveau un nouvel éditeur. Le vi ne fait pas exception dans ce cas. Ce qui est important ici, c'est qu'on ne pas quitter le vi en mode *Insert*. Vous devez donc d'abord quitter le mode *Insert* avec la touche (ESC). Puis, on différencie deux cas de figure :

1. *Quitter sans enregistrer :* si vous désirez quitter l'éditeur sans sauvegarder les modifications, alors entrez dans le mode *Command* la combinaison de touches (:)(Q)(!). Le (!) a pour effet que vi ignore les modifications effectuées.

2. *Quitter et enregistrer :* pour sauvegarder les modifications et ensuite quitter l'éditeur, vous disposez de plusieurs possibilités. Dans le mode *Command*, vous disposez de la commande (Shift) (Z) (Z). Notez que, dans les listes de commandes courantes, la touche (Shift) n'est pas mentionnée puisque le (Z) majuscule implique déjà la touche (Shift).

   Conformément à l'arrêt sans enregistrement, vous disposez également d'une commande *Extended*. La combinaison de touches est alors (:) (W) (Q).

Comme vous pouvez aisément le comprendre, dans le mode *Extended* (W) signifie "write" (écrire) et (Q) veut dire "quit" (quitter).

Le vi dans la vie de tous les jours

Le vi peut être utilisé comme un éditeur tout à fait normal. Dès que vous êtes en mode *Insert*, vous pouvez entrer le texte et à l'aide de la touche de retour en arrière et d'effacement, il est également possible d'effacer du texte. Pour bouger le curseur, vous pouvez utiliser les touches de contrôle du curseur.

Mais on est souvent confronté à des problèmes, justement avec ces touches de commande. Ceci provient du fait qu'il existe un grand nombre de types de terminaux différents qui utilisent chacun des codes de touches qui leur sont propres. C'est à ce moment qu'entre en jeu le mode *Command*.

Appuyez sur la touche (ESC) pour commuter du mode *Insert* vers le mode Command. Dans le mode *Command*, vous pouvez également faire bouger le curseur avec les touches (H), (J), (K) et (L). Ces touches signifient :

(H) un caractère vers la gauche

(J) une ligne vers le bas

(K) une ligne vers le haut

(L) un caractère vers la droite

Les commandes en mode *Command* du vi connaissent diverses variations. Si vous désirez exécuter plusieurs fois une commande, vous pouvez entrer simplement sous forme de chiffre le nombre de répétitions, et ensuite appeler la commande voulue. Donc, si vous entrez la séquence de commande (5) (L), le curseur bougera de cinq caractères vers la droite.

Informations supplémentaires

Le vi connaît énormément de commandes. On peut lui écrire des macros, on peut utiliser des raccourcis, il existe ce qu'on appelle des tampons, et beaucoup d'autres choses utiles. Les décrire ici en détails nous mènerait trop loin. Une version améliorée de vi peut être utilisée sous SUSE LINUX, le vim (vi improved). Il existe de nombreuses sources d'informations traitant de ce programme :

- vimtutor est un didacticiel interactif pour le vim.
- Vous recevez dans le vim, grâce à la commande `:help`, de l'aide concernant de nombreux domaines
- Vous trouverez sur internet un livre (en anglais) sur le vim sous `http://www.truth.sk/vim/vimbook-OPL.pdf`.
- Sur les pages internet du projet vim, vous trouverez toutes les nouveautés, les listes de diffusion et autres documentations. Vous trouverez ces pages sous `http://www.vim.org`.
- Vous trouverez sur internet également quelques tutoriels au sujet de vim. A savoir sous : `http://www.selflinux.org/selflinux/html/vim.html`, `http://www.linuxgazette.com/node/view/9039` et `http://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.html`. Vous trouverez d'autres liens vers des tutoriels sous `http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html`.

Remarque

La licence VIM

vim est ce qu'on appelle un "logiciel de bienfaisance". Ceci signifie que les auteurs ne veulent pas recevoir d'argent pour les logiciels mais qu'ils incitent à supporter un projet d'intérêt général à l'aide de dons. Ce projet servira à venir en aide aux enfants en Ouganda. Vous trouverez de plus amples informations à ce sujet sur internet sous `http://iccf-holland.org/index.html`, `http://www.vim.org/iccf/` et `http://www.iccf.nl/`.

Remarque

9.2 Consoles virtuelles

Linux est un système multitâches et multi-utilisateurs. Même si vous êtes le seul utilisateur sur votre machine, vous apprendrez à apprécier les avantages apportés par ces capacités.

Vous avez accès à six consoles virtuelles en mode texte que vous pouvez activer à l'aide des combinaisons de touches (Alt)-(F1) à (Alt)-(F6). La septième console est réservée à X11, la huitième à une session X11 supplémentaire. En modifiant le fichier `/etc/inittab`, vous pouvez réserver un nombre plus grand ou plus petit de consoles. Pour revenir à une console texte depuis X11 sans quitter X11, utilisez les combinaisons de touches (Ctrl)-(Alt)-(F1) à (Ctrl)-(Alt)-(F6). (Alt)-(F7) vous permet de revenir à X11.

9.3 Assignation des touches

Les fichiers suivants, entre autres, ont été modifiés afin d´uniformiser l´assignation des touches des programmes :

```
/etc/inputrc
/usr/X11R6/lib/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/X11R6/lib/X11/app-defaults/XTerm
/usr/share/emacs/<VERSION>/site-lisp/term/*.el
```

Ces modifications n'affectent que les applications qui lisent la base de données `terminfo` ou dont les fichiers de configuration ont été modifiés directement (`vi`, `less`, etc.). Il faudrait adapter sur ce modèle les applications qui ne sont pas livrées avec SUSE LINUX.

Vous obtiendrez la touche Compose (Multi_key) sous X grâce à la combinaison de touches (Strg)-(Shift) (droite). Attention toutefois : vérifiez que cela correspond bien au réglage indiqué dans `/usr/X11R6/lib/X11/Xmodmap`.

L'"extension X Keyboard" (XKB) permet une configuration plus poussée. Cette extension est utilisée également par les environnements de bureau GNOME (gswitchit) et KDE (kxkb). Vous trouverez plus d'informations relatives à XKB dans `/etc/X11/xkb/README` et les documents qui y sont cités.

Vous trouverez des informations supplémentaires concernant la saisie en chinois, japonais ou coréen (CJC) sur le site de Mike Fabian: `http://www.suse.de/~mfabian/suse-cjk/input.html`.

9.4 Adaptations locales et linguistiques

SUSE LINUX est internationalisé et s'adapte avec souplesse aux contraintes locales. L'internationalisation (I18N) permet des localisations dans des langues particulières (L10N). Les abréviations I18N et L10N signifient respectivement *internationalisation* et *localisation* : on prend l'initiale et la dernière lettre et on fait figurer entre elles le nombre de lettres omises.

Les réglages se font au moyen des variables `LC_` définies dans le fichier `/etc/sysconfig/language`. Il ne s'agit pas seulement de régler la langue de l'interface et des avertissements des programmes (prise en charge de la langue maternelle, *native language support*), mais de régler individuellement les catégories suivantes : les *messages* (langue), les *types de caractères*, l'*ordre de classement*, les *date et heure*, les *nombres* et la *monnaie*. Chacune de ces catégories peut être définie soit de manière ciblée grâce à une variable propre soit indirectement grâce à une variable parent dans le fichier `language` (cf. la page de manuel `man locale`).

1. `RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY` : ces variables sont passées à l'interpréteur de commandes sans le préfixe `RC_` et définissent les catégories nommées plus haut. Les fichiers concernés sont énumérés ci-après.

   Vous pouvez obtenir le réglage courant grâce à la commande `locale`.
2. `RC_LC_ALL`: Cette variable écrase, si elle a été initialisée, les valeurs des variables de la liste.
3. `RC_LANG` : Si aucune des variables nommées plus haut n'a été initialisée, on se rabat sur cette valeur. Par défaut, SUSE LINUX ne définit que `RC_LANG` ; ainsi, il est plus simple pour l'utilisateur de saisir ses propres valeurs.
4. `ROOT_USES_LANG`: Une variable binaire `yes/no`. Si elle vaut `no`, `root` travaille toujours dans l'environnement POSIX.

Les variables devront être réglées grâce à l'éditeur `sysconfig`. La valeur d'une telle variable est composée de l'indication du code de la langue (*language code*), du pays ou du territoire (*country code*), du jeu de caractères (*encoding*) et du modificateur optionnel (*modifier*). Les différentes indications sont séparées par des caractères spéciaux :

LANG=⟨*language*⟩[[_⟨*COUNTRY*⟩].⟨*Encoding*⟩[@⟨*Modifier*⟩]]

9.4.1 Quelques exemples

Il est important de toujours définir conjointement la langue et le pays. Le code de langue suit le standard ISO 639 (`http://www.evertype.com/standards/iso639/iso639-en.html` et `http://www.loc.gov/standards/iso639-2/`), les codes de pays sont définis dans la norme ISO 3166 (voir `http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html`). Naturellement, on ne peut choisir que des valeurs pour lesquelles il existe des fichiers de description utilisables dans `/usr/lib/locale`. On peut générer de nouveaux fichiers de description à l'aide de `localedef` sur la base des fichiers contenus dans `/usr/share/i18n`.

`LANG=fr_FR.UTF-8` Il s'agit de la configuration par défaut lorsque l'on effectue l'installation en français. Si une autre langue est utilisée pour l'installation, le codage des caractères restera UTF-8, mais la langue du système sera celle de l'installation.

`LANG=fr_FR.ISO-8859-1` C'est avec cette commande qu'on associe à la langue française le jeu de caractères `ISO-8859-1`. Ce jeu de caractères ne comprend pas le caractère euro. On l'utilise toutefois lorsqu'un logiciel n'a pas été adapté à le codage `UTF-8`.

L'indication du jeu de caractères (dans le cas présent `ISO-8859-1`) est utilisée par exemple par l'éditeur Emacs.

`LANG=fr_FR@euro` Ceci donne un exemple d'utilisation d'une option (`euro`).

SuSEconfig lit les variables de `/etc/sysconfig/language` et écrit les instructions dans `/etc/SuSEconfig/profile` et `/etc/SuSEconfig/csh.cshrc`. `/etc/SuSEconfig/profile` est lu par `/etc/profile` (au moyen d'une instruction source) et `/etc/SuSEconfig/csh.cshrc` par `/etc/csh.cshrc`. De cette manière, les réglages sont disponibles pour tous les utilisateurs du système.

Les utilisateurs peuvent écraser les réglages par défaut du système dans `~/.bashrc`. Donc, dans le cas où le réglage commun est `fr_FR`, l'utilisateur peut, si les messages des programmes en français ne lui conviennent pas, passer en version anglaise : `LC_MESSAGES=en_US`.

9.4.2 Réglage de la langue

Les fichiers de la catégorie *messages* se trouvent en général uniquement dans le répertoire propre à la langue (par exemple `fr`), afin d'avoir une solution de repli. Donc, si l'on règle `LANG` à `fr_CA` alors que le fichier de messages n'existe pas dans `/usr/share/locale/fr_CA/LC_MESSAGES`, les programmes se rabattent sur `/usr/share/locale/fr/LC_MESSAGES`.

On peut également définir un système de replis successifs avec `LANGUAGE`; par exemple : breton → français ou galicien → espagnol → portugais :

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Ou pour passer aux variantes norvégiennes nynorsk ou bokmål (avec un repli supplémentaire sur `no`):

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

ou

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

Pour ce qui est du norvégien, il faut également tenir compte du fait que `LC_TIME` est traité différemment.

Problèmes possibles

Le point marquant les milliers n'est pas reconnu : `LANG` est probablement réglé par exemple à `fr`. Comme la description à laquelle la bibliothèque glibc fait appel se trouve dans `/usr/share/lib/fr_FR/LC_NUMERIC`, `LC_NUMERIC` devrait valoir par exemple `fr_FR`.

Pour plus d'informations :

- *The GNU C Library Reference Manual*, chapitre "Locales and Internationalization" ; dans le paquetage `glibc-info`.
- Jochen Hein, au mot-clé "NLS".
- *Francophones-Howto* de Guylhem-Aznar `file:/usr/share/doc/howto/en/html/Francophones-HOWTO.html`.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, actuellement à l'adresse suivante : `http://www.cl.cam.ac.uk/~mgk25/unicode.html`.

- *Unicode-Howto* de Bruno Haible en anglais `file:/usr/share/doc/howto/en/html/Unicode-HOWTO.html` ou en français `file:/usr/share/doc/howto/fr/a-jour/html/Unicode-HOWTO.html`.
- *CJK Support in SuSE Linux* en anglais de Mike Fabian `http://www.suse.de/~mfabian/suse-cjk/suse-cjk.html`.

Processus d'amorçage

L'amorçage et l'initialisation d'un système Unix sont, même pour un administrateur système, loin d'être évidents. Ce chapitre est une brève introduction au processus d'amorçage de SUSE LINUX. L'implémentation actuelle de l'initialisation du système met en œuvre le standard LSB (cf. la section *Standards et spécifications* page 727).

Avec le message lapidaire "Décompression de Linux..." , le noyau prend le contrôle de l'ensemble du matériel constituant le système. Il vérifie et définit la console — ou plus précisément : le registre BIOS de la carte graphique et le format d'affichage —, pour ensuite pouvoir lire les paramètres dans le BIOS et initialiser les interfaces élémentaires de la carte mère. Au cours des étapes suivantes, les pilotes — qui font déjà partie intégrante du noyau — "sondent" le matériel disponible pour l'initialiser, le cas échéant. Une fois les partitions vérifiées et le montage du système de fichiers racine effectué, le noyau démarre le programme init. init permet de "monter" (jargon Unix) le système lui-même et les nombreux services et leur configuration sont ainsi démarrés. Le noyau gère ensuite l'ensemble du système : il surveille le temps de calcul de chaque programme, il met de la mémoire à disposition et contrôle les accès au matériel.

10.1 Démarrer avec le disque virtuel initial

10.1.1 Énoncé du problème

Dès que le noyau Linux est chargé et le système de fichiers racine (`/`) est monté, des programmes peuvent être exécutés et d'autres modules du noyau peuvent être ajoutés, afin de mettre à disposition des fonctionnalités supplémentaires. Mais avant de pouvoir monter le système de fichiers racine, différentes conditions doivent être remplies : le noyau requiert les pilotes correspondants pour pouvoir entrer en contact avec le périphérique sur lequel se trouve le système de fichiers racine (en particulier le pilote SCSI). En plus, le noyau doit contenir le code nécessaire à la lecture du système de fichiers (`ext2`, `reiserfs`, `romfs` etc.). Il est en outre possible que le système de fichiers racine soit déjà chiffré. Dans ce cas, il est nécessaire de saisir le mot-clé/mot de passe.

Si l'on considère le problème des pilotes SCSI, diverses solutions sont envisageables. Le noyau peut contenir tous les pilotes possibles. C'est problématique puisque les différents pilotes peuvent interférer. De plus, cela augmente la taille du noyau. Une autre possibilité est de mettre différents noyaux à disposition, ne comportant chacun qu'un ou très peu de pilotes SCSI. Cette alternative aussi est problématique puiqu'elle nécessite un très grand nombre de noyaux différents. Ce problème est encore aggravé par les noyaux optimisés de façon différente (optimisation Athlon, SMP).

La solution consistant à charger le pilote SCSI comme module conduit à une problématique générale, à laquelle on remédie par le concept du *disque virtuel initial* : la mise en place d'une possibilité de pouvoir exécuter des programmes de l'espace utilisateur avant de monter le système de fichiers racine.

10.1.2 Concept du disque virtuel initial

Le *disque virtuel initial* (appelé aussi initdisk ou initrd) résout exactement les problèmes décrits plus haut. Le noyau Linux offre la possibilité de charger un (petit) système de fichiers dans un disque virtuel initial et d'y faire exécuter les programmes avant de monter le véritable système de fichiers racine. Le chargement de `initrd` est pour cela pris en charge par le gestionnaire d'amorçage (GRUB, LILO etc.) ; tous ces gestionnaires d'amorçage n'ont besoin que de routines BIOS pour charger des fichiers prenant en charge l'amorçage. Si le gestionnaire d'amorçage peut charger le noyau, il peut aussi charger le disque virtuel initial. Vous n'avez donc pas besoin de pilotes spéciaux.

10.1.3 Déroulement du processus de démarrage avec initrd

Le gestionnaire d'amorçage charge le noyau et le disque virtuel `initrd` en mémoire et démarre le noyau, tout en informant le noyau qu'un disque virtuel `initrd` est disponible, et en lui indiquant son emplacement en mémoire. Si le disque virtuel `initrd` est compressé (ce qui est généralement le cas), le noyau décompresse le disque virtuel `initrd` et le monte en tant que système fichiers racine temporaire.Puis, un programme du nom de linuxrc est démarré dans le disque virtuel `initrd`. Ce programme peut alors faire tout ce qui est nécessaire pour monter le véritable système de fichiers racine. Lorsque `linuxrc` a terminé, le disque virtuel `initrd` (temporaire) est démonté (*unmounted*) et le processus d'amorçage normal reprend avec le montage des bons systèmes de fichiers. Le montage du disque virtuel `initrd` et l'exécution de linuxrc peuvent être considérés un court intermède pendant le processus normal d'amorçage. Le noyau essaie après l'amorçage de la bonne partition racine de monter le disque virtuel `initrd` dans le répertoire `/initrd`. Si cela échoue, lorsque par exemple le point de montage `/initrd` n'existe pas, le noyau essaie de démonter le disque virtuel `initrd`. Si cela échoue également, le système reste totalement fonctionnel, mais la mémoire utilisée par le disque virtuel `initrd` n'est jamais libérée et n'est donc plus disponible.

Le programme linuxrc

Le programme linuxrc de `initrd` n'a que peu d'exigences. Le programme doit porter le nom spécial de `linuxrc` et doit se trouver dans le répertoire racine du disque virtuel `initrd`. En dehors de cela il doit seulement pouvoir être exécuté par le noyau. Ceci signifie que linuxrc peut tout à fait être lié de façon dynamique. Dans ce cas, les bibliothèques partagées (*shared librairies*) doivent naturellement être toutes disponibles dans le répertoire `/lib` du disque virtuel `initrd`. `linuxrc` peut aussi être un script shell. Dans ce cas, un interpréteur de commande doit bien sûr être présent dans `/bin`. En bref, le disque virtuel `initrd` doit comporter un système Linux minimal qui permette l'exécution du programme linuxrc. Lors de l'installation de SUSE LINUX, on utilise un linuxrc lié de façon statique afin de pouvoir garder le disque virtuel `initrd` aussi petit que possible. linuxrc est exécuté avec les droits `root`.

Le véritable système de fichiers racine

Dès que linuxrc a terminé, le disque virtuel `initrd` est démonté et écarté, le processus de démarrage continue normalement et le noyau monte le véritable système de fichiers racine. Le système de fichiers à monter en tant que racine peut être déterminé par linuxrc. Pour cela, linuxrc doit simplement monter le système de fichiers `/proc` et écrire l'emplacement du véritable système de fichiers racine sous forme numérique dans `/proc/sys/kernel/real-root-dev`.

10.1.4 Gestionnaire d'amorçage

La plupart des gestionnaires d'amorçage (en particulier GRUB, LILO et syslinux) sont compatibles avec `initrd`. Les différents gestionnaires d'amorçage reçoivent l'instruction d'utiliser un disque virtuel `initrd` comme suit :

GRUB Ajout de la ligne suivante dans `/boot/grub/menu.lst` :

```
initrd
       (hd0,0)/initrd
```

Comme l'adresse de chargement du disque virtuel initrd est écrite dans l'image du noyau déjà chargée, la commande `initrd` doit suivre la commande `kernel`.

LILO Ajout de la ligne suivante dans `/etc/lilo.conf` :

```
initrd=/boot/initrd
```

Le fichier `/boot/initrd` est le *disque virtuel initial*. Il peut être compressé.

syslinux Ajout de la ligne suivante dans `syslinux.cfg` :

```
append
       initrd=initrd
```

D'autres paramètres peuvent suivre sur cette ligne.

10.1.5 Utilisation de initrd avec SUSE

Installation du système

Le disque virtuel `initrd` est déjà utilisé depuis longtemps pour l'installation : pendant une installation manuelle, l'utilisateur peut charger des modules du noyau dans linuxrc et entreprendre les actions nécessaires à l'installation. linuxrc démarre alors YaST, qui conduit l'installation. Lorsque YaST a terminé son travail, il informe linuxrc de l'endroit où se situe le système de fichiers racine du système fraîchement installé. linuxrc sauvegarde cette valeur dans `/proc` puis redémarre le système. YaST redémarre alors, et installe le reste des paquetages dans le système nouvellement installé.

Démarrage du système installé

Dans le passé, YaST proposait plus de 40 noyaux pour l'installation dans le système, les noyaux se différenciaient essentiellement par le fait que chaque noyau contenait un pilote SCSI défini. Ceci était nécessaire afin de pouvoir monter le système de fichiers racine après le démarrage. On pouvait ensuite charger d'autres pilotes comme modules.

Mais comme entre-temps on dispose aussi de noyaux optimisés, ce concept n'est plus valable – on aurait entre-temps besoin de bien plus de 100 images noyau .

C'est pour cela qu'on utilise aussi pour le démarrage normal du système un disque virtuel `initrd`. Le fonctionnement est semblable à une installation. Le programme linuxrc employé ici est cependant simplement un script shell qui n'a pour tâche que de charger quelques modules indiqués. Il ne s'agit généralement que d'un seul module, à savoir le pilote SCSI nécessaire pour pouvoir accéder au système de fichiers racine.

Création d'un disque virtuel initrd

La création d'un fichier `initrd` s'effectue à l'aide du script `mkinitrd` (précédemment nommé `mk_initrd`). Les modules à charger sont définis dans SUSE LINUX par l'identificateur `INITRD_MODULES` dans `/etc/sysconfig/kernel`. Après une installation, une valeur correcte est automatiquement affectée à cette variable (le linuxrc d'installation sait quels modules ont été chargés). Les modules sont chargés suivant l'ordre exact dans lequel ils apparaissent dans `INITRD_MODULES`. C'est particulièrement important quand on utilise plusieurs pilotes SCSI, sinon la désignation des disques serait modifiée. Il suffirait à proprement parler de ne charger que le pilote SCSI nécessaire à l'accès au système de fichiers racine. Cependant, comme le chargement automatique de pilotes SCSI supplémentaires est problématique, nous chargeons tous les pilotes SCSI nécessaires à l'installation à l'aide de `initrd`.

Remarque

Comme le chargement de `initrd` par le gestionnaire d'amorçage se fait exactement comme le chargement du noyau lui-même (LILO note dans son fichier `map` la situation des fichiers), le gestionnaire d'amorçage doit être, lors de l'utilisation de LILO, réinstallé après toute modification de `initrd`. – lors de l'utilisation de GRUB, cela n'est pas nécessaire !

Remarque

10.1.6 Difficulté possible – noyau auto-compilé

Si on compile soi-même un noyau, cela peut conduire aux problèmes suivants : le pilote SCSI est lié par inadvertance dans le noyau, mais le fichier `initrd` existant reste inchangé. Il se passe la chose suivante au démarrage : le noyau comporte déjà le pilote SCSI, le matériel est reconnu. Cependant, le `initrd`essaie maintenant de charger à nouveau le pilote comme module. Ceci provoque pour quelques pilotes SCSI (particulièrement pour `aic7xxx`) l'arrêt du système. Il s'agit au sens strict d'une erreur du noyau (un pilote déjà existant n'a pas le droit d'être chargé une deuxième fois en tant que module) – on connaît déjà le problème à propos des pilotes en série.

Il existe plusieurs solutions : soit configurer le pilote comme module (il est alors correctement chargé dans le disque virtuel `initrd`) soit ôter la déclaration du `initrd` de `/etc/grub/menu.lst` ou de `/etc/lilo.conf`. Equivalent

à la dernière solution, on peut ôter le pilote de `INITRD_MODULES` et appeler `mkinitrd`, qui ensuite constate qu'aucun `initrd` n'est nécessaire.

10.1.7 Perspectives

Il est pensable dans l'avenir qu'un `initrd` soit utilisable pour des choses plus nombreuses (et plus compliquées) que seulement pour le chargement des modules nécessaire pour l'accès à `/`.

- Système de fichiers racine sur logiciel RAID (linuxrc démarre les périphériques `md`)
- Système de fichiers racine sur LVM
- Le système de fichiers racine est chiffré (linuxrc demande le mot de passe)
- Système de fichiers racine sur un disque SCSI sur adapteur PCMCIA

Informations supplémentaires

- `/usr/src/linux/Documentation/initrd.txt`
  (Seulement disponible quand les sources noyau ont été installées)
- La page de manuel de initrd.

10.2 Le programme init

Le programme init est le processus responsable de l'initialisation correcte du système ; tous les processus du système sont donc des "fils" d'init.

Dans tous les programmes, init joue un rôle bien particulier : init est directement démarré par le noyau et est immunisé contre le signal 9, qui permet normalement de "tuer" tous les processus. Tous les autres processus sont démarrés soit par init même, soit par un de ses "processus fils".

init se configure de manière centralisée, avec le fichier `/etc/inittab` ; c'est ici que sont définis les différents "niveaux d'exécution" (*run levels*) (on donne plus d'indications à ce sujet à la section *Les niveaux d'exécution* page suivante) ainsi que les services et les démons qui sont censés être disponibles pour chaque niveau. init appelle différents scripts en fonction des définitions qui se trouvent dans `/etc/inittab`. Ces scripts sont regroupés dans le répertoire `/etc/init.d` pour des raisons de clarté..

L'ensemble du démarrage du système — et bien entendu aussi son arrêt — est ainsi uniquement géré par le processus init ; sur ce point, le noyau peut être considéré presque comme un "processus en arrière-plan" dont les tâches consistent à gérer les processus démarrés, leur accorder du temps de calcul et autoriser et contrôler l'accès au matériel.

10.3 Les niveaux d'exécution

Il existe, sous Linux, différents *niveaux d'exécution* qui définissent l'état actuel du système. Le niveau d'exécution par défaut que le système doit atteindre après l'amorçage se définit dans le fichier `/etc/inittab` grâce au mot-clé `initdefault`. Il s'agit généralement du niveau d'exécution `3` ou `5` (voir la vue d'ensemble du tableau 10.1 page suivante). Il est aussi possible d'indiquer le niveau d'exécution souhaité lors de l'amorçage (par exemple à l'invite d'amorçage) ; le noyau transmet les paramètres qu'il n'exploite pas lui-même sans les modifier au processus init.

Pour passer plus tard à un autre niveau d'exécution, il est possible d'appeler init avec le numéro du niveau d'exécution correspondant ; seul l'administrateur système peut initier un changement de niveau d'exécution, par exemple à l'aide de la commande `init 1` ou `shutdown now` en mode mono-utilisateur (en anglais, *single user mode*), qui sert à réparer et à administrer le système. Lorsque l'administrateur système a terminé son travail, il peut utiliser la commande `init 3` pour faire redémarrer le système à nouveau dans le mode d'exécution normal utilisé pour faire tourner tous les programmes applicatifs et dans lequel les utilisateurs peuvent s'identifier auprès du système. Utilisez `init 0` ou `shutdown -h now` pour arrêter le système ou `init 6` ou `shutdown -r now` pour le redémarrer.

Remarque

Niveau d'exécution 2 pour une partition /usr/ montée via NFS

N'utilisez pas le niveau d'exécution 2 sur un système dont la partition `/usr` est montée via NFS. La partition `/usr/` contient des programmes importants nécessaires pour que votre système fonctionne sans incident. Comme le service NFS n'est pas encore disponible au niveau d'exécution 2 (mode multi-utilisateur en local sans réseau distant), le fonctionnement de votre système en serait fortement perturbé.

Remarque

TAB. *10.1:* *Liste des niveaux d'exécution sous Linux*

Niveau d'exécution	Signification
0	Arrêt du système (en anglais, *system halt*)
S	Mode mono-utilisateur (en anglais, *single user mode*) ; à partir de l'invite d'amorçage, avec disposition de clavier américain
1	Mode mono-utilisateur (en anglais, *single user mode*)
2	Mode multi-utilisateur local sans réseau distant (en anglais, *local multiuser without remote network*) (c'est-à-dire NFS)
3	Mode multi-utilisateur complet avec réseau (en anglais, *full multiuser with network*)
4	Non attribué (en anglais, *not used*)
5	Mode multi-utilisateur complet avec réseau et KDM (par défaut), GDM ou XDM (en anglais, *full multiuser with network and xdm*)
6	Redémarrage du système (en anglais, *system reboot*)

Sur une installation standard de SUSE LINUX, c'est le niveau d'exécution `5` qui est défini par défaut, de manière à ce que les utilisateurs puissent directement s'identifier auprès du système par l'intermédiaire de l'interface graphique.

Si vous souhaitez passer du niveau d'exécution `3` au `5`, vous devez vous assurer que le système X Window est déjà correctement configuré ; (voir le chapitre *Le système X Window* page 273). Pour tester si le système fonctionne comme vous le souhaitez, saisissez la commande `init 5`. Dans l'affirmative, vous pouvez utiliser YaST pour modifier le niveau d'exécution par défaut et choisir `5`.

Attention

Modifications personnalisées de /etc/inittab

Un fichier `/etc/inittab` erroné peut provoquer un mauvais démarrage du système. Procédez toujours avec la plus grande précaution lorsque vous modifiez ce fichier et conservez toujours une copie d'un fichier intact. Pour réparer le dommage, vous pouvez essayer de saisir à l'invite d'amorçage le paramètre `init=/bin/sh` pour amorcer directement dans un interpréteur de commandes et recréer le fichier à partir de là. Après l'amorçage, vous pouvez remettre en place la copie de sauvegarde à l'aide de la commande `cp`.

Attention

10.4 Changement de niveau d'exécution

Voici ce qu'il se produit généralement lors d'un changement de niveau d'exécution : les *scripts d'arrêt* du niveau d'exécution actuel sont exécutés — ce qui implique généralement aussi un arrêt des programmes exécutés sous ce niveau — et les *scripts de démarrage* du nouveau niveau d'exécution sont exécutés. La plupart du temps, dans un pareil cas, quelques programmes sont démarrés.

Pour clarifier cela, nous avons illustré dans un exemple le passage du niveau d'exécution 3 au niveau d'exécution 5 :

- L'administrateur (`root`) informe le processus init que le niveau d'exécution doit être modifié. Dans ce cas, il le fait en saisissant la commande `init 5`.
- init consulte le fichier de configuration `/etc/inittab` et constate que le script `/etc/init.d/rc` doit être appelé avec comme paramètre le nouveau niveau d'exécution.
- Ensuite, rc appelle tous les scripts d'arrêt du niveau d'exécution correspondant et pour lesquels il n'existe pas de script de démarrage dans le nouveau niveau d'exécution : dans notre exemple, il s'agit de tous les scripts qui se trouvent dans le répertoire `/etc/init.d/rc3.d` (l'ancien niveau d'exécution était `3`) et qui commencent par `K`. Le nombre qui se trouve après `K` garantit le respect d'un ordre défini, car, selon les circonstances, certains programmes dépendent d'autres.

- Sont enfin appelés les scripts de démarrage du nouveau niveau d'exécution ; ces derniers se trouvant, dans notre exemple, dans `/etc/init.d/rc5.d` et commençant par un S. On respecte ici aussi un ordre donné défini par le nombre suivant le S.

Si vous passez au même niveau d'exécution que celui dans lequel vous vous trouvez déjà, l'application init ne lit que le fichier `/etc/inittab`, recherche s'il a été modifié et, le cas échéant, prend les mesures nécessaires, comme par exemple le démarrage d'une commande `getty` sur une autre interface.

10.5 Les scripts d'initialisation

Les scripts dans `/etc/init.d` se divisent en deux catégories :

- Les scripts appelés *directement* par init : ce n'est le cas que lors de l'amorçage ou lors d'un arrêt immédiat du système (en cas de coupure de courant ou si l'utilisateur appuie sur les touches Strg-Alt-Suppr).
- Les scripts lancés *indirectement* par init : cela se produit lors d'un changement de niveau d'exécution ; c'est généralement le script de niveau supérieur /etc/init.d/rc qui est exécuté. C'est lui qui est responsable de surveiller que les scripts utiles sont appelés dans le bon ordre.

Tous les scripts se trouvent dans `/etc/init.d`. Vous trouverez également les scripts pour le changement du niveau d'exécution dans ce répertoire ; ils sont toutefois généralement appelés en tant que liens symboliques à partir de l'un des répertoires `/etc/init.d/rc0.d` à `/etc/init.d/rc6.d`. Cela permet de conserver une vue d'ensemble sur les scripts et permet d'éviter que les scripts soient recopiés à plusieurs endroits lorsqu'ils sont utilisés à différents niveaux d'exécution. Comme chacun de ces scripts peut indifféremment être appelé comme script de démarrage ou d'arrêt, ils doivent en plus interpréter les deux paramètres possibles `start` et `stop`. Les scripts réagissent, en plus, aux options `restart`, `reload`, `force-reload` et `status` ; vous trouverez la signification de ces différentes options dans le tableau 10.2 page suivante.

TAB. *10.2:* *Présentation des options des scripts d'initialisation*

Option	Signification
`start`	Démarre le service
`stop`	Arrête le service
`restart`	Arrête le service et le redémarre si le service est déjà en cours ; sinon, démarre le service
`reload`	Lit à nouveau la configuration du service sans l'arrêter ni le redémarrer
`force-reload`	Lit à nouveau la configuration du service, si le service prend en charge ce type d'option ; sinon identique à `restart`
`status`	Affiche l'état actuel

Les liens dans les répertoires spécifiques des différents niveaux d'exécution ne servent qu'à permettre un classement des différents scripts en fonction des niveaux d'exécution. L'insertion ou la suppression de liens nécessaires se fait à l'aide de insserv (ou du lien `/usr/lib/lsb/install_initd`) lors de l'installation ou de la désinstallation des paquetages respectifs ; cf. la page de manuel consacrée à insserv.

Vous trouverez ci-après une brève description du premier script d'amorçage et du dernier script d'arrêt ainsi que du script de commande :

`boot` exécuté au démarrage du système et démarré directement par init. Il est indépendant du niveau d'exécution par défaut souhaité et n'est exécuté qu'une seule fois : en substance, les systèmes de fichiers `proc` et `pts` sont, "montés", blogd (en anglais, *Boot Logging Daemon*) est activé et — après une première installation ou une mise à jour du système — une nouvelle configuration de base est lancée.

Le démon blogd est un démon démarré par les scripts boot *et* rc avant tous les autres et qui, une fois son travail accompli, (par exemple, l'appel de sous-scripts), est à nouveau arrêté. Ce démon écrit dans le fichier journal `/var/log/boot.msg` lorsque le répertoire `/var` est monté en lecture/écriture, sinon il met en mémoire tampon toutes les données à l'écran jusqu'à ce que le répertoire `/var` soit monté en lecture/écriture. Vous trouverez plus d'informations au sujet de blogd dans `man blogd`.

Ce script passe ensuite la main au répertoire `/etc/init.d/boot.d` ; tous les scripts qui se trouvent dans ce répertoire et qui commencent par un `S` sont automatiquement exécutés au démarrage du système. Les systèmes de fichiers sont vérifiés, les fichiers superflus dans `/var/lock` sont supprimés et le réseau du périphérique de bouclage est configuré, si c'est prévu ainsi. L'horloge système est ensuite réglée.

En cas d'erreur grave lors de la vérification et de la réparation automatique des systèmes de fichiers, l'administrateur système peut, après avoir saisi son mot de passe racine, résoudre manuellement le problème. Enfin, le script `boot.local` est exécuté.

`boot.local` Vous pouvez saisir ici d'autres actions à effectuer lors du démarrage avant que le système n'entre dans un niveau d'exécution donné : on peut le comparer, par son fonctionnement, au fichier `AUTOEXEC.BAT` utilisé sous DOS.

`boot.setup` Réglages de base qui doivent être effectués lors du passage du mode mono-utilisateur à n'importe quel niveau d'exécution. C'est ici que sont chargés la disposition des touches du clavier et la configuration de la console.

`halt` Ce script n'est exécuté que lors de l'entrée dans le niveau d'exécution 0 ou 6. Il est ainsi appelé soit sous le nom de `halt` soit sous celui de `reboot`. Selon la façon dont `halt` est appelé, le système est soit redémarré, soit complètement arrêté.

`rc` Le script de niveau supérieur appelé à chaque changement de niveau d'exécution. Il exécute les scripts d'arrêt du niveau d'exécution actuel, puis les scripts de démarrage du nouveau niveau.

10.5.1 Ajouter des scripts d'initialisation

Vous pouvez facilement intégrer des scripts d'initialisation supplémentaires en suivant l'organisation décrite précédemment. En cas de questions relatives au format, à l'attribution de noms et à l'organisation des scripts init, reportez-vous aux indications du LSB et des pages de manuel de `init`, de `init.d` et de `insserv`. Les pages de manuel des commandes `startproc` et `killproc` sont également utiles dans ce cadre.

Attention

Élaboration de scripts d'initialisation personnalisés

Des scripts d'initialisation erronés peuvent "geler" le système tout entier. Procédez avec la plus grande attention lorsque vous écrivez vos scripts personnalisés et vérifiez — dans la mesure du possible — leur innocuité dans l'environnement multi-utilisateur. Vous trouverez des informations de base sur l'utilisation des niveaux d'exécution et des scripts d'initialisation dans la section *Les niveaux d'exécution* page 260.

Attention

Si vous écrivez un script d'initialisation pour votre propre programme ou pour votre propre service système, utilisez le fichier `/etc/init.d/skeleton` comme modèle. Enregistrez ce fichier sous un nouveau nom et éditez les noms de programmes et de fichiers ainsi que les chemins d'accès et ajoutez, si nécessaire, vos propres bouts de scripts nécessaires à l'exécution correcte du script d'initialisation.

Éditez le bloc `INIT INFO` obligatoire qui se trouve au début du fichier :

Exemple 10.1: *Un bloc INIT INFO minimal*

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

Sur la première ligne de l'en-tête `INFO`, indiquez après `Provides:` le nom du programme ou du service qui doit être piloté avec ce script init. `Required-Start:` et `Required-Stop:` contiennent tous les services qui doivent être démarrés ou arrêtés avant le démarrage ou l'arrêt du service ou du programme concerné. Ces informations sont exploitées pour générer la numérotation des scripts de démarrage et d'arrêt dans les répertoires des niveaux d'exécution. Indiquez le niveau d'exécution auquel votre application doit automatiquement être démarrée ou arrêtée dans `Default-Start:` et `Default-Stop:`. Terminez en saisissant une brève description de votre application dans `Description:`.

Utilisez la commande `insserv <Nom du nouveau script>` pour placer les liens du fichier `/etc/init.d/` dans les répertoires des niveaux d'exécution correspondants (`/etc/init.d/rc?.d/`). insserv évalue automatiquement les informations indiquées dans l'en-tête du script d'initialisation et place les liens des scripts d'arrêt et de démarrage dans les répertoires des niveaux d'exécution correspondants. L'enchaînement correct des démarrages et des arrêts au sein d'un niveau d'exécution est également assuré par la numérotation des scripts faite par insserv. Vous pouvez utiliser comme outil de configuration graphique pour le placement des liens l'éditeur de niveaux d'exécution de YaST : cf. la section *Éditeur de niveaux d'exécution de YaST* de la présente page.

Si vous souhaitez intégrer aux différents niveaux d'exécution un script déjà existant du répertoire `/etc/init.d/`, utilisez insserv ou l'éditeur de niveaux d'exécution de YaST pour placer les liens dans les répertoires de niveaux d'exécution correspondants et activer le service. Vos modifications seront prises en charge lors du prochain démarrage du système et le nouveau service démarrera automatiquement.

10.6 Éditeur de niveaux d'exécution de YaST

Une fois ce module démarré, vous arrivez dans un aperçu qui indique tous les services disponibles ainsi que leur état d'activation. Choisissez à l'aide du boutons radio l'un des deux modes : 'Easy' (facile) ou 'Expert'. La valeur par défaut est le mode 'Easy' (facile), qui suffit pour la plupart des utilisations. Vous voyez dans un tableau tous les services et tous les démons disponibles sur votre système, classés par ordre alphabétique. Dans la colonne de gauche figurent les noms des services, au milieu leur état d'activation et dans la colonne de droite une brève description. Sous cet aperçu se trouve une description complète du service actuellement sélectionné. Pour activer un service, sélectionnez-le dans l'aperçu, puis cliquez sur 'Activer'. Procédez de la même manière pour désactiver les services actifs.

Si vous souhaitez influencer de manière ciblée le niveau d'exécution dans lequel un service est démarré ou arrêté ou modifier le niveau d'exécution par défaut, passez avec le bouton radio en mode 'Expert'. Ce formulaire indique tout d'abord le niveau d'exécution par défaut actuel. C'est ce "mode d'exploitation" qui est lancé après l'amorçage de votre système. Pour SUSE LINUX, il s'agit généralement du niveau d'exécution 5 (mode multi-utilisateur complet avec réseau et

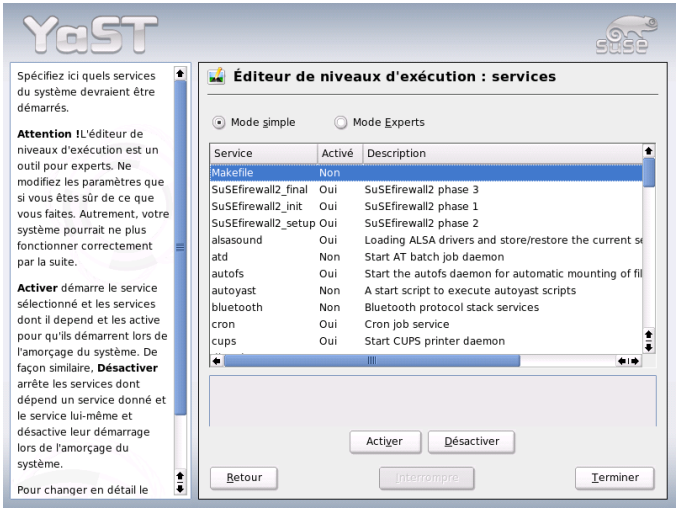


FIG. *10.1:* *Éditeur de niveaux d'exécution de YaST*

XDM). Serait également adapté par exemple le niveau d'exécution 3 (mode multi-utilisateur complet avec réseau). Vous pouvez, à cet endroit, également définir un autre niveau d'exécution par défaut à l'aide de YaST ; cf. le tableau 10.1 page 261. L'activation et la désactivation des services et des démons se fait dans l'aperçu en colonnes. Celui-ci donne notamment des informations au sujet des services et des démons disponibles, comme par exemple, s'ils sont activés pour votre système et pour quel niveau d'exécution. Si vous sélectionnez une ligne par un clic de souris, vous pouvez cocher les cases des niveaux d'exécution 'B', '0', '1', '2', '3', '5', '6' et 'S' et ainsi définir pour quels niveaux d'exécution le service ou le démon correspondant doit être activé. Le niveau d'exécution 4 n'est pas défini — il est laissé libre pour les paramétrages personnalisés. Immédiatement sous cet aperçu, une brève description du service ou du démon sélectionné est affichée.

Utilisez les options 'Lancer/Arrêter/Mise à jour' pour décider si un service doit être mis en service. 'Mise à jour de létat' vous permet de vérifier l'état actuel si cela n'est pas effectué automatiquement. Par 'Appliquer/Restaurer' vous sélectionnez si l'état configuré par vous sera appliqué ou bien si l'état initial avant l'appel de l'éditeur niveau d'exécution sera restauré. Utilisez 'Terminer' pour enregistrer la configuration du système.

Attention

Éditer la configuration des niveaux d'exécution

Une configuration erronée des services système et des niveaux d'exécution peut rendre votre système inutilisable. Informez-vous, préalablement à toute modification de cette configuration, de ses conséquences possibles, afin de toujours garantir le bon fonctionnement de votre système.

Attention

10.7 SuSEconfig et /etc/sysconfig

Utilisez, pour la configuration principale de SUSE LINUX, les fichiers de configuration qui se trouvent dans `/etc/sysconfig`. Les versions précédentes de SUSE LINUX utilisaient, pour la configuration, le fichier `/etc/rc.config`, devenu obsolète entre-temps. Ce fichier n'est plus fourni avec les nouvelles installations de SUSE LINUX. Utilisez les fichiers de `/etc/sysconfig` pour procéder à la configuration complète du système. En cas de mise à jour, un fichier `/etc/rc.config` existant est cependant conservé.

Seuls quelques scripts accèdent, de manière ciblée, aux fichiers dans `/etc/sysconfig` ; cela permet de garantir que par exemple la configuration du réseau n'est évaluée que par les scripts réseau. En outre, de nombreux autres fichiers de configuration du système sont générés en fonction des fichiers qui se trouvent dans `/etc/sysconfig` ; et c'est SuSEconfig qui s'en charge. Ainsi, le fichier `/etc/host.conf` est à nouveau généré après une modification de la configuration réseau, car il varie en fonction du type de configuration.

Si vous modifiez les fichiers cités, vous devez, par la suite, toujours appeler SuSEconfig pour que les nouveaux réglages soient répercutés partout où c'est nécessaire. Si vous utilisez l'éditeur de niveaux d'exécution de YaST pour modifier la configuration, vous n'avez pas besoin de vous en préoccuper particulièrement : YaST démarre automatiquement SuSEconfig, qui met à jour les fichiers concernés.

Ce système permet d'entreprendre des modifications fondamentales de la configuration de la machine sans avoir à la redémarrer. Comme certains réglages ont des répercussions assez profondes, vous devrez cependant parfois redémarrer quelques programmes pour que les modifications soient prises en compte.

Si, par exemple, vous avez modifié la configuration du réseau, utilisez `rcnetwork stop` et `rcnetwork start` pour redémarrer les programmes réseau concernés.

Procédez de la manière suivante pour configurer le système :

- Utilisez la commande `init 1` pour mettre le système en *mode mono-utilisateur* (niveau d'exécution 1).
- Procédez aux modifications des fichiers de configuration souhaitées. Vous pouvez aussi utiliser pour ce faire, un éditeur de texte ou, mieux encore, YaST ; cf. la section *L'éditeur de variables de Sysconfig de YaST* page suivante.

Attention

Édition manuelle de la configuration du système

Si vous n'utilisez *pas* YaST pour modifier les fichiers dans `/etc/sysconfig`, veillez à remplacer un paramètre vide par deux guillemets qui se suivent (par exemple `KEYTABLE=""`) et à inclure dans des guillemets les paramètres qui contiennent des espaces. Pour les variables composées d'un seul mot, les guillemets sont inutiles.

Attention

- Exécutez SuSEconfig pour enregistrer les modifications dans les différents autres fichiers de configuration. Cela s'effectue automatiquement si vous avez utilisé YaST pour définir le niveau d'exécution.
- Utilisez la commande `init 3` pour remettre le système dans le niveau d'exécution précédent (dans cet exemple, `3`).

Ce processus est naturellement uniquement disponible pour les modifications étendues des réglages du système (par exemple la configuration du réseau) ; pour les tâches plus simples, il n'est pas nécessaire de passer en "mode mono-utilisateur" ; cependant, assurez-vous que vraiment tous les programmes concernés par les modifications sont bien redémarrés.

Remarque

Vous pouvez arrêter la configuration automatique par SuSEconfig *globalement* en attribuant à la variable `ENABLE_SUSECONFIG` dans `/etc/sysconfig/suseconfig` la valeur `no`. Si vous souhaitez, en revanche, bénéficier de l'assistance pendant l'installation, vous devez attribuer à la variable `ENABLE_SUSECONFIG` la valeur `yes`. Vous pouvez également désactiver certaines parties de l'auto-configuration, de manière ciblée.

Remarque

10.8 L'éditeur de variables de Sysconfig de YaST

Le répertoire `/etc/sysconfig` contient les fichiers contenant les réglages les plus importants de SUSE LINUX. L'éditeur de variables de configuration système de YaST présente clairement toutes les possibilités de configuration. Les valeurs peuvent être modifiées et ensuite reportées dans les différents fichiers de configuration. Toutefois, l'édition manuelle est en général inutile, dans la mesure où lors de l'installation d'un paquetage ou de la définition d'un service, les fichiers sont automatiquement adaptés.

Attention

Modifications des fichiers /etc/sysconfig/*

Les modifications que vous effectuez dans le fichier `/etc/sysconfig/*` ont des conséquences importantes pour l'ensemble de votre système. Veuillez vous informer, préalablement à toute modification, sur les conséquences éventuelles. Vous serez ainsi assuré que votre système continuera à fonctionner correctement. Toutes les variables de configuration système des fichiers `/etc/sysconfig/` sont accompagnées de brefs commentaires qui expliquent la fonction de chacune d'entre-elles.

Attention

L'éditeur de variables de Sysconfig de YaST démarre par un formulaire composé de trois parties. Dans la partie gauche de ce formulaire, vous pouvez sélectionner, dans une arborescence, les variables à configurer. Dès que vous sélectionnez une variable, une description de la sélection et la valeur actuelle de la variable apparaissent dans la moitié droite de la fenêtre. Sous cette variable, une brève description, les valeurs possibles, la valeur par défaut, ainsi que le fichier dans lesquels cette variable est enregistrée. Ce formulaire indique également quel script de configuration est exécuté en cas de modification de cette variable et quel service est redémarré. YaST vous demande de confirmer les modifications et vous indique quels scripts exécuter lorsque vous quittez le module en cliquant sur 'Terminer'. Vous pouvez sauter le démarrage de certains services ou scripts si vous ne souhaitez pas les démarrer pour l'instant.

Le système X Window

Le Système X Window (X11) est pratiquement le standard pour les interfaces utilisateur graphiques sous Unix. X11 est par ailleurs orienté réseau : ainsi des applications exécutées sur un ordinateur peuvent afficher leurs résultats sur un autre ordinateur, lorsque ces deux ordinateurs sont connectés l'un à l'autre. Le type de réseau (réseau local LAN ou Internet) n'a ici aucune importance.

Dans ce chapitre, nous vous présentons des possibilités d'optimisation pour votre environnement Système X Window, nous vous donnons des informations de base pour vous familiariser avec les polices de caractères sous SUSE LINUX et nous détaillons la configuration OpenGL/3D. Vous trouverez la description du module de YaST pour la configuration de l'écran, de la carte graphique, de la souris et du clavier dans le la partie consacrée à l'installation de ce manuel (section *Carte graphique et moniteur (SaX2)* page 70).

11.1 Optimiser l'installation du Système X Window

Avec "X.Org", vous disposez d'une implémentation Open Source du système X window. Celle-ci est développée par la fondation "X.Org Foundatation" qui est également responsable du développement de nouvelles technologies et standards du système X window.

Afin de pouvoir utiliser de façon optimale le matériel à votre disposition (souris, carte graphique, écran, clavier), vous pouvez optimiser la configuration manuellement. Dans ce qui suit, nous présentons quelques aspects de l'optimisation. Vous trouverez des informations détaillées sur la configuration du système X window dans différents fichiers du répertoire `/usr/share/doc/packages/Xorg` ainsi, bien sûr, que dans la page de manuel `man XF86Config`.

Attention

La configuration du système X window doit être réalisée avec un soin tout particulier ! Il ne faut en aucun cas démarrer X11 avant d'avoir terminé la configuration. Un système mal configuré peut conduire à des dommages irréparables du matériel ; les moniteurs à fréquence fixe sont à ce titre particulièrement menacés. Les auteurs de ce livre et la société SUSE LINUX AG déclinent toute responsabilité pour les dommages pouvant éventuellement survenir. Ce texte a été établi avec le plus grand soin. Nous ne pouvons cependant pas absolument garantir que les méthodes présentées ici sont correctes et ne causeront aucun dommage à votre matériel.

Attention

Par défaut, les programmes SaX2 et xf86config construisent le fichier `XF86Config` dans le répertoire `/etc/X11`. Ceci est le fichier de configuration primaire pour le système X window. C'est ici que se trouvent les données relatives à la souris, à l'écran et à la carte graphique.

La structure du fichier de configuration `/etc/X11/XF86Config` vous est présentée ici. Ce fichier est partagé en sections introduites chacune par le mot-clé `Section "Description de la section"` et terminées par `EndSection`. Vous trouverez dans la suite une présentation sommaire des sections les plus importantes.

`XF86Config` est composé de plusieurs sections qui traitent chacune d'un aspect de la configuration. Une section se présente toujours sous la forme :

```
Section Description de la section
déclaration 1
déclaration 2
déclaration n
EndSection
```

Les types de sections suivants existent :

TAB. *11.1:* *Sections dans /etc/X11/XF86Config*

Type	Signification
`Fichiers`	Cette section décrit les chemins utilisés pour les jeux de caractères et la palette chromatique RGB.
`ServerFlags`	Les commutateurs généraux sont renseignés ici.
`InputDevice`	Les périphériques d'entrée sont configurés dans cette section. Les claviers et les souris aussi bien que les périphériques d'entrée spéciaux (tablettes graphiques, manettes de jeu, etc.) sont configurés ici. Les identificateurs importants sont ici `Driver` et les options qui déterminent le protocole (`Protocol`) et le périphérique (`Device`).
`Monitor`	Décrit l'écran utilisé. Les éléments de cette section sont constitués d'un nom, auquel il est ensuite fait référence lors de la définition de l'affichage (`Screen`) ainsi que la description de la bande passante (`Bandwidth`) et des fréquences de synchronisation autorisées (`HorizSync` et `VertRefresh`). Les valeurs peuvent être indiquées en MHz, en kHz ou en Hz. Le serveur refuse en principe tout *modeline* ne correspondant pas aux spécifications de l'écran. Cela permet d'éviter d'envoyer par mégarde à l'écran des fréquences trop élevées lorsque l'on essaie les modelines.

`Modes`	C'est ici que sont fixés les paramètres représentatifs de chaque résolution d'écran. Ces paramètres peuvent être calculés par SaX2 sur la base des valeurs indiquées par l'utilisateur et ne doivent pas, en règle générale, être modifiés. Vous pouvez toutefois intervenir manuellement sur ces valeurs, par exemple si vous souhaitez intégrer un écran à fréquence fixe.Une explication détaillée de chacun des paramètres sortirait du cadre de ce livre, mais vous pouvez obtenir plus de précisions sur la signification des différentes valeurs des paramètres dans le fichier HOWTO `/usr/share/doc/howto/en/XFree86-Video-Timings-HOWTO.gz`.
`Device`	Cette section définit une carte graphique donnée. Celle-ci est référencée par le nom saisi.
`Screen`	Cette section finale lie un `Monitor` (écran) et un `Device` (carte graphique) : il en résulte les déclarations nécessaires pour X.Org. La sous-section `Display` permet de renseigner la taille virtuelle de l'écran (`Virtual`), le `ViewPort` et les `Modes` utilisés avec ce Screen.
`ServerLayout`	Cette section détermine la structure d'une configuration Single ou Multihead. Les périphériques d'entrée `InputDevice` et les périphériques d'affichage `Screen` sont liés dans leur ensemble.

Les sections `Monitor`, `Device` et `Screen` sont abordées en détails. Vous trouverez plus d'information sur les autres sections dans la page de manuel de `X.Org` et dans la page de manuel de `XF86Config`.

Dans `XF86Config`, il peut exister plusieurs sections `Monitor` et `Device`. Plusieurs sections `Screen` sont également possibles ; c'est de la section suivante, `ServerLayout`, que va dépendre le choix de la section `Screen` utilisée.

11.1.1 Screen Section

La section Screen doit d'abord être considérée avec attention. Celle-ci comporte une section Monitor et une section Device, et définit quelles résolutions doivent être mises à disposition avec quelle profondeur de couleurs.

Une section Screen peut se présenter par exemple comme dans le listing 11.1.

Exemple 11.1: *La section Screen du fichier /etc/X11/XF86Config*

```
Section "Screen"
  DefaultDepth  16
  SubSection "Display"
    Depth       16
    Modes       "1152x864" "1024x768" "800x600"
    Virtual     1152x864
  EndSubSection
  SubSection "Display"
    Depth       24
    Modes       "1280x1024"
  EndSubSection
  SubSection "Display"
    Depth       32
    Modes "640x480"
  EndSubSection
  SubSection "Display"
    Depth        8
    Modes       "1280x1024"
  EndSubSection
  Device        "Device[0]"
  Identifier    "Screen[0]"
  Monitor       "Monitor[0]"
EndSection
```

La ligne `Identifier` (ici `Screen[0]`) donne à cette section un identificateur unique. On peut ensuite faire référence à cette section de manière univoque dans la section suivante `ServerLayout`. La carte graphique définie précédemment dans le fichier et l'écran sont associés de façon univoque au `Screen` dans les lignes `Device` et `Monitor`. Ce ne sont donc rien de plus que des références aux sections de périphérique et d'écran au moyen des noms (aussi appelés identificateurs) correspondants. Par la suite, nous entrerons plus dans les détails sur ces sections.

La déclaration `DefaultDepth` permet de définir la profondeur de couleurs avec laquelle le serveur démarre si aucune indication particulière ne lui est fournie au démarrage. Chaque profondeur de couleur est suivie d'une sous-section `Display`. La profondeur de couleurs valable pour la sous-section est fixée par le mot-clé `Depth`. Les valeurs possibles pour `Depth` sont 8, 15, 16 et 24. Tous les modules serveurs X n'admettent pas forcément chacune de ces valeurs.

Après la profondeur de couleurs, on fixe avec `Modes` une liste de résolutions. Le serveur X parcourt cette liste de gauche à droite. Pour chaque résolution, il cherche une `Modeline` appropriée dans la section `Modes`, en se basant sur la section `Monitor`, et qui corresponde aux capacités d'affichage de l'écran et de la carte graphique.

La première résolution appropriée, dans le sens où on l'entend ici, est celle avec laquelle démarre le serveur X (appelée *default mode*). Avec les touches Ctrl-Alt-+ gris on peut se déplacer dans la liste vers la droite, avec Ctrl-Alt-- gris vers la gauche. On peut donc faire varier la profondeur de couleur de l'écran pendant que le Système X Window est en marche.

La dernière ligne de la sous-section `Display` avec `Depth 16` se rapporte à la taille de l'écran virtuel. La taille maximale possible de l'écran virtuel dépend de la structure de la mémoire de la carte vidéo et de la profondeur de couleurs souhaitée, et non de la résolution maximale de l'écran. Comme les cartes graphiques modernes offrent une grande quantité de mémoire dédiée, elles permettent de créer des bureaux virtuels de grande taille. Notez que vous ne pourrez ensuite éventuellement plus utiliser de fonctionnalités 3D si vous remplissez pratiquement toute la mémoire graphique avec le bureau virtuel. Si la carte dispose par exemple de 16 Mo de RAM vidéo, l'écran virtuel peut atteindre une taille de 4096x4096(!) pixels avec une profondeur de couleur de 8 bits. Il est cependant vivement recommandé, spécialement pour les serveurs accélérés, de ne pas utiliser l'intégralité de la mémoire de la carte vidéo pour l'écran virtuel, puisque l'espace–mémoire non utilisé sur la carte vidéo est utilisé par ces serveurs pour différents caches pour des jeux de caractères et les domaines graphiques.

11.1.2 Device-Section

Une section Device décrit une carte graphique précise. Il peut y avoir un nombre quelconque de sections Device dans `XF86Config`, tant que leurs noms, indiqués par le mot-clé `Identifier` se différencient. En règle générale – si vous avez installé plusieurs cartes graphiques – les sections sont simplement numérotées, la première est désignée par `Device[0]`, la seconde par `Device[1]`, etc.. Vous voyez dans le fichier suivant l'extrait d'une section `Device` d'un ordinateur dans lequel est installée une carte graphique Matrox Millennium PCI :

```
Section "Device"
  BoardName     "MGA2064W"
  BusID         "0:19:0"
  Driver        "mga"
  Identifier    "Device[0]"
  VendorName    "Matrox"
  Option        "sw_cursor"
EndSection
```

Si vous utilisez SaX2 pour la configuration, la section Device devrait ressembler, à peu de choses près, à ce qui est décrit ci-dessus. En particulier,`Driver` et `BusID` dépendent bien sûr du matériel installé sur votre ordinateur et sont définis automatiquement par SaX2. Le `BusID` détermine l'emplacement PCI ou AGP dans lequel la carte graphique est enfichée. Celui-ci correspond à l'identificateur (*ID*) fourni par la commande lspci. Notez que le serveur X affiche les données en numération décimale, alors que le programme lspci les affiche en notation hexadécimale !

Avec le paramètre `Driver`, vous définissez le pilote à utiliser pour la carte graphique. Dans le cas de la carte Matrox Millennium, le module du pilote s'appelle `mga`. Le serveur X recherche ce module dans le sous-répertoire `Files` via le `ModulePath`défini dans la section `Files`. Dans une installation par défaut, c'est le répertoire `/usr/X11R6/lib/modules/drivers`. Le nom est simplement suivi de `_drv.o` , dans le cas du pilote `mga`, le fichier pilote `mga_drv.o` est chargé.

Le comportement respectif du serveur X ou du pilote peut être influencé par des options supplémentaires. Dans la section Device, l'option `sw_cursor` est proposée à titre d'exemple. Cette option désactive le curseur matériel de la souris et représente le pointeur au niveau logiciel. Suivant le module du pilote, vous disposez de différentes options que vous trouverez dans les fichiers de description des modules du pilote dans le répertoire `/usr/X11R6/lib/X11/doc`. Vous trouverez également les options valables dans les cas génériques dans les pages de manuel `man XF86Config` et `man X.Org`.

11.1.3 Sections Monitor et Modes

Les sections Monitor et la section Modes décrivent, comme les sections Device, chacune un écran. Le fichier de configuration `/etc/X11/XF86Config` peut comporter à son tour autant de sections Monitor possibles différentes. Il est ensuite établi dans la section ServerLayout quelle section Monitor est prépondérante.

Pour la définition de l'écran, encore plus que pour la description de la carte graphique, il convient que seuls des utilisateurs expérimentés ne créent une section d'écran et particulièrement une section modes. Ce qu'on appelle les Modelines sont la partie essentielle de la section modes, dans lesquelles sont indiquées les fréquences de synchronisation horizontales et verticales pour chaque résolution. Les propriétés de l'écran, en particulier les fréquences de balayage sont renseignées dans la section Monitor.

Attention

Il est préférable de ne rien changer aux modelines si on ne dispose pas d'une connaissance fondamentale du fonctionnement de l'écran et de la carte graphique, car cela pourrait provoquer, dans certains cas, la destruction de l'écran !

Attention

Ceux qui se font suffisamment confiance pour développer leurs propres configurations d'écran doivent se familiariser avec la documentation du répertoire `/usr/X11/lib/X11/doc`. Il faut mentionner expressément [6], où les fonctions du matériel et l'établissement de modelines sont décrits en détails. Vous trouverez une introduction à ce sujet dans le chapitre X.Org à cet emplacement [7].

Heureusement, il n'est aujourd'hui quasiment jamais nécessaire d'établir manuellement des modelines ou des définitions d'écrans. Si vous utilisez un écran Multisync moderne, les domaines de fréquences et les résolutions optimales peuvent être, en règle générale, directement lus à partir de l'écran via le DDC du serveur X, comme cela est mentionné dans la section de configuration SaX2. Si cela n'est pas possible, vous pouvez aussi utiliser un des modes VESA pré-configurés du serveur X. Cela devrait fonctionner sans problèmes sur presque toutes les combinaisons carte graphique/écran.

11.2 Installation et configuration de polices de caractères

L'installation de polices supplémentaires sous SUSE LINUX est très simple. Il suffit de copier les polices à l'implacement de votre choix, à deux conditions : d'une part, que celui-ci se trouve dans le chemin désignant les polices pour X11 (voir à cet effet la section *Polices X11 de base* page 285) ; d'autre part, qu'il soit un sous-répertoire des répertoires configurés dans le fichier `/etc/fonts/fonts.conf`, et ce afin que les polices soient utilisables dans le nouveau système de rendu des polices Xft (voir pour cela la section *Xft* page suivante).

Vous pouvez copier manuellement, en tant qu'utilisateur `root`, les fichiers de police dans un répertoire répondant à ces critères, par exemple à l'emplacement `/usr/X11R6/lib/X11/fonts/truetype`. Vous pouvez aussi utiliser le programme d'installation de police de KDE du centre de contrôle KDE. Le résultat est identique.

Naturellement, vous pouvez tout aussi bien créer des liens symboliques plutôt que de copier effectivement les polices, par exemple lorsque vous disposez sur une partition Windows de polices sous licence que vous souhaitez utiliser. Appelez ensuite la commande `SuSEconfig --module fonts`.

`SuSEconfig --module fonts` appelle le script `/usr/sbin/fonts-config` qui prend en charge la configuration des polices. Pour plus de détails sur ce script et ses effets, vous pouvez lire la page de manuel correspondante (`man fonts-config`).

Le type de police à installer n'a ici aucune importance, la procédure d'installation reste identique pour les polices Bitmap, les polices TrueType/OpenType et les polices PostScript Type 1. Tous ces types de police peuvent chacun être installé dans un répertoire séparé. Les polices codées en CID représentent la seule exception : reportez-vous à la section *Polices codées en CID* page 286.

11.2.1 Détails sur les systèmes de polices

X.Org contient deux systèmes de police totalement différents, d'une part le déjà ancien *Système de polices X11 de base*, d'autre part le tout nouveau système *Xft/fontconfig*. Dans ce qui suit, vous trouverez une courte présentation des deux systèmes.

Xft

Dès le début de la conception de Xft, il a été apporté le plus grand soin à la prise en charge des polices vectorielles, en particulier le lissage. Contrairement à la gestion effectuée par le système de polices X11 de base, lorsque l'on utilise Xft, c'est le programme utilisant les polices qui effectue lui-même le rendu, et non le serveur X. Ainsi, le programme en question accède aux fichiers de polices lui-même, et contrôle les moindres détails de rendu des caractères. D'une part, cela permet une représentation correcte de caractères dans de nombreuses langues, d'autre part, l'accès direct aux fichiers de polices est particulièrement intéressant pour inclure (en anglais *to embed*) les polices à l'impression et ainsi obtenir un résultat sur papier équivalent à ce qu'on observe sur l'écran.

Par défaut, sous SUSE LINUX, les deux environnements de bureau KDE et Gnome Mozilla et de nombreuses autres applications utilisent déjà Xft. Xft est ainsi d'ores et déjà utilisé par un nombre d'applications bien plus important que l'ancien système de polices X11 de base.

Xft utilise la bibliothèque Fontconfig pour trouver les polices ainsi que pour influer sur l'art et la manière dont elles sont rendues. Le comportement de fontconfig est dirigé par le fichier de configuration `/etc/fonts/fonts.conf`, qui s'étend à l'ensemble du système, et par le fichier de configuration `~/.fonts.conf` qui est spécifique à l'utilisateur. Chacun de ces fichiers de configuration fontconfig doit commencer par

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

et finir par

```
</fontconfig>
```

Pour indiquer les répertoires dans lesquels aller chercher les polices, vous pouvez saisir des lignes telles que :

```
<dir>/usr/local/share/fonts/</dir>
```

Ceci est toutefois rarement nécessaire. Le répertoire `~/.fonts`, propre à l'utilisateur, est déjà renseigné par défaut dans `/etc/fonts/fonts.conf`. Lorsqu'un utilisateur souhaite installer des polices pour son usage personnel, il lui suffit donc de les copier dans le répertoire `~/.fonts`.

Vous pouvez également introduire des règles pour modifier l'apparence des polices, par exemple

```
<match target="font">
 <edit name="antialias" mode="assign">
  <bool>false</bool>
 </edit>
</match>
```

pour désactiver le lissage pour l'ensemble des polices, ou bien

```
<match target="font">
 <test name="family">
  <string>Luxi Mono</string>
  <string>Luxi Sans</string>
 </test>
 <edit name="antialias" mode="assign">
 <bool>false</bool>
 </edit>
</match>
```

lorsque vous ne souhaitez le désactiver que pour des polices bien définies.

La plupart des applications utilisent par défaut les noms de police `sans-serif` (ou son équivalent : `sans`), `serif` ou `monospace`. Ce ne sont pas des polices réelles mais simplement des redirections qui pointent vers les polices appropriées en fonction de la langue configurée.

Chaque utilisateur peut ainsi intégrer à son fichier `~/.fonts.conf` des règles simples pour faire pointer ces redirections vers ses polices favorites :

```
<alias>
 <family>sans-serif</family>
 <prefer>
  <family>FreeSans</family>
 </prefer>
</alias>
<alias>
 <family>serif</family>
 <prefer>
  <family>FreeSerif</family>
 </prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer>
  <family>FreeMono</family>
 </prefer>
</alias>
```

Comme la plupart des applications utilisent par défaut ce système de redirection, ces règles peuvent s'appliquer à la quasi-totalité du système. Ainsi, vous pouvez utiliser presque partout vos polices préférées, à peu de frais, sans avoir à modifier individuellement la configuration de chaque programme.

Pour obtenir une liste des polices installées et disponibles, vous pouvez utiliser la commande `fc-list`.

`fc-list ""` renvoie par exemple la liste de toutes les polices. Si vous souhaitez connaître les polices vectorielles (`:outline=true`) disposant de tous les caractères hébraïques (`:lang=he`) disponibles dans le système, et que vous voulez obtenir, pour chacune de ces polices, le nom (`family`), le style (`style`), la graisse (`weight`) et le nom du fichier contenant cette police, vous pouvez utiliser par exemple la commande suivante :

```
fc-list ":lang=he:outline=true" family style weight file
```

Le résultat d'une telle commande pourrait avoir l'allure suivante :

```
/usr/X11R6/lib/X11/fonts/truetype/FreeSansBold.ttf: FreeSans:style=Bold:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSerif.ttf: FreeSerif:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeMono.ttf: FreeMono:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSans.ttf: FreeSans:style=Medium:weight=80
/usr/X11R6/lib/X11/fonts/truetype/FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
/usr/X11R6/lib/X11/fonts/truetype/FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

Les paramètres essentiels pouvant être utilisés avec `fc-list` sont :

TAB. *11.2:* *Paramètres possibles pour fc-list*

Paramètres	Signification et valeurs possibles
family	Nom de la famille de police, par exemple `FreeSans`
foundry	Société ayant produit la police, par exemple `urw`
style	Style de la police, par exemple `Medium`, `Regular`, `Bold`, `Italic`, `Heavy`, ...
lang	Langues prises en charge par la police ; par exemple `fr` pour le français, `ja` pour le japonais, `zh-TW` pour le chinois traditionnel, `zh-CN` pour le chinois simplifié ...
weight	*Graisse* de la police, par exemple `80` pour une police maigre, `200` pour une police grasse.
slant	*Degré de cursivité*, principalement `0` pour une police non cursive, `100` pour une police cursive.

file	Nom du fichier contenant la police
outline	`true` s'il s'agit d'une police "Outline", `false` sinon.
scalable	`true` s'il s'agit d'une police vectorielle, `false` sinon.
bitmap	`true` s'il s'agit d'une police bitmap, `false` sinon.
pixelsize	Taille de la police en pixels. Cette option utilisée avec fc-list n'a de sens que pour les polices bitmap.

Polices X11 de base

Actuellement, le système de polices X11 de base prend en charge non seulement les polices bitmap, mais aussi les polices vectorielles telles que les polices Type1, les polices TrueType/OpenType ou encore les polices codées en CID. Les polices unicode sont également déjà prises en charge depuis longtemps.

À l'origine, le système de polices X11 de base a été développé en 1987 pour X11R1 afin de gérer les polices bitmap monochromes. On constate que, jusqu'à aujourd'hui, toutes les extensions mentionnées ci-dessus ont été introduites ultérieurement dans le système.

Ainsi, par exemple, les polices vectorielles ne sont prises en charge que sans lissage et sans rendu à précision subpixel ; le chargement de polices vectorielles de grande taille, gérant les caractères pour plusieurs langues, peut être particulièrement lent. L'utilisation de polices unicode peut aussi s'avérer lent et utiliser plus de mémoire.

Le système de polices X11 de base possède quelques faiblesses de fond. On peut raisonnablement dire qu'il a vieilli et qu'il n'est plus sensé de chercher à développer des extensions. Pour des raisons de compatibilité ascendante, il reste disponible, mais il est conseillé d'utiliser, dès que possible, le système Xft/fontconfig, bien plus moderne.

Veillez toutefois à ce que le serveur X utilise uniquement les répertoires qui

- sont renseignés en tant que `FontPath`dans la section `Files` du fichier `/etc/X11/XF86Config`.
- possèdent un fichier `font.dir` valide (un tel fichier est généré par SuSEconfig).
- ne sont pas libérés pendant l'exécution du serveur X par la commande `xset -fp`.
- ou, respectivement, sont intégrés en cours d'exécution du serveur X à l'aide de la commande`xset +fp`.

Lorsque le serveur X est déjà lancé, des polices qui viennent d'être installées dans des répertoires déjà intégrés peuvent être mises à disposition à l'aide de la commande `xset fp rehash`. Cette commande est également appelée auparavant par `SuSEconfig --module fonts`.

Comme la commande `xset` nécessite un accès au serveur X en cours d'exécution, ceci ne peut fonctionner que si `SuSEconfig --module fonts` est lancée à partir d'un interpréteur de commandes ayant un accès au serveur X qui s'exécute. Le plus simple pour parvenir à ce résultat est d'utiliser la commande `sux` et de saisir le mot de passe de `root` dans un terminal pour prendre la main en tant qu'utilisateur `root` : `sux` transmet à l'interpréteur `root` les droits de l'utilisateur ayant lancé le serveur X.

Pour tester si les polices ont été installées correctement et sont disponibles dans le système de polices X11 de base, vous pouvez utiliser la commande `xlsfonts` qui dresse la liste de toutes les polices disponibles.

SUSE LINUX utilise par défaut l'encodage UTF-8 local, en conséquence, il vous est conseillé d'utiliser en règle générale les polices Unicode, que vous pouvez reconnaître, en demandant la liste des polices avec la commande `xlsfonts`, à leur terminaison en `iso10646-1`. Vous pouvez ainsi obtenir la liste de toutes les polices Unicode disponibles à l'aide de la commande `xlsfonts | grep iso10646-1`.

La quasi-totalité des polices Unicode disponibles dans SUSE LINUX contiennent a minima tous les caractères nécessaires pour les langues européennes, pour lesquelles les encodages utilisés autrefois étaient de la forme `iso-8859-*`.

Polices codées en CID

Contrairement aux autres types de polices, les polices codées en CID ne peuvent pas être installées dans un répertoire quelconque. Elles doivent toujours être installées dans le répertoire `/usr/share/ghostscript/Resource/CIDFont`. Cela n'a pas une importance capitale pour Xft/fontconfig, en revanche Ghostscript et le système de polices X11 de base l'exigent.

Remarque

Des informations complémentaires concernant les polices dans le système X11 sont disponibles à l'adresse `http://www.xfree86.org/current/fonts.html`.

Remarque

11.3 Configuration de OpenGL/3D

Sous Linux, Direct3D n'est disponible que sur les systèmes x86 et compatibles en tant que partie de l'émulateur Windows WINE qui utilise l'interface OpenGL pour son implémentation.

11.3.1 Prise en charge du matériel

SUSE LINUX comprend divers pilotes OpenGL pour la prise en charge du matériel 3D. Vous trouverez un aperçu dans le tableau 11.3.

TAB. *11.3:* *Matériel 3D pris en charge*

Pilote OpenGL	Matériel pris en charge
nVidia	Chipset nVidia : tous sauf Riva 128(ZX)
DRI	3Dfx Voodoo Banshee, 3Dfx Voodoo-3/4/5, Intel i810/i815/i830M, Intel 845G/852GM/855GM/865G, Matrox G200/G400/G450/G550, ATI Rage 128(Pro)/Radeon

Lors d'une première installation avec YaST, la 3D peut être activée dès l'installation, si YaST offre la prise en charge correspondante. En présence de composants graphiques nVidia, il faut d'abord installer le pilote nVidia. Pour cela, choisissez pendant l'installation le correctif du pilote nVidia dans YOU (YaST Online Update). Nous ne pouvons malheureusement pas vous fournir le pilote nVidia pour des questions de licence.

Si une mise à jour a été installée, la prise en charge du matériel 3D doit être configurée de manière différente. La procédure dépend là du pilote OpenGL à utiliser et est expliquée plus précisément dans la section suivante.

11.3.2 Pilote OpenGL

nVidia et DRI

Ces pilotes OpenGL peuvent être aisément configurés avec SaX2. Notez que pour des cartes nVidia, le pilote nVidia doit être installé au préalable (voir plus haut). Utilisez la commande `3Ddiag` pour vérifier si la configuration de nVidia ou DRI est correcte.

Pour des raisons de sécurité, seuls les utilisateurs du groupe `video` ont accès au matériel 3D. Assurez-vous par conséquent que tous les utilisateurs travaillant localement sur l'ordinateur se sont enregistrés dans le groupe `video`. Sinon, on utilise pour les programmes OpenGL le plus lent *Software Rendering Fallback* du pilote OpenGL. Utilisez la commande `id` pour vérifier si l'utilisateur actuel appartient au groupe `video`. Si ce n'est pas le cas, vous pouvez l'ajouter à ce groupe avec YaST.

11.3.3 Outil de diagnostic 3Ddiag

Pour pouvoir vérifier la configuration 3D sous SUSE LINUX, vous disposez de l'outil de diagnostic 3Ddiag. Veuillez noter qu'il s'agit d'un outil en ligne de commande que vous devez utiliser dans un terminal.

Le programme vérifie, par exemple, la configuration de X.Org, si le paquetage correspondant pour la prise en charge 3D est installé et si la bibliothèque OpenGL ainsi que l'extension GLX correctes sont utilisées. Veuillez suivre les instructions de 3Ddiag quand apparaissent des messages "failed". En cas de succès, seuls des messages "done" sont affichés à l'écran.

`3Ddiag -h` détaille les options admises pour 3Ddiag.

11.3.4 Programmes test pour OpenGL

Outre `glxgears`, des jeux comme `tuxracer` et `armagetron` (paquetage du même nom) conviennent bien comme programmes de test pour OpenGL. Si la prise en charge de la 3D est activée, ils s'affichent de manière fluide sur l'écran d'un ordinateur à peu près actuel. Sans prise en charge de la 3D, ceci est insensé (effet diapositives). L'affichage de `glxinfo` informe précisément de l'état d'activation de la prise en charge de la 3D. `direct rendering` doit ici être sur `Yes`.

11.3.5 Dépannage

Si le résultat du test 3D OpenGL s'avère être négatif, (pas de jeu fluide possible), vérifiez d'abord avec 3Ddiag s'il n'existe pas d'erreur de configuration (messages `failed`), et dans ce cas les réparer. Si cela ne change rien ou s'il n'y avait aucune erreur failed, il suffit souvent de consulter les fichiers Log de X.Org. Ici, on trouve souvent dans `/var/log/Xorg.0.log` de X.Org la ligne `DRI is disabled`. Il peut y avoir plusieurs causes que l'on ne peut cependant trouver qu'en effectuant un examen précis du fichier Log, ce qui souvent dépasse le débutant.

Dans ces cas, il ne s'agit pas en règle générale d'une erreur de configuration puisque celle-ci aurait déjà été détectée par 3Ddiag. Donc, il ne reste plus que le Software Rendering Fallback du pilote DRI, qui n'offre cependant aucune prise en charge de la 3D. De même, il vaut mieux renoncer à l'utilisation de la prise en charge de la 3D quand surviennent des erreurs de représentation OpenGL ou même des problèmes de stabilité. Utilisez SaX2 pour désactiver la prise en charge de la 3D.

11.3.6 Assistance à l'installation

Outre le Software Rendering Fallback du pilote DRI, tous les pilotes OpenGL sous Linux sont encore au stade de développement et ne sont à considérer que comme expérimentaux. Nous avons cependant pris la décision de fournir les pilotes dans cette distribution, car il y a une grosse demande d'accélération matérielle 3D sous Linux. En raison du stade actuel expérimental des pilotes OpenGL, nous ne pouvons cependant pas étendre le cadre de l'assistance à l'installation à la configuration de l'accélération matérielle 3D et ne pouvons pas vous venir en aide en cas de problèmes s'y rapportant. L'installation de base de l'interface utilisateur graphique X11 ne comprend donc en aucun cas aussi l'installation de l'accélération matérielle 3D. Cependant nous espérons que ce chapitre a déjà répondu à beaucoup de vos questions à ce sujet. Si vous rencontrez des problèmes avec la prise en charge du matériel 3D, nous vous conseillons, en cas de doute, de vous passer de cette prise en charge.

11.3.7 Suite de la documentation en ligne

- DRI: `/usr/X11R6/lib/X11/doc/README.DRI` (`xorg-x11-doc`)

Imprimante (utilisation)

Dans ce chapitre nous abordons des connaissances de base sur le fonctionnement de l'imprimante. Ce chapitre sert aussi en particulier à apporter des solutions appropriées aux problèmes de fonctionnement des imprimantes en réseau.

12.1 Préparatifs et autres considérations

CUPS est le système d'impression par défaut sous SUSE LINUX. CUPS est très "orienté utilisateur". Dans de nombreux cas, il est compatible avec LPRng ou peut le devenir de façon relativement aisée. Ce n'est que pour des raisons de compatibilité que LPRng est compris dans la distribution de SUSE LINUX.

Les imprimantes se distinguent par leurs interfaces (USB, réseau) ainsi que par les langages d'impression. Lors de l'achat d'une imprimante, il convient d'accorder de l'importance tant à une interface appropriée prise en charge par le matériel, qu'au langage d'impression.

On peut, pour simplifier, répartir les imprimantes dans les trois catégories suivantes de langages d'impression :

Imprimantes PostScript PostScript est le langage d'impression dans lequel la plupart des travaux d'impression sous Linux/Unix sont générées et traités en interne par le système d'impression. Ce langage, très puissant, est déjà ancien. Lorsque les documents PostScript peuvent être traités directement par l'imprimante et ne nécessitent pas d'étapes de transformation supplémentaires au sein du système d'impression, le nombre de sources d'erreur potentielles s'en trouve réduit. Comme les imprimantes PostScript sont soumises à une licence et que les coûts qui en découlent ne sont pas négligeables, ces imprimantes sont généralement plus onéreuses que les imprimantes non dotées d'un interpréteur PostScript.

Langages d'impression usuels comme PCL et ESC/P
Ces langages d'impression existent depuis longtemps, mais sont encore aujourd'hui étendus pour pouvoir s'adapter aux dernières évolutions des imprimantes. Lorsqu'il s'agit de langages d'impression usuels, les travaux du système d'impression PostScript peuvent être transformés à l'aide de Ghostscript dans le langage d'impression (on dit "interprétés"). Les langages les plus connus sont PCL, que l'on trouve essentiellement dans les imprimantes HP et leurs "clones" ainsi que ESC/P, répandu dans les imprimantes Epson. On peut partir du principe que ce type de langages d'impression donnera aussi de bons résultats d'impression sous Linux. À part les pilotes `hpijs` développés par la société HP elle-même, il n'existe actuellement (en 2004) aucun fabricant d'imprimantes qui développe des pilotes pour Linux et les met à la disposition des distributeurs Linux sous une licence OpenSource. Les imprimantes de cette catégorie se situent le plus souvent dans une fourchette de prix moyenne.

Imprimantes propriétaires, le plus souvent des imprimantes GDI
Dans la catégorie des imprimantes propriétaires, il n'existe normalement qu'un ou des pilotes Windows. Avec ces imprimantes, aucun langage d'impression usuel n'est implémenté, et le langage d'impression lui-même peut varier d'une version du modèle à l'autre.
Pour plus d'informations sur cette problématique, reportez-vous également à la section *Imprimante sans langage d'impression standard* page 306.

Avant d'acheter une nouvelle imprimante, il convient de consulter les sources d'information suivantes afin de connaître le degré de prise en charge offert pour l'imprimante choisie :

- `http://cdb.suse.de/` ou `http://hardwaredb.suse.de/` — la base de données d'imprimantes de SUSE LINUX
- `http://www.linuxprinting.org/` — la base de données d'imprimantes sur Linuxprinting.org
- `http://www.cs.wisc.edu/~ghost/` — la page d'accueil de Ghostscript
- `file:/usr/share/doc/packages/ghostscript/catalog.devices` — les pilotes intégrés

Il va de soi que les bases de données en ligne indiquent toujours l'état actuel de la prise en charge sous Linux et qu'un produit ne peut pas offrir un pilote publié après sa date de fabrication ; il est donc possible qu'une imprimante actuellement classée comme "parfaitement prise en charge" ne l'était en fait pas encore au moment de la production de SUSE LINUX. Les bases de données n'indiquent donc pas nécessairement l'état correct, mais plutôt une bonne approximation — seule la base de données d'imprimantes de SUSE LINUX vous permet de vérifier quelles sont les imprimantes prises en charge par la présente version du logiciel.

12.2 Raccordement de l'imprimante

On peut raccorder une imprimante au système de plusieurs façons. Avec le système d'impression CUPS, le fait qu'une imprimante soit reliée au système en local ou en réseau n'a pas d'influence sur la configuration. Sous Linux, les imprimantes locales sont connectées exactement comme le décrit le manuel fourni par le fabricant de l'imprimante. CUPS prend en charge les types de connexion suivants : "série", "USB", "parallèle" et "SCSI". En ce qui concerne le raccordement des imprimantes, lisez également l'article présentant des notions de base *CUPS in a Nutshell* (en anglais) dans la base de données d'assistance à l'adresse `http://portal.suse.com`. Indiquez *cups* dans le formulaire de recherche.

Attention

Raccordement par câble à l'ordinateur

Lors du câblage à l'ordinateur, il faut savoir que seules les liaisons USB sont prévues pour être connectées ou déconnectées en cours de fonctionnement. On ne devrait modifier les autres branchements que lorsque l'ordinateur est éteint.

Attention

12.3 Installation du logiciel

"PostScript Printer Description" (PPD) est le langage informatique qui décrit les propriétés (la résolution) et les options (le mode duplex) des imprimantes. Ces decriptions sont nécessaires pour pouvoir utiliser les différentes options de l'imprimante sous CUPS. Sans fichier PPD, les données d'impression sont transmises à l'imprimante à l'état "brut", ce qui n'est en général pas souhaitable. Avec SUSE LINUX, beaucoup de fichiers PPD sont pré-installés afin de pouvoir utiliser même des imprimantes qui ne prennent pas en charge PostScript.

Avec une imprimante PostScript, il est recommandé de se procurer le fichier PPD approprié ; le paquetage `manufacturer-PPDs` en contient une multitude qui sont installés automatiquement lors d'une installation standard. Reportez-vous aux sections *Fichiers PPD se trouvant dans différents paquetages* page 303 et *Il manque un fichier PPD adapté à l'imprimante PostScript* page 307.

On peut placer les nouveaux fichiers PPD dans le répertoire `/usr/share/cups/model/` ou de les ajouter avec YaST au système d'impression. Reportez-vous pour cela à la section *Configuration manuelle* page 66. On choisira de préférence un tel fichier PPD lors de l'installation.

La prudence est cependant de mise si un fabricant d'imprimantes demande non seulement de modifier les fichiers de configuration mais également d'installer des paquetages logiciels complets. D'une part, une telle installation vous fait perdre l'assistance SUSE ; d'autre part, il se peut que les commandes d'impression ne fonctionnent plus comme auparavant et qu'il ne soit plus possible de piloter des périphériques provenant d'autres fabricants. C'est pourquoi il est en général déconseillé d'installer le logiciel fourni par le fabricant.

12.4 Configuration de l'imprimante

Après avoir connecté l'imprimante à l'ordinateur et installé le logiciel, il faut configurer l'imprimante au niveau du système. Si possible, n'utilisez pour cela que les outils fournis avec SUSE LINUX. Comme la sécurité est très importante pour SUSE LINUX, les outils provenant de tiers ne sont pas toujours adaptés aux restrictions imposées par la sécurité et s'avérent ainsi souvent plus problématiques qu'utiles.

12.4.1 Imprimantes locales

Si, lors de la connexion, une imprimante locale qui n'a pas encore été configurée est détectée, un module de YaST sera lancé afin de pouvoir procéder à la configuration ; voir la section *Configuration avec YaST* page 65. Pour la configuration à l'aide d'outils en mode de ligne de commande (voir ci-dessous) un URI de périphérique est nécessaire. Il peut s'agir de `parallel:/dev/lp0` (imprimante sur le premier port parallèle) ou de `usb:/dev/usb/lp1` (première imprimante reconnue sur le port USB).

12.4.2 Imprimante réseau

Une imprimante réseau est capable de prendre en charge plusieurs protocoles, dont certains même simultanément. La plupart des protocoles reconnus sont standardisés ; il n'est pourtant pas exclu que le standard soit étendu ou modifié par les fabricants, soit parce qu'ils testent sur des systèmes sous lesquels le standard n'est pas correctement implémenté, soit parce qu'ils souhaitent certaines fonctions qui n'existent pas dans le standard. Ils n'offrent de tels pilotes que pour certains systèmes d'exploitation, dont Linux fait malheureusement rarement partie. Pour le moment, on ne peut pas considérer que tous les protocoles fonctionnent sous Linux sans poser de problèmes, et il convient d'expérimenter différentes possibilités afin d'obtenir une configuration qui fonctionne.

Sous CUPS, les protocoles `socket`, `LPD`, `IPP` et `smb` sont pris en charge. Vous trouverez ci-après quelques informations détaillées concernant ces protocoles :

socket On désigne sous le nom de "socket" une liaison dans laquelle les données sont envoyées sur un socket internet sans prise de contact (*handshake* préalable. Les numéros de port socket typiquement utilisés sont `9100` ou `35`. Un exemple d'URI de périphérique : `socket://`⟨*host-printer*⟩`:9100/`

LPD (Line Printer Daemon) Le protocole LPD est traditionnellement éprouvé. LPD signifie "Line Printer Daemon" et est décrit dans le RFC 1179. Ce protocole comprend l'envoi de quelques données concernant le travail avant l'envoi des données d'impression proprement dites, la file d'attente. C'est la raison pour laquelle il est nécessaire d'indiquer également une file d'attente lors de la configuration du protocole LPD pour la transmission de données. Les implémentations de divers fabricants d'imprimantes sont réalisées de façon tellement souple qu'elles acceptent n'importe quel nom comme file d'attente. Le nom à utiliser se trouve, en cas de besoin, dans le manuel d'utilisation de l'imprimante. Très souvent, les noms sont LPT, LPT1, LP1 ou des noms du même genre. Il est bien sûr possible de configurer de la même manière une file d'attente LPD sur un autre ordinateur basé sur Linux ou sur Unix dans le système CUPS. Le numéro du port du service LPD est `515`. Exemple d'URI de périphérique : `lpd://`⟨*`host-printer`*⟩`/LPT1`

IPP (Internet Printing Protocol) L'Internet Printing Protokoll, en abrégé IPP, est encore relativement récent (il date de 1999) et est basé sur le protocole HTTP. IPP est le protocole le plus utilisé pour envoyer les données concernant le travail. CUPS se sert de IPP pour la transmission interne de données. On choisira ce protocole si l'on souhaite établir une file d'attente de redirection entre deux serveurs CUPS. Ici encore, le nom de la file d'attente d'impression est nécessaire afin de pouvoir configurer correctement IPP. Le numéro de port pour IPP est `631`. Exemple d'URI de périphérique : `ipp://`⟨*`host-printer`*⟩`/ps` ou `ipp://`⟨*`host-cupsserver`*⟩`/printers/ps`

SMB (partage Windows) CUPS prend finalement en charge l'impression sur des imprimantes sur le partage Windows. Le protocole correspondant est le SMB et les numéro de port `137`, `138` et `139` sont utilisés. Exemple d'URI de périphérique : `smb://`⟨*`user`*⟩`:`⟨*`password`*⟩`@`⟨*`workgroup`*⟩`/`⟨*`server`*⟩`/`⟨*`printer`*⟩ ou `smb://`⟨*`user`*⟩`:`⟨*`password`*⟩`@`⟨*`host`*⟩`/`⟨*`printer`*⟩ ou `smb://`⟨*`server`*⟩`/`⟨*`printer`*⟩

Avant de procéder à la configuration, il faut par conséquent trouver le protocole reconnu par l'imprimante. S'il n'est pas indiqué par le fabricant, il est possible de le rechercher en saisissant la commande `nmap` (paquet `nmap`). `nmap` examine un hôte pour trouver des ports libres ; voici un exemple :

```
nmap -p 35,137-139,515,631,9100-10000 <adresse IP de l'imprimante>
```

12.4.3 Opérations de configuration

Configuration d'une imprimante réseau

La configuration d'une imprimante réseau s'effectue en utilisant YaST ; YaST facilite la configuration et les limitations imposées par la sécurité de CUPS ne lui posent aucun problème ; voir aussi la section *Interface web (CUPS) et administration sous KDE* page 301 .

Configuration de CUPS dans le réseau

Consultez sous `http://portal.suse.com` l'article de base *CUPS in a nutshell*, qui pourra vous servir de guide en ce qui concerne la configuration de "CUPS dans le réseau". Saisissez le mot-clé *cups* pour faire une recherche dans la base de données support.

On fait, pour "CUPS dans le réseau", la distinction entre les trois principaux sujets suivants :

1. Configurez sur le serveur les files d'attente pour les imprimantes faisant partie du serveur.
2. Autorisez l'accès aux files d'attente se référant aux ordinateurs clients.
3. Activez l'envoi d'informations de navigation aux ordinateurs clients.

Pour le point 1, on différencie les cas de figure suivants :

Imprimante de réseau ou boîte de serveur d'impression
via socket TCP : avec filtrage local (par défaut) ou sans filtrage local
via protocole LPD : avec filtrage local (par défaut) ou sans filtrage local
via protocole IPP : avec filtrage local (par défaut) ou sans filtrage local
Pour plus d'informations détaillées sur les protocoles, consultez la section *Imprimante réseau* page 295.

File d'attente sur serveur LPD (toujours via protocole LPD)
sans filtrage local (par défaut) ou avec filtrage local

File d'attente sur serveur IPP (toujours via protocole IPP)
sans filtrage local (par défaut) ou avec filtrage local

File d'attente sur serveur SMB (toujours via protocole SMB)
avec filtrage local (par défaut) ou sans filtrage local

File d'attente sur serveur (toujours via Novell IPX)
avec filtrage local (par défaut) ou sans filtrage local

File d'attente via d'autres URI avec ou sans filtrage local

Pour le point 2, les préréglages sont habituellement suffisants ; en cas de doute, consultez l'article de portail mentionné ci-dessus.

Pour le point 3, procédez avec YaST aux étapes suivantes :

1. 'Démarrer la configuration de l'imprimante YaST' → 'Modifier...' → 'Etendu' → 'Réglages du serveur CUPS'
2. Ensuite : 'Scruter les adresses' → 'Ajouter' L'adresse IP de transmission du réseau doit être entrée à cet endroit ou alors `@LOCAL`.
3. La configuration se termine par les actions suivantes (tous les boutons se trouvent toujours en bas à droite) : 'OK' → 'Suivant' → 'Appliquer' → 'Terminer'

Configuration avec les outils en mode ligne de commande

Une autre variante consiste à configurer CUPS par l'intermédiaire des outils de la ligne de commande. Si tout est déjà préparé (le fichier PPD est connu ainsi que le nom de l'URI de périphérique), il suffit de procéder comme suit :

```
lpadmin -p <nom de file> -v <URI de périphérique> \
 -P <fichier PPD> -E
```

Veillez à ce que le `-E` ne soit pas la première option car pour toutes les commandes de CUPS, `-E` en tant que premier argument signifie qu'il faut utiliser une liaison chiffrée (en anglais encrypted) et non, comme on en a l'intention ici, activer l'imprimante (en anglais enable). Voici un exemple concret :

```
lpadmin -p ps -v parallel:/dev/lp0 \
  -P /usr/share/cups/model/Postscript.ppd.gz -E
```

Exemple analogue pour une imprimante réseau :

```
lpadmin -p ps -v socket://192.168.1.0:9100/ \
  -P /usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Modifier des options

YaST propose lors de l'installation d'activer certaines options par défaut. On peut modifier ces options à chaque travail d'impression (dans les limites de ce que permet l'outil d'impression utilisé) ; on peut toutefois aussi redéfinir ces réglages plus tard (avec YaST).

En utilisant les outils en mode ligne de commande, on procède comme suit :

1. On affiche d'abord toutes les options :

   ```
   lpoptions -p <file> -l
   ```

   Exemple :

   ```
   Resolution/Output Resolution: 150dpi *300dpi 600dpi
   ```

2. L'option activée par défaut se reconnaît au moyen de l'astérisque : *
3. Modifiez ensuite une option à l'aide de `lpadmin` :

   ```
   lpadmin -p <file> -o Resolution=600dpi
   ```

4. Vérifiez que tout a fonctionné correctement :

   ```
   lpoptions -p <file> -l

   Resolution/Output Resolution: 150dpi 300dpi *600dpi
   ```

12.5 Particularités de SUSE LINUX

CUPS a été adapté par endroits pour être utilisé sous SUSE LINUX. Pour comprendre l'intégration, il est nécessaire de présenter ici quelques-unes des modifications les plus importantes.

12.5.1 Le serveur CUPS et le pare-feu

Il y a de nombreuses manières de déclarer CUPS en tant que client d'un serveur réseau.

1. On peut, pour chaque file d'attente sur le serveur réseau, mettre en place une file d'attente locale et transmettre par son intermédiaire toutes les demandes aux files d'attentes correspondantes sur le serveur. Cette méthode n'est en règle générale pas conseillée, car si la configuration du serveur réseau est modifiée, cela nécessite de reconfigurer toutes les machines clientes.
2. Il est possible de relayer des travaux d'impression directement sur un serveur réseau en particulier. Pour une telle configuration, il n'est pas nécessaire d'avoir un Démon CUPS actif ; la commande `lpr` (ou tout appel de la bibliothèque correspondante par d'autres programmes) permet d'envoyer des travaux directement sur un serveur réseau. Toutefois, une telle configuration ne fonctionne pas si l'on souhaite imprimer sur une imprimante locale.
3. Il est possible d'écouter les diffusions IPP. Le démon CUPS peut se tenir à l'écoute de tels paquets de diffusion IPP envoyés par d'autres serveurs réseau qui souhaitent signaler la mise à disposition des files d'attentes inactives. C'est la meilleure manière de régler CUPS lorsque l'on souhaite pouvoir imprimer sur des serveurs CUPS distants. Une telle configuration comporte toutefois le risque qu'un attaquant fasse en sorte que des diffusions IPP mentionnant des files d'attentes semblent provenir du démon. Le démon local accède ensuite à ces files d'attentes, et lorsque l'attaquant propose une file d'attente portant le même nom qu'une autre file du serveur local, et que le paquet IPP a été intercepté auparavant, alors l'utilisateur croit avoir transmis un travail au serveur local — mais, en réalité, le travail parvient au serveur de l'attaquant. Lorsque l'on souhaite utiliser cette méthode, le port UDP 631 doit être ouvert aux paquets entrants.

YaST dispose de deux méthodes pour trouver le serveur CUPS :

1. Parcourir le réseau (le "scannen"), c'est-à-dire demander à toutes les machines d'un réseau si elles proposent ce service.
2. Surveiller la diffusion IPP, en suivant la même méthode que celle que l'on a décrit auparavant. Cette méthode est également utilisée pendant l'installation pour trouver les serveurs CUPS proposés.

La deuxième méthode suppose que le port UDP accepte les paquets entrants.

Il faut encore ajouter, au sujet des pare-feux, les remarques suivantes : la configuration par défaut du pare-feu (telle qu'elle est suggérée) est de ne permettre *aucune* diffusion IPP sur une interface. Cela signifie que la deuxième méthode de détection ainsi que l'accès aux files d'attente distantes suivant la troisième méthode ne peuvent pas fonctionner. Il est de plus impératif de modifier la configuration du pare-feu : soit l'une des interfaces où le port est ouvert par défaut doit être marquée comme `internal`, soit le port d'une des interfaces ouvertes vers l'extérieur (`external`) doit être ouvert de façon ciblée. En effet, pour des raisons de sécurité, aucune des interfaces de la configuration prédéfinie ne peut être ouverte. Même le fait de n'ouvrir que pour détecter les serveurs afin de pouvoir configurer l'accès aux files distantes suivant la méthode 2 constitue un problème de sécurité — il est possible que des utilisateurs ne lisent pas ce qui est proposé et acceptent ainsi le serveur d'un agresseur.

Pour résumer, nous pouvons dire que l'utilisateur doit modifier la configuration du pare-feu qui lui est proposée de manière à permettre à CUPS de trouver les files d'attente distantes au cours de l'installation. ('Port ouvert dans le pare-feu') et par la suite, en fonctionnement normal, à permettre l'accès aux différents serveurs distants depuis le système local. On peut aussi envisager que l'utilisateur lance la recherche du serveur CUPS tout en analysant activement les ordinateurs du réseau local ou en configurant à la main toutes les files d'attente, bien que nous ne conseillons pas cette possibilitée pour les raisons évoquées auparavant.

12.5.2 Interface web (CUPS) et administration sous KDE

Afin de pouvoir utiliser l'administration par l'interface web (de CUPS) ou par l'outil d'administration de l'imprimante (de KDE), l'utilisateur doit être déclaré en tant qu'administrateur CUPS avec le groupe d'administration de CUPS `sys` et un mot de passe pour CUPS ; pour cela, saisissez en tant que la commande suivante :

```
lppasswd -g sys -a root
```

Dans d'autres cas, l'administration depuis l'interface web ou depuis l'outil d'administration n'est pas possible car l'authentification échoue si aucun administrateur CUPS n'est installé. Au lieu de , on peut également définir un autre utilisateur en tant qu'administrateur CUPS ; voir la section suivante : *Modifications du démon cupsd* page suivante .

12.5.3 Modifications du démon cupsd

Le paquetage originel de cups a subi quelques modifications sous SUSE LINUX. Ces modifications sont présentées rapidement dans ce qui suit. Plus d'informations sur ce sujet sont disponibles dans l'article suivant de la base de donnée d'assistance "Printer configuration in SUSE LINUX 9.1 on" (article en anglais) sur `http://portal.suse.com`. Saisissez comme critère de recherche *Printing*.

Le démon cupsd fonctionne en tant qu'utilisateur lp

Après le démarrage, `cupsd` passe de l'utilisateur à l'utilisateur `lp`, ce qui augmente la sécurité car le service d'impression CUPS ne fonctionne pas avec des droits illimités, mais uniquement avec les droits nécessaires au service d'impression.

L'inconvénient résulte cependant dans le fait que l'authentification (à savoir : la vérification du mot de passe) ne peut pas s'effectuer par le biais de `/etc/shadow` étant donné que `lp` n'a pas accès à `/etc/shadow`, ce qui signifie que l'authentification spécifique de CUPS via `/etc/cups/passwd.md5` doit être utilisée. Pour ce faire, l'administrateur CUPS, le groupe d'administration CUPS `sys` et le mot de passe CUPS doivent être déclarés dans `/etc/cups/passwd.md5` ; en tant qu'utilisateur il faut saisir :

```
lppasswd -g sys -a <nom admin CUPS>
```

Autres conséquences :

- Lorsque `cupsd` fonctionne en tant que `lp`, le fichier `/etc/printcap` ne peut pas être créé, car `lp` n'est pas autorisé à créer des fichiers dans /etc/. C'est la raison pour laquelle cupsd crée `/etc/cups/printcap`. `/etc/printcap` est un lien symbolique vers `/etc/cups/printcap` afin que les programmes applicatifs qui ne peuvent lire le nom de la file d'attente que depuis `/etc/printcap` puissent continuer à fonctionner correctement.
- Dès que cupsd fonctionne en tant que `lp` il est impossible d'ouvrir le port 631. C'est pourquoi cupsd ne peut plus être rechargé par le biais de `rccups reload`. Il convient dont d'utiliser `rccups restart`.

Fonctionnalité généralisée pour BrowseAllow/BrowseDeny

Les conditions d'accès configurées pour BrowseAllow et BrowseDeny se réfèrent à tous les types de paquets envoyés au démon cupsd. Les réglages par défaut dans `/etc/cups/cupsd.conf` sont :

```
BrowseAllow @LOCAL
BrowseDeny All
```

et

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
  Allow From @LOCAL
</Location>
```

On peut ainsi accéder exactement aux ordinateurs de type `LOCAL` sur le démon cupsd à un serveur CUPS. Les ordinateurs de type `LOCAL` sont des ordinateurs dont l'adresse IP n'appartient pas à une interface point-à-point (à savoir : les interfaces dont le flag `IFF_POINTOPOINT` n'est pas à 1) et dont l'adresse IP appartient au même réseau que le serveur CUPS. Tous les autres ordinateurs rejettent immédiatement quelque paquet que ce soit.

Le démon cupsd est activé par défaut

Lors d'une installation standard, le démon cupsd est automatiquement activé, ce qui permet d'accéder confortablement aux files d'attente de serveurs réseau CUPS, sans avoir recours à d'autres opérations manuelles. Les deux points ci-dessus en sont les conditions nécessaires ; dans le cas contraire, la sécurité ne serait pas suffisante pour activer automatiquement cupsd.

12.5.4 Fichiers PPD se trouvant dans différents paquetages

Configuration de l'imprimante uniquement avec les fichiers PPD

Lors de la configuration de l'imprimante avec YaST, les files d'attente de CUPS ne sont créées qu'avec les fichiers PPD installés sur le système correspondant dans `/usr/share/cups/model/`. Pour un modèle d'imprimante particulier, YaST relève les fichiers PPD appropriés en comparant le nom du fabricant et celui du modèle relevé lors de la détection de matériel avec les noms des fabricants et ceux des modèles dans tous les fichiers PPD présents dans le système dans `/usr/share/cups/model/`. Pour ce faire, la configuration de l'imprimante

avec YaST génère une base de données à partir des informations concernant le fabricant et le modèle se trouvant dans les fichiers PPD. Cela vous permet de choisir votre imprimante par le biais du nom du fabricant et de celui du modèle et d'obtenir par conséquent les fichiers PPD correspondant aux noms du fabricant et du modèle.

L'avantage d'une configuration exécutée uniquement à l'aide de fichiers PPD et sans aucune autre source d'informations est que les fichiers PPD sont modifiables à volonté dans `/usr/share/cups/model/`. La configuration de l'imprimante avec YaST relève les modifications et regénère la base de données comprenant les noms des fabricants et des modèles. Si vous utilisez uniquement des imprimantes PostScript, vous n'avez normalement besoin ni des fichiers PPD Foomatic du paquetage cups-drivers ni les fichiers PPD GimpPrint du paquetage cups-drivers-stp ; mais vous pouvez copier les fichiers PPD adaptés exactement à vos imprimantes PostScript dans `/usr/share/cups/model/` (si ceux-ci ne sont pas déjà présents dans le paquetage manufacturer-PPDs) et configurer vos imprimantes de manière optimale.

Fichiers PPD CUPS du paquetage cups

Les fichiers PPD génériques du paquetage cups ont été spécialement complétés pour les imprimantes PostScript Niveau 2 et Niveau 1 avec les fichiers PPD Foomatic adaptés suivants :

- `/usr/share/cups/model/Postscript-level1.ppd.gz`
- `/usr/share/cups/model/Postscript-level2.ppd.gz`

Les fichiers PPD du paquetage cups-drivers

Pour les imprimantes non PostScript, on utilise normalement le filtre d'impression Foomatic "foomatic-rip" en même temps que Ghostscript. Les fichiers PPD Foomatic adaptés sont caractérisés par les enregistrements "*NickName: ... Foomatic/⟨*driver Ghostscript*⟩" et "*cupsFilter: ... foomatic-rip". Ces fichiers PPD se trouvent dans le paquetage cups-drivers.

YaST utilise de préférence un fichier PPD Foomatic si les conditions suivantes sont remplies :

- Un fichier PPD Foomatic "recommended" (recommandé) s'adapte au modèle d'imprimante caractérisé par l'enregistrement "*NickName: ... Foomatic ... (recommended)".
- Il n'existe aucun fichier PPD dans manufacturer-PPDs qui s'adapterait mieux (voir ci-dessous).

Les fichiers PPD de Gimp-Print du paquetage cups-drivers-stp

Pour beaucoup d'imprimantes non PostScript, il est possible d'utiliser comme alternative à "foomatic-rip" le filtre CUPS "rastertoprinter" de GimpPrint. Ce filtre et les fichiers PPD GimpPrint appropriés se trouvent dans le paquetage cups-drivers-stp. Les fichiers PPD GimpPrint se trouvent dans `/usr/share/cups/model/stp/` et sont caractérisés par les enregistrements "*NickName: ... CUPS+Gimp-Print" et "*cupsFilter: ... rastertoprinter".

Fichiers PPD de fabricants d'imprimantes dans le paquetage manufacturer-PPDs

Le paquetage manufacturer-PPDs contient des fichiers PPD de fabricants d'imprimantes couverts par une licence assez libre. Il convient de configurer les imprimantes PostScript avec le fichier PPD adapté du fabricant d'imprimantes, le fichier PPD du fabricant d'imprimante permettant d'utiliser toutes les fonctions de l'imprimante PostScript. YaST utilise de préférence un fichiers PPD de manufacturer-PPDs si les conditions suivantes sont remplies :

- Le nom du fabricant et du modèle correspond au nom du fabricant et du modèle dans un fichier PPD de manufacturer-PPDs.
- Soit le fichier PPD de manufacturer-PPDs est le seul fichier PPD s'adaptant au modèle d'imprimante, soit un fichier PPD Foomatic avec l'enregistrement suivant : "*NickName: ... Foomatic/Postscript (recommended)" s'adapte également au modèle d'imprimante.

Dans les cas suivants, YaST n'utilise donc aucun fichier PPD de manufacturer-PPDs :

- Quant au nom du fabricant et du modèle, le fichier PPD de manufacturer-PPDs ne s'adapte pas, ce qui est surtout le cas si, pour des modèles similaires, il n'existe qu'un seul fichier PPD de manufacturer-PPDs (si pour une série de modèles, il n'y a pas un fichier PPD par modèle, mais qu'on trouve comme nom de modèle dans le fichier PPD quelque chose dans le genre de "Funprinter 1000 series").
- La raison pour laquelle le fichier PPD Foomatic Postscript n'est pas "recommended" est la suivante : en mode PostScript, le modèle d'imprimante ne fonctionne pas correctement (lorsque l'imprimante fonctionne de manière peu fiable parce qu'elle n'a par défaut pas suffisamment de mémoire, ou lorsqu'elle est trop lente parce que son processeur n'est pas assez puissant) ou parce que PostScript ne prend par défaut pas en charge l'imprimante (lorsque la prise en charge de PostScript n'est disponible que comme module optionnel).

Si, pour une imprimante PostScript donnée, il existe un fichier PPD de manufacturer-PPDs correspondant à cette imprimante, mais que YaST n'est pas à même de le configurer pour les raisons mentionnées ci-dessus, il faut alors choisir à la main dans YaST le modèle d'imprimante adapté.

12.6 Problèmes éventuels et leurs solutions

Dans les chapitres suivants, on décrit les problèmes matériels et logiciels les plus fréquents en matière d'impression et on indique des solutions pour lever ou contourner ces problèmes.

12.6.1 Imprimante sans langage d'impression standard

Une imprimante qui ne peut être pilotée que par des séquences de contrôle qui lui sont propres s'appelle une *Imprimante GDI*. Ce type d'imprimantes fonctionne uniquement avec des versions du système d'exploitation pour lesquelles le fabricant livre un pilote. *GDI* est une interface de programmation pour la représentation graphique développée par Microsoft. Le problème ne réside pas dans l'interface de programmation mais dans le fait que les imprimantes GDI peuvent *uniquement* être pilotées au moyen du langage d'impression propriétaire de ce modèle d'imprimante.

Il existe des imprimantes qui, en plus du mode GDI, comprennent un langage d'impression standard, lorsque l'imprimante est configurée de manière adéquate ou lorsque l'on actionne un commutateur. Pour certaines imprimantes GDI, il existe des pilotes propriétaires offerts par le fabricant de l'imprimante. Les pilotes d'impression propriétaires ont le désavantage de ne pouvoir garantir ni leur fonctionnement avec le système d'impression actuellement installé ni leur fonctionnement pour les diverses plates-formes matérielles. En revanche, les imprimantes capables de comprendre un langage d'impression standard ne dépendent ni d'une version particulière du système d'impression, ni d'une plate-forme matérielle particulière.

Il est en général moins onéreux d'acheter une imprimante prise en charge que de gaspiller du temps à adapter un pilote pour Linux propriétaire, surtout parce qu'avec une imprimante appropriée, le problème lié au pilote est résolu pour de bon. Cela signifie que vous n'aurez plus à installer ni à éventuellement configurer un logiciel pilote spécial, ni à vous procurer des mises à jour du pilote dans le cas où le système d'impression aurait encore évolué.

12.6.2 Il manque un fichier PPD adapté à l'imprimante PostScript

Si le paquetage manufacturer-PPDs ne contient aucun fichier PPD adapté à une imprimante PostScript, il devrait être possible d'utiliser le fichier PPD à partir du CD de pilote du fabricant de l'imprimante ou de télécharger un fichier PPD adapté à partir du page internet du fabricant de l'imprimante.

Lorsque le fichier PPD se présente en tant qu'archive zip (.zip) ou bien en tant qu'archive zip auto-extractible (`.exe`), vous pouvez le décomprimer avec `unzip`. Informez-vous d'abord sur les conditions de licence du fichier PPD. Vérifiez ensuite au moyen du programme `cupstestppd` si le fichier PPD correspond à "Adobe PostScript Printer Description File Format Specification, Version 4.3". Si le résultat est "FAIL", les erreurs dans le fichiers PPD sont tellement graves que vous pouvez vous attendre à des problèmes plus conséquents. Il convient de réparer les points problématiques indiqués par `cupstestppd`. Si nécessaire, demandez un fichier PPD adapté directement auprès du fabricant de l'imprimante.

12.6.3 Ports parallèles

La méthode la plus sûre consiste à connecter l'imprimante directement sur la première interface parallèle et de procéder dans le BIOS aux réglages suivantes de l'interface parallèle :

- Adresse IO `378` (hexadécimal)
- L'interruption n'est pas importante
- Mode `Normal`, `SPP` ou `Output-Only`
- DMA n'est pas utilisé

Si, malgré ces réglages du BIOS, on ne peut pas communiquer avec l'imprimante depuis la première interface parallèle, il faut saisir l'adresse d'entrée-sortie dans `/etc/modprobe.conf` en relation avec la configuration du BIOS

de façon explicite sous la forme `0x378`. S'il existe deux interfaces parallèles, réglées sur les adresses IO `378` et `278` (hexadécimal), il faut les saisir sous la forme `0x378,0x278`.

Lorsque l'interruption `7` est encore libre, le mode interruption peut être activé par l'enregistrement dans le fichier 12.1. Avant d'activer le mode interruption, vérifiez dans le fichier `/proc/interrupts` quelles interruptions sont déjà utilisées, sachant que seules sont affichées les interruptions actuellement utilisées, ce qui peut varier en fonction du matériel utilisé activement. L'interruption pour l'interface parallèle ne doit pas être utilisée ailleurs. En cas de doute, optez pour le mode polling en saisissant `irq=none`.

Exemple 12.1: */etc/modprobe.conf : mode interruption pour la première interface parallèle*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

12.6.4 Connexion de l'imprimante en réseau

Mettre en évidence des problèmes de réseau
Connectez l'imprimante directement sur l'ordinateur. Configurez l'imprimante en tant qu'imprimante locale pour effectuer un test. Si l'imprimante fonctionne, des problèmes de réseau sont à l'origine de l'erreur.

Tester le réseau TCP/IP Le réseau TCP/IP doit fonctionner correctement, y compris la résolution du nom.

Tester un démon lpd distant Grâce à la commande suivante, il est possible de vérifier si une liaison TCP au démon lpd (port `515`) est généralement possible sur l'ordinateur ⟨*hôte*⟩ :

```
netcat -z <hôte> 515 && echo ok || echo failed
```

S'il n'est pas possible de se connecter au démon lpd, cela signifie soit que le démon lpd ne fonctionne pas, soit qu'il existe des problèmes de réseau fondamentaux, étant alors à l'origine de l'erreur.

Il est possible de demander en tant qu'utilisateur un rapport d'état (éventuellement assez long) sur la file d'attente ⟨*file*⟩ de l'ordinateur (distant) ⟨*hôte*⟩ avec la commande suivante, à condition que le démon lpd qui s'y trouve fonctionne et qu'il soit possible de lui envoyer des requêtes :

```
echo -e "\004<file>" \
  | netcat -w 2 -p 722 <hôte> 515
```

Si le démon lpd ne répond pas, cela signifie soit que lpd ne fonctionne pas, soit qu'il existe des problèmes de réseau sous-jacents qui sont à l'origine de l'erreur. Si lpd répond, il faudra clarifier la raison pour laquelle il n'est possible d'imprimer sur la file d'attente `file` de l'ordinateur `hôte` – Exemples :

Exemple 12.2: *Message d'erreur de lpd*

```
lpd: your host does not have line printer access
lpd: queue does not exist
printer: spooling disabled
printer: printing disabled
```

Lorsqu'une telle réponse est générée par lpd, c'est le démon lpd distant qui pose problème.

Tester un démon cupsd distant Grâce à la commande suivante, il est possible de tester s'il existe dans le réseau un serveur réseau CUPS puisqu'il devrait, en théorie, diffuser sa file d'attente sur le port UDP `631` par défaut toutes les 30 secondes :

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Après 40 secondes, il devrait apparaître un message du type suivant si un serveur réseau CUPS effectue une diffusion :

Exemple 12.3: *Transmission à partir du serveur réseau CUPS*

```
ipp://<hôte>.<domaine>:631/printers/<fichier>
```

On peut, à l'aide de la commande suivante, vérifier si une liaison TCP au cupsd (port 631) sur l'ordinateur ⟨*hôte*⟩ est généralement possible :

```
netcat -z <hôte> 631 && echo ok || echo failed
```

S'il n'est pas possible de se connecter au démon cupsd, cela signifie soit que le démon cupsd ne fonctionne pas, soit qu'il existe des problèmes de réseau fondamentaux, étant alors à l'origine de l'erreur.

```
lpstat -h <hôte> -l -t
```

Ce faisant, on obtient un rapport d'état (éventuellement assez long) de toutes les files d'attente de l'ordinateur ⟨*hôte*⟩, à condition que le démon cupsd s'y trouvant fonctionne et qu'il soit possible de lui envoyer des requêtes.

```
echo -en "\r" \
  | lp -d <fichier> -h <hôte>
```

Pour tester si la file d'attente ⟨*file*⟩ sur l'ordinateur ⟨*hôte*⟩ accepte un travail d'impression, la requête d'impression se composant d'un seul caractère carriage return — c'est-à-dire qu'il ne s'agit que d'un testet non d'une impression — et, le cas échéant, d'une page vide uniquement.

L'imprimante réseau ou le boîtier serveur d'impression ne fonctionne pas de manière fiable

Le gestionnaire de file d'attente qui fonctionne dans un boîtier serveur d'impression pose parfois problème dès que la quantité des requêtes d'impression est élevée. Étant donné que le gestionnaire de file d'attente du boîtier serveur d'impression est à l'origine des problèmes, on ne peut rien y faire. Il est cependant possible de contourner le gestionnaire de file d'attente du boîtier serveur d'impression en pilotant directement au moyen de sockets TCP l'imprimante connectée au boîtier serveur d'impression, voir la section *Imprimante réseau* page 295.

Par conséquent, le boîtier serveur d'impression ne fait plus qu'office de convertisseur entre les différentes formes de transmission de données (réseau TCP/IP et connexion d'imprimante locale), ce qui signifie que le port TCP correspondant sur le boîtier serveur d'impression doit être connu. Lorsque l'imprimante est connectée et allumée sur le boîtier serveur d'impression, il est normalement possible de relever ce port TCP un laps de temps après avoir allumé le boîtier serveur d'impression au moyen du programme `nmap` du paquetage `nmap`.

Ainsi, la commande `nmap` ⟨*`adresse IP`*⟩ fournit, pour un boîtier serveur d'impression, :

```
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
515/tcp    open        printer
631/tcp    open        cups
9100/tcp   open        jetdirect
```

Cet affichage signifie que l'imprimante connectée au moyen du port `9100` au boîtier serveur d'impression peut être commandée par socket TCP. `nmap` n'examine qu'une certaine liste de ports bien connus, listés dans `/usr/share/nmap/nmap-services`. Afin d'examiner tous les ports possibles, utilisez la commande : `nmap -p` ⟨*from_port*⟩-⟨*to_port*⟩ ⟨*adresse IP*⟩ (cette manoeuvre peut prendre un peu de temps) — consultez également la page du manuel `man nmap`.

Avec les commandes du type

```
echo -en "\rHello\r\f" | netcat -w 1 <adresse IP> <port>
cat <fichier> | netcat -w 1 <adresse IP> <port>
```

il est possible d'envoyer directement des chaînes de caractères ou des données au port correspondant pour tester si l'imprimante peut être commandée au moyen de ce port.

12.6.5 Impressions défectueuses sans message d'erreur

Le système d'impression considère le travail d'impression comme entièrement achevé lorsque le backend CUPS a terminé la transmission des données vers le récepteur (l'imprimante). Si par la suite le récepteur ne réussit pas à effectuer le traitement suivant (si l'imprimante n'arrive pas à sortir sur papier les données qui lui sont destinées), le système d'impression ne s'en rend pas compte. Si l'imprimante n'arrive pas à sortir sur papier les données qui lui sont destinées, il convient de choisir un autre fichier PPD alors mieux adapté à l'imprimante.

12.6.6 Files d'attente désactivées

Lorsque la transmission des données au récepteur a finalement échoué après plusieurs essais, le backend de CUPS (`usb` ou `socket`) signale une erreur au système d'impression, au démon cupsd. Le backend décide s'il convient d'entreprendre d'autres essais ainsi que le nombre d'essais avant de signaler qu'il est impossible de transmettre les données. Comme d'autres essais ne sont pas utiles, cupsd désactive (`disable`) alors l'impression sur la file d'attente concernée. Après avoir éliminé l'origine du problème, l'administrateur système doit réactiver l'impression à l'aide de la commande `/usr/bin/enable`.

12.6.7 Effacer des travaux d'impression diffusées par CUPS

Lorsqu'un serveur réseau CUPS communique ses files d'attente aux ordinateurs clients par diffusion et que le démon cupsd local correspondant est exploité sur les ordinateurs clients, c'est le démon cupsd du client qui accepte les travaux d'impression des programmes d'utilisation pour les remettre immédiatement au démon cupsd du serveur. Lorsqu'un démon cupsd accepte une requête d'impression, il lui est conféré un nouveau numéro d'impression. C'est la raison pour laquelle le numéro d'impression sur l'ordinateur client est différent du numéro sur le serveur. Si un travail d'impression est immédiatement remis, il ne peut pas être annulé sous le numéro de l'ordinateur client parce que le démon cupsd du client considère la requête d'impression comme totalement achevée dès qu'il l'a transmise de façon correcte (voir ci-dessus). Pour annuler une requête d'impression sur le serveur, il faut saisir la requête suivante pour relever le numéro d'impression sur le serveur à condition que le serveur n'ait pas terminé la requête d'impression (c'est-à-dire envoyé à l'imprimante) :

```
lpstat -h <serveur impression> -o
```

Ensuite, il est possible d'annuler le travail d'impression sur le serveur :

```
cancel -h <serveur impression> <fichier>-<numéro travail>
```

12.6.8 Travaux d'impression erronés ou transfert de données perturbé

Si vous éteignez et réallumez l'imprimante ou l'ordinateur pendant que la procédure d'impression est en cours, les travaux restent dans les files d'attente et seront éventuellement réimprimées à partir du début. Vous devez effacer un travail d'impression eronné de la file d'attente à l'aide de la commande `cancel`.

Si un travail d'impression est erronée ou si la communication entre l'ordinateur et l'imprimante est perturbée, l'imprimante n'est plus à même de traiter les données de manière intelligente, entraînant l'impression d'une quantité de feuilles couvertes de caractères confus.

1. Sortez d'abord tout le papier dans le cas d'imprimantes à jet d'encre ou bien ouvrez les cassettes de papier dans le cas d'imprimantes laser pour arrêter l'impression. Les imprimantes haut de gamme sont souvent dotées d'un bouton sevant à stopper l'impression en cours.

2. Étant donné que le travail d'impression n'est retiré de la file d'attente qu'après été envoyée à l'imprimante, elle devrait normalement rester dans la file d'attente. Entrez `lpstat -o` (ou `lpstat -h` ⟨*`serveur d'impression`*⟩ `-o`) pour savoir à partir de quelle file d'attente l'impression est effectuée et annulez le travail d'impression en saisissant `cancel` ⟨*`file d'attente`*⟩`-`⟨*`numéro d'impression`*⟩ (ou `cancel -h` ⟨*`serveur d'impression`*⟩ ⟨*`file d'attente`*⟩`-`⟨*`numéro d'impression`*⟩). Avec KDE, vous disposez également des programmes kprinter ou kjobviewer.
3. Il est possible que, bien que le travail d'impression ait été retiré de la file d'attente, quelques données sont encore transmises à l'imprimante. Contrôlez si, pour la file d'attente concernée, un processus backend CUPS est encore en cours et mettez-y fin si nécessaire. Dans le cas d'une imprimante connectée au port parallèle, on peut tuer tous les processus qui accèdent encore à l'imprimante (plus exactement, au port parallèle) au moyen de la commande `fuser -k /dev/lp0`.
4. Désactivez complètement l'imprimante en la déconnectant du réseau pendant un certain laps de temps. Puis réalimentez-la en papier et rebranchez-la.

12.6.9 Analyse des problèmes dans le système d'impression CUPS

Pour analyser les problèmes d'impression avec CUPS, nous recommandons la méthode suivante :

1. Déclarez `LogLevel debug` dans `/etc/cups/cupsd.conf`.
2. Arrêtez le démon cupsd.
3. Déplacez `/var/log/cups/error_log*` afin de ne pas avoir à faire des cherches dans des fichiers journaux trop volumineux.
4. Démarrez le démon cupsd.
5. Répétez l'opération qui a provoqué le problème.
6. Vous trouverez ensuite de nombreux messages dans `/var/log/cups/error_log*` qui vous aideront à trouver l'origine du problème.

Travail nomade sous Linux

Ce chapitre donne un aperçu des divers aspects du travail nomade sous Linux. Les différents champs d'application sont brièvement présentés, accompagnés de la description des solutions matérielles et logicielles pouvant y être apportées. Le chapitre se termine par une vue d'ensemble des plus importantes sources d'informations relatives à ce sujet.

La plupart d'entre nous associe le travail nomade avec les ordinateurs portables, PDA et téléphones portables et leurs possibilités de communiquer entre eux. Ce chapitre élargit le concept aux composants matériels mobiles comme les disques durs externes, cartes mémoire ou appareils photo numériques pouvant communiquer avec des ordinateurs portables ou des ordinateurs de bureau.

Le concept de travail nomade entraîne les questions suivantes :

Ordinateurs portables

- Qu'est-ce qui distingue le matériel utilisé ? Où se trouvent les particularités et les problèmes résultant du matériel utilisé ?
- Comment tire-t-on le rendement maximum des ordinateurs portables ? Comment peut-on réduire la consommation d'énergie ?
- Quel logiciel convient bien à une utilisation nomade ? Quels programmes peuvent aider à garder les données synchronisées ? Comment intègre-t-on au mieux des ordinateurs portables dans différents environnements ? Comment communique-t-on avec d'autres périphériques ? Comment sécurise-t-on des données et l'ensemble de la communication contre un accès non autorisé ?
- Comment et à quel endroit trouve-t-on des informations et une assistance en cas de problèmes ?

Matériel "nomade" : disques durs, cartes mémoire, appareils photo

- Quels types de périphériques sont supportés ?
- Quelles interfaces/Quels protocoles sont supportés ?
- Comment sécurise-t-on des données ?
- Comment et à quel endroit trouve-t-on des informations et une assistance en cas de problèmes ?

Communication "nomade" : téléphones portables et PDA

- Quels types de périphériques sont supportés ?
- Quelles interfaces/Quels protocoles sont supportés et de quelles applications dispose-t-on ?
- Comment et à quel endroit trouve-t-on des informations et une assistance en cas de problèmes ?

13.1 Travail nomade avec des ordinateurs portables

13.1.1 Particularités du matériel de l'ordinateur portable

L'équipement matériel d'ordinateurs portables se distingue de celui d'un ordinateur de bureau normal dans la mesure où, pour une utilisation nomade, les critères comme l'interchangeabilité, le besoin de place et d'énergie sont prépondérants. Les fabricants de matériel mobile ont développé le standard PCMCIA (*Personal Computer Memory Card International Association*). Les cartes mémoire, cartes réseau, cartes ISDN, cartes modem et les disques durs externes répondent à ce standard.

Vous apprendrez au chapitre *PCMCIA* page 329 en détail comment est réalisée l'assistance d'un tel matériel sous Linux et ce à quoi vous devez faire attention lors de la configuration, quels programmes sont à votre disposition pour le contrôle de PCMCIA et comment, en cas de message d'erreur, vous résolvez les éventuels problèmes.

13.1.2 Economies d'énergie en utilisation nomade

Le choix de composants de systèmes à consommation d'énergie réduite lors de la fabrication d'un ordinateur portable est un facteur contribuant à ce que les ordinateurs portables soient utilisables de façon appropriée même séparés du réseau d'alimentation. La contribution de votre système d'exploitation à l'économie d'énergie est tout aussi importante. SUSE LINUX supporte différentes méthodes influençant la consommation d'énergie de votre ordinateur portable, ayant ainsi des répercussions plus ou moins importantes sur l'autonomie de la batterie (classées de la plus grande à la plus petite économie d'énergie) :

- Diminution de la fréquence du processeur
- Arrêt de l'éclairage de l'écran dans les phases d'inactivité
- Diminution manuelle de l'éclairige de l'écran
- Déconnexion des périphériques hotplug non utilisés (USB-CDROM, souris externe, cartes PCMCIA non utilisées, etc.)
- Arrêt du disque dur en cas de non-utilisation

Vous trouverez au chapitre *Gestion de l'énergie* page 347 des informations de fond détaillées concernant la gestion de l'énergie sous SUSE LINUX ainsi que l'utilisation du module de gestion de l'énergie YaST.

13.1.3 Intégration dans des environnements d'exploitation variables

En utilisation nomade, votre système doit s'intégrer à des environnements d'exploitation changeant sans cesse. Beaucoup de fonctionnalités dépendent de l'environnement, et la configuration des services qui en forment la base doit être modifiée. SUSE LINUX accomplit cette tâche pour vous.

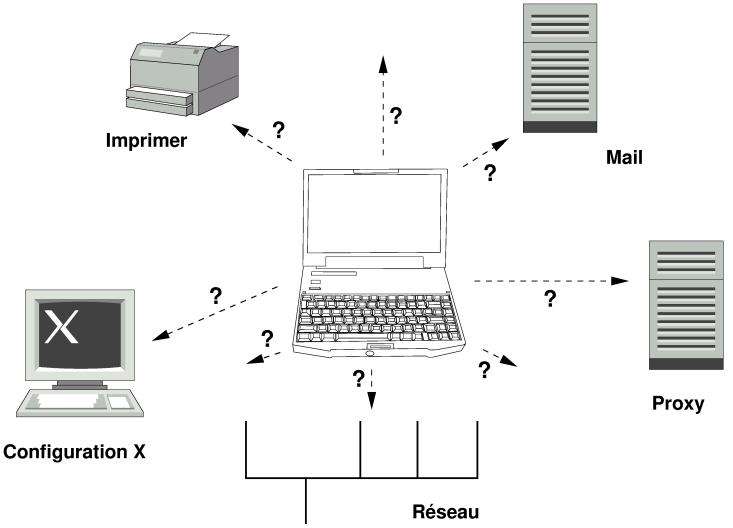


FIG. *13.1:* *Intégration d'un ordinateur portable dans le réseau*

Les services et fonctionnalités concernés sont, dans le cas d'un ordinateur portable faisant la navette entre un petit réseau domestique et un réseau d'entreprise :

Configuration du réseau L'attribution d'une adresse IP, résolution du nom et rattachement à internet ou à d'autres réseaux en font partie.

Impression Il doit exister une base de données actuelle des imprimantes disponibles et également, selon le réseau, un serveur d'impression disponible.

E-mail et proxies Comme pour l'impression, la liste des serveurs concernés doit être actuelle.

Configuration X Si vous reliez temporairement votre ordinateur portable avec un vidéoprojecteur ou un écran externe, la configuration modifiée de l'écran doit également être conservée.

Vous avez avec SUSE LINUX deux possibilités (combinables) d'intégrer votre ordinateur portable aux environnements d'exploitation existants :

SCPM SCPM (*System Configuration Profile Management*) vous permet de geler n'importe quel état de configuration de votre système dans une sorte de "photo instantanée" (appelée *Profil*). On peut créer des profils pour les situations les plus diverses. Ils s'y prêtent si le système est exploité dans des environnements variables (réseau domestique/réseau d'entreprise)ou si vous travaillez dans une configuration mais que vous en utilisez une autre pour l'expérimenter. Il est possible de commuter à tout moment entre les différents profils. Vous trouverez des informations de fond sur SCPM dans le chapitre *SCPM — System Configuration Profile Management* page 339. Vous pouvez sous KDE commuter via l'applet Kicker Profile Chooser entre les profils. Cependant, le programme vous demande avant la commutation le mot de passe root.

SLP Le *Service Location Protocol* (en abrégé : SLP) simplifie la configuration de clients en réseau à l'intérieur d'un réseau local. Pour configurer votre ordinateur portable dans un environnement réseau, vous auriez besoin, en tant qu'administrateur, de connaissancs détaillées sur les serveurs disponibles sur le réseau. Avec SLP, tous les clients sont informés de la disponibilité d'un type de service précis dans le réseau local. Vous pouvez utiliser les applications supportées par SLP par l'intermédiaire des informations distribuées par SLP ; elles sont ainsi automatiquement configurables. SLP peut même être employé pour l'installation d'un système sans que vous ayez à vous donner la peine de chercher une source d'installation adéquate. Vous trouverez des informations détaillées sur SLP à la section *SLP — Transmission de services dans le réseau* page 484.

L'atout de SCPM se situe dans le fait qu'il permet et qu'il reçoit des conditions de système reproductibles tandis que SLP facilite largement la configuration automatique d'un ordinateur en réseau.

13.1.4 Logiciels pour une utilisation nomade

Dans une utilisation nomade, plusieurs problèmes sont traités par des logiciels spéciaux : surveillance du système (en particulier état de charge de la batterie), synchronisation des données et communication sans fil avec des périphériques et internet. Les sections suivantes présentent pour chaque point les applications les plus importantes comprises dans SUSE LINUX.

Surveillance du système

Cette section vous présente deux outils KDE destinés à la surveillance du système, compris dans SUSE LINUX. L'affichage d'état en lui-même de la batterie de l'ordinateur portable est repris par l'applet KPowersave dans Kicker ; vous pouvez effectuer une surveillance complexe du système avec KSysguard. Sous GNOME, les fonctions décrites vous sont proposées par GNOME ACPI (en tant que panneau d'applet) et System Monitor.

KPowersave KPowersave est un applet qui vous donne essentiellement à partir d'un petit icône dans la barre de contrôle des informations sur l'état de charge de la batterie. L'icône s'adapte au type d'alimentation en courant. En mode réseau, vous voyez un petit icône en forme de prise ; en mode batterie, il est remplacé par un icône en forme de pile. Vous démarrez à partir du menu approprié, après avoir entré le mot de passe root, le module YaST de gestion d'énergie, dans lequel vous pouvez configurer le fonctionnement de l'ordinateur en fonction de l'alimentation en courant. Vous trouverez des informations sur la gestion de l'énegie et le module YaST correspondant dans le chapitre *Gestion de l'énergie* page 347.

KSysguard KSysguard est une application autonome, qui regroupe tous les paramètres du système pouvant être surveillés dans un environnement de surveillance. KSysguard possède des écrans de contrôle pour ACPI (état de la batterie), le degré d'utilisation du processeur, le réseau, l'état d'occupation des partitions, la charge du processeur et l'utilisation de la mémoire. Il peut en plus collecter et représenter l'ensemble des processus du système. Vous définissez vous-même le type de représentation ou de filtrage des données détectées. Vous pouvez surveiller dans plusieurs fenêtres divers paramètres du système ou alors collecter en parallèle les données de plusieurs ordinateurs par l'intermédiaire du réseau. KSysguard peut également fonctionner comme démon sur les ordinateurs ne possédant pas d'environnement KDE. Vous trouverez plus d'informations sur ce programme grâce à la fonction d'aide intégrée du programme ou via l'assistance SUSE.

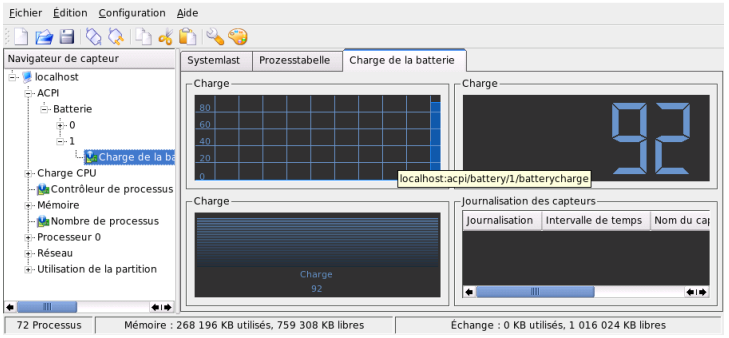


FIG. *13.2:* *Surveillance de l'état de charge de la batterie avec KSysguard*

Synchronisation des données

Si vous commutez sans cesse entre un travail nomade sur ordinateur portable non relié au réseau et une station de travail en réseau sur votre lieu de travail, vous vous trouvez confronté au problème de garder les données traitées synchronisées entre les deux instances. On parle ici de dossiers E-mails ou de dossiers ou de fichiers entiers, dont vous devez traiter le contenu autant sur votre lieu de travail qu'en voyage. Voici comment se présentent les solutions pour ces deux cas:

Synchronisation des E-mails Utilisez dans le réseau d'entreprise un compte IMAP pour enregistrer vos E-mails. Vous lisez sur votre station de travail vos messages avec le logiciel de messagerie de votre choix déconnecté et supportant IMAP (Mozilla Thunderbird Mail, Evolution ou KMail, voir *Guide de l'utilisateur*). Configurez, sur tous vos systèmes à partir desquels vous lisez vos messages, le logiciel de messagerie de telle sorte que ce soit toujours le même dossier qui soit utilisé pour `Messages envoyés`. Tous les messages, y compris les affichages d'état, sont disponibles après le processus de synchronisation. Utilisez dans tous les cas le service SMTP contenu dans le logiciel de messagerie pour envoyer des messages au lieu de MTA au niveau du système (postfix ou sendmail) afin de recevoir une information en retour fiable concernant les messages qui n'ont pas encore été envoyés.

Synchronisation de documents/fichiers individuels

Si vous voulez disposer également sur votre lieu de travail de documents que vous avez créés en dehors du bureau, utilisez unison. Vous synchronisez via le réseau à l'aide de ce programme des fichiers et des répertoires entiers. Si vous désirez synchroniser votre répertoire Poste de travail, limitez le processus si possible à des dossiers individuels et évitez la synchronisation de fichiers et de répertoires commençant par un point (par ex. `.kde/`). Ces fichiers peuvent contenir des configurations spécifiques à la machine, qui pourraient occasionner une confusion sur l'autre ordinateur. Vous trouverez plus d'informations sur unison au chapitre *Introduction à unison* page 599 et sur le site internet du projet sous `http://www.cis.upenn.edu/~bcpierce/unison/`.

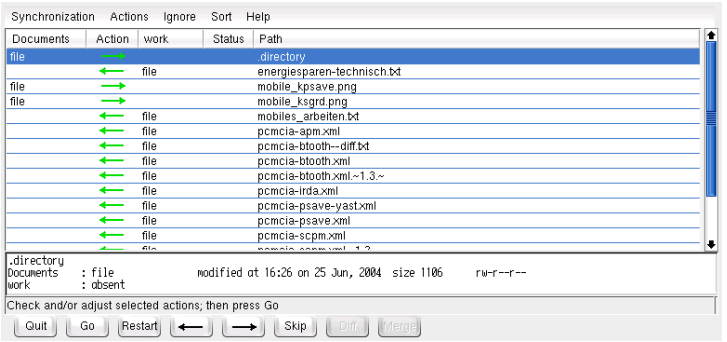


FIG. *13.3:* *Synchronisation de données avec Unison*

Communication sans fil

Exception faite de la communication fixe par câble dans le réseau domestique ou en entreprise, votre ordinateur portable peut également communiquer sans câble fixe avec d'autres ordinateurs, périphériques, téléphones portables ou PDA. Linux supporte trois types de communication sans fil :

WLAN WLAN, possédant la plus grande portée de ce qu'on appelle les radiotechnologies, est le seul à pouvoir être utilisé pour le montage de grands réseaux, même physiquement séparés. On peut à l'aide de WLAN des ordinateurs individuels en un réseau autonome sans fil ou les relier à internet. Ce qu'on appelle les points d'accès forment pour les ordinateurs supportant

WLAN une sorte de station de base permettant l'accès à internet. L'utilisateur nomade peut commuter avec son ordinateur compatible WLAN entre différents points d'accès, selon l'endroit où il se trouve et le point d'accès offrant la meilleure connexion. Comme pour la téléphonie portable, un utilisateur WLAN dispose d'un large réseau sans devoir, pour l'accès, être relié physiquement de quelle forme que ce soit. Vous trouverez des détails concernant WLAN dans le chapitre *Réseau local sans fil (WLAN)* page 376 nach.

Bluetooth Bluetooth dispose du plus large spectre d'utilisation de toutes les technologies sans fil. Il peut être utilisé exactement comme IrDA pour la communication entre ordinateur (notebook) et PDA ou téléphone portable ; il peut aussi bien être utilisé pour mettre en réseau plusieurs ordinateurs qui se trouvent à la vue l'un de l'autre. Bluetooth est en outre utilisé pour relier des composants du système sans fil comme les claviers ou les souris. La portée de cette technologie n'est cependant pas suffisante pour mettre en réseau des systèmes physiquement séparés. Pour une communication sans fil par-delà des obstacles comme les murs de maison, WLAN est l'idéal. Vous trouverez plus d'informations sur Bluetooth, ses possibilités d'utilisation et sa configuration dans le chapitre *Bluetooth* page 385.

IrDA IrDA est la technologie sans fil ayant la plus petite portée. Il ne doit se trouver aucun obstacle entre les deux partenaires de communication. Les obstacles comme les murs ne peuvent pas être surmontés. Un scénario possible d'utilisation pour IrDA est l'envoi d'un fichier de l'ordinateur portable par l'intermédiaire d'un téléphone portable. En outre, la courte distance entre l'ordinateur portable et le téléphone portable via IrDA est couverte ; le transport longue distance jusqu'au destinataire du fichier est réalisé par l'intermédiaire d'un réseau de téléphonie mobile performant. Une autre possibilité d'utilisation pour IrDA est l'envoi sans fil de requêtes d'impression au bureau. Vous trouverez plus d'informations sur IrDA au chapitre *Infrared Data Association* page 395.

13.1.5 Sécurité des données

Sécurisez au mieux vos données sur l'ordinateur portable à plusieurs égards contre l'accès non autorisé. Les mesures de sécurité peuvent être classifiées selon les aspects suivants :

Sécurité antivol Sécurisez toujours physiquement votre système, si possible, contre le vol. Différents systèmes de sécurité sont disponibles dans le commerce (comme par exemple des câbles antivol).

Sécurisation des données dans le système
Cryptez les données importantes pas seulement lors d'un transfert via un réseau mais également sur le disque dur de votre système. Ainsi, en cas de vol, vos données sont au moins à l'abri. Voyez dans la sectiont *Chiffrer les partitions et les fichiers* page 672 comment créer sous SUSE LINUX une partition cryptée.

Sécurité du réseau Peu importe la façon dont vous communiquez avec votre entourage, le transfert de données en direction et en provenance de vos partenaires devrait toujours être sécurisé. Vous obtiendrez des détails concernant les aspects généraux de sécurité sous Linux et en réseau au chapitre *La sécurité est une affaire de confiance* page 675. Vous trouverez plus d'informations sur les aspects de la sécurité dans le fonctionnement en réseau sans fil au chapitre portant sur la communication sans fil, voir chapitre *Communications sans fil* page 375.

13.2 Matériel nomade

SUSE LINUX supporte la reconnaissance automatique de périphériques de mémoire mobiles via Firewire (IEEE 1394) ou USB. On entend par "périphériques de mémoire mobiles" tous les types de disques durs Firewire/USB, cartes mémoire USB ou appareils photo numériques. Dès que ces périphériques sont reliés au système par l'interface adéquate, ils sont automatiquement reconnus par Hotplug et configurés. subfs/submount veille à ce que les périphériques soient rattachés aux endroits appropriés dans le système de fichiers. En tant qu'utilisateur, vous vous épargnez entièrement le montage et le démontage manuel que vous connaissiez dans les précédentes versions de SUSE LINUX. Dès que le périphérique n'est plus utilisé par aucun programme, vous pouvez simplement le débrancher.

Disques durs externes (USB et Firewire)
Dès qu'un disque dur externe a été correctement reconnu par le système, vous pouvez voir ses icônes sous 'Mon ordinateur' (KDE) ou 'Ordinateur' (GNOME) dans la vue d'ensemble des lecteurs montés. Si vous cliquez avec la touche gauche de la souris sur l'icône, le contenu du lecteur apparaît. Vous pouvez à cet endroit créer des fichiers ou des dossiers, les éditer ou les effacer. Si vous désirer appeler le disque dur d'une autre manière que le nom donné par le système, cliquez avec la touche droite de la souris sur l'icône pour arriver dans le menu contextuel s'y rapportant et renommez-le.

Cette modification du nom se limite cependant à l'affichage dans le gestionnaire de fichiers — la désignation sous laquelle le périphérique est monté sous `/media/usb-xxx` ou `/media/ieee1394-xxx` reste inchangée.

Cartes mémoire USB Les cartes mémoire USB sont considérées par le système exactement comme des disques durs externes. Il est également possible de renommer leurs fichiers dans le gestionnaire de fichiers.

Appareils photo numériques (USB et Firewire)
Les appareils photo numériques reconnus par le système apparaissent également en tant que lecteurs externes dans la vue d'ensemble du gestionnaire de fichiers. Vous pouvez sous KDE lire et regarder les images enregistrées par l'intermédiaire de l'URL `camera:/`. Utilisez digikam ou gimp pour éditer les images. Sous GNOME, les images sont affichées dans Nautilus dans leur dossier de fichiers respectif. GThumb se prête bien à une gestion et une édition aisée des images. On effectue l'édition d'image avancée avec Gimp. Excepté GThumb, vous retrouverez la description de tous les programmes mentionnés dans le *Guide de l'utilisateur*.

Si vous avez l'intention d'acheter un appareil photo numérique et vous voulez savoir si et comment celui-ci est supporté par Linux, les listes d'appareils photo suivantes peuvent vous être utiles dans le choix du modèle : `http://gphoto.org/proj/libgphoto2/support.php` et `http://www.teaser.fr/~hfiguiere/linux/digicam.html`). La seconde liste est la plus acutelle et la plus complète. Vous trouverez des informations générales au sujet de la photographie numérique sous Linux sous `http://dplinux.org/`.

Remarque

Sécuriser des supports de données mobiles

Tout comme les ordinateurs portables, les disques durs mobiles ou les cartes mémoire ne sont pas à l'abri des vols. Afin d'empêcher qu'un tiers fasse mauvais usage des données contenues, il est conseillé de créer une partition cryptée, comme décrit dans la section *Chiffrer les partitions et les fichiers* page 672.

Remarque

13.3 Communication mobile : téléphones portables et PDA

La communication d'un ordinateur de bureau ou d'un ordinateur portable avec un téléphone portable peut avoir lieu via Bluetooth ou alors IrDA. Quelques modèles supportent les deux protocoles, certains n'en supportent qu'un seul. Les domaines d'utilisation des deux protocoles et la documentation supplémentaire s'y rapportant ont déjà été mentionnés à la section *Communication sans fil* page 322. Vous trouverez dans la documentation du périphérique une description concernant la façon de configurer vous-même les protocoles sur le téléphone portable. Vous trouverez la description de la configuraiton du site Linux aux sections *Bluetooth* page 385 et *Infrared Data Association* page 395.

Le support pour la synchronisation avec des PDA est déjà intégré dans Evolution et Kontact. La configuration de base de la connexion au PDA est dans les deux cas facile à exécuter avec l'aide d'un assistant. Si le support pilote est configuré, définissez quels types de données vous voulez synchroniser (données d'adresses, RDV ou autres). Les deux collecticiels sont décrits dans le *Guide de l'utilisateur*.

Le programme KPilot intégré dans Kontact est également disponible en tant que programme individuel ; vous trouverez une description dans le *Guide de l'utilisateur*. Il existe à côté de cela le programme KitchenSync pour la synchronisation de données d'adresses.

Pour d'autres informations sur Evolution, Kontact et KPilot, veuillez consulter les sites suivants :

- Evolution: `http://www.ximian.com/support/manuals/evolution_14/book1.html`
- Kontact: `http://docs.kde.org/en/3.2/kdepim/kontact/`
- KPilot: `http://docs.kde.org/en/3.2/kdepim/kpilot/`

13.4 Informations supplémentaires

La référence centrale pour toutes les questions concernant les périphériques mobiles sous Linux est `http://tuxmobil.org/`. Plusieurs sections de ce site internet traitent des aspects de matériel et de logiciel concernant les ordinateurs portables, PDA, téléphones portables et autres matériels mobiles :

- Ordinateurs portables : `http://tuxmobil.org/mylaptops.html`

- PDA : `http://tuxmobil.org/pda_linux.html`
- Téléphones portables : `http://tuxmobil.org/phones_linux.html`
- HOWTOS ("Comment faire ?") autour du travail nomade : `http://tuxmobil.org/howtos.html`
- Liste de diffusion : `http://tuxmobil.org/mobilix_ml.html`

`http://www.linux-on-laptops.com/` poursuit la même prétention que `http://tuxmobil.org/`. Vous trouverez dans ces sites des informations sur les ordinateurs portables et les PDA :

- Ordinateurs portables : `http://www.linux-on-laptops.com/`
- PDA : `http://www.linux-on-laptops.com/palmtops.html`
- Configuration de périphériques mobiles : `http://www.linux-on-laptops.com/components.html`
- Forums de discussion/Listes de diffusion : `http://www.linux-on-laptops.com/discussion.html`

SUSE entretient sa propre liste de diffusion portant sur les ordinateurs portables (en allemand) : `http://lists.suse.com/archive/suse-laptop/`. Des utilisateurs et développeurs discutent sur cette liste de tous les aspects du travail nomade sous SUSE LINUX. On répond aux messages en anglais, mais la majeure partie des informations archivées est disponible exclusivement en allemand.

En cas de problèmes avec la gestion de l'énergie sur les ordinateurs portables sous SUSE LINUX, il est recommandé de jeter un oeil sur les fichiers `Lisez-moi` sous `/usr/share/doc/packages/powersave`. Dans ces fichiers sont souvent intégrés les retours d'expérience de testeurs et développeurs jusqu'à la dernière minute du processus de développement, si bien que vous pouvez souvent trouver à cet endroit de précieuses indications pour la résolution de vos problèmes.

PCMCIA

Ce chapitre traite des particularités des ordinateurs portables et plus particulièrement sur les apects matériels et logiciels de PCMCIA. PCMCIA (en anglais, *Personal Computer Memory Card International Association*) est un terme générique qui désigne tous les logiciels et tout le matériel informatique de ce type.

14.1 Matériel

Le composant essentiel est la carte PCMCIA dont on distingue deux types :

Cartes PC Ces carte existent depuis les premiers jours de PCMCIA. Elles utilisent un bus de 16 bits pour le transfert des données et sont relativement économiques. Certains ponts PCMCIA modernes ont du mal à reconnaître ces cartes. Cependant, une fois reconnues, elles sont, en règle générale, prises en charge sans problème et de manière stable.

Cartes CardBus Il s'agit d'un nouveau standard de cartes. Elles utilisent un bus de 32 bits, et sont donc plus rapides mais aussi plus chères. Elles sont connectés au système comme des cartes PCI et sont donc utilisables sans problème.

Pour savoir quelle carte vous utilisez, lorsque le service PCMCIA est actif, saisissez la commande `cardctl ident` . Vous trouverez une liste des cartes prises en charge dans le fichier `SUPPORTED.CARDS` dans le répertoire `/usr/share/doc/packages/pcmcia`. Vous y trouverez aussi la version actuelle du PCMCIA-HOWTO.

Le deuxième composant indispensable est le contrôleur PCMCIA ou également la carte PC / le pont CardBus.

Celui-ci assure la connexion entre la carte et le bus PCI. Tous les modèles courants sont pris en charge. Utilisez la commande `pcic_probe` pour déterminer le type du contrôleur. S'il s'agit d'un appareil PCI, la commande `lspci -vt` permet aussi d'obtenir des informations intéressantes.

14.2 Logiciel

14.2.1 Modules de base

Les modules du noyau nécessaires se trouvent dans les paquetages du noyau. Vous avez, en outre, besoin des paquetages `pcmcia` et `hotplug`. Lors du démarrage de PCMCIA, les modules `pcmcia_core`, `yenta_socket` et `ds` sont chargés. Dans quelques rares cas, le module `tcic` est nécessaire comme alternative à `yenta_socket`. Ils permettent d'initialiser les contrôleurs PCMCIA disponibles et proposent des fonctionnalités de base.

14.2.2 Gestionnaire de cartes

Comme les cartes PCMCIA peuvent être changées pendant le fonctionnement de l'ordinateur, les activités au niveau des emplacements doivent être surveillées. Cette tâche est effectuée par les *Services cartes* implémentés dans le modules de base. L'initialisation d'une carte insérée est faite soit par le *gestionnaire de cartes* (pour cartes PC), soit par le système de connexion à chaud (en anglais, *hotplug*) du noyau (CardBus). Le gestionnaire de cartes est démarré à l'aide du script de démarrage PCMCIA après le chargement des modules de base ; la connexion à chaud est automatiquement active.

Lors de l'insertion d'une carte, le gestionnaire de cartes ou la connexion à chaud établit son type et sa fonction et charge les modules adaptés. Si ces derniers sont correctement chargés, le gestionnaire de cartes ou la connexion à chaud, selon la fonction de la carte, démarrent des scripts d'initialisation particuliers qui établissent la connexion réseau de leur côté, montent des partitions de disques SCSI externes ou effectuent d'autres actions propres au matériel. Les scripts du gestionnaire de cartes se trouvent dans `/etc/pcmcia`. Les scripts de connexion à chaud se trouvent dans `/etc/hotplug`. Lorsque la carte est à nouveau retirée, le gestionnaire de cartes ou la connexion à chaud utilisent les mêmes scripts pour mettre un terme aux diverses activités relatives aux cartes. Enfin, les modules devenus inutiles sont à nouveau déchargés.

Pour des processus de ce type, il existe des événements "hotplug". Lorsque des disques durs ou des partitions sont ajoutés (événements "block"), les scripts hotplug veillent à ce que les nouveaux supports de données soient immédiatement disponibles dans `/media` à travers `subfs`. Pour monter des supports de données à travers les anciens scripts PCMCIA, Hotplug doit être déconnecté dans `subfs`.

Aussi bien le processus de démarrage de PCMCIA que les événements relatifs aux cartes sont enregistrés dans le journal du système (`/var/log/messages`). Les modules qui sont chargés et les scripts qui sont exécutés pour la configuration y sont précisés.

Théoriquement, une carte PCMCIA peut être retirée simplement. Cela fonctionne également particulièrement bien pour les cartes réseau, modem ou RNIS, en l'absence de connexion réseau encore active. Cela ne fonctionne en revanche pas pour ce qui concerne les partitions montées d'un disque dur externe ou les répertoires NFS. Vous devez, pour ce faire, veiller à ce que les unités soient synchronisées et démontées proprement. Cela n'est naturellement plus possible si la carte a déjà été retirée. En cas de doute, n'hésitez pas à utiliser la commande `cardctl eject` . Cette commande permet de désactiver toutes les cartes qui se trouvent toujours dans le portable. Pour ne désactiver qu'une seule des cartes, vous pouvez aussi indiquer son numéro d'emplacement, par exemple, `cardctl eject 0`.

14.3 Configuration

Pour choisir de démarrer PCMCIA lors de l'amorçage, utilisez l'éditeur de niveaux d'exécution de YaST. Démarrez ce module avec 'Système' → 'Éditeur de niveaux d'exécution'.

Trois variables se trouvent dans le fichier `/etc/sysconfig/pcmcia` :

`PCMCIA_PCIC` contient le nom du module piloté par le contrôleur PCMCIA. Normalement, le script de démarrage détermine ce nom tout seul. Ce n'est qu'en cas d'échec que le module doit être enregistré ici. Sinon cette variable doit rester vide.

`PCMCIA_CORE_OPTS` est prévu pour les paramètres du module `pcmcia_core` ; ils ne sont cependant que très rarement utilisés. Ces options sont décrites dans la page de manuel de la commande `pcmcia_core`. Étant donné que cette page de manuel fait référence au module de même nom du paquetage `pcmcia-cs` de David Hinds, elle contient plus de paramètres que n'en propose réellement le module du noyau, c'est à dire tous ceux qui commencent par `cb_` et `pc_debug`.

`PCMCIA_BEEP` allume et éteint les signaux acoustiques du gestionnaire de cartes.

L'association de pilotes aux cartes PCMCIA pour le gestionnaire de cartes se trouve dans les fichiers `/etc/pcmcia/config` et `/etc/pcmcia/*.conf`. Est d'abord lu `config`, puis `*.conf` dans l'ordre alphabétique. C'est le dernier élément trouvé pour une carte qui est décisif. Vous trouverez des détails sur la syntaxe de ces fichiers sur la page de manuel relative à la commande `pcmcia`.

L'attribution de pilotes aux cartes CardBus se fait dans les fichiers `/etc/sysconfig/hardware/hwcfg-<descriptiondupériphérique>`. Ces fichiers sont créés par YaST lors de la configuration d'une carte. Vous trouverez plus de détails sur les descriptions des périphériques sous `/usr/share/doc/packages/sysconfig/README` et dans la page de manuel de `getcfg`.

14.3.1 Cartes réseau

À l'instar des cartes réseau ordinaires, vous pouvez installer les cartes réseaux Ethernet, Wireless LAN et TokenRing avec YaST. Si votre carte n'est pas reconnue, vous ne devez que préciser comme type de carte, `PCMCIA`, lors de la configuration du matériel. Tous les autres détails relatifs à la mise en place du réseau sont décrits dans la section *L'intégration dans le réseau* page 468. Lisez bien

les conseils relatifs aux cartes pouvant être connectées à chaud (section *PCMCIA / USB* page 482).

14.3.2 RNIS

Vous pouvez aussi configurer les cartes PC RNIS comme des cartes RNIS ordinaires avec YaST. Peu importe laquelle des cartes RNIS PCMCIA proposées vous choisissez : la seule chose importante est qu'il s'agisse bien d'une carte PCMCIA. Lors de la configuration du matériel et de la sélection du fournisseur d'accès, il faut veiller à ce que le mode de fonctionnement soit toujours `hotplug`, et pas `onboot`. Il existe aussi des modems RNIS dans les cartes PCMCIA. Il s'agit de cartes modem ou multifonctions avec un kit de connexion RNIS supplémentaire. Elles sont traitées comme un modem.

14.3.3 Modem

Les cartes PC modem ne disposent normalement d'aucun réglage spécifique PCMCIA. Dès qu'une carte modem est insérée, elle est disponible dans `/dev/modem`. Il existe aussi pour les cartes PCMCIA ce que l'on appelle des modems logiciels. Ils ne sont généralement pas pris en charge. S'il existe des pilotes pour ces derniers, vous devrez les intégrer individuellement au système.

14.3.4 SCSI et IDE

Le module de pilotes adapté est chargé par le gestionnaire de cartes ou la connexion à chaud. Ainsi, dès l'insertion d'une carte SCSI ou IDE, les appareils qui y sont connectés sont disponibles. Les noms des appareils sont déterminés de manière dynamique. Vous trouverez des informations sur les appareils SCSI ou IDE dans `/proc/scsi` ou dans `/proc/ide`.

Les disques durs, les lecteurs de cédéroms et autres appareils externes de ce type doivent être éteints avant d'insérer la carte PCMCIA dans son emplacement. Les appareils SCSI doivent être arrêtés de manière active.

Attention

Retrait d'une carte SCSI ou IDE

Avant de retirer une carte SCSI ou IDE, il faut démonter toutes les partitions des appareils qui y sont connectés (avec la commande `umount`). Si vous oubliez de le faire, vous ne pourrez à nouveau accéder à ces appareils qu'après un redémarrage du système.

Attention

14.4 Autres programmes d'aide

Le programme cité ci-avant, cardctl, est l'outil pour obtenir des informations sur PCMCIA ou exécuter certaines actions. Vous trouverez des détails dans la page de manuel de `cardctl`. Après la saisie de `cardctl`, vous obtenez une liste des options disponibles. Il existe également un frontal graphique pour ce programme, cardinfo, avec lequel les choses les plus importantes sont contrôlables. Pour cela le paquetage `pcmcia-cardinfo` doit être installé.

`ifport`, `ifuser`, `probe` et `rcpcmcia` du paquetage `pcmcia` vous apporteron également de l'aide. Cependant, ils ne sont pas toujours nécessaires.

Pour savoir exactement quels fichiers sont contenus dans le paquetage `pcmcia`, utilisez la commande `rpm -ql pcmcia`.

14.5 Problèmes possibles et solutions

En cas de problèmes avec PCMCIA sur certains ordinateurs portables ou avec certaines cartes, vous réglerez la plupart de ces difficultés assez facilement, dans la mesure où vous traiterez toujours le problème de manière systématique. Tout d'abord, il faut déterminer si le problème vient de la carte ou s'il s'agit d'un problème au niveau du système de base PCMCIA. Vous devez donc, dans tous les cas, commencer par démarrer l'ordinateur sans que la carte ne soit insérée. Ce n'est que quand le système de base fonctionnera apparemment sans problème que vous pourrez réinsérer la carte. Tous les messages sont enregistrés dans le fichier journal `/var/log/messages`. Vous devez donc particulièrement surveiller ce fichier avec `tail -f /var/log/messages` pendant les tests. Ainsi l'erreur se limite à l'un des deux cas suivants.

14.5.1 Le système de base PCMCIA ne fonctionne pas

Lorsque le système reste bloqué lors de l'amorçage dès le message PCMCIA "PCMCIA: Starting services" (démarrage des services) ou que d'autres choses surprenantes se produisent, vous pouvez empêcher le démarrage de PCMCIA lors du prochain amorçage en saisissant `NOPCMCIA=yes` dans l'invite d'amorçage. Pour limiter encore plus le risque d'erreur, chargez ensuite les trois modules de base du système PCMCIA utilisé, l'un après l'autre, manuellement.

Pour charger un module PCMCIA manuellement, utilisez, les commandes `modprobe pcmcia_core`, `modprobe yenta_socket` et `modprobe ds` en tant qu'utilisateur `root`. Dans quelques rares cas, l'un des modules `tcic`, `i82365` ou `i82092` doit être utilisé à la place de `yenta_scoket`. Les modules critiques sont les deux premiers chargés.

Si l'erreur survient lors du chargement de `pcmcia_core`, reportez-vous à la page de manuel relative à `pcmcia_core`. Les options qu'elle décrit peuvent tout d'abord être testées avec la commande `modprobe`. Nous pouvons, à titre d'exemple, utiliser la vérification de domaines d'E/S IO libres. Cette vérification isolée peut poser un problème si d'autres composants matériels s'en trouvent perturbés. On peut éviter ce problème à l'aide de l'option `probe_io=0` :

```
modprobe  pcmcia_core probe_io=0
```

Si l'option sélectionnée donne satisfaction, attribuez la valeur `probe_io=0` à la variable `PCMCIA_CORE_OPTS` dans le fichier `/etc/sysconfig/pcmcia`. Si vous souhaitez utiliser plusieurs options, séparez-les par des espaces :

```
PCMCIA_CORE_OPTS="probe_io=0 setup_delay=10"
```

Une erreur lors du chargement du module `yenta_socket` signifie un problème fondamental, tel que, par exemple, la répartition des ressources par ACPI.

En outre, les fichiers `/etc/pcmcia/config` et `/etc/pcmcia/config.opts` sont exploités par le gestionnaire de cartes. Les réglages qu'ils contiennent sont utiles en partie lors du démarrage de cardmgr et en partie lors du chargement des modules pilote pour les cartes PC.

Vous pouvez aussi inclure ou non des IRQ, des ports d'E/S et des domaines mémoire dans le fichier `/etc/pcmcia/config.opts`. Dans quelques cas rares, l'accès à un mauvais domaine d'E/S peut planter tout le système. Dans ce cas, limiter en partie le domaine peut résoudre le problème.

14.5.2 La carte PCMCIA ne fonctionne pas (correctement)

Il existe à ce sujet essentiellement trois variantes d'erreur : la carte n'est pas reconnue, le pilote ne peut pas être chargé ou le port préparée par le pilote a été mal configuré. Vous devez vérifier si la carte est traitée par le gestionnaire de cartes ou par la connexion à chaud. Le gestionnaire de cartes gère les cartes PC Card et la connexion à chaud les cartes CardBUS.

Pas de réaction lorsqu'une carte est insérée
Lorsque le système ne réagit pas à l'insertion d'une carte et que même la saisie manuelle de `cardctl insert` ne provoque aucune réaction, l'attribution des interruptions aux périphériques PCI n'est peut-être pas correcte. Souvent, d'autres périphériques PCI que la carte réseau ont des problèmes. Dans ce cas, le paramètre d'amorçage `pci=noacpi` ou d'autres paramètres PCI ou ACPI peuvent être utile.

La carte n'est pas reconnue Si la carte n'est pas reconnue, le message "unsupported Card in Slot x" apparaît dans le fichier `/var/log/messages`. Ce message indique seulement que le gestionnaire de cartes ne peut associer aucun pilote à la carte. Les fichiers `/etc/pcmcia/config` ou `/etc/pcmcia/*.conf` sont nécessaires pour réaliser cette attribution. Ces fichiers sont, pour ainsi dire, la base de données des pilotes. Cette base de données des pilotes peut facilement être complétée en prenant ses éléments disponibles comme modèle. Vous pouvez utiliser la commande `cardctl ident` pour découvrir la manière dont la carte s'identifie. Vous trouverez plus d'informations à ce sujet dans le PCMCIA-HOWTO (section 6) et dans la page de manuel relative à `pcmcia`. Une fois les fichiers `/etc/pcmcia/config` ou `/etc/pcmcia/*.conf` modifiés, l'attribution des pilotes doit à nouveau être chargée ; cela se fait à l'aide de la commande `rcpcmcia reload` .

Le pilote n'est pas chargé L'une des raisons de ce type de problème est qu'une mauvaise attribution est enregistrée dans la base de données des pilotes. Cela peut, par exemple, être dû au fait qu'un fabricant a intégré une autre puce dans un modèle de carte apparemment non modifié. Parfois, il existe aussi d'autres pilotes qui fonctionnent mieux sur certains modèles que le pilote réglé par défaut (ou qui sont même les seuls à fonctionner d'ailleurs). Dans ces cas, vous avez besoin d'informations précises au sujet de la carte. Vous pouvez aussi obtenir de l'aide sur une liste de discussion ou en contactant le service d'assistance avancé (en anglais, *Advanced Support Service*).

Pour les cartes Cardbus, il faut saisir l'entrée `HOTPLUG_DEBUG=yes` dans le fichier `/etc/sysconfig/hotplug`. On obtient alors des messages dans le journal du système qui indique si le pilote a été chargé (avec succès).

Une autre raison peut être un conflit de ressources. Pour la plupart des cartes PCMCIA, aucune importance avec quel IRQ, port d'E/S ou domaine mémoire elles sont exploitées, mais il y a des exceptions.

Il convient donc toujours d'abord de ne tester qu'une seule carte et d'interrompre momentanément les autres composants système tels que, par exemple, les cartes son, l'IrDA, le modem ou l'imprimante.

Vous pouvez (en tant qu'utilisateur `root`) consulter la répartition des ressources du système à l'aide de la commande `lsdev`. Il est absolument normal que plusieurs appareils PCI utilisent le même IRQ.

Une solution possible consiste à trouver une option appropriée pour le module du pilote de la carte à l'aide de `modinfo` ⟨*pilote*⟩ .

La plupart des modules ont une page de manuel qui leur est consacrée. `rpm -ql pcmcia | grep man` énumère toutes les pages de manuel du paquetage `pcmcia`. Pour tester les options, les pilotes des cartes peuvent aussi être déchargés à la main.

Lorsque vous avez trouvé une solution,

vous pouvez autoriser ou interdire l'utilisation d'une ressource particulière de manière universelle dans le fichier `/etc/pcmcia/config.opts`. Les options pour les pilotes de cartes peuvent également être entrées dans ce fichier. Si, par exemple, le module `pcnet_cs` doit exclusivement être exploité avec l'IRQ 5, l'élément suivant est nécessaire :

```
module pcnet_cs opts irq_list=5
```

L'interface est mal configurée Dans ce cas, nous vous conseillons de vérifier à nouveau la configuration de l'interface et le nom de la configuration à l'aide de `getcfg` pour exclure toute erreur de configuration éventuelle. À cette fin, attribuez la valeur `yes` aux variables `DEBUG` et `HOTPLUG_DEBUG` dans les fichiers respectifs `/etc/sysconfig/network/config` et `/etc/sysconfig/hotplug`. Pour les autres cartes ou si cette modification n'est d'aucun secours, vous pouvez encore incorporer dans le script exécuté par le gestionnaire de cartes ou par hotplug (reportez-vous à `/var/log/messages`) une ligne `set -vx` . Cela permet d'ordonner que chaque commande du script soit systématiquement enregistrée dans le journal du système. Si vous avez détecté le point critique dans un script, vous pouvez aussi saisir les commandes correspondantes dans un terminal et les y tester.

14.6 Informations complémentaires

Si vous êtes intéressé par des expériences relatives à des portables particuliers, consultez dans tous les cas le site Web Linux Laptop à l'adresse suivante : `http://linux-laptop.net`. Une autre bonne source d'informations est le site Web de TuxMobil à l'adresse : `http://tuxmobil.org/`. Vous y trouverez, outre de nombreuses informations intéressantes, également des howto pour les portables et l'IrDA. Vous trouverez aussi dans la base de données d'assistance plusieurs articles sur le travail nomade sous SUSE LINUX. Cherchez sous `http://portal.suse.de/sdb/en/index.html`, sous le mot-clé*Laptop* (portable).

SCPM — System Configuration Profile Management

Ce chapitre vous présente SCPM (en anglais, *System Configuration Profile Management*). SCPM vous aide à adapter la configuration de votre ordinateur à des modifications de l'environnement de travail ou de la configuration du matériel. SCPM gère un jeu de profils de système qui sont configurés en fonction des scénarios correspondants. Une simple commutation d'un profil de système à un autre dans SCPM remplace la reconfiguration manuelle du système.

Il existe des situations exigeant que la configuration du système soit modifiée. On rencontre souvent cette situation lorsqu'un ordinateur portable est utilisé sur différents sites. Il est également possible, toutefois, que l'on doive utiliser temporairement d'autres composants matériels sur une machine de bureau. Il peut arriver également que l'on souhaite simplement expérimenter quelque chose. Dans tous les cas, il importe que la restauration du système initial soit simple à réaliser, l'idéal étant que ce changement de configuration soit aisément reproductible. SCPM permet de définir une partie de la configuration système dont on peut disposer librement, et dont les différents états peuvent être enregistrés dans des profils de configuration séparés.

La configuration réseau d'ordinateurs portables constitue probablement le principal domaine d'utilisation de SCPM. Toutefois, des configurations réseau différentes ont généralement des incidences sur d'autres éléments tels que la configuration de la messagerie ou celle des serveurs de proximité. À cela s'ajoutent aussi les différentes imprimantes utilisées au bureau et à la maison, la configuration X.Org pour les projecteurs servant lors de présentations, ou encore des paramètres d'économie d'énergie pour l'alimentation du portable en déplacement, ou les différents fuseaux horaires appliqués dans les implantations à l'étranger.

15.1 Terminologie

Examinons tout d'abord les principaux termes employés par ailleurs dans les autres documents sur SCPM et dans le module de YaST.

- La *configuration système* fait référence à la configuration de l'ordinateur dans son ensemble. Elle recouvre tous les paramètres de base tels que, par exemple, les partitions des disques durs ou la configuration réseau, la définition des fuseaux horaires ou la configuration du clavier.
- Un *profil* ou un *profil de configuration* est un état de la configuration système qui a été enregistré et peut être restauré si nécessaire.
- Le *profil actif* est toujours le dernier profil activé. Cela ne signifie pas que la configuration système courante correspond exactement à ce profil, dans la mesure où la configuration est modifiable à tout moment de manière indépendante.
- Les *ressources* dans la terminologie SCPM correspondent à tous les éléments contribuant à la configuration du système. Cela peut être un fichier ou un lien symbolique avec ses méta-données telles que l'utilisateur, les privilèges ou l'heure et la date d'accès. Il peut également s'agir d'un service système s'exécutant dans un profil et désactivé dans un autre.

- Les ressources sont organisées au sein de *groupes de ressources*. Ces groupes comportent des ressources formant un tout logique. Cela signifie, pour la plupart des groupes, qu'ils comportent un service et les fichiers de configuration correspondants. Ce mécanisme offre un moyen simple pour combiner des ressources manipulées par le programme SCPM, sans qu'il soit nécessaire de savoir quels fichiers de configuration sont requis pour chaque service. Le programme SCPM intègre une liste prédéfinie de groupes de ressources activés, qui devrait normalement être suffisante pour la plupart des utilisateurs.

15.2 Konfiguration

En principe, vous disposez de deux interface frontales pour la configuration de SCPM. Un frontal à la ligne de commande est contenu dans le paquetage `scpm` et vous pouvez configurer SCPM graphiquement à l'aide du module YaST 'Gestionnaire de profils'. Étant donné que les deux interface frontales ont les mêmes fonctionnalités et qu'il est très utile de connaître le frontal à la ligne de commande pour la compréhension du module YaST, c'est surtout le frontal à la ligne de commande qui est décrit ci-après. Les particularités du module YaST seront commentés lors de la description des opérations à la ligne de commande correspondantes.

15.2.1 Démarrage de SCPM et définition des groupes de ressources

Avant de pouvoir utiliser SCPM, il est nécessaire de l'activer au préalable. La commande`scpm enable` active SCPM. Lorsque SCPM est activé pour la première fois, il est initialisé, opération qui dure quelques secondes. SCPM peut être désactivé à tout moment à l'aide de la commande `scpm disable` afin d'éviter des changements de profils non souhaités. Après avoir été réactivé, SCPM se remet simplement à fonctionner.

SCPM gère par défaut les paramètres réseau et imprimantes ainsi que la configuration de X.Org et quelques services réseau. Dans le cas où vous souhaiteriez gérer d'autres services ou fichiers de configuration, vous devez activer les groupes de ressource correspondants. Vous pouvez lancer la commande `scpm list_groups` pour afficher les groupes de ressources de ressources déjà définis. La commande `scpm list_groups -a` permet d'afficher uniquement les groupes activés. Les commandes en ligne de commande doivent être exécutées en tant qu'administrateur `root`.

```
scpm list_groups -a

nis                 Network Information Service client
mail                Mail subsystem
ntpd                Network Time Protocol daemon
xf86                X-Server settings
autofs              Automounter service
network             Basic network settings
printer             Printer settings
```

Vous pouvez activer et désactiver les groupes avec `scpm activate_group NAME` ou `scpm deactivate_group NAME`, en remplaçant `NAME` par le nom de groupe correspondant. Vous pouvez également utiliser le Gestionnaire de profils YaST pour configurer les groupes de ressources.

15.2.2 Création et gestion de profils

Lorsque SCPM a été activé, il existe déjà un profil `default`. La commande `scpm list` affiche la liste de tous les profils disponibles. Il y a à l'origine un seul profil, qui est nécessairement le profil actif. Le nom du profil actif est affiché à l'aide de la commande `scpm active`. Le profil `default` est conçu comme la configuration par défaut servant de base pour décliner les autres profils. Il est donc recommandé de commencer par définir les paramètres communs à l'ensemble des profils. La commande `scpm reload` permet ensuite d'enregistrer ces modifications dans le profil actif. Toutefois, le profil `default` peut être copié et renommé sans restriction comme base pour de nouveaux profils.

L'ajout d'un nouveau profil peut se faire de deux façons. Si l'on veut que le nouveau profil (intitulé ici `work`) soit par exemple basé sur le profil `default`, il convient de lancer la commande `scpm copy default work`. On peut ensuite passer au nouveau profil à l'aide de la commande `scpm switch work` puis le configurer. Il peut arriver cependant que la configuration système ait déjà été modifiée pour répondre à des besoins particuliers et que l'on veuille la conserver par la suite dans un nouveau profil. Il convient alors d'exécuter la commande `scpm add work`. La configuration système est alors enregistrée dans le profil`work` et le nouveau profil apparaît comme étant le profil actif ; cela signifie que la commande `scpm reload` enregistre les modifications dans le profil `work`.

Il est bien entendu possible de renommer ou de supprimer des profils. Ces opérations sont réalisées respectivement par les commandes `scpm rename x y` et `scpm delete z`. Ainsi, si l'on veut, par exemple, remplacer le nom `work` par `travail`, il faut lancer la commande `scpm rename work travail`. Si `travail` doit ensuite être effacé, utilisez la commande `scpm delete travail`. Seul le profil actif ne peut pas être supprimé.

Remarques concernant le module de YaST : celui-ci comporte uniquement le bouton 'Ajouter'. La question qui se pose alors pour l'utilisateur est de savoir s'il souhaite copier un profil existant ou enregistrer la configuration système courante. Si l'on veut renommer un profil, il convient d'utiliser le bouton 'Modifier'.

15.2.3 Commuter entre profils de configuration

Pour commuter d'un profil à un autre (ici `work`), on utilise la commande `scpm switch work`. Il est permis de commuter vers le profil actif pour enregistrer dans ce profil les modifications qui ont été apportées à la configuration système. Cette opération peut également être exécutée à l'aide de la commande `scpm reload`.

Examinons ci-après la procédure de commutation, ainsi que les questions qui pourraient survenir à cette occasion, afin d'en permettre une meilleure compréhension. Dans un premier temps, SCPM vérifie quelles ressources du profil actif ont été modifiées depuis le dernier commutation. La liste des groupes de ressources modifiés est créée à partir de la liste des ressources modifiées. Pour chacun de ces groupes, SCPM demande ensuite si ces modifications doivent être copiées dans le profil actif. Dans le cas où – comme c'était le cas dans les version antérieures de SCPM – vous préférez afficher les différentes ressources séparément, exécutez la commande switch avec le paramètre `-r`, par exemple : `scpm switch -r work`.

```
scpm switch -r work

Checking for modified resources
Checking for Resources to be started/shut down
Checking for dependencies
Restoring profile default
```

SCPM compare ensuite la configuration système actuelle avec le nouveau profil vers lequel commuter. Cela permet d'identifier les services système qui doivent être arrêtés ou (re)démarrés en fonction des changements de configuration ou de dépendances croisées. Cette opération s'apparente à un redémarrage du système, à ceci près que celui-ci ne concerne qu'une partie du système et que le reste continue à fonctionner sans modification.

Les actions suivantes peuvent être ensuite exécutées :

1. Les services système sont arrêtés.
2. Toutes les modification des ressources (les fichiers de configuration par exemple) sont enregistrées.
3. Les services système sont redémarrés.

15.2.4 Paramètres de profil avancés

Vous pouvez saisir pour chaque profil une description qui sera ensuite affichée à l'aide de la commande `scpm list`. Cette description peut être saisie pour le profil actif à l'aide de la commande `scpm set description "text"`. Il est par ailleurs nécessaire de spécifier les profils qui ne sont pas actifs, ce qui donne la commande `scpm set description "text" work`

Il arrive parfois qu'en basculant sur un autre profil, il soit nécessaire d'exécuter des actions supplémentaires qui n'ont pas encore été prévues dans SCPM. La solution consiste à lier à chaque profil quatre programmes ou scripts exécutables qui seront exécutés à différents repères temporels du commutation. Ces repères sont les suivants :

prestop avant l'arrêt de services au moment de quitter le profil

poststop après l'arrêt de services au moment de quitter le profil

prestart avant le démarrage de services au moment d'activer le profil

poststart après le démarrage de services au moment d'activer le profil

Ces actions sont également raccrochées à la commande `set`, soit à l'aide des commandes `scpm set prestop <nomfichier>`, `scpm set poststop <nomfichier>`, `scpm set prestart <nomfichier>` ou `scpm set poststart <nomfichier>`. Le fichier en question doit être un programme exécutable : en d'autres termes, les scripts doivent spécifier l'interpréteur à utiliser.

Attention

Intégration de scripts propres

Les scripts exécutables par SCPM doivent également être lisibles et exécutables pour le super-utilisateur (`root`). L'accès à ces fichiers devraient être interdits à tous les autres utilisateurs. Utilisez les commandes `chmod 700 <nom_du_fichier>` et `chown root:root <nom_du_fichier>` pour attribuer uniquement à `root` les droits sur ces fichiers.

Attention

Tous les paramètres supplémentaires saisis à l'aide de la commande `set` peuvent être consultés à l'aide de la commande `get`. Ainsi, la commande `scpm get poststart` fournit le nom du programme poststart ou bien ne fournit tout simplement aucune information, lorsque rien n'a été associé au programme poststart. De tels paramètres sont supprimés en les écrasant avec `""`; autrement dit, la commande `scpm set prestop ""` supprime le programme poststop.

De manière analogue à la création de la description, toutes les commandes `set` et `get` peuvent être appliquées à n'importe quel profil. Il convient alors de préciser le nom du profil en question. Ainsi, on a les commandes `scpm set prestop <nomfichier> work` et `scpm get prestop work`.

15.2.5 Choix du profil lors du démarrage

Si vous souhaitez choisir un profil dès l'amorçage du système, il suffit de presser F4 pendant l'écran de démarrage pour afficher les profils disponibles et sélectionner le profil souhaité avec les touches de direction. Confirmez votre choix avec Enter et le profil sélectionné sera proposé comme option d'amorçage.

15.3 Problèmes possibles et solutions

15.3.1 Interruption lors d'une opération de commutation

Il peut arriver, dans certaines conditions, qu'une erreur d'exécution interrompe SCPM lors d'une opération de commutation. Cet événement peut être dû à des facteurs extérieurs – par exemple une interruption par l'utilisateur ou la batterie de l'ordinateur portable qui est déchargée, etc. – il peut également s'agir de

bogues du programme SCPM lui-même. En tout cas, vous obtiendrez à la prochaine exécution de SCPM un message indiquant que SCPM est verrouillé. Cette mesure vise à protéger votre système, dans la mesure où les données enregistrées par SCPM dans sa base de données sont probablement incompatibles avec l'état de votre système. Vous devez alors supprimer le fichier verrou à l'aide de la commande `rm /var/lib/scpm/#LOCK` et revenir à un état cohérent à l'aide de la commande `scpm -s reload`. Vous pouvez après cela utiliser votre ordinateur comme à l'accoutumée.

15.3.2 Modification de la configuration du groupe de ressources

Si vous souhaitez modifier la configuration du groupe de ressources alors que SCPM a déjà été initialisé, exécutez la commande `scpm rebuild` après avoir ajouté ou supprimé des groupes. Cette opération ajoute de nouvelles ressources à tous les profils et supprime ceux qui ont été retirés. Toutefois, ces derniers sont définitivement supprimés. Si vous avez avez configuré les ressources effacées différemment dans les divers profils, ces données de configuration sont alors perdues – à l'exception de la version courante de votre système, bien entendu, qui n'est pas touchée par SCPM. Dans le cas où vous décidez de modifier la configuration avec YaST il n'est pas nécessaire de faire de reconstruction (*rebuild*), cette opération étant assurée par YaST à votre place.

15.4 Informations complémentaires

Vous trouverez la documentation la plus récente dans les pages d'information de SCPM. Vous pouvez les visualiser avec des outils tels que Konqueror ou Emacs (`konqueror info:scpm`). Dans un terminal, utilisez `info` ou `pinfo`. Des informations pour les développeurs se trouvent sous `/usr/share/doc/packages/scpm`.

Gestion de l'énergie

Ce chapitre présente les différentes techniques de gestion de l'énergie sous Linux. La configuration de toutes les techniques possibles depuis APM (en anglais, *Advanced Power Management*) en passant par ACPI (en anglais, *Advanced Configuration and Power Interface*) jusqu'à l'adaptation de la fréquence du processeur (en anglais, *CPU Frequency Scaling*) est détaillée ici.

De la gestion de l'énergie pure sur les portables avec APM, le développement s'est poursuivi pour parvenir à ACPI, un outil d'information et de configuration du matériel disponible sur tous les ordinateurs modernes (portables, de bureau et serveurs). Il est en outre possible d'adapter la fréquence du processeur, en fonction de chaque situation, sur de nombreux types de matériel modernes, ce qui permet, sur les appareils mobiles, d'économiser la durée de vie de la batterie (*adaptation de la fréquence du processeur* ; en anglais, *CPU Frequency Scaling*).

Toutes les techniques de gestion de l'énergie présupposent de disposer de matériel et de routines BIOS adaptés. La plupart des portables et de nombreux ordinateurs de bureau et serveurs modernes satisfont à cette exigence. On a souvent utilisé APM(en anglais, *Advanced Power Management*) sur le matériel ancien. Comme APM se compose essentiellement d'un ensemble de fonctionnalités implémenté dans le BIOS, la prise en charge APM est, selon le matériel et les circonstances, plus ou moins bonne. ACPI est bien plus complexe et varie encore plus qu'APM, pour ce qui concerne sa prise en charge, en fonction du type de matériel. C'est pour cette raison qu'il n'y aurait aucun sens à privilégier un système plutôt qu'un autre. Testez les différents procédés sur votre matériel et utilisez la technologie la mieux prise en charge.

Remarque

Gestion de l'énergie sur les processeurs AMD64

Les processeurs AMD64 avec un noyau 64 bits ne permettent d'utiliser qu'ACPI.

Remarque

16.1 Fonctionnalités d'économie d'énergie

Les fonctionnalités d'économie d'énergie ne représentent pas seulement un intérêt pour les ordinateurs portables mais également dans le cadre d'une utilisation fixe. Les fonctionnalités les plus importantes sont décrites ci-après ainsi que leur utilisation dans le cadre des deux systèmes d'économie d'énergie APM et ACPI :

Mise en attente (*standby*) Dans ce type de fonctionnement, seul l'écran est éteint et, pour certains appareils, les performances du processeur limitées. Certains APM ne proposent pas cette fonctionnalité. Avec ACPI, elle correspond à l'état S1 ou S2.

Mise en veille (sur mémoire) (*suspend (to memory)*)
Dans ce mode, la totalité de l'état du système est inscrite dans la mémoire de travail et l'ensemble du système, en dehors de la mémoire de travail est mis en veille. Dans cet état, l'ordinateur n'a besoin que de très peu d'énergie. L'avantage de cet état est qu'il est possible en l'espace de quelques secondes seulement de reprendre son travail au point où l'on s'était arrêté sans avoir à amorcer l'ordinateur et à recharger les programmes nécessaires. Dans le cas des ordinateurs qui fonctionnent avec APM, il suffit souvent de rabattre l'écran en position fermée pour déclencher ce mode de veille et simplement de l'ouvrir à nouveau pour reprendre le travail. Avec ACPI, ce mode correspond à l'état S3. La prise en charge de ce mode est encore en développement et dépend donc fortement du matériel utilisé.

Hibernation (mise en veille sur disque)
Dans ce mode de fonctionnement, l'état du système est complètement enregistré sur le disque dur et le système ensuite éteint. La reprise à partir de cet état dure entre 30 et 90 secondes et dans ce cas aussi, c'est l'état exact avant la mise en veille qui est repris tel que. Certains fabricants proposent des formes hybrides de ce mode (par exemple, RediSafe pour les Thinkpads d'IBM). Avec ACPI, l'hibernation correspond à l'état S4. Sous Linux la *mise en veille sur disque* est exécutée par des routines du noyau qui sont indépendantes de APM et ACPI.

Contrôle de l'état de la batterie ACPI et APM contrôlent tous les deux l'état de charge de la batterie et affichent des messages relatifs à l'état de charge courant. En outre, ces deux systèmes coordonnent l'exécution d'actions simples lorsqu'un état de charge critique est atteint.

Mise hors tension automatique Une fois éteint, l'ordinateur est complètement mis hors tension. Cela a un sens avant tout lorsqu'un arrêt automatique est effectué, peu avant que la batterie soit vide.

Arrêt des composants système L'arrêt du disque dur apporte la contribution la plus importante à l'économie d'énergie de tout le système. Selon la fiabilité de l'ensemble du système il peut être mis en sommeil plus ou moins longtemps. Cependant, plus la période de sommeil du disque est longue, plus le risque de perte de données augmente. Vous pouvez désactiver les autres composants via ACPI (du moins théoriquement) ou, durablement, dans la configuration du BIOS.

Contrôle de la performance du processeur
Avec le processeur, il est possible d'économiser de l'énergie de trois façons différentes : l'adaptation de la fréquence et de la tension (connue aussi sous les noms PowerNow! et Speedstep), la diminution de la cadence (throttling) et la mise en sommeil du processeur (états C). Selon le type d'utilisation de l'ordinateur, ces différentes façons peuvent être combinées suivant vos besoins.

16.2 APM

Le BIOS APM assure seul certaines fonctionnalités d'économie d'énergie. Vous pouvez, sur de nombreux ordinateurs portables, activer la mise en attente et la mise en veille à l'aide de combinaisons de touches ou en rabattant l'écran. Le système d'exploitation ne propose, en premier lieu, aucune fonctionnalité pour ce faire. Si vous souhaitez pouvoir utiliser ce type de fonctionnement en saisissant une commande, il est recommandé d'exécuter un certain nombre d'actions avant la mise en sommeil. Pour l'affichage de l'état de charge de la batterie, des paquetages spécifiques et un noyau approprié sont nécessaires.

La prise en charge d'APM est parfaitement intégrée dans les noyaux de SUSE LINUX. Cependant, celle-ci n'est activée que si aucun ACPI n'est implémenté dans le BIOS et qu'un BIOS APM est trouvé. Pour activer la prise en charge APM, vous devez désactiver ACPI à l'invite d'amorçage en saisissant `acpi=off`. Vous pouvez facilement vérifier si APM a été activé, avec la commande `cat /proc/apm`. Si une ligne contenant divers nombres apparaît, tout est en ordre. Vous devez alors saisir une commande `shutdown -h` pour éteindre l'ordinateur.

Comme certaines implémentations de BIOS ne respectent pas les standards, on peut rencontrer des problèmes lors de l'utilisation de APM. Vous pouvez en contourner certains avec des paramètres d'amorçage particuliers. Tous les paramètres sont fournis à l'invite d'amorçage sous la forme `apm=<parameter>` :

on/off Activer ou désactiver la prise en charge APM

(no-)allow-ints Autoriser les interruptions pendant l'exécution des fonctions du BIOS.

(no-)broken-psr Le BIOS a une fonctionnalité "GetPowerStatus" qui ne fonctionne pas correctement.

(no-)realmode-power-off Repasser le processeur en mode réel avant l'arrêt.

(no-)debug Enregistrer les événements APM dans le journal système.

(no-)power-off Mettre le système hors tension après l'arrêt.

bounce-interval=⟨*n*⟩ Temps en centièmes de secondes au bout duquel, après un événement de mise en sommeil, les autres événements de mise en sommeil sont ignorés.

idle-threshold=⟨*n*⟩ Pourcentage d'inactivité système à partir duquel la fonctionnalité BIOS `idle` est appelée (0=toujours, 100=jamais).

idle-period=⟨*n*⟩ Temps en centièmes de secondes au bout duquel l'(in)activité du système est déterminée.

Le démon APM apmd utilisé auparavant n'est plus utilisé. Sa fonctionnalité est contenue dans le nouveau powersaved, qui maîtrise également ACPI et la régulation de la fréquence du processeur.

16.3 ACPI

ACPI (en anglais, *Advanced Configuration and Power Interface*) doit permettre au système d'exploitation d'organiser et de gérer les différents composants matériel individuellement. Ainsi ACPI remplace aussi bien le Plug and Play qu'APM. ACPI fournit aussi d'autres informations diverses sur la batterie, l'alimentation en énergie, la température et le ventilateur et renseigne sur les événements système, tels que par exemple "rabattre l'écran" ou "charge de la batterie faible".

Le BIOS contient des tables dans lesquelles sont répertoriées des informations sur les différents composants et les méthodes d'accès au matériel. Ces informations sont par exemple utilisées par le système d'exploitation pour attribuer des interruptions ou mettre sous ou hors tension des composants, le cas échéant. Mais comme le système d'exploitation exécute des instructions qui se trouvent dans le BIOS, tout dépend là encore de l'implémentation du BIOS. Vous trouverez dans `/var/log/boot.msg` les messages d'amorçage. ACPI les utilise pour signaler les tables trouvées et qu'il a pu lire. Vous trouverez plus d'informations sur le dépannage des problèmes ACPI dans la section *Problèmes possibles et leurs solutions* page 357.

16.3.1 Pratique

Lorsque le noyau reconnaît un BIOS ACPI lors de l'amorçage, ACPI est automatiquement activé (et APM désactivé). Le paramètre d'amorçage `acpi=on` peut tout au plus être utile sur les vieilles machines. L'ordinateur doit prendre en charge ACPI 2.0 ou une version plus récente. Vous pouvez vérifier si ACPI a été activé dans les messages d'amorçage du noyau, dans `/var/log/boot.msg`.

Doivent ensuite encore être chargés un certain nombre de modules. Ceux-ci sont chargés par le script de démarrage du démon ACPI. Si l'un de ces modules rencontre un problème, vous pouvez l'exclure du chargement ou du déchargement dans `/etc/sysconfig/powersave/common`. Vous trouverez dans le journal du système (`/var/log/messages`) les messages du module et les composants qui ont été reconnus.

Vous pouvez trouver maintenant dans `/proc/acpi` un ensemble de fichiers qui informent au sujet de l'état du système ou que vous pouvez utiliser pour modifier de manière active certains états. Les fonctionnalités ne sont pas encore toutes totalement prises en charge dans la mesure où quelques unes sont encore en phase de développement et que la prise en charge de certaines dépend fortement de l'implémentation du fabricant.

Vous pouvez afficher tous les fichiers (à l'exception de `dsdt` et `fadt`) avec la commande `cat`. Pour certains d'entre eux, vous pouvez modifier quelques réglages en indiquant avec `echo X > <datei>` les valeurs appropriées pour X. Pour accéder à ces informations et possibilités de contrôle, utilisez toujours la commande `powersave`. Pour plus de détails, vous trouverez ci-après une description des fichiers les plus importants :

`/proc/acpi/info` Informations générales à propos d'ACPI

`/proc/acpi/alarm` Définissez ici quand le système doit reprendre après une période de sommeil. Cette fonctionnalité n'est actuellement pas encore suffisamment prise en charge.

`/proc/acpi/sleep` Donne des informations sur les différents états de sommeil.

`/proc/acpi/event` Tous les événements sont consignés ici. Ils sont traités par le démon Powersave (`powersaved`). Si aucun démon n'est en train d'y accéder, vous pouvez lire les événements avec `cat /proc/acpi/event` (appuyez Ctrl + C pour terminer). Un effleurement sur l'interrupteur de mise sous tension ou l'écran rabattu sont de tels événements.

/proc/acpi/dsdt et /proc/acpi/fadt
C'est ici que se trouvent les tables ACPI, DSDT (*Differentiated System Description Table*) et FADT (*Fixed ACPI Description Table*). Vous pouvez les lire avec les commandes `acpidmp`, `acpidisasm` et `dmdecode`. Vous trouverez ces programmes et la documentation correspondante dans le paquetage `pmtools`. Exemple : `acpidmp DSDT | acpidisasm`.

/proc/acpi/ac_adapter/AC/state
L'ordinateur est-il raccordé à l'alimentation en énergie ?

/proc/acpi/battery/BAT*/{alarm,info,state}
Informations détaillées sur l'état des batteries. Pour pouvoir consulter l'état de charge, vous devez comparer `last full capacity` dans `info` avec `remaining capacity` dans `state`. Vous pouvez effectuer la même opération plus confortablement avec des programmes spéciaux tels que présentés dans la section *Outils supplémentaires* page 356. Vous pouvez préciser dans `alarm` la capacité à partir de laquelle un événement de batterie doit être déclenché.

/proc/acpi/button Ce répertoire contient des informations sur les différents interrupteurs.

/proc/acpi/fan/FAN/state Indique si le ventilateur fonctionne correctement. Vous pouvez également le mettre sous ou hors tension en inscrivant `0` (=activé) ou `3` (=désactivé) dans ce fichier. Attention, car aussi bien le code ACPI dans le noyau que le matériel (ou le BIOS) écrasent ce réglage en cas de trop forte chauffe.

/proc/acpi/processor/CPU*/info
Informations concernant les possibilités d'économie d'énergie du processeur.

/proc/acpi/processor/CPU*/power
Informations relatives à l'état actuel du processeur. Un astérisque à côté de `C2` signifie marche à vide ; c'est l'état le plus courant comme le laisse voir la valeur pour `usage`.

/proc/acpi/processor/CPU*/throttling
Vous pouvez ici configurer la réduction de la fréquence du processeur. Dans la plupart des cas, il est possible de procéder à huit niveaux de réduction. Ceci est indépendant de l'adaptation de la fréquence.

/proc/acpi/processor/CPU*/limit
Lorsque la performance (désuet) et l'étranglement (throttling) sont automatiquement réglés par un démon, indiquez ici les limites à ne pas dépasser.

Il existe des limites définies par le système et certaines qui peuvent être réglées par l'utilisateur.

`/proc/acpi/thermal_zone/` Un sous-répertoire est prévu ici pour chaque zone thermique. Une zone thermique est un domaine avec des propriétés thermiques semblables ; leur nombre et leur nom est choisi par le fabricant de matériel informatique. Les nombreuses possibilités proposées par ACPI sont cependant rarement implémentées. En revanche, la gestion de la température est effectuée de manière classique, directement par le BIOS, sans accorder le moindre droit à la parole au système d'exploitation car c'est tout simplement la durée de vie du matériel qui est ici en jeu. Les descriptions ci-après sont donc partiellement théoriques.

`/proc/acpi/thermal_zone/*/temperature`
La température actuelle de la zone thermique.

`/proc/acpi/thermal_zone/*/state`
L'état indique si tout est `ok` ou si ACPI assure un refroidissement `actif` ou `passif`. Pour les systèmes de ventilation indépendants d'ACPI, l'état est toujours `ok`.

`/proc/acpi/thermal_zone/*/cooling_mode`
Vous pouvez choisir ici la méthode de refroidissement contrôlée par ACPI préférée ; passive (moins de performances mais économique) ou active (100 % de performance et 100 % du bruit du ventilateur).

`/proc/acpi/thermal_zone/*/trip_points`
Vous pouvez définir ici à partir de quelle température une mesure doit être entreprise. Les options possibles varient entre un refroidissement passif ou actif jusqu'à la mise en sommeil (`hot`) voire à la mise hors tension de l'ordinateur (`critical`). Les actions possibles sont définies, selon les appareils, dans la table DSDT. Les points de déclenchement définis dans les spécifications ACPI sont : `critical`, `hot`, `passive`, `active1` et `active2`. Même s'ils ne sont pas tous implémentés, vous devez, lorsque vous écrivez dans le fichier `trip_points`, les saisir tous dans cet ordre. Ainsi une entrée comme `echo 90:0:70:0:0 > trip_points` correspond à une température de `90` pour `critical` et de `70` pour `passive`.

`/proc/acpi/thermal_zone/*/polling_frequency`
Lorsque la valeur dans `temperature` n'est pas automatiquement mise à jour, dès que la température varie, il est possible ici de passer au mode d'interrogation (en anglais, *polling modus*). La commande `echo X > /proc/acpi/thermal_zone/*/polling_frequency` implique que la température est sondée toutes les `X` secondes. Utilisez `X=0` pour à nouveau désactiver l'interrogation.

Vous n'avez pas besoin de régler manuellement ces informations, configurations et événements. Pour cela, vous disposez du démon Powersave (powersaved) et de différentes applications telles que powersave, kpowersave et wmpowersave (voir section *Outils supplémentaires* page suivante). Étant donné que powersaved contient les fonctionnalités de l'ancien acpid, celui-ci n'est plus nécessaire.

16.3.2 Contrôle de la performance du processeur

Avec le processeur, il est possible d'économiser de l'énergie de trois façons différentes qui, selon le type d'utilisation de l'ordinateur peuvent être combinées suivant vos besoins. Économie d'énergie signifie également que le système chauffe moins et qu'il sollicite donc moins la ventilation.

Adaptation de la fréquence et de la tension
PowerNow! et Speedstep sont les noms donnés par les entreprises AMD et Intel pour cette technique qui existe aussi dans les processeurs d'autres fabricants. Ici, la fréquence du processeur et sa tension intrinsèque sont toutes deux diminuées. L'avantage réside dans une économie d'énergie plus que linéaire. C'est à dire que pour une fréquence (et donc une performance) diminuée de moitié, c'est nettement plus que la moitié de l'énergie qui est économisée. Cette technique fonctionne indépendamment de APM ou de ACPI et nécessite un démon qui régule la fréquence et les performances requises. Les paramètres peuvent être configurés dans le répertoire `/sys/devices/system/cpu/cpu*/cpufreq/`.

Réduction de la cadence d'horloge Cette technique est connue sous le nom de throttling. Ici, un certain pourcentage des cycles d'horloge du processeur est supprimé. Un quart est supprimé pour un étranglement de 25%, et pour un étranglement de 87,5%, il n'y a plus qu'un huitième des cycles d'horloge. Cependant, l'économie d'énergie n'est pas tout à fait linéaire. On utilise le throttling uniquement lorsqu'il n'y a pas de régulation de la fréquence ou pour une économie maximale. Cette technique doit également être contrôlée par un processus propre. L'interface du système est `/proc/acpi/processor/*/throttling`.

Mise en sommeil du processeur Le processeur est toujours mis en sommeil par le système d'exploitation lorsqu'il n'y a rien à faire. Dans ce cas, le système d'exploitation envoie au processeur l'instruction `halt` prévue à cet effet. Il existe différents niveaux C1, C2 et C3. Dans l'état C3, le plus économique, même le processus de comparaison de la mémoire cache du processeur avec la mémoire principale est arrêté ; cet état ne peut donc être pris que lorsqu'aucun périphérique ne modifie le contenu de la mémoire principale par activité de bus maître. Certains pilotes empêchent ainsi l'utilisation de C3. L'état courant est affiché dans `/proc/acpi/processor/*/power`.

L'adaptation de la fréquence comme la réduction de la cadence d'horloge ne sont intéressants lorsque le processeur a quelque chose à faire car dans le cas contraire, ce sont les états C, plus économiques qui sont favorisés.

Cependant, lorsque le processeur est occupé, la régulation de la fréquence est la meilleur méthode d'économie d'énergie. Souvent, le processeur n'est que partiellement occupé. Une fréquence réduite lui suffit alors pour fonctionner. En général, l'adaptation dynamique de la fréquence à l'aide d'un démon (par exemple powersaved) est la meilleure solution. Lorsque l'ordinateur fonctionne sur batterie ou lorsqu'il doit ne doit pas chauffer, c'est à dire être silencieux, la spécification d'une fréquence basse définie peut être préférable.

Le throttling ne devrait être utilisé qu'en dernière extrémité lorsque l'on souhaite, par exemple, augmenter la durée de vie des batteries malgré le fonctionnement du système. Cependant, certains systèmes ne fonctionnent plus correctement lorsque l'étranglement est trop important. La suppression de cycles d'horloge n'est d'aucun intérêt lorsque le processeur n'a que peu à faire.

Le démon powersave contrôle aussi ces techniques sous SUSE LINUX. La configuration nécessaire à cette fin est décrite dans une section qui lui est propre (voir *Le paquetage powersave* page 360).

16.3.3 Outils supplémentaires

Il existe un grand nombre d'outils ACPI plus ou moins volumineux, notamment des outils d'informations purs, qui indiquent l'état de la batterie, la température, etc. (acpi, klaptopdaemon, wmacpimon etc.). D'autres facilitent l'accès aux structures sous `/proc/acpi` ou aident à observer les modifications (akpi, acpiw, gtkacpiw). De plus, il existe aussi des outils pour le traitement des tables ACPI dans le BIOS (paquetage `pmtools`).

16.3.4 Problèmes possibles et leurs solutions

Il existe deux groupes de problèmes différents. D'une part, il peut naturellement y avoir des erreurs dans le code ACPI du noyau qui n'ont pas encore été relevées. D'autre part, il peut toutefois y avoir une solution à télécharger. Les problèmes au niveau du BIOS de l'ordinateur sont malheureusement moins agréables et aussi plus fréquents. Il arrive malheureusement que des écarts aient été insérés par rapport aux spécifications ACPI du BIOS pour contourner des erreurs de l'implémentation ACPI dans d'autres systèmes d'exploitation très développés. Il existe aussi du matériel connu pour ses erreurs graves dans l'implémentation ACPI et qui est donc répertorié dans une liste noire afin de ne pas utiliser dessus ACPI pour le noyau Linux.

En cas de problème, la première chose à faire est la mise à jour du BIOS. Si l'ordinateur n'amorce pas du tout, l'un des paramètres d'amorçage suivants peut se révéler utile :

pci=noacpi Ne pas utiliser ACPI pour la configuration des appareils PCI.

acpi=oldboot Ne procéder qu'aux configurations de ressources simples, sinon, ne pas utiliser ACPI.

acpi=off Ne pas utiliser ACPI.

Attention

Problèmes lors de l'amorçage sans ACPI

Certains ordinateurs de la nouvelle génération, notamment les systèmes SMP et AMD64 ont besoin d'ACPI pour configurer correctement le matériel. Si l'on désactive ACPI, cela peut engendrer des problèmes.

Attention

Surveillez bien les messages du système lors de l'amorçage. Utilisez pour cela la commande `dmesg | grep -2i acpi` après l'amorçage (ou alors on affiche tous les messages, car ACPI n'est pas nécessairement responsable du problème). En cas d'erreur lors de l'analyse d'une table ACPI, vous avez la possibilité, du moins pour la table la plus importante, la table DSDT, de créer une table corrigée dans un noyau individuel. La DSDT erronée du BIOS est par la suite ignorée. La procédure à suivre est détaillé dans la section *Problèmes possibles et solutions* page 366.

Vous disposez, lors de la configuration du noyau, d'un interrupteur pour activer les messages de débogage d'ACPI. Lorsque vous compilez un noyau avec le débogage ACPI et que vous l'installez, vous pouvez fournir des informations détaillées aux experts à la recherche d'erreurs.

En cas de problèmes relatifs au BIOS ou au matériel, il est toujours judicieux de s'adresser au fabricant de l'appareil. Même quand ces derniers ne sont pas toujours d'un grand secours lorsqu'il s'agit d'un système fonctionnant sous Linux, il est important de les informer d'éventuels problèmes. Ce n'est que lorsque les fabricants auront remarqué que suffisamment de leurs clients optent pour Linux qu'ils le prendront au sérieux.

Informations complémentaires

Vous trouverez plus de documentation et d'aide relatives à ACPI dans :

- le magazine allemand c't 2002, Heft 25: Schöne neue Welt (Dominik Brodowski, Oliver Diedrich)
- `http://www.cpqlinux.com/acpi-howto.html` (HowTo ACPI un peu plus précis, contient des correctifs de la DSDT)
- `http://www.intel.com/technology/iapc/acpi/faq.htm` (FAQ ACPI chez Intel)
- `http://acpi.sourceforge.net/` (Le projet ACPI4Linux de Sourceforge)
- `http://www.poupinou.org/acpi/` (Correctifs DSDT de Bruno Ducrot)

16.4 Pause du disque dur

Le disque dur peut être complètement arrêté sous Linux lorsqu'il n'est pas utilisé ou lorsque vous utilisez un mode économique ou silencieux. Cependant, notre expérience montre qu'il n'est pas intéressant, dans le cas de ordinateurs portables modernes, d'arrêter en partie un disque dur car ceux-ci se mettent d'eux-mêmes dans un mode économique lorsqu'ils ne sont pas utilisés. Néanmoins, si vous souhaitez être particulièrement économe, vous pouvez tester l'une des possibilités suivantes. La plupart des fonctionnalités peuvent être contrôlées à l'aide de powersaved.

Le programme hdparm est utilisé pour procéder à différents réglages du disque dur. L'option `-y` permet de mettre le disque immédiatement en attente, l'option `-Y` (Attention !) permet de l'arrêter complètement. `hdparm -S <x>` permet d'arrêter le disque dur après une certaine durée d'inactivité. Le joker ⟨*x*⟩ a la signification suivante : `0` arrête ce mécanisme, le disque dur fonctionne toujours. Les valeurs de `1` à `240` sont multipliées par cinq secondes. `241` à `251` correspondent à entre 1 et 11 fois 30 minutes.

Les possibilités d'économie d'énergie internes au disque dur sont contrôlées à l'aide de l'option `-B`. Ici, il est possible de choisir un nombre entre `0` (économie maximale) et `255` (performance maximale). Le résultat dépend du disque utilisé et est difficile à juger. Pour qu'un disque dur soit plus silencieux, l'option `-M` peut être utilisée. Ici aussi, on choisit une valeur entre `128` (silencieux) et `254` (rapide).

Il n'est cependant pas toujours si facile d'écrire des données sur le disque dur, puis de redémarrer le disque, car il existe sous Linux un grand nombre de processus qui gardent toujours le disque dur éveillé. Il est donc capital que vous compreniez à présent la manière dont Linux traite les données qui doivent être écrites sur le disque dur. Toutes les données sont tout d'abord enregistrées de manière intermédiaire dans une mémoire tampon de la mémoire de travail. Ce tampon est surveillé par le démon de mise à jour du noyau, "Kernel Update Daemon" (kupdated). À chaque fois que des données atteignent un certain âge ou que le tampon atteint un certain niveau de remplissage, le tampon est vidé et les données écrites sur le disque dur. La taille du tampon est du reste dynamique et dépend de la taille de la mémoire et du degré d'exploitation du système. Comme l'objectif principal est la sécurité des données, kupdated est réglé par défaut sur de petits intervalles de temps. Il vérifie la mémoire tampon toutes les 5 secondes et informe le démon bdflush lorsque les données ont plus de 30 secondes ou quand le tampon est rempli à 30 %. Le démon bdflush écrit alors les données sur le disque dur. Il les écrit aussi sans se soucier de kupdated quand par exemple le tampon est rempli.

Attention

Atteinte à la sécurité des données

Les modifications des réglages du démon de mise à jour du noyau mettent en danger la sécurité des données.

Attention

Outre tous ces processus, les "systèmes de fichiers journalisés" tels que, par exemple, ReiserFS ou Ext3 écrivent leurs méta-données sur le disque dur indépendamment de bdflush, ce qui empêche naturellement une mise en sommeil du disque dur. Pour l'éviter, il existe à présent une extension dans le noyau qui a été tout spécialement développée pour les appareils mobiles. Vous en trouverez une description précise dans le fichier `/usr/src/linux/Documentation/laptop-mode.txt`.

Il faut, en outre, naturellement surveiller la manière dont les programmes que vous utilisez déjà se comportent. Ainsi, les bons éditeurs de texte écrivent régulièrement des sécurités cachées des données qui viennent d'être modifiées sur le disque dur, avec pour conséquence que le disque dur est sans arrêt sollicité. Vous pouvez inhiber ce type de comportements des programmes, mais ici aussi au prix de la sécurité des données. Pour trouver quel processus écrit sur le disque, il est possible d'activer un mode de débogage avec `echo 1 > /proc/sys/vm/block_dump`. De cette façon, toutes les activités des disques sont archivés dans le journal du système. Un `0` dans ce fichier désactive à nouveau ce mode.

À ce propos, il existe pour le démon de messagerie postfix une variable `POSTFIX_LAPTOP`. Si celle-ci a la valeur `yes`, postfix accède beaucoup moins au disque dur. Cela n'a cependant aucune importance si l'intervalle de kupdated a été allongé.

16.5 Le paquetage powersave

Le paquetage `powersave` est responsable de l'économie d'énergie lors du fonctionnement sur batteries des ordinateurs portables. Certaines de ses caractéristiques sont toutefois aussi intéressantes pour les ordinateurs de bureau et les serveurs, par exemple, les modes veille et attente, la gestion des boutons ACPI et l'extinction des disques durs IDE.

Ce paquetage rassemble toutes les fonctions de gestion d'énergie pour votre ordinateur. Il prend en charge le matériel utilisant ACPI, APM, la gestion des disques durs IDE et les technologies PowerNow! ou SpeedStep suivant les cas. Les fonctionnalités offertes par les paquetages `apmd`, `acpid`, `ospmd` et `cpufreqd` (et, dans le même temps, `cpuspeed`) sont rassemblées dans le paquetage `powersave`. Il est déconseillé d'exécuter les démons de ces paquetages parallèlement au démon powersave.

Il est conseillé d'utiliser le démon powersave pour le contrôle des fonctions d'économie d'énergie, même si votre système ne comprend pas tous les éléments matériels cités précédemment. ACPI et APM s'excluent mutuellement ; vous ne pouvez utiliser que l'un des deux sur votre système. Des modifications éventuelles de la configuration matérielle sont reconnues automatiquement par le démon.

Remarque

Informations sur powersave

Des informations actualisées sur le paquetage powersave sont également disponibles, en plus de ce chapitre, dans le fichier `/usr/share/doc/packages/powersave`.

Remarque

16.5.1 Configuration du paquetage powersave

D'une manière générale, la configuration de powersave est répartie sur plusieurs fichiers :

`/etc/sysconfig/powersave/common`
Ce fichier contient des paramètres généraux pour le démon powersave. Entre autres, le nombre de messages de débogage (dans `/var/log/messages`) peut être augmenté en changeant la valeur de la variable `POWERSAVE_DEBUG`.

`/etc/sysconfig/powersave/events`
Ce fichier est nécessaire au démon powersave pour garantir le traitement des événements (en anglais *Events*) du système qui se produisent. Des actions externes ou des actions que le démon traite lui-même peuvent être attribuées à un événement. On parle d'actions externes lorsque le démon essaie d'activer un fichier exécutable qui est situé dans `/usr/lib/powersave/scripts/`. Les actions internes prédéfinies :

- ignore
- throttle
- dethrottle
- suspend_to_disk
- suspend_to_ram
- standby
- do_suspend_to_disk

- do_suspend_to_ram
- do_standby

`throttle` ralentit le processeur de la valeur qui est définie par `POWERSAVE_MAX_THROTTLING`. Cette valeur est dépendante du profil utilisé actuellement. `dethrottle` redonne ses performances initiales au processeur. `suspend_to_disk`, `suspend_to_ram` et `standby` initient l'événement système pour un mode de sommeil. Ces trois dernières actions sont généralement reponsables de la mise en sommeil mais devraient toujours être soumis à des événements systèmes bien définis.

Des scripts pour le traitement d'événements se trouvent dans le répertoire `/usr/lib/powersave/scripts` :

notify Avertissement à travers la console, le fenêtre X ou un signal acoustisque d'un événement se produisant

screen_saver Activation de l'économiseur d'écran

switch_vt utile lorsque, après une mise en veille ou en attente, l'écran est déplacé

wm_logout enregistrement de la configuration et déconnexion de GNOME ou KDE ou d'autres gestionnaires de fenêtre

wm_shutdown enregistrement de la configuration GNOME ou KDE et arrêt du système

Si, par exemple, la variable `POWERSAVE_EVENT_GLOBAL_-SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_-disk"` est définie, les deux scripts ou actions exécutés sont traités dans l'ordre défini dès que l'utilisateur donne à powersaved l'ordre pour le mode sommeil `Suspend to disk`. Le démon exécute le script externe `/usr/lib/powersave/scripts/prepare_suspend_to_disk`. Lorsque celui-ci est traité avec succès, le démon exécute l'action interne `do_suspend_to_disk` et met l'ordinateur définitivement en sommeil une fois que le script a arrêté les modules et les services critiques.

Une modification des actions pour l'événement d'un bouton (Sleep) pourrait être comme suit :
`POWERSAVE_EVENT_BUTTON_SLEEP="notify suspend_to_disk"`
Dans ce cas, l'utilisateur est informé de la mise en veille par le script externe `notify`. Ensuite, l'événement `POWERSAVE_EVENT_GLOBAL_-SUSPEND2DISK` est créé qui a pour suite l'exécution des actions décrites ci-dessus et garantit un mode de mise en veille sûr du système.

Le script `notify` peut être modifié dans `/etc/sysconfig/powersave/common` avec la variable `POWERSAVE_NOTIFY_METHOD`.

/etc/sysconfig/powersave/cpufreq
Le fichier contient des variables pour l'optimisation des paramètres dynamiques de la fréquence du processeur.

/etc/sysconfig/powersave/battery
Contient les limites de la batterie et d'autres paramètres spécifiques à la batterie.

/etc/sysconfig/powersave/sleep
Dans ce fichier, vous pouvez définir quels modules et quels services doivent être arrêtés avant que la mise en sommeil soit effectuée. Ceux-ci seront rechargés et démarrés lors de la remise en route du système. En outre, vous pouvez retarder une mise en sommeil déclenchée (pour éventuellement encore sécuriser des données).

/etc/sysconfig/powersave/thermal
Ici, le contrôle pour la régulation de la ventilation et de la chaleur est activé. Vous trouverez plus de détails à ce sujet dans le fichier `/usr/share/doc/packages/powersave/README.thermal`.

/etc/sysconfig/powersave/scheme_*
Il s'agit des différents profils, qui régissent l'ajustement de la consommation d'énergie suivant des scénarios d'utilisation déterminés. Un certain nombre de schémas sont préconfigurés et utilisables sans autre modification. Toutefois, vous pouvez aussi intégrer à ce fichier vos propres profils.

16.5.2 Configuration d'APM et ACPI

Mise en veille (Suspend) et mise en attente (Standby)

Par défaut, les modes de mise en sommeil sont désactivés étant donné qu'ils ne fonctionnent toujours pas sur certains ordinateurs. Il existe trois modes de mise en sommeil ACPI et deux modes APM :

Suspend to Disk (ACPI S4, APM suspend)
Enregistre le contenu entier de la mémoire sur le disque dur. L'ordinateur s'arrête complètement et n'utilise pas de courant.

Suspend to RAM (ACPI S3, APM suspend)
Enregistre l'état de tous les appareils dans la mémoire principale. Il n'y a plus que la mémoire principale qui soit alimentée en courant.

Standby (ACPI S1, APM standby) Arrête, selon le fabricant, quelques appareils.

Dans le fichier `/etc/sysconfig/powersave/sleep`, vous pouvez activer ces modes et définir quels modules et services critiques doivent être arrêtés avant un événement de mise en veille ou en attente. Lorsque, plus tard, le système est remis en route, ceux-ci sont rechargés et démarrés. La pré-configuration concerne principalement les modules USB et PCMCIA. Si la mise en veille ou la mise en attente échoue, cela est probablement dû à certains modules. Vous trouverez des conseils pour déterminer l'erreur dans la section *Problèmes possibles et solutions* page 366.

Assurez-vous que les options standard suivantes pour le traitement correct de la mise en veille ou en attente ou la reprise soient correctement définies dans le fichier `/etc/sysconfig/powersave/events`. (pré-configuré après l'installation de SUSE LINUX) :

```
POWERSAVE_EVENT_GLOBAL_SUSPEND2DISK=
    "prepare_suspend_to_disk do_suspend_to_disk"
POWERSAVE_EVENT_GLOBAL_SUSPEND2RAM=
    "prepare_suspend_to_ram do_suspend_to_ram"
POWERSAVE_EVENT_GLOBAL_STANDBY=
    "prepare_standby do_standby"
POWERSAVE_EVENT_GLOBAL_RESUME_SUSPEND2DISK=
    "restore_after_suspend_to_disk"
POWERSAVE_EVENT_GLOBAL_RESUME_SUSPEND2RAM=
    "restore_after_suspend_to_ram"
POWERSAVE_EVENT_GLOBAL_RESUME_STANDBY=
    "restore_after_standby"
```

États de la batterie définis par l'utilisateur

Dans le fichier `/etc/sysconfig/powersave/battery`, vous pouvez définir trois niveaux de charge de la batterie (en pourcentage). Lorsque ces niveaux sont atteints, le système envoie un message d'avertissement ou exécute des opérations déterminées.

```
POWERSAVED_BATTERY_WARNING=20
POWERSAVED_BATTERY_LOW=10
POWERSAVED_BATTERY_CRITICAL=5
```

Les opérations ou scripts à exécuter lorsque la charge de la batterie descend en dessous d'un seuil donné sont définis dans le fichier de configuration `/etc/sysconfig/powersave/events`. Vous pouvez modifier les actions standard pour les boutons tel que décrit dans la section *Configuration du paquetage powersave* page 361.

```
POWERSAVE_EVENT_BATTERY_NORMAL="ignore"
POWERSAVE_EVENT_BATTERY_WARNING="notify"
POWERSAVE_EVENT_BATTERY_LOW="notify"
POWERSAVE_EVENT_BATTERY_CRITICAL="wm_shutdown"
```

Ajustement de la consommation d'énergie dans différentes conditions de travail.

Il est possible de faire dépendre le comportement du système de son alimentation électrique. Ainsi, la consommation du système devrait être réduite lorsque le système est déconnecté du réseau électrique et fonctionne sur batterie. Inversement, les performances du système devraient automatiquement revenir à un niveau élevé dès que le système est reconnecté au réseau électrique. La fréquence du processeur, la fonction d'économie d'énergie des disques durs IDE ainsi que quelques autres paramètres ont une influence réelle sur la consommation d'énergie.

Lors d'une connexion au réseau électrique ou de la déconnexion, l'exécution de certaines actions bien définies est spécifiée dans `/etc/sysconfig/powersave/events`. Vous définissez les scénarios à appliquer (qu'on appelle profils) dans le fichier `/etc/sysconfig/powersave/common` :

```
POWERSAVE_AC_SCHEME="performance"
POWERSAVE_BATTERY_SCHEME="powersave"
```

Chaque profil est stocké dans un fichier lui correspondant, dans le répertoire `/etc/sysconfig/powersave`. Les noms de fichiers sont constitués de la manière suivante : `scheme_<Nom du profil>`. Dans l'exemple ci-dessus, deux profils sont référencés : `scheme_performance` et `scheme_powersave`. Les profils `performance`, `powersave`, `presentation` et `acoustic` sont livrés pré-configurés. Vous pouvez à tout moment, au moyen du module de gestion de l'énergie de YaST (voir section *Le module de gestion d'énergie de YaST* page 369), mettre en place de nouveaux profils, modifier ou supprimer des profils existants ou modifier leur affectation aux états d'alimentation électrique.

16.5.3 Autres fonctionnalités d'ACPI

Si vous êtes amené à utiliser ACPI, vous pouvez contrôler la réaction de votre système aux boutons ACPI (Power, Sleep et "Écran ouvert", "Écran rabattu"). L'exécution des opérations correspondantes est définie dans le fichier `/etc/sysconfig/powersave/events`. Pour plus d'informations sur chacune des options, veuillez vous référer à ce fichier de configuration.

POWERSAVE_EVENT_BUTTON_POWER="wm_shutdown"
Si vous appuyez sur le bouton (Power), le système provoque l'extinction du gestionnaire de fenêtres (KDE, GNOME, fvwm...).

POWERSAVE_EVENT_BUTTON_SLEEP="suspend_to_disk"
Si vous appuyez sur le bouton (Sleep), le système passe en mode veille sur disque.

POWERSAVE_EVENT_BUTTON_LID_OPEN="ignore"
L'ouverture de l'écran ne déclenche aucune action.

POWERSAVE_EVENT_BUTTON_LID_CLOSED="screen_saver"
L'économiseur d'écran est activé quand l'écran est rabattu.

Si, pendant une certaine durée, le processeur n'est pas utilisé au delà d'une certain proportion, vous pouvez réduire son activité en conséquence. La variable `POWERSAVED_CPU_LOW_LIMIT` vous permet de définir le niveau en dessous duquel, au delà d'un certain temps — durée que vous définissez dans la variable `POWERSAVED_CPU_IDLE_TIMEOUT` — l'activité du processeur est réduite.

16.5.4 Problèmes possibles et solutions

On trouve un enregistrement de chaque erreur et de chaque message d'avertissement dans le fichier `/var/log/messages`. Si vous ne trouvez à première vue aucune indication, affectez à la variable `DEBUG` la valeur powersave dans le fichier `/etc/sysconfig/powersave/common` de façon à obtenir des messages plus détaillés. Puis incrémentez la valeur de cette variable à `7` ou même à `15` et relancez le démon. Grâce aux messages d'erreur désormais plus détaillés disponibles dans le fichier `/var/log/messages`, vous devriez être en mesure de cerner le problème. Les questions et réponses suivantes couvrent les problèmes rencontrés le plus fréquemment avec powersave.

ACPI est activé mais les fonctionnalités décrites dans ce chapitre ne sont pas disponibles bien qu'elles devraient être prises en charge par mon matériel

Si vous avez des problèmes avec l'ACPI, utilisez la commande suivante pour rechercher des messages spécifiques à l'ACPI parmi les résultats de `dmesg` : `dmesg|grep -i acpi`.

Pour résoudre ce problème, une mise à jour du BIOS peut s'avérer nécessaire. Consultez la page d'accueil du fabricant de votre ordinateur portable, recherchez-y une version actualisée du BIOS et installez-la sur votre système. Indiquez au fabricant de votre ordinateur qu'il doit se conformer aux dernières spécifications ACPI.

Si les mêmes problèmes surviennent encore après la mise à jour du BIOS, recherchez dans les sites web suivants la dernière version de la DSDT correspondant à votre système et remplacez dans votre BIOS la table DSDT erronée :

1. Téléchargez la DSDT correspondant à votre système à l'adresse `http://acpi.sourceforge.net/dsdt/tables`. Assurez-vous que le fichier est décompressé et compilé (ce que vous pouvez vérifier avec l'extension de fichier en `.aml` (*ACPI Machine Language*)). Si tel est bien le cas, vous pouvez poursuivre à la troisième étape.
2. Si la table que vous avez téléchargée a pour extension de fichier `.asl` (*ACPI Source Language*), elle doit être compilée avec l'application `iasl` du paquetage `pmtools`. Exécutez à cette fin, la commande `iasl -sa <fichier>.asl`. La version la plus récente d'`iasl` (compilateur Intel ACPI) est par ailleurs disponible à l'adresse `http://developer.intel.com/technology/iapc/acpi/downloads.htm`.
3. Copiez le fichier `DSDT.aml` à l'emplacement qui vous convient (nous conseillons l'emplacement `/etc/DSDT.aml`). Éditez `/etc/sysconfig/kernel` et renseignez le chemin d'accès au fichier DSDT avec la valeur correspondante. Lancez `mkinitrd` (commande du paquetage `mkinitrd`). Dès que vous désinstallerez votre noyau et que vous construirez un `initrd` à l'aide de `mkinitrd`, la nouvelle table DSDT sera intégrée et chargée au démarrage.

CPU Frequency (PowerNow!/SpeedStep) ne fonctionne pas

Vérifiez, en vous basant sur les sources du noyau (`kernel-source`), si votre processeur est bien pris en charge et si vous devez éventuellement utiliser un module-noyau spécifique, ou une option de module particulière, pour activer CPU-Frequency. Ces informations sont disponibles dans les fichiers `/usr/src/linux/Documentation/cpu-freq/*`. Lorsqu'un module ou une option particuliers sont requis, vous devez configurer les variables `CPUFREQD_MODULE` et `CPUFREQD_MODULE_OPTS` dans le fichier `/etc/sysconfig/powersave/cpufreq`.

La mise en veille ou en attente (Suspend/Standby) ne fonctionne pas

Il existe plusieurs problèmes connus, liés au noyau, qui empêchent l'utilisation de la mise en veille ou en attente (Suspend/Standby) sur des systèmes **ACPI** :

- Actuellement, les systèmes dotés de plus d'1 Go de RAM ne permettent pas (encore) d'utiliser la mise en veille (Suspend).
- Les systèmes multi-processeurs ou basés sur le processeur P4 (avec l'Hyper-threading) ne permettent pas, pour le moment, d'utiliser la mise en veille (Suspend).

Le problème peut également venir d'une implémentation défectueuse de votre DSDT (BIOS). Dans ce cas, importez une nouvelle DSDT.

Sur des systèmes **ACPI** et **APM** s'applique ce qui suit :

Dès que votre système cherche à retirer de la mémoire des modules défectueux, l'ordinateur se bloque et l'événement de mise en veille n'est pas déclenché. Le processus inverse est également possible, si vous ne déchargez ou ne stoppez pas des modules/services qui empêchent Suspend de se réaliser. Dans les deux cas, vous devrez tenter de localiser les modules posant problème. Les fichiers de journalisation créés par le démon powersave dans `/var/log/<Schlafmodus>` sont très utiles. Si l'ordinateur ne passe pas du tout en mode sommeil, il faut en rechercher la cause dans le dernier module à décharger. Vous pouvez décharger les modules problématiques avant la mise en veille/attente en manipulant les paramètres suivants dans le fichier `/etc/sysconfig/powersave/common` :

```
POWERSAVE_UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
POWERSAVE_UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
POWERSAVE_UNLOAD_MODULES_BEFORE_STANDBY=""
POWERSAVE_SUSPEND2DISK_RESTART_SERVICES=""
POWERSAVE_SUSPEND2RAM_RESTART_SERVICES=""
POWERSAVE_STANDBY_RESTART_SERVICES=""
```

Si vous utilisez la mise en veille/attente dans différents environnements de réseau ou en connexion avec des systèmes de fichiers montés distants (par exemple, Samba, NIS, etc.), préférez alors automounter, pour monter ceux-ci ou entrez les services correspondants (par exemple, `smbfs` ou `nfs`) dans la variable citée ci-dessus. Lorsqu'un programme accède à un système de fichiers monté distant avant une mise en veille/attente, le service ne peut pas être arrêté correctement et le système de fichiers ne peut pas être vraiment libéré. Après la reprise du système, le système de fichiers peut être corrompu et devoir être monté à nouveau.

Lorsque j'utilise ACPI, le démon Powersave ne reconnaît pas si un seuil de charge de la batterie est atteint

Dans le cadre d'ACPI, le système de gestion de l'énergie peut demander au BIOS d'envoyer un message lorsqu'un seuil de charge de la batterie est franchi. L'avantage de cette méthode est qu'il n'est pas indispensable de lire en permanence l'état de charge de la batterie, ce qui réduirait les performances de l'ordinateur. Toutefois, il peut arriver que ce processus d'alerte en provenance du BIOS, qui devrait certes fonctionner, ne se déclenche en fait jamais, même en cas de franchissement de la limite de charge.

Si vous observez un tel comportement sur votre système, attribuez la valeur `yes` à la variable `POWERSAVED_FORCE_BATTERY_POLLING` dans le fichier `/etc/sysconfig/powersave/battery` afin de forcer la lecture de l'état de la batterie.

16.6 Le module de gestion d'énergie de YaST

Le module Gestion d'énergie de YaST vous permet de configurer toutes les options de la gestion d'énergie décrites dans les sections précédentes.

Lorsque vous lancez le module dans le Centre de contrôle de YaST ('Système' → 'Gestion d'énergie'), le premier dialogue du module (voir la figure 16.1 page suivante) s'affiche, et vous pouvez y choisir les "profils" (*schemas*) à utiliser pour les différents modes de fonctionnement — Fonctionnement sur batterie ou Fonctionnement sur alimentation électrique.

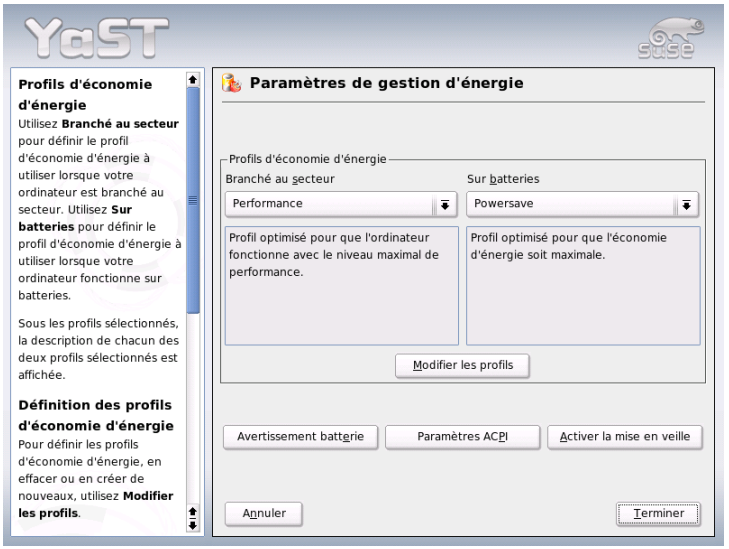


FIG. *16.1:* *Gestion d'énergie de YaST : choix des profils*

Vous pouvez choisir ici l'un des profils existants au moyen d'un menu déroulant, ou bien, en appuyant sur le bouton 'Éditer les profils', obtenir un aperçu de ces profils disponibles (figure 16.2 page suivante).

Dans l'aperçu des profils, sélectionnez le profil que vous voulez modifier et cliquez sur 'Modifier' pour accéder à la boîte d'édition (voir la figure 16.3 page 372). Vous pouvez aussi créer un nouveau profil en appuyant sur le bouton 'Ajouter'. Dans les deux cas, la boîte de dialogue suivante est identique.

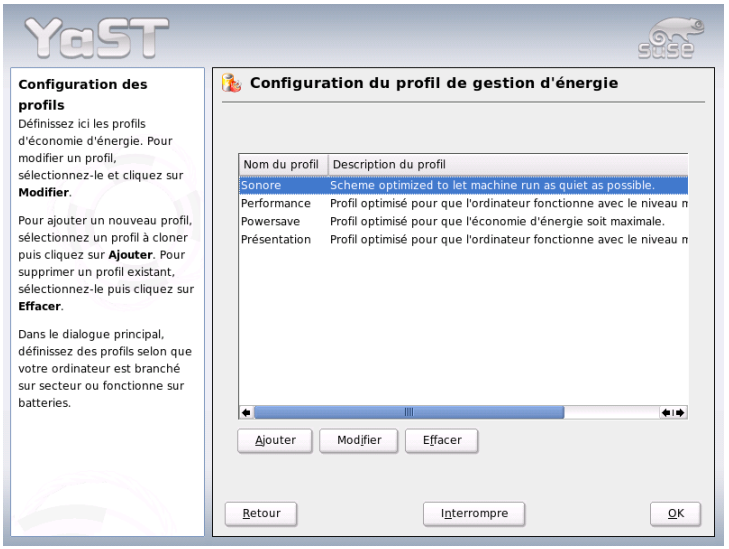


FIG. *16.2:* *Gestion d'énergie de YaST : Aperçu des profils disponibles*

Commencez par donner au nouveau profil ou profil modifié un nom (significatif) et une description. Définissez d'abord si et comment les performances du processeur doivent être réglées pour ce profil. Définissez si et à quel point le 'Cadrage de la fréquence' et le 'Throttling' doivent être utilisés. Dans le dialogue suivant, définissez les 'Règles du mode attente' qui doivent être réglées soit sur un mode de performance maximale, soit sur une consommation d'énergie minimale. Les 'Règles sonores' règlent le niveau de bruit du disque dur (ceci n'est malheureusement supporté que par peu de disques durs IDE). Les 'Règles de refroidissement' gèrent la manière dont la machine est refroidie. Malheureusement, ce type de régulation de la température n'est que rarement pris en charge par le BIOS. Veuillez consulter `/usr/share/doc/packages/powersave/README.thermal` pour savoir comment utiliser la ventilation et les méthodes de refroidissement passives.

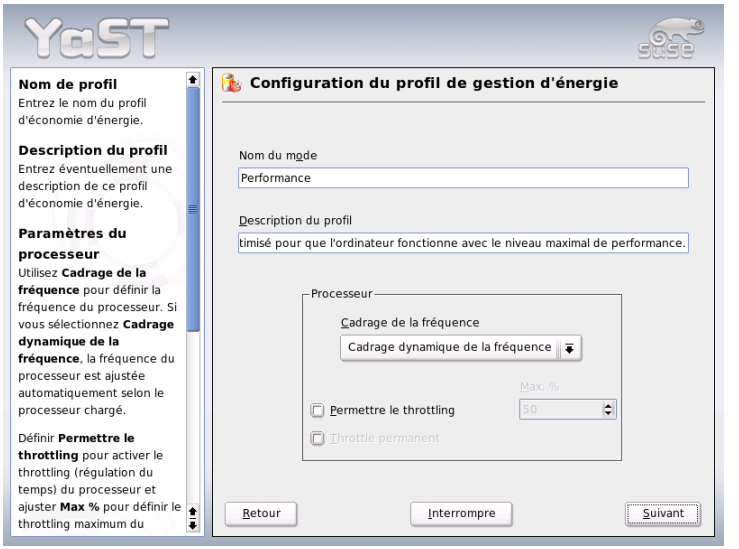


FIG. *16.3:* *Gestion d'énergie de YaST : Création d'un profil*

Cliquez sur 'Suivant' pour accéder à la boite de dialogue de configuration de l'économie d'énergie pour l'écran. Cochez la case 'Activer l'économiseur d'écran' pour diminuer la consommation d'énergie de l'écran lorsque l'ordinateur n'est pas utilisé. Avec 'Activer la gestion d'énergie de l'écran', définissez les délais de mise en attente, de mise en veille ou d'arrêt de l'écran. Une fois que vous avez terminé tous les réglages du profil, quittez cette boîte de dialogue avec 'OK', et retournez à la boîte de dialogue initiale (figure 16.1 page 370). Vous pouvez alors y choisir votre profil personnalisé pour un des deux modes de fonctionnement. Quittez cette boîte de dialogue avec 'OK', votre configuration est alors active.

Depuis la fenêtre de démarrage (voir figure 16.1 page 370), vous pouvez choisir un profil pour chaque mode de fonctionnement ainsi qu'une configuration globale de la gestion de l'énergie. Pour ce faire, cliquez sur 'Avertissements Batterie', 'Paramètres ACPI' ou 'Autoriser la mise en veille'. Pour accéder à la boite de dialogue de l'état de charge de la batterie, cliquez sur 'Avertissements Batterie' (16.4 page suivante).

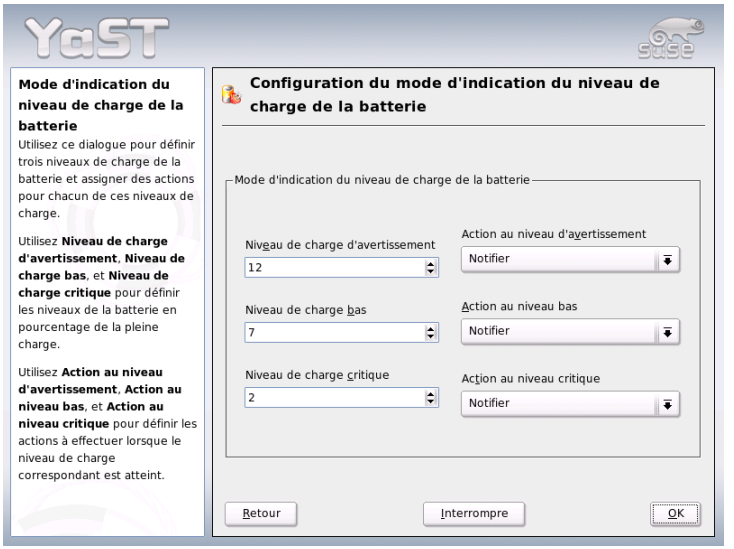


FIG. *16.4:* *Gestion de l'énergie de YaST : état de charge de la batterie*

Le BIOS de votre système informe le système d'exploitation lorsque certains seuils de capacité, configurables, sont atteints. Certaines actions peuvent alors en découler. Dans cette boîte de dialogue, vous pouvez fixer trois seuils en deçà desquels certaines actions doivent être déclenchées. Ce sont 'Mise en garde batterie', 'Niveau de batterie faible' et 'Niveau de batterie critique'. Dans les deux premiers cas, l'utilisateur ne recevra probablement qu'un avertissement, tandis que le passage en dessous du dernier seuil critique provoquera un arrêt de l'ordinateur, car l'énergie restante permet à peine au système de fonctionner correctement pendant un très court laps de temps. Choisissez les niveaux de charge et actions correspondant à vos souhaits et quittez la boîte de dialogue avec 'OK'. Vous revenez alors à la boite de dialogue initiale, qui vous permet d'accéder à la boîte de dialogue suivante, 'Paramètres ACPI', qui traite de la configuration des boutons ACPI (voir figure 16.5 page suivante).

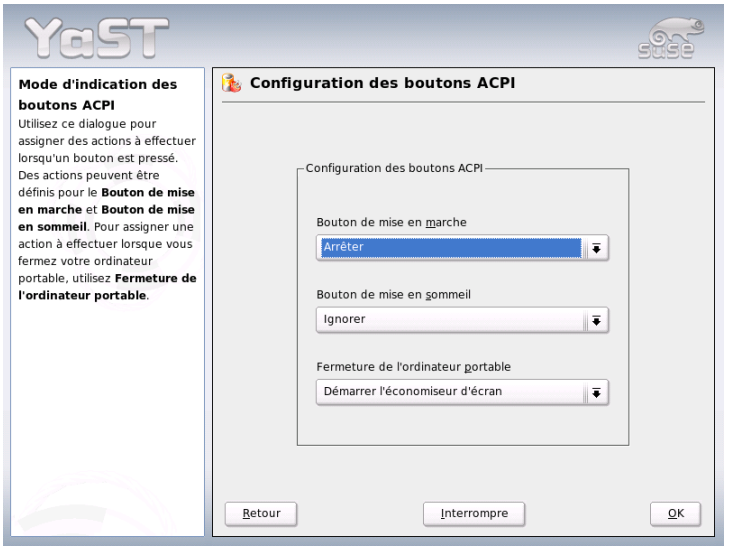


FIG. *16.5:* *Gestion d'énergie de YaST : Réglages de l'ACPI*

Les réglages des boutons ACPI (*ACPI Buttons*) vous permettent de définir la réaction du système à l'utilisation des différents interrupteurs. ACPI identifie ces interrupteurs et événements comme "Boutons" (*Buttons*). Configurez la réponse du système à l'appui sur la touche (Power), sur une touche (Sleep) et au rabattage de l'écran du portable. Vous pouvez conclure la configuration en appuyant sur 'OK' et retourner à la boîte de dialogue initiale (figure 16.1 page 370). En sélectionnant 'Autoriser la mise en veille', vous ouvrez un dialogue dans lequel vous configurez si et comment un utilisateur peut utiliser les fonctionnalités de mise en veille ou en attente de ce système. Cliquez sur 'OK' pour revenir au dialogue principal. Fermez complètement le module en appuyant à nouveau sur 'OK', pour confirmer la configuration de votre gestion d'énergie.

Communications sans fil

Vous disposez de plusieurs possibilités pour communiquer depuis votre système Linux avec d'autres ordinateurs, des téléphones portables ou des périphériques. Si vous souhaitez mettre en réseau des ordinateurs portables, choisissez un WLAN (*Wireless LAN*, réseau local sans fil). Bluetooth permet de connecter entre eux des composants système séparés (souris, clavier), des périphériques, des téléphones portables, des assistants personnels et des ordinateurs isolés. IrDA est principalement utilisé pour les communications avec des assistants personnels et des téléphones portables. Ce chapitre vous présente ces trois méthodes ainsi que leur configuration.

17.1 Réseau local sans fil (WLAN)

Dans le domaine des périphériques mobiles, il n'est plus pensable de se passer des réseaux locaux sans fil (Wireless LAN). Il n'existe pratiquement plus d'ordinateurs portables qui soient encore livrés sans carte WLAN. Le standard de transmission des cartes WLAN a été défini par l'organisation IEEE. Il s'agit du standard 802.11 qui prévoit des vitesses de transmission allant jusqu'à 2 MBit/s. Pour augmenter encore les taux de données, il a été fait depuis plusieurs ajouts. Ceux-ci définissent, entre autres, le type de modulation, le taux de transmission et, naturellement, les vitesses de transmission :

TAB. *17.1:* *Aperçu de différents standards pour WLAN*

Nom	Bande [GHz]	Taux de transfert max. [MBit/s]	Remarque
802.11	2,4	2	obsolète, il n'existe pratiquement plus de matériels d'extrémité
802.11b	2,4	11	très répandu
802.11a	5	54	peu répandu en Allemagne
802.11g	2,4	54	rétrocompatible avec 11b

En outre, il existe aussi des standards propriétaires tels que, par exemple, la variante 802.11b de Texas Instruments (appelé parfois 802.11b+) avec un taux de transfert maximal de 22 MBit/s. Les cartes qui utilisent ce standard sont peu répandues.

17.1.1 Matériel

Les cartes 802.11 ne sont pas prises en charge par SUSE LINUX, par contre, les cartes 802.11a, b et/ou g sont pour la plupart prises en charge. Les cartes actuelles ont très souvent le standard 802.11g mais il existe encore des cartes 802.11b. En principe, les cartes avec les puces suivantes sont prises en charge :

- Lucent/Agere Hermes
- Intel PRO/Wireless 2100
- Intersil Prism2/2.5/3

- Intersil PrismGT
- Atheros 5210, 5211, 5212
- Atmel at76c502, at76c503, at76c504, at76c506
- Texas Instruments ACX100

Quelques cartes plus anciennes qui ne sont maintenant plus en vente mais que l'on peut encore rencontrer à quelques rares occasions sont également prises en charge.

Vous trouverez une liste contenant beaucoup de cartes WLAN et les puces utilisées sur le site de *AbsoluteValue Systems* : `http://www.linux-wlan.org/docs/wlan_adapters.html.gz`

Consultez l'URL suivant pour avoir un aperçu des différentes puces WLAN : `http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz`

Certaines cartes nécessitent un micrologiciel (firmware) image qui doit être chargé dans la carte lors de l'initialisation du pilote. Ceci est le cas pour Intel PRO/Wireless 2100 (Centrino), Intersil PrismGT, Atmel et ACX100. Vous pouvez l'installer à l'aide de la mise en jour en ligne de YaST. Vous trouverez plus d'informations à ce sujet dans le système installé sous `/usr/share/doc/packages/wireless-tools/README.firmware`.

17.1.2 Fonctionnement

Mode d'exploitation

En terme de réseaux sans fil on distingue essentiellement les réseaux gérés et les réseaux ad hoc. Les réseaux gérés comporte un élément d'administration, le point d'accès. Dans ce mode (appelé également mode infrastructure), toutes les connexions des postes de travail WLAN se trouvant dans le réseau fonctionnent à travers le point d'accès ; celui-ci peut également servir comme interface de connexion vers un Ethernet. Les réseaux ad hoc ne comportent pas de point d'accès, les postes de travail communiquent directement les uns avec les autres. La portée et le nombre de postes de travail étant très limités dans les réseaux ad hoc, il est généralement préférable d'utiliser un point d'accès. Il est même possible d'utiliser une carte WLAN comme point d'accès car la plupart supporte cette fonctionnalité.

Étant donné qu'un réseau sans fil est beaucoup plus vulnérable qu'un réseau câblé, des méthodes d'authentification et de chiffrement sont prévues dans les différents standards. Dans la première version du standard IEEE 802.11, ces méthodes sont décrites sous le terme WEP. Cependant, comme il s'est avéré que WEP n'était pas sûr (voir section *Sécurité* page 383), l'industrie WLAN (unie sous le nom *Wi-Fi Alliance*) a défini son propre complément du standard nommé WPA qui devait éliminer les points faibles de WEP. Le standard 802.11i plus récent de IEEE (parfois également nommé WPA2, WPA était en fait inspiré d'une ébauche de 802.11i) comporte le dispositif de sécurité WPA ainsi que quelques méthodes d'authentification et de chiffrement supplémentaires.

Authentification

Dans les réseaux gérés, différents mécanismes d'authentification sont utilisés pour s'assurer que seuls les postes de travail autorisés puissent se connecter :

Open Un système est dit ouvert lorsqu'il n'est procédé à aucune authentification. Chaque poste de travail peut entrer dans le réseau. Cependant, une methode de chiffrement conforme à WEP (voir *Chiffrement* page suivante) peut être utilisée.

Clé partagée (selon IEEE 802.11) Ici, la clé WEP est utilisée pour l'authentification. Cependant, cela ne devrait pas être fait car cela rend la clé WEP plus vulnérable. Il suffit à un intrus potentiel d'"épier" suffisamment longtemps la communication entre le poste de travail et le point d'accès ; les deux échangent les mêmes informations lors du processus d'authentification, une fois chiffrée et une fois en clair ; avec les outils appropriés, on peut alors reconstruire la cle utilisée. Étant donné que, dans ce système, la clé WEP est utilisée aussi bien pour l'authentification que pour le chiffrement, la sécurité du réseau n'est pas améliorée. Un poste de travail qui est en possession de la clé WEP correcte peut à la fois s'authentifier et chiffrer et déchiffrer. Un poste de travail qui n'est pas en possession de la clé WEP correcte échouera, au plus tard, lorsqu'il s'agira de déchiffrer les paquets reçus. Il ne peut donc pas communiquer, qu'il puisse s'authentifier ou non.

WPA-PSK (selon IEEE 802.1x) WPA-PSK (PSK pour *Pre Shared Key*, clé prépartagée) fonctionne de la même façon que dans le cas de la clé partagée. Tous les postes de travail participants ainsi que le point d'accès nécessitent la même clé. Celle-ci a une longueur de 256 bits et est normalement entrée comme une phrase d'authentification. Ce système ne nécessite pas une gestion complexe des clés comme c'est le cas pour WPA-EAP et est plutôt conçu pour une utilisation privée. WPA-PSK est donc appelé quelquefois aussi WPA "Home".

WPA-EAP (selon IEEE 802.1x) En fait, WPA-EAP n'est pas un système d'authentification mais seulement un protocole de transport des informations nécessaires à l'authentification. Il est utilisé au sein des entreprises pour la sécurisation des réseaux sans fil. Dans les réseaux privés, il est pratiquement inutilisé. WPA-EAP est donc appelé quelquefois aussi WPA "Enterprise".

Chiffrement

Afin de s'assurer qu'aucun tiers non autorisé puisse lire les paquets de données échangés dans un réseau sans fil ou même accéder au réseau, il existe des méthodes de chiffrement :

WEP (défini dans IEEE 802.11) Ce standard utilise l'algorithme de chiffrement RC4, avec une clé de 40 bits à l'origine puis avec une clé de 104 bits aussi. Souvent, on parle de longueurs de 64 ou 128 bits selon que l'on tient compte des 24 bits du vecteur d'initialisation. Ce standard a des points faibles. Il existe des méthodes d'attaque des clés générées par ce système qui fonctionnent. Cependant, il est préférable d'utiliser WEP qu'un réseau sans chiffrement.

TKIP (défini dans WPA/IEEE 802.11i)
Ce protocole de gestion des clés défini dans le standard WPA utilise le même algorithme de chiffrement que WEP en palliant à ses faiblesses. Étant donné que, pour chaque paquet de données, une nouvelle clé est générée, les attaques de cette clé n'ont pratiquement aucune chance de réussir. TKIP est utilisé avec WPA-PSK.

CCMP (défini dans IEEE 802.11i) Défini dans IEEE 802.11i, CCMP décrit la gestion des clés qui sont utilisées normalement avec WPA-EAP mais peuvent également être utilisées avec WPA-PSK. Le chiffrement est fait ici selon AES et est plus fiable que le chiffrement RC4 du standard WEP.

17.1.3 Configuration avec YaST

Pour la configuration de votre carte réseau sans fil, démarrez le module de YaST 'Cartes réseau'. Dans le dialogue 'Configuration des adresses réseau', sélectionnez le type de périphérique 'sans fil' et cliquez sur 'Suivant'.

Dans le dialogue 'Configuration de la carte réseau sans fil' (voir figure 17.1 page suivante), procédez à la configuration de base pour l'exploitation WLAN :

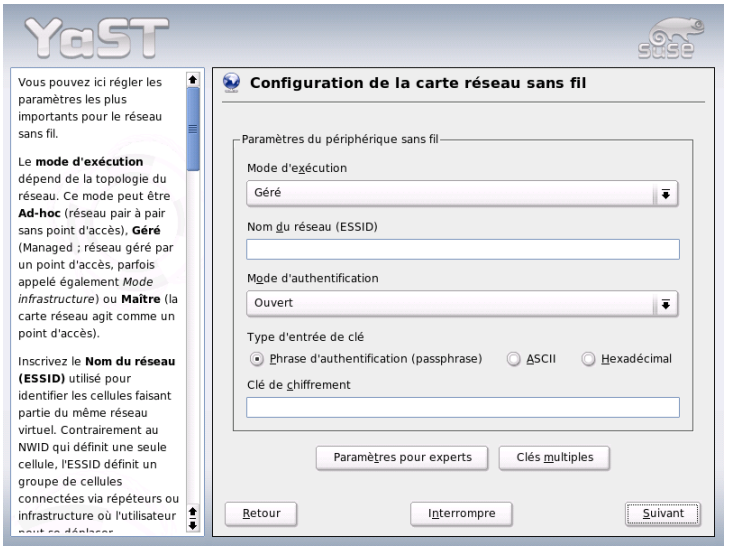


FIG. *17.1:* *Configuration YaST de la carte réseau sans fil*

Nom de réseau (ESSID) Tous les postes de travail d'un réseau sans fil nécessitent le même ESSID afin de pouvoir communiquer. Si rien n'a été précisé, la carte recherche automatiquement un point d'accès qui n'est peut-être pas identique à celui que vous souhaitiez utiliser.

Mode d'exploitation Il existe trois diffétents modes selon lesquels votre poste de travail peut être intégré dans un WLAN. Le mode approprié à votre cas dépend du type de réseau dans lequel vous désirez communiquer : 'ad hoc' (réseau pair à pair pur sans point d'accès), 'géré' (le réseau est géré depuis un point d'accèst) et 'maître' (votre carte réseau doit agir comme point d'accès).

Authentification Choisissez une méthode d'authentification appropriée à votre réseau. Vous disposez de : 'Ouvert', 'Clé partagée WEP' et 'WPA-PSK'. Si vous choisissez 'WPA-PSK', vous devrez définir un nom de réseau. En cliquant sur 'Suivant', vous entrez dans un dialogue permettant la configuration détaillée de la méthode de chiffrement souhaitée.

Experts Avec ce bouton, vous ouvrez un dialogue pour la configuration détaillée de votre accès WLAN. Vous trouverez plus bas une description détaillée de ce dialogue.

Une fois que vous avez terminé la configuration de base, votre poste de travail prête pour l'utilisation dans un WLAN.

Remarque

Sécurité dans un réseau sans fil

Veillez à utiliser une des méthodes d'authentification et de chiffrement prises en charge afin de sécuriser votre réseau. Les connexions WLAN non chiffrées permettent à des tiers d'accéder sans encombres à toutes les données du réseau. Même une méthode de chiffrement faible (WEP) est préférable à rien du tout. En cas de doute, veuillez lire les sections *Chiffrement* page 379 et *Sécurité* page 383 pour plus d'informations relatives à la *Sécurité dans un WLAN*.

Remarque

Selon la méthode d'authentification choisie, YaST vous propose, dans un autre dialogue, de procéder à des réglages fins de la méthode en question. Si vous avez choisi 'Ouvert', il n'y a rien d'autre à configurer, étant donné que ce choix suppose une exploitation non chiffrée sans authentification.

Clés WEP Définissez la longueur de la clé. Vous avez le choix entre '128 bits' et '64 bits'. La configuration par défaut est '128 bit'. La liste sous le dialogue peut comporter jusqu'à quatre clés différentes que votre poste de travail peut employer pour le chiffrement. Avec 'Défini par défaut', définissez une de ces clés comme la clé par défaut. Si vous ne le faites pas, YaST considérera la première clé comme étant la clé par défaut. Si vous effacez la clé par défaut, vous devrez sélectionner manuellement une des clés restantes comme par clé par défaut. Utilisez 'Modifier' pour changer les entrées de la liste ou ajouter de nouvelles clés. Un menu contextuel vous permet de choisir parmi différents types d'entrée ('Phrase d'authentification', 'ASCII' ou 'Hexadécimal'). Si vous choisissez le type d'entrée 'Phrase d'authentification', saisissez un mot ou une chaîne de caractères à partir de quoi une clé de la longueur définie précédemment sera générée. Avec 'ASCII', vous devrez entrer cinq caractères pour une longueur de clé de 64 bits et treize caractères pour une longueur de clé de 128 bits. Si vous avez choisi le type d'entrée 'Hexadécimal', entrez dix caractères hexadécimaux pour une longueur de clé de 64 bits et 26 caractères hexadécimaux pour une longueur de clé de 128 bits.

WPA-PSK Pour entrer une clé pour WPA-PSK, choisissez le type d'entrée 'Phrase d'authentification' ou 'Hexadécimal'. Dans le mode 'Phrase d'authentification', l'entrée doit comprendre entre huit et 63 caractères ; dans le mode 'Hexadécimal', l'entrée doit comprendre 64 caractères.

Avec 'Experts', vous passez du dialogue de configuration de base de l'accès WLAN au dialogue de configuration pour experts. Vous disposez des options suivantes :

Kanal La spécification d'un canal particulier que votre poste de travail WLAN doit utiliser n'est nécessaire que dans les modes 'ad hoc' ou 'maître'. Dans le mode 'géré', la carte recherche automatiquement les points d'accès dans les canaux disponibles. Dans le mode 'ad hoc', vous pouvez sélectionner l'un des douze canaux offerts pour que votre poste de travail communique avec les autres postes de travail. Dans le mode 'maître', définissez sur quel canal votre carte doit offrir le service d'un point d'accès. La configuration par défaut de cette option est 'auto'.

Débit binaire Selon les performances de votre réseau, il est utile de prédéfinir un débit binaire avec lequel les données doivent être transmises d'un point à un autre. Dans la configuration par défaut 'auto', votre système utilise la vitesse de transmission la plus rapide possible. Veuillez noter que la configuration du débit binaire n'est pas pris en charge par toutes les cartes WLAN.

Point d'accès Dans un environnement avec plusieurs points d'accès, vous pouvez en présélectionner un ici en entrant son adresse MAC.

Utiliser la gestion d'énergie Si vous êtes en déplacement, il est conseillé d'augmenter la durée d'utilisation des batteries grâce à des techniques d'économie d'énergie. Pour en savoir plus sur la gestion d'énergie sous Linux, veuillez lire le chapitre *Gestion de l'énergie* page 347.

17.1.4 Programmes d'aide utiles

hostap (paquetage `hostap`) est utilisé pour exploiter une carte WLAN comme un point d'accès. Vous trouverez plus d'informations relatives à ce paquetage sur le site web du projet (`http://hostap.epitest.fi/`).

kismet (paquetage `kismet`) est un outil de diagnostic du réseau avec lequel vous pouvez surveiller le transfert de paquets WLAN ou même l'épier et ainsi déceler des tentatives d'intrusion dans votre réseau. Vous trouverez plus d'informations à ce sujet sous `http://www.kismetwireless.net/` ou dans les pages de manuel correspondantes.

17.1.5 Trucs et astuces pour la configuration d'un WLAN

Stabilité et vitesse

La performance et la fiabilité d'un réseau sans fil dépendent tout d'abord de la netteté du signal que se transmettent les posts de travail qui appartiennent au réseau. Bien entendu, les obstacles, tels que des murs, affaiblissent considérablement le signal. Plus le signal est faible, plus la vitesse de transfert diminue. Vous pouvez établir la force du signal pendant le fonctionnement avec le programme iwconfig à la ligne de commande (champ 'Link Quality') ou kwifimanager sous KDE. Si vous avez des problèmes avec la qualité du signal, essayez de placer autrement les appareils ou de changer l'angle de l'antenne de votre point d'accès. Pour certaines cartes WLAN PCMCIA, il existe des antennes supplémentaires qui améliorent considérablement la réception. La vitesse donnée par le fabricant (par exemple 54 MBit/s) est toujours une valeur nominale. Il ne s'agit que du maximum théorique. En pratique, la vitesse de transfert atteint au mieux la moitié de cette valeur.

Sécurité

Lorsque vous souhaitez configurer un réseau sans fil, pensez que, sans mesures de sécurité particulières, votre réseau est facilement accessible à tous ceux se trouvant à sa portée. Activez donc, dans tous les cas, une méthode de chiffrement. Chaque périphérique d'extrémité, qu'il s'agisse d'une carte WLAN ou d'un point d'accès, prend en charge le chiffrement selon le protocole WEP. Ceci n'est pas absolument sûr mais cela représente tout de même une certaine protection contre les attaques potentielles. Pour une utilisation privée, WEP est généralement suffisant. Il serait encore préférable d'utiliser WPA-PSK. Cependant, cette méthode n'est pas implémentée dans les points d'accès ou les routeurs avec fonctionnalité WLAN plus anciens. Pour certains, il est possible d'implémenter WPA en procédant à une mise à jour avec un micrologiciel (firmware), mais pas pour tous. Même du côté de Linux, la prise en charge de WPA n'est pas assurée sur tous les matériels. À l'heure où nous rédigeons ce chapitre, WPA ne fonctionne qu'avec les cartes qui utilisents une puce Atheros ou Prism2/2.5/3 ; et pour cette dernière, uniquement lorsque le pilote hostap est utilisé (voir section *Problèmes avec cartes Prism2* page suivante). Cependant, dans les cas où il n'est pas possible d'utiliser WPA, il est toujours préférable d'utiliser WEP qu'aucune méthode de chiffrement. Au sein d'une entreprise où les exigences en matière de sécurité sont plus importantes, un réseau sans fil ne devrait jamais être utilisé sans WPA.

17.1.6 Problèmes possibles et solutions

Si votre carte WLAN ne fonctionne pas, assurez-vous que vous avez téléchargé le micrologiciel (firmware) correspondant si nécessaire. Consultez, à ce sujet, la section *Matériel* page 376 au début de ce chapitre. Vous trouverez quelques conseils pour les problèmes connus.

Plusieurs périphériques réseau

Les portables actuels sont normalement équipés d'une carte réseau et d'une carte WLAN. Si vous avez configuré ces deux périphériques avec DHCP (assignation automatique d'adresse), vous pourrez éventuellement avoir des problèmes avec la résolution de noms et la passerelle par défaut. Vous pourrez alors faire un ping sur le routeur mais vous ne pourrez pas surfer sur Internet. Il existe une article SDB à ce sujet, recherchez le mot-cle "DHCP" sur `http://portal.suse.de/sdb/en/index.html`.

Problèmes avec cartes Prism2

Pour les périphérique équipés de puces Prism2, il existe plusieurs pilotes qui fonctionnent plus ou moins bien avec les différentes cartes. Avec ces cartes, WPA n'est possible qu'avec le pilote hostap. Si vous avez des problèmes avec une telle carte, qu'elle ne fonctionne pas du tout ou que de façon sporadique, veuillez lire `/usr/share/doc/packages/wireless-tools/README.prism2`.

WPA

La prise en charge de WPA est offerte pour la première fois par SUSE LINUX et n'est pas encore arrivée complètement à maturité sous Linux en général. À l'aide de YaST, vous ne pouvez configurer que WPA-PSK. Avec de nombreuses cartes, WPA ne fonctionne pas du tout. Certains nécessitent une mise à jour du micrologiciel (firmware) pour que WPA puisse fonctionner. Si vous souhaitez utiliser WPA, veuillez lire `/usr/share/doc/packages/wireless-tools/README.wpa`.

17.1.7 Informations complémentaires

Vous trouverez une mine d'informations utiles au sujet des réseaux sans fil sur les pages web de Jean Tourrilhes qui a développé les *Wireless Tools* pour Linux : `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html`

17.2 Bluetooth

Bluetooth est une technologie radio qui permet de connecter plusieurs appareils entre eux : téléphones mobiles, PDA, périphériques ou composants système tels que clavier ou souris, ordinateurs portables. Le nom provient du roi danois Harold Blatand ("Harold Bluetooth" en anglais) qui a unifié au dixième siècle différentes factions se combattant entre elles en Scandinavie. Le logo de Bluetooth est basé sur les runes représentant les lettres "H" (qui ressemble à une étoile) et "B".

Bluetooth se distingue de l'IrDA en plusieurs points essentiels : d'une part, les différents appareils n'ont pas besoin de se "voir" directement pour échanger des données, d'autre part il est possible de mettre au point des réseaux entiers en rassemblant plusieurs appareils. Cette technologie ne permet toutefois d'atteindre que des débits de 720 Kbit/s maximum (dans la version 1.1 actuelle). En théorie, on peut, avec Bluetooth, envoyer des données par radio à travers les murs. Dans la pratique, cela dépend fortement des murs en question et du type des appareils. Enfin, la portée maximale d'envoi est répartie en trois classes qui varient de 10 à 100 mètres.

17.2.1 Principes de base

Logiciels

Pour pouvoir utiliser Bluetooth, vous avez besoin d'un adaptateur Bluetooth (intégré à l'appareil ou sous la forme d'une clé électronique externe), de pilotes et de ce que l'on appelle une "pile de protocoles Bluetooth".

Le noyau Linux contient déjà les pilotes de base permettant d'utiliser Bluetooth. On utilise comme pile de protocoles le système Bluez. Afin que les différentes applications puissent fonctionner avec Bluetooth, vous devez, en outre, installer les paquetages de base suivants : `bluez-libs`, `bluez-utils` qui préparent quelques services et programmes de service nécessaires. Pour quelques adaptateurs (Broadcom, AVM BlueFritz!), il est par ailleurs nécessaire d'installer `bluez-firmware`. Les paquetages précédemment connus sous les noms de `bluez-pan` et `bluez-sdp` sont intégrés aux paquetages de base. Le paquetage `bluez-cups` permet l'impression par une connexion Bluetooth.

Interaction générale

Un système Bluetooth est constitué de quatre couches imbriquées de manière à fournir en bout de chaîne les fonctions souhaitées :

Matériel L'adaptateur et le pilote approprié qui assure la prise en charge par le noyau Linux.

Fichiers de configuration Le paramétrage du système Bluetooth

Démons Services qui, par l'intermédiaire des commandes du fichier de configuration, mettent à disposition les fonctionnalités.

Applications Programmes qui permettent à l'utilisateur d'utiliser et de piloter les fonctionnalités mises à disposition par les démons.

À l'insertion de l'adaptateur Bluetooth, le pilote correspondant est chargé par le système Hotplug. Une fois le pilote chargé, les fichiers de configuration permettent de vérifier si Bluetooth doit être démarré. Si tel est le cas, le système détermine également quels services doivent être démarrés. Les démons correspondants sont alors lancés en conséquence. Pour des raisons de sécurité, le système Bluetooth dans une configuration standard est désactivé.

Profils

Dans Bluetooth, les services sont définis au moyen de ce que l'on appelle des profils. On définit ainsi dans le standard Bluetooth des profils pour le transfert de données ("File Transfer"), l'impression ("Basic Printing") et les connexions réseau ("Personal Area Network").

Pour qu'un appareil puisse utiliser le service d'un autre, ces deux appareils doivent pouvoir comprendre le même profil — information qui, souvent, n'est malheureusement disponible ni sur l'emballage ni dans le manuel des appareils concernés. Cela est d'autant plus compliqué que tous les fabricants ne respectent pas scrupuleusement les définitions des différents profils. En règle générale toutefois, la compréhension entre les appareils fonctionne plutôt bien.

17.2.2 Configuration

Configuration Bluetooth avec YaST

Avec le module Bluetooth de YaST (voir illustration 17.2 page ci-contre), vous pouvez configurer la prise en charge de Bluetooth sur votre système. Dès que Hotplug reconnaît un adaptateur Bluetooth connecté à votre système, Bluetooth est automatiquement démarré suivant les indications données ici.

La première étape de la configuration vous permet de définir si des services Bluetooth doivent être démarrés sur votre système. Si un code d'identification personnel est nécessaire pour établir une connexion avec les différents appareils souhaités, vous renseignez ce code avec la suite de chiffres correspondante. Vous arrivez ensuite, en cliquant sur le bouton 'Configuration avancée du démon', sur la

FIG. *17.2:* *Configuration Bluetooth dans YaST*

fenêtre de choix et de configuration détaillée des services proposés (également connu dans Bluetooth sous le nom de *Profils*). Tous les services à votre disposition sont donnés dans une liste, et les boutons 'Activer' et 'Désactiver' permettent d'effectuer sur chaque service l'opération correspondante. Le bouton 'Modifier' ouvre une nouvelle fenêtre dans laquelle vous pouvez fournir des arguments supplémentaires au service (démon) sélectionné. N'effectuez des modifications que dans les services que vous connaissez suffisamment bien. Lorsque la configuration du démon est terminée, vous quittez la boite de dialogue en cliquant sur 'Ok'. Depuis la fenêtre principale, vous arrivez sur une fenêtre de configuration de la sécurité en cliquant sur 'Options Sécurité', laquelle vous permet de configurer l'encryption, la méthode d'authentification et de balayage. Si vous fermez la fenêtre de configuration de la sécurité, vous revenez sur la boite de dialogue principale. Si vous quittez celle-ci en cliquant sur le bouton 'Terminer', votre système Bluetooth est prêt à être utilisé.

Si vous souhaitez utiliser Bluetooth pour construire un réseau, vous activez 'PAND'dans la boite de dialogue 'Configuration Avancée du Démon' puis, en choisissant 'Modifier', ajustez le mode du démon. Pour que la connexion réseau Bluetooth fonctionne, il est nécessaires qu'une instance de pand fonctionne en mode 'Ecoute' et que le récepteur soit en mode 'Recherche'. Par défaut, le mode 'Ecoute' est pré-configuré. Ajustez le comportement de votre instance locale de pand. De plus, vous pouvez configurer au moyen du module 'Carte réseau' de YaST l'interface `bnepX` (`X` représente le numéro du périphérique dans le système).

Configuration manuelle de Bluetooth

Les fichiers de configuration pour les composants isolés du système Bluez se trouvent dans le répertoire `/etc/bluetooth`. La seule exception à cette règle est le fichier `/etc/sysconfig/bluetooth` utilisé pour le démarrage des composants et traité par le module de YaST.

Vous ne pouvez modifier les fichiers de configuration présentés ci-après qu'en tant qu'utilisateur `root`. Il n'existe pour l'instant malheureusement pas encore d'interface utilisateur graphique pour régler les paramètres correspondants. Vous devez donc modifier les fichiers dans un éditeur de texte. Toutefois, en règle générale, les réglages d'origine devraient suffire.

Une première protection contre les connexions indésirables consiste à utiliser une protection par un numéro d'identification personnel (PIN). Les téléphones mobiles demandent généralement à l'utilisateur de saisir son numéro d'identification personnel lors du premier contact (ou de la création d'un contact pour l'appareil sur le téléphone). Pour que deux appareils puissent échanger des informations, ils doivent tous les deux s'identifier avec le même numéro d'identification personnel. Ce dernier se trouve dans le fichier `/etc/bluetooth/pin` sur l'ordinateur. Il n'existe actuellement sous Linux qu'un seul numéro d'identification personnel, quel que soit le nombre d'appareils Bluetooth installés. La communication avec plusieurs appareils ayant des numéros d'identification personnels différents n'est malheureusement pas prise en charge actuellement. Vous devez donc soit définir tous les appareils de manière à ce qu'ils aient tous le même numéro d'identification personnel soit complètement désactiver l'authentification par numéro d'identification personnel.

Remarque

Sécurité des connexions Bluetooth

Malgré le numéro d'identification personnel, il faut garder à l'esprit qu'une connexion entre deux appareils n'est absolument pas garantie contre les écoutes. Prenez garde au fait qu'en mode d'émission, l'authentification et le chiffrement des connexions Bluetooth sont désactivées.

Remarque

Le fichier de configuration `/etc/bluetooth/hcid.conf` permet de modifier différents paramètres tels que les noms des périphériques et le mode de sécurité. Normalement, les réglages par défaut doivent suffire. Le fichier contient des commentaires qui décrivent les options des différents paramètres. Nous évoquons ici rapidement deux réglages particuliers.

Dans le fichier fourni se trouvent deux sections désignées par `options` et `device`. La première contient toutes les informations générales utilisées au démarrage d'hcid, la seconde contient les réglages pour les périphériques Bluetooth locaux individuels. On entend ici par local le fait que le périphérique est connecté physiquement à l'ordinateur. Tous les autres périphériques auxquels on ne peut accéder que par une connexion sans fil seront décrits comme des périphériques distants.

L'un des réglages les plus importants de la partie `options` est `security auto;`. Il permet d'activer la nécessité d'un numéro d'identification personnel. `auto`, en cas de problème, permet de passer à `ne pas utiliser de numéro d'identification personnel`. Pour un niveau de sécurité plus élevé, il est conseillé de régler cet élément sur `user`, de façon à ce que l'utilisateur doive fournir un numéro d'identification personnel à chaque connexion.

La section `device` est intéressante car elle permet de définir le nom sous lequel l'ordinateur apparaît face à ses correspondants. Sont également définis ici les classes des appareils (`Desktop` - PC de bureau, `Laptop` - portable, `Server` - serveur), ainsi que l'authentification et le chiffrement.

17.2.3 Composants système et assistants utiles

Ce n'est qu'après avoir combiné plusieurs services que Bluetooth peut véritablement être utilisé. Vous avez besoin d'au moins deux démons à exécuter en tâche de fond : d'une part, hcid (*Host Controller Interface*). Celui-ci sert d'interface avec l'appareil Bluetooth et le pilote. D'autre part, vous avez besoin de sdpd (*Service Discovery Protocol*). sdpd permet à un appareil de découvrir quels services l'ordinateur propose. Aussi bien hcid que sdpd peuvent — si cela ne se produit pas déjà automatiquement lors du démarrage du système — être mis en service avec la commande `rcbluetooth start`. Cependant, seul l'utilisateur a les droits pour le faire.

Dans la suite nous traiterons brièvement des outils en mode ligne de commande les plus importants qui peuvent être utilisés pour travailler avec Bluetooth. Même si Bluetooth peut être utilisé par le biais de différents composants graphiques, nous vous recommandons de jeter un œil à ces programmes.

Certaines commandes ne peuvent être lancées qu'en tant qu'utilisateur . C'est le cas de `l2ping <adresse-périphérique>` qui permet de tester la connexion avec un périphérique distant.

hcitool

hcitool permet de déterminer facilement si des périphériques locaux et/ou distants ont été détectés. La commande `hcitool dev` permet d'afficher un périphérique particulier. Le résultat génère, pour chaque périphérique local trouvé, une ligne de la forme suivante : `<nom-interface> <adresse-périphérique>`.

Utilisez la commande `hcitool inq` pour rechercher des périphériques distants. Vous obtenez ici trois valeurs par périphérique trouvé : l'adresse du périphérique, une différence d'heure et la classe du périphérique. La plus importante est l'adresse du périphérique. Elle est utilisée par d'autres commandes pour identifier le périphérique cible. La différence d'heure n'est normalement intéressante que d'un point de vue technique. Dans la classe, le type de périphérique et le type de service sont codés en valeur hexadécimale.

Vous pouvez utiliser la commande `hcitool nom <adresse-appareil>` pour obtenir le nom d'un appareil distant. S'il s'agit alors d'un ordinateur distant, la classe et le nom de l'appareil obtenus correspondraient alors aux informations contenues dans le fichier `/etc/bluetooth/hcid.conf` de celui-ci. Les adresses d'appareils locaux génèrent une erreur en sortie.

hciconfig

`/usr/sbin/hciconfig` fournit des informations supplémentaires pour les périphériques locaux. L'appel de `hciconfig` sans argument fournit des informations sur le périphérique comme le nom du périphérique (`hciX`), l'adresse physique du périphérique (12 chiffres sous la forme `00:12:34:56:78`) ainsi que des informations sur toutes les données transmises.

`hciconfig hci0 name` renvoie le nom qui est renvoyé par votre ordinateur à toute demande d'appareils distants.`hciconfig` ne sert cependant pas qu'à répondre aux requêtes des appareils vers l'appareil local, mais permet également d'effectuer des modifications sur ce nom. La commande `hciconfig hci0 name TEST` permet de donner à l'appareil le nom `TEST`.

sdptool

Utilisez le programme sdptool pour savoir quel service est mis à disposition par un appareil donné. `sdptool browse <adresse_appareil>` fournit une liste de tous les services d'un appareil, tandis que `sdptool search <abréviation_service>` permet de rechercher un service donné. Cet appel interroge tous les appareils qui peuvent être joints pour leur demander s'ils proposent le service recherché. S'il est effectivement proposé par un appareil, le programme indique le nom du service (complet) proposé par l'appareil et une brève description. Pour obtenir une liste de toutes les abréviations de services possibles, exécutez la commande `sdptool` sans paramètre particulier.

17.2.4 Applications graphiques

Konqueror vous permet d'afficher la liste des périphériques Bluetooth locaux et distants grâce à l'URL `sdp:/`. Un double clic sur le périphérique vous affiche une vue d'ensemble des services proposés par ce périphérique. Si vous passez la souris sur un des services fournis, vous pouvez voir dans la barre d'état du navigateur le profil utilisé pour ce service. Cliquez sur un service, une fenêtre apparaît alors pour vous demander ce que vous désirez faire : enregistrer, utiliser le service (il faut pour cela qu'un programme utilisateur soit lancé) ou annuler votre action. Vous pouvez aussi cocher une case pour que cette fenêtre ne s'affiche plus mais exécute toujours une action que vous aurez choisie. Attention : pour certains services il n'existe pas (encore) de prise en charge, et pour d'autres des paquetages doivent éventuellement être installés.

17.2.5 Exemples

Connexion réseau entre deux ordinateurs O1 et O2

Dans le premier exemple, on doit construire une connexion réseau entre deux ordinateurs *O1* und *O2*. Chacun des deux ordinateurs possède une adresse de périphérique Bluetooth, respectivement *baddr1* et *baddr2*, laquelle, comme il a été décrit ci-dessus, peut être définie à l'aide de la commande `hcitool dev` sur chaque ordinateur. Les ordinateurs doivent finalement se voir par leur adresse IP respective soit `192.168.1.3` (*O1*) et`192.168.1.4` (*O2*).

La connexion Bluetooth a lieu grâce à pand (*Personal Area Networking*). Les commandes suivantes doivent être lancées par l'utilisateur . Nous omettons délibérement toute explication de la commande réseau (ip) pour nous concentrer sur les actions propres à Bluetooth :

Sur l'ordinateur *O1*, on démarre pand avec la commande `pand -s`. Sur le deuxième ordinateur *O2*, on peut alors construire une connexion avec la commande `pand -c <baddr1>`. Si vous demandez maintenant, sur l'un ou les deux ordinateurs, une liste des interfaces réseau à disposition, avec la commande `ip link show`, vous devez obtenir une réponse de la forme suivante :

```
bnep0: <BROADCAST,MULTICAST
> mtu 1500 qdisc noop qlen 1000
 link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

(l'adresse de périphérique locale *baddr1* ou *baddr2*doit figurer à la place de `00:12:34:56:89:90`). Il faut à présent associer à cette interface une adresse IP et l'activer.

Utilisez pour ce faire, sur *O1*, les deux commandes

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

ou, de la même manière, sur *O2*

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

O1 peut ainsi être joint par *O2* sous l'adresse IP `192.168.1.3`. Avec `ssh 192.168.1.4` vous pouvez à présent vous connecter à partir d'*O1* (dans la mesure où sshd fonctionne sur *O2* comme c'est le cas par défaut sous SUSE LINUX). L'appel `ssh 192.168.1.4` fonctionne du reste désormais aussi en tant qu'utilisateur "normal".

Transfert de données d'un téléphone mobile vers l'ordinateur

Le deuxième exemple consiste à transférer sur un ordinateur une image prise par un téléphone mobile doté d'un appareil photo (sans coûts supplémentaires liés à l'envoi d'un message multimédia). Notez que chaque téléphone mobile possède une arborescence de menus qui lui est propre mais que le processus est la plupart du temps analogue. Consultez si nécessaire le mode d'emploi de votre téléphone. Vous trouverez ci-après une description du transfert d'une photo d'un téléphone Sony Ericsson vers un ordinateur portable. Il faut, pour ce faire, que le service Obex-Push soit disponible sur l'ordinateur et d'autre part que l'ordinateur autorise l'accès au téléphone mobile. La première étape consiste à rendre disponible le service sur l'ordinateur portable. Utilisez pour cela le démon opd extrait du paquetage `bluez-utils`. Démarrez-le avec :

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

Deux paramètres sont alors importants. `--sdp` déclare le service auprès de sdpd. Le paramètre `--path /tmp` indique au programme où il doit enregistrer les fichiers reçus — dans le cas présent, dans `/tmp`. Vous pouvez indiquer d'autres chemins exactement de la même manière. Il vous suffit de disposer des droits d'écriture dans le répertoire concerné.

À présent, le téléphone mobile doit reconnaître l'ordinateur. Cherchez alors le menu 'Connexions' du téléphone et choisissez l'option 'Bluetooth'. Allez dans 'Se connecter' avant de choisir l'option 'Propre appareil'. Choisissez 'Nouvel appareil' et laissez votre téléphone chercher l'ordinateur portable. Lorsqu'un appareil est trouvé, son nom s'affiche à l'écran. Choisissez l'appareil correspondant à l'ordinateur portable. Une demande de numéro d'identification personnel doit ensuite s'afficher, dans laquelle vous devez saisir le numéro d'identification personnel extrait de `/etc/bluetooth/pin`. Cela permet ainsi au téléphone de reconnaître le portable et donc d'échanger des données avec celui-ci. Quittez à présent ce menu et cherchez le menu des photos. Choisissez une photo que vous souhaitez transférer, puis appuyez sur le bouton 'Plus'. Dans le menu qui s'affiche à présent, 'Envoyer', vous disposez d'un choix de différents modes d'expédition. Choisissez 'Par Bluetooth'. Le portable doit à présent pouvoir être choisi comme appareil cible. Une fois l'ordinateur sélectionné, le transfert a lieu et la photo est placée dans le répertoire indiqué dans l'appel de opd. Vous pourriez procéder de la même manière bien entendu pour transférer un morceau de musique.

17.2.6 Problèmes possibles et solutions correspondantes

En cas de problème de connexion, veuillez vérifier les points de la liste suivante. N'oubliez cependant pas que le problème peut se trouver de part et d'autre de la connexion, et dans le pire des cas des deux côtés. Dans la mesure du possible, vous devez essayer de comprendre le problème en utilisant un appareil Bluetooth supplémentaire afin de pouvoir écarter les problèmes liés au matériel.

L'appareil local apparait-il dans le résultat de la commande `hcitool dev` ?
Vérifiez le résultat de la commande `hcitool dev`. Le périphérique local est-il affiché ? Si ce n'est pas le cas, c'est que soit hcid n'est pas démarré, soit que l'appareil n'est pas reconnu en tant qu'appareil Bluetooth (soit parce que le pilote ne le reconnaît pas, soit parce que l'appareil est défectueux). Utilisez la commande `rcbluetooth restart` pour redémarrer le démon et consultez `/var/log/messages` pour rechercher d'éventuelles erreurs.

Votre adaptateur Bluetooth nécessite-t-il un microprogramme ?
Dans ce cas, veuillez installer `bluez-bluefw` et redémarrer le système Bluetooth avec la commande `rcbluetooth restart`.

La commande `hcitool inq` renvoie-t-elle d'autres appareils ?
Testez cet appel plusieurs fois. Il peut arriver que la connexion ne fonctionne pas totalement, car la bande de fréquence utilisée par Bluetooth est également utilisée par d'autres appareils.

Les numéros d'identification personnels se correspondent-ils ?
Vérifiez que le numéro d'identification personnel sous `/etc/bluetooth/pin` correspond à celui de l'appareil cible utilisé.

L'autre appareil "voit-il" votre ordinateur ?
Essayez de lancer la connexion à partir de l'autre appareil. Vérifiez si cet appareil voit l'ordinateur.

Est-il possible de construire une connexion réseau (voir exemple 1) ?
Si le premier exemple (connexion réseau) ne fonctionne pas, il existe plusieurs causes possibles : tout d'abord, cela peut être dû au fait que l'un des deux ordinateurs ne comprend pas le protocole ssh. Essayez de voir si `ping 192.168.1.3` ou `ping 192.168.1.4` fonctionnent. Dans l'affirmative, vérifiez si sshd fonctionne. Un autre problème peut être que vous possédez déjà des adresses qui génèrent des conflits avec l'adresse `192.168.1.X` citée dans l'exemple. Essayez tout simplement avec d'autres adresses, telles que `10.123.1.2` et `10.123.1.3`.

L'ordinateur portable apparait-il comme appareil cible (exemple 2) ? L'appareil mobile reconnaît-il le service Obex-Push sur l'ordinateur portable ?

Allez dans le menu 'Appareil propre' de l'appareil concerné et affichez la 'Liste des services'. Si Obex-Push n'y figure pas (même après la mise à jour de la liste), le problème vient alors d'opd sur le portable. opd est-il démarré ? Disposez-vous des droits d'écriture dans le répertoire indiqué ?

Le second exemple fonctionne-t'il en sens inverse ?

Si vous avez installé `obexftp`, cela fonctionne aussi avec `obexftp -b <adresseappareil> -B 10 -p <image>` pour quelques autres appareils. Différents modèles des marques Siemens et Sony Ericsson ont été testés et fonctionnent. Veuillez pour cela consulter la documentation du paquetage `/usr/share/doc/packages/obexftp`.

17.2.7 Informations supplémentaires

Informations et instructions utiles :

- GPRS (service général de radio-communication en mode paquet) via Bluetooth (page en anglais) : `http://www.van-schelve.de/edv-wissen/linux/bluetooth_1.htm`
- Connexion avec un assistant numérique personnel PalmOS (page en anglais) : `http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html`

Vous trouverez une bonne vue d'ensemble des différentes procédures à suivre pour utiliser et configurer Bluetooth à l'adresse suivante : `http://www.holtmann.org/linux/bluetooth/`

Howto officiel pour la *pile de protocoles Bluetooth* intégrée au noyau (page en anglais) : `http://bluez.sourceforge.net/howto/index.html`

17.3 Infrared Data Association

IrDA (en anglais, *Infrared Data Association*) est un standard de communication sans fil par infrarouge. De nombreux ordinateurs portables commercialisés actuellement sont équipés d'un émetteur/récepteur compatible irDA qui permet la communication avec d'autres appareils, tels que les imprimantes, les modems, les réseaux locaux ou d'autres ordinateurs portables. Le débit varie de 2 400 bps jusqu'à 4 Mbps.

Il existe deux modes d'exploitation pour IrDA. En mode par défaut SIR, on communique avec le port infrarouge au moyen d'une interface série. Ce mode fonctionne sur presque tous les appareils et est suffisant dans de nombreux cas. Le mode le plus rapide FIR nécessite un pilote spécial pour le composant IrDA. Il n'existe cependant pas de tel pilote pour tous les composants. De plus, il faut régler le mode souhaité lors de la configuration du BIOS de l'ordinateur. C'est également là que vous voyez quelle interface série est utilisée pour le mode SIR.

Vous trouverez des informations au sujet de l'IrDA dans le howto de Werner Heuser sous `http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html` et sur le site Web du projet IrDA Linux : `http://irda.sourceforge.net/`.

17.3.1 Logiciels

Vous trouverez les modules de noyau nécessaires dans le paquetage du noyau. Le paquetage `irda` prépare les utilitaires pour la prise en charge de l'interface infrarouge. Une fois le paquetage installé, vous trouverez la documentation correspondante à l'emplacement `/usr/share/doc/packages/irda/README`.

17.3.2 Configuration

Le service système IrDA n'est pas automatiquement démarré lors de l'amorçage. Utilisez le module IrDA de YaST pour son activation. Seul un paramètre y est modifiable : l'interface série du périphérique infrarouge. Dans la fenêtre de test proposée, il existe deux sorties. La première est celle du programme irdadump qui journalise tous les paquets IrDA émis et reçus. Dans cette sortie, le nom de l'ordinateur et les noms de tous les appareils infrarouges à portée devraient apparaître régulièrement. Vous trouvez un exemple de cette sortie dans la section *Problèmes possibles et solutions* page 398. Tous les appareils avec lesquels il existe une liaison IrDA apparaissent dans la partie inférieure de la fenêtre.

Malheureusement, l'IrDA nécessite beaucoup plus d'énergie (de la batterie) car toutes les deux secondes un paquetage de découverte est envoyé pour la reconnaissance automatique d'autres périphériques. C'est pour cette raison qu'il est conseillé, lorsque vous souhaitez économiser vos batteries, de ne démarrer l'IrDA qu'à la demande. Utilisez la commande `rcirda start` pour activer manuellement l'interface à tout instant ou la désactiver (avec le paramètre `stop`). Lorsque l'interface est activée, les modules du noyau nécessaires sont automatiquement chargés.

Vous pouvez procéder à la configuration manuelle dans le fichier `/etc/sysconfig/irda`. Celui-ci ne contient qu'une variable `IRDA_PORT` qui définit quelle interface utiliser en mode SIR.

17.3.3 Utilisation

Si vous souhaitez imprimer des documents par infrarouge, vous pouvez envoyer vos données via le fichier des appareils `/dev/irlpt0`. Le fichier des appareils `/dev/irlpt0` se comporte comme l'interface connectée par un câble normal `/dev/lp0`, à la différence que les données à imprimer sont transmises sans fil par de la lumière infrarouge. Lors de l'impression, veillez à ce que l'imprimante soit à portée de l'interface infrarouge de l'ordinateur et que la prise en charge de l'infrarouge soit démarrée.

Vous pouvez configurer une imprimante exploitée par l'intermédiaire d'une interface infrarouge comme à votre habitude, à l'aide de YaST. L'imprimante n'est pas reconnue automatiquement, configurez alors 'Autres (pas reconnues)'. Dans le dialogue suivant, vous pouvez sélectionner 'Imprimante via IrDA'. Comme port `irlpt0` est pratiquement toujours correct. Vous trouvez des détails sur l'utilisation des imprimantes sous Linux dans le chapitre *Imprimante (utilisation)* page 291.

Si vous souhaitez utiliser l'interface infrarouge avec d'autres ordinateurs, des téléphones mobiles ou d'autres appareils de ce type, vous pouvez le faire qu moyen du fichier périphérique `/dev/ircomm0`. Ainsi avec le téléphone mobile S25 de Siemens, vous pouvez vous connecter à l'Internet sans fil par de l'infrarouge grâce au programme wvdial. Une synchronisation des données avec un Palm Pilot est également possible, il vous suffit de saisir simplement le nom de périphérique `/dev/ircomm0` dans le programme correspondant.

Vous ne pouvez communiquer qu'avec les appareils qui prennent en charge les protocoles Printer ou IrCOMM. Vous pouvez utiliser des programmes spéciaux comme irobexpalm3 ou irobexreceive pour vous adresser à des appareils qui utilisent le protocole IROBEX (3Com Palm Pilot). Vous trouverez des détails à ce sujet dans *IR-HOWTO* (`http://tldp.org/HOWTO/Infrared-HOWTO/`). La liste des protocoles pris en charge par l'appareil est affichée par `irdadump` après le nom de l'appareil entre crochets. La prise en charge du protocole IrLAN est "en cours de développement".

17.3.4 Problèmes possibles et solutions

Si certains appareils ne réagissent pas au niveau du port infrarouge, vous pouvez, en tant qu'utilisateur `root`, saisir la commande `irdadump` pour vérifier si l'autre appareil est reconnu par l'ordinateur.

Dans le cas d'une imprimante BJC-80 Canon en vue de l'ordinateur, on obtient alors un résultat semblable au suivant et qui se répète régulièrement (voir le résultat 17.1).

Exemple 17.1: *Sortie d'irdadump*

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                        hint=8804 [Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* terre
                        hint=0500 [ PnP Computer ] (21)
```

Si aucun résultat n'est obtenu ou si l'autre appareil ne se signale pas en retour, vérifiez la configuration de l'interface. Utilisez-vous vraiment la bonne interface ? Vous trouverez parfois aussi l'interface infrarouge sous le nom `/dev/ttyS2` ou `/dev/ttyS3` ou un autre quand l'interruption 3 est utilisée. Vous pouvez toutefois configurer ces paramètres pour presque tous les ordinateurs portables dans la configuration du BIOS.

Vous pouvez aussi utiliser une caméra vidéo pour facilement vérifier si la LED infrarouge s'allume – contrairement aux yeux de l'homme, la plupart des caméras vidéos peuvent voir la lumière infrarouge.

Le système Hotplug

Le système de branchement à chaud (Hotplug) sous SUSE LINUX trouve son origine dans le *Linux Hotplug Project*, mais s'en différencie sur certains points. La différence principale est que sous SUSE LINUX on utilise non pas le multiplexeur d'événement `/etc/hotplug.d`, mais directement les scripts Hotplug. De plus, quand c'est possible, les scripts `/sbin/hwup` et `/sbin/hwdown` sont déployés afin d'initialiser ou d'arrêter des périphériques.

Le système Hotplug n'est pas seulement utilisé pour les périphériques pouvant être branchés et débranchés durant le fonctionnement, mais pour tous les périphériques qui ne sont reconnus qu'après l'amorçage du noyau. Ces périphériques, ainsi que leurs interfaces, sont renseignés dans le système de fichiers `sysfs`, qui se trouve dans le répertoire `/sys`. Avant l'amorçage du noyau, seuls les périphériques absolument nécessaires comme le système de bus, les disquettes d'amorçage ou le clavier sont initialisés.

Les périphériques sont normalement reconnus par un pilote et, en conséquence, un événement Hotplug est émis et géré par les scripts appropriés. Toutefois, il existe des périphériques qui ne sont pas reconnus automatiquement. Dans ce cas, vous disposez de Coldplug qui applique sans condition des réglages statiques aux périphériques qui ne peuvent pas être reconnus.

Si l'on laisse de côté quelques exceptions historiques, la plupart des périphériques sont actuellement initialisés à l'amorçage ou au branchement. Cette initialisation a fréquemment pour résultat l'enregistrement d'une interface. L'enregistrement de l'interface entraîne en retour l'émission d'événements Hotplug qui déclenchent l'installation automatique des interfaces concernées. Là où, auparavant, on se basait sur un ensemble de données de configuration pour initialiser des périphériques, on part aujourd'hui des périphériques et on recherche pour ceux-ci les données de configuration correspondantes. Le déroulement de l'initialisation s'est donc ainsi inversé, ce qui a permis une gestion plus souple des périphériques branchés à chaud.

Vous configurez les fonctions Hotplug les plus importantes dans deux fichiers : vous trouverez dans `/etc/sysconfig/hotplug` des variables qui commandent le comportement de `hotplug` et `coldplug`. Chaque variable est détaillée par un commentaire. Le fichier `/proc/sys/kernel/hotplug` comporte le nom du programme exécutable qui est appelé par le noyau. Les réglages de périphériques se trouvent dans le fichier `/etc/sysconfig/hardware`.

18.1 Périphériques et interfaces

Un périphérique (*en anglais device*) est systématiquement lié à une interface ; un bus peut être vu comme une interface multiple. Outre les périphériques physiques, il existe également des périphériques virtuels (par exemple un tunnel réseau). Chaque interface (en anglais *en anglais interface*) est associée soit à un périphérique, soit à une application. La séparation entre périphérique et interface est ici utilisée pour faciliter la compréhension du concept global.

On trouve dans `/sys/devices` les périphériques déclarés dans `sysfs` ; les interfaces se trouvent dans `/sys/class` ou `/sys/block`. Dans le fichier `sysfs`, toutes les interfaces doivent comporter un lien (*en anglais link*) vers leur périphérique. Toutefois, il existe encore quelques pilotes qui n'ajoutent pas automatiquement ces liens.

Les périphériques sont identifiés au moyen d'une description de périphérique. Ceci peut être le "devicepath" dans le fichier `sysfs` (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0`), une description de l'emplacement de connexion (`bus-pci-0000:02:00.0`), un identifiant individuel (`id-32311AE03FB82538`) ou toute méthode comparable d'identification. Les interfaces étaient jusqu'à présent toujours identifiées par leur nom. Toutefois, ces noms sont une simple numérotation des périphériques existants, qui peuvent donc être modifiés lorsque l'on insère ou retire des périphériques. C'est pourquoi on peut aussi identifier les interfaces par une description du périphérique correspondant. C'est alors généralement le contexte qui permet de déterminer si c'est de la description du périphérique lui même ou de son interface dont il est question. Des exemples typiques de périphériques, d'interfaces et de leur descriptions sont par exemple :

Carte réseau PCI Un périphérique lié au bus PCI (`/sys/devices/pci0000:00/0000:00:1e.0/0000:02:00.0` ou `bus-pci-0000:02:00.0`) et qui dispose d'une interface réseau (`eth0`, `id-00:0d:60:7f:0b:22` ou `bus-pci-0000:02:00.0`). Celle-ci est utilisée par des services réseau ou est liée à un périphérique réseau virtuel comme un tunnel ou un réseau virtuel privé, lequel possède en retour une interface.

Contrôleur PCI SCSI Un périphérique (`/sys/devices/pci0000:20/0000:20:01.1`, etc.) qui met à disposition plusieurs interfaces physiques sous la forme d'un bus (`/sys/class/scsi_host/host1`).

Disque dur SCSI Un périphérique (`/sys/devices/pci0000:20/0000:20:01.1/host1/1:0:0:0`, `bus-scsi-1:0:0:0`) avec plusieurs interfaces (`/sys/block/sda*`).

18.2 Événements Hotplug

Il existe pour chaque périphérique et pour chaque interface ce qu'on appelle un événement Hotplug qui est traité par les agents Hotplug correspondants. Les événements Hotplug sont déclenchés par le noyau lorsqu'une liaison avec un périphérique est établie, ou lorsqu'un pilote enregistre une interface.

Un événement Hotplug est l'appel d'un programme, normalement `/sbin/hotplug`, lorsque rien d'autre n'est spécifié dans le fichier `/proc/sys/kernel/hotplug`. Le fichier `/sbin/hotplug` recherche un agent Hotplug qui correspond au type d'événement. S'il ne trouve aucun agent approprié, le programme s'arrête.

Remarque

Ignorer certains événements Hotplug

Si des événements de type défini doivent en principe être ignorés, éditez pour cela le ficher `/etc/sysconfig/hotplug` et déclarez les noms des événements non souhaités dans la variable `HOTPLUG_SKIP_EVENTS`.

Remarque

18.3 Agents Hotplug

Un agent Hotplug est un programme exécutable qui accomplit les actions appropriées pour un événement. Pour les événements de périphériques, les agents se trouvent dans le fichier `/etc/hotplug` et sont intitulés `<Eventname>.agent`. Pour les événements d'interfaces, la commande `udev` lance les programmes de `/etc/dev.d`.

Les agents de périphériques chargent en majorité des modules de noyau, mais doivent toutefois occasionnellement appeler aussi des commandes additionnelles. Sous SUSE LINUX, ceci est pris en charge par `/sbin/hwup` ou `/sbin/hwdown`. Ces programmes recherchent dans le fichier `/etc/sysconfig/hardware` une configuration adaptée au périphérique et l'utilisent le cas échéant. Si un périphérique donné ne doit pas être initialisé, un fichier de configuration correspondant doit être mis en place avec le mode de démarrage `manual` ou `off`. Si `/sbin/hwup` ne trouve aucune configuration, des modules sont automatiquement chargés par les agents. Plus d'informations sur ce sujet sont disponibles dans la section *Chargement automatique de modules* page 404. Vous trouverez des informations sur `/sbin/hwup` dans le fichier `/usr/share/doc/packages/sysconfig/README` et à la page de manuel de `hwup`.

Les agents d'interfaces sont appelés indirectement par la commande `udev`. De cette manière, `udev` construit tout d'abord un fichier spécial de périphérique (*en anglais device node*) sur laquelle le système peut prendre la main. La commande `udev` permet de donner des noms persistants aux interfaces. Des détails sur ce point sont disponibles au chapitre *Noeuds de périphériques dynamiques avec udev* page 409. Enfin, les agents individuels installent l'interface. Les opérations correspondant à quelques interfaces sont décrites dans ce qui suit.

18.3.1 Activation des interfaces réseau

Les interfaces réseau sont initialisées avec `/sbin/ifup` et désactivées avec `/sbin/ifdown`. Vous trouverez des détails à ce sujet dans le fichier `/usr/share/doc/packages/sysconfig/README` et dans la page de manuel de la commande `ifup`. Comme Linux n'utilise pas de fichiers spéciaux ("device nodes") pour les interfaces réseau, ceux-ci ne sont pas non plus gérés par la commande `udev`.

Si un ordinateur dispose de plusieurs périphériques réseau avec différents pilotes, il se peut que les désignations d'interfaces soient modifiées après l'amorçage, dans le cas où un autre pilote a été chargé plus rapidement. C'est pour cela que dans SUSE LINUX les périphériques réseau PCI sont administrés par une file d'attente. Vous pouvez désactiver ce comportement dans le fichier `/etc/sysconfig/hotplug` par l'intermédiaire de la variable `HOTPLUG_PCI_QUEUE_NIC_EVENTS=no`.

Le meilleur moyen pour obtenir des désignations d'interfaces cohérentes consiste cependant à indiquer le nom souhaité dans les fichiers de configuration de chaque interface. Vous trouverez des détails sur cette méthode dans le fichier `/usr/share/doc/packages/sysconfig/README`.

18.3.2 Activation des périphériques de stockage

Les interfaces des périphériques de stockage doivent être intégrée pour pouvoir y accéder. Cela peut se faire soit de façon totalement automatique, soit être configuré à l'avance. La configuration s'effectue dans le fichier `/etc/sysconfig/hotplug` au moyen des variables `HOTPLUG_DO_MOUNT`, `HOTPLUG_MOUNT_TYPE`, `HOTPLUG_MOUNT_SYNC` et dans le fichier `/etc/fstab`.

Le fonctionnement complètement automatisé est activé en fixant la variable `HOTPLUG_DO_MOUNT=yes`. Il prend en charge deux modes et l'on passe de l'un à l'autre au moyen de la variable `HOTPLUG_MOUNT_TYPE`.

En mode HOTPLUG_MOUNT_TYPE=subfs, un répertoire dont le nom est construit à partir des caractéristiques du périphérique est placé dans le répertoire /media. Le volume y est monté et démonté automatiquement par la commande submountd. Ainsi les données sont toujours écrites immédiatement. En conséquence, des périphériques fonctionnant dans ce mode peuvent aussi être retirés facilement lorsque le témoin d'accès est éteint.

En mode HOTPLUG_MOUNT_TYPE=fstab, les périphériques de stockage sont montés comme il est indiqué dans le fichier /etc/fstab. La variable HOTPLUG_MOUNT_SYNC permet de choisir si l'accès doit se faire en mode synchrone ou asynchrone. En fonctionnement asynchrone, le temps d'accès en écriture est plus court, car les résultats sont stockés dans un espace intermédiaire ; il se peut toutefois que les données ne puissent pas être écrites complètement lorsque le volume est retiré sans précaution. En fonctionnement synchrone, toutes les données sont toujours écrites immédiatement, mais le temps d'accès est par conséquent plus long. La déconnexion du périphérique doit s'effectuer manuellement par la commande umount.

Le fonctionnement totalement automatique est désactivé en fixant la variable HOTPLUG_DO_MOUNT=no. Le périphérique doit alors être monté et démonté manuellement.

Les deux dernières méthodes de fonctionnement se prêtent à l'utilisation de noms persistents pour les périphériques, car les noms de périphériques traditionnels peuvent changer selon l'ordre d'initialisation. Vous pourrez trouver plus de détails sur les noms persistents pour les périphériques dans le chapitre *Noeuds de périphériques dynamiques avec udev* page 409.

18.4 Chargement automatique de modules

Si un périphérique n'avait pas pu être initialisé avec /sbin/hwup, l'agent explore ce qu'on appelle les "tables de correspondance de modules" (*Module Maps*) à la recherche d'un pilote adapté. Il examine en premier les tables de correspondance dans /etc/hotplug/*.handmap ; s'il n'a rien trouvé, il cherche également dans /lib/modules/<kernelversion>/modules.*map. Si vous voulez utiliser un autre pilote que le pilote standard du noyau, déclarez-le dans /etc/hotplug/*.handmap car ce fichier est le premier a être lu.

Veuillez noter les différences suivantes entre USB et PCI. L'agent USB cherche également dans les fichiers `/etc/hotplug/usb.usermap` et `/etc/hotplug/usb/*.usermap` des pilotes en mode utilisateur. Les pilotes Usermode sont des programmes qui règlent l'accès au périphérique en lieu et place d'un module noyau. On peut de cette façon appeler d'autres programmes exécutables pour des périphériques déterminés.

Dans le cas de périphériques PCI, `pci.agent` interroge d'abord `hwinfo` au sujet de modules de pilote. L'agent ne recherche dans le `pci.handmap` et le kernelmap que si `hwinfo` ne connaît aucun pilote ; cela a déjà été tenté auparavant par `hwinfo` et doit donc également échouer. `hwinfo` dispose d'une base de données supplémentaire d'assignation des pilotes. La commande lit également `pci.handmap`, ce qui permet de s'assurer qu'une assignation donnée dans ce fichier est réellement utilisée.

L'agent `pci.agent` peut être limité à des périphériques d'un type déterminé ou aux modules pilotes qui se trouvent dans un sous-répertoire défini dans `/lib/modules/<kernelversion>/kernel/drivers`. Dans le premier cas, des classes de périphériques PCI peuvent être ajoutées dans le fichier `/etc/sysconfig/hotplug` au niveau des variables `HOTPLUG_PCI_CLASSES_WHITELIST` et`HOTPLUG_PCI_CLASSES_BLACKLIST`, comme on peut le voir à la fin du fichier `/usr/share/pci.ids`. Pour le second cas, vous spécifiez un ou plusieurs répertoires dans les variables `HOTPLUG_PCI_DRIVERTYPE_WHITELIST` et `HOTPLUG_PCI_DRIVERTYPE_BLACKLIST`. Les modules de ces répertoires exclus ne seront jamais chargés. Dans les deux cas, une liste blanche (whitelist) totalement vide signifie que toute possibilité, à l'exception de celles exclues dans la liste noire (blacklist), est licite. Indiquez aussi dans le fichier `/etc/hotplug/blacklist` les modules qui ne devront jamais être chargés par un agent. Écrivez chacun des noms de modules sur sa propre ligne.

Si plusieurs modules appropriés sont trouvés dans une table de correspondance, seul le premier module sera chargé. Si vous souhaitez que tous les modules soient chargés, déclarez la variable `HOTPLUG_LOAD_MULTIPLE_MODULES=yes`. Il est encore mieux toutefois d'établir une configuration matérielle `/etc/sysconfig/hardware/hwcfg-*` particulière pour ce périphérique.

Cela ne concerne pas les modules chargés à l'aide de `hwup`. Le chargement automatique de modules n'a lieu qu'exceptionnellement, et sera encore davantage restreint dans les versions futures de SUSE LINUX.

18.5 Hotplug avec PCI

Quelques ordinateurs autorisent également le branchement à chaud de périphériques PCI. Afin de pouvoir utiliser pleinement cette possibilité, des modules de noyau particuliers doivent être chargés, qui peuvent provoquer des dommages sur les ordinateurs Hotplug non-PCI. Les emplacements PCI Hotplug ne peuvent malheureusement pas être reconnus automatiquement ; vous devez donc configurer cette fonction manuellement. Pour ce faire, renseignez la variable `HOTPLUG_DO_REAL_PCI_HOTPLUG` à la valeur `yes` dans le fichier `/etc/sysconfig/hotplug`.

18.6 Les scripts d'amorçage Coldplug et Hotplug

La commande `boot.coldplug` est utilisée pour tous les périphériques qui ne sont pas reconnus automatiquement, c'est-à-dire pour lesquels aucun événement Hotplug n'a pu être généré. Dans ce cas, c'est simplement la commande `hwup` seule qui est appelée pour chaque configuration matérielle statique `/etc/sysconfig/hardware/hwcfg-static-*`. Ceci peut également être utilisé pour initialiser des périphériques intégrés dans un ordre différent de celui qui serait utilisé par Hotplug : en effet, la commande `coldplug` est exécutée avant `hotplug`.

`boot.hotplug` déclenche le traitement des événements Hotplug. Le paramètre d'amorçage `khelper_max=0` permet en effet d'empêcher l'émission d'événements Hotplug au début de la phase d'amorçage. Ces événements déjà créés sont donc encore dans une file d'attente du noyau. `boot.hotplug` renseigne ensuite dans le fichier `/etc/sysconfig/hotplug` combien d'événements ont été émis parallèlement, à un moment donné. De cette façon, aucun événement Hotplug n'est perdu.

18.7 Analyse d'erreurs

18.7.1 Fichiers journaux

`hotplug` n'envoie en standard que quelques informations importantes à `syslog`. Pour recevoir plus d'informations, configurez la variable `HOTPLUG_DEBUG` du fichier `/etc/sysconfig/hotplug` à la valeur `yes`. Si vous donnez à cette variable la valeur `max`, chaque commande du shell de tous les scripts Hotplug sera consignée. La taille du fichier `/var/log/messages` dans lequel `syslog` enregistre toutes les informations augmentera en conséquence. Comme `syslog` n'est démarré, pendant l'amorçage, qu'après `hotplug` et `coldplug`, il n'est pas pas encore possible de consigner les premières informations. Si ces informations sont importantes pour vous, créez au moyen de la variable `HOTPLUG_SYSLOG` un autre fichier journal. Notez à ce sujet les commentaires se trouvant dans `/etc/sysconfig/hotplug`.

18.7.2 Problèmes d'amorçage

Si un ordinateur se fige au démarrage, vous pouvez désactiver `hotplug` ou `coldplug` en entrant `NOHOTPLUG=yes` ou `NOCOLDPLUG=yes` dans l'invite de commande d'amorçage. La désactivation de Hotplug a simplement pour conséquence qu'aucun événement Hotplug n'est émis par le noyau. Vous pouvez réactiver Hotplug pendant que le système est en marche en entrant la commande `/etc/init.d/boot.hotplug start`. Tous les événements Hotplug créées jusqu'alors sont émis et traités. Pour supprimer des événements en cas de congestion, vous pouvez auparavant indiquer `/bin/true` dans `/proc/sys/kernel/hotplug`, puis, après un certain temps, revenir à `/sbin/hotplug`. La désactivation de Coldplug a simplement pour conséquence que les réglages statiques ne sont pas appliqués. Naturellement, vous pouvez aussi réactiver Coldplug au moyen de la commande `/etc/init.d/boot.coldplug start`.

Pour savoir si un module donné, chargé par `hotplug`, est responsable des problèmes, déclarez `HOTPLUG_TRACE=<N>` dans l'invite d'amorçage. Les noms de tous les modules devant être chargés sont affichés l'un après l'autre à l'écran avant d'être effectivement chargés après $\langle N \rangle$ secondes. Vous ne pouvez cependant pas intervenir ici de façon interactive.

18.7.3 L'enregistreur d'événements

Le script `/sbin/hotplugeventrecorder` est appelé à chaque événement par `/sbin/hotplug`. S'il existe un répertoire `/events`, tous les événements Hotplug y sont enregistrés comme des fichiers individuels. De cette façon, on peut générer à nouveau, à des fins de test, des événements particuliers conformes à l'original. Si le répertoire n'existe pas, aucun enregistrement n'est créé.

18.7.4 Charge système trop élevée ou amorçage trop lent

La valeur de la variable `HOTPLUG_MAX_EVENTS`, du fichier `/etc/sysconfig/hotplug`, est transmise au noyau au démarrage de Hotplug et détermine le nombre d'événements qui peuvent être traités simultanément. Si Hotplug génère à l'amorçage une charge système trop importante, vous pouvez réduire cette valeur. Si toutefois Hotplug effectue ses traitements trop lentement, cette valeur doit être augmentée.

19

Noeuds de périphériques dynamiques avec udev

Avec le noyau Linux 2.6, il existe une nouvelle solution *Userspace* pour un répertoire de périphériques dynamique `/dev` avec des désignations de périphériques cohérentes : `udev`. L'implémentation précédente de `/dev` avec `devfs` ne fonctionne plus et est remplacée par `udev`.

Des noeuds de périphériques (*en angl. device nodes*)ont été traditionnellement enregistrés sur les systèmes Linux dans le répertoire `/dev`. Il existait un noeud pour chaque type de périphérique, indépendamment du fait de savoir s'il existait effectivement dans le système. En conséquence, la taille de ce répertoire devenait importante. On atteignit une amélioration sensible avec `devfs` car seuls les périphériques existant réellement obtinrent un noeud de périphériques dans `/dev`.

`udev` s'y prend autrement pour créer des noeuds de périphériques. Il compare les informations mises à disposition par `sysfs` avecs les entrées de l'utilisateur sous forme de règles. `sysfs` est un nouveau système de fichiers du noyau 2.6 et offre les informations de base sur les périphériques connectés dans le système. Il se situe sous `/sys`.

La création de règles par l'utilisateur n'est pas absolument nécessaire. Si on connecte un périphérique, le noeud de périphérique correspondant est alors créé. Les règles offrent cependant la possibilité de modifier le nom des noeuds. Ceci permet de remplacer le nom cryptique d'un périphérique par un nom de périphérique plus facile à retenir, et de conserver en outre des noms de périphériques cohérents si vous avez connecté deux périphériques de même type.

Deux imprimantes reçoivent deux désignations `/dev/lp0` et `/dev/lp1` par défaut. Mais le noeud de périphérique attribué à chacune dépend de l'ordre dans lequel elles ont été mises sous tension. Un autre exemple sont les périphériques de mémoire de masse comme les disques durs USB. Avec `udev`, on entre les chemins du périphérique exacts dans `/etc/fstab`.

19.1 Bases de la création de règles

Avant que `udev` crée des noeuds de périphériques sous `/dev`, il lit le fichier `/etc/udev/udev.rules`. La première règle qui convient à un périphérique est utilisée, même s'il en existe d'autres. Les commentaires commencent par le signe #. Les règles ont la forme suivante :

```
Code, [Code,...] NOM [, SYMLINK]
```

Un code au minimum doit être indiqué puisque la règle va être affectée à un périphérique par l'intermédiaire de ce code. Le nom est également obligatoirement nécessaire car le noeud de périphérique sera établi sous ce nom dans `/dev`. Le paramètre Symlink optionnel permet d'établir des noeuds de périphériques dans d'autres endroits. Une règle pour une imprimante pourrait alors se présenter comme ceci :

```
BUS="usb", SYSFS{serial}="12345", NAME="lp_hp", SYMLINK="printers/hp"
```

Il y a dans cet exemple deux codes : BUS et SYSFS{serial}. udev va comparer le numéro de série avec celui du périphérique auquel le bus USB est connecté. Tous les codes doivent coïncider afin d'attribuer au périphérique le nom lp_hp dans le répertoire /dev. De plus, il créera un /dev/printers/hp symbolique qui renvoie au noeud de périphérique. Le répertoire printers est alors créé automatiquement. Les requêtes d'impression peuvent ensuite être envoyées à /dev/printers/hp ou /dev/lp_hp.

19.2 Automatisation avec NAME et SYMLINK

Les paramètres NAME et SYMLINK permettent l'utilisation d'opérateurs pour l'automatisation d'affectations. Ces opérateurs se réfèrent à des données du noyau au sujet du périphérique correspondant. Voici un exemple simple en guise d'illustration :

```
BUS="usb", SYSFS{vendor}="abc", SYSFS{model}="xyz", NAME="camera%n"
```

L'opérateur %n est remplacé dans le nom par le numéro prévu pour l'appareil photo périphérique : camera0, camera1, etc. Un autre opérateur utile est %k, remplacé par le nom du périphérique standard du noyau, par exemple hda1. A la page de manuel de udev, vous trouverez une liste de tous les opérateurs.

19.3 Expressions régulières dans les codes

Dans les codes, des expressions régulières peuvent être utilisées dans le shell comme les jockers, ainsi par exemple le signe * en tant que caractère de remplacement pour n'importe quel signe ou ? pour un certain caractère précis.

```
KERNEL="ts*", NAME="input/%k"
```

Avec cette règle, un périphérique, dont la désignation commence avec les lettres "ts", reçoit le nom de noyau standard dans le répertoire standard. Vous trouverez des informations détaillées sur l'utilisation d'expressions régulières dans les règles udev à la page de manuel `man udev`.

19.4 Conseils pour choisir les codes appropriés

Le choix d'un bon code constitue la condition pour toute règle udev apte à fonctionner. Les codes standard sont par exemple :

BUS Type de bus du périphérique

NOYAU Nom du périphérique que le noyau utilise

ID Numéro du périphérique sur le bus (par ex. Bus PCI ID)

PLACE Emplacement physique auquel le périphérique est connecté (par ex. pour USB)

Les codes ID et Place peuvent s'avérer utiles, mais la plupart du temps les codes `BUS` et `KERNEL` ainsi que `SYSFS{...}` sont utilisés. De plus, `udev` met à disposition des codes qui appellent des scripts externes et évaluent leur résultat. Vous trouverez plus d'informations détaillées à la page de manuel `man udev`.

`sysfs` ne classe aucun fichier contenant des informations matérielles dans une arborescence de répertoire. Chaque fichier ne reçoit alors en règle générale qu'une information, comme le nom du périphérique, le fabricant et le numéro de série. Chacun de ces fichiers peut être utilisé comme valeur de code. Si vous voulez utiliser plusieurs codes `SYSFS{...}` dans une règle, vous ne devez cependant utiliser que des fichiers du même répertoire.

udevinfo s'avère être ici un outil utile. Vous devez seulement trouver sous `/sys` un répertoire se rapportant au périphérique correspondant, comprenant un fichier `dev`. Vous trouverez tous ces répertoires sous `/sys/block` ou `/sys/class`.

S'il existe déjà un noeud de périphérique pour le périphérique, `udevinfo` peut faire le travail à votre place. La commande `udevinfo -q path -n /dev/sda` affiche `/block/sda`. Ceci signifie que le répertoire recherché est `/sys/block/sda`. Appelez ensuite `udevinfo` avec la commande suivante : `udevinfo -a -p /sys/block/sda`. Les deux commandes peuvent également être combinées

: `udevinfo -a -p ‘udevinfo -q path -n /dev/sda‘`. Un extrait de l’affichage pourrait ressembler à ceci :

```
BUS="scsi"
ID="0:0:0:0"
SYSFS{detach_state}="0"
SYSFS{type}="0"
SYSFS{max_sectors}="240"
SYSFS{device_blocked}="0"
SYSFS{queue_depth}="1"
SYSFS{scsi_level}="3"
SYSFS{vendor}="        "
SYSFS{model}="USB 2.0M DSC    "
SYSFS{rev}="1.00"
SYSFS{online}="1"
```

Sélectionnez dans toutes les nombreuses sorties d’informations les codes cohérents que vous ne voulez pas modifier. Pensez qu’en règle générale les codes issus de répertoires différents ne doivent pas être utilisés.

19.5 Noms cohérents pour périphériques de mémoir de masse

Avec SUSE LINUX sont livrés des scripte qui vous aident à toujours affecter les mêmes désignations aux disques durs et autres périphériques de mémoire. `/sbin/udev.get_persistent_device_name.sh` est un script Wrapper. Il appelle d’abord `/sbin/udev.get_unique_hardware_path.sh` qui détecte le chemin d’accès vers un périphérique donné. De plus, `/sbin/udev.get_unique_drive_id.sh` se renseigne sur le numéro de série. Les deux informations sont transmises à `udev`, qui crée des liens symboliques ves le noeud de périphérique sous `/dev`. Le script Wrapper peut être utilisé directement dans les règles udev. Un exemple pour SCSI, qu’on peut également étendre à USB ou IDE (à indiquer en une ligne) :

```
BUS="scsi", PROGRAM="/sbin/udev.get_persistent_device_name.sh",
NAME="%k" SYMLINK="%c{1+}"
```

Dès qu'un pilote pour un périphérique de mémoire de masse a été chargé, il se manifeste auprès du noyau avec tous les disques durs en présence. Chacun d'entre eux déclenchera un événement Hotplug Block qui appelle `udev`. `udev` lit d'abord les règles afin de constater si un Symlink doit être créé.

Si le pilote est chargé via `initrd`, les événements Hotplug sont perdus. Cependant, toutes les informations sont enregistrées dans `sysfs`. Le programme d'aide `udevstart` trouve tous les fichiers de périphériques sous `/sys/block` et `/sys/class`, puis démarre `udev`.

Il existe en outre un script de démarrage `boot.udev` qui qui recrée pendant l'amorçage tous les noeuds de périphériques. Le script de démarrage peut cependant être activé via le l'éditeur de niveaux d'exécution de YaST ou à l'aide de la commande `insserv boot.udev`.

Remarque

Il existe un bon nombre d'outils et de programmes qui croient sans réserve que `/dev/sda` est un disque dur SCSI et `/dev/hda` un disque dur IDE. Si cela n'est pas le cas, ces programmes ne fonctionnent plus. Mais YaST a connaissance de ces outils et ne travaille pour cette raison qu'avec les désignations de périphériques du noyau.

Remarque

Systèmes de fichiers sous Linux

Linux prend en charge un grand nombre de systèmes de fichiers. Ce chapitre présente brièvement les systèmes de fichiers les plus connus sous Linux, dont nous vous présenterons de manière plus précise la conception et les avantages ainsi que les domaines d'utilisation. Nous vous fournirons également quelques informations relatives au "Large File Support" (la prise en charge des gros fichiers) sous Linux.

20.1 Glossaire

Métadonnées Structure de données interne d'un système de fichiers qui garantit le respect d'une structuration et la disponibilité des données sur le disque dur. Il s'agit en fait des "données concernant les données". Presque chaque système de fichiers possède sa propre structure de métadonnées. Il s'agit également en partie d'une des raisons des différentes caractéristiques de performance des différents systèmes de fichiers. Il est particulièrement important de conserver intactes les métadonnées car, dans le cas contraire, le système de fichiers dans son ensemble en serait perturbé.

Inode Les inodes contiennent toutes les informations relatives à un fichier, sa taille, le nombre des liens, la date, la date de création, les modifications, l'accès ainsi que les pointeurs (en anglais, *pointer*) vers les blocs de disque dur dans lesquels le fichier est enregistré.

Journal Quand on parle de système de fichiers, un journal est une structure interne au disque utilisant une sorte de fichier journal dans lequel le pilote du système de fichiers enregistre les données et les métadonnées à modifier du système de fichiers. La "journalisation" permet de réduire considérablement le temps de restauration d'un système Linux dans la mesure où le pilote du système de fichiers n'a pas besoin de lancer une recherche systématique des métadonnées abîmées sur la totalité du disque. À la place, ce sont les enregistrements du fichier journal qui sont réappliqués.

20.2 Les principaux systèmes de fichiers sous Linux

Contrairement à il y a deux ou trois ans, un système de fichiers pour Linux ne se choisit plus en quelques secondes (Ext2 ou ReiserFS ?). Les noyaux à partir de la version 2.4 proposent une grande variété de systèmes de fichiers. Vous trouverez ci-après un vue d'ensemble des principaux modes de fonctionnement de ces systèmes de fichiers et leurs avantages respectifs.

Gardez à l'esprit qu'aucun système de fichiers ne peut convenir à tous les usages de la même manière. Chaque système de fichiers possède ses propres forces et faiblesses, que vous devez étudier au préalable. Même le système de fichiers le plus élaboré du monde ne pourra jamais remplacer une politique de sauvegarde raisonnable.

Les termes "intégrité des données" ou "cohérence des données" ne font pas référence dans ce chapitre à la cohérence des données enregistrées d'un utilisateur (les données que votre application écrit dans vos fichiers). C'est l'application elle-même qui doit assurer la cohérence de ces données.

Remarque

Organisation des systèmes de fichiers

Sauf si nous indiquons le contraire, toutes les tâches de partitionnement, d'organisation et de traitement des systèmes de fichiers peuvent s'effectuer confortablement avec YaST.

Remarque

20.2.1 ReiserFS

Officiellement, l'une des principales fonctionnalités du noyau version 2.4, ReiserFS, était disponible depuis SUSE LINUX version 6.4 en tant que correctif du noyau pour le noyau 2.2.x SuSE. ReiserFS a été développé par Hans Reiser et l'équipe de développement Namesys. ReiserFS s'est positionné en tant que puissante alternative à Ext2. Ses principaux avantages sont : une meilleure gestion de l'espace disque, de meilleures performances d'accès aux disques et une restauration plus rapide après un plantage. Reste cependant une petite pointe d'amertume : ReiserFS accorde beaucoup d'importance aux métadonnées mais pas aux données elles-mêmes. Les prochaines générations de ReiserFS comprendront également une fonctionnalité de journalisation des données (aussi bien les métadonnées que les données elles-mêmes sont enregistrées dans un fichier journal) ainsi que des accès en écriture ordonnés (voir `data=ordered` sous Ext3). Les points forts de ReiserFS en détail :

Une meilleure gestion de l'espace disque
: Dans ReiserFS, toutes les données sont organisées dans une structure d'arbre équilibré dénommée B^*. Cette structure arborescente contribue à une meilleure gestion de l'espace disque car les petits fichiers peuvent être enregistrés directement dans les ramifications de l'arbre B^* au lieu d'être enregistrés en d'autres endroits et gèrent simplement le pointeur sur l'endroit en question. En outre, l'espace disque n'est pas alloué par unités d'1 ou de 4 Ko, mais exactement par l'unité nécessaire. Un avantage supplémentaire consiste en l'attribution dynamique des inodes. Cela confère au système de fichiers une plus grande flexibilité par rapport aux

systèmes de fichiers classiques tels que par exemple Ext2, dans lesquels il faut indiquer la densité d'inodes au moment de la définition du système de fichiers.

Meilleures performances d'accès aux disques durs
Pour les petits fichiers, vous pourrez souvent remarquer qu'aussi bien les données de fichiers que les informations (inodes) "stat_data" sont enregistrées les unes à côté des autres. Un seul accès au disque dur suffit pour que vous disposiez de toutes les informations nécessaires.

Restauration rapide après un plantage
Grâce à l'utilisation d'un fichier journal pour l'observation des modifications de métadonnées entreprises récemment, la vérification du système de fichiers se réduit, même pour les gros systèmes de fichiers, à quelques secondes.

20.2.2 Ext2

Les origines d'Ext2 remontent au début de l'histoire de Linux. Son prédécesseur, l'Extended File System, a été mis en œuvre en avril 1992 et intégré à Linux 0.96c. L'Extended File System a subi un grand nombre de modifications, pour devenir pendant des années le système de fichiers le plus connu sous Linux sous le nom d'Ext2. Avec l'apparition des systèmes de fichiers journalisés et leurs temps de restauration étonnamment courts, Ext2 a perdu sa position de vedette.

Un bref résumé des points forts d'Ext2 devrait vous aider à comprendre pourquoi il est tellement apprécié des utilisateurs de la communauté Linux, qui lui accordent encore aujourd'hui leur préférence.

Stabilité En tant que véritable "ancêtre", Ext2 a connu de nombreuses améliorations et a été testé de manière très complète pour avoir une réputation de système de fichiers "solide comme un roc". En cas de panne du système, dans laquelle le système de fichiers ne peut pas être démonté proprement, e2fsck démarre une analyse des données du système de fichiers. Les métadonnées sont remises dans un état cohérent et les fichiers ou les blocs de données égarés sont écrits dans un répertoire prévu à cet effet (nommé `lost+found`). Contrairement à (la plupart) des systèmes de fichiers journalisés, e2fsck analyse la totalité du système de fichiers et pas seulement les bits de métadonnées qui viennent d'être modifiés. Cela dure significativement plus longtemps que la vérification des données de journalisation d'un système de fichiers journalisé. Selon l'importance du système de fichiers, cela peut durer d'une demi-heure à plusieurs heures. Il ne faut donc

pas choisir Ext2 pour un serveur qui doit être beaucoup disponible. Comme Ext2 n'a pas besoin de gérer un fichier journal et utilise significativement moins d'espace disque, il est parfois plus rapide que d'autres systèmes de fichiers.

Mise à niveau simple Fondé sur les solides bases d'Ext2, Ext3 a pu être développé en tant que système de fichiers adulé de la génération suivante. Sa fiabilité et sa stabilité ont été habilement associées aux avantages d'un système de fichiers journalisé.

20.2.3 Ext3

Ext3 a été lancé par Stephen Tweedie. Contrairement à tous les autres systèmes de fichiers de la "génération suivante", Ext3 respecte un principe de conception complètement nouveau. Il est fondé sur Ext2. Ces deux systèmes de fichiers sont très intimement liés. Un système de fichiers Ext3 peut très facilement être construit à partir d'un système de fichiers Ext2 ; la différence fondamentale entre Ext2 et Ext3 étant qu'Ext3 prend en charge la journalisation.

En résumé, on reconnaît trois avantages principaux à Ext3 :

Mises à niveau simples et extrêmement fiables à partir d'Ext2
Comme Ext3 est basé sur le code d'Ext2 et partage également son format de disque ainsi que son format de métadonnées, les mises à niveau d'Ext2 en Ext3 sont très simples. Vous pouvez les effectuer lorsque vos systèmes de fichiers Ext2 sont montés. Contrairement au passage à d'autres système de fichiers journalisés, comme par exemple ReiserFS, JFS ou XFS, qui peuvent se révéler fastidieux (vous devez réaliser des copies de sauvegarde de tout le système de fichiers et le recréer à partir de zéro), le passage à Ext3 ne prend que quelques minutes.De même ce passage est très sûr, dans la mesure où la restauration de l'ensemble d'un système de fichiers de zéro ne permet pas toujours d'éliminer toutes les erreurs. Si l'on considère le nombre de systèmes Ext2 disponibles en attente d'une mise à niveau pour un système de fichiers journalisé, on peut facilement comprendre la signification d'Ext3, pour nombre d'administrateurs système. Une rétrogradation d'Ext3 en Ext2 est tout aussi facile qu'une mise à niveau. Démontez simplement proprement le système de fichiers Ext3 et remontez-le en tant que système de fichiers Ext2.

Fiabilité et performance Les autres systèmes de fichiers journalisés respectent le principe de journalisation des "métadonnées seulement", à savoir que leurs métadonnées restent dans un état cohérent ; ce qui ne peut cependant pas être garanti automatiquement pour les données du système de fichiers eux-mêmes. Ext3 est en mesure de s'occuper aussi bien des métadonnées que des données elles-mêmes. Vous pouvez régler la précision avec laquelle Ext3 doit s'occuper des métadonnées et des données. Pour obtenir le niveau de sécurité (c'est-à-dire d'intégrité des données) le plus élevé, démarrez Ext3 en mode `data=journal` ; cela est cependant susceptible de ralentir le système dans la mesure où aussi bien les métadonnées que les données elles-mêmes sont répertoriées dans le fichier journal. Une approche relativement nouvelle consiste à utiliser le mode `data=ordered` qui garantit l'intégrité aussi bien des données que des métadonnées, mais qui n'utilise la journalisation que pour les métadonnées. Le pilote du système de fichiers rassemble tous les blocs de données qui appartiennent à une mise à jour de métadonnées. Ces blocs sont regroupés en tant que "transactions" et sont écrits sur le disque avant l'actualisation des métadonnées. Cela permet de garantir la cohérence des métadonnées et des données sans perte de performance. Un troisième type d'utilisation est `data=writeback`. Avec ce dernier, les données peuvent être écrites dans le système de fichiers principal, une fois les métadonnées transmises au fichier journal. Cette option est, pour beaucoup, le meilleur réglage en terme de performance. Il peut cependant se produire, avec cette option, que les anciennes données, après une panne et une restauration, apparaissent dans des fichiers tout en garantissant la cohérence interne du système de fichiers. Sauf spécification contraire, Ext3 est démarré avec le paramètre par défaut `data=ordered`.

Passage d'un système de fichiers Ext2 à Ext3

Création du fichier journal : Appelez la commande `tune2fs -j` en tant qu'utilisateur `root`. tune2fs crée le fichier journal Ext3 avec les paramètres par défaut. Si vous souhaitez définir vous-même la taille du fichier journal et sur quel disque il doit être créé, appelez à la place `tune2fs -J` avec les deux paramètres `size=` et `device=`. Pour plus d'informations sur tune2fs, consultez la page de manuel correspondante.

Déclaration du type de système de fichiers dans `/etc/fstab`
Pour que le système de fichiers Ext3 soit également reconnu en tant que tel, ouvrez le fichier `/etc/fstab` et modifiez le type de système de fichiers de la partition concernée de `ext2` en `ext3`. Votre modification entrera en vigueur lors du prochain redémarrage de votre système.

Utilisation de `ext3` pour le répertoire `root`
Si vous voulez amorcer votre système de fichiers `root` comme `ext3`, il est également nécessaire d'intégrer les modules `ext3` et `jbd` dans `initrd`. À cette fin, entrez les deux modules dans le fichier `/etc/sysconfig/kernel` dans les `INITRD_MODULES` et exécutez la commande `mk_initrd`.

20.2.4 JFS

JFS, le "Journaling File System" a été développé par IBM pour AIX. La première version bêta du portage JFS-Linux a été mis à la disposition de la communauté Linux au cours de l'été 2000. La version 1.0.0 a été publiée en 2001. JFS est conçu pour répondre aux attentes des environnements serveur haut débit, car dans ce cas, seule la performance compte. En tant que système de fichiers 64 bits complet, JFS prend en charge les partitions et les fichiers volumineux (LFS ou *Large File Support*), ce qui représente un point positif supplémentaire pour son utilisation dans des environnements serveur.

Une étude plus détaillée de JFS permet de montrer pourquoi ce système de fichiers peut peut-être se révéler la bonne option pour votre serveur Linux :

Journalisation efficace JFS a, à l'instar de ReiserFS, une approche des "métadonnées seulement". Plutôt qu'une vérification complète, seules sont vérifiées les modifications de métadonnées provoquées par de brèves activités du système de fichiers. Cela permet d'économiser énormément de temps lors de la restauration. Les activités simultanées nécessitant plusieurs enregistrements dans le fichier journal peuvent être regroupées dans une opération de validation groupée, ce qui permet de limiter considérablement les baisses de performance du système de fichiers dues aux nombreuses opérations d'écriture.

Gestion efficace des répertoires JFS reste fidèle à différentes structures de répertoires. Pour les petits répertoires, il permet d'enregistrer directement le contenu du répertoire dans son inode. Pour les répertoires plus volumineux, on utilise des arborescences B^+ qui simplifient la gestion des répertoires.

Meilleure utilisation de l'espace disque grâce à l'attribution dynamique des inodes

Sous Ext2, vous devez indiquer à l'avance la densité des inodes (l'espace occupé par les informations de gestion). C'est pour cette raison que le nombre maximum de fichiers ou de données de votre système de fichiers est limité. JFS vous évite ces problèmes — il attribue l'espace des inodes de manière dynamique et le remet à nouveau à disposition s'il n'est pas nécessaire.

20.2.5 XFS

À l'origine conçu comme système de fichiers pour son système d'exploitation IRIX, SGI a commencé le développement de XFS au début des années 90. XFS devait permettre d'obtenir un système de fichiers journalisé 64 bits haute performance qui a évolué en fonction des exigences extrêmes de la période actuelle. XFS est particulièrement bien adapté pour le maniement de gros fichiers et se caractérise par de bonnes performances sur le matériel de pointe. XFS présente cependant une faiblesse. À l'instar de ReiserFS, XFS accorde beaucoup d'importance à l'intégrité des métadonnées et moins à celle des données.

Un bref examen des fonctionnalités clés de XFS permet de comprendre pourquoi il pourrait être un concurrent de poids par rapport aux autres système de fichiers journalisés, pour ce qui concerne le traitement avancé des données.

Évolutivité élevée grâce à l'utilisation de "groupes d'allocation"

Au moment de la création d'un système de fichiers XFS, le périphérique par blocs hébergeant le système de fichiers est divisée en au moins huit domaines linéaires de taille identique, qui sont appelés "groupes d'allocation". Chaque groupe d'allocation gère lui-même les inodes et l'espace libre. On peut en fait considérer les groupes d'allocation comme des "systèmes de fichiers dans le système de fichiers". Comme les groupes d'allocation sont relativement autonomes, le noyau peut s'adresser à plusieurs d'entre-eux simultanément. Et c'est cet aspect qui contribue à l'excellente évolutivité de XFS. Le système des groupes d'allocation autonomes répond ainsi naturellement aux exigences des systèmes multiprocesseurs.

Performances élevées grâce à une gestion efficace de l'espace disque
L'espace libre et les inodes sont gérés par les arborescences B^+ des groupes d'allocation. L'utilisation des arborescences B^+ contribue considérablement aux performances et à l'évolutivité de XFS. L'une des fonctionnalités véritablement unique de XFS est "l'allocation différée". XFS gère l'allocation de l'espace disque en divisant le processus en deux. Une transaction "en suspens" est enregistrée dans la mémoire vive et l'espace disque correspondant réservé. XFS ne décide pas encore précisément où (c'est-à-dire dans quels blocs du système de fichiers) les données vont être enregistrées. Cette décision est repoussée jusqu'au dernier moment. Certaines données de courte durée, temporaires, ne sont ainsi jamais enregistrées sur le disque, car elles sont déjà obsolètes au moment où XFS décide de leur lieu d'enregistrement. C'est ainsi que XFS permet d'améliorer les performances et de limiter la fragmentation du système de fichiers. Comme cependant un classement différé entraîne moins de processus d'écriture que dans les autres systèmes de fichiers, il est probable que la perte de données après une panne qui survient au cours du processus d'écriture est plus importante.

Préallocation pour éviter la fragmentation du système de fichiers
Avant d'écrire les données dans le système de fichiers, XFS réserve l'espace disque nécessaire pour un fichier (préallocation). Cela permet de limiter considérablement la fragmentation du système de fichiers. Les performances sont améliorées, car le contenu des fichiers n'est pas réparti sur la totalité du système de fichiers.

20.3 Autres systèmes de fichiers pris en charge

Le tableau 20.1 page suivante contient d'autres systèmes de fichiers pris en charge par Linux. Ils sont principalement pris en charge pour garantir la compatibilité et l'échange des données entre les différents supports ou avec d'autres systèmes d'exploitation.

TAB. *20.1:* *Types de systèmes de fichiers sous Linux*

cramfs	*Compressed ROM file system* : un système de fichiers avec accès en lecture seulement pour les mémoires mortes.
hpfs	*High Performance File System* : le système de fichiers par défaut de OS/2 — uniquement pris en charge en mode lecture seulement.
iso9660	Système de fichiers standard des cédéroms.
ncpfs	Système de fichiers pour le montage de volumes Novell via le réseau.
nfs	*Network File System* : permet d'enregistrer des données sur n'importe quel ordinateur d'un réseau et de garantir l'accès à ces données en réseau.
smbfs	*Server Message Block* : utilisé par des produits tels que par exemple Windows pour l'accès aux données en réseau.
sysv	utilisé sous SCO UNIX, XENIX et Coherent (systèmes commerciaux UNIX pour PC).
ufs	utilisé par BSD, SunOS et NeXTstep. Pris en charge uniquement en lecture seulement.
umsdos	*UNIX on MSDOS* : installé sur un système de données `fat` (à table d'allocation de fichier) normal. Offre les fonctionnalités d'UNIX (droits, liens, longs noms des fichiers) grâce à la création de fichiers spéciaux.
vfat	*Virtual FAT* : extension du système de fichiers `fat` (prend en charge les longs noms de fichiers).
ntfs	*Windows NT file system* : accès en lecture seulement.

20.4 Prise en charge des gros fichiers sous Linux

À l'origine, Linux prenait en charge des fichiers d'une taille maximale de 2 Go. Le développement de l'utilisation de Linux pour la gestion de bases de données, pour le traitement de données audio et vidéo et bien d'autres encore ont rendu nécessaire d'adapter le noyau et la bibliothèque GNU C (*glibc*) pour la prise en

charge des fichiers de plus de 2 Go. De nouvelles interfaces applicatives ont été mises au point. Aujourd'hui, (presque) tous les principaux systèmes de fichiers proposent une prise en charge LFS, qui permet le traitement avancé des données.

Le tableau 20.2 propose un aperçu des limites actuelles des fichiers et des systèmes de fichiers Linux.

TAB. *20.2:* *Taille maximale des systèmes de fichiers (format sur disque)*

Système de fichiers	Taille maximale des fichiers	Taille maximale du système de fichiers
Ext2 ou Ext3 (Taille des blocs : 1 Ko)	2^{34} (16 Go)	2^{41} (2 To)
Ext2 ou Ext3 (Taille des blocs : 2 Ko)	2^{38} (256 Go)	2^{43} (8 To)
Ext2 ou Ext3 (Taille des blocs : 4 Ko)	2^{41} (2 To)	2^{44} (16 To)
Ext2 ou Ext3 (Taille des blocs : 8 Ko) (Systèmes avec des pages de 8 Ko (comme Alpha))	2^{46} (64 To)	2^{45} (32 To)
ReiserFS 3.5	2^{32} (4 Go)	2^{44} (16 To)
ReiserFS 3.6 (à partir de Linux 2.4)	2^{60} (1 Eo)	2^{44} (16 To)
XFS	2^{63} (8 Eo)	2^{63} (8 Eo)
JFS (Taille des blocs : 512 octets)	2^{63} (8 Eo)	2^{49} (512 To)
JFS (Taille des blocs : 4 Ko)	2^{63} (8 Eo)	2^{52} (4 Po)
NFSv2 (côté client)	2^{31} (2 Go)	2^{63} (8 Eo)
NFSv3 (côté client)	2^{63} (8 Eo)	2^{63} (8 Eo)

Remarque

Limites du noyau Linux

Le tableau décrit les limites du format sur le disque. La taille maximale d'un fichier et d'un système de fichiers pouvant être traités par le noyau correctement, est soumise, sous les noyaux 2.6 aux limites suivantes :

- *Taille de fichier:* les fichiers sur les systèmes de 32 bit ne peuvent pas faire plus de 2 To (2^{41} octet).
- *Systèmes 64 bits :* les systèmes de fichiers peuvent faire jusqu'à 2^{73} octet) ; cette valeur limite n'est pas (encore) atteinte par le matériel actuel.

Remarque

20.5 Pour plus d'informations

Chaque projet de système de fichiers décrit ci-dessus possède son propre site Internet sur lequel vous trouverez des informations extraites de listes de discussion, ainsi que de la documentation additionnelle et des FAQ.

- `http://e2fsprogs.sourceforge.net/ext2.html`
- `http://www.zipworld.com.au/~akpm/linux/ext3/`
- `http://www.namesys.com/`
- `http://oss.software.ibm.com/developerworks/opensource/jfs/`
- `oss.sgi.com/projects/xfs/`

Vous trouverez un cours complet en plusieurs parties sur les systèmes de fichiers Linux, sur le site des *IBM DeveloperWorks* à l'adresse suivante : `http://www-106.ibm.com/developerworks/library/l-fs.html`

Vous trouverez une comparaison des différents systèmes de fichiers journalisés sous Linux réalisée par Juan I. Santos Florido pour la *Linux Gazette* à l'adresse suivante : `http://www.linuxgazette.com/issue55/florido.html`

Vous trouverez un travail complet au sujet de LFS sous Linux sur les pages LFS du site Internet d'Andreas Jaegers à l'adresse suivante : `http://www.suse.de/~aj/linux_lfs.html`

PAM – Pluggable Authentication Modules

PAM (en anglais *Pluggable Authentication Modules*) est utilisé sous Linux pour la communication entre les utilisateurs et les applications lors de l'identification (identification). Les modules PAM sont disponibles centralement et peuvent être appelés de chaque application. Le contenu de ce chapitre a pour but de montrer comment cette identification modulaire se configure et comment elle fonctionne.

Les administrateurs et les développeurs désirent limiter l'accès à des domaines spécifiques du système ou l'utilisation de certaines fonctions d'une application. Sans PAM, il faudrait adapter chaque application à toute nouvelle méthode d'identification (p.ex. LDAP ou Samba). Cette façon de faire coûte cher en temps et augmente les risques d'erreur. L'idée est donc de séparer l'identification de l'application et de la déléguer à un module central: cela permet d'éviter ces inconvénients. Si une nouvelle méthode d'identification doit être mise en oeuvre, il suffit d'adapter ou de développer un module PAM que l'application peut utiliser.

Il existe un fichier de configuration propre pour chaque programme qui utilise PAM, sous Für jedes Programm, das PAM nutzt, liegt eine eigene Konfigurationsdatei `/etc/pam.d/<service>`. On détermine dans ce fichier la liste du ou des modules PAM qui doivent être utilisés pour l'identification des utilisateurs. Une configuration globale de la plupart des modules PAM se trouve sous `/etc/security` et détermine le comportement exact du module concerné (par exemple: `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.conf`, `time.conf` etc). Une application qui utilise un module PAM appelle une séquence de fonctions PAM qui traitent les informations des divers fichiers de configuration et transmettent le résultat à l'application.

21.1 Construction d'un fichier de configuration PAM

Une ligne d'un fichier de configuration PAM se construit à partir d'au plus quatre colonnes:

```
<Type de module> <Fanion de contrôle> <Chemin du module> <Options>
```

Les modules PAM sont traités en pile. Les divers modules ont des tâches différentes. Un module se charge de la vérification des mots de passe, un autre vérifie la provenance d'un accès et un autre interroge des configurations systèmes spécifiques à l'utilisateur.

PAM connaît quatre type de modules:

`auth` Les modules de ce type servent à vérifier si l'utilisateur est authentifié. Cette vérification se fait traditionnellement par une demande de mot de passe, mais peut également s'effectuer par carte à puce ou par des informations biométriques (empreintes digitales, rétinienne, etc).

`account` Les modules de ce type vérifient si l'utilisateur est autorisé à utiliser le service demandé. Par exemple, personne ne devrait pouvoir se connecter à un système alors que son compte a expiré.

`password` Les modules de ce type servent à la modification des données d'identification. Dans la plupart des cas, il s'agit d'un mot de passe.

`session` Les modules de ce type servent à l'administration et à la configuration de sessions utilisateur. Ces modules sont activés avant et après l'identification, de manière à journaliser les tentatives de connexion et à configurer l'environnement de l'utilisateur (chemin d'accès au courrier électronique, répertoire personnel, limites systèmes, etc).

La deuxième section contient un fanion de contrôle qui configure la réaction à l'échec ou la réussite du module:

`required` L'identification ne peut continuer que si le module réussit son exécution. En cas d'erreur lors de l'exécution d'un module `required`, les autres modules sont également exécutés, avant que les utilisateurs ne reçoivent l'information que la tentative d'identification n'a pas aboutit.

`requisite` Les modules doivent réussir leur exécution de la même manière que dans le cas de `required`. Cependant, lors d'une erreur, l'échec est immédiatement communiqué à l'utilisateur sans exécuter d'autres modules. En cas de succès, les modules suivants sont exécutés de la même manière que dans le cas `required`. Ce fanion peut servir de filtre simple, de manière à garantir que toutes les conditions requises pour une identification correcte soient nécessaires.

`sufficient` Si un module de ce type s'exécute avec succès, le programme appelant obtient immédiatement l'information que l'identification a réussi et aucun autre module n'est exécuté, dans la mesure où aucun module précédemment exécuté sans succès ne portait le fanion `required`. Si l'exécution d'un module `sufficient` est sans succès, cela n'a pas de conséquence, les modules suivants sont simplement traités en suivant.

`optional` La réussite ou l'échec n'a pas d'effet. Cette propriété peut être par exemple utilisé pour un module qui informe l'utilisateur de la réception d'e-mail mais n'a pas d'autre effets.

Le chemin du module n'est pas spécifié s'il réside dans le répertoire usuel `/lib/security` (respectivement sous `/lib64/security` pour toutes les versions 64 bits de SUSE LINUX). Comme quatrième colonne, une option peut être passée au module, comme par exemple `debug` (mode de débogage) ou `nullok` (des mots de passe vides sont autorisés).

21.2 La configuration PAM de sshd

Après la théorie de la configuration PAM, vous trouverez ici un exemple pratique, la configuration PAM de sshd:

Exemple 21.1: *Configuration PAM de sshd*

```
#%PAM-1.0
auth required   pam_unix2.so # set_secrpc
auth required   pam_nologin.so
auth required   pam_env.so
account required        pam_unix2.so
account required        pam_nologin.so
password required       pam_pwcheck.so
password required       pam_unix2.so    use_first_pass use_authtok
session required        pam_unix2.so    none     # trace or debug
session required        pam_limits.so
# Enable the following line to get resmgr support for
# ssh sessions (see /usr/share/doc/packages/resmgr/README.SuSE)
#session  optional      pam_resmgr.so fake_ttyname
```

Tout d'abord, sshd appelle les trois modules de type `auth`. Le premier module, `pam_unix2` vérifie le login (nom) et le mot de passe de l'utilisateur à l'aide de `/etc/passwd` et de `/etc/shadow`. Le prochain module (`pam_nologin`) vérifie si le fichier `/etc/nologin` existe. Dans ce cas, à part `root`, aucun utilisateur n'a permission d'accps. Le troisième module, `pam_env`, lit les données du fichier `/etc/security/pam_env.conf` et configure les variables d'environnement spécifiées. Ici se configure par exemple la variable `DISPLAY` à la bonne valeur, car `pam_env` sait d'où l'utilisateur tente de se connecter. La "pile" (en anglais *stack*) du module `auth` est traitée avant que le daemon ssh obtienne un résultat (identification réussie ou non). Tous les modules portent donc un fanion de contrôle `required` et doivent donc être tous traités avant que la réussite soit communiquée à l'sshd abgesetzt wird. En cas d'échec d'un de ces modules, le résultat final communiqué sera négatif, mais sshd ne l'apprendra que lorsque tous les modules de ce type auront été traités.

La pile suivante de module traitée est celle des modules de type `account`. Ces modules vérifient l'autorisation d'accès au service. Ici, les modules `pam_unix2` et `pam_nologin` doivent être à nouveau exécutés avec succès (`required`). Si `pam_unix2` informe que l'utilisateur existe et si `pam_nologin` a vérifié qu'il a le droit de se connecter, le succès est communiqué à sshd et le prochain groupe de modules est attaqué.

Les deux modules suivants appartiennent au type `password` et doivent également être traités avec succès (fanion de contrôle `required`) lorsque l'application change les données d'identification. De manière à changer un mot de passe ou une autre donnée d'identification, la sécurité des données entrées doit être vérifiée. Le module PAM `pam_pwcheck` se charge de faire assurer la sécurité du mot de passe par la bibliothèque cracklib, ce qui permet d'avertir l'utilisateur si le mot de passe choisi par lui n'est pas sûr (trop court, trop simple). Le module déjà connu `pam_unix2` prend les anciens et nouveaux mots de passe de `pam_pwcheck`. L'utilisateur ne doit pas s'identifier à nouveau. De plus, on évite de passer outre les contrôles de `pam_pwcheck`. Les modules de type `password` devraient toujours être exécutés dans la mesure où les modules précédents de type `account` ou `auth` avertissent d'un mot de passe périmé.

Enfin, les modules de type `session` sont appelés, de manière à configurer la session pour cet utilisateur de la façon prévue. Le module `pam_unix2` est appelé à nouveau, sans effet en pratique en raison de l'option `none`. Le module `pam_limits` lit le fichier `/etc/security/limits.conf` et configure les limites d'utilisation de ressources systèmes éventuelles. Lorsque l'utilisateur se déconnecte, les modules de type `session` sont à nouveau appelés.

21.3 Configuration des modules PAM

Le mode d'exécution des modules PAM est configurable. Les fichiers de configurations relatifs se trouvent sous `/etc/security`. Cette section décrit brièvement les fichiers utilisés dans l'exemple de sshd. Ces fichiers sont `pam_unix2.conf`, `pam_env.conf`, `pam_pwcheck.conf` et `limits.conf`.

21.3.1 pam_unix2.conf

Pour l'identification traditionnelle par mot de passe, le module PAM `pam_unix2` est utilisé. Il lit ses données de `/etc/passwd`, `/etc/shadow`, de tables NIS ou NIS+, ou d'une base de données LDAP. On peut configurer ce module soit individuellement dans la configuration PAM de l'application, ou globalement dans `/etc/security/pam_unix2.conf`.

Dans le cas le plus simple, les fichiers ont le contenu suivant:

Exemple 21.2: *pam_unix2.conf*

```
auth:   nullok
account:
password:       nullok
session:        none
```

L'option `nullok`, pour les types de modules `auth` et `password`, signifie que des mots de passe vides sont admis pour ce type de compte. L'utilisateur a le droit de changer les mots de passe. On demande à l'aide de l'option `none` pour le type `session` qu'aucun message ne soit journalisé (configuration standard). Vous pouvez obtenir d'autres options de configuration dans ce fichier ou dans la page de manuel de pam_unix2.

21.3.2 pam_env.conf

Ce fichier peut être utilisé pour donner un environnement standardisé aux utilisateurs, via l'appel du module `pam_env`. La syntaxe de configuration de variables d'environnement est:

```
VARIABLE  [DEFAULT=[valeur]]  [OVERRIDE=[valeur]]
```

`VARIABLE` Désignation de la variable d'environnement qui doit être assignée

`[DEFAULT=[valeur]]` Valeur standard configurée par l'administrateur (utilisée par défaut)

`[OVERRIDE=[valeur]]` Les valeurs qui peuvent être déterminées par `pam_env` et assignées à la place de la valeur standard

Un exemple célèbre de mise en oeuvre de `pam_env` pour l'adaptation de la variable DISPLAY en cas de connexion par réseau:

Exemple 21.3: *pam_env.conf*

```
REMOTEHOST      DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY         DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

La première ligne configure la valeur de la variable `REMOTEHOST` à `localhost`, donc `pam_env` ne peut pas indiquer une autre valeur. La variable `DISPLAY` utilise la valeur de la variable `REMOTEHOST` par défaut. Vous pouvez obtenir plus d'information dans les commentaires situés dans le fichier `/etc/security/pam_env.conf`.

21.3.3 pam_pwcheck.conf

Le module `pam_pwcheck` cherche dans ce fichier les options de tous les modules de type `password`. Les configurations stockées ici sont lues avant celles des configurations de l'application. Si l'application n'a pas de configuration spécifique, les configurations globales sont utilisées. Par exemple:

Exemple 21.4: *pam_pwcheck.conf*

```
password:    nullok blowfish use_cracklib
```

On informe `pam_pwcheck` d'autoriser les mots de passe vide, le chiffrement Blowfish lors de changement de mots de passe et d'assurer le contrôle de la qualité des mots de passe choisis via la bibliothèque cracklib. Vous trouverez plus d'options dans le fichier `/etc/security/pam_pwcheck.conf`.

21.3.4 limits.conf

Le module `pam_limits` configure les limites systèmes pour des utilisateurs ou groupes spécifiques depuis le fichier `limits.conf` aus. Théoriquement, on peut configurer dans ce fichier des limites dures (sans dépassement possible) et molles (faibles: des dépassement temporaires sont possibles), posées sur des ressources systèmes. Vous trouverez des informations sur la syntaxe et les options possibles directement dans le fichier.

21.4 Plus d'informations

Sur votre système, vous trouverez dans le répertoire `/usr/share/doc/packages/pam` les documentations suivantes:

READMEs Au plus haut niveau de ce répertoire se trouvent des READMEs généraux. Dans le sous-répertoire `modules` vous trouverez des READMEs traitant des modules PAM disponibles.

The Linux-PAM System Administrators' Guide
Tout ce qu'un administrateur système doit savoir sur PAM: vous trouverez ici des thèmes comme la syntaxe d'un fichier de configuration PAM ou traitant des aspects de sécurité. Ce document est disponible dans les formats PDF, HTML ou texte.

The Linux-PAM Module Writers' Manual
Vous trouverez ici les informations dont le développeur a besoin pour écrire des modules PAM conformes aux standards. Ce document est disponible dans les formats PDF, HTML ou texte.

The Linux-PAM Application Developers' Guide
Ce document contient tout ce qu'un développeur d'application désireux d'utiliser les bibliothèques PAM doit savoir. Ce document est disponible dans les formats PDF, HTML ou texte.

Une introduction de base à PAM de Thorsten Kukuk est disponible sous `http://www.suse.de/~kukuk/pam/PAM_lt2000/siframes.htm`. Sous `http://www.suse.de/~kukuk/pam/` vous trouverez des informations supplémentaires sur certains modules PAM, qui ont été développés par lui pour SUSE LINUX. (NDT: en allemand, respectivement en anglais!)

Troisième partie

Services

Grands principes de la mise en réseau

Linux, qui a vu le jour en même temps que l'Internet, met à votre disposition toutes les paramétrages et les outils réseau nécessaires à l'intégration dans diverses structures de réseau. Vous trouverez ci-après une présentation du protocole TCP/IP que Linux utilise normalement, de ses services et de ses particularités. Enfin, nous vous expliquerons comment procéder à l'installation d'un accès réseau au moyen d'une carte réseau sous SUSE LINUX avec YaST. Nous vous présentons les principaux fichiers de configuration et quelques-uns des outils les plus importants. Comme la configuration d'un réseau peut-être particulièrement complexe, ce chapitre ne présente que les principaux mécanismes.

22.1 TCP/IP – Introduction

Linux et les autres systèmes d'exploitation Unix utilisent le protocole TCP/IP. Il s'agit plus particulièrement d'une famille de protocoles offrant des services totalement différents. Le protocole TCP/IP a été développé à partir d'une application militaire et défini, dans sa forme actuelle, vers 1981, dans ce que l'on appelle un RFC (appel à commentaires). On entend par RFC (en anglais, *Request for comments*) un document qui décrit les différents protocoles Internet et la marche à suivre pour les implémenter dans un système d'exploitation et des applications. Vous pouvez accéder directement à ces documents RFC sur le Web à l'adresse suivante : `http://www.ietf.org/`. Quelques améliorations ont entre-temps été apportées au protocole TCP/IP, mais le protocole d'origine n'a pas été modifié de manière considérable depuis 1981.

Remarque

Les documents RFC décrivent la construction des protocoles Internet. Si vous souhaitez approfondir vos connaissances au sujet d'un protocole particulier, le seul document de référence est le document RFC correspondant : `http://www.ietf.org/rfc.html`

Remarque

Les services énumérés dans le tableau 22.1 permettent d'échanger des données entre deux ordinateurs fonctionnant sous Linux au moyen de TCP/IP :

TAB. 22.1: *Différents protocoles de la famille de protocoles TCP/IP*

Protocole	Description
TCP	(en anglais *Transmission Control Protocol*). Un protocole sécurisé, orienté connexion. Les données à transmettre sont, du point de vue de l'application, envoyées sous forme de flux de données et c'est le système d'exploitation lui-même qui les met au format de transport adapté. Les données arrivent dans l'application cible, sur l'ordinateur cible, exactement sous la forme du flux de données dans lequel elles ont été envoyées. Le protocole TCP permet de garantir qu'aucune donnée ne soit perdue ou n'arrive dans le désordre. Ce protocole est utilisé quand l'ordre des données est important et que le terme 'connexion' a un sens.

UDP	(en anglais, *User Datagram Protocol*). Un protocole sans connexion, non sécurisé. Les données à transmettre sont envoyées par paquets, ces paquets de données étant générés, au préalable, par l'application. L'ordre d'arrivée des données chez le destinataire n'est pas garanti et il se peut aussi que certains paquets de données soient perdus. Le protocole UDP est particulièrement adapté pour les applications orientées trames et se caractérise par des temps morts inférieurs à ceux du protocole TCP.
ICMP	(en anglais, *Internet Control Message Protocol*) C'est un protocole qui ne s'adresse en général pas à l'utilisateur, il s'agit plutôt un protocole de contrôle spécial qui transmet les états d'erreur et qui peut piloter le comportement de l'ordinateur en charge de la transmission de données TCP/IP. Le protocole ICMP propose, en outre, un mode écho spécial que vous pouvez tester avec le programme ping.
IGMP	(en anglais, *Internet Group Management Protocol*) Ce protocole contrôle le comportement des ordinateurs dans le cadre de la multidiffusion IP. Nous ne pourrons malheureusement pas aborder le sujet de la multidiffusion IP dans cet ouvrage.

Presque tous les protocoles matériel sont orientés paquets. Les données à transmettre doivent être placées dans de "petits paquets" et ne peuvent pas être envoyées "en une fois". C'est pour cette raison que le protocole TCP/IP utilise aussi de petits paquets de données. La taille maximale d'un paquet TCP/IP est d'environ 64 Ko. En pratique, les paquets sont généralement plus petits, dans la mesure où le matériel réseau est le facteur limitatif. Ainsi la taille maximale autorisée d'un paquet de données sur Ethernet est de 1 500 octets. C'est donc pour cette raison que la taille des paquets TCP/IP est limitée lorsque les données sont envoyées sur un réseau Ethernet. Lorsque l'on souhaite transmettre davantage de données, le système d'exploitation doit également envoyer davantage de paquets de données.

22.1.1 Modèle en couches

Le protocole IP (en anglais, *Internet Protocol*) permet la transmission non sécurisée de données. Le protocole TCP (en anglais,*Transmission Control Protocol*) n'est, pour ainsi dire, qu'un complément venant se greffer sur IP pour garantir une transmission sécurisée des données. IP est, d'autre part, un complément venant se greffer lui-même sur le protocole dépendant du matériel sous-jacent, par exemple Ethernet. Les spécialistes parlent alors d'un "modèle en couches". Reportez-vous à l'illustration 22.1.

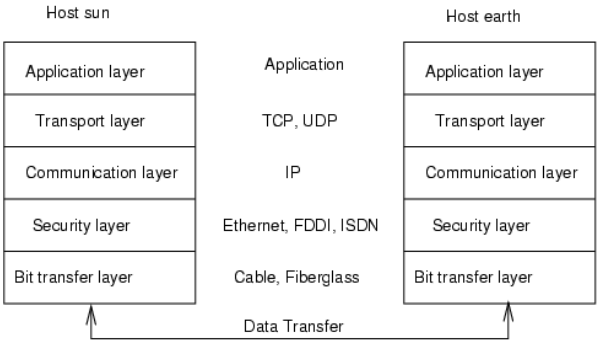


FIG. 22.1: *Modèle en couches de TCP/IP simplifie*

L'illustration montre un ou deux exemples pour chaque couche. Comme vous pouvez le voir, les couches sont classées par "niveau d'abstraction", la couche inférieure étant la plus proche du matériel. La couche supérieure, en revanche, fait pratiquement intégralement abstraction du matériel sous-jacent. Chacune des couches a une fonction bien particulière, déjà décrite en grande partie par son nom. C'est ainsi que le réseau utilisé (par exemple Ethernet) est représenté par la couche physique et par la couche liaison.

- Pendant que la couche 1 prend en charge des éléments aussi variés que les types de câble, les formes des signaux, le codage des signaux et autres, la couche 2 est responsable du processus d'accès (quel ordinateur a le droit d'envoyer des données et quand ?) et de la correction des erreurs. La couche 1 est appelée *couche physique*.

- La couche 3 au contraire, la *couche réseau*, est responsable de la transmission de données sur de longues distances. La couche réseau garantit que les données, même en cas de longues distances, parviennent au destinataire voulu et peuvent être distribuées.
- La couche 4, la *couche transport*, est responsable des données de l'application et garantit que les données arrivent dans l'ordre approprié et ne sont pas perdues. La couche liaison n'est responsable que du fait que les données qui arrivent sont correctes. C'est la *couche transport* qui assure une protection contre la "perte" de données.
- Enfin, la couche 5 concerne le traitement des données par l'application même.

Pour que chacune de ces couches puisse exécuter la tâche qui lui revient, des informations supplémentaires relatives à chaque couche doivent être enregistrées dans les paquets de données, au niveau de l'*en-tête*. Chacune des couches dispose d'un petit bloc de données, appelé "en-tête de protocole" (en anglais, *Protocol header*) qui se trouve avant le paquet en formation. Observons un paquet de données TCP/IP quelconque en route sur un câble Ethernet. Il se présente comme sur l'image 22.2.

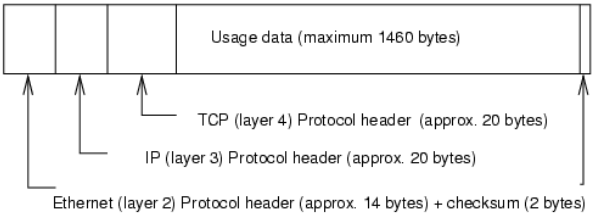


FIG. 22.2: *Paquet TCP/IP sur Ethernet*

Comme vous pouvez le voir, le monde est loin d'être aussi simple qu'on le voudrait. La somme de contrôle de la couche liaison se trouve à la fin du paquet et pas au début. Cela représente toutefois une simplification pour le matériel réseau. La quantité maximale de données utilisées dans un paquet s'élève, dans un réseau Ethernet, à 1 460 octets.

Ainsi, si une application souhaite envoyer des données sur le réseau, les données passent au travers des différents niveaux de couches mis en œuvre dans le noyau Linux (à l'exception de la couche 1 : la carte réseau). Chacune des couches est responsable de préparer les données de manière à ce qu'elles puissent être transmises à la couche sous-jacente. La couche la plus basse est, au final, responsable

de l'envoi des données à proprement parler. Lors de la réception, le processus inverse se produit. Un peu comme pour les différentes peaux d'un oignon, les en-têtes de protocole de chaque couche sont retirés, au fur et à mesure, des données utiles. La couche 4 est, au final, responsable de la préparation des données pour l'application sur l'ordinateur cible. C'est pour cette raison qu'une couche ne communique jamais qu'avec la couche directement au-dessus ou en dessous d'elle. Le fait que les données sont transmises par un réseau FDDI 100 Mbit/s ou une connexion 56 Kbit/s n'a donc que très peu d'importance. A l'inverse, peu importe pour la connexion de données, quelles données sont effectivement envoyées, dans la mesure où elle sont correctement empaquetées.

22.1.2 Adresses IP et routage

Remarque

Les sections suivantes présentent les réseaux IPv4. Vous trouverez des informations sur son successeur, le protocole IPv6, dans la section *IPv6 – L'Internet de la nouvelle génération* page 447.

Remarque

Adresses IP

Chaque ordinateur de l'Internet possède une adresse 32 bits unique. Ces 32 bits (soit 4 octets) se présentent normalement comme dans la seconde ligne de l'exemple 22.1.

Exemple 22.1: *Structure d'une adresse IP*

```
Adresse IP  (binaire) :  11000000 10101000 00000000 00010100
Adresse IP (décimale) :      192.     168.       0.      20
```

Les quatre octets sont séparés par un point lorsqu'ils sont écrits dans le système décimal. L'adresse IP est associée à un ordinateur ou à une interface réseau, elle ne peut donc être utilisée nulle part ailleurs dans le monde. Certes il existe des exceptions à cette règle, mais elles n'ont aucune influence sur les considérations suivantes.

La carte Ethernet aussi possède une adresse non équivoque, appelée adresse *MAC* (en anglais, *Media Access Control*). Cette adresse fait 48 bits de long, est unique dans le monde entier et est enregistrée physiquement par le fabricant, directement sur la carte réseau. L'attribution de l'adresse par le fabricant présente toutefois un inconvénient non négligeable : les adresses *MAC* ne constituent pas un système hiérarchique, mais sont au contraire plus ou moins réparties de manière aléatoire. Elles ne peuvent donc pas servir à adresser un ordinateur distant. L'adresse *MAC* joue en revanche un rôle décisif lors de la communication entre les ordinateurs d'un réseau local (il s'agit de l'élément principal de l'en-tête de protocole de la couche 2).

Revenons aux adresses IP : les points suggèrent que les adresses IP constituent un système hiérarchique. Jusque dans les années 90, les adresses IP étaient réparties en classes, de manière fixe. Ce système s'est toutefois révélé particulièrement rigide et c'est pour cette raison que l'on a abandonné cette répartition. On utilise désormais un "routage ne faisant pas appel à des classes" (CIDR (en anglais, *Classless Inter Domain Routing*)).

Masques réseau et routage

Comme l'ordinateur avec l'adresse IP 192.168.0.0; ne peut tout simplement pas savoir où se trouve l'ordinateur avec l'adresse IP 192.168.0.20, il a fallu introduire les masques réseau.

Pour simplifier, les masques de (sous)-réseau définissent, sur un ordinateur disposant d'une adresse IP, ce qui se trouve "à l'intérieur" et ce qui se trouve "à l'extérieur". Les ordinateurs qui se trouvent "à l'intérieur" (les spécialistes disent : "sur le même sous-réseau"), peuvent être adressés directement. Les ordinateurs qui se trouvent "à l'extérieur" ("pas sur le même sous-réseau"), doivent être adressés par l'intermédiaire d'une passerelle ou d'un routeur. Comme chaque interface réseau est susceptible de posséder sa propre adresse IP, vous imaginez comme tout cela peut vite devenir compliqué.

Voilà ce qui se produit, avant l'envoi d'un paquet sur le réseau : on combine l'adresse cible et le masque réseau au moyen d'un ET binaire. Après cela, on combine aussi l'adresse source et le masque réseau au moyen d'un ET binaire (reportez-vous au tableau 22.2 page suivante). Lorsque plusieurs interfaces réseau sont disponibles, toutes les adresses d'envoi possibles sont, en règle générale, vérifiées.

Les résultats des combinaisons au moyen de ET binaires sont comparés. Si les résultats sont rigoureusement identiques, cela signifie que l'ordinateur cible se trouve dans le même sous-réseau. Dans le cas contraire, il doit être adressé par l'intermédiaire d'une passerelle. Cela signifie, que plus il y a de bits "1" dans le masque réseau, moins il est possible d'adresser de machines directement et qu'il faut donc passer systématiquement par une passerelle. Vous pouvez consulter, à titre d'illustration, les différents exemples 22.2.

Exemple 22.2: *Rattachements des adresses IP avec le masque réseau*

```
Adresse IP (192.168.0.20) :     11000000 10101000 00000000 00010100
Masque réseau (255.255.255.0) : 11111111 11111111 11111111 00000000
_____________________________________________________________________
Résultat (binaire) :            11000000 10101000 00000000 00000000
Résultat (décimal) :                 192.     168.       0.       0
Adresse IP (213.95.15.200) :    11010101 10111111 00001111 11001000
Masque réseau (255.255.255.0) : 11111111 11111111 11111111 00000000
---------------------------------------------------------------------
Résultat (binaire) :            11010101 10111111 00001111 00000000
Résultat (décimal) :                 213.      95.      15.       0
```

Les masques réseau – à l'instar des adresses IP – s'écrivent également sous forme de nombres décimaux, séparés par des points. Comme le masque réseau est également une valeur 32 bits, on l'exprime également sous la forme d'une suite de quatre valeurs décimales. C'est l'utilisateur qui doit indiquer quelle passerelle ou quel domaine d'adresses sont accessibles par l'intermédiaire de quelle interface réseau.

Un autre exemple : tous les ordinateurs raccordés au même câble Ethernet se trouvent, en règle générale, *sur le même sous-réseau* et sont directement accessibles. Même si le brin Ethernet est segmenté par des commutateurs ou des ponts, ces ordinateurs demeurent toujours directement accessibles.

Si vous souhaitez parcourir une plus longue distance, la technologie Ethernet économique n'est alors plus appropriée. Vous devez alors confier les paquets IP à d'autres types de matériels (par exemple FDDI ou RNIS). Des appareils de ce type s'appellent des routeurs ou des passerelles. Une machine Linux peut bien entendu aussi se charger de ce genre de tâches, grâce à l'option `ip_forwarding`.

Lorsqu'au moins une passerelle est configurée, le paquet IP est envoyé à la passerelle appropriée. Cette dernière essaie alors de nouveau d'envoyer ce paquet selon le même schéma. Et ce processus se reproduit sur chaque ordinateur autant de fois que nécessaire, jusqu'à ce que le paquet ait atteint l'ordinateur cible ou que sa "durée de vie" TTL (en anglais, *time to live*) soit écoulée.

TAB. 22.2: *Adresses spéciales*

Type d'adresse	Description
Adresse de base du réseau	Il s'agit du masque réseau ET d'une adresse quelconque du réseau, ce qui est illustré par l'exemple 22.2 page ci-contre sous `Résultat`. Cette adresse ne peut être attribuée à aucun ordinateur.
Adresse de diffusion (*broadcast*)	Elle signifie : "s'adresser à tous les ordinateurs de ce sous réseau". Pour la produire, le masque réseau est inversé binairement et combiné à l'adresse de base réseau avec un OU. L'exemple ci-dessus permet donc d'obtenir 192.168.0.255. Bien entendu, cette adresse ne peut non plus être attribuée à aucun ordinateur.
Hôte local	L'adresse `127.0.0.1` est attribuée, sur chaque ordinateur, de manière fixe, à ce que l'on appelle le "dispositif de bouclage". Cette adresse peut permettre d'établir une connexion avec l'ordinateur lui-même.

Comme les adresses IP doivent être uniques à l'échelle mondiale, vous ne pouvez naturellement pas inventer des adresses quelconques. Mais pour que vous puissiez tout de même mettre au point un réseau IP, il existe trois domaines d'adresses que vous pouvez utiliser sans plus de formalités. Vous ne pouvez pas les utiliser telles quelles sur l'Internet, car ces adresses ne sont pas acheminées sur l'Internet.

Il s'agit donc des domaines d'adresses définis dans le document RFC 1597 :

TAB. 22.3: *Domaines d'adresses IP privés*

Réseau/Masque réseau	Domaine
`10.0.0.0/255.0.0.0`	`10.x.x.x`
`172.16.0.0/255.240.0.0`	`172.16.x.x - 172.31.x.x`
`192.168.0.0/255.255.0.0`	`192.168.x.x`

22.1.3 Résolution de noms (Domain Name System – DNS)

Le DNS est utilisé pour que vous n'ayez pas besoin de vous souvenir de toutes les adresses IP. Le DNS permet d'associer une adresse IP à un ou plusieurs noms et à l'inverse un nom à une adresse IP. Sous Linux, cette conversion est assurée par un logiciel spécial appelé bind. L'ordinateur qui réalise ensuite cette conversion s'appelle le *serveur de noms*. Les noms constituent alors un système hiérarchique dans lequel les composants individuels du nom sont séparés par des points. La hiérarchie de noms est toutefois indépendante de la hiérarchie des adresses IP décrite précédemment.

Examinons un instant un nom complet, par exemple `laurent.suse.de` écrit au format `nomhôte.domaine`. Un nom complet – les experts parlent de "nom pleinement qualifié" (*Fully Qualified Domain Name* ou en abrégé *FQDN*) est composé d'un nom d'hôte et d'une partie correspondant au domaine, qui est construite à partir d'une portion que l'on peut choisir librement – dans l'exemple ci-dessus `suse` – et du *domaine de premier niveau* (*Top Level Domain*, *TLD*).

Pour des raisons historiques, l'attribution des TLD est quelque peu déconcertante. Ainsi, on utilise aux États-Unis des TLD classiques de trois lettres, tandis que partout ailleurs on utilise les désignations de pays ISO composées de deux lettres ; depuis 2000, on dispose de TLD supplémentaires pour des domaines spéciaux qui, en partie, comptent plus de trois lettres (par exemple `.info`, `.name`, `.museum`, etc.).

Aux débuts de l'Internet (avant 1990), il existait à cet effet un fichier `/etc/hosts`, dans lequel étaient enregistrés tous les noms des ordinateurs présents sur l'Internet. Ceci s'est révélé rapidement impraticable en raison de la croissance extrêmement rapide du nombre d'ordinateurs connectés à l'Internet. C'est pour cette raison que l'on a mis en place une base de données décentralisée qui peut stocker les noms d'ordinateurs de manière distribuée. Cette base de données répartie sur les serveurs de noms ne contient pas toutes les données de tous les ordinateurs présents sur l'Internet, mais peut faire suivre à d'autres serveurs de noms des demandes qui lui sont adressées.

Tout en haut de la hiérarchie, on trouve les "serveurs de noms racine" *Root-Nameserver*, qui gèrent les domaines de premier niveau. Les serveurs de noms racine sont gérés par le Network Information Center (*NIC*). Le serveur de noms racine connaît les serveurs de noms responsables pour un domaine de premier niveau. Dans le cas du domaine de premier niveau allemand `de`, le NIC DE est responsable des domaines qui se terminent par `de`. Pour plus d'informations sur le NIC DE, consultez le site web `http://www.denic.de`, pour plus d'informations sur le NIC des domaines de premier niveau, consultez `http://www.internic.net`.

Pour que votre ordinateur soit également capable de convertir un nom en adresse IP, il doit au moins connaître l'adresse IP d'un serveur de noms. YaST vous permet de configurer facilement un serveur de noms. Si vous utilisez une connexion par modem, il se peut que le protocole utilisé pour la connexion indique l'adresse du serveur de noms dès l'établissement de la connexion.

Non seulement le DNS permet de résoudre des noms d'ordinateurs, mais est capable de beaucoup plus. Ainsi, le serveur de noms "sait" aussi quel ordinateur prend en charge les messages électroniques pour tout un domaine, ce que l'on appelle le serveur de messagerie *Mail exchanger (MX)*.

Vous trouverez une description de la configuration sous SUSE LINUX de l'accès au serveur de noms à la section *DNS – Domain Name System* page 487.

Le protocole `whois` est intimement lié au DNS. Vous pouvez utiliser le programme du même nom, whois, pour retrouver rapidement le responsable d'un domaine donné.

22.2 IPv6 – L'Internet de la nouvelle génération

Avec l'invention du WWW (en anglais, *World Wide Web*), l'Internet et donc le nombre d'ordinateurs qui "comprennent" le TCP/IP ont connu une croissance exponentielle. Depuis l'invention du WWW par Tim Berners-Lee en 1990 au CERN (`http://public.web.cern.ch/`), le nombre des hôtes Internet est passé de quelques milliers à environ 100 millions.

Comme vous le savez déjà, une adresse IP ne contient "que" 32 bits. De nombreuses adresses IP ne peuvent, pour des raisons organisationnelles, pas être utilisées et sont donc perdues. Rappel : l'Internet est divisé en sous-réseaux. Ces derniers comprennent toujours une puissance de deux moins deux adresses IP utilisables. Un sous-réseau se compose alors, par exemple de 2, 6, 14, 30, etc. adresses IP. Si vous souhaitez par exemple connecter 128 ordinateurs à l'Internet, vous aurez donc besoin d'un sous-réseau comportant 256 adresses IP, dont 254 sont utilisables. Comme vous l'avez vu plus haut, deux adresses IP du sous-réseau disparaissent, à savoir l'adresse de diffusion et l'adresse de base du réseau.

Pour atténuer la pénurie prévisible d'adresses, on utilise sous le protocole IPv4 momentanément utilisé des mécanismes tels que le DHCP ou le NAT (en anglais, *Network Address Translation*). Ces deux processus permettent d'atténuer, avec la convention des domaines d'adresses privés et publics le besoin urgent d'adresses Internet. L'inconvénient de ces méthodes est qu'elles sont relativement compliquées à configurer et nécessitent une maintenance considérable. Elles impliquent de connaître, pour la configuration correcte d'un ordinateur sur un réseau IPv4, de nombreuses informations, notamment, sa propre adresse IP, son masque de sous-réseau, l'adresse de la passerelle et impérativement un serveur de noms. Vous devez "connaître" toutes ces informations et ne pouvez les déduire d'aucune autre donnée.

Avec IPv6, la pénurie d'adresses et les configurations complexes appartiennent désormais au passé. Vous allez, dans les sections suivantes, en apprendre davantage sur les nouveautés et les avantages d'IPv6 et sur le passage de l'ancien protocole au nouveau.

22.2.1 Avantages d'IPv6

L'avantage le plus important et le plus évident de ce nouveau protocole est qu'il augmente de façon énorme l'espace d'adresses disponibles. Une adresse IPv6 comprend 128 bits contre 32 bits jusqu'alors. On dispose alors de plusieurs milliards (!) d'adresses IP.

Les adresses IPv6 diffèrent des anciennes, non seulement par leur longueur, mais également par leur structure interne différente et permettent de coder des informations spéciales relatives au système correspondant et à son réseau. Vous trouverez plus d'informations à ce sujet, à la section *Le système d'adresses d'IPv6* page 450.

D'autres avantages significatifs du nouveau protocole, en bref :

Auto-configuration IPv6 transpose le principe du "Plug and Play" au réseau. Un système fraîchement installé s'intègre, sans qu'aucune configuration supplémentaire ne soit nécessaire, au réseau (local). Le mécanisme d'auto-configuration du terminal déduit sa propre adresse des informations qui lui sont communiquées par les routeurs voisins via le protocole ND "Neighbor Discovery Protocol". Ce processus ne nécessite aucune intervention de l'administrateur et présente, par rapport au distributeur d'adresses DHCP utilisé sous IPv4, l'avantage supplémentaire de supprimer le besoin de maintenir un serveur central des adresses disponibles.

Mobilité IPv6 permet d'associer à une interface réseau plusieurs adresses simultanées. Vous disposez ainsi, en tant qu'utilisateur d'un système, facilement et sans configuration supplémentaire, d'un accès à plusieurs réseaux différents. On peut comparer cette fonction aux utilisateurs "itinérants" des les réseaux de radiotéléphonie. Si vous êtes à l'étranger avec votre téléphone mobile, votre téléphone se connecte automatiquement sur le réseau local. Où que vous soyez, vous êtes assuré d'être toujours joignable via votre numéro de téléphone normal et vous utilisez le réseau étranger pour téléphoner comme s'il s'agissait de votre réseau habituel.

Une communication sûre Des communications sécurisées étaient certes disponibles sous IPv4, mais uniquement en faisant appel à des outils complémentaires, IPSec et donc la communication sécurisée entre deux systèmes via un tunnel traversant l'Internet non sécurisé sont désormais compris dans IPv6.

Compatibilité avec l'existant On ne peut pas envisager de façon réaliste de faire passer tout l'Internet d'IPv4 à IPv6. Il est donc important que les deux versions puissent cohabiter sur l'Internet et sur un même système. La coexistence de ces deux protocoles sur l'Internet est garantie par l'utilisation d'adresses compatibles (les adresses IPv4 se transforment facilement en adresses IPv6) et l'utilisation de différents "tunnels" (reportez-vous à la section *IPv4 par rapport à IPv6 – passer d'un monde à l'autre* page 454). La "double pile IP" (*Dual Stack IP*) permet de prendre en charge des deux protocoles sur un seul système. Chacun des deux protocoles utilise sa propre pile réseau de manière à ce que les deux versions de protocoles ne se télescopent pas.

La multidiffusion – une offre de service sur mesure
Si avec IPv4, certains services (par exemple SMB) devaient diffuser leurs paquets à tous les membres du réseau local, on dispose d'un processus très différent avec IPv6. Grâce à la multidiffusion, il est possible de s'adresser à un groupe d'ordinateurs en une seule fois : pas à tous les ordinateurs simultanément ("diffusion" – *broadcast*), ou à un seul uniquement ("envoi ciblé" – *unicast*), mais par exemple à quelques-uns d'entre eux. C'est l'application qui détermine les ordinateurs en question. Il existe toutefois quelques groupes de multidiffusion bien définis, tels que "tous les serveurs de noms" (en anglais, *all nameservers multicast group*) ou "tous les routeurs" (en anglais, *all routers multicast group*).

22.2.2 Le système d'adresses d'IPv6

Comme nous l'avons déjà évoqué, le protocole IP utilisé jusqu'à présent présentait deux inconvénients non négligeables. Tout d'abord, on dispose de moins en moins d'adresses IP disponibles et ensuite, la configuration du réseau et la gestion des tables de routage est de plus en plus compliquée et nécessite une maintenance toujours plus importante. IPv6 s'est attaqué au premier problème en étendant l'espace d'adressage à 128 bits. La solution du deuxième problème réside dans la structure d'adresse hiérarchique, dans les mécanismes conçus pour l'attribution des adresses au sein d'un réseau et dans la possibilité de "rattachement multiple" (en anglais, *multi-homing*, plusieurs adresses par interface avec accès à différents réseaux).

En ce qui concerne IPv6, vous devez pouvoir distinguer trois types d'adresses :

unicast (à un seul destinataire) Les adresses de ce type appartiennent à une seule interface réseau. Les paquets possédant une adresse de ce type sont livrés à un seul destinataire. Les adresses de diffusion individuelle sont utilisées pour adresser des ordinateurs individuels du réseau local ou sur l'Internet.

multicast (à plusieurs destinataires) Les adresses de ce type représentent un groupe d'interfaces. Les paquets possédant une adresse de ce type sont envoyés à tous les destinataires membres de ce groupe. Les adresses de multidiffusion sont, pour la plupart, utilisées par des services réseau particuliers, pour adresser des groupes particuliers ciblés d'ordinateurs.

anycast (pour tout les destinataires) Les adresses de ce type représentent un groupe d'interfaces. Les paquets possédant une adresse de ce type sont livrés aux membres du groupe qui est le plus "proche" de l'expéditeur au sens du protocole de routage utilisé. Les adresses anycast sont utilisées pour permettre aux terminaux de trouver un serveur proposant un service donné dans leur domaine réseau. Tous les serveurs d'un type donné possèdent la même adresse anycast. Si le terminal demande un service, c'est le serveur le plus proche de l'hôte, selon l'évaluation du protocole de routage, qui répond. En cas d'indisponibilité de ce serveur, c'est le deuxième plus proche qui est alors utilisé ….

Structure d'une adresse IPv6

Une adresse IPv6 se compose de huit blocs de 16 bits chacun, séparés par `:` (deux-points) et représentés en écriture hexadécimale. On peut omettre les octets nuls de tête dans un groupe, mais pas ceux qui se trouvent au milieu ou à la fin d'un groupe. On peut représenter plus de quatre octets nuls qui se suivent par le signe d'omission `::`. Toutefois on ne peut utiliser qu'un seul signe d'omission dans une adresse. Ce processus d'omission est appelé en anglais "collapsing". L'exemple 22.3 illustre ce processus à l'aide de trois modes d'écriture équivalents pour la même adresse.

Exemple 22.3: *Exemple d'adresse IPv6*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                            : 10 : 1000 : 1a4
```

Chaque partie d'une adresse IPv6 a une signification particulière. Les premiers octets constituent un préfixe et indiquent le type de l'adresse. La partie centrale adresse un réseau ou n'a pas de signification particulière et la fin de l'adresse indique la partie hôte. Les masques réseau se définissent sous IPv6 par la longueur du préfixe indiquée par un `/` à la fin de l'adresse. Une adresse représentée comme dans l'exemple 22.4 signifie que les 64 derniers bits constituent la partie hôte et les 64 bits du début la partie réseau de l'adresse. Autrement dit, le nombre `64` indique que le masque réseau est rempli de bits 1 à partir de la gauche. Il y a donc dans le masque réseau 64 bits 1. Comme avec IPv4, on combine avec ET le masque réseau et l'adresse IP pour déterminer si l'ordinateur se trouve dans le même sous-réseau ou un autre.

Exemple 22.4: *Adresse IPv6 avec indication du préfixe*

```
fe80::10:1000:1a4/64
```

IPv6 reconnaît différents préfixes avec différentes significations (reportez-vous au tableau 22.4 page suivante).

TAB. 22.4: *Différents préfixes IPv6*

Préfixe (hexadécimal)	Utilisation
`00`	Les adresses IPv4 et les adresses de compatibilité IPv4/IPv6. Il s'agit d'une adresse compatible IPv4. Un routeur approprié doit convertir le paquet IPv6 en IPv4. D'autres adresses spéciales (par exemple dispositif de bouclage *loopback*) possèdent également ce préfixe.
premier chiffre `2` ou `3`	(en anglais, *Aggregatable Global Unicast Address*). Comme auparavant, vous pouvez aussi obtenir avec IPv6 des réseaux partiels. On dispose, à l'heure actuelle, des espaces d'adresses suivants : `2001::/16` (*production quality address space*, *espace d'adressage de production*), `2002::/16` (*6to4 address space*, *espace d'adressage 6vers4*).
`fe80::/10`	(en anglais, *link-local*) Les adresses avec ce préfixe ne peuvent pas être routées et ne peuvent donc être jointes qu'à l'intérieur du même sous-réseau.
`fec0::/10`	(en anglais, *site-local*) Ces adresses peuvent certes être routées, mais uniquement au sein d'une organisation. C'est pour cette raison que ces adresses correspondent aux réseaux jusqu'alors "privés" (exemple : `10.x.x.x`).
`ff`	(en anglais, *multicast*) Les adresses IPv6 qui commencent par `ff` sont des adresses de multidiffusion.

Les adresses d'envoi ciblé respectent un principe de construction en trois parties :

Topologie publique La première partie qui comprend, entre autres, l'un des préfixes présentés précédemment, sert au routage du paquet sur l'Internet public. C'est dans cette partie que les informations relatives au fournisseur d'accès ou à l'institution sont codées pour préparer l'accès au réseau.

Topologie du site La deuxième partie contient des informations de routage relatives au sous-réseau qui doit distribuer le paquet.

Identificateur de l'interface La troisième partie identifie clairement l'interface à laquelle le paquet est adressé. Cela permet ainsi d'utiliser l'adresse MAC en tant que composant de l'adresse. Comme cette adresse est unique dans

le monde entier et attribuée par le fabricant du matériel, la configuration de l'ordinateur est considérablement simplifiée. En réalité, les 64 premiers bits sont rassemblés en une unité lexicale `EUI-64`. Parallèlement, les derniers 48 bits de l'adresse MAC sont retirés et les derniers 24 bits contiennent des informations spéciales indiquant le type de l'unité lexicale. Cela permet aussi d'attribuer des unités lexicales `EUI-64` à des appareils ne disposant pas d'adresse MAC (connexions PPP et RNIS).

De cette structure de base, on déduit cinq types différents d'adresses unicast :

`::` (non spécifié) Un ordinateur utilise cette adresse comme adresse source s'il s'agit de la première initialisation de son interface réseau et qu'il ne possède pas encore d'informations sur son adresse.

`::1` (bouclage) Adresse du dispositif de bouclage.

Adresse compatible IPv4 L'adresse IPv6 est tirée de l'adresse IPv4 et d'un préfixe de 96 bits 0 au début de l'adresse. C'est ce type d'adresses de compatibilité que l'on utilise pour la tunnelisation (reportez-vous à la section *IPv4 par rapport à IPv6 – passer d'un monde à l'autre* page suivante). Les hôtes IPv4/IPv6 peuvent ainsi communiquer avec d'autres se trouvant dans un réseau IPv4 pur.

Adresse IPv4 avec équivalent IPv6 Ce type d'adresse indique l'adresse IPv6 d'un ordinateur IPv4 pur.

Adresses locales Il existe deux types d'adresses pour une utilisation purement locale :

link-local Ce type d'adresse est exclusivement conçu pour une utilisation dans le sous-réseau local. Les routeurs n'ont pas le droit de transmettre sur l'Internet ou à d'autres sous-réseaux les paquets dont l'adresse cible ou source est de ce type. Ces adresses se caractérisent par un préfixe spécial (`fe80::/10`) et l'identificateur d'interface de la carte réseau. La partie centrale de l'adresse est composée d'octets nuls non significatifs. Les méthodes d'auto-configuration utilisent ce type d'adresse pour s'adresser à des ordinateurs du même sous-réseau.

site-local Ce type d'adresse peut être routé entre différents sous-réseaux mais ne pas parvenir à l'extérieur d'une organisation (en anglais, *site*) sur l'Internet. Ces adresses sont utilisées pour les intranets et sont équivalentes des adresses privées d'IPv4. Ces adresses comportent, en plus d'un préfixe particulier (`fec0::/10`) et de l'identificateur de l'interface, un champ de 16 bits dans lequel l'identificateur du sous-réseau est codé. Le reste est à nouveau comblé par des octets nuls.

IPv6 utilise également une nouvelle invention. Plusieurs adresses IP sont généralement attribuées à une interface réseau, l'avantage étant que plusieurs réseaux différents sont disponibles. Chacun d'entre eux peut, à l'aide de l'adresse MAC et d'un préfixe connu, se transformer en un réseau configuré entièrement automatiquement, afin que tous les ordinateurs du réseau local soient accessibles directement après le démarrage d'IPv6 sans que cela ne nécessite de travaux de configuration supplémentaires au moyen d'adresses dites "link-local"). L'adresse MAC en tant que composante de l'adresse IP permet de distinguer chacune de ces adresses au niveau mondial. Seules les parties "topologie du site" ou "topologie publique" peuvent varier selon le réseau dans lequel l'ordinateur se trouve actuellement.

Si un ordinateur se "déplace" entre plusieurs réseaux, il a besoin d'au moins deux adresses. L'une, son "adresse personnelle" (*home address*), contient outre l'identificateur de l'interface, des informations relatives à son réseau d'exploitation d'origine et le préfixe correspondant. L'"adresse personnelle" est statique et n'est pas modifiée. Tous les paquets adressés à cet ordinateur lui sont transmis, qu'il se trouve sur son propre réseau ou sur un réseau étranger. La distribution sur le réseau étranger est prise en charge par des nouveautés essentielles du protocole IPv6, notamment l'"auto-configuration sans état" et la "découverte de voisins". L'ordinateur mobile possède, outre son "adresse personnelle", une ou plusieurs autres adresses qui se trouvent sur les réseaux étrangers dans lequel il se déplace. Ces adresses sont des adresses "aux bons soins de" (*care-of address*). Il doit y avoir dans le réseau d'origine de l'ordinateur mobile une instance qui "redirige" sur son "adresse personnelle" lorsqu'il se trouve dans un autre réseau. Cette fonction est assurée, dans un scénario IPv6 par le "Home Agent". Ce dernier distribue tous les paquets adressés à l'adresse personnelle de l'ordinateur mobile via un tunnel. Les paquets dont l'adresse de destination est la "care-of address" peuvent ainsi être distribués directement.

22.2.3 IPv4 par rapport à IPv6 – passer d'un monde à l'autre

Le passage d'IPv4 à IPv6 de tous les ordinateurs présents sur l'Internet ne se fera pas d'un coup. Au contraire, l'ancien et le nouveau protocole devraient encore cohabiter pendant un certain temps. La coexistence, sur un ordinateur, est assurée par la "double pile", mais reste encore la question de la communication entre les ordinateurs IPv6 et IPv4 et comment IPv6 doit être transporté sur les réseaux IPv4 encore majoritaires. La tunnelisation et l'utilisation d'adresses de compatibilité (reportez-vous à la section *Structure d'une adresse IPv6* page 451) sont des méthodes qui permettent d'y parvenir.

Les îlots IPv6 dans le réseau IPv4 mondial échangent leurs données par l'intermédiaire de tunnels. Dans le cadre de la tunnelisation, les paquets IPv6 sont encapsulés dans des paquets IPv4 pour pouvoir être transportés via un réseau IPv4 pur. Un tunnel est une connexion entre deux points terminaux IPv4. Il convient donc d'indiquer l'adresse IPv6 cible (ou le préfixe correspondant) à laquelle les paquets IPv6 déguisés doivent être envoyés et l'adresse IPv4 distante qui doit recevoir les paquets tunnelisés. Dans les cas les plus simples, les administrateurs configurent ce type de tunnel entre leurs réseaux *manuellement* et après accord. On parle alors de tunnelisation *statique*.

La tunnelisation manuelle n'est cependant pas toujours suffisante pour organiser et gérer tous les tunnels nécessaires aux travaux quotidiens de mise en réseau. C'est pour cette raison que les développeurs ont mis au point trois différents processus qui autorisent la tunnelisation *dynamique*.

6sur4 (6over4) Les paquets IPv6 sont automatiquement encapsulés dans des paquets IPv4 et envoyés via un réseau IPv4 dans lequel la multidiffusion est activée. Pour IPv6, la totalité du réseau (d'un internet) apparaît comme un seul réseau local (en anglais, LAN *Local Area Network*) immense. Cela permet toujours de déterminer automatiquement le point terminal IPv4 du tunnel. Un inconvénient de cette méthode réside dans sa mauvaise adaptabilité et dans le fait que la multidiffusion IP n'est en aucun cas disponible sur la totalité de l'Internet. Cette solution est adaptée pour les petits réseaux de sociétés ou d'institutions qui permettent de faire de la multidiffusion IP. Le RFC correspondant est le RFC 2529.

6vers4 (6to4) Cette méthode génère automatiquement des adresses IPv4 à partir d'adresses IPv6. Les îlots IPv6 peuvent ainsi communiquer les uns avec les autres via un réseau IPv4. Il demeure cependant quelques problèmes pour ce qui concerne la communication entre les îlots IPv6 et l'Internet. Le RFC correspondant est le RFC 3056.

IPv6 Tunnel Broker Cette approche prévoit des serveurs spéciaux qui définissent automatiquement des tunnels pour l'utilisateur. Le RFC correspondant est le RFC 3053.

Remarque

L'initiative 6Bone

Au sein de l'Internet "à l'ancienne mode", le *6Bone* (`www.6bone.net`) constitue un réseau mondial réparti de sous-réseaux IPv6 qui sont reliés les uns avec les autres par des tunnels. IPv6 est testé au sein du réseau 6Bone. Les développeurs de logiciels et les fournisseurs d'accès qui développent ou proposent des services IPv6 peuvent utiliser cet environnement de test pour réaliser des expériences avec ce nouveau protocole. Vous trouverez davantage d'informations à ce sujet sur la page du projet 6Bone.

Remarque

22.2.4 Documentation et liens supplémentaires au sujet d'IPv6

La présentation ci-dessus ne peut et ne se veut en aucun cas une introduction complète au sujet très complexe qu'est IPv6. Pour une approche plus approfondie d'IPv6, vous pouvez consulter la documentation en ligne et les ouvrages suivants :

`http://www.ngnet.it/e/cosa-ipv6.php`
Série d'articles avec de très bonnes descriptions sur les principes fondamentaux d'IPv6. Particulièrement appropriés pour une première approche de ce sujet.

`http://www.bieringer.de/linux/IPv6/`
Linux-IPv6-HOWTO et nombreux liens.

`http://www.6bone.de/` Se connecter à IPv6 par un tunnel.

`http://www.ipv6.org/` Tout sur IPv6.

RFC 2640 Le RFC d'introduction au sujet d'IPv6.

IPv6 Essentials Présentation en anglais d'IPv6. Hagen, Silvia : *IPv6 Essentials*. O'Reilly & Associates, 2002. - (ISBN 0-596-00125-8).Voir aussi en français : Cizault, Gisèle :*IPv6, théorie et pratique*. O'Reilly & Associates, 2002. - (ISBN : 2-84177-139-3).

22.3 Configuration manuelle du réseau

Les logiciels gérant le réseau ne devraient être configurés manuellement qu'en second recours. Nous recommandons d'utiliser YaST. Une connaissance des mécanismes sous-jacents de la configuration réseau facilitera votre travail avec YaST.

Toute carte réseau — qu'elle soit intégrée ou qu'elle soit un périphérique qui puisse être branché à chaud (PCMCI, USB, et certaines cartes PCI)— sera reconnue par le biais d'Hotplug et installée. Pour comprendre cette procédure, gardez les points suivants en tête :

Différentes manières de voir les cartes réseau
: Une carte réseau est vue par le système de deux manières. Elle est d'une part considérée comme un *périphérique* (*device*) et d'autre part comme une *interface*. Le branchement ou la reconnaissance du périphérique entraîne un événement de branchement à chaud (*hotplug event*). Cet événement entraîne alors l'initialisation du périphérique par le biais du script `/sbin/hwup`. Lors de l'initialisation de la carte réseau en tant que nouvelle interface réseau, le noyau déclenche un événement supplémentaire. Cela entraîne l'installation de l'interface par le biais de `/sbin/ifup`.

Attribution des noms d'interfaces par le noyau
: Le noyau associe les interfaces réseau suivant l'ordre de leur enregistrement. L'ordre d'initialisation est déterminant pour l'attribution des noms. Si, en présence de plusieurs cartes réseau, la première tombe en panne, la numérotation de toutes celles qui sont initialisées ensuite sera décalée. Avec les cartes qui peuvent "réellement" être branchées à chaud, l'ordre détermine à quelle interface le périphérique sera associé.

Pour permettre une configuration flexible, la configuration des périphériques (matériel) et celle des interfaces sont séparées et l'association des configurations à leurs périphériques et interfaces respectifs ne dépend plus des noms des interfaces. La configuration des périphériques se trouve dans `/etc/sysconfig/hardware/hwcfg-*` tandis que la configuration des interfaces se trouve dans `/etc/sysconfig/network/ifcfg-*`. Les noms des configurations sont choisis de manière à ce qu'ils décrivent leurs périphériques et interfaces respectifs. Comme l'association précédente entre les pilotes et les noms d'interface s'appuie sur des noms d'interface constants, cette association ne peut plus se faire dans `/etc/modprobe.conf`. Les alias dans ce fichier pourront mener avec ce nouveau concept à des effets annexes imprévus.

Les noms des configurations, c'est à dire tout ce qui suit `hwcfg-` ou `ifcfg` peuvent décrire le périphérique par l'endroit où il est monté, par un identifiant propre au périphérique ou par le nom de l'interface. Pour une carte PCI il peut ainsi s'agir de `bus-pci-0000:02:01.0` (emplacement PCI) ou de `vpid-0x8086-0x1014-0x0549` (identifiant du vendeur et du produit). Pour l'interface correspondante, on peut aussi utiliser `bus-pci-0000:02:01.0` ou encore `wlan-id-00:05:4e:42:31:7a` (adresse MAC).

Si on ne veut pas associer une configuration à une carte donnée mais plutôt à une carte d'un type donné (une seule carte de ce type étant branchée à la fois), on choisit un nom de configuration moins particulier. On utilise alors par exemple `bus-pcmcia` pour toutes les cartes PCMCIA. D'autre part, les noms peuvent aussi être limités par l'utilisation du type d'interface. Ainsi, `wlan-bus-usb` concernera toutes les cartes WLAN branchées avec USB.

La configuration utilisée est toujours celle qui décrit le mieux l'interface ou le périphérique qui fournit l'interface. La meilleure configuration sera recherchée par `/sbin/getcfg`. `getcfg` fournit toutes les informations que l'on peut utiliser pour décrire un périphérique. La spécification exacte des noms de configuration se trouve dans la page de manuel de `getcfg`.

Avec la méthode décrite, une interface réseau reste associée à la bonne configuration, même lorsque le périphérique réseau n'est pas initialisé dans l'ordre prévu. Il reste comme précédemment le problème que le nom de l'interface dépend toujours de l'ordre d'initiialisation. Si toutefois l'interface doit être associée de manière fiable à une carte réseau donnée, il existe deux moyens d'arriver à ce résultat.

- `/sbin/getcfg-interface <nom-de-la-configuration>` rend le nom à l'interface réseau correspondante. C'est pourquoi il est également possible dans les fichiers de configuration de certains (malheureusement pas encore tous) services d'indiquer le nom de la configuration à la place du nom de l'interface (qui n'est pas persistant) (c'est le cas par exemple pour le pare-feu, pour `dhcpd`, pour le routage et pour diverses interfaces réseau virtuelles (tunnel)).
- Pour toutes les interfaces dont la configuration n'est pas nommée d'après le nom de l'interface, un nom d'interface persistant ne peut pas être donné. On parvient à ce but par le biais de l'élément `PERSISTENT_NAME=<nomp>` dans une configuration d'interface (`ifcfg-*`). Le nom persistant ⟨*pname*⟩ ne peut en revanche pas être un nom que le noyau donnerait automatiquement. Les noms en `eth*`, `tr*`, `wlan*`, `qeth*`, `iucv*`, etc. ne sont pas non plus permis. Par contre, vous pouvez utiliser par exemple `net*` ou des noms descriptifs tels que `externe`, `interne` ou `dmz`. Les noms persistants ne sont attribués qu'immédiatement après l'enregistrement, c'est pourquoi

les pilotes des cartes réseau doivent être rechargés (par exemple en lançant `hwup <description-du-périphérique>`).`rcnetwork restart` ne suffit pas.

Remarque

Modifier des noms d'interfaces persistants

Veuilles noter que la modification des noms d'interface n'a pas encore été testée dans tous les domaines. Il peut arriver que des applications données ne s'en sortent pas avec les noms d'interfaces librement choisis. Merci de nous informer dans ce cas au moyen de `http://feedback.suse.de`.

Remarque

`ifup` n'initialise pas le matériel, mais suppose une interface déjà existante. Pour initialiser le matériel on peut utiliser la commande `hwup`, qui est appelée par `hotplug` (ou `coldplug`). Dès qu'un périphérique est initialisé, `ifup` est appelé automatiquement par `hotplug` pour la nouvelle interface et il est mis en service si le mode de démarrage est `onboot`, `hotplug` ou `auto` et si le service `network` est démarré. Il était précédemment d'usage que `ifup <nom-de-l-interface>` lance l'initialisation du matériel. La manière d'organiser les choses est maintenant vraiment inversée. Un périphérique est d'abord initialisé ; toutes les actions suivantes en dépendent. Il est par là même possible d'installer toujours de manière optimale une quantité variable de périphériques avec un ensemble de configurations appropriées.

Le meilleur aperçu de tout ceci est la table suivante résumant l'essentiel à propos des scripts associés aux configurations réseau. Dans la mesure du possible, les aspects matériel et lié à l'interface ont été séparés :

TAB. 22.5: *Scripts pour la configuration manuelle du réseau*

Étape de la configuration	Commande	Fonction
Matériel	`hw{up,down,status}`	Les scripts `hw*` sont appelés par le sous-système de branchement à chaud pour initialiser un périphérique, annuler son initialisation, ou demander le statut d'un périphérique. De plus amples informations sont disponibles dans `man hwup`.

Interface	`getcfg`	`getcfg` vous permet d'obtenir à partir du nom d'une configuration ou d'une description matérielle le nom de l'interface correspondante. De plus amples informations sont disponibles dans `man getcfg`.
Interface	`if{up,down,status}`	Les scripts `if*` activent ou désactivent les interfaces existantes ou donnent le statut des interfaces nommées. Vous trouverez plus d'informations dans `man ifup`.

Vous trouverez plus d'informations à propos du *Branchement à chaud* et des *Noms de périphériques* dans les chapitres *Le système Hotplug* page 399 et *Noeuds de périphériques dynamiques avec udev* page 409.

22.3.1 Fichiers de configuration

Cette section donne un aperçu des fichiers de configuration réseau et explique leur fonction ainsi que le format utilisé.

/etc/syconfig/hardware/hwcfg-*

Vous trouverez dans ces fichiers les réglages des cartes réseau et des autres périphériques. Ils contiennent les paramètres essentiels comme le module du noyau, le mode d'amorçage et l'ordre des scripts. Vous trouverez des détails à ce propos dans la page de manuel de `hwup`. Les fichiers de configuration `hwcfg-static-*` seront utilisées au démarrage de Coldplug indépendamment du matériel présent.

/etc/sysconfig/network/ifcfg-*

Ces fichiers contiennent les réglages des interfaces réseau. Ils contiennent entre autres le mode d'amorçage et l'adresse IP. Les paramètres possibles sont décrits dans la page de manuel de `ifup`. Il est également possible d'utiliser toutes les variables des fichiers `dhcp`, `wireless` et`config` dans les fichiers `ifcfg-*` lorsqu'un réglage par ailleurs commun ne doit être utilisé que pour une seule interface.

/etc/sysconfig/network/config,dhcp,wireless

Le fichier `config` contient les réglages généraux concernant le comportement de `ifup`, `ifdown` et `ifstatus`. Il est commenté de manière exhaustive. On trouve de même des commentaires dans `dhcp` et `wireless`, où sont regroupés des réglages généraux concernant DHCP et les cartes réseau sans fil. Toutes les variables de ces fichiers peuvent également être utilisées dans `ifcfg-*` et y sont prioritaires.

/etc/sysconfig/network/routes,ifroute-*

Le routage statique pour TCP/IP est réglé ici. Dans ces fichiers, la première colonne représente la destination de la route, la deuxième la passerelle, la troisième le masque réseau de la destination et la quatrième une interface réseau optionnelle. La cinquième colonne et les suivantes peuvent accueillir des options spéciales. Les colonnes vides seront matérialisées par un `-`. Vous trouverez plus de détails dans la page de manuel de `routes` et en section *Le routage sous SUSE LINUX* page 483.

Si l'interface réseau ne fonctionne pas, la route de chaque interface installée sera essayée, ce qui ne fonctionne qu'avec les interfaces compatibles. Cela peut être utilisé par exemple pour la route par défaut. Les noms de configuration peuvent naturellement être utilisés à la place des noms des interfaces.

Si une route doit n'être utilisée qu'avec une seule configuration d'interface, elle peut être mise dans ifroute-<Nom-de-la-configuration> au lieu de `routes`. Différentes routes par défaut peuvent également être réglées. L'interface réseau configurée la dernière sera toujours celle utilisée.

/etc/resolv.conf

Ce fichier, comme précédemment le fichier `/etc/host.conf`, joue aussi un rôle en ce qui concerne la résolution de noms d'hôtes, grâce à la bibliothèque *resolver*.

Ce fichier indique à quel domaine l'hôte appartient (mot-clé `search`) et quelle sera l'adresse du serveur de noms (mot-clé `nameserver`) chargé de répondre. On peut indiquer plusieurs noms de domaine. Lors de la résolution d'un nom qui n'est pas pleinement qualifié, on cherche à produire un nom pleinement qualifié valide en accolant les différents suffixes contenus dans `search`. Plusieurs serveurs de noms peuvent être indiqués au moyen de plusieurs lignes commençant par `nameserver`. Les commentaires sont ici aussi introduits par le caractère #. C'est ici que YaST enregistre le serveur de noms indiqué.

Le listing 22.5 page suivante présente un exemple de `/etc/resolv.conf`.

Exemple 22.5: `/etc/resolv.conf`

```
# Notre domaine
search exemple.com
# Nous utilisons soleil (192.168.0.20) comme serveur de noms
 nameserver 192.168.0.20
```

Certains services comme `pppd` (`wvdial`), `ipppd` (`isdn`), `dhcp`(`dhcpcd` et `dhclient`), `pcmcia` et `hotplug` modifient le fichier `/etc/resolv.conf` grâce au script `modify_resolvconf`.

Lorsque le fichier `/etc/resolv.conf` a été temporairement modifié par ce script, il contient un commentaire précis qui fournit des renseignements permettant de savoir quel service l'a modifié, à quel endroit le fichier d'origine a été sauvegardé et comment on peut revenir sur les modifications automatiques.

Lorsqu'on modifie plusieurs fois `/etc/resolv.conf`, cet emballage des modifications est retiré proprement lorsque vous déterminez un autre ordre ; cela peut tout à fait se produire avec `isdn`, `pcmcia` et `hotplug`

Lorsqu'on n'a pas mis fin à un service proprement, il est possible de reconstituer l'état d'origine à l'aide du script `modify_resolvconf`. Lors de l'amorçage, il faut vérifier s'il ne reste pas un `resolv.conf` modifié (par exemple, en raison d'un plantage du système). Le `resolv.conf` original (non modifié) est alors reconstitué.

YaST détermine au moyen de `modify_resolvconf check` si `resolv.conf` a été modifié et avertit l'utilisateur que ses modifications seront perdues après la restauration. YaST n'utilise pas sinon `modify_resolvconf`, c'est-à-dire qu'une modification du fichier `resolv.conf` par le biais de YaST et une modification manuelle sont équivalentes. Toutes deux correspondent à une modification ciblée et durable, tandis qu'une modification par un des services cités n'est que temporaire.

/etc/hosts

Ce fichier (voir le listing 22.6 page suivante) associe les noms d'hôtes et les adresses IP correspondantes. Si aucun serveur de noms n'est utilisé, il faut énumérer ici tous les ordinateurs avec lesquels une connexion IP doit être établie. On trouve dans ce fichier pour chaque ordinateur une ligne composée de l'adresse IP, du nom d'hôte pleinement qualifié et du nom de machine (par exemple, `terre`). L'adresse IP doit être placée au début de la ligne, et les autres éléments sont séparés par des espaces et/ou des tabulations. Les commentaires sont précédés de caractères #.

Exemple 22.6: /etc/hosts

```
127.0.0.1 localhost
192.168.0.20 soleil.exemple.com soleil
192.168.0.0; terre.exemple.com; terre
```

/etc/networks

C'est ici que les noms de réseaux sont convertis en adresses réseau. Leur format ressemble à celui du fichier `hosts`, mais ce sont les noms de réseaux qui précèdent les adresses (reportez-vous au fichier 22.7).

Exemple 22.7: /etc/networks

```
loopback     127.0.0.0
localnet     192.168.0.0
```

/etc/host.conf

La résolution de noms – c'est-à-dire la traduction de noms d'hôtes et/ou de noms de réseaux au moyen de la bibliothèque *resolver* – est contrôlée par ce fichier. On ne l'utilise que pour les programmes liés à la libc4 ou la libc5 ; pour les programmes glibc actuels, reportez-vous aux réglages contenus dans le fichier `/etc/nsswitch.conf` ! Un paramètre doit se trouver dans une ligne qui lui est propre, les commentaires commencent par des caractères #. Le tableau 22.6 page suivante présente les paramètres possibles.

TAB. 22.6: *Paramètres de /etc/host.conf*

order *hosts*, *bind*	Il s'agit d'établir l'ordre de consultation des services de résolution d'un nom. Les arguments possibles sont (séparés l'un de l'autre par des espaces ou des virgules) : *hosts* : chercher dans le fichier `/etc/hosts` *bind* : solliciter un serveur de noms *nis* : au moyen de NIS
multi *on*/*off*	Détermine si un ordinateur donné peut avoir plusieurs adresses IP dans `/etc/hosts`.
nospoof *on* spoofalert *on*/*off*	Ces paramètres agissent sur la prévention d'*usurpation* (*spoofing*) du serveur de noms, mais n'ont pas d'autre impact sur la configuration réseau.
trim `nom_domaine`	Le nom de domaine indiqué est supprimé du nom de machine à résoudre (dans la mesure où le nom de machine contient effectivement ce nom de domaine).Cette option est utile si le fichier `/etc/hosts` ne contient que des noms dans le domaine local qui doivent être également reconnus avec un nom de domaine accolé.

Le listing 22.8 présente un exemple de fichier `/etc/host.conf`.

Exemple 22.8: *`/etc/host.conf`*

```
# Le démon named tourne
order hosts bind
# Permettre des adresses multiples
multi on
```

/etc/nsswitch.conf

La version 2.0 de la bibliothèque GNU C a introduit le Name Service Switch (NSS) (reportez-vous à la page de manuel `man 5 nsswitch.conf`, ainsi qu'au très complet manuel *The GNU C Library Reference Manual*, au chapitre "System Databases and Name Service Switch").

Le fichier `/etc/nsswitch.conf` permet de fixer l'ordre de consultation de certaines informations. Le listing 22.9 montre un exemple de fichier `nsswitch.conf`. Les commentaires sont précédés du caractère #. Ici par exemple, la ligne concernant la base de données `hosts` signifie qu'après l'examen de `/etc/hosts` (`files`), une requête DNS est effectuée (reportez-vous à la section *DNS – Domain Name System* page 487).

Exemple 22.9: `/etc/nsswitch.conf`

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

Les bases de données offertes par NSS sont énumérées dans le tableau 22.7. De plus, on peut s'attendre à l'avenir à `automount`, `bootparams`, `netmasks` et `publickey`.

TAB. 22.7: *Bases de données disponibles dans /etc/nsswitch.conf*

`aliases`	Alias de courrier utilisés par `sendmail` ; reportez-vous à la page de manuel `man 5 aliases`.
`ethers`	Adresses Ethernet.
`group`	Spécifie les groupes d'utilisateurs utilisés par `getgrent` ; reportez-vous à la page de manuel `man 5 group`.

`hosts`	Spécifie les noms d'hôtes et les adresses IP utilisés par `gethostbyname` et autres fonctions similaires.
`netgroup`	Il s'agit de la liste en vigueur sur le réseau des hôtes et des utilisateurs pour le contrôle des droits d'accès ; reportez-vous à la page de manuel `man 5 netgroup`.
`networks`	Noms et adresses des réseaux utilisés par `getnetent`.
`passwd`	Mots de passe utilisateur utilisés par `getpwent` ; reportez-vous à la page de manuel `man 5 passwd`.
`protocols`	Protocoles réseau utilisés par `getprotoent` ; reportez-vous à la page de manuel `man 5 protocols`.
`rpc`	Noms et adresses d'appels de procédure distants (*Remote Procedure Call*) utilisés par `getrpcbyname` et d'autres fonctions similaires.
`services`	Services réseau utilisés par `getservent`.
`shadow`	Mots de passe *shadow* des utilisateurs utilisés par `getspnam` ; reportez-vous à la page de manuel `man 5 shadow`.

Les possibilités de configuration des bases de données NSS se trouvent dans le tableau 22.8.

TAB. 22.8: *Possibilités de configuration des bases de données NSS*

`files`	accès direct à des fichiers, par exemple à `/etc/aliases`.
`db`	accès à une base de données.
`nis`	NIS, reportez-vous à la section *NIS – Network Information Service* page 509.
`nisplus`	
`dns`	Utilisable uniquement avec `hosts` et `networks` sous forme d'extension.
`compat`	Utilisable uniquement avec `passwd`, `shadow` et `group` sous forme d'extension.

De plus, il est possible de déclencher des réactions différentes suivant les résultats de la consultation ; vous trouverez plus de détails dans la page de manuel `man 5 nsswitch.conf`.

/etc/nscd.conf

Ce fichier permet de configurer nscd *Name Service Cache Daemon* - Démon de Cache du Service de Noms - (reportez-vous à `man 8 nscd` et à `man 5 nscd.conf`). Par défaut, les informations provenant de `passwd` et `groups` sont enregistrées dans le cache. C'est essentiel dans le cas des services de répertoires tels que NIS et LDAP pour une bonne performance, car sinon, chaque accès aux noms ou groupes nécessitera une connexion réseau.`hosts` n'est normalement pas mis en cache puisque l'ordinateur ne peut alors plus se fier aux "recherches de noms/recherches inverses" (*forward/reverse lookups*) de ce service de noms. Au lieu de transmettre la fonction à nscd, vous devriez mettre en place un serveur de nom "avec un cache".

La mise en cache de `passwd` par exemple dure généralement 15 secondes jusqu'à ce que le système soit informé de la création d'un nouvel utilisateur local. On peut raccourcir ce délai d'attente en redémarrant nscd avec la commande `rcnscd restart`.

/etc/HOSTNAME

C'est ici que se trouve le nom de l'ordinateur, c'est-à-dire seulement le nom d'hôte sans le nom de domaine. Ce fichier est lu par différents scripts au cours du démarrage de l'ordinateur. Il ne peut contenir qu'une ligne, dans laquelle figure le nom d'ordinateur !

22.3.2 scripts de démarrage

Outre les fichiers de configuration décrits, il existe différents scripts qui démarrent les programmes réseau pendant l'amorçage de l'ordinateur. Ceux-ci sont démarrés dès que le système passe au *niveau d'exécution multi-utilisateur* (reportez-vous au tableau 22.9 page suivante).

TAB. 22.9: *Quelques scripts de démarrage des programmes réseau*

`/etc/init.d/network`	Ce script gère la configuration des interfaces réseau. Le matériel doit pour cela déjà être initialisé par `/etc/init.d/coldplug` (par le biais de `hotplug`). Si le service `network` n'a pas été démarré, les interfaces réseau ne sont pas installées non plus par Hotplug au moment de leur branchement.
`/etc/init.d/xinetd`	Démarre xinetd. xinetd permet de lancer les services disponibles d'un système à la demande. Par exemple, il peut lancer vsftpd lorsqu'une connexion FTP est initialisée.
`/etc/init.d/portmap`	Démarre *portmapper*, qui est requis pour pouvoir utiliser un serveur RPC, comme par exemple un serveur NFS.
`/etc/init.d/nfsserver`	Démarre le serveur NFS.
`/etc/init.d/postfix`	Contrôle le processus postfix.
`/etc/init.d/ypserv`	Démarre le serveur NIS.
`/etc/init.d/ypbind`	Démarre le client NIS.

22.4 L'intégration dans le réseau

TCP/IP est devenu le protocole réseau par défaut grâce auquel tous les systèmes d'exploitation modernes peuvent communiquer. Cependant, Linux prend également en charge d'autres protocoles réseau, le protocole (antérieur) utilisé par Novell Netware, IPX, ou celui utilisé par les ordinateurs Macintosh, Appletak. Dans ce document, nous n'aborderons que l'intégration d'un ordinateur Linux dans un réseau TCP/IP. Si vous souhaitez intégrer des cartes réseau exotiques Arcnet, Token-Ring ou FDDI, vous trouverez une aide approfondie dans le répertoire `/usr/src/linux/Documentation` des sources du noyau, à installer séparément avec le paquetage `kernel-source`.

22.4.1 Préparatifs

L'ordinateur doit disposer d'une carte réseau prise en charge. Celle-ci a généralement déjà été reconnue lors de l'installation et le pilote approprié mis en place. Si votre carte a été correctement installée, vous pourrez constater entre autres que la sortie de la commande `ip address list eth0` indique le périphérique réseau `eth0`.

Si la carte réseau est prise en charge par un module du noyau – comme c'est normalement le cas avec le noyau SUSE –, le nom du module doit être déclaré dans `/etc/sysconfig/hardware/hwcfg-*`. S'il ne s'y trouve pas, la commande `hotplug` cherche automatiquement un pilote. Il n'y a pas de différence entre les cartes réseau que l'on peut brancher à chaud et les cartes intégrées, `hotplug` se charge d'associer un pilote dans tous les cas.

22.4.2 Configurer une carte réseau avec YaST

Après le démarrage du module de YaST, vous obtenez un résumé de la configuration réseau. Dans la partie supérieure da la boîte de dialogue, toutes les cartes réseau à configurer sont affichées. Si votre carte a été détectée correctement à l'amorçage du système, elle sera mentionnée ici. Les périphériques non reconnus apparaissent comme 'Autre (non détecté)'. Dans la partie inférieure de la fenêtre d'affichage, les périphériques déjà configurés sont affichés ainsi que leurs type et adresse réseau. Vous pouvez maintenant configurer les nouvelles cartes réseau ou changer une configuration déjà existante.

Configuration manuelle de la carte réseau

Pour configurer une carte réseau non détectée, réalisez les configurations basiques suivantes :

Configuration du réseau Configurez le type de périphérique de l'interface et le nom de la configuration. Une zone de liste modifiable vous permet de choisir le type de périphérique ; vous pouvez choisir vous-même le nom de la configuration suivant vos besoins. Les paramètres par défaut conviennent généralement et peuvent être repris. Des informations sur les conventions de nommage pour les noms de configuration se trouvent dans la page de manuel de `getcfg`.

Module du noyau ‘Nom de la configuration du matériel’ détermine le nom du fichier `/etc/sysconfig/hardware/hwcfg-*` dans lequel la configuration matérielle de votre carte réseau (le nom du module du noyau correspondant) est écrite. YaST propose dans la plupart des cas des noms judicieux pour les périphériques PCMCIA et USB. Pour tous les autres périphériques, `0` n’a de sens dans la plupart des cas que si cette carte est aussi déclarée dans `hwcfg-static-0`.

Si la carte réseau est un périphérique PCMCIA ou USB, activez les cases à cocher correspondantes et quittez la boîte de dialogue en cliquant sur ‘Suivant’. Si ce n’est pas le cas, choisissez le modèle de votre carte réseau à l’aide du bouton ‘Sélectionner dans la liste’. YaST choisira alors automatiquement le module de noyau adéquat. Cliquez sur ‘Suivant’ pour quitter cette boîte de dialogue.

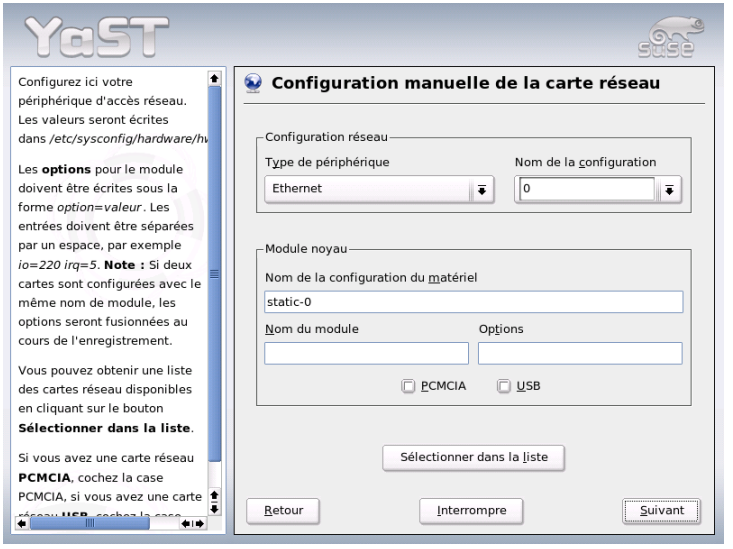


FIG. 22.3: *Configuration d’une carte réseau*

Configuration des adresses réseau

Configurez le type de périphérique de l'interface et le nom de la configuration. Une zone de liste modifiable vous permet de choisir le type de périphérique ; vous pouvez choisir vous-même le nom de la configuration suivant vos besoins. Les paramètres par défaut conviennent généralement et peuvent être repris. Des informations sur les conventions de nommage pour les noms de configuration se trouvent dans la page de manuel de `getcfg`.

Si vous choisissez 'sans fil' comme type de périphérique pour l'interface, la boîte de dialogue suivante vous proposera une 'Configuration de la carte réseau sans fil' dans laquelle vous pourrez configurer le mode de fonctionnement, le nom du réseau (ESSID) et le chiffrement. Fermez la configuration de la carte avec 'OK'. Une description détaillée de la configuration des cartes WLAN se trouve en section *Configuration avec YaST* page 379. Pour tous les autres types d'interfaces, il vous faudra approfondir la manière d'assigner des adresses pour votre carte réseau.

'Affectation dynamique d'adresses (via DHCP)'
: Si vous disposez d'un serveur DHCP dans votre réseau, vous pouvez en obtenir automatiquement les données de configuration pour votre carte réseau. Activez également l'affectation d'adresses IP via DHCP si votre fournisseur d'accès à l'ADSL n'attribue pas d'adresse IP statique à votre système. Pour accéder à la configuration du client DHCP, utilisez l'option 'Options du client DHCP'. Ici vous pouvez indiquer si le serveur DHCP doit toujours répondre à une diffusion générale (broadcast). En outre, vous avez la possibilité d'indiquer un identificateur. Par défaut, l'ordinateur identifie la carte réseau au moyen de l'adresse matérielle. Si vous utilisez plusieurs machines virtuelles qui font appel à la même carte réseau, vous pouvez les différencier à l'aide d'identificateurs différents.

'Configuration de l'adresse statique' Si vous disposez d'une adresse IP, cochez la case correspondante. Saisissez ici votre adresse IP et le masque sous-réseau qui convient à votre réseau. La configuration par défaut du masque sous-réseau est suffisante pour un réseau domestique ordinaire.

Vous pouvez quitter cette boîte de dialogue en cliquant sur 'Suivant' ou bien configurer le nom de l'ordinateur, le serveur de noms et le routeur (voir la section *Nom d'hôte et DNS* page 89 et la section *Routage* page 92).

Grâce à la zone de liste modifiable 'Avancé...', vous pouvez effectuer des réglages complexes. Entre autres, vous trouverez dans 'Paramètres Détaillés' la possibilité de déléguer le contrôle des cartes réseau depuis l'administrateur (le `root`) à un utilisateur normal grâce à 'Contrôlé par l'utilisateur'. Dans un contexte d'informatique nomade, ceci permet à l'utilisateur de s'adapter plus facilement à des connexions réseau changeantes car il peut activer ou désactiver l'interface lui-même. Vous pourrez aussi configurer dans cette boîte de dialogue le MTU (*Maximum Transmission Unit* - Unité de Transmission Maximale) et la méthode d''Activation du périphérique'.

Modem câble

Dans certains pays (Autriche, États-Unis), l'accès Internet par câble télévision est très répandu. L'abonné reçoit de l'opérateur de réseau câblé un modem relié d'une part au câble TV et d'autre part à une carte réseau dans l'ordinateur au moyen d'un câble 10Base-T (paire torsadée). Ce modem représente alors pour la machine une ligne permanente avec une adresse IP fixe.

Après avoir configuré votre fournisseur d'accès, choisissez entre 'Assignation dynamique d'adresses (via DHCP)' ou 'Assignation statique d'adresses', en fonction des informations que vous avez obtenues de votre fournisseur d'accès Internet. La plupart des fournisseurs d'accès utilisent aujourd'hui DHCP. Une adresse IP statique est généralement utilisée par les fournisseurs d'accès Internet. Dans un tel cas, le fournisseur d'accès vous a affecté une adresse IP fixe.

Nous vous recommandons de consulter les articles de la base de données d'assistance se rapportant aux configurations de modems câbles que vous pouvez obtenir en ligne à l'adresse `http://sdb.suse.de/en/sdb/html/cmodem8.html`.

22.4.3 Modem

Dans le centre de contrôle de YaST, vous trouverez la configuration du modem dans 'Périphériques réseau'. Si la détection automatique n'aboutit pas, choisissez la configuration manuelle. Dans la boîte de dialogue qui s'ouvre, indiquez l'interface dans 'Modem'.

Si votre ligne passe par un central téléphonique privé, vous devrez éventuellement indiquer un préfixe (normalement zéro ; vous pouvez vous en assurer en consultant le mode d'emploi de votre central téléphonique) pour passer des appels extérieurs. Choisissez en outre entre la numérotation par tonalité et la numérotation par impulsions. Vous pouvez aussi décider si la sortie son du modem

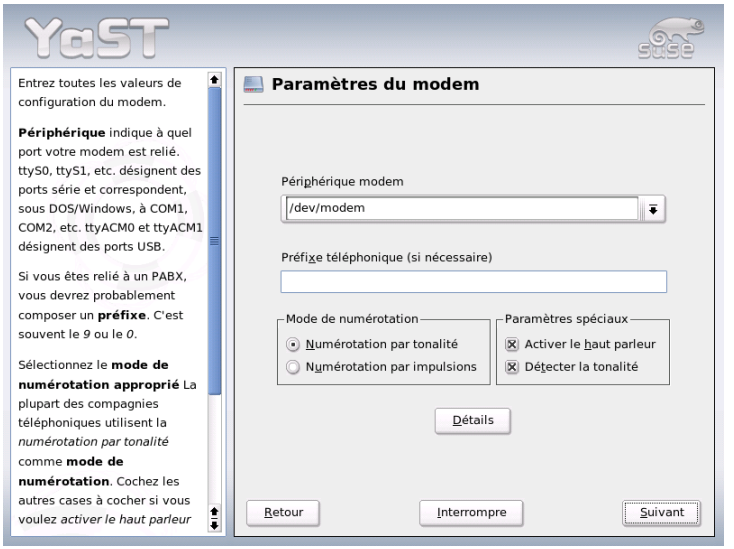


FIG. 22.4: *Configuration du modem*

doit être activée et si vous désirez attendre la tonalité. Vous ne devriez pas utiliser cette dernière option si votre modem est relié à un autocommutateur (PABX).

Dans 'Détails', vous trouverez des valeurs concernant la vitesse en bauds et les chaînes d'initialisation du modem. Vous ne devriez rien changer ici, sauf si votre modem n'a pas été reconnu automatiquement et s'il doit être spécialement réglé pour le transfert de données. C'est notamment le cas pour les adaptateurs terminaux RNIS. Quittez la boîte de dialogue en cliquant sur 'OK'. Si vous voulez permettre le contrôle du modem par un utilisateur normal sans droits root, cochez 'Contrôlé par l'utilisateur'. L'utilisateur sans droits d'administration peut alors prendre lui-même en main l'activation ou la désactivation d'une interface. Saisissez dans l'option 'Expression régulière du préfixe de numérotation' une expression régulière à laquelle doit se conformer un utilisateur normal dans KInternet lorsqu'il modifie le 'Préfixe de numérotation'. Si ce champ est laissé vide, l'utilisateur ne peut pas modifier le 'Préfixe de numération' sans droits d'administration.

Dans la boîte de dialogue suivante, choisissez le FAI (Fournisseur d'Accès Internet). Vous pouvez choisir un fournisseur d'accès par défaut dans la liste prévue pour votre pays, dans ce cas cliquez sur le bouton radio 'Pays'. Vous pouvez également cliquer sur 'Nouveau' et saisir à la main les paramètres du FAI. Saisissez le nom pour la numérotation, le nom du FAI et son numéro de téléphone. Saisissez également le nom d'utilisateur et le mot de passe que votre FAI vous a attribué pour la connexion. Cochez la case 'Toujours demander' si vous souhaitez que le mot de passe vous soit demandé à chaque connexion.

Dans la dernière boîte de dialogue, saisissez les paramètres de connexion :

'Connexion à la demande' Si vous souhaitez utiliser une connexion à la demande, indiquez au moins un serveur de noms.

'Modifier le DNS après connexion' Cette case étant cochée par défaut, le serveur de noms s'ajustera donc automatiquement lors de chaque connexion à Internet. Désactivez ce paramètre et définissez des serveurs de noms spécifiques si vous vous décidez pour la 'Composition automatique'.

'Mode stupide' Cette option est activée par défaut. Les requêtes du serveur de commutation seront ignorées pour faciliter l'établissement de la connexion.

'Activer le pare-feu' Ici, activez le pare-feu SUSE Firewall et protégez-vous de cette façon des intrus lorsque vous êtes connecté à Internet.

'Délai d'inactivité (secondes)' Vous pouvez fixer le délai après lequel la communication sera automatiquement coupée si aucun échange d'informations n'a lieu.

Détails IP Ce bouton permet d'ouvrir la boîte de dialogue de configuration de l'adresse. Si votre fournisseur d'accès ne vous a attribué aucune adresse IP dynamique, décochez la case 'Adresse IP dynamique' et saisissez l'adresse IP locale de votre ordinateur et l'adresse IP distante. Vous pouvez obtenir ces adresses auprès de votre fournisseur d'accès. Laissez la configuration de 'Route par défaut' activée et quittez la boîte de dialogue en cliquant sur 'OK'.

Cliquez sur 'Suivant' pour retourner à la boîte de dialogue d'aperçu dans laquelle la configuration est affichée. Quittez la configuration avec 'Terminer'.

22.4.4 DSL

Pour configurer une connexion ADSL, utilisez le module de YaST 'DSL' dans la rubrique 'Périphériques réseau'. Plusieurs boîtes de dialogue vous permettent da saisir les paramètres d'accès à Internet via ADSL. Avec YaST, vous pouvez configurer des connexions ADSL qui utilisent les protocoles suivants :

- PPP sur Ethernet (PPPoE) - Allemagne
- PPP sur ATM (PPPoATM) - Royaume Uni
- CAPI pour ADSL (Cartes Fritz)
- Protocole de tunnel pour le point à point (PPTP) - Autriche

N'oubliez pas qu'avant d'entreprendre la configuration ADSL avec PPPoE et PPTP, vous devez déjà avoir configuré correctement votre carte réseau. Si vous ne l'avez pas encore configurée, ouvrez la boîte de dialogue correspondante en cliquant sur 'Configurer les cartes réseau' (voir section *Configurer une carte réseau avec YaST* page 469). Dans le cas de l'ADSL, l'affectation automatique des adresses IP n'est pas effectuée avec le protocole DHCP. C'est pourquoi vous ne devrez pas utiliser l'option 'Assignation dynamique d'adresses (via DHCP)' mais affecter une adresse IP statique fictive, par exemple `192.168.22.1` qui constitue un bon choix. Dans le champ 'Masque sous-réseau', vous devez saisir la valeur `255.255.255.0`. Pour un système monoposte, veillez absolument à ne rien saisir dans le champ 'Passerelle par défaut'.

Remarque

Les valeurs pour l''adresse IP' de votre machine et pour le 'masque sous-réseau' ne sont que des valeurs fictives. Elles ne sont d'aucune importance pour l'établissement de la connexion avec DSL et ne sont nécessaires que pour activer la carte réseau.

Remarque

Au début de la configuration (voir figure 22.5 page suivante), choisissez le mode PPP et la carte Ethernet à laquelle le modem est connecté (il s'agit en général de `eth0`). La zone de liste modifiable 'Activation du périphérique' vous permet de déterminer si la connexion ADSL doit être établie au démarrage du système ou plus tard, manuellement. L'option 'Contrôlé par l'utilisateur' vous permet de transmettre à un utilisateur normal sans droit d'administrateur la possibilité d'activer ou de désactiver les interfaces avec KInternet. Vous pouvez ensuite choisir votre pays et votre fournisseur d'accès. Le contenu des boîtes de dialogue suivantes dépend beaucoup des paramètres choisis. Par conséquent, ils ne seront décrits que brièvement. En cas de doute, veuillez lire les textes d'aide très détaillés des boîtes de dialogue.

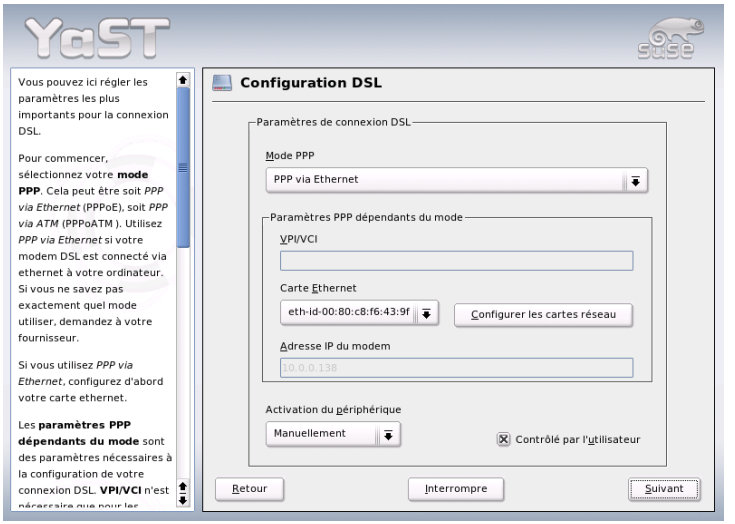


FIG. 22.5: *Configuration ADSL*

Pour pouvoir utiliser l'option 'Connexion à la demande' sur les systèmes monopostes, vous devez configurer le serveur DNS (serveur de noms) au cas par cas. La plupart des fournisseurs d'accès prennent actuellement en charge l'affectation dynamique du DNS : cela signifie que l'adresse IP actuelle du serveur de noms vous est transmise lorsque vous établissez la connexion. Dans cette boîte de dialogue, pensez cependant à saisir une adresse de remplacement pour un serveur DNS pour votre système monoposte, comme `192.168.22.99`. Si aucun serveur de noms ne vous a été affecté dynamiquement, indiquez ici les adresses IP du serveur de noms de votre fournisseur d'accès.

La liste déroulante 'Temps d'inactivité (secondes)' vous permet de définir un délai d'inactivité (sans transfert de données) après lequel la connexion sera automatiquement désactivée. Il est conseillé d'utiliser une valeur comprise entre 60 et 300 secondes.

Remarque

Connexion à la demande

Si vous avez choisi une 'Connexion à la demande', la connexion ne se désactive pas complètement après le délai d'inactivité mais reste dans un état qui lui permet une reconnexion dès que des données doivent être transférées. Si vous n'utilisez pas une 'Connexion à la demande', la connexion est réellement désactivée. Il est donc nécessaire de rétablir manuellement la connexion si des données doivent être à nouveau transférée. Dans ce cas, vous pouvez éviter la désactivation de la connexion en fixant le délai d'inactivité à 0 secondes.

Remarque

Pour configurer T-DSL (utilisé en Allemagne), procédez comme pour les connexions ADSL. Si vous choisissez 'T-Online' comme fournisseur d'accès, vous arrivez automatiquement à la boîte de dialogue de configuration de T-DSL. Saisissez alors les données suivantes : nom de connexion, numéro d'appel de T-Online, nom d'utilisateur et mot de passe. Ces informations sont disponibles sur votre document d'inscription à T-DSL.

22.4.5 RNIS

Ce module vous permet de configurer une ou plusieurs cartes RNIS dans votre système. Si YaST ne détecte pas automatiquement la carte réseau, choisissez-la à la main. Vous pouvez en principe configurer plusieurs interfaces mais normalement, mais cela ne devrait pas être nécessaire pour les utilisateurs privés, étant donné que l'on peut configurer plusieurs fournisseurs d'accès pour une même interface. Les boîtes de dialogue suivantes servent à la configuration des différents paramètres pour l'utilisation de la carte RNIS.

La boîte de dialogue suivante (voir figure 22.7 page 479) permet la 'Sélection du protocole RNIS'. L'option par défaut est 'Euro-ISDN (EDSS1)' (voir ci-dessous cas 1. et 2.a). Le protocole '1TR6' est utilisé pour les systèmes téléphoniques déjà anciens ou pour les grandes installations (voir cas 2.b). Aux États-Unis, on utilise 'NI1'. Vous pouvez chercher le code du pays dans la liste, le préfixe correct apparaît alors dans le champ de saisie à côté (par exemple, +33 pour la France). En outre, vous devez saisir le préfixe local dans 'Préfixe régional' (par exemple, 1 pour la région parisienne). Si nécessaire, saisissez également le numéro pour accéder à la ligne extérieure.

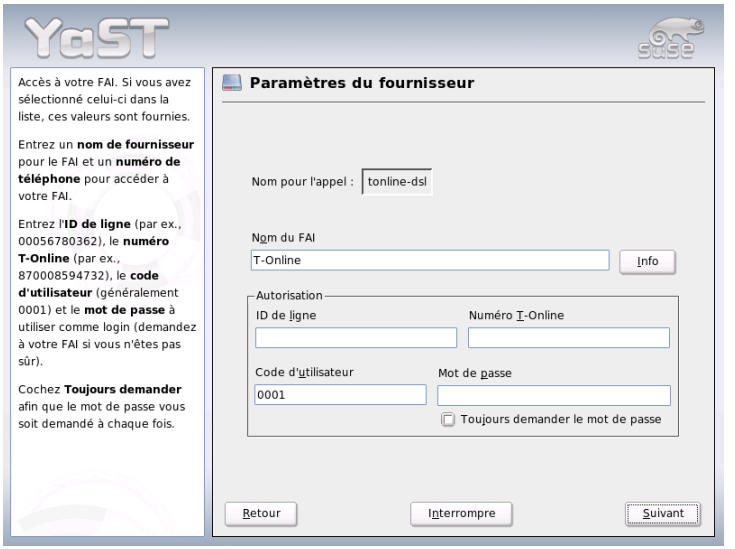


FIG. 22.6: *Configuration de T-DSL en Allemagne*

La liste 'Mode de démarrage' sert à définir le mode de démarrage pour la carte RNIS actuelle. 'Lors de l'amorçage' provoque le démarrage du pilote RNIS lors de l'amorçage du système. Si vous choisissez 'Manuel', l'utilisateur devra démarrer le pilote RNIS manuellement à l'aide de la commande `rcisdn start`. L'option 'Hotplug' charge le pilote lors du montage de la carte PCMCIA ou du périphérique USB. Une fois que vous avez configuré tous les paramètres, cliquez sur 'OK'.

Utilisez la boîte de dialogue suivante pour définir l'interface de la carte RNIS ou pour affecter d'autres fournisseurs d'accès à une interface existante. Les interfaces peuvent être définis avec les modes `SyncPPP` ou `RawIP`. La majorité des fournisseurs d'accès à Internet utilisent le mode `SyncPPP`, que nous décrivons ici.

La manière d'indiquer 'votre numéro de téléphone' sera différente selon les cas :

1. **La carte RNIS est branchée directement au NTBA de votre compagnie téléphonique**
   RNIS vous offre normalement trois numéros de téléphone par connexion (MSN, *Multiple Subscriber Number*) qui, sur demande, peuvent être augmentés à dix numéros. Vous devez affecter un des numéros MSN à votre

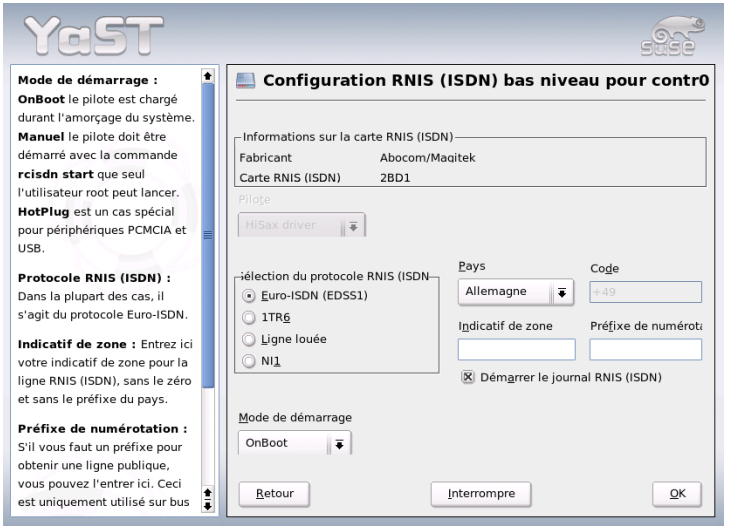


FIG. 22.7: *Configuration RNIS*

carte RNIS (à indiquer sans préfixe). Si vous faites une erreur, cela devrait malgré tout fonctionner, car votre compagnie téléphonique devrait dans ce cas remplacer le numéro erroné par le premier MSN attribué à votre raccordement RNIS.

2. **La carte RNIS est reliée à un central téléphonique**
   Selon le cas d'application, différentes indications sont nécessaires.

   (a) Pour l'utilisation privée : le protocole de l'autocommutateur (PABX) pour les raccordements internes est Euro-ISDN/EDSS1 (c'est généralement le cas pour les petites installations à usage privé). Ces installations sont dotées d'un bus S0 interne et utilisent des numéros internes pour les appareils connectés.

   Utilisez un des numéros internes pour indiquer le MSN. L'un ou l'autre des numéros devrait fonctionner à condition que l'accès vers l'extérieur soit disponible pour ce MSN. Mais en cas de besoin, un simple zéro devrait aussi pouvoir fonctionner. Vous trouverez des informations plus précises dans la documentation qui accompagne votre PABX.

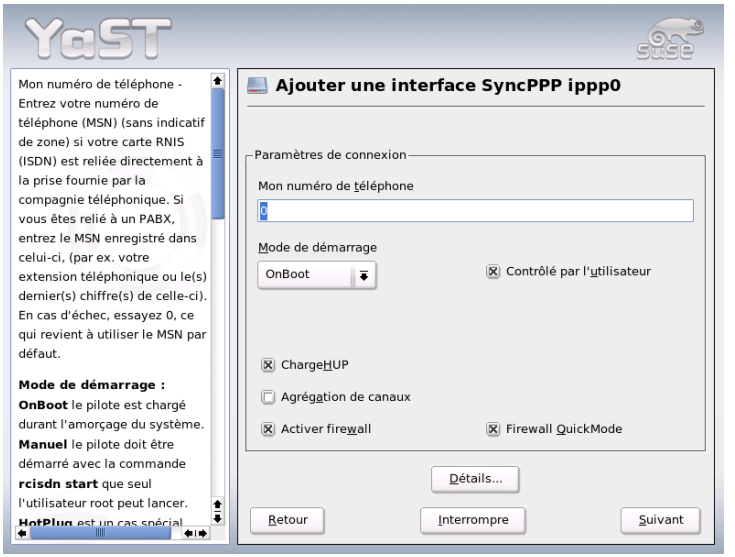


FIG. 22.8: *Configuration des interfaces RNIS*

(b) Pour un usage professionnel : le protocole de l'autocommutateur (PABX) pour les raccordements internes est 1TR6 (ceci n'est cependant le cas que pour les grandes installations en entreprise). Le MSN est ici remplacé par l'EAZ (en allemand, *Endgeräte-Auswahl-Ziffer* = numéro de sélection de l'appareil terminal). Lors de la configuration sous Linux, seul le dernier chiffre de l'EAZ doit en principe être spécifié. En cas d'urgence, essayez les chiffres de 1 à 9.

Cochez la case correspondante si vous souhaitez une déconnexion automatique avant le début de la prochaine unité de taxation ('ChargeHUP'). Notez que ce mécanisme ne fonctionne pas encore avec tous les fournisseurs d'accès. Pour bénéficier d'une 'aggrégation de canaux' (Multilink PPP), cochez la case correspondante. Si SuSEfirewall2 doit être démarré, cochez la case Activer le pare-feu. Pour permettre à un utilisateur normal sans droits d'administrateur d'activer ou de désactiver l'interface, cochez la case 'Contrôlé par l'utilisateur'.

Un clic sur Détails ouvre une boîte de dialogue consacrée à la configuration de cas de connexion plus complexes. Ceci ne présente généralement aucun intérêt pour les utilisateurs privés. Quittez cette boîte de dialogue en cliquant sur 'Suivant'.

Dans la boîte de dialogue suivante, indiquez les paramètres relatifs à l'affectation des adresses IP. Si votre fournisseur d'accès ne vous a affecté aucune adresse IP statique, choisissez 'Adresse IP dynamique'. Dans le cas contraire, saisissez dans les champs correspondants et selon les instructions de votre fournisseur d'accès, l'adresse IP locale de votre ordinateur ainsi que l'adresse IP distante. Si vous souhaitez utiliser cette interface en tant que route par défaut, cochez la case 'Route par défaut'. Notez que vous ne pouvez utiliser qu'une interface comme route par défaut par système. Quittez cette boîte de dialogue en cliquant sur 'Suivant'.

Dans la boîte de dialogue suivante, indiquez votre pays et votre fournisseur d'accès. Les fournisseurs d'accès de la liste sont du type Call-by-Call. Si vous souhaitez faire appel à un fournisseur d'accès qui ne se trouve pas dans la liste, cliquez sur 'Nouveau'. La fenêtre 'Paramètres ISP' apparaît, dans laquelle vous pouvez procéder à toutes les configurations liées à votre fournisseur d'accès. Dans 'Type RNIS', l'option par défaut est 'RNIS SyncPPP'. Les chiffres qui constituent le numéro de téléphone ne doivent pas être séparés par des virgules ou des espaces. Saisissez ensuite le nom d'utilisateur et le mot de passe qui vous ont été communiqués par votre FAI. Ppur finir, cliquez sur 'Suivant'.

Pour pouvoir utiliser l'option 'Connexion à la demande' sur les systèmes isolés, vous devez configurer le serveur DNS (serveur de noms) au cas par cas. La plupart des fournisseurs d'accès prennent actuellement en charge l'affectation dynamique du DNS : cela signifie que l'adresse IP actuelle du serveur de noms vous est transmise lorsque vous établissez la connexion. Dans cette boîte de dialogue, pensez cependant à saisir une adresse de remplacement pour un serveur DNS pour votre système isolé, `192.168.22.99`. Si un serveur de noms ne vous est pas affecté dynamiquement, indiquez ici les adresses IP du serveur de noms de votre fournisseur d'accès. En outre, vous pouvez fixer un délai d'inactivité après lequel la connexion sera automatiquement désactivée s'il n'y a pas eu de transfert de données. Cliquez sur 'Suivant' pour valider votre configuration et retourner à la boîte de dialogue d'aperçu dans laquelle la configuration de l'interface est affichée. Pour finir, activez votre configuration en cliquant sur 'Terminer'.

22.4.6 PCMCIA / USB

Les périphériques branchés à chaud ne nécessitent plus de prise en charge particulière puisque tous les périphériques sont initialisés avec Hotplug. Il faut tout de même en venir aux particularités du branchement à chaud correct/physique. Puisque que les périphériques intégrés sont toujours initialisés dans le même ordre, ils obtiennent toujours le même nom d'interface du noyau. Les noms d'interface sont attribués dynamiquement par le noyau ; dès qu'une interface est enregistrée elle reçoit le nom disponible suivant. Comme les périphériques que l'on peut brancher à chaud peuvent être détectés dans un ordre variable, ils ne reçoivent pas toujours le même nom d'interface et donc pas la même configuration puisque celle-ci dépend du nom d'interface. Si des noms d'interface persistants sont nécessaires, vous pouvez ajouter `PERSISTENT_NAME=` ⟨*nom*⟩ dans le fichier de configuration d'interface correspondant (`/etc/sysconfig/network/ifcfg-*`). Cette configuration prendra le relais à la prochaine initialisation (insertion) de carte.

22.4.7 Configuration d'IPv6

Si vous souhaitez configurer l'utilisation d'IPv6, il n'est en général pas nécessaire de configurer les postes de travail. Toutefois, vous devez mettre en œuvre la prise en charge d'IPv6. En tant qu'utilisateur , invoquez la commande `modprobe ipv6`.

En raison de la philosophie de configuration automatique d'IPv6, une adresse `lien local` est alors affectée à la carte réseau au sein du réseau. Aucune table de routage n'est en principe maintenue sur un poste de travail. Celui-ci peut consulter les routeurs dans le réseau grâce au Router Advertisement Protocol (protocole d'annonce de la présence d'un routeur) pour savoir quel préfixe et quelles passerelles utiliser. Pour mettre en place un routeur IPv6, appelez le programme radvd en saisissant `radvd`. Ce programme communique aux postes de travail le préfixe à utiliser pour les adresses IPv6 et le(s) routeur(s). On peut également installer le programme zebra prévu pour la configuration automatique d'adresses et à la configuration du routage.

Pour pouvoir affecter une adresse IPv6 à un poste de travail, il est donc conseillé d'installer et de configurer un routeur avec le programme radvd ou zebra. Les postes de travail se voient alors automatiquement attribuer l'adresse IPv6.

Pour mettre en service différents tunnels à l'aide des fichiers contenus dans `/etc/sysconfig/network`, vous trouverez des informations importantes dans la page de manuel de ifup (`man ifup`).

22.5 Le routage sous SUSE LINUX

Les réglages de la table de routage se trouvent dans les fichiers de configuration `/etc/sysconfig/network/routes` et `/etc/sysconfig/network/ifroute-*`.

Vous pouvez saisir dans le fichier `/etc/sysconfig/network/routes` toutes les routes statiques requises pour les différentes fonctions d'un système : une route vers une machine, une route vers une machine via une passerelle et une route vers un réseau. C'est ici par exemple que la passerelle par défaut est configurée dans le cas de routes statiques :

```
default
  GATEWAY - -
```

où GATEWAY est l'adresse IP de la passerelle.

Pour toutes les interfaces ayant besoin d'un routage individuel, il est possible d'utiliser un fichier distinct pour chaque interface : `/etc/sysconfig/network/ifroute-*`. Le caractère `*` doit être remplacé par le nom de l'interface. Les déclarations peuvent être organisées comme suit :

```
DESTINATION            GATEWAY  NETMASK    INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION            GATEWAY  PREFIXLEN  INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION/PREFIXLEN  GATEWAY  -          INTERFACE [ TYPE ] [ OPTIONS ]
```

Dans le cas où les paramètres GATEWAY, NETMASK, PREFIXLEN ou INTERFACE ne sont pas spécifiés, ils doivent être remplacés par le caractère `-`. Les paramètres TYPE et OPTIONS peuvent être simplement omis.

- La première colonne comporte la destination d'une route. Il peut s'agir de l'adresse IP d'un réseau ou d'une machine ou bien, dans le cas de serveurs de noms *accessibles*, du nom qualifié d'un réseau ou d'une machine.
- La deuxième colonne contient soit la passerelle par défaut soit une passerelle à partir de laquelle on peut accéder à une machine ou à un réseau.
- La troisième colonne comporte le masque réseau pour les réseaux ou les machines situés derrière une passerelle. Pour les machines situées derrière une passerelle, le masque est par exemple `255.255.255.255`.
- La dernière colonne est destinée aux réseaux connectés sur la machine locale (loopback, Ethernet, RNIS, PPP, ...). Elle doit comporter le nom du périphérique.

22.6 SLP — Transmission de services dans le réseau

Le *Service Location Protocol* (SLP) a été développé afin de simplifier la configuration des clients reliés au réseau à l'intérieur d'un réseau local. Pour configurer un client réseau, y compris tous les services souhaités, son administrateur a traditionnellement besoin d'une connaissance détaillée des serveurs disponibles dans son réseau. Avec SLP, la disponibilité d'un type de service défini est indiquée à tous les clients du réseau local. Les applications supportant SLP peuvent utiliser les informations émises via SLP et peuvent ainsi être configurées automatiquement.

22.6.1 Support SLP dans SUSE LINUX

SUSE LINUX supporte l'installation de sources d'installation transmises par SLP et comporte beaucoup de services système avec support intégré pour SLP. YaST et Konqueror dispose tous les deux d'applications correspondantes pour SLP. Utilisez SLP afin de mettre à la disposition des clients connectés les fonctions centrales comme le serveur d'installation, le serveur YOU, le serveur de fichiers ou le serveur d'impression sur votre SUSE LINUX.

Enregistrer ses propres services

Beaucoup d'applications sous SUSE LINUX disposent déjà d'un support SLP intégré par l'intermédiaire de l'utilisation de la bibliothèque `libslp`. Si vous désirez en outre rendre disponibles des services supplémentaires via SLP qui n'ont aucun support SLP intégré, plusieurs possibilités s'offrent à vous :

Enregistrement statique via `/etc/slp.reg.d`
Créez pour chaque nouveau service un fichier d'enregistrement propre. Voyez ci-dessous un exemple de ce type de fichier pour l'enregistrement d'un service scanner :

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

La ligne la plus importante de ce fichier est ce qu'on appelle l'*URL de service*, qui commence par `service:`. Elle contient le type de service (`scanner.sane`) et l'adresse sous laquelle le service est disponible sur le serveur. ⟨*$HOSTNAME*⟩ est automatiquement remplacé par le nom d'hôte complet. Séparé par deux points, arrive ensuite le port TCP sur lequel le service concerné écoute. Indiquez maintenant, séparée de l'URL de service par des guillemets, également la langue dans laquelle le service doit être indiqué et la durée de vie de l'enregistrement en secondes. La valeur pour la durée de vie de l'enregistrement peut se situer entre `0` et `65535`. Si vous indiquez `0`, l'enregistrement ne serait pas valable, avec `65535`, il n'est pas limité.

Le fichier d'enregistrement comporte en outre les deux variables `watch-tcp-port` et `description`. Le premier connecte l'indication SLP à ces variables, même si le service correspondant est actif, tandis que le slpd contrôle l'état du service. La dernière variable comporte une description plus précise du service qui est indiquée dans les navigateurs appropriés.

Enregistrement statique `/etc/slp.reg`
La seule différence avec la procédure décrite plus haut est la concentration de tous les services dans un unique fichier central.

Enregistrement dynamique avec slptool
Si un enregistrement SLP doit se faire à partir des propres scripts d'un service, utilisez l'application en lignes de commandes slptool.

Applications SLP dans SUSE LINUX

SUSE LINUX comporte plusieurs applications servant à interroger et à réutiliser les informations SLP via un réseau :

slptool slptool est un programme de lignes de commandes simple pouvant être utilisé pour transmettre des requêtes SLP sur le réseau ou également pour annoncer ses propres services. `slptool --help` énumère toutes les options et les fonctions disponibles. slptool peut également être appelé à partir de scripts qui doivent traiter les informations SLP.

YaST navigateur SLP YaST comporte sous 'Services réseau' → 'Navigateur SLP' son propre navigateur SLP, qui liste sous forme d'arborescence graphique tous les services annoncés dans le réseau local via SLP.

Konqueror Utilisé comme nagivateur de réseau, Konqueror peut indiquer avec l'appel `slp:/` tous les services SLP disponibles dans le réseau local. En cliquant sur les icônes apparaissant sur la fenêtre principale, vous recevrez des informations plus précises sur le service en question.

Si vous appelez Konqueror avec `service:/`, un clic sur l'icône correspondant dans la fenêtre du navigateur vous amène vers le service choisi.

Activer SLP

Remarque

Activation de slpd

Le slpd doit fonctionner sur votre système dès que vous voulez offrir vos propres services de serveur. Pour la seule interrogation de services, un démarrage de ce démon n'est pas nécessaire.

Remarque

Le démon slpd est contrôlé, comme la plupart des services système sous SUSE LINUX, via son propre script Init. Le démon est inactif par défaut. Si vous désirez l'activer pour la durée d'une session, utilisez comme `root` la commande `rcslpd start` afin de le démarrer et `rcslpd stop` pour l'arrêter. Avec `restart` ou `status`, vous déclenchez un redémarrage ou une demande d'état. Si slpd doit être actif par défaut, appelez une fois en tant que `root` la commande `insserv slpd`. Ainsi, slpd est automatiquement intégré dans la liste des services à démarrer lors de l'amorçage du système.

22.6.2 Informations supplémentaires

Pour des informations plus approfondies relatives au SLP, vous disposez des sources suivantes :

RFC 2608, 2609, 2610 RFC 2608 traite en général de la définition de SLP. RFC 2609 entre plus en détails dans la syntaxe des URL de service utilisés et RFC 2610 traite de DHCP via SLP.

http://www.openslp.com Le site du projet OpenSLP.

file:/usr/share/doc/packages/openslp/* Vous trouverez dans ce répertoire toute la documentation disponible au sujet de SLP ainsi qu'un `Lisez-moi.SuSE` avec les spécification SUSE LINUX, les RFC mentionnés ci-dessus et deux documents HTML d'introduction. Les programmeurs souhaitant utiliser les fonctions SLP doivent installer le paquetage `openslp-devel` afin d'exploiter le *Guide du Programmeur* joint.

22.7 DNS – Domain Name System

DNS (en anglais, *Domain Name System*) sert à résoudre les noms de domaines et de machines, c'est-à-dire à les convertir en adresses IP. Avant de configurer votre propre serveur de noms, nous vous recommandons de consulter les informations d'ordre général relatives au DNS dans la section *Résolution de noms (Domain Name System – DNS)* page 446.

Les exemples de configuration suivants font référence à BIND.

22.7.1 Démarrer le serveur de noms BIND

Le serveur de noms BIND (*Berkeley Internet Name Domain*) est déjà configuré dans SUSE LINUX de manière à ce que vous puissiez le démarrer tout de suite après avoir effectué l'installation. Lorsque vous avez déjà une connexion Internet qui fonctionne et que vous indiquez dans le fichier `/etc/resolv.conf` le serveur de noms `127.0.0.1` pour `localhost`, vous possédez déjà, en règle générale, une résolution de noms fonctionnant parfaitement sans connaître le DNS du fournisseur d'accès. BIND effectue alors la résolution de noms par l'intermédiaire du serveur de noms racine, ce qui est en revanche beaucoup plus lent. On devra normalement indiquer le DNS du fournisseur d'accès ainsi que son adresse IP dans le fichier de configuration `/etc/named.conf` dans la rubrique `forwarders` pour bénéficier d'une résolution de noms efficace et sûre. Tant que cela fonctionne, le serveur de noms fonctionne en tant que serveur de noms "cache seulement" (*caching-only*). Ce n'est que lorsque l'on mettra à sa disposition ses propres zones qu'il deviendra un véritable serveur de noms. Vous en trouverez un exemple simple dans le répertoire de documentation : `/usr/share/doc/packages/bind/sample-config`.

Remarque

Adaptation automatique des déclarations de serveurs de noms

Les déclarations des serveurs de noms peuvent être adaptées automatiquement à la situation, suivant la façon d'accéder à Internet ou l'environnement réseau actuel. Pour cela, positionnez la variable `MODIFY_NAMED_CONF_DYNAMICALLY` du fichier `/etc/sysconfig/network/config` à la valeur `yes`.

Remarque

Il ne faut cependant pas définir un nom de domaine officiel sans l'avoir fait au préalable approuver par l'institution compétente – pour `.fr`, il s'agit de l'AFNIC –. Même lorsque vous disposez de votre propre domaine, mais que celui-ci est géré par votre fournisseur d'accès, nous vous recommandons de ne pas l'utiliser dans la mesure où BIND ne redirigerait plus aucune requête pour ce domaine et que par exemple le serveur web du fournisseur d'accès dédié à votre propre domaine ne serait plus joignable.

Pour démarrer le serveur de noms, saisissez en tant que `root` la ligne de commande suivante :

```
rcnamed start
```

Si "done" apparaît en vert à droite, le processus `named`, c'est-à-dire le processus du serveur de noms, est démarré avec succès. Vous pouvez tester immédiatement sur le système local le fonctionnement du serveur de noms avec les programmes `host` ou `dig`. `localhost` doit apparaître comme serveur par défaut avec l'adresse `127.0.0.1`. Si tel n'était pas le cas, cela signifierait qu'un mauvais nom de serveur figure dans le fichier `/etc/resolv.conf` ou que ce fichier n'existe tout simplement pas. Pour un premier essai, saisissez `host 127.0.0.1`, qui fonctionne normalement toujours ; si vous obtenez un message d'erreur, utilisez la commande suivante pour vérifier que le processus `named` a bien été lancé

```
rcnamed status
```

Si le serveur de noms ne démarre pas ou présente un comportement incorrect, vous en trouverez la cause, la plupart du temps, dans le fichier `/var/log/messages`.

Pour utiliser en tant que "redirecteur" (*forwarder*) le serveur de noms du fournisseur d'accès ou un de vos propres serveurs de noms déjà en service sur votre réseau local, il faut l'indiquer (ou les indiquer) dans la section `options` avec le mot-clé `forwarders`. Les adresses IP utilisées dans l'exemple 22.10 page ci-contre sont choisies de manière arbitraire et doivent être adaptées à vos propres besoins.

Exemple 22.10: *Options de redirection (forwarding) dans named.conf*

```
options {
        directory "/var/lib/named";
        forwarders { 10.11.12.13; 10.11.12.14; };
        listen-on { 127.0.0.1; 192.168.0.99; };
        allow-query { 127/8; 192.168.0/24; };
        notify no;
        };
```

Après les `options` viennent les déclarations de zones, celles de `localhost`, `0.0.127.in-addr.arpa`, ainsi que de `.` de `type hint` qui doivent toujours être disponibles. Les fichiers correspondants ne doivent pas être modifiés, dans la mesure où ils fonctionnent en l'état. Vous devez veiller également à ce que chaque ligne soit suivie d'un `;` et que les accolades soient placées correctement. Si vous avez entrepris des modifications dans le fichier de configuration `/etc/named.conf` ou dans les fichiers des zones, vous devez ordonner à BIND de les lire à nouveau à l'aide de la commande `rcnamed reload`. Une autre solution consiste à redémarrer complètement le serveur de noms avec la commande `rcnamed restart`. Vous pouvez arrêter à tout moment le serveur de noms avec la commande `rcnamed stop`.

22.7.2 Le fichier de configuration /etc/named.conf

Tous les paramétrages du serveur de noms BIND s'effectuent dans le fichier `/etc/named.conf`. Les données de zone, les noms des machines, les adresses IP, etc. des domaines à gérer doivent être classés dans des fichiers séparés du répertoire `/var/lib/named`. Vous trouverez davantage d'informations à ce sujet plus loin.

Le fichier `/etc/named.conf` se divise principalement en deux parties : d'une part, la section `options` pour les paramètres d'ordre général et, d'autre part, les déclarations de `zone` des différents domaines. Vous pouvez, en outre, également définir une section `logging`, ainsi que des déclarations de type `acl` (en anglais,*Access Control List*). Les lignes de commentaires commencent par le signe #, mais vous pouvez également utiliser `//`.

L'exemple 22.11 page suivante présente un fichier `/etc/named.conf` minimaliste.

Exemple 22.11: *Fichier /etc/named.conf minimaliste*

```
options {
        directory "/var/lib/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
       type master;
       file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

Remarque

Informations complémentaires pour la configuration de BIND

Vous trouverez d"autres informations à jour concernant la configuration de BIND sous SUSE LINUX dans `/usr/share/doc/packages/bind/README.SuSE`.

Remarque

22.7.3 Les options de configuration les plus importantes de la section Options

répertoire "⟨*nom-du-repertoire*⟩" indique le répertoire dans lequel BIND trouve les fichiers contenant les données de zones. Il s'agit en général de `/var/lib/named`.

forwarders { ⟨*adresse-ip*⟩; }; indique le ou les serveurs de noms (la plupart du temps celui ou ceux du fournisseur d'accès) vers lequel ou lesquels on redirige les requêtes DNS auxquelles il n'est pas possible de répondre directement. À la place d'⟨*adresse-ip*⟩ vous devez mettre une adresse IP comme `10.0.0.1`.

forward first; a pour effet que les requêtes DNS sont redirigées avant même que le serveur de noms racine n'essaie de les résoudre. Vous pouvez utiliser `forward only` à la place de `forward first` pour que toutes les requêtes soient redirigées et que le serveur de noms racine ne soit plus du tout consulté. Cela peut se révéler utile pour la configuration des pare-feu.

listen-on port 53 { 127.0.0.1; ⟨*adresse-ip*⟩; };
indique à BIND sur quelles interfaces réseau et sur quel port il doit écouter les requêtes des clients. Vous n'êtes pas obligé de saisir `53` dans la mesure où 53 est de toute façon le port par défaut. `127.0.0.1` permet d'accepter les requêtes de localhost. Si vous omettez complètement cette ligne, par défaut toutes les interfaces sont utilisées.

listen-on-v6 port 53 { any; }; indique à BIND sur quel port il doit écouter les requêtes des clients qui utilisent IPv6. Outre `any`, seul `none` est également autorisé car le serveur écoute toujours l'adresse joker IPv6.

query-source address * port 53; Cette directive peut être utile lorsqu'un pare-feu bloque les requêtes DNS externes. Cela oblige BIND à effectuer ses requêtes vers l'extérieur à partir du port 53 et pas des ports supérieurs à 1024.

query-source-v6 address * port 53; Cette directive doit être utilisée pour les requêtes basées sur IPv6.

allow-query { 127.0.0.1; ⟨*réseau*⟩; }; précise les réseaux à partir desquels les clients ont le droit d'envoyer des requêtes DNS. Il faut mettre à la place de ⟨*réseau*⟩ une adresse de la forme i`192.168.1/24` où `/24` est un raccourci pour le nombre de bits dans le masque réseau, soit dans ce cas `255.255.255.0`.

allow-transfer { ! *; }; détermine quels ordinateurs sont autorisés à effectuer des transferts de zone. Cet exemple les interdit complètement du fait de la présence de `! *`. Sans cete directive, il est possible de réaliser des transferts de zone sans aucune limitation et depuis n'importe où.

statistics-interval 0; Sans cette directive, BIND produit toutes les heures plusieurs lignes de messages de statistiques dans `/var/log/messages`. saisissez `0` pour les empêcher complètement ; vous pouvez saisir ici l'intervalle en minutes.

cleaning-interval 720; Cette option définit au bout de quel intervalle BIND vide son cache. Cette action est à chaque fois consignée dans un enregistrement du fichier `/var/log/messages`. Le temps est indiqué ici en minutes. La valeur par défaut est de 60 minutes.

interface-interval 0; BIND parcourt régulièrement les interfaces réseau pour détecter de nouvelles interfaces ou celles qui ne sont plus disponibles. Réglez cette valeur à `0` pour l'en empêcher et pour que BIND n'écoute que les interfaces trouvées au démarrage. Vous pouvez aussi préciser l'intervalle en minutes. La valeur par défaut est de 60 minutes.

notify no; Le `no` signifie qu'aucun autre serveur de noms n'est averti en cas de modifications apportées aux données de zone ou lors du redémarrage du serveur de noms.

22.7.4 La section de configuration Logging

Vous pouvez configurer ce qui est consigné dans un journal, comment et à quel endroit de manière très souple avec BIND. Les paramétrages par défaut sont normalement suffisants. L'exemple 22.12 montre la forme la plus simple d'une telle directive et permet d'empêcher complètement la journalisation.

Exemple 22.12: *La journalisation est inhibée*

```
logging {
        category default { null; };
};
```

22.7.5 Structure des déclarations de zones

Après le mot-clé `zone`, on indique le nom du domaine géré – ici on a arbitrairement choisi `mon-domaine.fr`. Ce nom est suivi de `in` puis, entre accolades, d'un bloc d'options s'appliquant à ce domaine : cf. 22.13.

Exemple 22.13: *Déclaration de zone pour mon-domaine.fr*

```
zone "mon-domaine.fr" in {
       type master;
       file "mon-domaine.zone";
       notify no;
};
```

Si vous souhaitez définir une zone "esclave" (*slave*), changez juste la valeur du `type` en `slave` et indiquez un serveur de noms qui gère cette zone en tant que "maitre" (*master*) – mais il peut aussi s'agir d'un autre "esclave" ; cf. le fichier 22.14.

Exemple 22.14: *Déclaration de zone pour autre-domaine.fr*

```
zone "autre-domaine.fr" in {
       type slave;
       file "slave/autre-domaine.zone";
       masters { 10.0.0.1; };
};
```

Les options de zones :

type master; Le mot-clé `master` indique que cette zone est gérée par ce serveur de noms. Cela suppose que l'on dispose d'un fichier de zone correct.

type slave; Cette zone est transférée depuis un autre serveur de noms. Elle doit être utilisée en conjonction avec des serveurs maîtres.

type hint; La zone `.` de type `hint` est utilisée pour indiquer le serveur de noms racine. Vous pouvez laisser cette définition de zone telle quelle.

file "mon-domaine.zone" ou file "slave/autre-domaine.zone"; Cette déclaration indique le fichier dans lequel figurent les données de zone du domaine. Dans le cas d'un esclave, ce fichier n'est pas nécessaire car son contenu est récupéré sur un autre serveur de noms. Pour bien distinguer les fichiers maîtres des fichiers esclaves, on place les fichiers esclaves dans le répertoire `slave`.

masters { ⟨*adresse-ip-du-serveur*⟩; }; Cette directive n'est utile que pour les zones esclaves et elle indique depuis quel serveur de noms le fichier de zones doit être transférés.

allow-update { ! *; }; cette option régit l'accès en écriture depuis l'extérieur à ces données de zones. Les clients pourraient ainsi s'inscrire eux-mêmes dans le DNS, ce qui, pour des raisons de sécurité, ne serait pas souhaitable. Lorsque cette directive n'est pas présente, les mises à jour des zones sont généralement interdites. Dans cet exemple, cela ne changerait rien non plus dans la mesure où `! *` interdit également tout.

22.7.6 Structure des fichiers de zones

Deux types de fichiers de zones sont nécessaires : les premiers servent à associer l'adresse IP au nom de l'ordinateur et les autres fonctionnent en sens inverse et fournissent, pour une adresse IP donnée, le nom de l'ordinateur.

Remarque

Point (.) dans les fichiers de zones

Le `.` a une signification importante dans le fichier des zones. Si vous indiquez les noms des ordinateurs sans `.` final, la zone est toujours complétée. Il est donc important de terminer les noms d'ordinateurs complets par un `.` final, pour que le domaine n'y soit pas encore ajouté. Les principales causes d'erreurs dans la configuration des serveurs de noms sont les points oubliés ou mal placés.

Remarque

Considérons, tout d'abord, le fichier de zone `monde.zone`, responsable du domaine `monde.entier`, voir le fichier 22.15.

Exemple 22.15: *Fichier /var/lib/named/monde.zone*

```
1  $TTL 2D
2  monde.entier.   IN SOA      gateway  root.monde.entier. (
3              2003072441  ; serial
4              1D          ; refresh
5              2H          ; retry
6              1W          ; expiry
7              2D )        ; minimum
8
9              IN NS       gateway
10             IN MX       10 soleil
11
12 gateway     IN A        192.168.0.1
13             IN A        192.168.1.1
14 soleil       IN A        192.168.0.2
15 lune        IN A        192.168.0.3
16 terre        IN A        192.168.1.2
17 mars        IN A        192.168.1.3
18 www         IN CNAME    lune
```

Ligne 1 : `$TTL` définit la durée de vie par défaut (en anglais, *Time To Live*), c'est-à-dire la durée de vie valable de toutes les directives de ce fichier : 2 jours (2D = 2 days).

Ligne 2 : C'est ici que commence l'`enregistrement de contrôle SOA` (SOA = Start of Authority): :

- En première position, on trouve le nom du domaine à gérer `monde.entier`, ce dernier se terminant par un `.` car sinon la zone serait à nouveau ajoutée. Sinon, on peut aussi écrire ici un `@` pour que la zone de la directive correspondante soit extraite du fichier `/etc/named.conf`.
- Après `IN SOA`, on trouve le nom du serveur de noms qui sert de maître pour cette zone. Dans ce cas, le nom `gateway` est complété pour devenir `gateway.monde.entier` car il ne se termine pas par un `.`.
- Vient ensuite l'adresse électronique de la personne responsable du serveur de noms. Comme le signe `@` a déjà une signification particulière, il faut simplement écrire un `.` à la place. Ainsi, pour `root@monde.entier`, on écrit `root.monde.entier.`. N'oubliez pas le `.` à la fin, sans quoi la zone serait à nouveau ajoutée.
- Vient enfin une parenthèse `(` qui permet d'englober les lignes qui suivent jusqu'à la parenthèse `)` dans l'enregistrement SOA.

Ligne 3 : Le `numéro de série` est un nombre arbitraire qui doit être incrémenté à chaque modification de ce fichier. Il sert à informer les serveurs de noms secondaires (serveurs esclaves) des modifications entreprises. On a donc introduit pour ce faire un nombre à dix chiffres composé de la date et d'un numéro d'ordre de la forme `AAAAMMJJNN`.

Ligne 4 : La `fréquence d'actualisation` indique à quels intervalles le serveur de noms secondaire vérifie le `numéro de série` de la zone. Dans cet exemple, on a pris 1 jour (1D = 1 day).

Ligne 5 : La `fréquence des tentatives` indique l'écart de temps qui s'écoule avant qu'un serveur de noms secondaire, en cas d'erreur, n'essaie de contacter à nouveau le serveur principal. Dans le cas présent, on a 2 heures (2H = 2 hours).

Ligne 6 : La `durée d'expiration` indique la durée au bout de laquelle un serveur de noms secondaire jette les données mises en cache s'il n'a plus réussi à contacter le serveur principal. Dans le cas présent, il s'agit d'une semaine (1W = 1 week).

Ligne 7 : La dernière ligne du SOA est la `durée de vie de mise en cache des échecs`. Elle indique combien de temps les résultats des requêtes DNS des autres serveurs qui n'ont pu être résolues peuvent être conservées en mémoire cache.

Ligne 9 : `IN NS` indique le serveur de noms responsable de ce nom de domaine. Ici aussi, le nom `gateway` est complété pour devenir `gateway.monde.entier` car il ne se termine pas par un `.`. On peut utiliser plusieurs lignes de ce type, une pour le serveur principal et une pour chaque serveur de noms secondaire. Si `notify` dans le fichier `/etc/named.conf` ne vaut pas `no`, tous les serveurs de noms indiqués ici sont informés des modifications des données de la zone.

Ligne :10 : L'enregistrement MX indique le serveur de messagerie qui prend en charge, modifie ou redirige les messages pour le domaine `monde.entier`. Dans cet exemple, il s'agit de l'ordinateur `soleil.monde.entier`. Le chiffre qui précède le nom de l'ordinateur est la valeur de préférence. Ainsi, s'il existe plusieurs déclarations MX, c'est le serveur de messagerie dont la valeur de préférence est la plus petite qui est pris, et si la remise de courrier à ce serveur échoue, on essaie celui ayant la valeur plus élevée suivante.

Lignes 12 à 17 : Il s'agit là des véritables enregistrements d'adresses (en anglais, *address records*), dans lesquels on attribue une ou plusieurs adresses IP à un nom d'ordinateur. Les noms figurent ici sans `.` final, car ils sont indiqués sans domaine à leur suite et sont donc tous complétés par `monde.entier`. Deux adresses IP sont attribuées à l'ordinateur `gateway` car il est équipé de deux cartes réseau. Le `A` indique une adresse de machine traditionnelle ; on utilise `A6` pour les adresses IPv6. `AAAA` est un format dépassé pour les adresses IPv6.

Ligne 18 : On peut utiliser l'alias `www` pour désigner `lune` (`CNAME` = `canonical name`, nom canonique).

Pour la résolution inverse (en anglais, *reverse lookup*) des adresses IP en noms de machines, on utilise le pseudo-domaine `in-addr.arpa`. Ce dernier est ajouté à l'adresse réseau écrite dans l'ordre inverse. `192.168.1` devient donc `1.168.192.in-addr.arpa`.

Exemple 22.16: *Résolution inverse des adresses*

```
1
2  $TTL 2D
3  1.168.192.in-addr.arpa. IN SOA gateway.monde.entier. root.monde.entier. (
4                           2003072441      ; serial
5                           1D              ; refresh
6                           2H              ; retry
7                           1W              ; expiry
8                           2D )            ; minimum
9
```

```
10                              IN NS           gateway.monde.entier.
11
12  1                           IN PTR          gateway.monde.entier.
13  2                           IN PTR          terre.monde.entier.
14  3                           IN PTR          mars.monde.entier.
```

Ligne 1 : $TTL définit la durée de vie par défaut valable ici pour toutes les directives.

Ligne 2 : Ce fichier permet en principe la "résolution inverse" (*reverse lookup*) pour le réseau `192.168.1.0`. Comme la zone s'appelle ici `1.168.192.in-addr.arpa`, on ne souhaite bien entendu pas l'ajouter au nom d'hôte, c'est pour cette raison que l'on saisit ce dernier en entier avec le domaine et le `.` final. Le reste correspond à ce qui a déjà été décrit dans l'exemple précédent pour la zone `monde.entier`.

Lignes 3 à 7 : Voir l'exemple précédent pour `monde.entier`.

Ligne 9 : Cette ligne indique ici aussi à nouveau le serveur de noms responsable de cette zone, mais cette fois-ci, le nom est indiqué en entier, avec le domaine et le `.` final.

Lignes 11 à 13 : Il s'agit d'enregistrements pointeurs (*pointer records*) qui, pour une adresse IP pointent vers le nom d'ordinateur correspondant. On trouve au début de cette ligne uniquement le dernier chiffre de l'adresse IP, sans `.` final. Si l'on y ajoute la zone et que l'on fait abstraction de `.in-addr.arpa`, on obtient bien l'adresse IP complète en ordre inversé.

Les transferts de zones entre différentes versions de BIND ne doivent, normalement, pas poser de problème.

22.7.7 Transactions sécurisées

On peut effectuer des transactions sécurisées avec les "signatures de transactions" (TSIG, *transaction SIGnatures*). On utilise, pour ce faire, des clés de transaction (en anglais, *transaction keys*) et des signatures de transaction (en anglais, *transaction signatures*). La section suivante explique comment les générer et les utiliser.

Les transactions sécurisées sont nécessaires dans le cadre de la communication d'un serveur à un autre et pour l'actualisation dynamique des données de zones. Ainsi, un contrôle d'accès fondé sur des clés permet d'obtenir un niveau de sécurité bien plus élevé qu'un contrôle fondé sur les adresses IP.

Vous pouvez générer une clé de transaction avec la commande suivante (pour plus d'informations, cf. la page de manuel relative à la commande `dnssec-keygen`) :

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

Cette commande génère deux fichiers portant, par exemple, les noms suivants :

```
Khost1-host2.+157+34265.private
Khost1-host2.+157+34265.key
```

La clé est contenue dans les deux fichiers (par exemple `ejIkuCyyGJwwuN3xAteKgg==`). Pour une utilisation ultérieure, `Khost1-host2.+157+34265.key` doit être transmis par un chemin sécurisé (par exemple avec `scp`) à l'ordinateur distant et inséré sur ce dernier dans le fichier `/etc/named.conf` pour établir une communication sécurisée entre `host1` et `host2` :

```
key host1-host2. {
  algorithm hmac-md5;
  secret "ejIkuCyyGJwwuN3xAteKgg==";
};
```

Attention

Droits d'accès de `/etc/named.conf`

Faites attention à ce que les droits d'accès au fichier `/etc/named.conf` restent restreints ; la valeur par défaut est `0640` pour `root` et le groupe `named` ; vous pouvez aussi stocker la clé dans un fichier protégé indépendant pour l'inclure ensuite.

Attention

Pour que la clé pour `host2` soit utilisée sur le serveur `host1` avec, par exemple, l'adresse `192.168.2.3`, il faut saisir, sur le serveur, dans le fichier `/etc/named.conf`, les informations suivantes :

```
server 192.168.2.3 {
  keys { host1-host2. ;};
};
```

Il faut aussi saisir les directives correspondantes dans les fichiers de configuration de `host2`.

Pour effectuer des transactions sécurisées, il faut, en plus des ACL basées sur les adresses et les intervalles d'adresses IP, ajouter des clés TSIG, dont un exemple peut se présenter ainsi :

```
allow-update { key host1-host2. ;};
```

Pour en savoir plus, consultez le *Manuel de référence de l'administrateur BIND* sous `update-policy`.

22.7.8 Actualisation dynamique des données de zones

La mise à jour dynamique (en anglais, *dynamic update*) est le terme technique qui décrit l'ajout, la modification et la suppression de directives dans les fichiers de zones d'un serveur maître. Ce mécanisme est décrit dans la RFC 2136.

Les mises à jour dynamiques se configurent, par zone, à l'aide des options `allow-update` ou `update-policy` au niveau des déclarations des zones. Vous ne devez pas modifier manuellement les zones mises à jour de manière dynamique.

La commande `nsupdate` sert à transmettre au serveur les enregistrements à mettre à jour ; pour connaître sa syntaxe exacte, reportez-vous à la page de manuel de `nsupdate`. Pour des raisons de sécurité, la mise à jour doit impérativement s'effectuer au moyen de transactions sécurisées (TSIG) : cf. section *Transactions sécurisées* page 497.

22.7.9 DNSSEC

DNSSEC (en anglais, *DNS Security*, sécurité DNS) est décrite dans la RFC 2535 . Le manuel de BIND décrit les outils disponibles permettant d'utiliser DNSSEC.

Une zone sûre doit posséder une ou plusieurs clés de zones ; utilisez aussi pour générer celles-ci, à l'instar des clés d'hôtes, la commande `dnssec-keygen`. On utilise actuellement DSA pour le chiffrement.

Les clés publiques (en anglais, *public keys*) doivent être intégrées dans les fichiers de zones au moyen de `$INCLUDE`.

Toutes les clés sont regroupées en un ensemble à l'aide de la commande `dnssec-makekeyset`, lequel doit être acheminé jusqu'à la zone parent (*parent zone*) par un chemin sûr pour y être signé à l'aide de la commande `dnssec-signkey`. Les fichiers générés lors de cette signature doivent être utilisés pour signer les zones avec la commande `dnssec-signzone` et les fichiers en résultant doivent finalement être intégrés au fichier `/etc/named.conf` pour chaque zone.

22.7.10 Configuration avec YaST

Le module DNS de YaST sert à configurer un serveur DNS dans le réseau local. ce module connaît deux types différents de modes de fonctionnement :

Configuration avec l'assistant Lorsque le module démarre pour la première fois, vous devez prendre certaines décisions fondamentales en tant qu'administrateur. Une fois la configuration initiale terminée, le serveur est sommairement préconfiguré et en principe prêt à l'emploi.

Configuration avancée Le mode expert sert pour des tâches de configuration plus avancées comme les ACL, la journalisation; les clés TSIG, entre autres.

Configuration avec l'assistant

L'assistant se subdivise en trois boîtes de dialogue, à partir desquelles vous pouvez bifurquer à l'endroit approprié dans la configuration avancîe.

Installation du serveur DNS : paramètres des redirecteurs
Cette boîte de dialogue (voir figure 22.9 page suivante) apparaît lorsque ce module démarre pour la première fois. Décidez si vous souhaitez recevoir une liste des redirecteurs à partir du démon PPP dans le cas d'une connexion à haut débit (ADSL) ou RNIS ('Démon PPP définit les redirecteurs'), ou les lui donner vous-même ('Spécifier les redirecteurs manuellement').

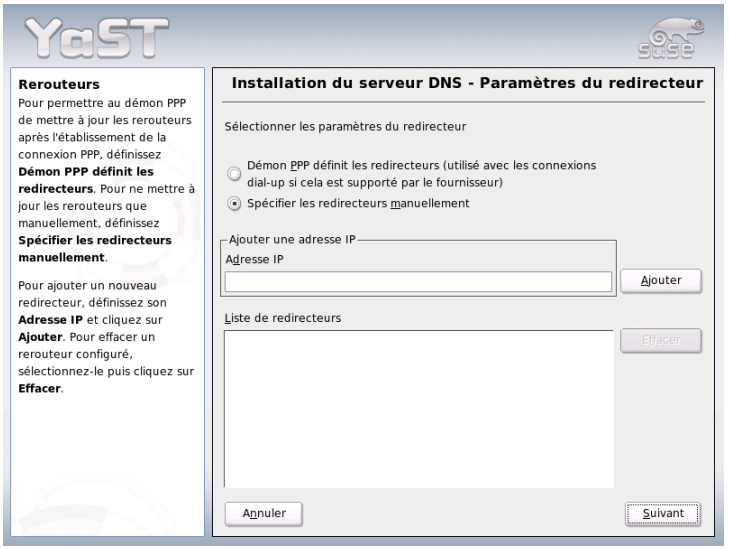


FIG. 22.9: *Installation du serveur DNS : redirecteurs*

Installation du serveur DNS : zones DNS
Les éléments de ce module sont expliqués dans l'installation en mode expert (voir la section *Serveur DNS : zones DNS* page 504).

Installation du serveur DNS : terminer avec l'assistant
Comme un pare-feu est activé pendant l'installation, vous pouvez pour terminer ouvrir le port DNS (port 53) du pare-feu avec 'Ouvrir port dans pare-feu' ainsi que configurer le comportement du serveur DNS à l'amorçage ('Marche' ou 'Arrêt'). Il est aussi possible d'accéder depuis cet endroit à la configuration avancée ('Configuration pour experts du serveur DNS...') (voir figure 22.10 page suivante).

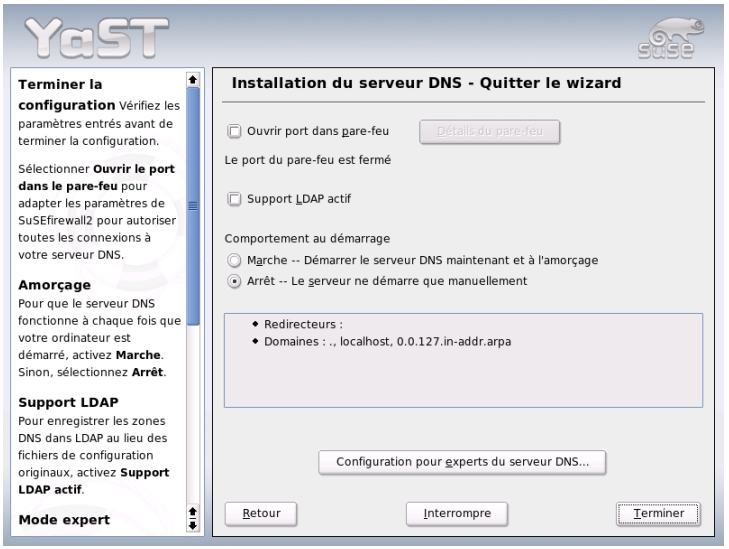


FIG. 22.10: *Installation du serveur DNS : terminer avec l'assistant*

Configuration avancée

Lorsque le module démarre pour la première fois, YaST ouvre une fenêtre offrant plusieurs possibilités de configuration. Dès que la configuration est terminée, le serveur DNS est en principe prêt à fonctionner :

Serveur DNS : démarrage Dans la section 'Amorçage', vous pouvez mettre en route le serveur DNS ('Marche') ou l'arrêter ('Arrêt'). Les boutons 'Démarrer le serveur DNS maintenant' et 'Arrêter le serveur DNS maintenant' permettent respectivement de démarrer et d'arrêter le serveur DNS. 'Enregistrer les paramètres et redémarrer le serveur DNS maintenant' vous permet d'enregistrer la configuration actuelle.

Vous pouvez ouvrir le port DNS du pare-feu ('Ouvrir port dans pare-feu') et modifier l'installation du pare-feu dans 'Paramètres du pare-feu'.

Serveur DNS : redirecteurs Cette boîte de dialogue est identique à celle qui apparaît au démarrage de l'assistant de configuration (voir section *Installation du serveur DNS : paramètres des redirecteurs* page 500).

Serveur DNS : journalisation Cette rubrique vous servira à paramétrer ce que le serveur DNS doit consigner dans son journal et où ce journal doit se trouver.

Précisez dans 'Type de journal' l'endroit auquel le serveur DNS doit consigner ses messages. Vous pouvez les laisser dans le système ('Journaliser dans le journal système' dans `/var/log/messages`) ou définir explicitement le fichier avec ('Journaliser dans le fichier'). Si vous avez choisi cette dernière possibilité, vous pouvez aussi indiquer la taille maximale du fichier en méga-octets et le nombre de ces fichiers journaux.

'Journalisations additionnelles' vous permet d'ajuster d'autres options. 'Journaliser les requêtes nommées' enregistre *chaque* requête. Le fichier journal peut donc devenir très volumineux rapidement. Vous ne devriez choisir cette option qu'à des fins de débogage. Pour piloter les mises à jour de zones entre le serveur DHCP et le serveur DNS, choisissez l'option'Journaliser les mises à jour de zone'. Pour consigner le flux de données lors du transfert des données de zones (transfert de zones) du maître vers l'esclave, activez l'option 'Journaliser les transferts de zone' (voir figure 22.11).

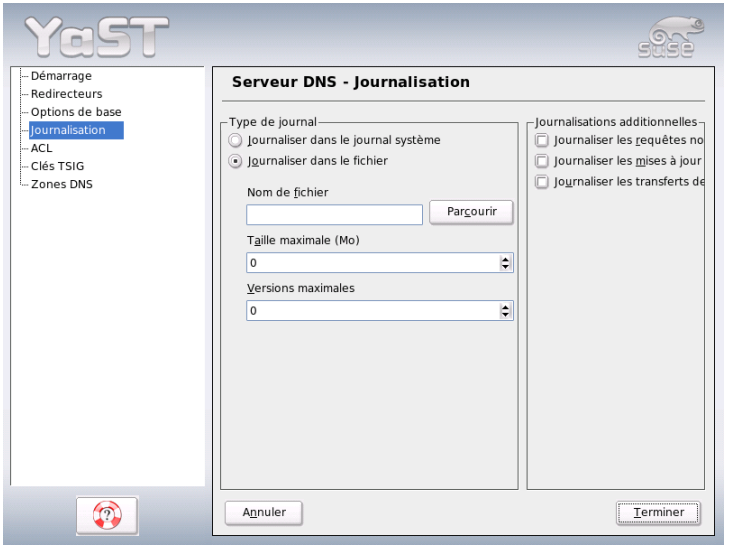


FIG. 22.11: *Serveur DNS : journalisation*

Serveur DNS : zones DNS Cette boîte de dialogue est divisée en plusieurs parties et permet ainsi de gérer des fichiers de zones (voir section *Structure des fichiers de zones* page 494).

Dans 'Nom de zone' saisissez le nouveau nom d'une zone. Pour créer des zones inverses, le nom de la zone doit se terminer par `.in-addr.arpa`. Choisissez le type (maître ou esclave) avec 'Type de zone' (voir figure 22.12). Le bouton 'Modifier zone...' vous permet de modifier d'autres réglages. Lorsque vous voulez supprimer une zone, choisissez 'Effacer zone'.

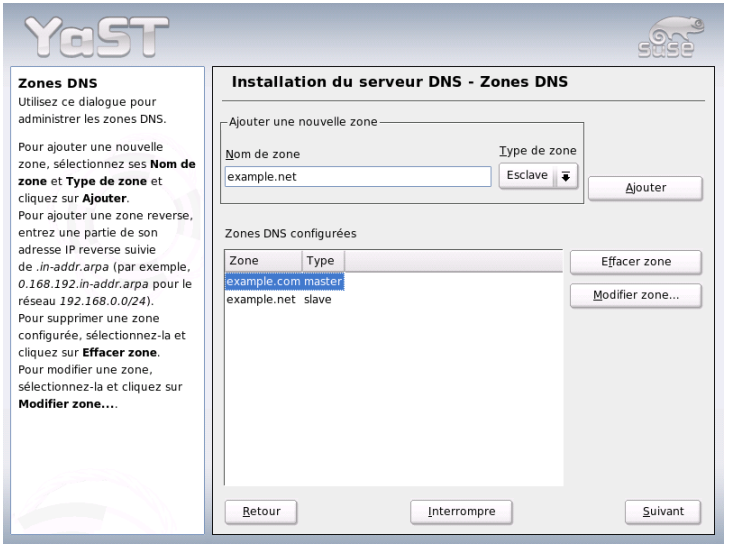


FIG. 22.12: *Serveur DNS : zones DNS*

Serveur DNS : éditeur de zones esclaves

Cette boîte de dialogue apparaît si vous avez choisi dans le point *Serveur DNS : zones DNS* page ci-contre 'Esclave' comme type de zone. Indiquez dans le champ 'Serveur DNS maître' le serveur maître auquel l'esclave doit s'adresser. Si vous souhaitez limiter l'accès, vous pouvez choisir les ACL définies au préalable dans la liste (voir figure 22.13).

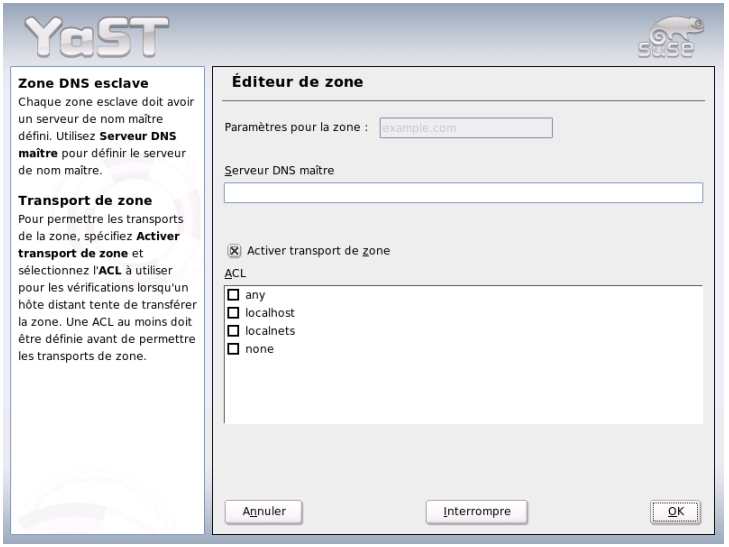


FIG. 22.13: *Serveur DNS : éditeur de zones esclaves*

Serveur DNS : éditeur de zones maîtres

Cette boîte de dialogue apparaît si vous avez choisi dans le point *Serveur DNS : zones DNS* page 504 'Maître' comme type de zone. Elle se subdivise en plusieurs vues : les bases (la page que vous voyez pour le moment), les enregistrements NS, les enregistrements MX, SOA et Enregistrements. Tous les points décrits ci-après se réfèrent à ceux qui ont été cités.

D'après la figure 22.14, vous définissez les réglages du DNS dynamique et les conditions d'accès concernant les transferts de zones au serveur de noms clients et esclave. Pour autoriser la mise à jour dynamique des zones, choisissez 'Autoriser les mises à jour dynamiques' et les clés de transaction correspondantes (TSIG). Veillez à ce qu'une clé ait déjà été définie au préalable avant de démarrer le processus de mise à jour.

Pour autoriser les transferts de zone, vous devez choisir l'ACL correspondante. Il faudra également que vous ayez déjà défini à l'avance les ACL.

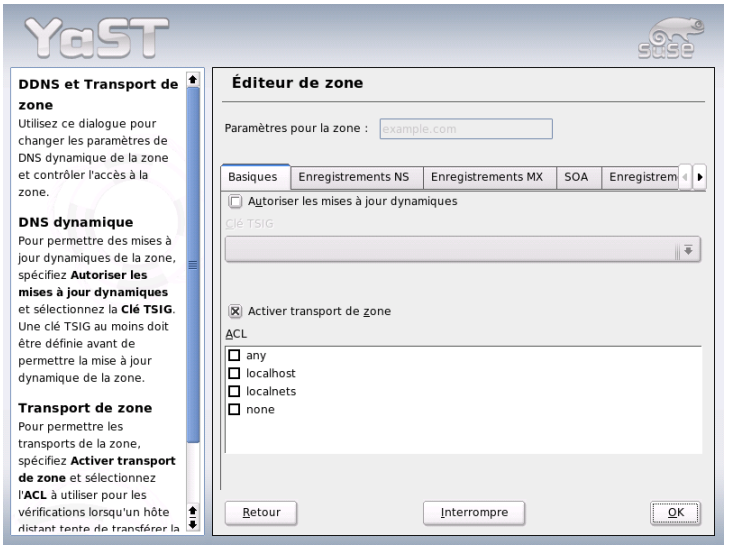


FIG. 22.14: *Serveur DNS : éditeur de zones (bases)*

Serveur DNS : éditeur de zones (enregistrements NSe)

Cette boîte de dialogue permet de définir un serveur de noms secondaire pour ces zones. Veillez à ce que le serveur de nom proprement dit soit contenu dans la liste. Pour saisir un nouvel enregistrement, indiquez dans 'Serveur de nom à ajouter' le nom correspondant et confirmez au moyen de 'Ajouter' (voir figure 22.15).

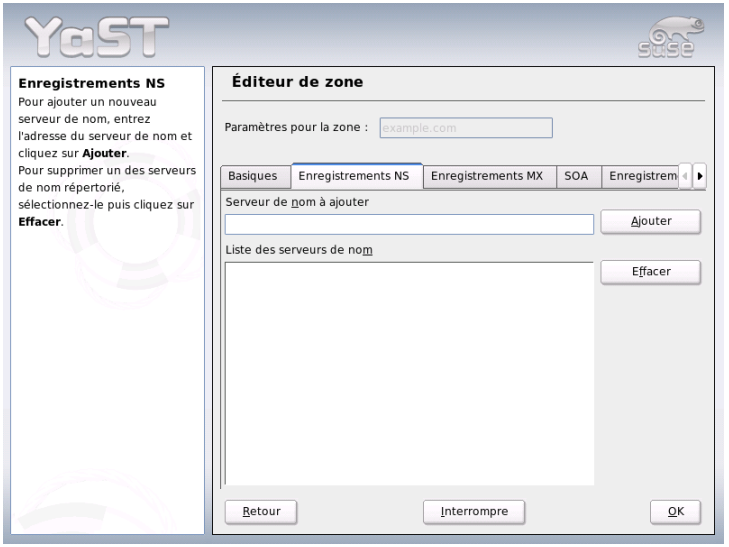


FIG. 22.15: *Serveur DNS : éditeur de zones (enregistrements NS)*

Serveur DNS : éditeur de zones (enregistrements MX)

Pour ajouter un nouveau serveur de messagerie pour la zone actuelle à la liste en place, indiquez l'adresse et les priorités qui conviennent. Confirmez au moyen de 'Ajouter' (voir figure 22.16 page suivante).

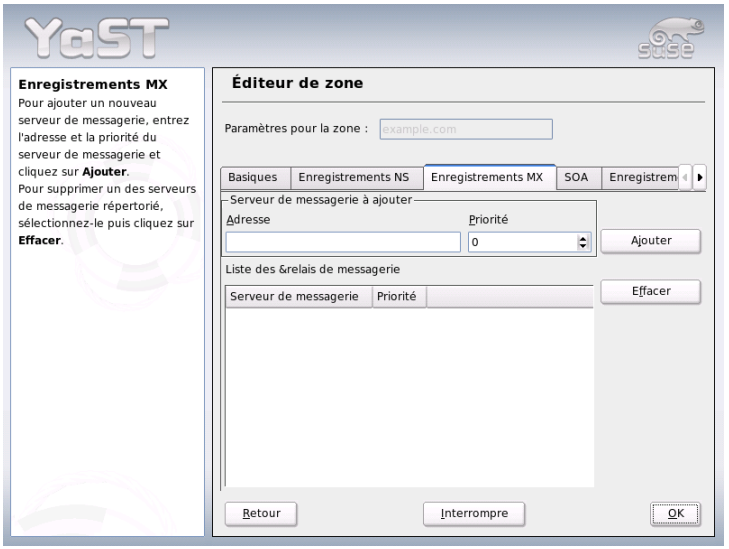


FIG. 22.16: *Serveur DNS : éditeur de zones (enregistrements MX)*

Serveur DNS : éditeur de zones (SOA)
Le message *SOA Record Configuration* (voir figure 22.17 page ci-contre) est utilisé pour indiquer les enregistrements SOA (*Start of Authority*). La signification des différentes options peut etre consultée dans l'exemple 22.15 page 494. Veillez à ce que cette option ne soit pas disponible avec des zones dynamiques en combinaison avec LDAP.

Serveur DNS : éditeur de zones (enregistrements)
Cette boîte de dialogue gère une liste d'affectations de noms à des adresses IP. Indiquez dans la zone de saisie 'Clé d'enregistrement' le nom d'hôte et choisissez le type (dans le menu du même nom). 'A-Record' est l'enregistrement principal ; 'CNAME' est un alias et dans 'MX-Relay', le nom (name) est remplacé par la valeur (value).

22.7.11 Informations supplémentaires

Nous vous recommandons notamment de consulter le *Manuel de référence de l'administrateur BIND* que vous trouverez en ligne dans `/usr/share/doc/packages/bind/`, ainsi que les RFC mentionnés dans ce dernier et les pages de manuel fournies avec BIND 9.

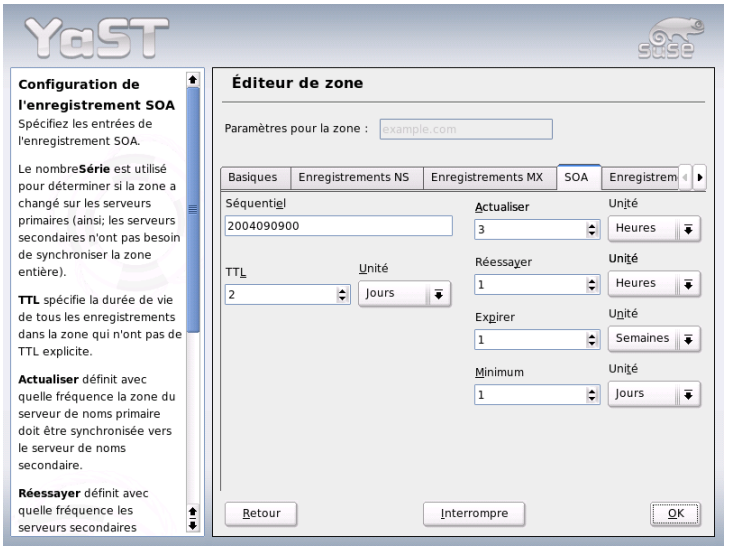


FIG. 22.17: *Serveur DNS : éditeur de zones (SOA)*

22.8 NIS – Network Information Service

Lorsque plusieurs systèmes Unix veulent accéder, au sein d'un réseau, à des ressources communes, il est nécessaire de s'assurer que les numéros des utilisateurs et des groupes sont cohérents sur toutes les machines. Le réseau doit être transparent pour l'utilisateur. Quelle que soit la machine sur laquelle l'utilisateur se trouve, ce dernier doit toujours retrouver le même environnement. Ceci est rendu possible par les services NIS et NFS. Le service NFS est chargé du partage des systèmes de fichiers en réseau. Il sera présenté à la section *NFS – Systèmes de fichiers partagés* page 541.

NIS (en anglais, *Network Information Service*) peut être envisagé comme un service de base de données qui permet d'accéder aux informations contenues dans les fichiers `/etc/passwd`, `/etc/shadow` ou `/etc/group` où que l'utilisateur se trouve dans le réseau. NIS peut aussi être utilisé pour d'autres tâches (par exemple pour `/etc/hosts` ou `/etc/services`), que nous ne détaillerons cependant pas dans cet ouvrage. On utilise souvent comme synonyme de NIS le terme *YP*. Celui-ci est l'acronyme de *yellow pages*, c'est-à-dire les *pages jaunes* du réseau.

22.8.1 Serveur NIS maître et esclave

Pour configurer NIS, choisissez dans YaST 'Services réseau', puis 'Serveur NIS'. Dans le cas où votre réseau ne comporte pas encore de serveur NIS, vous devez activer l'option 'Installer et configurer un serveur NIS maître' dans le formulaire de saisie qui s'ouvre alors. Dans le cas où vous avez déjà un serveur NIS (c'est-à-dire un serveur "maître"), vous pouvez ajouter un serveur NIS esclave (par exemple si vous créez un nouveau sous-réseau). Examinons tout d'abord la configuration du serveur maître. Dans le cas où certains paquetages requis ne sont pas installés, YaST vous demandera d'insérer le cédérom ou le DVD correspondant afin d'installer automatiquement les paquetages. Saisissez le nom de domaine dans le premier formulaire de saisie (illustration : 22.18). Cochez les cases situées en dessous pour déterminer si le serveur NIS doit également être un client NIS et si les utilisateurs recevant les données du serveur NIS pourront également se connecter sur cette machine.

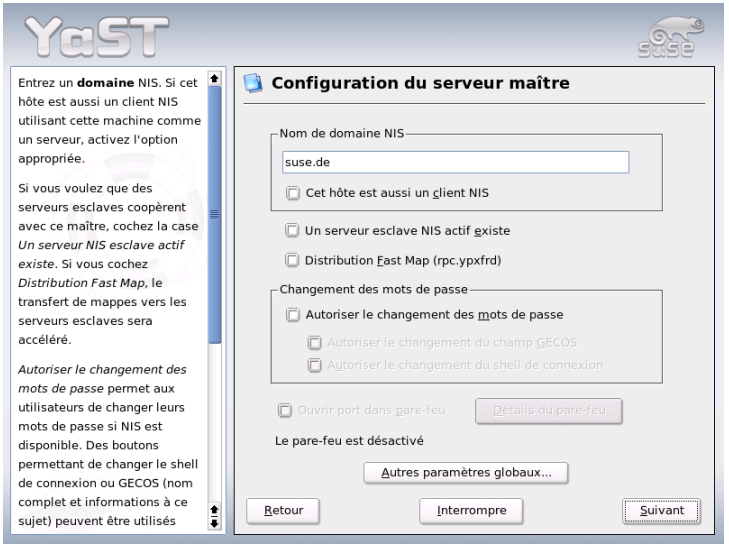


FIG. 22.18: *YaST : Utilitaire de configuration du serveur NIS*

Si vous souhaitez configurer des serveurs NIS supplémentaires (”serveurs esclaves“) dans votre réseau, vous devez cocher la case ‘Un serveur NIS esclave actif existe’. Vous devez aussi cocher la case ‘Distribution Fast Map’ qui a pour effet de transmettre rapidement les éléments de base de données du maître aux serveurs esclave.

Si vous souhaitez autoriser les utilisateurs de votre réseau à pouvoir modifier leurs mots de passe (avec la commande `yppasswd`, c’est-à-dire pas seulement les mots de passe locaux, mais ceux qui sont enregistrés sur le serveur NIS), vous pouvez aussi activer cette fonctionnalité ici. Les cases à cocher ‘Autoriser le changement du champ GECOS’ et ‘Autoriser le changement du shell de connexion’ sont alors aussi activées. ”GECOS“ signifie que l’utilisateur peut également modifier son nom et ses coordonnées (avec la commande `ypchfn`). ”SHELL“ signifie qu’il peut aussi modifier son interpréteur de commandes par défaut déclaré (avec la commande `ypchsh`, par exemple `bash` en `sh`).

Lorsque vous cliquez sur ‘Autres paramètres globaux...’, vous arrivez dans une boîte de dialogue (illustration : 22.19 page suivante) dans laquelle vous pouvez modifier le répertoire source du serveur NIS (par défaut `/etc`). Vous pouvez aussi y rassembler des mots de passe et des groupes. Laissez le réglage sur ‘Oui’ pour harmoniser les différents fichiers (`/etc/passwd` et `/etc/shadow` ou `/etc/group`). Vous pouvez aussi définir les numéros d’utilisateurs et de groupes les plus petits. Cliquez sur ‘OK’ pour confirmer les informations que vous avez saisies et pour revenir au formulaire précédent. Cliquez alors sur ‘Suivant’.

Dans le cas où vous avez précédemment coché la case ‘Un serveur esclave NIS actif existe’, vous devez à présent indiquer le nom des machines devant faire fonction d’esclave. Cliquez ensuite sur ‘Suivant’. Dans le cas où aucun serveur esclave n’est utilisé, vous arrivez directement à la boîte de dialogue pour la configuration de la base de données. Indiquez-y les ”tables de correspondance“ (en anglais, *maps*), autrement dit les parties de base de données qui doivent être transférées du serveur NIS au client correspondant. Les paramètres définis ici par défaut étant généralement judicieux, vous ne devriez normalement rien avoir à modifier.

Après avoir cliqué sur ‘Suivant’, vous arrivez à la dernière boîte de dialogue. Indiquez à partir de quels réseaux les requêtes adressées au serveur NIS seront émises (voir l’illustration : 22.20 page 513). Il s’agit normalement de votre réseau d’entreprise. Vous devriez alors avoir les deux lignes suivantes :

```
255.0.0.0 127.0.0.0
0.0.0.0   0.0.0.0
```

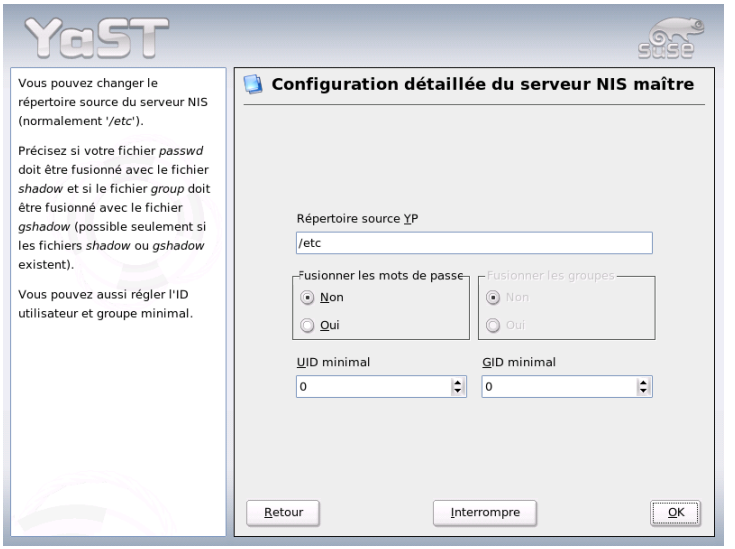


FIG. 22.19: *YaST : Serveur NIS : changer de répertoire et synchroniser les fichiers*

La première ligne autorise les liaisons provenant de votre propre machine, tandis que la seconde permet à toutes les machines ayant accès au réseau d'envoyer des requêtes au serveur.

Remarque

Configuration automatique du pare-feu

Si un pare-feu (SuSEfirewall2) fonctionne sur votre système, YaST procède à sa configuration pour le serveur NIS dès que vous sélectionnez 'Ouvrir ports dans le pare-feu'. YaST active alors le service `portmap`.

Remarque

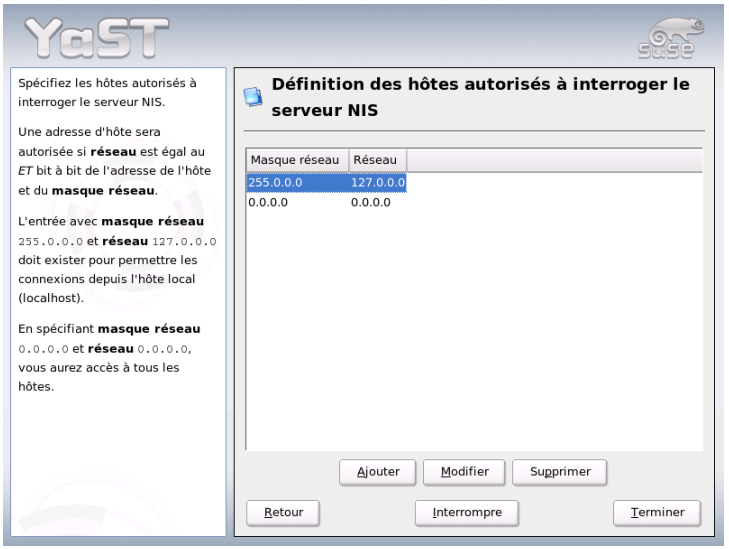


FIG. 22.20: *YaST : Serveur NIS : définition d'une autorisation de requête*

22.8.2 Le module client NIS dans YaST

Ce module vous permet de configurer aisément le client NIS. Après avoir choisi d'utiliser le serveur NIS dans le formulaire initial et décidé si cela se fait sous contrôle de l'automounter, vous arrivez au dernier formulaire. Indiquez-y si le client NIS possède une adresse IP statique ou s'il doit la recevoir par DHCP. Dans ce dernier cas, vous ne pouvez pas spécifier de domaine NIS ou d'adresse IP du serveur, dans la mesure où ces données sont également attribuées par DHCP. Pour plus d'informations sur le protocole DHCP, reportez-vous à la section *DHCP* page 546. Dans le cas où le client dispose d'une adresse IP valide, le domaine et le serveur NIS doivent être entrés à la main (voir l'illustration : 22.21 page suivante). Le bouton 'Rechercher' permet à YaST de chercher dans votre réseau un serveur NIS actif.

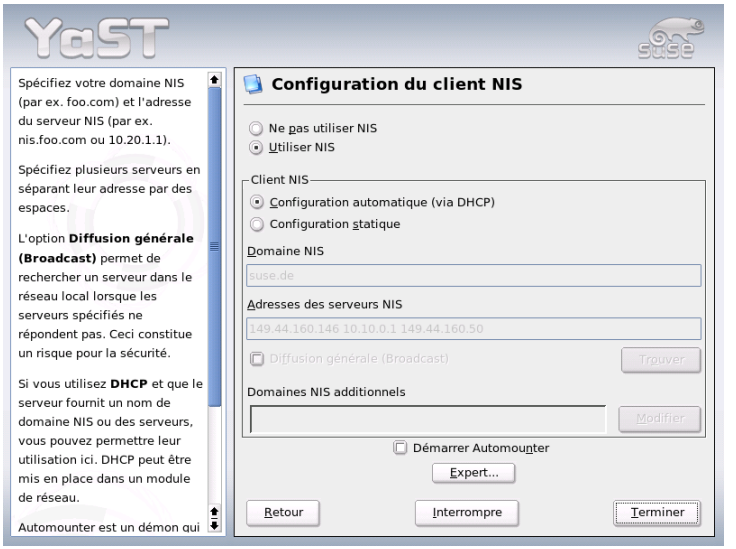


FIG. 22.21: *Saisie du domaine et de l'adresse du serveur NIS*

Vous avez également la possibilité de spécifier des domaines multiples ainsi qu'un domaine par défaut. Pour les différents domaines, vous pouvez utiliser le bouton 'Ajouter' pour déclarer plusieurs serveurs ainsi que la fonction de broadcast.

Vous pouvez éviter, dans la configuration experte, qu'une autre machine du réseau puisse demander quel serveur votre client utilise. Si vous activez 'Serveur défectueux', les réponses provenant d'un serveur sur un port non privilégié sont acceptées. Vous pourrez consulter les détails à ce sujet dans la page de manuel de `ypbind`.

22.9 LDAP – un service d'annuaire

Il est fondamental, dans un environnement de travail en réseau, de pouvoir disposer rapidement et de manière structurée de diverses informations importantes. Ce problème est résolu par un service d'annuaire permettant, comme les pages jaunes (en anglais *Yellow Pages*) du monde réel, d'accéder rapidement et de façon structurée aux informations recherchées.

Idéalement, il existe un serveur central gérant les données dans un annuaire et les partageant avec tous les clients dans le réseau à l'aide d'un protocole donné. Les données doivent être structurées de manière à permettre à la plus large gamme d'applications possible d'y accéder. Ainsi, il n'est pas nécessaire que chaque application d'agenda ou chaque client de messagerie gère ses propres bases de données, mais il suffit que chacun puisse accéder au référentiel commun. Ce mode de gestion réduit de manière appréciable la charge de gestion pour les informations concernées. Le fait d'utiliser un protocole ouvert et standardisé comme LDAP (*Lightweight Directory Access Protocol*) garantit qu'un maximum d'applications clientes peuvent accéder à ces informations.

Dans ce contexte, un annuaire est une sorte de base de données optimisée de manière à permettre une consultation et des recherches rapides et précises :

- Afin de permettre des accès en lecture nombreux (simultanés), on restreint l'accès en écriture par l'administrateur à un nombre d'actualisations réduit. Les bases de données classiques sont optimisées afin de pouvoir traiter très rapidement un volume de données considérable.
- Les accès en écriture ne doivent s'effectuer que de manière très limitée. C'est la raison pour laquelle on gère dans un service d'annuaire des informations *statiques*. En général, les données contenues dans une base de données classique se modifient très fréquemment (données *dynamiques*). Les numéros de téléphone dans un annuaire du personnel ont un rythme de modification beaucoup moins élevé que les chiffres traités par la comptabilité par exemple.
- Lorsque des données statiques sont gérées, il est très rare que les enregistrements existants soient mis à jour. Lorsque l'on gère des données dynamiques, en particulier pour des enregistrements tels que des comptes bancaires ou pour de la comptabilité, la cohérence des données est primordiale. Ainsi, si l'on doit débiter une somme à un endroit donné pour la créditer à un autre endroit, les deux opérations doivent être exécutées en même temps – dans le cadre d'une seule "transaction" afin de s'assurer que les données restent équilibrées. Les bases de données prennent en charge ce type de transactions, contrairement aux annuaires. Des incohérences temporaires dans les données sont tout à fait acceptables dans le cas des annuaires.

De par sa conception, un service d'annuaire tel que LDAP n'est pas prévu pour prendre en charge des mécanismes complexes de mises à jour ou de requêtes. Toutes les applications accédant à ce service doivent bénéficier d'un accès qui soit le plus aisé et le plus rapide possible.

Il y a eu et il y a encore un grand nombre de services d'annuaire, et pas uniquement dans le monde Unix : NDS de Novell, ADS de Microsoft, Street Talk de Banyan ainsi que la norme OSI X.500.

Le protocole LDAP était initialement conçu comme une variante allégée du protocole DAP (ou *Directory Access Protocol*), qui avait été conçu pour l'accès X.500. La norme X.500 régit l'organisation hiérarchique des enregistrements d'annuaire.

LDAP, qui a perdu quelques fonctions du protocole DAP, est multi-plate-forme et consomme peu de ressources, sans qu'il soit nécessaire de renoncer aux hiérarchies d'enregistrements définies dans X.500. L'utilisation de TCP/IP simplifie considérablement la réalisation d'interfaces entre les applications et le service LDAP.

Entre temps, le service LDAP a continué à se développer et est de plus en plus fréquemment utilisé comme solution à part entière sans prise en charge de X.500. Avec LDAPv3 (la version du protocole disponible avec le paquetage `openldap2` installé), LDAP prend en charge les *referrals* à l'aide desquels on peut créer des bases de données réparties. Autre nouveauté : la prise en charge de SASL (*Simple Authentication and Security Layer*), une couche d'authentification et de sécurité.

Le service LDAP ne se limite pas à l'interrogation de serveurs X.500, comme cela était initialement prévu. On utilise également le programme sldap, un serveur open source permettant d'enregistrer dans une base de données locale des informations sur des objets. Ce programme est complété par le programme slurpd, chargé de la réplication de plusieurs serveurs LDAP.

Le paquetage `openldap2` comporte deux programmes principaux.

slapd Un serveur LDAPv3 unique gérant des informations sur des objets dans une base de données de type BerkeleyDB.

slurpd Ce programme permet de répliquer des modifications apportées aux données du serveur LDAP local sur d'autres serveurs LDAP installés sur le réseau.

Autres outils de gestion système slapcat, slapadd, slapindex

22.9.1 LDAP par rapport à NIS

L'administrateur système Unix utilise traditionnellement le service NIS pour la résolution de noms et pour le partage des données au sein du réseau. Les clients se partagent en réseau les fichiers de configuration se trouvant sur un serveur central dans `/etc` ou dans l'un de ses sous-répertoires, comme `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` et `services`. S'agissant de simples fichiers de texte, la maintenance de ces fichiers ne pose pas de difficulté particulière. Toutefois, lorsque le volume de données est

important, ils s'avèrent peu pratiques à gérer en raison de l'absence de structuration. Le service NIS étant uniquement conçu pour les plate-formes Unix, il est impossible de l'utiliser pour une gestion centrale des données dans un réseau hétérogène.

À la différence du service NIS, le domaine d'utilisation du service LDAP ne se borne pas aux réseaux Unix. Les serveurs Windows (à partir de la version 2000) prennent en charge le service d'annuaire LDAP. Novell propose quant à lui également un service LDAP. Ce dernier ne se borne pas aux domaines d'utilisation précités.

Le principe de LDAP peut être appliqué à n'importe quel type de structures de données nécessitant une gestion centralisée. Voici quelques exemples d'applications :

- Utilisation à la place d'un serveur NIS
- Routage de messagerie (postfix, sendmail)
- Carnets d'adresses pour des clients de messagerie tels que Mozilla, Evolution, Outlook, ...
- Gestion de descriptions de zones pour un serveur de nom BIND9

Cette énumération pourrait se poursuivre, du fait de l'extensibilité de LDAP, à la différence de NIS. La structure hiérarchique clairement définie des données apporte une aide appréciable dans la gestion des volumes de données très importants, grâce aux facilités de recherche qu'elle autorise.

22.9.2 Structure d'une arborescence d'annuaires LDAP

Un annuaire LDAP utilise une structure arborescente. Tous les enregistrements (ou objets) de l'annuaire ont une position définie au sein de cette hiérarchie. Celle-ci est connue sous le nom *Directory Information Tree* ou DIT. Le chemin complet vers l'enregistrement souhaité permettant de l'identifier de manière unique est le *nom distingué* (*Distinguished name*) ou DN. Les différents nœuds du chemin vers cet enregistrement sont des *noms distingués relatifs* (*Relative Distinguished Name*) ou RDN. Les objets peuvent généralement être rattachés à deux types distincts :

Conteneur Ces objets peuvent contenir à leur tour d'autres objets. Ces classes d'objet sont `Root` (élément racine de l'arborescence qui n'existe pas réellement), `c` (pays, de l'anglais *country*), `ou` (unité d'organisation, de l'anglais *OrganizationalUnit*) et `dc` (composant de domaine, de l'anglais *DomainComponent*). Ce type d'objets peut également être comparé aux répertoires (dossiers) du système de fichiers.

Feuille Ces objets sont localisés à l'extrémité d'une branche. Aucun autre objet ne leur est rattaché. Les exemples sont `Person`, `InetOrgPerson` et `groupofNames`.

Un élément `Root` se trouve à la tête de l'arborescence. Vous pouvez lui rattacher au niveau suivant au choix `c` (*country*), `dc` (*domainComponent*) ou `o` (*organization*).

Les relations à l'intérieur d'une arborescence LDAP sont illustrées par l'exemple ci-après (voir l'illustration 22.22).

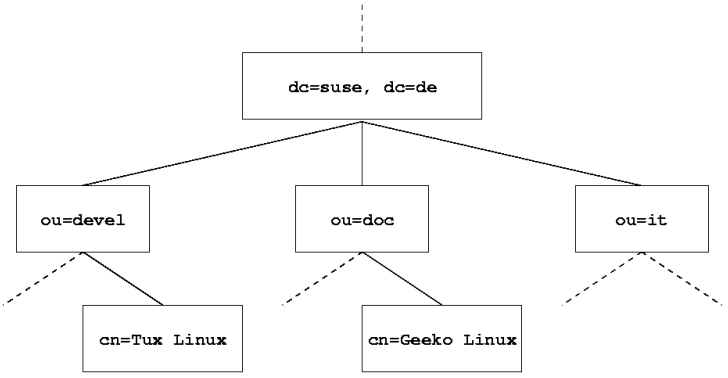


FIG. 22.22: *Structure d'un annuaire LDAP*

L'illustration décrit un *Directory Information Tree* fictif. Elle représente les enregistrements (*entries*) sur trois niveaux. Chaque enregistrement est représenté dans l'illustration par un rectangle. Le *nom distingué* (Distinguished Name) complet de l'employé SuSE fictif, `Geeko Linux` est en l'occurrence `cn=Geeko Linux,ou=doc,dc=suse,dc=de`. Il est formé en ajoutant le RDN `cn=Geeko Linux` au DN de l'enregistrement précédent `ou=doc,dc=suse,dc=de`.

Les types d'objets qu'on a décidé a priori d'enregistrer dans le DIT sont décrits par un *schéma*. Le type correspondant à un objet est défini par la *classe d'objet*. Celle-ci définit les attributs qui doivent ou qui peuvent être rattachés à l'objet concerné. Par conséquent, un schéma doit comporter les définitions de toutes les classes d'objets ainsi que les attributs utilisés dans le scénario de mise en œuvre souhaité. Il existe un certain nombre de schémas utilisables de manière générale (voir RFC 2252 et 2256). Il est également possible, toutefois, de créer des schémas

personnalisés ou d'en utiliser plusieurs sur une base de complémentarité, lorsque cela est requis par l'environnement dans lequel le serveur LDAP doit être mis en œuvre.

Le tableau 22.10 donne un aperçu des classes d'objet de `core.schema` et de `inetorgperson.schema` utilisées dans l'exemple ainsi que l'ensemble des attributs obligatoires requis et les valeurs d'attributs admises.

TAB. 22.10: *Classes d'objets et attributs fréquemment utilisés*

Classe d'objet	Signification	Exemple d'enregistrement	Attributs requis
dcObject	*domainComponent* (éléments constituant le nom du domaine)	suse	dc
organizationalUnit	*organizationalUnit* (unité d'organisation)	doc	ou
inetOrgPerson	*inetOrgPerson* (données nominatives pour intra-/Internet)	Geeko Linux	sn et cn

L'exemple 22.17 montre un extrait d'une instruction de schéma avec des explications utiles pour la compréhension de la syntaxe de nouveaux schémas.

Exemple 22.17: *Extrait de schema.core (les lignes ont été numérotées pour plus de clarté)*

```
...
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName')
#2        DESC 'RFC2256: organizational unit this object belongs to'
#3        SUP name )
...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5    DESC 'RFC2256: an organizational unit'
#6        SUP top STRUCTURAL
#7    MUST ou
#8        MAY (userPassword $ searchGuide $ seeAlso $ businessCategory $
              x121Address $ registeredAddress $ destinationIndicator $
```

```
                preferredDeliveryMethod $ telexNumber $
                teletexTerminalIdentifier $ telephoneNumber $
                internationaliSDNNumber $ facsimileTelephoneNumber $
                street $ postOfficeBox $ postalCode $ postalAddress $
                physicalDeliveryOfficeName $ st $ l $ description) )
...
```

L'exemple présente le type d'attribut `organizationalUnitName` et la classe d'objet correspondante `organizationalUnit`. La ligne 1 énumère le nom de l'attribut, son OID (identificateur d'objet, *Object Identifier*) (numérique) ainsi que la forme abrégée de l'attribut. La ligne 2 introduit avec `DESC` une brève description de l'attribut. Le RFC correspondant sur lequel est basée la définition y est également mentionné. `SUP` à la ligne 3 renvoie à un type d'attribut hiérarchiquement de niveau supérieur auquel cet attribut est rattaché.

La définition de la classe d'objet `organizationalUnit` commence à la ligne 4 par la définition d'attribut avec un OID et le nom de la classe d'objet. La ligne 5 comporte une brève description de la classe d'objet. À la ligne 6, l'enregistrement `SUP top` spécifie que cette classe d'objet n'est la sous-classe d'aucune classe d'objet. La ligne 7, commençant par `MUST`, énumère tous les types d'objets *obligatoirement* présents dans un objet de type `organizationalUnit`. La ligne 8 énumère, après `MAY`, tous les types d'attributs *utilisables* dans cette classe d'objet.

Vous trouverez une excellente introduction à l'utilisation des schémas dans la documentation OpenLDAP disponible dans votre système installé à l'emplacement `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

22.9.3 Configuration d'un serveur avec slapd.conf

Lorsque le système est installé, `/etc/openldap/slapd.conf` est disponible comme fichier de configuration complet pour le serveur LDAP. Vous trouverez ci-après une description des différents enregistrements, précisant les ajustements à apporter. Les lignes commençant par un # sont inactives. Pour activer ces lignes, il vous suffit de supprimer ce caractère de commentaire de la ligne choisie.

Instructions globales dans slapd.conf

Exemple 22.18: *slapd.conf : Instruction Include pour les schémas*

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/inetorgperson.schema
```

Cette première instruction de `slapd.conf` indique quel schéma est utilisé pour l'organisation de votre annuaire LDAP (voir l'exemple 22.18 page précédente). La ligne `core.schema` est toujours requise. Dans le cas où vous auriez besoin de schémas supplémentaires, ajoutez-les à la suite de cette instruction (l'exemple ajouté ici est `inetorgperson.schema`). Vous pourrez trouver d'autres schémas disponibles dans le répertoire `/etc/openldap/schema/`. Dans le cas où le service NIS doit être remplacé par un service LDAP équivalent, mentionnez à cet endroit les schémas `cosine.schema` et `rfc2307bis.schema`. Pour plus d'informations sur cette question, reportez-vous à la documentation OpenLDAP fournie.

Exemple 22.19: *slapd.conf : pidfile et argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Ces deux fichiers contiennent l'identificateur de processus (PID, de l'anglais *process id*) ainsi que différents arguments utilisés pour le lancement du processus slapd. Aucune modification n'est requise ici.

Exemple 22.20: *slapd.conf : Contrôle d'accès*

```
# Sample Access Control
#       Allow read access of root DSE
#       Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
#
access to dn="" by * read
access to *
       by self write
       by users read
       by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

L'exemple 22.20 page précédente correspond à la portion de code du fichier `slapd.conf` qui paramètre le contrôle d'accès à l'annuaire LDAP sur le serveur. Les paramètres qui sont définis dans la section globale du fichier `slapd.conf` s'appliquent tant qu'aucune règle d'accès particulière distincte n'a été établie dans la section propre à la base de données. Dans la configuration actuelle, tous les utilisateurs ont un accès en lecture à l'annuaire, mais l'administrateur (`rootdn`) est le seul à pouvoir écrire dans cet annuaire. La définition des privilèges d'accès sous LDAP est un processus extrêmement complexe. Nous vous présenterons donc quelques règles de base qui vous permettront de vous y initier.

- Chaque règle d'accès a la structure suivante :

  ```
  access to <what> by <who> <access>
  ```

- ⟨*what*⟩ représente l'objet ou l'attribut auquel vous accordez l'accès. Vous pouvez utiliser des règles séparées pour protéger de manière explicite différentes branches de l'arborescence ou des expressions rationnellles pour traiter des zones complètes de l'arborescence à l'aide d'une règle. Le programme slapd évalue toutes les règles dans l'ordre dans lequel elles ont été introduites dans le fichier de configuration. Vous devez donc toujours placer les règles génériques à la suite des règles plus spécifiques. La première règle pour laquelle slapd a établi qu'elle s'applique est évaluée et toutes les lignes suivantes sont ignorées.
- Le paramètre ⟨*who*⟩ détermine qui doit accéder aux domaines définis avec ⟨*what*⟩. Vous pouvez, ici aussi, utiliser des expressions rationnelles qui, convenablement conçues, vous permettront de gagner beaucoup de temps et d'énergie. Par ailleurs, le programme slapd interrompt l'évaluation de ⟨*who*⟩ après le première "concordance" ; ce qui revient à faire exécuter les règles plus spécifiques avant les règles plus générales. Il est possible d'avoir les enregistrements suivants (voir le tableau 22.11) :

TAB. 22.11: *Groupes d'utilisateurs autorisés*

Descripteur	Signification
*	tous les utilisateurs sans exception
`anonymous`	utilisateurs non authentifiés ("anonymes")
`users`	utilisateurs authentifiés
`self`	utilisateurs associés à l'objet cible
`dn.regex=<regex>`	Tous les utilisateurs auxquels cette expression rationnelle s'applique

- ⟨*access*⟩ spécifie le type d'accès. On ne fait pas la distinction entre les différentes possibilités présentes dans 22.12 :

TAB. 22.12: *Types d'accès*

Descripteur	Signification
`none`	Accès interdit
`auth`	pour la prise de contact avec le serveur
`compare`	pour l'accès aux objets pour comparaison
`search`	pour l'application de filtres de recherche
`read`	accès en lecture
`write`	accès en écriture

Le programme slapd compare les privilèges demandés par le client avec ceux qui sont accordés dans le fichier `slapd.conf`. Si des privilèges plus élevés ques ceux demandés par le client ou identiques sont accordés, le client reçoit l'autorisation d'accès. Si en revanche le client demande des élevés plus hauts que ce qui y est spécifié, il n'obtient aucune autorisation d'accès.

L'exemple 22.21 présente un exemple simple de contrôle d'accès que vous pouvez configurer à votre guise à l'aide d'expressions rationnelles.

Exemple 22.21: *slapd.conf: Exemple de contrôle d'accès*

```
access to  dn.regex="ou=([^,]+),dc=suse,dc=de"
   by dn.regex="cn=administrator,ou=$1,dc=suse,dc=de" write
   by user read
   by * none
```

Cette règle stipule que pour tous les enregistrements `ou`, seul l'administrateur concerné dispose de l'accès en écriture. Les autres utilisateurs authentifiés bénéficient d'un accès en lecture et le reste du monde n'a droit à aucun accès.

Remarque

Définition de règles d'accès

En l'absence de règle `access to` ou d'instruction `by <who>`, l'accès n'est pas autorisé. Seuls les droits d'accès spécifiés de manière explicite sont accordés. Dans le cas où aucune règle n'est définie, on applique le principe par défaut : droits en écriture pour l'administrateur et droits en lecture pour le reste du monde.

Remarque

Pour plus d'informations et un exemple de configuration portant sur les privilèges d'accès LDAP, reportez-vous à la documentation en ligne du paquetage `openldap2` installé. Pour la gestion des contrôles d'accès, il est possible d'utiliser, outre le fichier central de configuration du serveur (`slapd.conf`), les ACI, ou informations de contrôle d'accès (de l'anglais *Access Control Information*). Les ACI permettent d'enregistrer les informations d'accès à différents objets dans l'arborescence LDAP elle-même. Ce mode d'accès étant encore peu diffusé et étant considéré par les développeurs eux-mêmes comme étant de niveau expérimental, nous vous renvoyons ici aux pages correspondantes de la documentation du projet OpenLDAP : `http://www.openldap.org/faq/data/cache/758.html`.

Instructions propres à une base de données dans slapd.conf

***Exemple* 22.22:** *slapd.conf : Instructions propres à une base de données*

```
database ldbm
suffix "dc=suse,dc=de"
rootdn "cn=admin,dc=suse,dc=de"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap
# Indices to maintain
index   objectClass     eq
```

La première ligne de cette section (voir l'exemple 22.22 page ci-contre) définit le type de base de données, en l'occurrence LDBM. Le paramètre `suffix` à la seconde ligne définit la partie de l'arborescence LDAP dont ce serveur doit être responsable. Le `rootdn` suivant indique qui dispose des privilèges d'administrateur sur ce serveur. L'utilisateur indiqué ici ne doit pas pas posséder d'enregistrement LDAP ni exister comme utilisateur "normal". L'instruction `rootpw` définit le mot de passe de l'administrateur. Vous pouvez saisir ici à la place de `secret` le hachage du mot de passe de l'administrateur créé avec slappasswd. L'instruction `directory` spécifie le répertoire dans lequel les annuaires de la base de données sont enregistrés sur le serveur. La dernière instruction, `index objectClass eq`, permet de gérer un index à partir des classes d'objets. Le cas échéant, complétez quelques attributs parmi ceux que vous estimez les plus recherchés. Si vous ajoutez vos propres règles `Access` pour la base de données, elles sont utilisées à la place des règles `Access` globales.

Démarrage et arrêt du serveur

Lorsque la configuration du serveur LDAP est terminée et que tous les enregistrements souhaités ont été créés dans l'annuaire LDAP sur le modèle décrit ci-après (voir la section *Manipulation de données dans l'annuaire LDAP* de la présente page), démarrez le serveur LDAP en tant qu'utilisateur `root` à l'aide de la commande suivante :

```
rcldap start
```

Si vous voulez arrêter à nouveau le serveur à la main, saisissez la commande `rcldap stop`. On peut demander l'état d'exécution du serveur LDAP à l'aide de la commande `rcldap status`. Vous pouvez automatiser le démarrage et l'arrêt du serveur lors de la mise en marche et de l'arrêt de la machine concernée à l'aide de l'éditeur de niveaux d'exécution de YaST (voir la section *Éditeur de niveaux d'exécution de YaST* page 267) ou créer vous-même les liens correspondants pour les scripts de démarrage et d'arrêt à l'aide de la commande `insserv` (voir la section *Ajouter des scripts d'initialisation* page 265).

22.9.4 Manipulation de données dans l'annuaire LDAP

OpenLDAP met à votre disposition, pour votre activité d'administrateur, toute une série de programmes pour la gestion des données dans l'annuaire LDAP. Nous présenterons ci-après les quatre principaux d'entre eux pour les opérations d'ajout, de suppression, de recherche et de modification de données.

Création de données dans l'annuaire LDAP

À supposer que la configuration de votre serveur LDAP dans `/etc/openldap/slapd.conf` soit correcte et opérationnelle, c'est-à-dire qu'elle comporte les indications appropriées pour `suffix`, `directory`, `rootdn`, `rootpw` et `index`, vous pouvez commencer à présent à ajouter de nouveaux enregistrements. OpenLDAP propose à cet effet le programme `ldapadd`. Pour des raisons pratiques, il est recommandé, dans la mesure du possible, d'ajouter les objets à la base de données par groupes. Le service LDAP utilise à cette fin le format LDIF (de l'anglais *LDAP Data Interchange Format*). Un fichier LDIF est un fichier texte simple comportant un nombre quelconque de paires attribut-valeur. Les classes d'objets et les attributs disponibles figurent dans les fichiers schémas spécifiés dans `slapd.conf`. Le fichier LDIF destiné à créer un schéma grossier pour l'exemple 22.22 page 518 se présenterait ainsi (voir l'exemple 22.23) :

Exemple 22.23: *Exemple de fichier LDIF*

```
# L'organisation SuSE
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SuSE AG
dc: suse

# L'unité d'organisation Développement (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# L'unité d'organisation Documentation (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# L'unité d'organisation Informatique interne (it)
dn: ou=it,dc=suse,dc=de
objectClass: organizationalUnit
ou: it
```

Remarque

Codage des fichiers LDIF

LDAP utilise le codage UTF-8 (Unicode). Par conséquent, les caractères spéciaux et accentués doivent être convenablement codés à la saisie. Depuis SUSE LINUX 9.1, UTF-8 est le codage standard et est supporté par tous les éditeurs courants. Si vous avez défini un autre codage pour votre environnement (voir section *Adaptations locales et linguistiques* page 249), vous devrez soit vous passer complètement des caractères spéciaux et accentués, soit utiliser iconv pour le transcodage vers UTF-8 des données saisies.

Remarque

Enregistrez le fichier sous le nom `<fichier>.ldif` et transférez-le sur le serveur à l'aide de la commande suivante :

```
ldapadd -x -D <dn de l'administrateur> -W -f <fichier>.ldif
```

La première option `-x` indique que vous renoncez dans ce cas à utiliser l'authentification via SASL. Le paramètre `-D` désigne l'utilisateur chargé de cette opération ; saisissez ici le DN valide de l'administrateur tel qu'il a été configuré dans `slapd.conf`. Dans un exemple concret, nous aurions `cn=admin,dc=suse,dc=de`. Le paramètre `-W` permet de contourner la saisie du mot de passe sur la ligne de commande (en clair) et d'activer une demande de mot de passe séparée. Le mot de passe en question a été créé précédemment dans `slapd.conf` sous `rootpw`. Le paramètre `-f` passe le fichier. Vous pouvez voir dans l'exemple 22.24 le détail de l'appel de `ldapadd`.

Exemple 22.24: *ldapadd de exemple.ldif*

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f exemple.ldif

Enter LDAP password:
adding new entry "dc=suse,dc=de"
adding new entry "ou=devel,dc=suse,dc=de"
adding new entry "ou=doc,dc=suse,dc=de"
adding new entry "ou=it,dc=suse,dc=de"
```

Vous pouvez spécifier les données personnelles des différents employés dans des fichiers LDIF séparés. Dans l'exemple `tux.ldif` ci-après (voir l'exemple 22.25 page suivante), l'employé `Tux` est ajouté au nouvel annuaire LDAP :

Exemple 22.25: *Fichier LDIF pour Tux*

```
# Employé Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@suse.de
uid: tux
telephoneNumber: +49 1234 567-8
```

Un fichier LDIF peut comporter un nombre quelconque d'objets. Vous pouvez transférer au serveur des arborescences complètes ou uniquement des parties telles que des objets distincts. Si vous devez modifier vos données selon une fréquence relativement élevée, il est recommandé de définir une granularité fine avec des objets distincts, ce qui permet de faciliter le travail de recherche de l'objet à modifier dans un fichier de grande taille.

Modification des données dans l'annuaire LDAP

Lorsque des modifications sont prévues dans votre enregistrement, utilisez le programme `ldapmodify`. Le plus simple consiste à modifier dans un premier temps le fichier LDIF concerné, puis à transférer le fichier modifié au serveur LDAP. Ainsi, pour changer le numéro de téléphone de l'employé `Tux` de `+33 12 34 56 78 90` en `+33 12 34 56 78 45`, vous devez éditer le fichier LDIF, comme indiqué dans l'exemple 22.26.

Exemple 22.26: *Fichier LDIF modifié tux.ldif*

```
# Employé Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +33 12 34 56 78 90
```

Importez le fichier modifié dans l'annuaire LDAP à l'aide de la commande suivante :

```
ldapmodify -x -D cn=admin,dc=suse,dc=de -W -f tux.ldif
```

Autre possibilité : utiliser `ldapmodify` pour spécifier directement sur la ligne de commande les attributs à modifier. La procédure est la suivante :

1. Exécutez la commande `ldapmodify` et saisissez votre mot de passe :

   ```
   ldapmodify -x -D cn=admin,dc=suse,dc=de -W

   Enter LDAP password:
   ```

2. Faites vos modifications dans l'ordre suivant, en respectant la syntaxe indiquée ci-après :

   ```
   dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
   changetype: modify
   replace: telephoneNumber
   telephoneNumber: +33 12 34 56 78 45
   ```

Pour plus d'informations sur la commande `ldapmodify` et sur sa syntaxe, reportez-vous à la page de manuel de `ldapmodify`.

Rechercher ou extraire les données d'un annuaire LDAP

OpenLDAP fournit avec le programme ldapsearch un utilitaire en ligne de commande pour la recherche et l'extraction des données dans l'annuaire LDAP. Ainsi, une commande de recherche utiliserait la syntaxe suivante :

```
ldapsearch -x -b dc=suse,dc=de "(objectClass=*)"
```

L'option `-b` définit la base de la recherche, c'est-à-dire la partie de l'arbre dans laquelle la recherche doit se faire. Il s'agit dans le cas présent de `dc=suse, dc=de`. Pour effectuer une recherche plus fine dans des sous-domaines donnés de l'annuaire LDAP (par exemple uniquement dans la division `devel`), utilisez `-b` pour passer cette branche. Le programme `ldapsearch -x` indique qu'il faut utiliser une authentification simple. `(objectClass=*)` vous permet de décider que vous voulez lire tous les objets contenus dans votre annuaire. Utilisez cette commande après avoir constitué une nouvelle arborescence afin de vérifier si tous vos enregistrements ont été convenablement mis en place et si le serveur répond comme convenu. Vous trouverez des informations supplémentaires sur l'utilisation du programme `ldapsearch` dans la page de manuel correspondante (`man ldapsearch`).

Supprimer des données d'un annuaire LDAP

Supprimez les enregistrements dont vous n'avez plus besoin à l'aide du programme `ldapdelete`. La syntaxe est analogue à celle des commandes précédemment décrites. Ainsi, pour supprimer complètement du système l'enregistrement de l'utilisateur `Tux Linux`, vous devez saisir la commande suivante :

```
ldapdelete -x -D cn=admin,dc=suse,dc=de -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

22.9.5 Le client LDAP YaST

YaST supporte l'administration des utilisateurs avec LDAP. Pour activer ce support s'il ne l'a pas été lors de l'installation, passez par le module 'Services réseau' → 'Client LDAP'. YaST installe et configure automatiquement les adaptations LDAP décrites ci-dessous pour PAM et NSS.

Déroulement général

Pour comprendre le fonctionnement du module client LDAP de YaST, vous devez avoir une idée plus ou moins précise des processus s'exécutant en arrière-plan sur votre machine cliente. Dès que vous activez, lors de l'installation, l'utilisation de LDAP pour l'authentification réseau, ou que vous appelez le module YaST, les paquetages `pam_ldap` et `nss_ldap` sont installés et les deux fichiers de configuration correspondants sont modifiés. Le module PAM nommé `pam_ldap` est responsable de la communication entre les processus de login et l'annuaire LDAP utilisé comme source des données d'authentification.La bibliothèque partagée `pam_ldap.so` est installé et la configuration de PAM est modifiée (voir l'exemple 22.27).

Exemple 22.27: *pam_unix2.conf modifié pour LDAP*

```
auth:       use_ldap nullok
account:    use_ldap
password:   use_ldap nullok
session:    none
```

Si vous souhaitez configurer à la main des services supplémentaires en vue d'une utilisation par LDAP, il est nécessaire que le module LDAP PAM soit ajouté au fichier de configuration de PAM dans `/etc/pam.d/`. Les fichiers qui ont déjà été modifiés pour différents services se trouvent dans `/usr/share/doc/packages/pam_ldap/pam.d/`. Copiez les fichiers correspondants dans `/etc/pam.d/`.

Modifiez la résolution de noms de la bibliothèque `glibc` à l'aide du programme `nss_ldap` en utilisant le mécanisme `nsswitch` pour permettre l'utilisation de LDAP. En installant ce paquetage, un nouveau fichier `nsswitch.conf` modifié est enregistré dans `/etc`. Pour plus de précisions sur le fonctionnement de `nsswitch.conf`, reportez-vous à la section *Fichiers de configuration* page 460. Pour la gestion des utilisateurs ou leur authentification avec LDAP, votre fichier `nsswitch.conf` doit comporter les lignes suivantes (voir l'exemple 22.28 :

Exemple 22.28: *Adaptations dans nsswitch.conf*

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

Ces lignes demandent à la bibliothèque Resolver de `glibc`, faisant office de source de données d'authentification et sur les utilisateurs, d'évaluer dans un premier temps les fichiers correspondants présents localement sur le système dans `/etc` et d'accéder ensuite au serveur LDAP. Testez ce mécanisme en lisant à l'aide de de la commande `getent passwd` par exemple le contenu de la base de données des utilisateurs. Le résultat doit présenter aussi bien les utilisateurs locaux présents sur votre système que tous les utilisateurs présents sur le serveur LDAP.

Si vous voulez empêcher que les utilisateurs normaux administrés par LDAP ne puissent se connecter au serveur à l'aide de ssh ou de login, vous devez ajouter une ligne dans `/etc/passwd` et `/etc/group` : `+::::::/sbin/nologin` dans `/etc/passwd` et `+:::` dans `/etc/group`.

Configuration du client LDAP

Une fois que `nss_ldap` et `pam_ldap` ainsi que `/etc/passwd` et `/etc/group`ont été convenablement modifiés par YaST, vous pouvez commencer les opérations de configuration à proprement parler dans le premier formulaire de YaST.

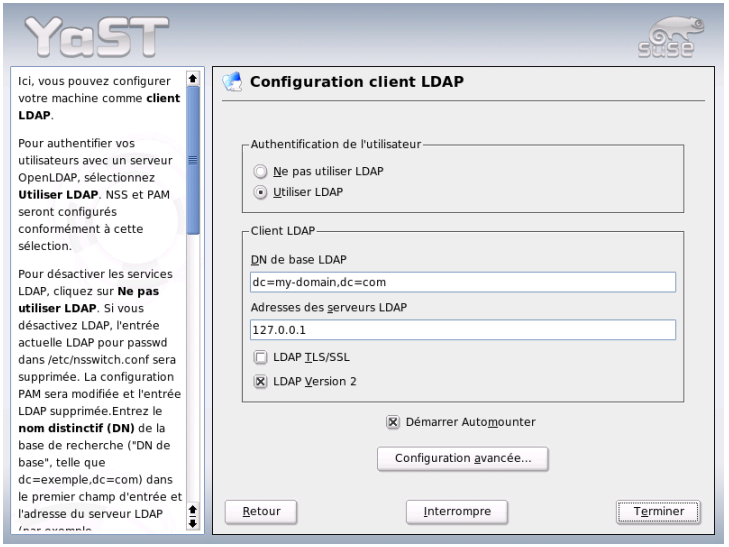


FIG. 22.23: *YaST : Configuration du client LDAP*

Dans la première boîte de dialogue (voir l'illustration 22.23), activez le bouton radio pour utiliser LDAP pour l'authentification des utilisateurs et saisissez dans la zone d'édition 'LDAP Base DN' la base de recherche sur le serveur, au-dessous de laquelle se trouvent toutes les données du serveur LDAP. Saisissez dans la seconde zone d'édition 'Adresse des serveurs LDAP' l'adresse à laquelle le serveur LDAP est accessible. Dans le cas où votre serveur prend en charge TLS/SSL, cochez la case 'LDAP TLS/SSL' afin d'autoriser les communications chiffrées entre votre client et le serveur. Si vous souhaitez monter des répertoires distants dans votre système de fichier, activez la case à cocher 'Démarrer automounter'. Si vous souhaitez modifier activement, en tant qu'administrateur, les données gérées sur le serveur, cliquez sur le bouton 'Configuration avancée'.

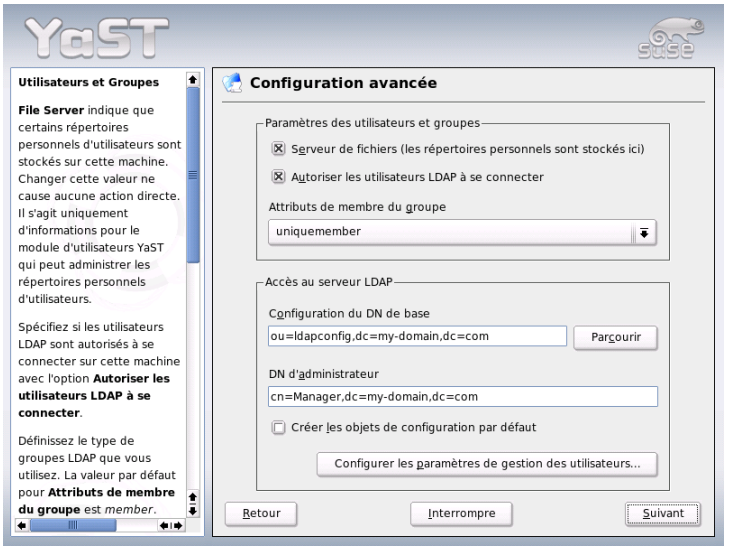


FIG. 22.24: *YaST : Configuration avancée*

Le dialogue suivant est divisé en deux : dans la partie supérieure, procédez à la configuration des paramètres généraux pour utilisateurs et groupes qui déterminent le comportement du module utilisateurs de YaST. Dans la partie inférieure, saisissez les données d'accès au serveur LDAP. Les paramètres relatifs aux utilisateurs et groupes se limitent aux entrées suivantes :

Serveur de fichiers Ce système est-il un serveur de fichiers et administre les répertoires `/home` des utilisateurs ? En activant la case à cocher, vous indiquez au module utilisateurs de YaST comment agir avec les repertoires personnels des utilisateurs sur ce système.

Autoriser la connexion des utilisateurs LDAP
Activez la case à cocher afin d'autoriser la connexion au système des utilisateurs administrés par LDAP.

Attribut pour membres du groupe Définissez le type de groupe LDAP à utiliser. Vous avez le choix entre : 'member' (configuration par défaut) et 'uniquemember'.

Remarque

Mise en œuvre du client YaST

Le client LDAP YaST est utilisé pour ajuster, et le cas échéant agrandir, de manière appropriée les modules YaST, en fonction de la gestion des utilisateurs et des groupes. Parallèlement à cela, vous avez la possibilité de définir des formulaires avec des valeurs par défaut pour les différents attributs, de manière à simplifier la saisie à proprement parler des données. Les valeurs par défaut créées ici sont elles-mêmes enregistrées dans l'annuaire LDAP sous forme d'objets LDAP. La saisie des données utilisateurs continue à être réalisé à l'aide des formulaires de modules YaST normaux. Les informations saisies sont enregistrées sous forme d'objets dans l'annuaire LDAP.

Remarque

Pour modifier des configurations sur le serveur LDAP, saisissez dans cette boîte de dialogue les données d'accès requises (voir l'illustration 22.24 page précédente). Il s'agit de la zone d'édition 'Configuration base DN' (dans laquelle tous les objets de configuration sont enregistrés) et de la zone d'édition 'DN administrateur'. Pour éditer les enregistrements sur le serveur LDAP, cliquez sur le bouton 'Configurer les paramètres pour l'administration des utilisateurs'. Une boîte de dialogue apparaît, dans laquelle vous êtes invité à saisir votre mot de passe LDAP pour vous authentifier sur le serveur. Les ACL ou ACI sur le serveur vous permettent ensuite d'accéder aux modules de configuration sur le serveur.

Dans la boîte de dialogue de configuration du module, vous avez la possibilité de sélectionner et de modifier des modules de configuration existants, d'en créer de nouveaux ou de créer et modifier des modèles (de l'anglais *Templates*) pour ces modules (voir l'illustration 22.25 page suivante). Pour modifier une valeur dans un module de configuration ou pour renommer un module, choisissez le type de module à l'aide de la liste déroulante au-dessus du sommaire du module courant. Une liste en forme de table apparaît alors dans la vue de détail avec l'ensemble des attributs et valeurs associées autorisés dans ce module. On y trouve, à côté des attributs définis, tous les autres attributs autorisés par le schéma utilisé mais qui ne sont pas utilisés actuellement. Si vous voulez copier un module, il vous suffit de modifier `cn`. Pour modifier individuellement des valeurs d'attributs, sélectionnez-les dans le contenu et cliquez sur le bouton 'Modifier'. Une boîte de dialogue s'ouvre alors, à partir de laquelle vous pouvez modifier tous les paramètres de l'attribut. Validez vos modifications en cliquant sur le bouton 'OK'.

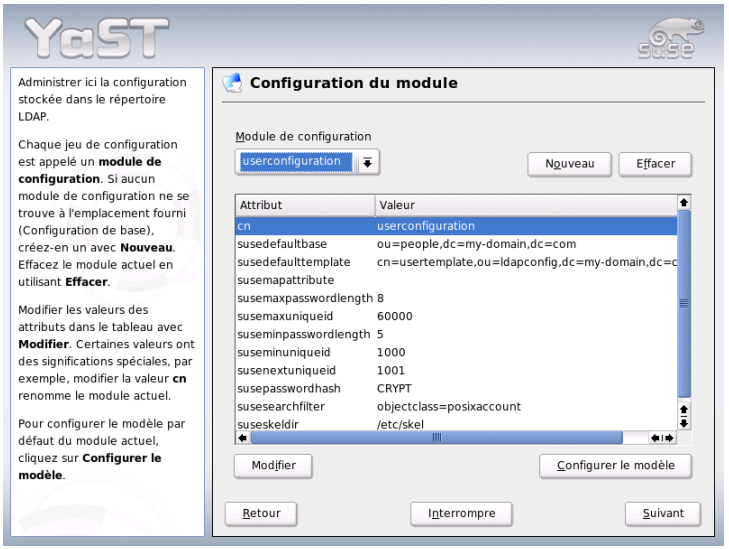


FIG. 22.25: *YaST : configuration du module*

Si vous souhaitez compléter les modules existants par l'ajout d'un nouveau module, cliquez sur le bouton 'Nouveau' au-dessus du sommaire. Après cela, saisissez dans la boîte de dialogue qui s'ouvre alors la classe d'objet du nouveau module (soit `suseuserconfiguration` soit `susegroupconfiguration`) ainsi que le nom du nouveau module. Si vous sortez de cette boîte de dialogue en cliquant sur le bouton 'OK', le nouveau module est ajouté à la liste de sélection des modules présents et peut être sélectionné et désélectionné à l'aide de la liste déroulante. Pour supprimer le module en cours de sélection, cliquez sur le bouton 'Supprimer'.

Les modules YaST pour la gestion des utilisateurs et des groupes intègrent des modèles utilisant des valeurs par défaut appropriées, dans le cas où vous les avez précédemment définies à l'aide du client LDAP YaST. Pour éditer un modèle à votre convenance, cliquez sur le bouton 'Configurer le modèle'. Le menu déroulant affiche soit des modèles existants modifiables soit un enregistrement vide donnant également accès au formulaire de modification des modèles. Sélectionnez l'un de ces modèles et configurez dans le formulaire suivant 'Configuration du modèle d'objet' les propriétés de ce modèle. Ce formulaire comporte deux vo-

FIG. 22.26: *YaST : Modification d'attributs dans la configuration du module*

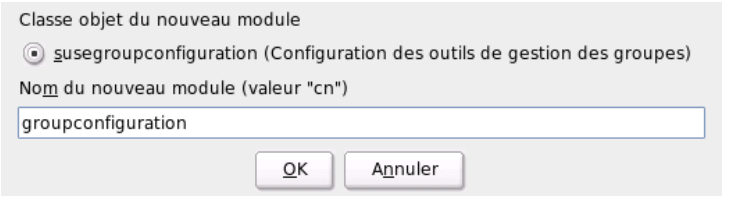


FIG. 22.27: *YaST : Création d'un nouveau module*

lets sous forme de table. Le volet supérieur comporte tous les attributs généraux du modèle. Définissez leurs valeurs conformément aux besoins de votre scénario de réalisation ou laissez d'autres valeurs vides. Les attributs "vides" sont supprimés du serveur LDAP.

La deuxième liste ('Valeurs par défaut pour de nouveaux objets') énumère tous les attributs de l'objet LDAP correspondant (ici : la configuration des groupes ou des utilisateurs), pour lesquels vous définissez une valeur par défaut. Vous pouvez ajouter d'autres attributs et leurs valeurs par défaut ainsi que supprimer des attributs. Un modèle peut être simplement copié, à la manière d'un module, en modifiant l'enregistrement `cn`, afin de créer un nouveau modèle. Reliez le modèle au module associé en fixant la valeur d'attribut de `susedefaulttemplate` du module au DN du modèle modifié, conformément à la procédure indiquée précédemment.

Remarque

Vous pouvez créer des valeurs par défaut pour un attribut formé à partir d'autres attributs, en utilisant une syntaxe avec des variables plutôt qu'une valeur absolue. Ainsi, `cn=%sn %givenName` est automatiquement créé lors de la création d'utilisateur à partir des valeurs d'attribut de `sn` et de `givenName`.

Remarque

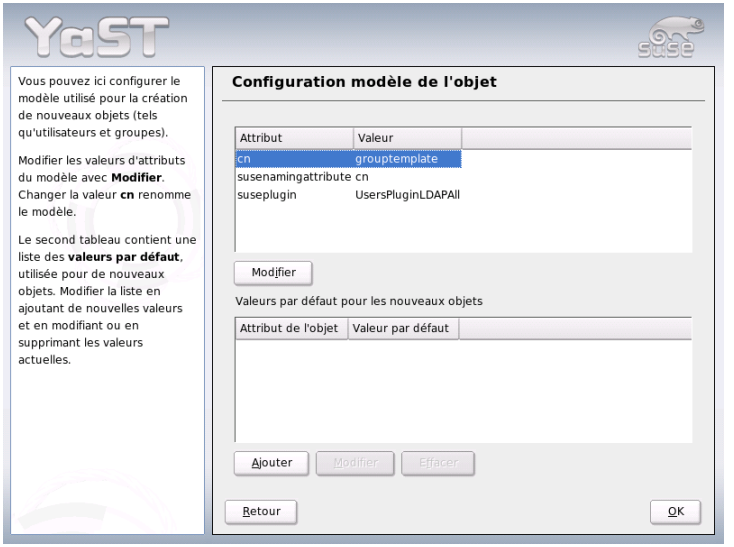


FIG. 22.28: *YaST : Configuration d'un modèle d'objet*

Lorsque tous les modules et modèles sont convenablement configurés et qu'ils sont opérationnels, créez à l'aide de YaST de nouveaux groupes et utilisateurs, en suivant la procédure habituelle.

Utilisateurs et groupes — Configuration avec YaST

Après avoir configuré des modules et des modèles pour le réseau, la saisie des données relatives aux utilisateurs et aux groupes diffère très légèrement de la procédure n'utilisant pas LDAP. Le guide ci-après concerne la gestion des utilisateurs, la procédure appliquée à la gestion des groupes étant analogue.

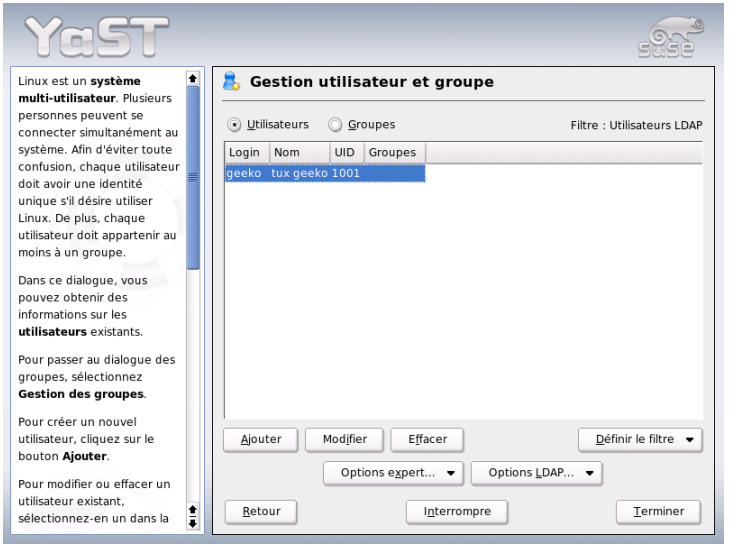


FIG. 22.29: *YaST : Gestion des utilisateurs*

La gestion des utilisateurs est accessible à partir du menu YaST 'Sécurité et Utilisateurs' → 'Modifier et créer des utilisateurs'. Pour ajouter un nouvel utilisateur, cliquez sur le bouton 'Ajouter'. Le formulaire de saisie des principales données utilisateurs (nom, login utilisateur et mot de passe) s'ouvre alors. Complétez ce formulaire et cliquez sur le bouton 'Détails'. Vous accédez alors à un formulaire permettant de configurer plus finement l'appartenance à d'autres groupes, le shell de connexion et le répertoire personnel. Les valeurs par défaut des zones de saisie ont été définies selon la procédure présentée à la section *Configuration du client LDAP* page 532. Lorsque le service LDAP est activé, vous accédez depuis ce formulaire à un autre formulaire de saisie des attributs LDAP (voir l'illustration 22.30 page suivante) . Sélectionnez ensuite tous les attributs dont vous souhaitez modifier la valeur et cliquez sur le bouton 'Modifier' pour ouvrir la fe-

nêtre d'édition correspondante. Sortez ensuite de ce formulaire en cliquant sur le bouton 'Suivant', ce qui vous fait revenir au formulaire initial de la gestion des utilisateurs.

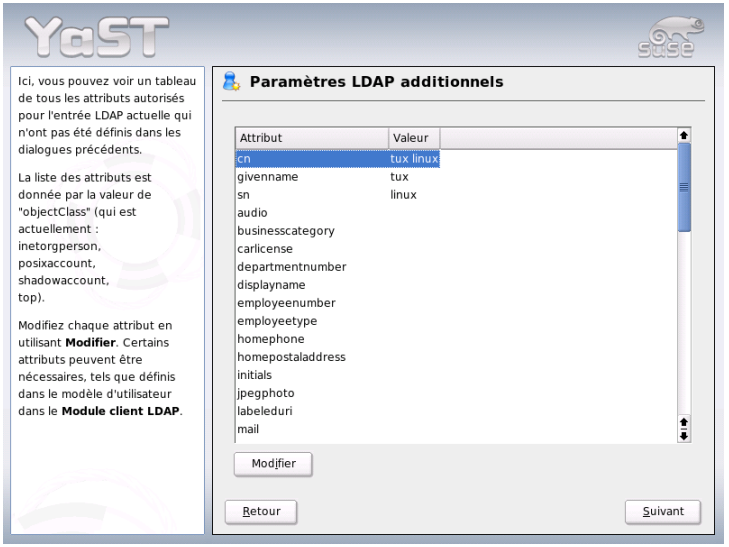


FIG. 22.30: *YaST : Paramètres LDAP supplémentaires*

À partir du formulaire initial de la gestion des utilisateurs (voir l'illustration 22.29 page ci-contre), le bouton 'Options LDAP' offre la possibilité d'appliquer des filtres de recherche LDAP à l'ensemble des utilisateurs disponibles ou d'entrer dans le module de configuration pour utilisateurs et groupes LDAP en sélectionnant 'Configuration des utilisateurs et groupes LDAP'.

22.9.6 Informations supplémentaires

Nous avons volontairement renoncé à traiter dans ce chapitre des sujets plus complexes tels que la configuration SASL ou la mise en place d'un serveur LDAP répliqué qui se partage la tâche avec plusieurs "esclaves". Pour plus d'informations sur ces deux sujets, reportez-vous au document *OpenLDAP 2.2 Administrator's Guide* (voir lien ci-après).

Vous trouverez sur les pages Web du projet OpenLDAP des documents complets pour les utilisateurs LDAP débutants et avancés.

OpenLDAP Faq-O-Matic Un recueil exhaustif de questions et de réponses sur l'installation, la configuration et l'utilisation de OpenLDAP : `http://www.openldap.org/faq/data/cache/1.html`

Quick Start Guide [Guide de démarrage rapide]
Un guide concis pour votre premier serveur LDAP : `http://www.openldap.org/doc/admin22/quickstart.html` ou dans le système installé à l'emplacement `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`.

OpenLDAP 2.2 Administrator's Guide [Guide de l'administrateur OpenLDAP 2.2]
Une introduction complète à tous les domaines importants de la configuration LDAP,y compris le contrôle d'accès et le chiffrement : `http://www.openldap.org/doc/admin22/` ou dans le système installé à l'emplacement `/usr/share/doc/packages/openldap2/admin-guide/index.html`

Par ailleurs les livres rouges d'IBM indiqués ci-après s'intéressent à la question de LDAP :

Understanding LDAP [Comprendre LDAP]
Une introduction générale et très complète aux principes de base de LDAP : `http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf`

LDAP Implementation Cookbook [Recettes pour la mise en pratique de LDAP]
Le groupe cible correspond en particulier aux administrateurs de *IBM SecureWay Directory*. On trouve toutefois également d'importantes informations d'ordre général sur LDAP dans :`http://www.redbooks.ibm.com/redbooks/pdfs/sg245110.pdf`

Documents imprimés en anglais sur LDAP :

- Howes, Smith & Good: *Understanding and Deploying LDAP Directory Services*. Addison-Wesley, 2ème éd., 2003. - (ISBN 0-672-32316-8)
- Hodges: *LDAP System Administration*. O'Reilly & Associates, 2003. - (ISBN 1-56592-491-6)

Les RFC (*Request for comments*) 2251 à 2256 sont des documents de référence faisant autorité sur LDAP.

22.10 NFS – Systèmes de fichiers partagés

Comme indiqué précédemment à la section *NIS – Network Information Service* page 509, NFS permet, comme NIS, de rendre un réseau transparent pour les utilisateurs. NFS permet de partager des systèmes de fichiers en réseau. Quel que soit le poste au sein du réseau sur lequel un utilisateur travaille, ce dernier retrouvera toujours le même environnement.

Tout comme NIS, NFS est un service asymétrique. Il se compose d'un serveur NFS et de clients NFS. Ces deux fonctions peuvent bien entendu coexister sur une même machine. Celle-ci proposera dans le même temps des systèmes de fichiers au réseau ("exportation") et montera des systèmes de fichiers appartenant à d'autres machines ("importation"). On utilise toutefois, en règle générale, des serveurs dotés d'une capacité disque importante, et ce seront leurs systèmes de fichiers qui seront montés par des clients.

22.10.1 Importation de systèmes de fichiers avec YaST

Chaque utilisateur qui en a reçu le droit peut monter des répertoires NFS de serveurs NFS dans sa propre arborescence de fichiers. La méthode la plus simple pour ce faire consiste à utiliser le 'client NFS' sous YaST. Il suffit alors d'indiquer le nom d'hôte de la machine faisant office de serveur NFS, le répertoire exporté depuis le serveur ainsi que le point de montage sous lequel il doit être monté sur le poste client. Pour ce faire, choisissez 'Ajouter' dans la première boîte de dialogue puis complétez les indications demandées (voir l'illustration 22.31).

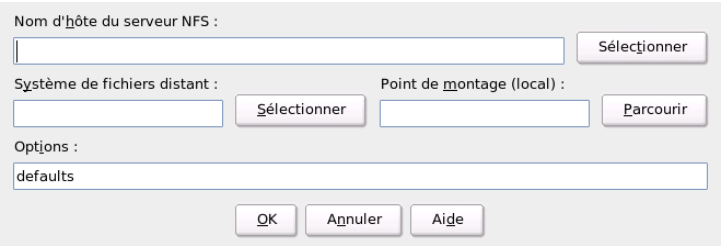


FIG. 22.31: *Configuration du client NFS*

22.10.2 Importation manuelle de systèmes de fichiers

Il est très simple d'importer à la main des systèmes de fichiers à partir d'un serveur NFS. Pour ce faire, il suffit simplement que le redirecteur de ports (*RPC portmapper*) soit en service. Pour le démarrer, exécutez la commande `rcportmap start` en tant qu'utilisateur `root`. Lorsque cette condition est satisfaite, des systèmes de fichiers distants peuvent, s'ils sont exportés depuis les machines correspondantes, être montés dans le système de fichiers à l'aide de la commande `mount`, comme s'il s'agissait de disques locaux. La syntaxe est la suivante :

```
mount machine:chemin-distant chemin-local
```

Ainsi, la commande pour importer les répertoires personnels de la machine soleil est la suivante :

```
mount soleil:/home /home
```

22.10.3 Exportation de systèmes de fichiers avec YaST

Avec YaST, vous pouvez mettre en place très rapidement un serveur NFS sur une machine de votre réseau. Il s'agit d'un serveur proposant des répertoires et des fichiers à toutes les machines auxquelles vous accordez l'accès. Ainsi, de nombreuses applications peuvent être mises à la disposition de vos collaborateurs, sans qu'il soit nécessaire de les installer en local sur leurs machines.

La procédure d'installation est la suivante : sous YaST choisissez 'Services réseau', puis 'Serveur NFS' (voir l'illustration 22.32 page suivante).

Ensuite, cochez 'Démarrer le serveur NFS' et cliquez sur le bouton 'Suivant'. Pour finir, saisissez dans la zone du haut les répertoires que vous souhaitez exporter et dans la zone du bas les machines de votre réseau auxquelles vous souhaitez accorder l'accès (voir l'illustration 22.33 page 544). La définition des machines peut être affinée à l'aide de quatre options : `single host`, `netgroups`, `wildcards` et `IP networks`. Pour plus de précisions sur ces options, veuillez vous reporter aux pages de manuel de `exports`.

Cliquez sur le bouton 'Terminer' pour achever la configuration.

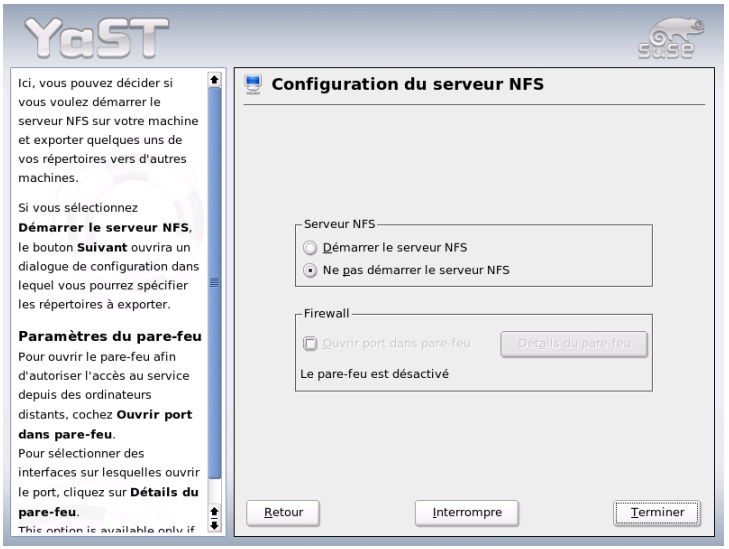


FIG. 22.32: *Utilitaire de configuration du serveur NFS*

Remarque

Configuration automatique du pare-feu

Si un pare-feu (SuSEfirewall2) fonctionne sur votre système, YaST procède à sa configuration pour le serveur NFS dès que vous sélectionnez 'Ouvrir ports dans le pare-feu'. YaST active alors le service `nfs`.

Remarque

22.10.4 Exportation manuelle de systèmes de fichiers

Si vous préférez renoncer à vous faire assister par YaST, vous devez vous assurer que les services suivants sont démarrés sur le serveur NFS :

- Redirecteur de ports RPC (portmap)
- Démon RPC Mount (rpc.mountd)
- Démon RPC NFS (rpc.nfsd)

FIG. 22.33: *Serveur NFS : saisir les répertoires exportés et les hôtes*

Pour permettre aux scripts `/etc/init.d/portmap` et `/etc/init.d/nfsserver` de lancer ces services lors du démarrage du système, saisissez les commande `insserv /etc/init.d/nfsserver` et `insserv /etc/init.d/portmap`.

Lorsque ces démons ont été lancés, il vous reste à spécifier quels systèmes de fichiers doivent être exportés et vers quelles machines. Ces éléments sont définis dans le fichier `/etc/exports`.

Chaque répertoire à exporter utilise une ligne pour les informations relatives aux machines autorisées à y accéder et à la manière d'y accéder. Tous les sous-répertoires d'un répertoire exporté sont automatiquement exportés à leur tour. Les machines autorisées sont habituellement désignées par leur nom (en incluant également le nom de domaine), mais il est également possible d'utiliser les caractères joker * et ? qui ont la même fonction que dans le programme bash. Dans le cas où aucun nom de machine n'est indiqué, toutes les machines sont autorisées à accéder à ce répertoire avec les droits spécifiés).

Les droits avec lesquels le répertoire est exporté sont spécifiés, pour chaque machine, dans une liste entre parenthèses. Les principales options associées aux droits d'accès sont décrites dans les tableaux suivants.

TAB. 22.13: *Droits d'accès aux répertoires exportés*

Options	Signification
`ro`	Le système de fichiers est exporté uniquement avec des droits en lecture (valeur par défaut).
`rw`	Le système de fichiers est exporté avec des droits en lecture/écriture.
`root_squash`	Grâce à cette option, l'utilisateur `root` de la machine mentionnée ne possède sur ce système de fichiers aucun des spéciaux spécifiques à l'administrateur `root`. Ce résultat est obtenu en utilisant le numéro d'utilisateur `65534 (-2)` pour les accès qui auraient dû se faire avec le numéro d utilisateur `0`. Ce numéro devrait être attribué à l'utilisateur `nobody` (valeur par défaut).
`no_root_squash`	Ne pas convertir les accès root ; les privilèges root sont donc conservés.
`link_relative`	Convertir les liens symboliques absolus (commençant par `/`) en une séquence correspondante de `../`. Cette option n'est utile que si le système de fichiers d'une machine a été monté dans sa totalité (valeur par défaut).
`link_absolute`	Laisser inchangés les liens symboliques.
`map_identity`	Le client utilise les mêmes numéros d'utilisateurs que sur le serveur (valeur par défaut).
`map_daemon`	Le client et le serveur utilisent des numéros d'utilisateurs distincts. Avec cette option, le programme `nfsd` va créer une table de conversion des numéros d'utilisateurs. Pour cela, le démon **ugidd** doit avoir été lancé auparavant.

Le fichier `exports` peut ressembler par exemple au fichier 22.29.

Exemple 22.29: */etc/exports*

```
#
# /etc/exports
#
/home            soleil(rw)   venus(rw)
/usr/X11         soleil(ro)   venus(ro)
/usr/lib/texmf   soleil(ro)   venus(rw)
/                terre(ro,root_squash)
/home/ftp        (ro)
# End of exports
```

Le fichier `/etc/exports` est lu par mountd et nfsd. Ainsi, lorsque ce fichier a été modifié, il est nécessaire de redémarrer mountd et nfsd afin de permettre à ces modifications d'être prises en compte. Pour ce faire, le plus simple est d'exécuter la commande :

```
rcnfsserver restart
```

22.11 DHCP

22.11.1 Le protocole DHCP

DHCP ("Dynamic Host Configuration Protocol") sert à configurer un réseau de façon centralisée à partir d'un serveur. On n'a donc pas besoin de configurer chaque poste de travail séparément. Un client configuré avec le protocole DHCP ne dispose pas d'adresses statiques, mais se configure complètement lui-même en fonction des indications fournies par le serveur DHCP.

Il est en outre possible d'identifier chaque client à partir de l'adresse matérielle de sa carte réseau et de le configurer toujours de la même façon, ou alors d'attribuer "dynamiquement" à chaque ordinateur "intéressé" des adresses puisées dans une réserve (en anglais, un *pool*) donnée. Dans ce cas, le serveur DHCP s'efforce d'attribuer toujours la même adresse à chaque client, lors de chaque requête (même après un long intervalle de temps) — ceci ne fonctionne toutefois que tant qu'il y a plus d'adresses que d'ordinateurs dans le réseau .

Un administrateur système peut donc profiter immédiatement à deux égards du protocole DHCP. D'une part, il peut entreprendre des modifications d'adresses réseau ou de configuration, même en grand nombre, de manière confortable et centralisée dans le fichier de configuration du serveur DHCP, sans avoir à configurer individuellement un grand nombre de clients. D'autre part, il est très facile d'intégrer de nouveaux ordinateurs dans le réseau, dans la mesure où une adresse IP tirée de la réserve d'adresses leur est affectée. De plus, pour les ordinateurs portables qui sont régulièrement utilisés dans plusieurs réseaux différents, il est intéressant de pouvoir obtenir la configuration réseau appropriée à partir d'un serveur DHCP.

Outre l'adresse IP et le masque réseau, le nom de l'ordinateur et du domaine, la passerelle à utiliser et les adresses du serveur de noms sont communiqués au client. Par ailleurs, quelques autres paramètres peuvent être configurés de manière centralisée, par exemple un serveur d'horloge auquel il est possible de demander l'heure actuelle ou un serveur d'impression. Nous souhaiterions maintenant vous montrer comment configurer complètement votre réseau, de manière centrale, à l'aide du protocole DHCP et du serveur DHCP dhcpd.

22.11.2 Paquetages logiciels DHCP

Avec SUSE LINUX, vous disposez non seulement d'un serveur DHCP, mais également de deux paquetages client. Le serveur DHCP dhcpd publié par l'Internet Software Consortium met à votre disposition la fonctionnalité serveur, tandis que pour les clients, vous pouvez utiliser dhclient, également publié par l'ISC, ainsi que le "DHCP Client Daemon" du paquetage `dhcpcd`.

Le démon dhcpcd installé par défaut avec SUSE LINUX est très facile à manipuler et démarre automatiquement lors du démarrage de l'ordinateur pour rechercher un serveur DHCP. Il est livré sans fichier de configuration et doit normalement fonctionner sans configuration supplémentaire.

Dans des situations complexes, on peut recourir au programme dhclient de l'ISC qui se règle avec le fichier de configuration `/etc/dhclient.conf`.

22.11.3 Le serveur DHCP dhcpd

Le protocole *Dynamic Host Configuration Protocol Daemon* est le cœur d'un système DHCP. Il "loue" des adresses et surveille leur utilisation en fonction de ce qui est indiqué dans le fichier de configuration `/etc/dhcpd.conf`. Grâce aux paramètres et aux valeurs définis dans ce fichier, l'administrateur système dispose d'un grand nombre de possibilités pour influencer comme il le souhaite le comportement du protocole DHCP.

Exemple de fichier `/etc/dhcpd.conf` simple :

Exemple 22.30: *Le fichier de configuration /etc/dhcpd.conf*

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "kosmos.uni";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
 {
  range 192.168.1.10 192.168.1.20;
  range 192.168.1.100 192.168.1.200;
 }
```

Ce fichier de configuration simple est suffisant pour que le protocole DHCP puisse attribuer des adresses IP au réseau. Faites tout particulièrement attention aux points-virgules à la fin de chaque ligne : le démon dhcpd ne peut pas démarrer si vous les oubliez !

Comme vous pouvez le voir, l'exemple de fichier ci-dessus peut se diviser en trois blocs. La première partie définit le nombre de secondes par défaut pendant lequel une adresse IP est "louée" à un ordinateur demandeur avant que ce dernier ne doive se préoccuper de demander une prolongation (`default-lease-time`, temps d'attribution par défaut). Est également indiquée ici la durée maximale pendant laquelle un ordinateur a le droit de conserver une adresse IP attribuée par le serveur DHCP sans avoir à demander de prolongation (`max-lease-time`, temps d'attribution maximal).

Le deuxième bloc définit de façon globale un certain nombre de paramètres réseau fondamentaux :

- L'option `option domain-name` (nom de domaine) définit le domaine par défaut de votre réseau.
- L'option `option domain-name-servers` (serveurs de noms de domaines) vous permet d'indiquer jusqu'à trois serveurs DNS à utiliser pour la conversion des adresses IP en noms d'hôtes et réciproquement. Idéalement, il serait préférable qu'un serveur de noms qui tienne à disposition un nom d'hôte pour les adresses dynamiques et réciproquement soit déjà en service sur votre système ou dans votre réseau. Pour plus d'informations sur la mise en place d'un serveur de noms, reportez-vous à la section *DNS – Domain Name System* page 487.
- L'option `option broadcast-address` (adresse de diffusion) définit l'adresse de diffusion que l'ordinateur demandeur doit utiliser.
- L'option `option routers` (routeurs) définit les destinations vers lesquelles les paquets de données qui ne peuvent pas être distribués dans le réseau local (du fait de l'adresse de l'hôte source ou cible ainsi que des masques de sous-réseau) peuvent être envoyés. Pour les petits réseaux, ce routeur est également la plupart du temps le point d'accès à l'Internet.
- L'option `option subnet-mask` (masque de sous-réseau) indique le masque réseau attribué au client.

Après ces réglages généraux, il faut encore définir un réseau à l'aide d'un masque de sous-réseau. Pour finir, il faut choisir un domaine d'adresses où le démon DHCP peut puiser pour attribuer des adresses aux clients qui en demandent. Dans l'exemple ci-dessus, toutes les adresses comprises entre `192.168.1.10` et `192.168.1.20` et entre `192.168.1.100` et `192.168.1.200` sont disponibles.

Après ces quelques lignes, vous devriez déjà être en mesure d'activer le démon DHCP avec la commande `rcdhcpd start` qui est directement disponible.

Pour des raisons de sécurité, le démon DHCP se démarre dans SUSE LINUX par défaut dans un environnement déraciné (*chroot*). Pour qu'il trouve les fichiers de configuration, vous devez également copier ces derniers dans le nouvel environnement. Cette opération s'effectue automatiquement avec la commande `rcdhcpd start`.

Vous pouvez aussi vérifier rapidement la syntaxe du fichier de configuration avec `rcdhcpd check-syntax`.Si, contre toute attente, vous rencontrez un problème avec la configuration et si le serveur s'interrompt avec une erreur et ne démarre pas avec un message "done", vous trouverez la plupart du temps des informations sur l'incident dans le journal système central `/var/log/messages` ainsi que sur la console numéro 10 (Ctrl-Alt-F10).

22.11.4 Ordinateur avec adresse IP fixe

Comme déjà mentionné précédemment, le protocole DHCP permet aussi d'attribuer à un ordinateur, lors de chaque demande, une adresse donnée, bien précise.

Ces attributions explicites d'adresses ont la priorité sur les adresses dynamiques extraites de la réserve. Contrairement aux adresses dynamiques, les informations d'adresses fixes n'expirent pas comme c'est le cas lorsqu'il n'y a plus assez d'adresses disponibles et qu'une nouvelle répartition est nécessaire.

Pour identifier un système défini à l'aide d'une adresse *statique*, dhcpd utilise ce que l'on appelle l'adresse matérielle. Il s'agit, en règle générale, d'un numéro unique dont dispose chaque périphérique réseau, défini de manière fixe, et composé de six paires d'octets, par exemple `00:00:45:12:EE:F4`.

Si le fichier de configuration de l' 22.30 page 548 est complété par une définition semblable à celle de l' 22.31, dhcpd enverra quoi qu'il arrive les mêmes données à l'ordinateur concerné.

Exemple 22.31: *Complément au fichier de configuration*

```
host terre {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

La structure de ces lignes est facile à comprendre. On indique tout d'abord le nom de l'ordinateur à définir (`host` ⟨*hostname*⟩, ici `terre`) et, sur la ligne suivante, son adresse MAC. Sur les ordinateurs sous Linux, cette adresse peut être déterminée à l'aide de la commande `ifstatus` suivie du périphérique réseau (par exemple `eth0`). Vous devez, le cas échéant, d'abord activer la carte : `ifup eth0`. Vous obtenez alors un affichage de la forme :

```
link/ether 00:00:45:12:EE:F4
```

Dans notre exemple, l'ordinateur dont la carte réseau possède l'adresse MAC `00:00:45:12:EE:F4` se verra donc attribuer l'adresse IP `192.168.1.21` ainsi que le nom d'hôte `terre`. De nos jours, le type de matériel utilisé est en général de type `ethernet`, même si la technologie `token-ring`, fréquente notamment sur les systèmes IBM, est également prise en charge.

22.11.5 Particularités propres à SUSE LINUX

Pour des raisons de sécurité, dans SUSE LINUX le serveur DHCP publié par l'ISC contient le correctif "non-root/chroot" d'Ari Edelkind. Ainsi, le dhcpd s'exécute en tant qu'utilisateur `nobody` et dans un environnement déraciné (`/var/lib/dhcp`). Le fichier de configuration `dhcp.conf` doit pour cela se trouver dans `/var/lib/dhcp/etc` ; il y sera automatiquement copié par le script d'initialisation lors du démarrage.

Ce comportement peut se configurer dans le fichier `/etc/sysconfig/dhcpd`. Pour laisserdhcpd s'exécuter sans l'environnement déraciné, positionnez la variable `DHCPD_RUN_CHROOTED` à "no" dans le fichier `/etc/sysconfig/dhcpd`.

Pour que le démon dhcpd puisse également résoudre les noms d'hôtes dans l'environnement déraciné, il faut copier quelques fichiers de configuration supplémentaires. Il s'agit de :

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

C'est pourquoi, au démarrage du script d'initialisation du système, ils sont copiés dans `/var/lib/dhcp/etc/`. Ces fichiers doivent être informés de toute modification dynamique par un script comme `/etc/ppp/ip-up`. En revanche, il n'y a aura aucun problème si l'on utilise uniquement des adresses IP dans le fichier de configuration à la place des noms d'hôtes.

Si, dans votre configuration, vous devez copier d'autres fichiers dans l'environnement déraciné, indiquez-les avec le paramètre `DHCPD_CONF_INCLUDE_FILES` dans le fichier `etc/sysconfig/dhcpd`.

Pour que le démon dhcp puisse continuer à enregistrer le journal à partir de l'environnement déraciné même si le démon Syslog est redémarré, ajoutez le paramètre `"-a /var/lib/dhcp/dev/log"` aux variables `SYSLOGD_PARAMS` dans `/etc/sysconfig/syslog`.

22.11.6 Configuration du protocole DHCP avec YaST

Le module DHCP de YaST sert à la configuration d'un serveur DHCP indépendant dans le réseau local. Ce module possède deux modes de fonctionnement différents :

Configuration initiale (assistant) Lorsque le module démarre pour la première fois, l'administrateur doit prendre certaines décisions fondamentales. Une fois la configuration terminée, le serveur est prêt à fonctionner et suffisamment configuré pour des scénarios simples.

Configuration pour les experts Le mode pour experts sert aux tâches de configuration complexes comme le DNS dynamique, la gestion des TSIG, etc.

Remarque

Navigation dans le module avancé et affichage du texte d'aide

Toutes les boîtes de dialogue du module serveur DHCP suivent un principe de construction similaire. Dans la partie gauche de la fenêtre de dialogue, une vue arborescente permet de naviguer dans les diverses parties de la configuration, tandis que le formulaire proprement dit est affiché dans la partie droite. Si vous souhaitez obtenir un texte d'aide pour le formulaire actuel, cliquez sur l'icône représentant une bouée de sauvetage sur le bord inférieur gauche. Pour quitter cette aide et revenir à la vue arborescente, cliquez sur l'icône figurant la vue arborescente stylisée.

Remarque

Configuration initiale (assistant)

Lorsque le module démarre pour la première fois, YaST appelle un assistant de configuration en quatre étapes. À la fin de cet assistant, un serveur DHCP simple est prêt à fonctionner.

Choix de l'interface réseau Lors de la première étape, YaST détermine les interfaces réseau installées dans votre système. Choisissez dans la liste proposée celle pour laquelle le serveur DHCP devra être lancé et décidez avec l'option 'Ouvrir le pare-feu pour l'interface sélectionnée' si le pare-feu doit être ouvert pour cette interface (voir figure 22.34).

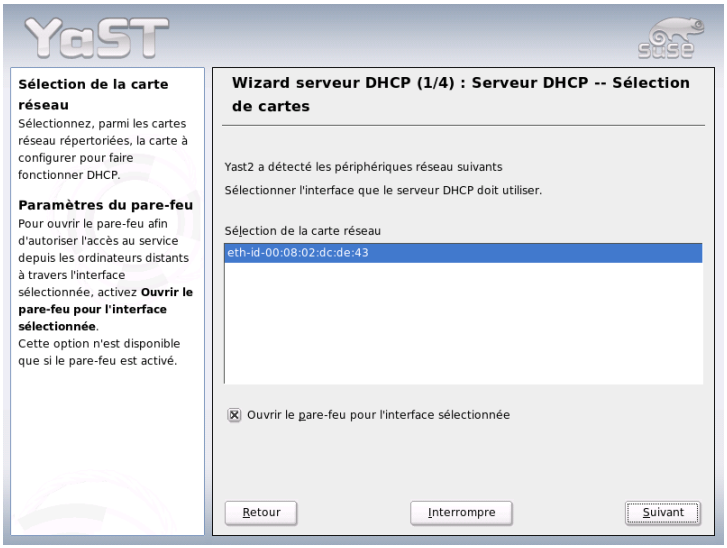


FIG. 22.34: *Serveur DHCP : choix de l'interface réseau*

Paramètres globaux Vous pourrez configurer les informations que doit recevoir chaque client géré par ce serveur DHCP dans les zones de saisie. Ces informations sont : le nom du domaine, l'adresse du serveur d'horloge, l'adresse des serveur de noms primaire et secondaire, l'adresse du serveur d'impression et celle du serveur WINS (pour l'intégration de clients Windows et Linux), ainsi que l'adresse de la passerelle et la durée du bail (voir figure 22.35 page suivante).

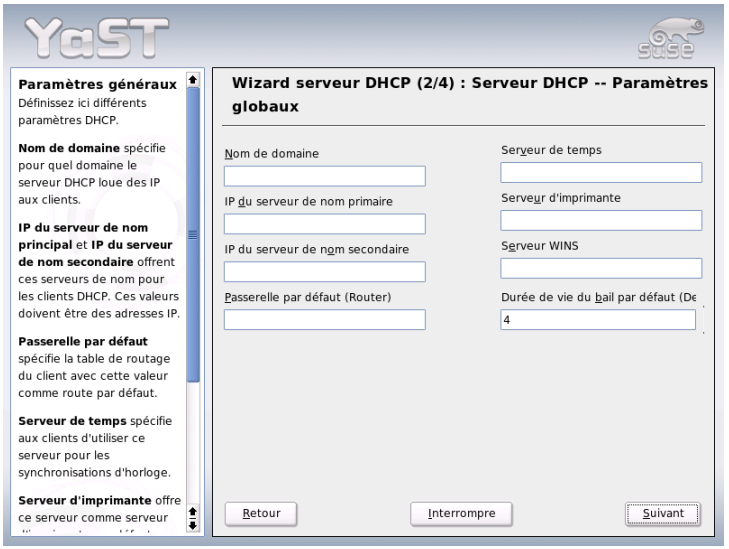


FIG. 22.35: *Serveur DHCP : paramètres globaux*

Serveur DHCP : DHCP dynamique Dans cette étape, vous configurerez l'affectation IP dynamique aux clients connectés. Pour cela, définissez une plage d'adresses IP au sein de laquelle les adresses à attribuer sont censées se trouver. Toutes les adresses à affecter doivent tomber sous un masque réseau commun. Terminez en fixant la durée du bail pendant laquelle le client peut garder une adresse sans "faire de demande" de prolongation. À titre facultatif, vous pouvez en outre établir la durée maximale du bail pendant laquelle telle adresse IP reste réservée sur le serveur pour tel client (voir figure 22.36 page suivante).

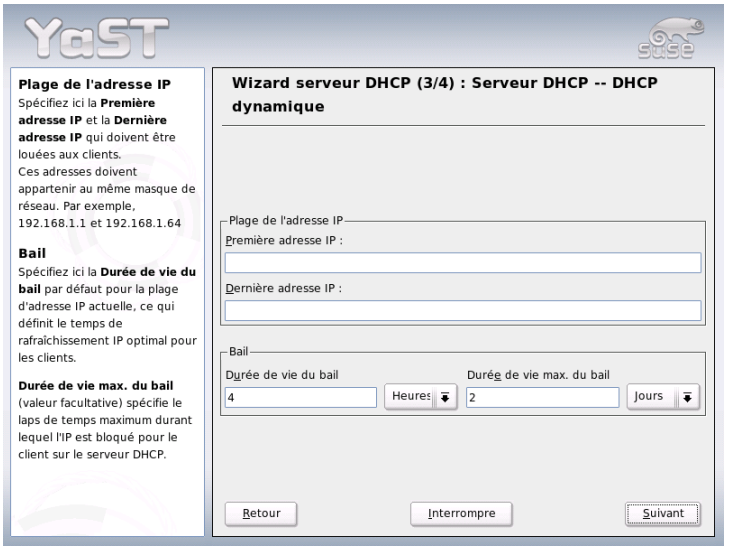


FIG. 22.36: *Serveur DHCP : DHCP dynamique*

Fin de la configuration et choix du mode de démarrage

Une fois que vous en avez terminé avec la troisième étape de l'assistant de configuration, vous accédez à une dernière boîte de dialogue consacrée aux options de démarrage du serveur DHCP. Vous pouvez y décider si le serveur DHCP doit être lancé automatiquement au démarrage du système ('Démarrer le serveur DHCP à l'amorçage') ou s'il doit être démarré manuellement à la demande ('Démarrer le serveur DHCP manuellement'). Cliquez sur 'Terminer' pour achever la configuration du serveur (voir figure 22.37 page suivante).

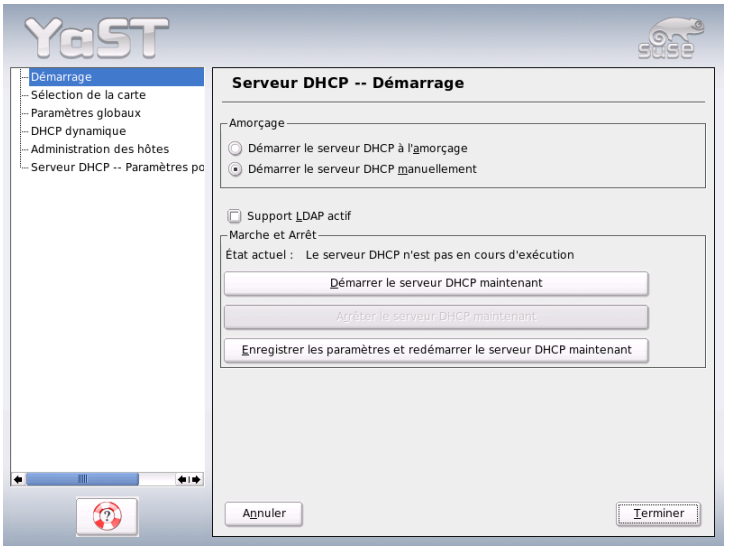


FIG. 22.37: *Serveur DHCP : Démarrage*

22.11.7 Pour plus d'informations

Vous trouverez des informations complémentaires par exemple sur le site de l'*Internet Software Consortium* qui propose des informations détaillées sur le protocole DHCP à l'adresse `http://www.isc.org/products/DHCP/` (en anglais).

En outre, les pages de manuel sont à votre disposition, en particulier celles de `dhcpd`, `dhcpd.conf`, `dhcpd.leases` et `dhcp-options`.

22.12 Synchronisation temporelle avec xntp

Pour de nombreuses opérations effectuées par un système informatique, il est fondamental de pouvoir s'appuyer sur une heure précise. C'est la raison de la présence d'une horloge sur toutes les machines. Malheureusement, celle-ci ne répond pas toujours aux attentes qui sont celles d'applications telles que les bases

de données. Pour ce faire, il faut régler en permanence l'horloge locale ou la corriger à partir du réseau. Dans l'idéal, il ne devrait jamais être nécessaire de reculer une horloge d'ordinateur et il ne faudrait pas laisser passer un intervalle de temps trop long entre deux avancements successifs de cette horloge. Il est relativement aisé de régler une fois ou l'autre l'horloge système à l'aide du programme ntpdate. Cette opération représente toutefois toujours un saut dans le temps brutal, qui n'est pas toléré par toutes les applications.

Ce problème trouve une solution intéressante avec le programme ntpdate. Celui-ci corrige en continu l'horloge système en recueillant des données de correction et parallèlement, il corrige de manière permanente l'horloge locale à l'aide de serveurs de temps présents sur le réseau. La troisième possibilité consiste à mettre en place des "étalons de temps" locaux tels que des horloges à fréquence radio.

22.12.1 Configuration réseau

Le programme xntp est préréglé de manière à utiliser uniquement l'horloge système locale comme référence temporelle. Le plus simple pour utiliser un serveur de temps sur le réseau est de spécifier des paramètres "serveur". Dans le cas où le réseau a accès à un serveur de temps nommé par exemple `ntp.example.com`, vous pouvez indiquer ce serveur comme suit dans le fichier `/etc/ntp.conf` : `server ntp.example.com`.

Il est facile d'ajouter des serveurs de temps en ajoutant de nouvelles lignes utilisant le mot-clé "server". Après avoir été lancé à l'aide de la commande `rcxntpd start`, le démon xntpd a besoin d'une heure jusqu'à ce que l'horloge se stabilise. Le fichier de dérive temporelle (fichier "drift") est alors créé afin de pouvoir corriger l'horloge système locale. L'avantage de ce fichier "drift" sur le long terme est qu'il permet de connaître le décalage de l'horloge système juste après avoir allumé la machine. La correction est alors immédiatement activée, ce qui permet d'offrir une grande stabilité de l'horloge système.

Lorsque vous pouvez accéder dans votre réseau au serveur d'horloge au moyen d'une diffusion, vous n'avez pas besoin de connaître son nom. Vous pouvez dans ce cas placer également dans le fichier de configuration `/etc/ntp.conf` la commande `broadcastclient`. Vous devez alors mettre en place les mécanismes d'authentification permettant d'éviter qu'un serveur de temps fonctionnant mal ne modifie par le réseau l'horloge de votre ordinateur.

Normalement, chaque démon xntpd peut également se comporter comme serveur de temps dans le réseau. Si vous souhaitez également utiliser le programme xntpd avec des diffusions, vous devez utiliser l'option `broadcast` :

```
broadcast 192.168.0.255
```

Pour ce faire, modifiez l'adresse de diffusion en fonction de vos propres besoins. Vous devez toutefois vous assurer que le serveur de temps utilise la bonne heure. Il convient pour cela d'utiliser un "étalon de temps".

22.12.2 Mise en place d'un étalon de temps local

L'application xntp comporte également des pilotes permettant de se connecter à des étalons de temps locaux. Vous trouverez la liste des horloges prises en charge dans le paquetage xntp-doc dans le fichier `file:/usr/share/doc/packages/xntp-doc/html/refclock.htm`. Chaque pilote est identifié par un numéro. La configuration de xntp à proprement parler est assurée à l'aide de pseudo adresses IP. Les horloges sont déclarées dans le fichier `/etc/ntp.conf` comme s'il s'agissait d'horloges disponibles sur le réseau. Ils reçoivent pour cela des adresses IP particulières sur le modèle suivant : `127.127.`⟨*t*⟩`.`⟨*u*⟩ . Vour trouverez la valeur de ⟨*t*⟩ dans la liste des horloges de référence. ⟨*u*⟩ représente le numéro de périphérique. Il n'est différent de `0` que si vous utilisez plusieurs horloges de même type sur votre machine. Ainsi, un "Type 8 Generic Reference Driver (PARSE)" utilise la pseudo adresse IP `127.127.8.0`.

Les différents pilotes ont normalement des paramètres spéciaux chargés de décrire plus en détail la configuration. Vous trouverez dans le fichier `file:/usr/share/doc/packages/xntp-doc/html/refclock.htm`, pour chaque pilote, un lien vers la page de pilote correspondante, avec la description des paramètres. Pour l'horloge de "type 8", il est par exemple nécessaire d'indiquer un mode supplémentaire chargé de spécifier l'horloge plus exactement. Ainsi, le module "Conrad DCF77 receiver module" utilise le "mode 5". Pour que cette horloge soit prise comme référence par xntp, vous pouvez également indiquer le mot-clé `prefer`. La ligne `server` complète d'un "module récepteur Conrad DCF77" est donc :

```
server 127.127.8.0 mode 5 prefer
```

D'autres horloges sont conçues sur le même schéma. La documentation sur xntp peut être consultée dans le répertoire `/usr/share/doc/packages/xntp-doc/html`, après l'installation du paquetage `xntp-doc`.

22.12.3 Configuration d'un client NTP avec YaST

Outre la configuration manuelle de xntp décrite précédemment, SUSE LINUX prend également en charge la configuration d'un client NTP par YaST. Vous disposez d'une configuration rapide simple ou une 'Configuration complexe'. Celles-ci sont décrites dans les sections ci-après.

Configuration rapide du client NTP

La configuration simple d'un client NTP se fait en deux dialogues. Dans le premier dialogue, définissez le mode de démarrage de xntpd et le serveur à interroger. Pour le démarrer automatiquement lors de l'amorçage du système, cliquez sur le bouton radio 'Lors de l'amorçage'. Pour déterminer un serveur de temps adapté pour votre réseau, cliquez sur 'Sélectionner' et entrez dans le second dialogue, le dialogue détaillé pour le choix du serveur.

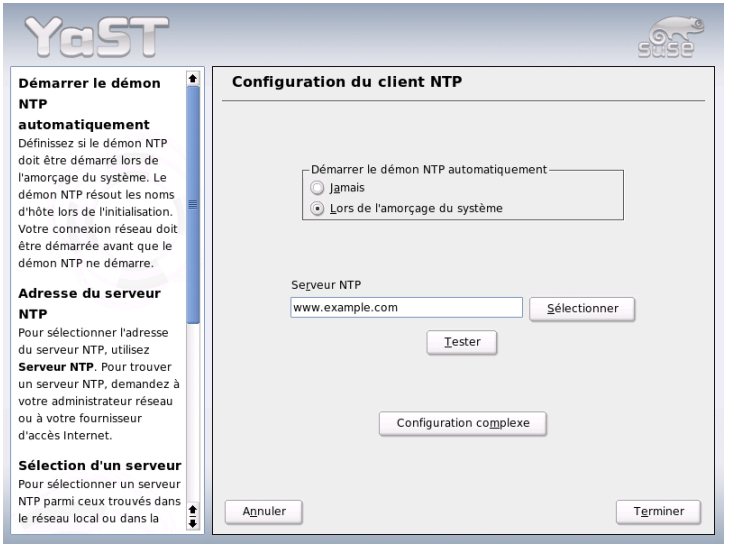


FIG. 22.38: *YaST : configuration du client NTP*

Dans le dialogue détaillé pour le choix du serveur, définissez d'abord si vous souhaitez utiliser un serveur de votre propre réseau (bouton radio 'Réseau local') ou un serveur de temps d'Internet de votre zone horaire (bouton radio 'Serveur NTP public') pour la synchronisation du temps. Dans le cas d'un serveur de temps local, cliquez sur 'Recherche' pour procéder à une requête SLP des serveurs de temps disponibles dans votre réseau. Dans la liste des résultats, sélectionnez le serveur adéquat et quittez le dialogue avec 'OK'. Vous revenez alors au dialogue principal décrit plus haut que vous quittez avec 'Terminer' une fois que vous avez vérifié la disponibilité du serveur sélectionné à l'aide de 'Test'. Dans le deuxième cas, pour sélectionner un serveur de temps public, sélectionnez votre pays (zone horaire) dans la zone de dialogue 'Serveur NTP public' et, dans la liste de serveurs qui s'affiche alors, le serveur qui vous convient. Quittez la configuration avec 'OK' et 'Terminer' une fois que vous avez vérifié la disponibilité du serveur sélectionné à l'aide de 'Test'.

Configuration complexe du client NTP

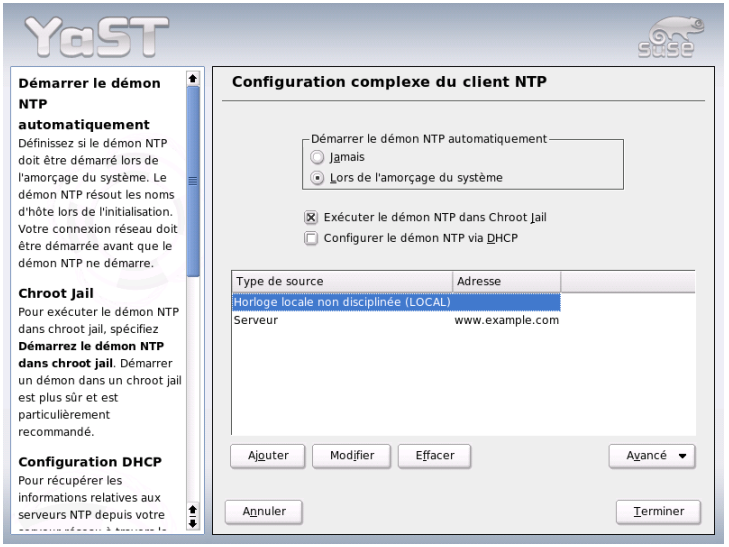


FIG. 22.39: *YaST : configuration complexe du client NTP*

Dans le dialogue 'configuration complexe du client NTP', définissez si xntpd doit être démarré dans un chroot-Jail. Cela augmente la sécurité dans le cas d'une attaque à travers xntpd, l'attaquant n'ayant alors pas la possibilité de compromettre le système entier. En outre, vous pouvez, avec 'Configurer le démon NTP via DHCP', configurer le client NTP de façon à ce qu'il soit informé par DHCP de la liste des serveurs NTP disponibles dans votre réseau. Dans la partie inférieure de la fenêtre de dialogue, les sources d'information du client sont répertoriées. Vous pouvez modifier cette liste avec 'Ajouter', 'Modifier' et 'Effacer'. Avec 'Avancé', vous avez la possibilité de consulter les fichiers de journalisation de votre client ou d'accorder (automatiquement) le pare-feu à la configuration du client NTP.

Pour ajouter une nouvelle source de synchronisation du temps, cliquez sur 'Ajouter'. Dans le dialogue suivant, sélectionnez le type de la source avec laquelle la synchronisation du temps doit se faire. Les options suivantes sont disponibles :

Serveur Dans le dialogue suivant, vous sélectionnez le serveur NTP (comme décrit dans la section *Configuration rapide du client NTP* page 559) et vous pouvez activer l'option 'Utiliser pour synchronisation initiale' afin de procéder à une synchronisation du temps entre serveur et client au moment de l'amorçage. Dans un autre champ de saisie, vous pouvez compléter des options supplémentaires pour xntpd. Vous trouverez plus d'informations à ce sujet sous `/usr/share/doc/packages/xntp-doc`.

Pair Si la synchronisation se fait avec un pair dans le même réseau plutôt qu'avec un serveur, saisissez l'adresse de ce système.

Le dialogue suivant est identique à celui du 'Serveur'.

Horloge radio Si vous utilisez une horloge radio dans votre système et souhaitez l'utiliser pour la synchronisation du temps, entrez dans ce dialogue le type de l'horloge, le numéro du périphérique, le nom du périphérique et les autres options. Avec 'Calibration du pilote', procédez à la configuration fine des pilotes correspondants. Vous trouverez des informations détaillées sur l'utilisation d'une horloge radio locale sous `file:///usr/share/doc/packages/xntp-doc/html/refclock.htm`.

Diffusion générale (broadcasting) Les informations et requêtes de temps peuvent également être transmises dans le réseau par diffusion générale.

Entrez dans ce dialogue les adresses auxquelles de telles diffusions générales doivent être envoyées. Vous pouvez configurer des options supplémentaires comme indiqués sous `/usr/share/doc/packages/xntp-doc`.

Accepter des paquets de diffusion générale

Si votre client doit recevoir ses informations par diffusion générale, entrez dans ce dialogue de quelles adresses les paquets correspondants doivent être acceptés. Vous trouverez plus d'options sous `/usr/share/doc/packages/xntp-doc`.

Le serveur web Apache

Nous présenterons dans ce chapitre le serveur web Apache. En dehors des précisions sur l'installation et la configuration, vous trouverez ici la description de quelques modules. Les variantes pour les hôtes virtuels sont également abordées.

23.1 Notions de base

Représentant une proportion de plus de 60 % (selon `http://www.netcraft.com`) Apache est le serveur web le plus répandu dans le monde. Pour des applications web, Apache est souvent combiné avec Linux, la base de données MySQL et les langages de programmation PHP et Perl. Cette combinaison est habituellement connue sous l'abréviation *LAMP*.

23.1.1 Serveur web

Un serveur web fournit à un client des pages HTML à sa demande. Ces pages peuvent être stockées sur un serveur (appelées pages passives ou statiques) ou générées comme réponse à une demande (contenus actifs).

23.1.2 HTTP

Les clients sont dans la plupart des cas des navigateurs web comme Konqueror et Mozilla. La communication entre le navigateur et le serveur web se fait par le protocole *H*yper*T*ext *T*ransfer *P*rotocol (HTTP). La version actuelle de HTTP 1.1 est documentée dans le RFC 2068 ainsi que dans sa mise à jour RFC 2616, ces RFC se trouvant à l'adresse `http://www.w3.org`.

23.1.3 Les URL

Un client demande une page au serveur par le biais d'une URL, `http://www.suse.fr/index.html`. Une URL est composée des composants suivants :

Protocole Les protocoles souvent utilisés sont

- `http://` Le protocole HTTP.
- `https://` Version sécurisée et chiffrée de HTTP.
- `ftp://` *F*ile *T*ransfer *P*rotocol (Protocole de Transfert de Fichiers), pour le téléchargement et l'envoi de fichiers.

Domaine Dans notre cas, `www.suse.fr`. Le domaine peut encore être subdivisé, la première partie `www` faisant référence à un ordinateur et la deuxième partie `suse.fr` au domaine proprement dit. Les deux parties ensemble sont également appelées FQDN (*Fully Qualified Domain Name* - Nom de domaine pleinement qualifié).

Ressource Dans notre cas, `index.html`. Cette partie indique le chemin d'accès complet à cette ressource. Cette ressource peut être un fichier, comme dans notre cas. Il peut également s'agir d'un script CGI, d'une Java Server Page, etc.

Ici, l'acheminement de la demande au domaine `www.suse.fr` est pris en charge par les mécanismes correspondants de l'Internet (*Domain Name System* - Système de Noms de Domaines, DNS) qui redirigent l'accès à un domaine vers un ou plusieurs ordinateurs qui en sont responsables. Apache lui-même fournit alors la ressource, donc dans ce cas la page `index.html` de son répertoire de fichiers. Dans ce cas, le fichier se trouve dans le niveau le plus élevé du répertoire ; il peut cependant aussi se trouver dans un sous-répertoire, `http://www.suse.fr/en/business/services/index.html`.

Ici, le chemin d'accès du fichier est relatif à ce qu'on appelle le "DocumentRoot" qui peut être modifié dans les fichiers de configuration en procédant comme décrit dans la section *DocumentRoot* page 571.

23.1.4 Affichage automatique d'une page par défaut

Il arrive que l'indication de la page manque. Dans ce cas, Apache ajoute automatiquement à l'URL le nom le plus utilisé pour ces pages. Cette page s'appelle le plus fréquemment `index.html`. Le fait qu'Apache effectue ou non cette opération et le nom des pages renvoyées peuvent être configurés. Ces réglages sont décrits dans la section *DirectoryIndex* page 572. Dans ce cas, il suffit d'appeler `http://www.suse.fr` et le serveur affiche la page `http://www.suse.fr/index.html`.

23.2 Installation du serveur HTTP avec YaST

Vous pouvez installer Apache rapidement et facilement avec YaST. Vous devez cependant disposer de quelques connaissances si vous avez l'intention de l'utiliser pour mettre en place un serveur web. Si vous cliquez dans le centre de contrôle YaST sur 'Services réseau' → 'Serveur HTTP', on vous demandera si nécessaire si YaST doit installer les paquetages manquants. Si tout est installé, vous arrivez dans la boîte de dialogue de configuration ('Configuration du serveur HTTP').

Activez-y tout d'abord le 'Service HTTP' ; le port correspondant du pare-feu (port 80) est alors immédiatement ouvert ('Ouvrir le pare-feu sur les ports sélectionnés'). Dans la partie basse de la fenêtre ('Paramètres/Résumé') on peur configurer le ou les différents serveurs HTTP : 'Listen on' (l'option par défaut est `Port 80`), 'Modules', 'Hôte par défaut' et 'Hôtes'. Vous pouvez modifier les réglages pour les points ainsi sélectionnés avec 'Appliquer'.

Vérifiez d'abord l''Hôte par défaut' et adaptez le cas échéant la configuration à vos besoins. Activez ensuite dans 'Modules' les modules désirés. Vous pourrez faire des réglages de détail dans les prochaines boîtes de dialogue, et en particulier régler les paramètres des hôtes virtuels.

23.3 Les modules d'Apache

On peut ajouter de nombreuses fonctions à Apache par le biais de modules et ainsi d'exécuter des scripts CGI dans différents langages. En plus de Perl et PHP, d'autres langages de scripts sont à votre disposition comme Python ou Ruby. Il existe aussi des modules pour le transfert sécurisé de données via SSL (*Secure Sockets Layer* - Couche de connexion sécurisée) qui permettent l'authentification des utilisateurs, une journalisation avancée et bien plus encore.

L'utilisateur ayant le savoir-faire nécessaire peut développer des modules pour Apache afin de l'adapter à tous ses besoins et à tous ses souhaits. Pour de plus amples informations, consultez les références dans la section *Autres sources* page 588

Lorsque Apache traite une demande, il peut faire appel à un ou plusieurs gestionnaires (*handler* pour cela, en fonction des directives contenues dans le fichier de configuration. Les gestionnaires peuvent faire partie d'Apache, mais on peut également appeler un module gestionnaire. Ainsi, on peut configurer le processus de façon très flexible. On peut enfin intégrer ses propres modules dans Apache et ainsi influencer le traitement des demandes.

Avec Apache, la modularité va très loin car le serveur ne remplit que des tâches minimales, tout le reste étant réalisé par des modules. Pour Apache cela va jusqu'à traiter HTTP par le biais de modules. Apache ne doit donc pas nécessairement être un serveur web mais il peut aussi assurer un tout autre type de tâches par le biais d'autres modules. Un serveur de messagerie (POP3) basé sur Apache existe au titre d'étude de faisabilité.

D'autres fonctions utiles seront décrites par la suite.

Hôtes virtuels Au moyen d'hôtes virtuels, on peut exploiter, avec une seule instance d'Apache, plusieurs sites web sur un seul ordinateur, le serveur web faisant pour l'utilisateur final l'effet de plusieurs serveurs web indépendants. Dans ce but, les hôtes virtuels peuvent être configurés sur des adresses IP différentes ou basés sur les noms, économisant ainsi les coûts d'investissement et les travaux d'administration nécessaires pour d'éventuels ordinateurs supplémentaires.

Transcription flexible d'URL Apache offre une multitude de possibilités de manipulation et de transcription d'URL (*URL rewriting*). Pour de plus amples informations, consultez la documentation d'Apache.

Négociation du contenu En fonction des capacités du client (navigateur), Apache peut fournir à ce client une page sur mesure. On peut donc fournir aux navigateurs anciens ou aux navigateurs qui ne fonctionnent qu'en mode texte (comme Lynx) des versions plus simples, sans cadres, des pages consultées. De la même manière, on peut éviter les incompatibilités notoires des différents navigateurs en ce qui concerne JavaScript, en fournissant aux différents navigateurs une version adaptée des pages — et éventuellement aller jusqu'à adapter le code JavaScript à chaque navigateur.

Gestion d'erreurs flexible En cas d'erreur (lorsqu'une page n'est pas disponible), il est possible de réagir de façon flexible et de donner une réponse appropriée. Cette réponse peut aussi être construite dynamiquement à l'aide d'un script CGI.

23.4 Les fils d'exécution (threads)

Un fil d'exécution (*thread*) est une sorte de processus léger qui, comparé à un vrai processus, consomme beaucoup moins de ressources, ce qui fait que l'utilisation de fils d'exécution à la place de processus augmente également la performance. Ceci a, par contre, pour inconvénient que les applications pour le traitement dans un environnement à base de fils d'exécution doivent être thread-safe. Cela signifie que :

- Les fonctions (ou dans le cas d'applications orientées vers des objets, les méthodes) doivent être "réentrantes", que la fonction avec la même entrée fournit toujours le même résultat, peu importe si elle est traitée simultanément par d'autres fils d'exécution. Les fonctions doivent donc être programmées de telle façon qu'elles puissent être appelées par plusieurs fils d'exécution en même temps.

- L'accès aux ressources (en général des variables) doit être configuré de manière à éviter les conflits entre les fils d'exécution qui se déroulent en même temps.

Apache 2 est capable d'exécuter des demandes en tant que processus séparés ou dans un module mixte comprenant des processus et des fils d'exécution. L'exécution en tant que processus est réalisée par le MPM "prefork", l'exécution en tant que fil d'exécution par le MPM Okay"worker". Lors de l'installation (voir section *Installation* de la présente page), on peut choisir quel MPM sera utilisé. Le développement du troisième module, "perchild" n'est pas encore tout à fait terminé et n'est donc pas (encore) disponible dans SUSE LINUX pour l'installation.

23.5 Installation

23.5.1 Choix des paquetages dans YaST

Pour les besoins simples, il suffit de choisir le paquetage Apache `apache2`. Installez en plus un des paquetages MPM (*Multiprocessing Module* - Module de Multitraitement), comme le paquetage `apache2-prefork` ou `apache2-worker`. Lorsque l'on choisit le MPM, il faut savoir que l'on ne peut pas faire fonctionner conjointement le MPM Worker, qui fonctionne par fils d'exécution, et `mod_php4` car les bibliothèques fournies par ce paquetage ne garantissent pas de pouvoir s'exécuter en parallèle (ne sont pas toutes *thread-safe*).

23.5.2 Activation d'Apache

Une fois installé, il faut activer Apache comme service dans l'éditeur de niveaux d'exécutions. Pour démarrer Apache à l'amorçage du système, il faut cocher dans l'éditeur de niveau d'exécution les niveaux 3 et 5. On peut vérifier si Apache fonctionne en appelant l'URL `http://localhost` dans un navigateur. Si Apache tourne, on peut alors voir une page d'exemple si le paquetage `apache2-example-pages` est installé.

23.5.3 Les modules pour les contenus dynamiques

Pour utiliser des contenus dynamiques à l'aide de modules, installez en plus les modules pour les différents langages de programmation. Il s'agit du paquetage `apache2-mod_perl` pour Perl, du paquetage `apache2-mod_php4` pour PHP

et enfin du paquetage `apache2-mod_python` pour Python. L'utilisation de ces modules est décrite dans la section *Générer des contenus dynamiques avec des modules* page 578.

23.5.4 Paquetages supplémentaires recommandés

Il est en outre recommandé d'installer la documentation (paquetage `apache2-doc`). Après l'installation de ce paquetage et l'activation du serveur (voir section *Activation d'Apache* page précédente), on peut appeler la documentation directement avec l'URL `http://localhost/manual`.

Si vous voulez développer des modules pour Apache ou compiler des modules venant d'autres fournisseurs, vous devez aussi installer le paquetage `apache2-devel`, ainsi que les outils de développement correspondants. Ceux-ci contiennent, entre autres, les outils `apxs`, décrits plus en détail dans la section *Installation de modules avec apxs* de la présente page.

23.5.5 Installation de modules avec apxs

apxs2 est un outil important pour les développeurs de modules. Ce module permet de compiler et d'installer en une seule commande des modules se présentant comme du code source, y compris les modifications nécessaires aux fichiers de configuration. Il est également possible d'installer des modules se présentant déjà comme des fichiers objet (d'extension `.o`) ou comme des bibliothèques statiques (d'extension `.a`). apxs2 génère à partir de ces sources un objet partagé dynamique (*Dynamic Shared Object* - DSO) qui peut être utilisé directement comme module par Apache.

L'installation d'un module à partir du texte source s'effectue avec la commande `apxs2 -c -i -a mod_chose.c`. D'autres options d'`apxs2` sont décrites dans la page de manuel s'y rapportant. Les modules doivent être activés dans la section `APACHE_MODULES` de `/etc/sysconfig/apache2`, comme il est décrit dans la section *Configuration avec SuSEconfig* page suivante.

Il existe plusieurs versions d'apxs2 : `apxs2`, `apxs2-prefork` et `apxs2-worker`. Tandis qu'`apxs2` installe un module de telle manière qu'il peut être utilisé par les deux MPM, les deux autres programmes installent les modules de telle sorte qu'ils ne seront utilisés que par un MPM (donc prefork ou worker). Ainsi, tandis que dans le cas d'`apxs2` un module est installé dans `/usr/lib/apache2`, dans le cas de l'utilisation d'`apxs2-prefork` ce module est installé dans `/usr/lib/apache2-prefork`.

23.6 Configuration

Une fois Apache installé, les modifications ne sont nécessaires que lorsque vous avez des besoins ou souhaits particuliers. Vous pouvez configurer Apache via YaST ou SuSEconfig ou en éditant directement le fichier `/etc/apache2/httpd.conf`.

23.6.1 Configuration avec SuSEconfig

SuSEconfig reporte les réglages que vous effectuez dans `/etc/sysconfig/apache2` dans les fichiers de configuration d'Apache. Ceux-ci comprennent les possibilités de réglage qui devraient être suffisantes dans un bon nombre de cas. Le fichier contient des commentaires explicatifs pour chaque variable.

Fichiers de configuration séparés

Au lieu de procéder aux modifications directement dans le fichier de configuration `/etc/apache2/httpd.conf`, on peut, à l'aide de la variable `APACHE_CONF_INCLUDE_FILES`, d'indiquer un fichier de configuration séparé (`httpd.conf.local`) qui sera ensuite inclus dans le fichier de configuration principal, permettant ainsi de conserver des modifications de réglages isolés même si le fichier `/etc/apache2/httpd.conf` est écrasé lors d'une réinstallation.

Les modules

Les modules déjà installés via YaST sont activés en ajoutant le nom du module dans liste indiquée pour la variable `APACHE_MODULES` (Apache 2). Vous trouverez cette variable dans le fichier `/etc/sysconfig/apache2`.

Les drapeaux (flags)

Par la variable `APACHE_SERVER_FLAGS`, on peut indiquer des drapeaux (*flags*) qui activent et désactivent certaines sections dans le fichier de configuration. Si, donc, le fichier de configuration contient une section entre

```
<IfDefine someflag>
.
.
.
</IfDefine>
```

celui-ci ne sera activé que si le drapeau correspondant est positionné dans la variable `ACTIVE_SERVER_FLAGS` : `ACTIVE_SERVER_FLAGS= ... undrapeau ...` On peut ainsi activer ou désactiver simplement de larges sections du fichier de configuration en guise de test.

23.6.2 Configuration manuelle

Le fichier de configuration

Le fichier de configuration `/etc/apache2/httpd.conf` permet de réaliser des modifications qui ne sont pas possibles au moyen de `/etc/sysconfig/apache` ou de `/etc/sysconfig/apache2`. Vous trouverez ci-dessous quelques paramètres réglables à cet endroit. Ils apparaissent à peu près dans le même ordre que dans ce fichier.

DocumentRoot

Un réglage essentiel est le `DocumentRoot` ; il s'agit du répertoire dans lequel Apache prévoit de mettre les pages web qui seront fournies par le serveur. Pour l'hôte virtuel par défaut, il est réglé à `/srv/www/htdocs` et ne doit normalement pas être modifié.

Timeout

Indique le laps de temps pendant lequel le serveur attend avant d'indiquer un dépassement de délai pour une demande.

MaxClients

Le nombre maximum de clients qu'Apache fournit simultanément. Le réglage par défaut est `150` ; cependant, cette valeur peut être insuffisante dans le cas d'un site web très fréquenté.

LoadModule

Les instructions `LoadModule` indiquent quels modules seront chargés. Pour la version 2 d'Apache utilisée ici, l'ordre de chargement est indiqué par les modules eux-mêmes. De plus, ces instructions indiquent dans quel fichier le module est contenu.

Port

Indique le port sur lequel Apache attend les demandes. C'est normalement le port 80, le port standard pour HTTP. Il vaut mieux ne pas modifier ce réglage. Une raison de faire écouter Apache sur un autre port est lorsque l'on veut tester une nouvelle version du site web. De cette manière, la version fonctionnelle du site web est toujours disponible sur le port standard 80.

Une autre raison est de vouloir ne mettre les pages à disposition que sur un intranet car elle contiennent des informations qui ne sont pas destinées à tout le monde. Ceci peut se faire en mettant la valeur du port à 8080 et en interdisant tout accès extérieur à ce port avec le pare-feu. Le serveur est alors sécurisé contre tout accès provenant de l'extérieur.

Directory

Par le biais de cette directive, les droits d'accès et autres droits sont fixés pour un répertoire. Une telle directive existe également pour le `DocumentRoot` ; le nom du répertoire y étant indiqué doit toujours être modifié en parallèle avec la `DocumentRoot`.

DirectoryIndex

Ceci permet de configurer les fichiers que Apache devra chercher pour compléter une URL dont le fichier n'est pas indiqué. Le réglage par défaut est `index.html`. Lorsque l'URL `http://www.exemple.com/sous/repertoire` est appelée par le client et si dans la DocumentRoot il existe un répertoire `sous/repertoire` contenant un fichier du nom de `index.html`, cette page est renvoyée au client par Apache.

AllowOverride

Chaque répertoire à partir duquel Apache fournit des documents peut contenir un fichier qui permet de modifier pour ce répertoire les droits d'accès globalement configurés et d'autres réglages. Ceux-ci sont valables de manière récursive pour le répertoire actuel et ses sous-répertoires jusqu'à ce qu'elles soient modifiées dans un sous-répertoire par un autre fichier similaire. Ceci signifie aussi que de tels réglages sont valables globalement si elles sont indiquées dans un fichier dans le `DocumentRoot`. Ces fichiers portent généralement le nom de `.htaccess`, mais ce nom peut être modifié. Voir à ce sujet la section *AccessFileName* page ci-contre.

`AllowOverride` permet de définir si les réglages indiquées dans les fichiers locaux pourront remplacer les réglages globales. Les valeurs possibles sont `None`, `All` ainsi que toutes les combinaisons possibles d'`Options`, de `FileInfo`, de `AuthConfig` et de `Limit`. La documentation relative à Apache donne une description précise de la signification de ces valeurs. Le réglage par défaut (sans risque) est `None`.

Order

Cette option a une influence sur l'ordre dans lequel les directives des droits d'accès `Allow`, `Deny` seront appliquées. L'ordre par défaut est :

```
Order allow,deny
```

Sont d'abord appliqués les droits d'accès pour les accès autorisés et ensuite les droits pour les accès non autorisés. Il y a deux façons d'envisager les droits :

allow all autoriser tout accès, mais en définissant des exceptions.

deny all refuser tout accès, mais en définissant des exceptions.

Exemple pour `deny all`:

```
Order deny,allow
Deny from all
Allow from exemple.com
Allow from 10.1.0.0/255.255.0.0
```

AccessFileName

On peut régler ici le nom des fichiers qui, dans des répertoires servis par Apache, pourront écraser les réglages globaux des droits d'accès, etc. (voir aussi à ce sujet la section *AllowOverride* page précédente). Le réglage par défaut est `.htaccess`.

ErrorLog

Indique le nom du fichier dans lequel Apache consigne des messages d'erreur. Le réglage par défaut est `/var/log/httpd/error log`. Les messages d'erreur pour les hôtes virtuels (voir section *Les hôtes virtuels* page 582) sont également consignés dans ce fichier lorsqu'aucun fichier journal n'a été indiqué dans la section `VirtualHost` du fichier de configuration.

LogLevel

Les messages d'erreur sont classés en différents niveaux selon l'urgence. Ce réglage indique le niveau d'urgence à partir duquel les messages sont émis. Un réglage sur un niveau indique l'émission de messages de ce niveau et de messages plus urgents. Le réglage par défaut est `warn`.

Alias

On peut indiquer grâce à un alias un raccourci vers un répertoire au moyen duquel il est possible d'accéder directement à ce répertoire. Ainsi, on peut accéder via l'alias `/manuel/` au répertoire `/srv/www/htdocs/manual` même si le répertoire configuré dans la DocumentRoot diffère du répertoire `/srv/www/htdocs`. Tant que la DocumentRoot est positionnée sur cette valeur, cela ne change rien. Dans le cas d'un alias, on peut accéder avec `http://localhost/manual` directement au répertoire correspondant. Il peut éventuellement s'avérer nécessaire d'indiquer pour le répertoire cible indiqué dans une directive `Alias` une directive `Directory` dans laquelle sont configurés les droits relatifs à ce répertoire (voir la section *Directory* page 572).

ScriptAlias

Cette instruction ressemble à l'instruction alias. Elle indique en plus que les fichiers du répertoire cible doivent être gérés comme des scripts CGI.

Server Side Includes

On peut activer les Server Side Includes qui chercheront des instructions SSI au sein des fichiers exécutables. Ceci se fait grâce à l'instruction suivante :

```
<IfModule mod_include.c>
XBitHack on
</IfModule>
```

Pour vérifier qu'un fichier contient des Server Side Includes, il suffit de le rendre exécutable par `chmod +x` ⟨*nomfichier*⟩. Il est sinon aussi possible d'indiquer explicitement le type de fichiers devant être examinés à la recherche d'instructions SSI. Ceci se fait par

```
AddType text/html .shtml
AddHandler server-parsed .shtml
```

Ce n'est pas une bonne idée d'indiquer ici tout simplement `.html` puisqu'Apache analyser alors toutes les pages à la recherche de Server Side Includes (même celles qui n'en contiennent certainement pas), ce qui diminue considérablement la performance. Pour SUSE LINUX, ces deux instructions figurent déjà dans le fichier de configuration ; il n'y a normalement rien à régler.

UserDir

A l'aide du module `mod_userdir` et de la directive `UserDir`, on peut indiquer un répertoire dans le répertoire personnel de l'utilisateur, dans lequel celui-ci pourra publier ses fichiers via Apache. Ceci est configuré pour SuSEconfig par le biais de la variable `HTTPD_SEC_PUBLIC_HTML`. Pour être à même de publier les fichiers, il faut que cette variable soit mise à la valeur `yes`. Ceci amène à la déclaration suivante dans le fichier `/etc/httpd/suse_public_html.conf` lu par `/etc/apache2/httpd.conf`.

```
<IfModule mod_userdir.c>
UserDir public_html
</IfModule>
```

23.7 Apache en action

Pour afficher vos propres pages web (statiques) avec Apache, il suffit de placer vos fichiers dans le répertoire approprié. Sous SUSE LINUX, il s'agit de `/srv/www/htdocs`. Il se peut que quelques courtes pages d'exemple soient déjà installées. Celles-ci ne servent qu'à tester après l'installation si Apache a été installé et fonctionne correctement ; elles peuvent être remplacées, ou encore mieux désinstallées, sans aucun problème. Vous installez vos propres scripts CGI dans `/srv/www/cgi-bin` .

Pendant qu'il fonctionne, Apache enregistre des messages dans les fichiers `/var/log/httpd/access_log` ou `/var/log/apache2/access_log`. On y trouve des informations sur les ressources et le moment auquel elles ont été demandées et fournies et avec quelle méthode (`GET`, `POST` ...). En cas d'erreur, vous trouverez des informations s'y rapportant dans le fichier `/var/log/apache2`.

23.8 Les contenus dynamiques

Apache offre plusieurs possibilités pour fournir des contenus actifs aux clients. On entend par contenus dynamiques des pages HTML qui ont été traitées à partir de données variables saisies par le client. Un exemple connu sont les moteurs de recherche qui, après avoir saisi un ou plusieurs mot clés, éventuellement liés par des opérateurs logiques comme ET ou OU, renvoient une liste de pages contenant ces mots.

Il existe avec Apache trois variantes pour générer des contenus dynamiques :

Server Side Includes (SSI) Il s'agit là d'instructions implantées dans une page HTML à l'aide de commentaires spéciaux. Apache évalue le contenu des commentaires et fournit le résultat en tant que partie de la page HTML.

Common Gateway Interface (CGI) Il s'agit de l'exécution de programmes qui se trouvent dans certains répertoires. Apache remet à ces programmes des paramètres transmis par le client et renvoie le résultat de ces programmes au client. Ce type de programmation est relativement simple, étant donné qu'on peut transformer des programmes de ligne de commande existants de telle manière qu'ils reçoivent des données d'Apache et qu'ils lui renvoient les résultats.

Modules Apache offre des interfaces permettant d'exécuter des modules quelconques comme partie du traitement d'une demande et autorise en plus à ces programmes l'accès à des informations importantes, comme la requête ou l'en-tête HTTP. Ceci permet, lors du traitement de la demande, de mettre en jeu des programmes qui ne sont pas seulement à même de générer des contenus dynamiques, mais peuvent aussi assurer d'autres fonctions (comme l'authentification). La programmation de tels modules requiert, bien sûr, un peu d'habileté, mais présente aussi l'avantage d'offrir de bonnes performances ainsi que des possibilités allant bien au-delà de SSI ou même de CGI.

Au contraire des scripts CGI appelés par Apache (sous l'identité de propriétaire), lorsque l'on utilise des modules, un interpréteur est chargé dans Apache et tournera alors en permanance sous l'identité du serveur web. L'interpréteur est "persistent". Ceci permet d'éviter de lancer et terminer pour chaque demande un nouveau processus (ce qui entraînerait des frais considérables de gestion de processus, de mémoire, etc.) ; le script est tout simplement transmis à l'interpréteur déjà lancé.

Ceci présente cependant un inconvénient : tandis que les scripts exécutés via CGI sont relativement robustes face une programmation négligée, l'utilisation de modules révèle ce défaut rapidement. En effet, les erreurs comme le fait de ne pas libérer les ressources et la mémoire dans un script CGI ne sont pas très graves puisque les programmes sont arrêtés après traitement et puisque les ressources non libérées à cause d'une erreur de programmation redeviennent disponibles. Lors de l'utilisation de modules, les effets d'erreurs de programmation s'accumulent puisque l'interpréteur fonctionne sans interruption. Si le serveur n'est pas redémarré, l'interpréteur fonctionner sans problème pendant plusieurs mois et alors les connexions aux base de données non fermées et les défauts du même genre se manifesteront.

23.8.1 Les Server Side Includes : SSI

Les Server Side Includes sont des instructions implantées dans des commentaires spéciaux et exécutées par Apache. Leur résultat est mis à leur place dans la sortie. Un exemple : la date actuelle peut être affichée par `<!-- #echo var="DATE_LOCAL" -->`. Ici, c'est le # au début du commentaire `<!--` qui indique à Apache qu'il s'agit d'une instruction SSI et non pas d'un commentaire habituel.

Il existe plusieurs possibilités pour activer des SSI. La variante la plus simple consiste à scruter tous les fichiers qui possèdent le droit d'exécution à la recherche d'instructions SSI. L'autre variante consiste à définir pour certains types de fichiers qu'ils doivent être analysés à la recherche de SSI. Les deux réglages sont expliquées dans la section *Server Side Includes* page 574.

23.8.2 L'interface Common Gateway Interface: CGI

CGI est l'abréviation de "Common Gateway Interface". Avec CGI, le serveur ne fournit pas seulement une page HTML statique, mais exécute tout un programme qui fournit la page. Il est ainsi possible de créer des pages qui sont le résultat d'un calcul, le résultat d'une recherche dans une base de données. Des arguments peuvent être transmis au programme exécuté, qui est donc à même de fournir une page de réponse individuelle à chaque demande.

CGI a l'avantage d'être une technique assez simple. Il suffit que le programme se trouve dans un certain répertoire pour pouvoir être exécuté par le serveur web exactement comme un programme dans la ligne de commande. Les sorties du programme sur la sortie standard (`stdout`) sont simplement transmises aux clients par le serveur.

23.8.3 GET et POST

Les paramètres d'entrée sont transmis au serveur par `GET` ou par `POST`. En fonction de la méthode utilisée, le serveur transmet les paramètres au script de différentes manières. Avec `POST`, le serveur transmet les paramètres au programme par l'entrée standard (`stdin`). S'il était démarré sur une console, le programme obtiendrait ses paramètres de la même manière.

Avec `GET`, le serveur transmet les paramètres au programme dans la variable d'environnement `QUERY_STRING`.

23.8.4 Les langages pour CGI

En principe, tous les langages de programmation peuvent être utilisés pour écrire des programme CGI. On utilise typiquement des langages de scripts (langages interprétés) comme Perl ou PHP ; dans certains cas, C ou C++ pourra être le langage par défaut pour les CGI dont la vitesse est critique.

Dans le cas le plus simple, Apache attend ces programmes dans un répertoire défini (`cgi-bin`). Ce répertoire peut être défini dans le fichier de configuration, voir la section *Configuration* page 570.

De plus, il est possible de permettre d'utiliser d'autres répertoires dans lesquels Apache pourra rechercher d'autres programmes exécutables. Ceci comporte un certain risque pour la sécurité puisque tout utilisateur (éventuellement mal intentionné) peut faire exécuter des programmes par Apache. Si les programmes ne peuvent être exécutés que dans `cgi-bin`, l'administrateur contrôler plus facilement qui y dépose des scripts et des programmes et si ceux-ci sont éventuellement de nature malveillante.

23.8.5 Générer des contenus dynamiques avec des modules

Apache dispose de toute une série de modules disponibles à l'utilisation. Tous les modules décrits ci-dessous sont disponibles comme paquetages dans SUSE LINUX. La notion de module a deux significations. Il existe d'une part des modules qui peuvent etre chargés dans Apache où ils assurent une certaine fonction, les modules présentés ci-dessous servant à implanter des langages de programmation dans Apache.

D'autre part, dans le contexte de langages de programmation, on comprend par modules une quantité exhaustive de fonctions, de classes et de variables. Ces modules sont implantés dans un programme pour mettre à disposition une certaine

fonctionnalité. On peut citer comme exemple les modules CGI existant dans tous les langages de scripts qui facilitent l'écriture d'application CGI en fournissant, entre autres, des méthodes pour lire les paramètres Request et pour afficher du code HTML.

23.8.6 mod_perl

Perl est un langage de script répandu et ayant fait ses preuves. Pour Perl, il existe une grande quantité de modules et de bibliothèques (dont une bibliothèque pour l'extension du fichier de configuration d'Apache). Vous trouverez un grand choix de bibliothèques pour Perl dans le CPAN (*Comprehensive Perl Archive Network* - Réseau Complet d'Archive pour Perl) : `http://www.cpan.org/`. `http://www.mongueurs.net/` est un site web en français pour les programmeurs Perl.

Configurer mod_perl

Pour mettre en place `mod_perl` dans SUSE LINUX, il suffit d'installer le paquetage correspondant (voir la section *Installation* page 568). Les déclarations nécessaires dans le fichier de configuration pour Apache sont déjà existantes, voir `/etc/apache2/mod_perl-startup.pl`. Vous trouverez un bon nombre d'informations sur `mod_perl` à l'adresse `http://perl.apache.org/` (en anglais).

mod_perl comparé à CGI

Dans le cas le plus simple, on peut faire fonctionner un script, jusqu'à présent CGI, en tant que script `mod_perl` en l'appelant à une autre URL. Le fichier de configuration contient des alias, qui font référence au même répertoire et appellent des scripts qu'il contient via CGI ou par `mod_perl`. Toutes ces déclarations figurent déjà dans le fichier de configuration. Pour CGI, la déclaration d'alias est :

```
ScriptAlias /cgi-bin/ "/srv/www/cgi-bin/"
```

Voici les déclarations pour `mod_perl` :

```
<IfModule mod_perl.c>
# Fournit deux alias au même répertoire cgi-bin
# pour illustrer les effets de deux mod_perl différents
```

```
# avec le module Apache::Registry
ScriptAlias /perl/         "/srv/www/cgi-bin/"
# avec le module Apache::Perlrun
ScriptAlias /cgi-perl/      "/srv/www/cgi-bin/"
</IfModule>
```

Les déclarations suivantes sont également requises pour `mod_perl`. Elles figurent aussi déjà dans le fichier de configuration.

```
#
# Si mod_perl est activé, charger les informations de configuration
#
<IfModule mod_perl.c>
Perlrequire /usr/include/apache/modules/perl/startup.perl
PerlModule Apache::Registry

#
# configure le module Apache::Registry pour l'alias /perl
#
<Location /perl>
SetHandler perl-script
PerlHandler Apache::Registry
Options ExecCGI
PerlSendHeader On
</Location>

#
# configure le module Apache::PerlRun pour l'alias /cgi-perl
#
<Location /cgi-perl>
SetHandler perl-script
PerlHandler Apache::PerlRun
Options ExecCGI
PerlSendHeader On
</Location>

</IfModule>
```

Ces déclarations créent des alias pour les modes `Apache::Registry` et `Apache::PerlRun`. La différence entre les deux modes est décrite ci-dessous :

Apache::Registry Tous les scripts sont compilés puis gardés dans un cache. Chaque script est créé en tant contenu d'un sous-programme, ce qui est bien du côté de la performance, mais qui a pourtant un inconvénient : la programmation des scripts doit être faite très soigneusement puisque les variables et les sous-programmes entre les différents appels ne bougent pas. Ceci signifie qu'il convient de remettre soi-même les variables à zéro, pour qu'elles puissent être réutilisées lorsqu'elles sont à nouveau appelées. Si on enregistre dans un script de banque en ligne le numéro de carte de crédit d'un client dans une variable, ce numéro pourra être présent lorsque le client suivant utilise cette application et donc appelle le même script.

Apache::PerlRun Les scripts sont recompilés pour chaque appel afin de faire disparaître de l'espace de nom les variables et les sous-programmes entre les appels. L'espace de nom est la totalité de tous les noms de variables et de routines définis à un moment donné pendant l'existence d'un script. Avec `Apache::PerlRun`, une programmation soigneuse n'est donc pas si importante car toutes les variables sont réinitialisées au lancement du script et elles ne peuvent plus contenir de valeurs provenant des appels précédents. Cela se fait au détriment de la vitesse, mais cela reste plus rapide qu'un CGI car il n'est pas nécessaire d'appeler un processus propre pour l'interpréteur. Le comportement de `Apache::PerlRun` est semblable à celui de CGI.

23.8.7 mod_php4

PHP est un langage de programmation spécialement conçu pour être utilisé avec des serveurs web. Il se distingue d'autres langages, dont les commandes sont enregistrées dans des fichiers à part (script), par le fait que lors de PHP, les commandes sont implantées dans une page HTML (semblable à SSI). L'interpréteur PHP traite les commandes PHP et implante le résultat du traitement dans une page HTML.

Vous trouverez le site web de PHP à l'adresse `http://www.php.net/`. Pour une site sur PHP en français, consultez `http://www.phpindex.com/`.

Le paquetage `mod_php4-core` doit en tout cas être installé. Apache 2 requiert en plus le paquetage `apache2-mod_php4`.

23.8.8 mod_python

Python est un langage de programmation orienté objet qui dispose d'une syntaxe très claire et très lisible. Ce qui est un peu inhabituel, mais après une courte

phase d'adaptation, vraiment agréable, est le fait que la structure du programme dépend du retrait. Les blocs ne sont pas définis par des accolades (comme c'est le cas dans C et Perl) ou d'autres séparateurs (comme `begin` et `end`), mais par la taille du retrait. Installez le paquetage `apache2-mod_python`.

Vous trouverez des informations plus détaillées à l'adresse `http://www.python.org/`. Pour plus d'informations sur `mod_python`, consultez `http://www.modpython.org/`.

23.8.9 mod_ruby

Ruby est un langage de programmation de haut niveau orienté objet relativement nouveau, présentant des ressemblances tant avec Perl qu'avec Python et particulièrement bien approprié pour les scripts. Comme Python, il présente une syntaxe claire et bien compréhensible tandis qu'il a repris de Perl les raccourcis tant aimés (et pour d'autres tant détestés) par beaucoup de programmateurs, comme `$.r`, le numéro de la dernière ligne lue à partir du fichier d'entrée. Pour ce qui est de la conception de base, Ruby ressemble beaucoup à Smalltalk.

Vous trouverez le site web de Ruby à l'adresse `http://www.ruby-lang.org/`. Pour Ruby, il existe également un module Apache, dont vous trouverez la page web à l'adresse `http://www.modruby.net/`.

23.9 Les hôtes virtuels

Les hôtes virtuels permettent de configurer plusieurs domaines sur un unique serveur du réseau. On économise ainsi les coûts et le travail d'administration nécessaires à l'installation d'un serveur par domaine. Il existe plusieurs possibilités pour les hôtes virtuels :

- les hôtes virtuels basés sur le nom ;
- les hôtes virtuels basés sur l'adresse IP.
- Faire fonctionner plusieurs instances d'Apache sur un seul ordinateur.

23.9.1 Les hôtes virtuels basés sur le nom

Plusieurs domaines peuvent être gérés par une seule instance d'Apache par le biais des hôtes virtuels basés sur le nom. La configuration de plusieurs adresses IP pour un ordinateur n'est alors pas nécessaire. Il s'agit de l'alternative la plus

simple et qui devrait être préférée. Des raisons pouvant s'opposer à l'utilisation d'hôtes virtuels basés sur le nom sont disponibles dans la documentation d'Apache.

Ce paramétrage s'effectue directement au moyen du fichier de configuration `/etc/apache2/httpd.conf`. Pour activer un hôte virtuel basé sur nom, il faut indiquer une directive adéquate : `nom hôte virtuel *`. Il suffit d'indiquer ici `*` afin qu'Apache reçoive simplement toutes les demandes qui arrivent. Vous devez ensuite configurer chaque hôte virtuel :

```
<VirtualHost *>
    ServerName www.
    DocumentRoot /srv/www/htdocs/
    ServerAdmin webmaster@
    ErrorLog /var/log/httpd/www.-error_log
    CustomLog /var/log/httpd/www.-access_log common
</VirtualHost>
```

Ici, comme dans la suite, il convient de modifier pour Apache le chemin d'accès aux fichiers journaux, en le changeant de `/var/log/httpd` en `/var/log/apache2`. Pour le domaine hébergé par le serveur à l'origine (`www.`), il faut également créer une déclaration d'hôte virtuel. Dans cet exemple, le domaine initial et un autre domaine (`www.monautreentreprise.fr`) sont donc hébergés sur le même serveur.

Dans les directives `VirtualHost`, il est indiqué un *, tout comme pour `NameVirtualHost`. Apache établit le rapport entre la demande et l'hôte virtuel par le champ d'hôte dans l'entête HTTP. La demande est remise à l'hôte virtuel, dont le `nom serveur` correspond au nom de l'hôte indiqué dans ce champ.

Dans les directives `ErrorLog` et `CustomLog`, il n'est pas crucial que fichiers contiennent le nom du domaine ; on peut utiliser des noms quelconques.

`Serveradmin` désigne l'adresse e-mail d'une personne responsable auquel on peut s'adresser en cas de problèmes. Si des erreurs se produisent, Apache indique cette adresse dans les messages d'erreur qu'il restitue au client.

23.9.2 Les hôtes virtuels basés sur l'adresse IP

Pour cette alternative, il faut configurer plusieurs adresses IP sur l'ordinateur. Une instance d'Apache commande ensuite plusieurs domaines, chaque domaine étant attribué à une adresse IP. L'exemple qui suit montre comment

configurer Apache afin qu'il héberge, outre sur son adresse IP d'origine `192.168.1.10`, encore deux autres domaines sur des adresses IP supplémentaires (`192.168.1.20` et `192.168.1.21`). Cet exemple concret ne fonctionne bien sûr que dans un intranet, puisque les adresses IP allant de `192.168.0.0` à `192.168.255.0` ne sont pas transmises (routées) dans l'Internet.

Configurer les alias IP

Pour qu'Apache puisse héberger plusieurs adresses IP, l'ordinateur sur lequel Apache fonctionne doit accepter les demandes pour plusieurs adresses IP, ce qu'on appelle le *Multi-IP-Hosting*. Cela nécessite d'abord que les alias IP soient activés dans le noyau, ce qui est le cas par défaut sous SUSE LINUX.

Une fois que le noyau est configuré pour prendre en charge les alias IP, on peut affecter plusieurs adresses IP à l'ordinateur en utilisant les commandes `ifconfig` et `route`. Pour exécuter ces commandes, l'utilisateur doit s'être connecté en tant que `root`. On suppose, par la suite, que l'ordinateur dispose déjà de sa propre adresse IP, `192.168.1.10` étant attribuée au périphérique réseau `eth0`.

On peut vérifier quelle adresse IP est utilisée par l'ordinateur en saisissant `ifconfig`. Pour ajouter d'autres adresses IP, procédez de la manière suivante :

```
/sbin/ifconfig eth0:0 192.168.1.20
/sbin/ifconfig eth0:1 192.168.1.21
```

Toutes ces adresses IP sont attribuées au même périphérique réseau physique (`eth0`).

Les hôtes virtuels basés sur l'adresse IP

Lorsque les alias IP ont été configurés sur le système ou bien que l'ordinateur a été configuré avec plusieurs cartes de réseau, on peut procéder à la configuration d'Apache. Indiquez pour chaque serveur virtuel son propre bloc `VirtualHost` :

```
<VirtualHost 192.168.1.20>
    ServerName www.monautreentreprise.fr
    DocumentRoot /srv/www/htdocs/monautreentreprise.fr
    ServerAdmin webmestre@monautreentreprise.fr
    ErrorLog /var/log/httpd/www.monautreentreprise.fr-error_log
```

```
    CustomLog /var/log/httpd/www.monautreentreprise.fr-access_log common
</VirtualHost>

<VirtualHost 192.168.1.21>
    ServerName www.encoreuneentreprise.fr
    DocumentRoot /srv/www/htdocs/encoreuneentreprise.fr
    ServerAdmin webmestre@encoreuneentreprise.fr
    ErrorLog /var/log/httpd/www.encoreuneentreprise.fr-error_log
    CustomLog /var/log/httpd/www.encoreuneentreprise.fr-access_log common
</VirtualHost>
```

On n'indique ici les directives d'hôte virtuel que pour les domaines supplémentaires ; le domaine initial (`www.`) est toujours configuré par les réglages correspondants (`DocumentRoot` etc.) en dehors des blocs `VirtualHost`.

23.9.3 Plusieurs instances d'Apache

Dans le cas des méthodes précédentes concernant les hôtes virtuels, les administrateurs d'un domaine sont capables de lire les données contenues dans les autres domaines. Si on veut séparer les différents domaines les uns des autres, on peut lancer plusieurs instances d'Apache qui utilisent chacune dans le fichier de configuration leurs propres réglages pour `User`, `Group` etc..

Indiquez dans le fichier de configuration par la directive `Listen` quelle instance d'Apache est compétente pour quelle adresse IP. Comme dans l'exemple précédent, la directive pour la première instance d'Apache serait :

```
Listen 192.168.1.10:80
```

Pour les deux autres instances, elle serait :

```
Listen 192.168.1.20:80
Listen 192.168.1.21:80
```

23.10 Sécurité

23.10.1 Limiter les risques

Si sur un ordinateur, aucun serveur web n'est nécessaire, il vaut mieux désactiver Apache dans l'éditeur de niveaux d'exécution ou ne pas l'installer (ou le désinstaller). Tout serveur ne fonctionnant pas sur un ordinateur veut dire une source d'attaque potentielle en moins. Cela vaut notamment pour les ordinateurs qui servent de pare-feu ; il est vivement recommandé, autant que possible, de ne pas faire fonctionner de serveur web sur ces ordinateurs.

23.10.2 Les droits d'accès

DocumentRoot devrait appartenir à root

Le répertoire `DocumentRoot` (`/srv/www/htdocs`) et le répertoire CGI appartiennent par défaut à l'utilisateur `root`, et il ne faut rien y changer. Si tout le monde peut écrire dans ces répertoires, il est également possible à tout utilisateur d'y enregistrer des fichiers. Ces fichiers sont ensuite exécutés par Apache, à savoir en tant qu'utilisateur `wwwrun`. Apache ne doit avoir aucun droit d'écriture sur les données et les scripts qu'il fournit. C'est la raison pour laquelle ceux-ci ne doivent pas appartenir à l'utilisateur `wwwrun`, mais à `root`.

Si on veut que les utilisateurs aient la possibilité de placer des fichiers dans la racine des documents d'Apache, il faut alors de créer un sous-répertoire inscriptible pour tout le monde, comme `/srv/www/htdocs/wir_ueber_uns`, au lieu de rendre la racine des documents d'Apache inscriptible.

Publier des documents à partir de son propre répertoire personnel

Lorsqu'un utilisateur veut mettre en ligne des fichiers sur le réseau, on peut indiquer dans le fichier de configuration un sous-répertoire du répertoire personnel de l'utilisateur dans lequel il pourra déposer ses fichiers destinés au web (`~/public_html`. Ceci est activé par SUSE LINUX dans la configuration par défaut ; plus de détails sont disponibles en section *UserDir* page 575.

On peut alors utiliser sur ces pages l'identité de l'utilisateur dans l'URL, qui contient l'indication ~ ⟨*nom d'utilisateur*⟩ comme raccourci vers le répertoire concerné du répertoire personnel de l'utilisateur.Par exemple, lorsque l'on saisit l'URL `http://localhost/~tux` dans un navigateur, les données du répertoire `public_html` du répertoire personnel de l'utilisateur sont affichées.

23.10.3 Toujours rester à la page

Tous ceux qui mettent en place un serveur web — et en particulier si ce serveur web est ouvert au public — devraient veiller à rester à la pointe de l'information en ce qui concerne les failles et les attaques potentielles qui en résultent.

Vous trouverez une liste des sources pour la recherche d'exploits et de correctifs dans la section *Sécurité* page suivante.

23.11 Résolution de problèmes

Si vous rencontrez des problèmes, si Apache n'affiche pas bien, voire pas du tout, une page, les mesures suivantes vous aideront à découvrir la source du problème.

- Consultez d'abord le journal des erreurs pour savoir si les messages vous indiquent le défaut : `/var/log/httpd/error_log` ou `/var/log/apache2/error_log`.
  Faites défiler, si possible dans une console, les fichiers journaux pour pouvoir voir en parallèle les accès au serveur et la manière dont il réagit. Pour cela, indiquez dans une console `root` la commande suivante :

  ```
  tail -f /var/log/apache2/*_log
  ```

- Consultez la base de données des bogues, disponible en ligne à l'adresse `http://bugs.apache.org/`.
- Consultez les listes de discussion et les forumss. La liste de discussion pour les utilisateurs se trouve à l'adresse `http://httpd.apache.org/userslist.html`. Nous conseillons le forum `comp.infosystems.www.servers.unix` et les forums apparentés.
- Si toutes les possibilités précédentes ne vous ont été d'aucune aide et si vous êtes sûr d'avoir trouvé un bogue dans Apache, adressez-vous directement à nous à l'adresse `http://www.suse.de/feedback/`.

23.12 Documentation complémentaire

23.12.1 Apache

Apache est fourni avec une documentation détaillée. La section *Installation* page 568 décrit comment l'installer. Elle est alors à votre disposition à l'adresse

http://localhost/manual. Bien sûr, la documentation la plus récente est toujours disponible sur le site web d'Apache : http://httpd.apache.org

23.12.2 CGI

Pour de plus amples informations sur CGI, consultez les pages suivantes :

- http://apache.perl.org/
- http://perl.apache.org/
- http://www.modperl.com/
- http://www.modperlcookbook.org/
- http://www.fastcgi.com/
- http://www.boutell.com/cgic/

23.12.3 Sécurité

Vous trouverez en permanence à l'adresse http://www.suse.de/security/ (en anglais) les correctifs actuels pour les paquetages SUSE LINUX. Consultez régulièrement cette URL à partir de laquelle on peut également s'abonner à la liste de diffusion "SUSE Security Announcements" (Annonces de SUSE relatives à la sécurité)

L'équipe d'Apache mène une politique d'information ouverte en ce qui concerne les erreurs possibles dans Apache. Vous trouverez des messages actuels sur les bogues et des points d'attaque pouvant éventuellement en résulter à l'adresse http://httpd.apache.org/security_report.html.

Si vous avez vous-même relevé un problème concernant la sécurité (vérifiez d'abord sur les pages ci-dessus s'il s'agit vraiment d'un problème inconnu), vous pouvez le signaler par courrier électronique à security@suse.de ou bien au moyen de security@apache.org.

23.12.4 Autres sources

Consultez toujours la base de données d'assistance de SUSE http://sdb.suse.de/ en cas de difficultés.

Un journal en ligne sur toutes les questions concernant Apache est disponible à l'URL : http://www.apacheweek.com/

Pour connaître l'origine d'Apache, vous trouverez une description détaillée à l'adresse `http://httpd.apache.org/ABOUT_APACHE.html`. Vous pourrez également y apprendre pourquoi le serveur s'appelle Apache.

Vous trouverez des informations relatives à la mise à niveau de la version 1.3 vers la version 2.0 sur le site `http://httpd.apache.org/docs-2.0/de/upgrading.html`.

Synchronisation des fichiers

De nos jours, beaucoup de personnes utilisent plusieurs ordinateurs : un ordinateur à la maison, un ou plusieurs ordinateurs sur le lieu de travail et éventuellement en plus un ordinateur portable ou un assistant personnel pour les déplacements. On a besoin d'une grande quantité de fichiers sur tous ces ordinateurs et on souhaiterait pouvoir les modifier. Par ailleurs, ces données doivent en plus être disponibles partout dans leur version actuelle.

24.1 Logiciels pour la synchronisation des fichiers

Sur des ordinateurs reliés en permanence entre eux par un réseau rapide, la synchronisation de fichiers ne pose aucun problème. Il suffit de choisir un système de fichiers réseau, comme NFS et d'enregistrer les fichiers sur un serveur. Ensuite, tous les ordinateurs accèdent aux mêmes données par l'intermédiaire du réseau.

Cette méthode ne fonctionne pas dans le cas d'une mauvaise connexion réseau ou si la liaison est partiellement indisponible. Les personnes qui voyagent avec un ordinateur portable sont amenées à avoir des copies de tous les fichiers sur le disque dur local. Mais lorsque les fichiers sont modifiés, le problème de la synchronisation se pose vite. Si un fichier a été modifié sur un ordinateur, il faut veiller à actualiser aussi la copie du fichier sur tous les autres ordinateurs. Si cette situation ne se produit que de temps en temps, les procédures de copie manuelle à l'aide de scp ou de rsync sont suffisantes. Avec une plus grande quantité de données, la tâche se complique rapidement et requiert une grande attention de la part de l'utilisateur pour éviter des erreurs, comme le remplacement d'une nouvelle version d'un fichier par une version plus ancienne.

Attention

Risque de perte de données

Il faut de toute façon se familiariser avec le logiciel utilisé et tester ses fonctions avant de gérer ses données à l'aide d'un système de synchronisation. Pour les données importantes, une sauvegarde est indispensable.

Attention

Pour s'épargner le travail fastidieux de la synchronisation des données comportant un risque élevé d'erreurs, il existe des logiciels qui automatisent cette tâche en se basant sur différentes méthodes. Les brefs aperçus suivants ont pour but de donner à l'utilisateur une idée de fonctionnement et de l'utilisation de ces logiciels. Avant de les mettre en œuvre réellement, il vaut mieux lire attentivement la documentation y afférant.

24.1.1 unison

Dans le cas d'unison, il ne s'agit pas d'un système de fichiers réseau. Ici, en revanche, on enregistre les fichiers et on travaille avec ces derniers tout à fait normalement en local. Le programme unison peut être appelé manuellement pour synchroniser des fichiers. Lors de la première synchronisation, une base de données est créée sur les deux ordinateurs concernés, dans laquelle sont enregistrés les sommes de contrôle, les pointeurs temporels et les autorisations des fichiers sélectionnés.

Lors de l'appel suivant, unison peut reconnaître quels fichiers ont été modifiés et en proposer la transmission d'un ordinateur vers l'autre. Dans le meilleur des cas, on peut accepter toutes les propositions.

24.1.2 CVS

Utilisé en général pour la gestion de versions de textes sources de logiciels, CVS offre la possibilité de disposer des copies de fichiers sur plusieurs ordinateurs. Il se prête donc parfaitement à ce que nous recherchons.

Dans le cas de CVS, il existe une base de données centrale (repository, ou en français, un référentiel) sur le serveur qui ne stocke pas seulement les fichiers mais également les modifications de ces fichiers. Toute modification effectuée localement est validée (commit) dans la base de données pour être reprise (update) par d'autres ordinateurs. Les deux procédures doivent être préparées par l'utilisateur.

En ce qui concerne les modifications, CVS est très tolérant vis-à-vis des erreurs : les modifications sont rassemblées, et il n'y a conflit que si des modifications ont été apportées aux mêmes lignes. Dans ce cas, la base de données reste dans un état stable, le conflit est visible et doit être résolu sur l'ordinateur client.

24.1.3 subversion

Contrairement à CVS qui a fait ses preuves, subversion est un projet en constante évolution ; subversion a été développé pour remplacer CVS et abolir ses limitations techniques.

Il est clair que subversion a été amélioré dans de nombreux domaines. En raison de son histoire, CVS ne gère que les fichiers et "ignore" tout des répertoires. Dans subversion, au contraire, les répertoires possèdent aussi un historique de versions et peuvent également être copiés et renommés exactement comme les

fichiers. En outre, il est possible d'ajouter à chaque fichier et à chaque répertoire des métadonnées qui sont également soumises à la gestion des versions. À la différence de CVS, subversion offre un accès réseau transparent grâce à quelques protocoles comme WebDAV .

Pour la réalisation de subversion, il a fallu avoir largement recours à des paquetages de programmes existants. Ainsi, pour faire fonctionner subversion, on utilise également toujours le serveur web apache avec l'extension WebDAV.

24.1.4 mailsync

Comparé aux outils de synchronisation mentionnés jusque-là, Mailsync sert uniquement à la synchronisation des messages électroniques entre les différentes boîtes aux lettres. Il peut s'agir aussi bien des fichiers de boîtes aux lettres locaux que de ceux des boîtes aux lettres hébergées sur un serveur IMAP.

Il est décidé, en fonction de l'identificateur de message (Message-ID) contenu dans l'en-tête du message électronique, individuellement pour chaque message s'il doit être sychronisé ou effacé. Une sychronisation est possible autant entre les différentes boîtes aux lettres qu'entre les hiérarchies de boîtes aux lettres.

24.1.5 rsync

Lorsque vous n'avez pas besoin du contrôle de versions mais que vous souhaitez synchroniser de grandes arborescences de fichiers sur des connexions réseau lentes, l'outil rsync est fait pour vous. rsync dispose de mécanismes minutieux pour transférer exclusivement des modifications à des fichiers. Cela ne concerne pas seulement les fichiers texte, mais également les fichiers binaires. Pour reconnaître les différences entre fichiers, rsync répartit les fichiers en blocs et calcule des sommes de contrôle correspondant à ces blocs.

L'effort consenti à reconnaître les modifications a aussi un prix. Pour que rsync fonctionne, il faut redimensionner généreusement les ordinateurs qui doivent être synchronisés. Il n'est surtout pas question d'économiser sur la RAM (mémoire vive).

24.2 Critères de choix du logiciel

24.2.1 Modèle client-serveur contre égalité des droits

Deux modèles différents de répartition de données sont répandus. Dans le premier modèle, il est possible d'utiliser un serveur central avec lequel tous les autres ordinateurs (appelés clients) synchronisent leurs données. Le serveur doit être accessible par le réseau au moins de temps en temps par tous les clients. Ce modèle est utilisé par subversion, CVS et WebDAV. Dans l'autre modèle, tous les ordinateurs peuvent étre connectés par le réseau au même niveau et synchroniser mutellement leurs données. Cette méthode est utilisée par unison. rsync fonctionne en réalité en mode client-serveur, mais on peut utiliser chaque client en tant que serveur.

24.2.2 Portabilité

Subversion, CVS, rsync et unison sont également disponibles sur de nombreux autres systèmes d'exploitation comme les autres Unix et sous Windows.

24.2.3 Interactif contre automatique

Dans le cas de subversion, de CVS, de WebDAV, de rsync et de unison, la synchronisation de données est lancée manuellement par l'utilisateur. Ce comportement permet de contrôler plus précisément les données à synchroniser et de gérer plus aisément les conflits. En revanche, la synchronisation risque d'être réalisée trop rarement, ce qui augmente les risques de conflit.

24.2.4 Conflits : survenue et solutions

Dans le cas de subversion ou de CVS, il est rare qu'un conflit survienne, même si plusieurs personnes collaborent dans un gros projet de logiciel. Ici, les documents sont réunis ligne par ligne. En cas de conflit, cela ne concerne toujours qu'un seul client. Un conflit est en principe facile à résoudre avec subversion ou CVS. Dans le cas d'unison, vous êtes informé des conflits et il est possible d'éviter la synchronisation du fichier. En revanche, les modifications ne sont pas si faciles à effecter, comparé à subversion ou à CVS.

Alors que dans subversion ou CVS il est également possible d'enregistrer partiellement des modifications en cas de conflit, WebDAV ne procède à la validation que si l'ensemble de la modification réussit.

rsync n'offre aucun moyen de traiter les conflits. L'utilisateur doit veiller lui-même à ne pas écraser des fichiers par erreur et à résoudre à la main tous les conflits susceptibles d'apparaître. Pour ne pas courir de risques, on peut utiliser en sus un système de contrôle de versions comme RCS.

24.2.5 Choisir et ajouter des fichiers

Dans le cas d'unison et de rsync, toute la structure arborescente du répertoire est synchronisée. Les nouveaux fichiers qui s'y présentent sont automatiquement concernés par la synchronisation.

Avec Subversion ou CVS, les nouveaux répertoires et fichiers doivent être ajoutés explicitement au moyen de `svn add` et `cvs add`, ce qui permet un contrôle précis des fichiers à synchroniser. En revanche, de nouveaux fichiers sont souvent négligés, surtout si, étant donné la quantité de fichiers, les '?' signalés par `svn update`, `svn status` et `cvs update` sont ignorés.

24.2.6 Historique

Subversion et CVS offrent comme fonctionnalité supplémentaire de reconstitution des anciennes versions de fichiers. Lors de chaque modification, il est possible d'ajouter une brève note de travail, permettant de suivre ensuite facilement le développement des fichiers grâce au contenu et aux annotations. Ceci constitue une aide très utile pour les projets de fin d'études et les textes de logiciels.

24.2.7 Quantité de données / Encombrement du disque dur

On a besoin sur tous les ordinateurs concernés de suffisamment d'espace pour héberger toutes les données réparties. Dans le cas de subversion et de CVS, il faut en plus prévoir de l'espace sur le serveur pour la base de données (le *repository*, ou référentiel). L'historique des données y étant enregistré, cet espace occupé est beaucoup plus grand que l'encombrement réel. Pour les fichiers au format texte, la place occupée est relativement raisonnable car seules les lignes modifiées sont à nouveau stockées. En revanche, pour les fichiers binaires, l'encombrement augmente à chaque modification de la taille du fichier.

24.2.8 Interface graphique utilisateur

L'interface graphique utilisateur d'unison propose les synchronisations possibles unison. Vous pouvez soit accepter la proposition soit rejeter certains fichiers de la synchronisation. En mode texte, il est en outre possible de s'acquitter des procédures individuellement de façon interactive.

Les utilisateurs expérimentés emploient normalement Subversion et CVS sur la ligne de commande. Il existe cependant des interfaces graphiques pour Linux (cervisia, ...) ainsi que pour Windows (wincvs). Beaucoup d'outils de développement (kdevelop) et d'éditeurs de texte (emacs) offrent une prise en charge de CVS. Ces interfaces permettent bien souvent de résoudre facilement les conflits.

24.2.9 Contraintes de l'utilisateur

unison et rsync sont assez faciles à utiliser et conviennent également aux débutants. CVS et subversion sont un peu plus complexes. Pour ces derniers, il faut avoir compris l'interaction entre référentiel et données locales. Les modifications des données doivent d'abord toujours être rassemblées en local dans le référentiel. Les commandes `cvs update` et `svn update` sont prévues à cet effet. Dès que cette opération est terminée, les données doivent être à nouveau renvoyées au référentiel avec les commandes `cvs commit` et `svn commit` Une fois qu'on a approfondi cette notion, CVS est facile à utiliser même pour les débutants.

24.2.10 Sécurité contre les attaques

Dans le cas idéal, la sécurité contre l'espionnage, voire la modification des données pendant leur transmission, est garantie.

unison comme CVS, rsync ou subversion s'utilisent facilement via ssh (Secure Shell) et sont sécurisés contre les attaques mentionnées ci-dessus. Il est préférable de ne pas faire appel à CVS ou à unison via rsh (Remote Shell) ; de même, les accès par le biais du mécanisme CVS pserver sont à déconseiller dans les réseaux non sécurisés. Grâce à l'utilisation d'Apache subversion offre ici déjà d'origine les mécanismes de sécurité nécessaires.

24.2.11 Sécurité contre la perte de données

Beaucoup d'utilisateurs font appel à CVS depuis longtemps déjà pour gérer leurs projets de logiciels ; il est particulièrement stable. En enregistrant l'historique du

développement, CVS offre même une protection contre certaines erreurs de l'utilisateur (l'effacement accidentel d'un fichier). Bien que subversion ne bénéficie pas encore d'une aussi grande diffusion en comparaison de CVS, on l'emploie déjà en productiion (pour le projet Subversion lui-même).

unison est encore relativement récent, mais offre une grande stabilité. Il est toutefois plus sensible aux erreurs de l'utilisateur. Lorsqu'on en a terminé avec la synchronisation de la procédure d'effacement d'un fichier, celui-ci est irrémédiablement perdu.

TAB. *24.1:* *Fonctionnalités des outils de synchronisation de fichiers -- = très mauvais, - = mauvais et/ou non disponible, o = médiocre, + = bon, ++ = très bon, x = disponible*

	unison	**CVS/subv.**	**rsync**	**mailsync**
Client / Serveur	égale	C-S/C-S	C-S	égale
Portable	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x
Interactif	x	x/x	x	-
Vitesse	-	o/+	+	+
Conflits	o	++/++	o	+
Sél. de fichiers	Répertoire	Sélectionner / Fichier, rép.	Répertoire	Boîte aux lettres
Historique	-	x/x	-	-
Espace disque	o	--	o	+
Interf. util.	+	o/o	-	-
Complexité	+	o/o	+	o
Attaques	+(ssh)	+/+(ssh)	+(ssh)	+(SSL)
Perte de donn.	+	++/++	+	+

24.3 Introduction à unison

24.3.1 Domaines d'application

Unison convient particulièrement à la synchronsation et au transfert de structures de répertoires complets. La synchronisation est bidirectionnelle et contrôlée par une interface graphique (sinon, vous pouvez aussi utiliser la version console). Il est également possible d'automatiser la synchronisation (c'est-à-dire, aucune interaction avec l'utilisateur) si l'on connaît exactement la manipulation.

24.3.2 Conditions requises

Unison doit être installé tant sur le client que sur le serveur ; on entend par serveur le deuxième ordinateur distant (contrairement à CVS, voir la section *CVS* page 593).

Puisque, par la suite, nous devrons nous limiter à l'utilisation d'unison avec ssh, un ssh-Client doit être installé sur le client et un ssh-Server sur le serveur.

24.3.3 Commande

Le principe de base d'Unison est de connecter deux répertoires (appelés "roots"). Cette connexion est de caractère symbolique, il ne s'agit pas d'une connexion en ligne. Supposons que le répertoire soit conçu de la manière suivante :

Client :	`/home/tux/rep1`
Serveur :	`/home/geeko/rep2`

Ces deux répertoires doivent être synchronisés. Sur le client, l'utilisateur est connu en tant que tandis que sur le serveur il est connu en tant que `geeko`. On veut d'abord tester si la comunication entre le client et le serveur fonctionne :

```
unison -testserver /home//rep1 ssh://geeko@server//homes/geeko/rep2
```

Voici les problèmes qui peuvent fréquemment survenir à ce moment :

- les versions d'unison utilisées sur le client et le serveur ne sont pas compatibles

- le serveur ne permet aucune connexion SSH
- aucun des deux chemins d'accès indiqués n'existe

Si tout se déroule bien, on supprime l'option `-testserver`. Lors de la synchronisation initiale, unison ne connaît pas encore la relation entre les deux répertoires et propose donc le sens de transfert des différents fichiers et répertoires. Les flèches de la colonne Action indiquent le sens de transfert. Un ? signifie qu'unison ne peut pas faire de proposition concernant le sens du transfert puisque les deux versions ont été modifiées entre-temps ou sont nouvelles.

Le sens de transfert de chaque enregistrement peut être réglé avec les touches fléchées. Si les sens de transfert de tous les enregistrements indiqués sont corrects, cliquez sur 'Go'.

Le comportement d'unison (si la synchronisation s'effectue automatiquement dans des cas sans équivoque) peut être contrôlé au démarrage par les paramètres de ligne de commande. Vous trouverez une liste complète de tous les paramètres dans `unison -help`.

Pour chaque liaison, la synchronisation est consignée dans le répertoire utilisateur `~/.unison`. Dans ce répertoire, il est possible de noter des jeux de configuration, `~/.unison/example.prefs`:

Exemple 24.1: *Le fichier /.unison/example.prefs*

```
root=/home/foobar/rep1
root=ssh://fbar@server//homes/fbar/rep2
batch=true
```

Pour lancer la synchronisation, il suffit tout simplement d'indiquer le fichier comme argument de ligne de commande : `unison example.prefs`

24.3.4 Documents permettant d'approfondir

La documentation officielle relative à unison est assez volumineuse ; cette section ne fournit qu'une brève introduction. Un manuel complet est disponible à l'adresse `http://www.cis.upenn.edu/~bcpierce/unison/` et dans le paquetage `unison` de SUSE.

24.4 Introduction à CVS

24.4.1 Domaines d'application

CVS est adapté à la synchronisation s'il s'agit de fichiers individuels fréquemment utilisés et dont le format est un format de fichier comme texte ASCII ou texte source de programme. L'utilisation de CVS pour la synchronisation de fichiers ayant un autre format (fichiers JPEG) est possible, mais conduit très vite à de grandes quantités de données puisque chaque variante d'un fichier est stockée en permanence sur le serveur CVS. En plus, dans ce type de cas, la plupart des possibilités offertes par CVS ne sont pas utilisées.

L'utilisation de CVS pour synchroniser des fichiers n'est possible que si tous les ordinateurs du lieu de travail ont accès au même serveur.

Au contraire, le logiciel unison permet le scénario suivant :

A > B > C > S

A, B et C sont les ordinateurs qui sont à même de traiter les données concernées.

24.4.2 Configuration d'un serveur CVS

Le serveur est le lieu où se trouvent tous les fichiers valables, notamment la version actuelle de chaque fichier. Le serveur peut être un ordinateur de bureau fixe. Il est souhaitable que les données du serveur CVS soient régulièrement intégrées dans un backup.

Une méthode intelligente pour créer un serveur CVS consiste à permettre à l'utilisateur d'accéder au serveur via SSH. Ainsi, un ordinateur de bureau fixe peut servir de serveur.

Si, sur ce serveur, l'utilisateur est connu comme et si le logiciel CVS est installé et sur le serveur et sur le client (ordinateur portable), il faut veiller du côté du client que les variables d'environnement suivantes soient configurées :

```
CVS_RSH=ssh CVSROOT=@server:/repserveur
```

Avec la commande `cvs init`, le serveur CVS est ensuite initialisable du côté du client (ne doit être effectué qu'une seule fois).

Enfin, il faut déterminer un nom pour la synchronisation. Choisissez ou créez sur un client un répertoire ne contenant que des données qui seront administrées

par CVS (il peut aussi être vide). Le nom du répertoire ne joue aucun rôle et sera, dans l'exemple présent, `synchome`. Changez de répertoire. Pour mettre le nom de la synchronisation dans `synchome`, entrez ce qui suit :

```
cvs import synchome tux tux_0
```

Remarque : Beaucoup de commandes de CVS requièrent un commentaire. A cet effet, CVS appelle un éditeur (celui qui est défini dans la variable d'environnement `$EDITOR`, sinon vi). On peut éviter d'appeler un éditeur en entrant la commande sur la ligne de commande, comme dans

```
cvs import -m 'ceci est un Test' synchome  tux tux_0
```

24.4.3 Utilisation de CVS

A partir de ce moment, il est possible de "récupérer" (*checkout*) le référentiel de synchronisation (*repository*) depuis un ordinateur quelconque :

```
cvs co synchome
```

Il en résulte un nouveau sous-répertoire `synchome` sur le client. Si vous réalisez des modifications que vous voulez transmettre au serveur, entrez dans le répertoire `synchome` (ou dans un des ses sous-répertoires) et saisissez la commande suivante :

```
cvs commit
```

Cela provoque, par défaut, la transmission au serveur de tous les fichiers se trouvent en-dessous du répertoire actuel et appartenant au CVS local. Si on ne souhaite transmettre que des fichiers ou répertoires individuels, il faut les indiquer :

```
cvs commit fichier1 ... répertoire1 ...
```

Avant leur transmission au serveur, il faut indiquer que les nouveaux fichiers /répertoires appartiennent à CVS :

```
cvs add fichier1 ... répertoire1 ...
```

et ensuite les transmettre

```
cvs commit fichier1 ... répertoire1 ...
```

Pour changer maintenant de poste de travail, il faut, au cas où cela n'a pas encore été fait lors des sessions précédentes sur le même poste de travail, le "mettre à jour" (*update*) par rapport au référentiel de synchronisation. La synchronisation avec le serveur est lancée par la commande :

```
cvs update
```

Il est également possible de choisir les fichiers /répertoires à actualiser :

```
cvs update fichier1 ... répertoire1 ...
```

Si on veut voir à l'avance les différences par rapport aux versions enregistrées sur le serveur, cela est possible grâce à la commande `cvs diff` ou explicitement par :

```
cvs diff fichier1 ... répertoire1 ...
```

Il est aussi possible de faire afficher les fichiers qui seront concernés par une mise à jour : `cvs -nq update` . Lors d'une mise à jour, les symboles d'état suivants sont (entre autres) utilisés :

U La version locale a été mise à jour. Cela concerne tous les fichiers mis à disposition par le serveur, mais qui n'existaient pas localement.

M La version locale a été modifiée. Si les modifications de la version ont eu lieu sur le serveur, les modifications ont pu être également exécutées localement.

P La version locale a été mise à jour à l'aide d'un correctif.

? Ce fichier n'est pas présent dans CVS.

L'état `M` marque les fichiers actuellement corrigés. Pour renvoyer les modifications au serveur, exécutez la commande `cvs commit`. Si en revanche vous préférez renoncer aux modifications que vous venez d'apporter et reprendre l'état actuel du serveur, enlevez la copie locale et réalisez ensuite un update. Le fichier manquant est ensuite repris par le serveur.

Si le même fichier a été modifié au même endroit par plusieurs utilisateurs, un problème se pose parce que CVS n'est plus à même de décider quelle version il faudra utiliser. Lors d'une mise à jour, ce cas de figure est marqué par le symbole `C`. Plusieurs procédures sont possibles pour résoudre le conflit. On entre dans le fichier correspondant aux endroits concernés des marques de conflits qui sont modifiables manuellement. Il est recommandé pour les débutants de se servir d'un programme auxiliaire, comme cervisia. Sinon, il est également possible de changer le nom du fichier propre et de réaliser une nouvelle mise à jour. Une fois les modifications terminées dans le fichier actuel, il convient de les transmettre au serveur par la commande `cvs commit`, ce qui réduit la probabilité d'un conflit.

24.4.4 Documents permettant d'approfondir

Les possibilités de CVS sont très étendues, et on n'a pu ici vous en donner qu'une toute petite idée. Vous trouverez une documentation plus détaillée p.ex. à l'adresse `http://www.cvshome.org/` et `http://www.gnu.org/manual/`.

24.5 Introduction à Subversion

24.5.1 Domaines d'application

Subversion est un système de contrôle de versions Open Source gratuit et souvent considéré comme le successeur de CVS. Par conséquent, les propriétés déjà présentées de CVS s'appliquent aussi en grande partie à subversion. Il présente de l'intére surtout si l'on souhaite bénéficier des avantages de CVS sans avoir à en subir les inconvénients. Beaucoup de ces qualités ont déjà été présentées dans les grandes lignes dans la section *subversion* page 593.

24.5.2 Configuration d'un serveur Subversion

La configuration d'un référentiel sur un serveur est une procédure assez simple. Pour cela, subversion met à disposition un outil d'admnistration propre, `svnadmin`. Pour installer un nouveau référentiel, saisissez :

```
svnadmin create /chemin/vers/le/referentiel
```

D'autres options sont disponibles via `svnadmin help`. Contrairement à CVS, subversion n'utilise pas RCS comme base de données, mais la base de données de Berkeley. Veillez à ne *pas* placer de référentiel sur des systèmes de fichiers distants comme NFS, AFS ou Windows SMB. La base de données nécessite les mécanismes de verrouillage POSIX que les systèmes mentionnés ci-dessus n'offrent pas.

Pour examiner le contenu d'un référentiel existant, utilisez la commande `svnlook` :

```
svnlook info /chemin/vers/le/referentiel
```

Pour que d'autres utilisateurs puissent accéder au référentiel, un serveur doit être configuré. Dans ce cas, on peut avoir recours au serveur web Apache ou utiliser le propre serveur de subversion, `svnserve`. Dès que `svnserve` tourne, on peut accéder au référentiel à l'aide du schéma `svn://` ou `svn+ssh://` saisi dans une URL. Le fichier de configuration `/etc/svnserve.conf` vous permet d'inscrire des utilisateurs qui doivent s'authentifier à l'invite de `svn`.

La décision pour ou contre l'un ou l'autre dépend de nombreux facteurs. Ici, un coup d'œil à l'ouvrage consacré à subversion s'impose (pour plus d'informations, voir la section *Documents permettant d'approfondir* page 607).

24.5.3 Utilisation

Pour accéder à un référentiel Subversion, il existe la commande `svn` (similaire à `cvs`). Si le serveur est correctement configuré (avec un référentiel correspondant), le contenu peut être indiqué par chaque client comme suit :

```
svn list http://svn.exemple.com/chemin/vers/le/projet
```

ou

```
svn list svn://svn.exemple.com/chemin/vers/le/projet
```

Grâce à la commande `svn checkout` vous pouvez valider un projet existant dans le répertoire actuel (en anglais. *check out*) :

```
svn checkout http://svn.exemple.com/chemin/vers/le/projet \
  nom_du_projet
```

La validation crée un nouveau sous-répertoire avec le `nom_du_projet` dans le client. On peut ainsi mettre en œuvre diverses modifications (ajout, copie, renommage, suppression) :

```
svn add file
svn copy oldfile newfile
svn move oldfile newfile
svn delete file
```

Chacune de ces commandes est applicable non seulement à des fichiers, mais aussi à des répertoires. De plus, subversion peut aussi attribuer ce que l'on appelle des *properties* (propriétés) à un fichier ou à un répertoire :

```
svn propset license GPL foo.txt
```

Dans l'exemple précédent concernant le fichier `foo.txt`, la propriété `license` se voit attribuer la valeur `GPL`. Grâce à `svn proplist`, vous pouvez afficher les propriétés :

```
svn proplist --verbose foo.txt
Properties on 'foo.txt':
  license : GPL
```

Pour publier, mettre à jour le serveur, saisissez :

```
svn commit
```

Pour qu'un autre utilisateur obtienne vos modifications dans son répertoire de travail en cours, il doit procéder à une synchronisation par rapport au serveur à l'aide de la commande suivante :

```
svn update
```

À la différence de CVS, l'état d'un répertoire de travail subversion peut être affiché *sans* avoir à accéder au référentiel :

```
svn status
```

Dans ce cas, les modifications locales sont affichées dans cinq colonnes, la colonne la plus importante étant la première :

- ″ Aucune modification
- **'A'** L'objet est placé en tant qu'ajout
- **'D'** L'objet est placé à fin de suppression
- **'M'** L'objet a été modifié
- **'C'** L'objet est en situation de conflit
- **'I'** L'objet a été ignoré
- **'?'** L'objet n'est pas soumis au contrôle de versions
- **'!'** L'objet est manquant. Ce marquage apparaît si la commande `svn` a été supprimée ou déplacée.
- ' ' L'objet a été pris en charge comme fichier bien qu'il ait été remplacé par un répertoire ou inversement.

La deuxième colonne indique l'état à partir des propriétés (ce que l'on appelle *properties*). Toutes les autres colonnes sont consultables dans l'ouvrage consacré à Subversion (voir prochaine section).

Si jamais vous ne savez plus les paramètres exacts d'une commande, `svn help` vous offre une aide supplémentaire :

```
svn help proplist
proplist (plist, pl): List all properties on files, dirs, or revisions.
usage: 1. proplist [PATH...]
       2. proplist --revprop -r REV [URL]

  1. Lists versioned props in working copy.
  2. Lists unversioned remote props on repos revision.
...
```

24.5.4 Documents permettant d'approfondir

Le premier point est la page d'accueil de subversion, sur le site `http://subversion.tigris.org`. Après l'installation du paquetage `subversion-doc`, vous trouvez un livre en langue anglaise très intéressant et complet dans le répertoire `file:///usr/share/doc/packages/subversion/html/book.html`. Cet ouvrage est également disponible en ligne à l'adresse `http://svnbook.red-bean.com/svnbook/index.html`.

24.6 Introduction à rsync

24.6.1 Domaine d'application

rsync s'impose toujours quand il s'agit de transférer régulièrement de grandes quantités de données qui ne changent pas de façon trop considérable. C'est fréquemment le cas lorsqu'on met en place une sauvegarde par exemple.

Un autre domaine d'application est ce que l'on appelle le *staging server* (serveur étape), donc le serveur qui contient par exemple l'arborescence complète d'un serveur web et qui est mis en miroir régulièrement sur le véritable serveur web.

24.6.2 Configuration et utilisation

On peut utiliser rsync dans deux modes différents. D'une part, rsync peut archiver ou copier des fichiers. Pour cela, il suffit de faire appel à un shell distant comme par exemple ssh, sur l'ordinateur cible. Cependant, rsync peut aussi se servir du `Démon` et mettre à disposition les répertoires dans le réseau.

L'utilisation principale de rsync n'exige aucune configuration particulière. Grâce à rsync, il est possible de mettre directement en miroir des répertoires complets sur un autre ordinateur. Par exemple, à l'aide de la commande suivante, on peut placer une sauvegarde du répertoire natif de sur un serveur soleil de sauvegarde :

```
rsync -baz -e ssh /home/tux/ tux@soleil:backup
```

Pour restaurer le répertoire, utilisez la commande suivante :

```
rsync -az -e ssh tux@soleil:backup /home/tux/
```

Ici, l'utilisation se différencie à peine d'un programme normal de copie comme scp

Afin que rsync puisse exploiter pleinement ses fonctionnalités, il faudra l'utiliser en mode "rsync". Pour ce faire le démon rsyncd est démarré sur un des ordinateurs. Dans ce cas, rsync doit être configuré sur le fichier `/etc/rsyncd.conf`. Si par exemple, il s'agit d'accéder au répertoire `/srv/ftp` via rsync, il est possible de faire appel au fichier de configuration suivant :

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
        path = /srv/ftp
        comment = An Example
```

Le démon rsyncd doit ensuite être démarré :

```
rcrsyncd start
```

Le démon rsyncd peut aussi être démarré automatiquement lors du processus d'amorçage. Pour cela, il faut soit activer ce service dans YaST dans l'éditeur de niveau d'exécution, soit saisir manuellement la commande `insserv rsyncd`.

À titre d'alternative, il est également possible de démarrer rsyncd à partir de xinetd. Ce n'est toutefois recommandé que pour les serveurs sur lesquels le rsyncd n'est pas trop souvent sollicité. Dans l'exemple ci-dessus, un fichier journal est également prévu sur toutes les connexions. Celui-ci est enregistré dans `/var/log/rsyncd.log`.

Maintenant, le transfert peut être mis au point depuis un ordinateur client. Cette opération a lieu à l'aide de la commande suivante :

```
rsync -avz soleil::FTP
```

Cette commande permet de répertorier tous les fichiers présents sur le serveur dans le répertoire `/srv/ftp`. Cette requête apparaît aussi dans le fichier journal enegistré dans `/var/log/rsyncd.log`. Pour démarrer le transfert de façon effective, il fautencore indiquer un répertoire cible. Pour le répertoire actuel, il peut également s'agir du ".", donc par exemple :

```
rsync -avz soleil::FTP .
```

Si le rsyncd doit toujours être appelé sur le serveur, on prendra soin de saisir deux caractères ":" entre le nom du serveur et le périphérique cible.

24.6.3 Problèmes éventuels

Par défaut, aucun fichier n'est supprimé lors de la synchonisation avec rsync. Lorsque la suppression doit être imposée, il faut indiquer l'option `--delete` en sus.

Pour garantir qu'aucun fichier récent fichier n'est écrasé, on peut indiquer l'option `--update`. Ainsi, les conflits qui en résultent doivent être résolus manuellement.

24.6.4 Documents permettant d'approfondir

Vous trouverez des informations importantes sur rsync dans les pages de manuel `man rsync` et `man rsyncd.conf`.

Vous trouverez de la documentation technique sur le fonctionnement de rsync dans `/usr/share/doc/packages/rsync/tech_report.ps`

Pour vous tenir informé sur rsync, vous pouvez consulter le site web du projet à l'adresse `http://rsync.samba.org`.

24.7 Introduction à mailsync

24.7.1 Domaine d'application

En principe, Mailsync s'utilise pour trois tâches :

- La synchronisation d'emails enregistrés localement avec des emails enregistrés sur un serveur.
- La migration de boîtes aux lettres dans un format différent ou vers un autre serveur.
- Le contrôle de l'intégrité d'une boîte aux lettres ou la recherche de doublettes.

24.7.2 Configuration et utilisation

Mailsync fait la distinction entre la boîte aux lettres elle-même (appelée Store) et la liaison entre deux boîtes aux lettres (appelée channel). Les définitions de stores et de channels sont enregistrées dans le fichier `~/.mailsync`. Vous trouverez ci-dessous la présentation de quelques exemples de stores. Voici une définition simple :

```
store saved-messages {
   pat     Mail/saved-messages
   prefix  Mail/
}
```

`Mail/` est un sous-répertoire dans le répertoire personnel (/home) de l'utilisateur qui contient des dossiers de courrier électronique, dont entre autres le dossier `saved-messages`. En appelant `mailsync` via la commande `mailsync -m saved-messages`, vous obtenez un index de tous les messages contenus dans saved-messages. Voici à quoi pourrait ressembler une autre définition :

```
store localdir {
   pat     Mail/*
   prefix  Mail/
}
```

Ici, l'appel de `mailsync -m localdir` fait apparaître une liste de tous les messages qui sont enregistrés dans les dossiers sous `Mail/`. L'appel de `mailsync localdir` affiche en revanche une liste des noms des dossiers.

On spécifie un store sur un serveur IMAP ainsi :

```
store imapinbox {
   server  {mail.uni-hannover.de/user=gulliver}
   ref     {mail.uni-hannover.de}
   pat     INBOX
}
```

Dans ce cas de figure, seul le dossier principal est adressé sur le serveur IMAP ; un store pour les sous-dossiers ressemble par contre à ceci :

```
store imapdir {
   server  {mail.uni-hannover.de/user=gulliver}
   ref     {mail.uni-hannover.de}
   pat     INBOX.*
   prefix  INBOX.
}
```

Si le serveur IMAP supporte des liaisons codées, il faudra modifier la spécification du serveur comme suit :

```
server {mail.uni-hannover.de/ssl/user=gulliver}
```

ou bien (si le certificat serveur n'est pas connu) à

```
server {mail.uni-hannover.de/ssl/novalidate-cert/user=gulliver}
```

Maintenant, on veut lier les dossiers se trouvant sous `Mail/` avec les sous-répertoires sur le serveur IMAP :

```
channel dossier localdir imapdir {
   msinfo .mailsync.info
}
```

Mailsync se rappelera dans le fichier indiqué avec `msinfo` quels messages ont déjà été synchronisés. Un appel de `mailsync Ordner` a les conséquences suivantes :

- Le type de boîte aux lettres (pat) est élargi des deux côtés.
- Le préfixe (prefix) résultant de chaque nom de dossier est éliminé.
- Les dossiers sont synchronisés (ou crées, s'ils n'existaient pas) par paires.

Un dossier `INBOX.sent-mail` sur le serveur IMAP est donc synchronisé avec le dossier local `Mail/sent-mail` (à condition de répondre aux définitions ci-dessus), la synchronisation entre les différents dossiers fonctionnant de la manière suivante :

- Si un message existe déjà des deux côtés, il ne se passe rien.
- Si le message manque d'un côté et s'il s'agit d'un nouveau message (non consigné dans le fichier msinfo), il y sera transféré.
- Si le message n'existe que d'un côté et s'il s'agit d'un ancien message (déjà consigné dans le fichier msinfo), il y sera effacé (en espérant qu'il existait de l'autre côté et qu'il y a été effacé).

Pour savoir d'avance quels messages seront transmis et lesquels seront effacés lors d'une synchronisation, on appelle mailsync avec un "channel" *et* un "store" en même temps : `mailsync Ordner localdir`.

Il en résulte une liste de tous les messages qui sont localement nouveaux ainsi qu'une liste de tous les messages qui seraient effacés du côté de IMAP lors d'une synchronisation !

On reçoit par `mailsync Ordner imapdir`, de façon inversée, une liste de tous les nouveaux messages du côté de IMAP ainsi qu'une liste de tous les messages qui seraient effacés localement lors d'une synchronisation.

24.7.3 Problèmes éventuels

Dans le cas d'une perte de données, la procédure la plus sûre est d'effacer le fichier de protocole de channel correspondant msinfo. Il en résulte que tous les messages qui n'existent que d'un seul côté sont considérés comme nouveaux et seront transmis lors de la prochaine synchronisation.

Seuls les messages portant un Message-ID sont pris en compte par la synchronisation tandis que ceux n'ayant pas de Message-ID sont tout simplement ignorés, ils ne sont ni transmis ni effacés. Un identificateur de message manquant est normalement le résultat de programmes défectueux dans le processus de remise ou de génération du courrier.

Sur certains serveurs IMAP, le dossier principal est appelé par `INBOX` et les sous-dossiers sont appelés par un nom quelconque (contrairement à INBOX et INBOX.name). C'est la raison pour laquelle des serveurs comme IMAP ne sont pas capables de spécifier exclusivement un modèle pour les sous-dossiers.

Les pilotes de boîtes aux lettres qu'utilise mailsync (c-client) placent, lorsque les messages ont fini d'être transmis sur un serveur, un drapeau d'état spécial, rendant impossible pour certains programmes de messagerie électronique, comme mutt de reconnaître qu'un message est nouveau. Dans le cas de mailsync, l'option `-n` empêche que ce drapeau d'état spécial soit installé.

24.7.4 Documents permettant d'approfondir

Le fichier `README` contenu dans le paquetage mailsync sous le nom de `/usr/share/doc/packages/mailsync/` contient des informations et conseils supplémentaires. Dans ce contexte, le RFC 2076 "Common Internet Message Headers" est particulièrement intéressant.

Samba

Samba permet d'utiliser un ordinateur Unix comme serveur de fichiers ou d'impression pour ordinateurs DOS, Windows et OS/2. Ce chapitre vous introduit aux principes de la configuration Samba et décrit les modules de YaST avec lesquels vous pouvez configurer Samba dans votre réseau.

Aujourd'hui, Samba est devenu un produit extrêmement complet. De ce fait, nous pourrons donner ici uniquement un premier aperçu de ses fonctionnalités. Cependant, vous trouverez des détails dans la documentation numérique qui l'accompagne. Celle-ci est constituée, pour une part, de pages de manuel — pour vous faire une idée du volume, exécutez la commande `apropos samba` — et, pour le reste, de documents et d'exemples que vous trouverez, après avoir installé Samba sur votre système, dans le répertoire `/usr/share/doc/packages/samba`. Vous y trouverez également, dans le sous-répertoire `examples` l'exemple de configuration commenté `smb.conf.SuSE`.

Vous disposez du paquetage `samba` dans sa version 3. Voici quelques-unes des nouveautés notables de ce paquetage :

- Prise en charge d'Active Directory.
- La prise en charge d'Unicode a été considérablement améliorée.
- Les mécanismes d'authentification internes ont complètement été remaniés.
- Meilleure prise en charge du système d'impression Windows 200x/XP.
- Configuration en tant que serveur membre (en anglais, *member server*) de domaines Active Directory.
- Reprise des domaines NT4 pour migrer d'un domaine NT4 vers un domaine Samba.

Remarque

Migration vers Samba3

Si vous souhaitez migrer de Samba 2.x vers Samba 3, vous devez veiller à certaines particularités. Un chapitre complet est consacré à ce sujet dans l'ensemble des HOWTO relatifs à Samba. Une fois le paquetage `samba-doc` installé, vous trouverez le HOWTO sous `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

Remarque

Samba utilise le protocole SMB (Server Message Block) qui est basé sur les services NetBIOS. Suite aux pressions de la société IBM, Microsoft a publié le protocole, ce qui a permis à d'autres éditeurs de logiciels de se connecter également à un domaine Microsoft. Samba fait s'appuyer SMB sur le protocole TCP/IP. En conséquence, le protocole TCP/IP doit être installé sur tous les clients. Nous recommandons d'utiliser exclusivement TCP/IP sur les clients.

NetBIOS est une interface logicielle (API) conçue afin de permettre à différents ordinateurs de communiquer entre eux. C'est dans ce contexte qu'a été conçu un service de nommage (*name service*) destiné à permettre l'identification mutuelle des machines. En matière de nommage, il n'existe aucune instance centrale qui serait chargée d'attribuer ou de vérifier les droits. Toute machine sur le réseau peut réserver un nombre quelconque de noms, pour autant qu'ils ne soient pas encore attribués. L'interface NetBIOS peut être implémentée sur différentes architectures réseau. Une implémentation relativement "proche" du matériel réseau porte le nom NetBEUI. NetBEUI est fréquemment désigné sous le nom NetBIOS. Les protocoles réseau par-dessus lesquels NetBIOS a été implémenté sont IPX (NetBIOS sur TCP/IP) de Novell et TCP/IP.

Les noms NetBIOS qui sont également attribués dans l'implémentation de NetBIOS sur TCP/IP n'ont rien à voir avec les noms attribués dans le fichier `/etc/host` ou par DNS. NetBIOS définit un espace de nommage complètement à part. Malgré cela, il est recommandé, afin de simplifier l'administration, d'attribuer au moins aux serveurs des noms NetBIOS correspondant à leurs noms d'hôtes DNS. C'est réglé ainsi par défaut dans les serveurs Samba.

Tous les systèmes d'exploitation majeurs tels que Mac OS X, Windows et OS/2 prennent en charge le protocole SMB. Le protocole TCP/IP doit être installé à cet effet. S'agissant des différents UNIX, Samba offre également un client. Linux comporte en outre un module noyau offrant un système de fichiers SMB, permettant d'intégrer des ressources SMB au niveau du système Linux.

Les serveurs SMB offrent aux clients de l'espace disque se présentant sous la forme de "partages" (*shares*). Un partage correspond à un répertoire et à tous ses sous-répertoires sur le serveur. Il est exporté sous son propre nom et des clients peuvent y accéder sous ce même nom. Le nom du partage peut être choisi librement, mais il ne peut pas être identique à celui du répertoire exporté. De la même manière, une imprimante exportée se voit attribuer un nom qui sera utilisé par les clients pour y accéder.

25.1 Configuration du serveur

Dans le cas où vous souhaitez utiliser Samba en tant que serveur, installez le paquetage `samba`. Démarrez les services requis pour Samba à l'aide de la commande `rcnmb start & & rcsmb start` et arrêtez-les à l'aide de la commande `rcsmb stop & & rcnmb stop`.

Le fichier de configuration central de Samba est `/etc/samba/smb.conf`. Ce fichier comporte deux parties logiques distinctes. La section `[global]` comporte la définition des paramètres globaux. La seconde section, intitulée `[share]`, comporte la définition des différents partages de fichiers et d'imprimantes. Ce mode d'organisation permet de définir les détails des partages soit de manière différenciée, soit avec une portée globale dans la section `[global]`. Le fichier de configuration gagne ainsi en lisibilité.

25.1.1 Section global de la configuration donnée en exemple

Les directives suivantes de la section `global` doivent être adaptées en fonction de la configuration de votre réseau afin de permettre à d'autres systèmes d'accéder à votre serveur Samba dans un réseau Windows au moyen de SMB.

workgroup = TUX-NET Le serveur Samba est rattaché à un groupe de travail à l'aide de cette ligne. Remplacez `TUX-NET` par votre groupe de travail ou configurez vos clients avec la valeur choisie ici. Votre serveur Samba est visible dans cette configuration avec son nom DNS dans le groupe de travail choisi, pour autant que le nom choisi n'ait pas encore été attribué.

Dans le cas où le nom a déjà été attribué, il peut être défini avec `netbios name = MONNOM`, et être différent du nom DNS. Pour obtenir plus de précisions sur cette directive, exécutez la commande `man smb.conf`.

os level = 2 Grâce à cette directive, votre serveur Samba décide s'il doit essayer de faire office d'explorateur maître local (LMB, *Local Master Browser*) pour son groupe de travail. La valeur utilisée dans notre exemple est volontairement faible afin d'éviter qu'un réseau Windows ne soit perturbé par un serveur Samba mal configuré. Pour plus de précisions sur cette question importante, reportez-vous aux fichiers `BROWSING.txt` et `BROWSING-Config.txt` dans le sous-répertoire `textdocs` de la documentation du paquetage.

En l'absence de serveur SMB préexistant — par exemple Windows NT ou 2000 Server —, lorsque c'est le serveur Samba qui fixe le nom des systèmes disponibles dans le réseau local, augmentez la valeur `os level` (par exemple à 65) afin de l'emporter dans l'élection pour la fonction de LMB.

Dans le cas où cette valeur est modifiée, vous devez être particulièrement prudent en raison des risques de dysfonctionnement auquel vous exposez un réseau Windows existant. Testez les modifications dans un premier temps dans un réseau isolé ou pendant une période non critique.

Prise en charge WINS et serveur WINS
Si vous avez l'intention d'intégrer le serveur Samba au sein d'un réseau Windows existant comportant déjà un serveur WINS, vous devez utiliser le paramètre `wins server` en supprimant le point-virgule et en ajustant l'adresse IP en fonction de votre situation.

Si vos systèmes Windows sont utilisés dans des sous-réseaux séparés mais doivent se voir les uns les autres, vous avez besoin d'un serveur WINS. Pour que votre serveur Samba fasse office de serveur WINS, il convient de déclarer `wins support = Yes`. Assurez-vous absolument que vous n'avez utilisé cette directive que pour un seul serveur Samba.

Les deux options `wins server` et `wins support` ne doivent jamais être activées ensemble dans votre fichier smb.conf.

25.1.2 Partages

Dans les exemples qui suivent, le lecteur de cédéroms d'une part, ainsi que les répertoires personnels des utilisateurs `homes` des clients SMB d'autre part, sont partagés.

[cdrom] Pour éviter qu'un cédérom ne soit partagé par inadvertance, toutes les lignes requises de ce partage sont désactivées à l'aide de mises en commentaires – des points-virgules, en l'occurrence –. Dans le cas où vous voulez partager le lecteur de cédéroms avec Samba, il vous suffit de supprimer les points-virgules de la première colonne.

Exemple 25.1: *Partage de cédéroms*

```
;[cdrom]
;      comment = CD-ROM Linux
;       path = /media/cdrom
;       locking = No
```

`[cdrom]` et `comment` La ligne `[cdrom]` est le nom du partage visible par les clients SMB. La directive `comment` permet d'offrir aux clients une description du partage.

`path = /media/cdrom` La directive `path` permet d'exporter le répertoire `/media/cdrom`.

Ce type de partage est uniquement disponible pour les utilisateurs présents sur le système, en raison de paramètres par défaut volontairement restrictifs. Dans le cas où tout le monde doit pouvoir accéder au partage, il convient d'ajouter la ligne `guest ok = Yes`. Compte tenu de la possibilité offerte à tous les utilisateurs de lire les données, la plus grande prudence est de mise avec cette directive, qui devrait être réservée uniquement à quelques partages choisis. La section `[global]` impose d'être particulièrement prudent.

[homes] Le partage `[homes]` est particulièrement important. Dans le cas où l'utilisateur possède un compte valide et son propre répertoire personnel sur le serveur de fichiers Linux, son client peut se connecter sur ce compte en fournissant un identifiant utilisateur et un mot de passe valides.

Exemple 25.2: *Partage "homes"*

```
[homes]
        comment = Home Directories
        valid users = %S
        browseable = No
        read only = No
        create mask = 0640
        directory mask = 0750
```

`[homes]` En l'absence de partage explicite avec le nom de partage de l'utilisateur qui souhaite se connecter, un partage dynamique est créé, en raison du partage `[homes]`. Le nom du partage est le même que celui de l'utilisateur.

`valid users = %S` Après établissement de la connexion, le `%S` est remplacé par le nom de partage réel. Comme celui-ci est toujours identique au nom d'utilisateur dans le cas du partage `[homes]`, les utilisateurs autorisés sont uniquement le propriétaire du répertoire de l'utilisateur. Cette possibilité vise à n'autoriser l'accès qu'au propriétaire.

`browseable = No` Cette directive masque le partage `[homes]` dans la liste des partages.

`read only = No` Dans sa configuration par défaut, Samba interdit l'accès en écriture aux partages exportés, `read only = Yes`. Ainsi, si vous voulez partager un répertoire en écriture, vous devez choisir la valeur `read only = No`. Ce paramétrage est équivalent à `writeable = Yes`.

`create mask = 0640` Les systèmes qui ne sont pas basés sur Windows NT ne connaissent pas le système des privilèges d'accès Unix. De ce fait, il n'est pas possible, en créant des fichiers, de définir les privilèges d'accès à appliquer. La directive `create mask` définit les privilèges d'accès à associer aux fichiers à créer. Cette fonctionnalité n'est disponible que pour les partages auxquels on accède en écriture. Ici, cela signifie concrètement que le propriétaire dispose des droits en lecture et écriture et que les membres du groupe primaire disposent des droits en lecture. À noter que `valid users = %S` interdit l'accès en lecture même lorsque le groupe dispose des droits en écriture. Ainsi, pour accorder l'accès en lecture/écriture au groupe, la ligne `valid users = %S` doit être désactivée.

25.1.3 Security Level

Le protocole SMB, issu du monde DOS/Windows, se préoccupe directement des problèmes de sécurité. Tout accès à un partage peut être protégé par mot de passe. SMB autorise trois modes de contrôle d'autorisations.

Sécurité au niveau du partage (security = share) :
Dans la sécurité au niveau du partage, un mot de passe est attribué à un partage. Tous ceux qui connaissent ce mot de passe ont accès au partage.

Sécurité au niveau de l'utilisateur (security = user) :
Cette variante introduit le concept de l'utilisateur dans SMB. Chaque utilisateur doit se connecter sur le serveur à l'aide d'un mot de passe. Après la phase d'authentification, le serveur peut ensuite offrir l'accès aux différents partages exportés en fonction du nom d'utilisateur indiqué.

Sécurité au niveau du serveur (security = server) :
Vis-à-vis des clients, Samba affirme travailler en mode sécurité au niveau de l'utilisateur. Il transmet cependant toutes les demandes de mot de passe à un autre serveur en mode sécurité au niveau de l'utilisateur qui assure l'authentification. Cette configuration prévoit une directive supplémentaire (`password server =`).

La distinction entre sécurité au niveau du partage, de l'utilisateur et du serveur s'applique au serveur dans son ensemble. Il n'est pas possible d'exporter certains partages d'un serveur configuré pour utiliser la sécurité au niveau du partage et d'autres en utilisant la sécurité au niveau de l'utilisateur. Vous pouvez toutefois exploiter sur un système un serveur Samba différent pour chaque adresse IP configurée.

Pour plus de précisions sur ce sujet, veuillez consulter l'ensemble des HOWTO relatifs à Samba. Si votre système comporte plusieurs serveurs, les paramètres `interfaces` et `bind interfaces only` vous concernent.

Remarque

L'administration du serveur Samba peut être simplifiée à l'aide du programme swat. Celui-ci comporte une interface Web simple permettant de configurer aisément le serveur Samba. Appelez dans un navigateur Web l'adresse `http://localhost:901` et connectez-vous en tant qu'utilisateur root. Il convient de noter que swat est également activé dans les fichiers `/etc/xinetd.d/samba` et `/etc/services`. Vous devez pour cela modifier dans `/etc/xinetd.d/samba` la ligne suivante : `disable = no`. Pour plus d'informations sur swat, reportez-vous à la page de manuel de swat.

Remarque

25.2 Samba en tant que serveur d'authentification

Dans les réseaux comportant essentiellement des clients Windows, il est généralement souhaitable de permettre uniquement aux utilisateurs disposant d'un compte et d'un mot de passe valides de se connecter. On peut offrir cette fonctionnalité à l'aide d'un serveur Samba. Dans un serveur basé sur Windows, cette fonction est assurée par le serveur Windows NT qui est configuré comme contrôleur de domaine primaire (*Primary Domain Controller* ou PDC). Les lignes correspondantes doivent être ajoutées à la section `[global]` de `smb.conf`, comme indiqué dans l'exemple 25.3 page suivante.

Exemple 25.3: *Section "global" dans smb.conf*

```
[global]
        workgroup = TUX-NET
        domain logons = Yes
        domain master = Yes
```

Lorsque des mots de passe chiffrés sont utilisés pour la vérification – ce qui est la règle dans les versions plus abouties de Windows 9x, Windows NT 4.0 service pack 3 et suivants, et dans tous les systèmes plus récents – le serveur Samba doit être en mesure de gérer cette fonctionnalité. C'est le rôle de la ligne `encrypt passwords = yes` dans la section `[global]` ; option spécifiée par défaut, à partir de la version 3 de samba. Parallèlement, les comptes utilisateur ou les mots de passe doivent être chiffrés en utilisant une méthode de chiffrement conforme à Windows. L'opération est réalisée à l'aide de la commande `smbpasswd -a nom`. Dans la philosophie Windows des domaines NT, les machines elles-mêmes ont besoin d'un compte de domaine. Celui-ci est créé à l'aide des commandes suivantes :

Exemple 25.4: *Création d'un compte de machine*

```
useradd nommachine\$
smbpasswd -a -m nommachine
```

Un signe dollar a été ajouté dans la commande `useradd`. La commande `smbpasswd` l'ajoute elle-même lorsqu'on utilise le paramètre `-m`.

Dans la configuration `/usr/share/doc/packages/samba/examples/smb.conf.SuSE`, qui nous sert d'exemple, certaines directives permettant d'automatiser ces opérations ont été prévues.

Exemple 25.5: *Création automatique d'un compte de machine*

```
add machine script = /usr/sbin/useradd -g nogroup -c \
"NT Machine Account" -s /bin/false %m\$
```

Pour que ce script puisse être correctement exécuté par Samba, vous avez encore besoin d'un utilisateur Samba détenant les droits d'administrateur. Ajoutez pour ce faire le groupe `ntadmin` à l'utilisateur souhaité. Vous pouvez alors ajouter tous les utilisateurs de ce groupe Unix au "Domain Admins" à l'aide de la commande suivante :

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Vous trouverez davantage d'informations à ce sujet dans l'ensemble des HOWTO relatifs à Samba, dans le chapitre 12: `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

25.3 Configuration du serveur Samba avec YaST

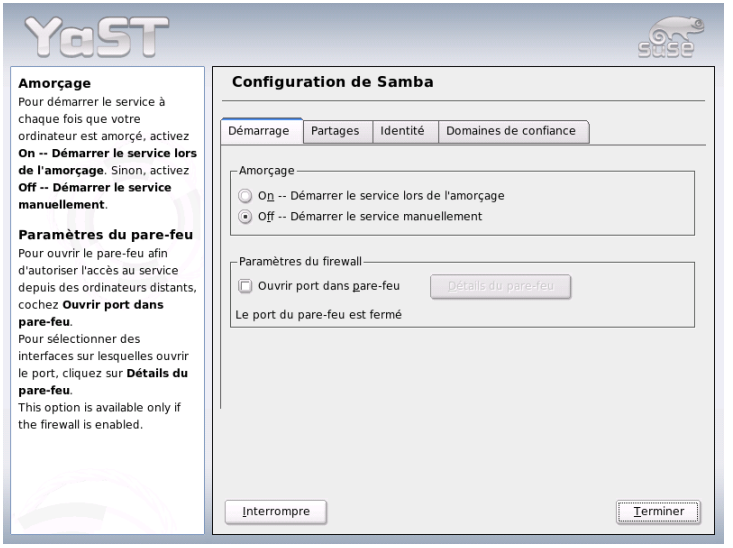


FIG. 25.1: *Configuration de Samba -- Démarrage*

Dans le menu ‘Démarrer’ (figure 25.1 page ci-contre), activez Samba. Le service sera alors démarré à chaque amorçage du système. À l’aide de la case à cocher ‘Ouvrir ports dans le pare-feu’ et le menu contextuel ‘Détails du pare-feu’, configurez automatiquement le pare-feu fonctionnant sur le serveur de façon à ce que sur toutes les interfaces (externes et internes) les ports pour les services `netbios-ns`, `netbios-dgm`, `netbios-ssn` et `microsoft-ds` soient ouverts et permettent un fonctionnement sans problèmes du serveur Samba.

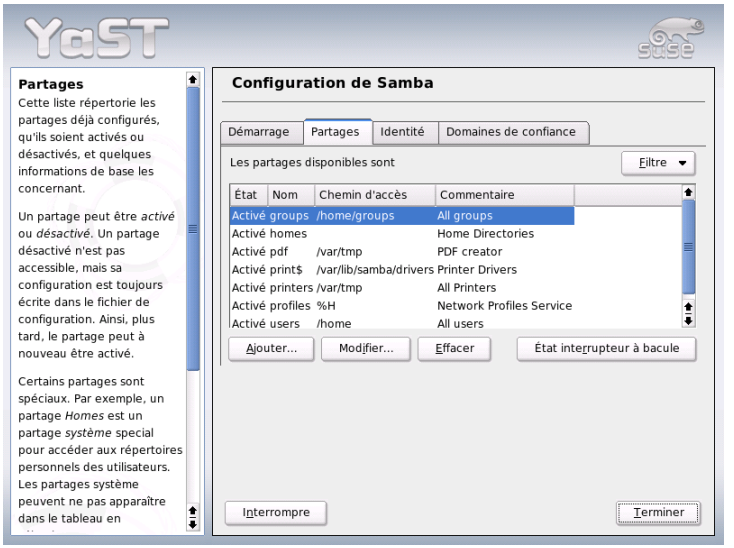


FIG. 25.2: *Configuration Samba -- partages*

Dans le menu ‘Paratages’ (figure 25.2), définissez quels partages Samba doivent être activés. Le bouton ‘Changer l’état’ permet de passer de l’état ‘actif’ à ‘inactif’ et vice-versa. Ajoutez de nouveaux partages avec ‘Ajouter’.

Dans le menu ‘Identité’ (figure 25.3 page suivante), définissez à quel domaine l’odinateur appartient (‘Configuration de base’) et si vous souhaitez un nom d’ordinateur alternatif dans le réseau (‘Nom NetBIOS’).

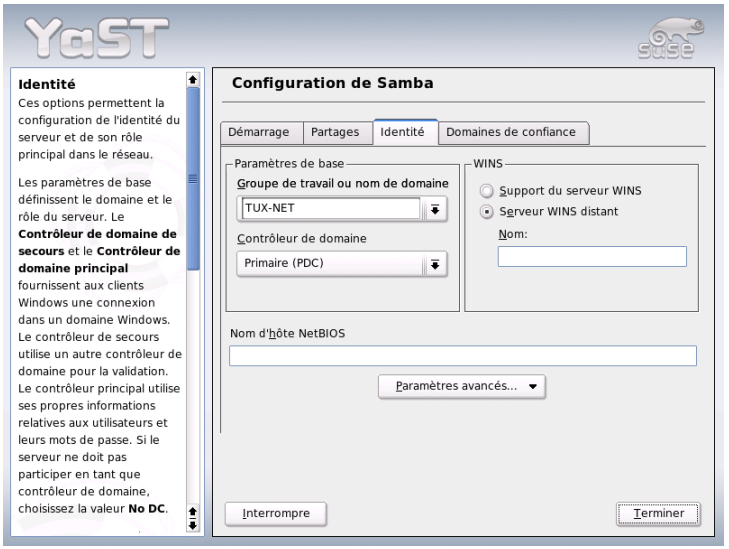


FIG. 25.3: *Configuration Samba -- identité*

25.4 Configuration des clients

Les clients ne peuvent accéder au serveur Samba que par TCP/IP. Les protocoles NetBUI ou NetBIOS par-dessus IPX ne peuvent pas être utilisés avec Samba.

25.4.1 Configuration d'un client Samba avec YaST

Configurez un client Samba pour accéder simplement aux ressources (fichiers ou imprimantes) disponibles sur le serveur Samba. Entrez, dans le dialogue 'Groupe de travail Samba', le domaine ou le groupe de travail. Dans 'Sélectionner', tous les groupes et domaines disponibles sont affichés. Vous pouvez alors sélectionner d'un clic de souris. Activez la case à cocher 'Utiliser les informations SMB aussi pour l'authentification Linux' et l'authentification des utilisateurs se fera à l'aide du serveur Samba. Lorsque vous avez procédé au réglage de tous les paramètres, cliquez sur 'Terminer' pour achever la configuration.

25.4.2 Windows 9x/ME

Windows 9x/ME prend en charge le protocole TCP/IP. Toutefois, celui-ci n'est pas installé dans l'installation par défaut, comme c'est également le cas avec Windows for Workgroups. Pour installer TCP/IP après l'installation du système, cliquez dans l'applet Réseau du Panneau de configuration. Dans l'onglet 'Configuration', cliquez ensuite sur le bouton 'Ajouter...'. Dans la boîte de dialogue 'Sélection du type de composant réseau' qui s'ouvre alors, sélectionnez le composant réseau 'Protocole' et cliquez sur le bouton 'Ajouter'. dans la boîte de dialogue 'Sélection de : Protocole réseau', choisissez 'Microsoft' dans le volet 'Constructeurs' et 'TCP/IP' dans le volet 'Protocoles réseau'. Après avoir redémarré la machine Windows, vous pouvez trouver le serveur Samba en double-cliquant sur l'icône 'Voisinage réseau' du Bureau.

Remarque

Pour utiliser une imprimante sur un serveur Samba, il convient d'installer le pilote d'imprimante générique ou Apple PostScript correspondant à la version de Windows concernée ; l'idéal est de se connecter avec la file d'impression Linux acceptant le format PostScript en entrée.

Remarque

25.5 Optimisation

Il est possible d'optimiser la configuration avec la directive `socket options`. Les paramètres par défaut de la configuration donnée en exemple s'appliquent à un réseau local Ethernet. Pour plus de détails, veuillez vous reporter à la page de manuel de `smb.conf`, à la section `socket options` ainsi qu'à la page de manuel de `socket(7)`. Pour plus d'informations à ce sujet, reportez-vous dans l'ensemble des HOWTO relatifs à Samba (`Samba-HOWTO-Collection`), au chapitre en anglais `Samba performance tuning` (optimisation des performances de Samba).

La configuration par défaut de `/etc/samba/smb.conf` tente de proposer des valeurs raisonnables, tout en se basant sur les paramètres par défaut de l'équipe Samba. Pour autant, il n'est pas possible de mettre au point d'emblée une configuration toute faite, qu'il s'agisse de la configuration du réseau ou du nom du groupe de travail. Vous trouverez dans le fichier commenté `examples/smb.conf.SuSE` comportant la configuration donnée en exemple de nombreuses informations complémentaires qui vous aideront à ajuster votre configuration en fonction de vos besoins propres.

Remarque

L'équipe Samba propose, dans `Samba-HOWTO-Collection`, une section consacrée à la recherche d'erreurs. La partie V contient en outre une marche à suivre détaillée pour la vérification de la configuration.

Remarque

Internet

Internet s'est imposé dans le monde entier comme plate-forme de communication. Linux, en tant que système d'exploitation réseau, peut prendre en charge de nombreuses tâches sur ce réseau, en tant que client comme en tant que serveur.Dans ce chapitre, nous traiterons quelques sujets intéressants : l'aide à la connexion smpppd (SUSE Meta PPP-Daemon - le méta-démon PPP de SUSE), la configuration manuelle d'un accès ADSL si des problèmes surviennent lors de l'installation avec YaST et la configuration du serveur de proximité Squid.

26.1 Le démon smpppd en tant qu'assistant à la numérotation

26.1.1 Programmes pour la connexion Internet

La plupart des utilisateurs privés n'utilisent pas de connexion continue à l'Internet et ne composent leur numéro de leur fournisseur qu'à la demande. Ce sont les applications ipppd ou pppd qui ont le contrôle sur cette connexion, selon le type de connexion (RNIS ou ADSL). Il suffit normalement de démarrer ces programmes correctement pour être en ligne.

Tant que l'utilisateur dispose d'un tarif forfaitaire qui n'entraîne aucun frais supplémentaire lors de la connexion, il suffit généralement de démarrer le démon de la manière appropriée. On souhaite cependant parfois pouvoir mieux contrôler la connexion, que ce soit à l'aide d'une applet KDE ou d'une interface à base de ligne de commande. En outre, il arrive souvent que la passerelle Internet ne soit pas l'ordinateur de travail même, si bien qu'il faut pouvoir gérer la connexion à un ordinateur connecté au réseau.

C'est à ce niveau qu'intervient smpppd (le méta-démon PPP de SUSE). Il met à la disposition des utilitaires une interface unique qui fonctionne dans deux directions. D'une part, il programme le démon pppd ou ipppd approprié et gère son comportement lors de la connexion. D'autre part, il propose aux programmes utilisateur différents fournisseurs d'accès et donne des informations sur l'état actuel de la connexion. Comme le démon smpppd peut également être géré via le réseau, il est particulièrement bien approprié pour gérer la connexion à l'Internet à partir d'un poste de travail dans le sous-réseau privé.

26.1.2 La configuration du démon smpppd

YaST configure automatiquement les connexions mises à disposition par smpppd.Les programmes de connexion à proprement parler, kinternet et cinternet sont également préconfigurés. Vous devez procéder manuellement lorsque vous souhaitez installer des fonctionnalités supplémentaires de smpppd, comme un service distant, par exemple.

Le fichier de configuration du démon smpppd se trouve dans `/etc/smpppd.conf`. Il est installé par défaut de manière à ce qu'aucun service distant ne soit possible. Les options les plus intéressantes de ce fichier de configuration sont :

open-inet-socket = ⟨*yes* | *no*⟩ Lorsque vous souhaitez pouvoir gérer le démon smpppd via le réseau, vous devez régler cette option à `yes`. Le port que le démon smpppd écoute alors est le port `3185`. Si ce paramètre vaut `yes`, vous devez définir les paramètres `bind-address`, `host-range` et `password` en conséquence.

bind-address = ⟨*ip*⟩ Quand un ordinateur possède plusieurs adresses IP, vous pouvez décider depuis quelles adresses IP le démon smpppd accepte des connexions.

host-range = ⟨*min ip*⟩ ⟨*max ip*⟩ Vous pouvez utiliser le paramètre `host-range` pour définir un intervalle réseau. L'accès au smpppd est alors autorisé aux ordinateurs dont les adresses IP se trouvent dans cet intervalle. Ou pour tourner les choses autrement, tous les ordinateurs ne se trouvant pas dans cet intervalle sont rejetés.

password = ⟨*password*⟩ En donnant un mot de passe, on peut limiter les clients aux ordinateurs autorisés. Comme il s'agit d'un mot de passe en texte clair, il ne faut pas surestimer la sécurité qu'il apporte. Si aucun mot de passe n'est attribué, tous les clients sont alors autorisés à accéder au démon smpppd.

slp-register = ⟨*yes* | *no*⟩ Avec ce paramètre, le service du démon smpppd peut être annoncé dans le réseau.

Pour plus d'informations sur le démon smpppd, consultez les pages de manuel `smpppd` (1) et `smpppd.conf` (5).

26.1.3 kinternet, cinternet et qinternet en utilisation distante

Les programmes kinternet, cinternet et qinternet peuvent aussi bien être utilisés en local que gérer un démon smpppd distant. cinternet est ainsi l'équivalent en ligne de commande du programme graphique kinternet. Si vous souhaitez préparer ces utilitaires à utiliser un démon smpppd distant, vous devez modifier le fichier de configuration `/etc/smpppd-c.conf` manuellement ou à l'aide de kinternet. Ce fichier ne permet d'utiliser que trois options :

`sites =` ⟨***`list of sites`***⟩ Ici, vous indiquez aux interfaces frontales où se trouve le démon smpppd. Les interfaces frontales essaieront les options dans l'ordre établi ici. L'option `local` renvoie à l'établissement d'une connexion au smpppd local, `gateway` à un smpppd sur la passerelle. Avec `config-file`, la connexion doit être établie comme il est spécifié dans ce fichier sous `server`. `slp` indique aux interfaces frontales de se connecter avec un smpppd trouvé par SLP.

server = ⟨***server***⟩ Vous pouvez indiquer ici l'ordinateur sur lequel smpppd est exécuté.

password = ⟨***password***⟩ Saisissez ici le mot de passe qui a aussi été choisi pour le smpppd.

Si le démon smpppd fonctionne, vous pouvez à présent essayer d'y accéder. Utilisez pour cela la commande `cinternet --verbose --interface-list`. Si vous rencontrez encore des difficultés à ce niveau, reportez-vous aux pages de manuel `smpppd-c.conf` (5) et `cinternet` (1).

26.2 Configuration d'une connexion ADSL / T-DSL

26.2.1 Configuration par défaut

Actuellement, SuSE Linux prend en charge des accès xDSL basés sur le protocole PPPoE (*Point-to-Point over Ethernet*). Il s'agit d'un protocole utilisé par les principaux fournisseurs d'accès. Si vous n'êtes pas sûr du protocole utilisé par votre FAI, contactez-le, il vous renseignera certainement volontiers.

Vous devez installer les paquetages `ppp` et `smpppd`. Utilisez de préférence YaST pour cela. Utilisez YaST pour configurer votre carte réseau. N'utilisez pas `dhcp`, saisissez plutôt une adresse IP statique, comme par exemple `192.168.2.22`.

Les paramètres utilisés avec le module DSL de YaST sont enregistrés dans le fichier `/etc/sysconfig/network/providers/<provider>`. Vous disposez également de fichiers de configuration du démon smpppd (méta-démon PPP de SUSE) et ses interfaces frontales kinternet et cinternet. Veuillez consulter à ce sujet la page de manuel `man smpppd`.

Démarrez le réseau si nécessaire avec la commande `rcnetwork start` puis le démon smpppd avec la commande `rcsmpppd start`.

Les commandes `cinternet --start` et `cinternet --stop` vous permettent d'établir ou d'interrompre une connexion sur un système ne disposant pas d'interface graphique. Lorsque vous disposez d'une interface utilisateur graphique, utilisez kinternet pour cela. Sous KDE, ce programme est lancé automatiquement si vous avez installé le xDSL avec YaST. Cliquez sur l'icône en forme de roue dentée dans le tableau de bord. Choisissez 'Internet' → 'Contrôle' → 'kinternet'. Un symbole en forme de fiche électrique apparaît dans la barre de boutons. Cliquez

dessus pour démarrer la connexion, puis cliquez à nouveau dessus pour l'interrompre.

26.2.2 Connexion xDSL à la demande

La connexion à la demande signifie que la connexion est établie automatiquement, à chaque fois qu'un utilisateur accède à l'Internet, par exemple lorsqu'il consulte une page web avec un navigateur ou lorsqu'il envoie des messages électroniques. Au bout d'une durée donnée (temps d'inaction) au cours de laquelle aucune donnée n'est envoyée ni reçue, la connexion est à nouveau interrompue. Comme avec le protocole PPPoE, le protocole pour l'ADSL, la connexion est établie très rapidement, on a l'impression de disposer d'une connexion continue à l'Internet.

- La plupart des fournisseurs d'accès interrompent la connexion au bout d'une durée donnée.
- En effet, on peut considérer qu'une connexion permanente est susceptible de gaspiller les ressources (par exemple les adresses IP).
- Le grand risque en terme de sécurité, dans le cas d'une connexion permanente, est qu'un attaquant essaie de rechercher les failles du système. Il est ainsi beaucoup plus difficile d'attaquer un système qui n'accède à l'Internet qu'à la demande et de surcroît, à chaque fois avec une nouvelle adresse IP.

Vous pouvez activer la connexion à la demande avec YaST ou le faire manuellement. Attribuez, dans le fichier `/etc/sysconfig/network/providers/<provider>` la valeur `"yes"` au paramètre `DEMAND=` et définissez un temps d'inaction à l'aide de la variable `IDLETIME="60"`. Cela permet d'interrompre une connexion non utilisée au bout de 60 secondes.

Pour la définition d'une passerelle DSL pour les réseaux privés, nous vous recommandons la lecture de l'article *DSL gateway for private network since SuSE Linux 8.0* de notre base de données support : `http://portal.suse.com`, mot-clé *gateway*.

26.3 Un serveur de proximité : Squid

Squid est un serveur cache de proximité pour les plates-formes Linux/UNIX. Nous allons expliquer comment le configurer, les exigences techniques que cela implique, comment le système à proprement parler doit être configuré pour mettre des fichiers à disposition de manière transparente, la manière d'obtenir

des statistiques sur l'utilisation du cache à l'aide de programmes tels que Calamaris et cachemgr ou comment filtrer le contenu Web avec squidGuard.

26.3.1 Qu'est-ce qu'un serveur cache de proximité ?

Squid est un serveur cache de proximité. Il transmet des demandes reçues des clients (dans ce cas, le navigateur Web) serveur. Lorsque les objets demandés arrivent du serveur, il les transmet au client et en garde une copie sur un cache de son disque dur.

L'avantage est notable quand plusieurs clients demandent le même objet : votre requête peut alors être satisfaite directement à partir du cache stocké sur le disque dur. Les clients reçoivent ainsi les données beaucoup plus rapidement que depuis l'Internet. Parallèlement, cela permet d'économiser beaucoup de bande passante.

Outre l'antémémoire (caching), Squid offre un large éventail de fonctionnalités. Il permet par exemple de définir des hiérarchies entre serveurs de proximité pour permettre de répartir la charge du système, de définir des règles d'accès précises pour l'ensemble des clients qui souhaitent accéder au serveur de proximité, d'autoriser ou de refuser l'accès à certaines pages web à l'aide d'autres applications ou d'établir des statistiques sur les pages web les plus consultées et ainsi le comportement de navigation de l'utilisateur.

Squid n'est pas un serveur de proximité générique. Normalement il ne sert de médiateur qu'entre des connexions HTTP. En outre, il prend en charge les protocoles FTP, Gopher, SSL et WAIS mais ne gère pas certains autres protocoles Internet tels que Real Audio, les forums (News) ou les vidéoconférences. Squid n'a recours au protocole UDP que pour la prise en charge de la communication entre différents caches. C'est pour cette raison qu'il ne prend pas non plus en charge d'autres programmes multimédia.

26.3.2 Informations au sujet du serveur cache de proximité

Squid et la sécurité

Vous pouvez utiliser Squid conjointement avec un pare-feu pour protéger de l'extérieur les réseaux internes en utilisant un serveur cache de proximité. Le pare-feu interdit à tout client, à l'exception de Squid, d'établir une connexion avec des services externes. Toutes les connexions WWW doivent donc être établies par l'intermédiaire du serveur de proximité.

Dans le cas d'un pare-feu avec une zone démilitarisée, installez votre serveur de proximité dans cette zone. Il est alors important que tous les ordinateurs de la DMZ n'envoient leurs fichiers de journalisation qu'à des ordinateurs à l'intérieur du réseau sécurisé.

Vous trouverez une possibilité d'implémentation d'un tel serveur de proximité "transparent" à la section *Configuration d'un serveur de proximité transparent* page 646.

Plusieurs caches

Vous pouvez configurer plusieurs serveurs de proximité de manière à ce qu'ils puissent échanger des objets entre eux. Ainsi, il est possible de réduire la charge du système et d'augmenter la probabilité de trouver un objet lorsque celui-ci est déjà disponible sur le réseau local. Il est également possible d'établir des hiérarchies de caches, afin qu'un cache soit en mesure soit de faire suivre des demandes d'objets aux caches de même niveau hiérarchique, soit de demander à un cache de niveau supérieur de télécharger les objets à partir d'un autre cache du réseau local ou directement à la source.

Il est important de choisir soigneusement la topologie pour la hiérarchie de caches afin de ne pas augmenter le trafic réseau global. Ainsi, dans un réseau constitué de nombreuses machines, il est possible de configurer un serveur de proximité pour chaque sous-réseau, et de lier ensuite celui-ci à un serveur de proximité de niveau supérieur, à son tour connecté au serveur cache de proximité du fournisseur d'accès Internet.

Toute la communication est gérée par le protocole ICP (*Internet Cache Protocol*) placé au-dessus du protocole UDP. L'échange de données entre les caches se fait à l'aide du protocole HTTP (*Hyper Text Transmission Protocol*) basé sur TCP.

Pour trouver les meilleurs serveurs pour les objets souhaités, un cache envoie une requête ICP à tous les serveurs de proximité du même niveau hiérarchique. Les serveurs de proximité réagissent alors à ces demandes avec des réponses ICP contenant le code "HIT" si l'objet a été trouvé ou le code "MISS" dans le cas contraire. S'il a obtenu plusieurs réponses HIT, le serveur de proximité désigne un serveur particulier pour le téléchargement. La rapidité de réponse d'un cache, ou sa proximité physique, font partie des paramètres de décision. Si la réponse n'est pas satisfaisante, la demande est transmise au cache de niveau supérieur.

Remarque

Pour éviter d'enregistrer plusieurs fois des objets dans différents caches du réseau, d'autres protocoles ICP sont également utilisés, comme par exemple CARP (*Cache Array Routing Protocol*) ou HTCP (*Hyper-Text Cache Protocol*). Plus il y a d'objets présents sur le réseau, plus il est facile de trouver celui qui est cherché.

Remarque

Enregistrement intermédiaire d'objets Internet

Tous les objets disponibles sur le réseau ne sont pas statiques. Il existe de nombreuses pages CGI générées de manière dynamique, des compteurs d'accès ou des documents SSL chiffrés pour garantir un certain niveau de sécurité. C'est pour cette raison que ce type d'objets n'est pas conservé en cache : en effet, à chaque nouvel accès, l'objet est modifié.

Pour tous les autres objets qui se trouvent dans le cache, se pose la question de savoir combien de temps ils doivent y rester. Tous les objets sont donc classés dans le cache en fonction de différents critères, afin de pouvoir prendre cette décision.

Les en-têtes `Last modified` ("dernière modification") ou `Expires` ("expire le") et la date correspondante permettent aux serveurs Web et de proximité de s'informer de l'état d'un objet. D'autres en-têtes sont également utilisées pour indiquer par exemple qu'un objet donné ne doit pas faire l'objet d'un enregistrement intermédiaire.

Les objets stockés dans le cache sont généralement remplacés si la place vient à manquer, et ce à l'aide d'algorithmes tels que *Last Recently Used* (LRU) développés spécialement pour la gestion des objets en cache. Le principe consiste, en substance, à remplacer les objets demandés le moins fréquemment.

26.3.3 Configuration requise

Vous devez tout d'abord déterminer la charge maximale du système. Il est capital d'accorder une attention particulière aux pointes du système dans la mesure où celles-ci peuvent être jusqu'à plus de quatre fois plus élevées que la moyenne quotidienne. En cas de doute, il est préférable de surévaluer la configuration requise car un Squid qui fonctionne à sa limite peut entraîner des pertes de qualité de service considérables.

Vous allez découvrir dans les sections suivantes les différents facteurs système, classés en fonction de leur importance.

Disque dur

La vitesse joue un rôle déterminant dans le processus d'enregistrement intermédiaire. Il convient donc d'accorder une attention toute particulière à ce facteur. Pour les disques durs, ce paramètre est désigné par le "temps d'accès direct", exprimé en millisecondes. On peut approximativement considérer que plus cette valeur est faible, plus le système sera performant. Pour une vitesse élevée, il est donc conseillé de choisir des disques durs rapides.

Comme, la plupart du temps, Squid lit ou écrit des blocs de données de petite taille, le temps d'accès d'un disque dur est plus déterminant que son débit. De ce point de vue, il est particulièrement intéressant de choisir des disques durs ayant une vitesse de rotation élevée, qui permet un positionnement rapide de la tête de lecture. Les disques durs SCSI rapides offrent aujourd'hui des temps d'accès inférieurs à 4 millisecondes.

Pour augmenter la vitesse, une solution consiste à utiliser simultanément plusieurs disques durs ou à utiliser des matrices de disques RAID (*Striping Raid Arrays*).

Taille du cache du disque dur

Dans un petit cache, la probabilité d'obtenir un HIT (l'objet souhaité est déjà présent) est faible, car le cache peut vite être rempli. Dans ce cas, les objets les moins fréquemment demandés sont remplacés par des nouveaux. Si par exemple le cache dispose d'1 Go et que l'utilisateur n'a besoin que de 10 Mo par jour pour naviguer, il faut donc plus de cent jours pour remplir le cache.

Le plus simple consiste à déterminer la taille du cache en fonction du débit maximal de la connexion. Pour une connexion à 1 Mbit/s, le débit maximal est égal à 125 Ko/s. Si la totalité des données du trafic arrive dans le cache, cela représente au bout d'une heure un volume de 450 Mo. Si l'on suppose ensuite que le trafic total de données n'est généré que pendant huit heures de travail, on obtient pour une journée 3,6 Go. Comme la connexion n'est généralement pas exploitée jusqu'à sa capacité maximale, on peut en déduire que le volume total de données traitées par le cache s'élève environ à 2 Go. Dans cet exemple, 2 Go d'espace disque sont donc nécessaires àSquid pour conserver en cache toutes les données de toutes les pages consultées en *une* journée.

Mémoire vive

La quantité de mémoire utilisée par Squid (RAM) dépend du nombre d'objets placés en cache. Squid stocke, dans la mémoire centrale, des renvois vers les objets en cache ainsi que les objets fréquemment demandés afin de pouvoir extraire ces données plus vite. La mémoire centrale est beaucoup plus rapide qu'un disque dur !

Squid conserve également d'autres données en mémoire par exemple une table de toutes les adresses IP attribuées, un cache de noms de domaines fixés, les objets les plus fréquemment demandés, des tampons, des listes de contrôle d'accès, etc.

Il est très important que le processus Squid dispose de suffisamment de mémoire. S'il devait avoir recours au disque dur, les performances du système s'en verraient considérablement réduites. Vous pouvez utiliser l'outil cachemgr.cgi pour la gestion du cache. Vous en trouverez une présentation à la section *cachemgr.cgi* page 649.

Processeur

Squid n'a pas besoin d'un processeur très puissant. Ce n'est que lors du démarrage et pendant la vérification du contenu du cache que la charge du processeur est plus élevée. L'utilisation d'ordinateurs multiprocesseurs n'augmente pas les performances du système. Pour augmenter l'efficacité, il est plutôt recommandé d'utiliser des disques durs rapides ou d'ajouter de la mémoire.

26.3.4 Démarrer Squid

Sous SUSE LINUX, Squid est préconfiguré de telle sorte que vous pouvez le démarrer dès l'installation terminée. L'une des conditions préalables à un démarrage en douceur est que le réseau soit configuré de manière à ce qu'au moins un serveur de noms et l'Internet dont on veut mettre en mémoire cache les données, soient accessibles. On peut rencontrer des problèmes lors de l'utilisation d'une connexion par ligne commutée avec une configuration DNS dynamique. Dans ce cas, au moins le serveur de noms doit être indiqué de manière fixe, car Squid ne démarre tout simplement pas s'il ne trouve pas de serveur DNS dans `/etc/resolv.conf`.

Commandes de démarrage et d'arrêt

Pour démarrer Squid, saisissez sur la ligne de commande (en tant qu'utilisateur `root`) la commande `rcsquid start`. La première fois, le script de démarrage

`/etc/init.d/squid` crée automatiquement la structure de répertoires dans `/var/squid/cache`, ce qui peut durer de quelques secondes à quelques minutes. Si `done` apparaît à droite en vert, Squid est correctement démarré. Vous pouvez alors tester immédiatement le fonctionnement de Squid en déclarant dans le navigateur un proxy à l'adresse `localhost` et sur le port `3128`.

Pour permettre à tous d'accéder à Squid et donc à l'Internet, vous n'avez besoin de changer dans le fichier de configuration `/etc/squid/squid.conf` que la ligne `http_access deny all` en `http_access allow all`. Il ne faut cependant pas oublier qu'en procédant de la sorte vous ouvrez complètement Squid à tout le monde. Partant de ce constat, vous devez impérativement définir des ACL (listes de contrôle d'accès) qui réglementent l'accès au serveur de proximité. Pour plus d'informations à ce sujet, se reporter à la section *Options liées au contrôle d'accès* page 643.

Si vous avez modifié le fichier de configuration `/etc/squid/squid.conf`, Squid doit prendre en compte vos changements avec la commande `rcsquid reload`. Vous pouvez aussi complètement redémarrer Squid : `rcsquid restart`.

La commande `rcsquid status` vous permet de déterminer si le serveur de proximité fonctionne. On arrête Squid avec la commande `rcsquid stop`. L'arrêt peut prendre un certain temps, car Squid attend jusqu'à trente secondes (option `shutdown_lifetime` dans `/etc/squid/squid.conf`) avant d'interrompre les connexions avec les clients et il lui reste encore, à ce moment-là, à écrire ses données sur disque.

Attention

Arrêt de Squid

Si vous arrêtez Squid avec `kill` ou `killall`, vous pouvez endommager le cache que vous devrez alors vider pour pouvoir redémarrer Squid.

Attention

Si Squid s'arrête peu de temps après avoir démarré apparemment correctement, cela peut être dû à un enregistrement de serveur de noms erroné ou à un fichier `/etc/resolv.conf` incorrect. Squid enregistre donc le motif de l'échec du démarrage dans le fichier `/var/squid/logs/cache.log`. Si Squid doit être démarré automatiquement lors de l'amorçage, Squid doit être activé pour le niveau d'exécution correspondant dans l'éditeur de niveaux d'exécution de YaST.

Lors d'une désinstallation de Squid, ni la hiérarchie de caches, ni les fichiers journaux ne sont supprimés. Vous devez supprimer manuellement le répertoire `/var/cache/squid`.

Serveur DNS local

Cela a un sens d'utiliser un serveur DNS local même s'il n'a pas à gérer son propre domaine. Il fonctionne alors seulement en tant que DNS de cache (*Caching- only DNS*) et peut, sans configuration particulière, résoudre les requêtes DNS grâce aux serveurs de noms racine ; pour plus d'informations, consultez la section *Démarrer le serveur de noms BIND* page 487. Si vous précisez ce serveur local dans le fichier `/etc/resolv.conf` avec l'adresse IP `127.0.0.1` pour `localhost`, Squid trouve toujours un serveur de noms valable lors du démarrage. Il est conseillé d'indiquer le serveur

de noms du fournisseur d'accès dans le fichier de configuration `/etc/named.conf` dans la catégorie `forwarders` avec son adresse IP. Si vous utilisez un pare-feu, vous devez veiller à ce qu'il laisse également passer les requêtes DNS.

26.3.5 Le fichier de configuration /etc/squid/squid.conf

Vous devez effectuer tous les réglages du serveur de proximité Squid dans le fichier `/etc/squid/squid.conf`. Pour pouvoir démarrer Squid la première fois, aucune modification n'est nécessaire ; l'accès des clients externes étant dans un premier temps impossible. `localhost` est a le droit d'utiliser le serveur de proximité et c'est le port `3128` qui est utilisé par défaut. Vous trouverez des explications complètes des options et de nombreux exemples dans le fichier `/etc/squid/squid.conf` préinstallé. Presque toutes les lignes sont précédées d'un signe # ; les spécifications correspondantes se trouvant en fin de ligne. Les valeurs indiquées correspondent presque toujours aux valeurs par défaut, si bien que la suppression du signe de commentaire, sans modifier le paramètre de l'option n'a, à quelques exceptions près, aucun effet. Il est donc préférable de conserver l'exemple commenté et de recopier l'option avec le paramètre modifié sur la ligne en-dessous. Vous pouvez ainsi distinguer sans problème les valeurs prédéfinies et les modifications qui y sont apportées.

Remarque

Corriger le ficher de configuration après une mise à jour

Si vous avez effectué une mise à jour à partir d'une version plus ancienne de Squid, il faut impérativement utiliser le nouveau fichier `/etc/squid/squid.conf` et ne reprendre que les modifications du fichier précédent. Si vous essayez de continuer à utiliser l'ancien `squid.conf`, vous courez le risque que votre configuration ne fonctionne plus parce que les options sont continuellement modifiées et que de nouvelles sont fréquemment ajoutées.

Remarque

Options de configuration générales (sélection)

`http_port 3128` C'est le port sur lequel Squid écoute les demandes des clients. La valeur par défaut est `3128`, `8080` est également fréquemment utilisé. Il est possible d'indiquer ici plusieurs numéros de port en les séparant par des espaces.

`cache_peer` ⟨***`hostname`***⟩ ⟨***`type`***⟩ ⟨***`proxy-port`***⟩ ⟨***`icp-port`***⟩
Vous pouvez saisir ici un serveur de proximité de niveau supérieur en tant que "parent" par exemple lorsque vous souhaitez ou devez utiliser celui du fournisseur d'accès. Indiquez dans ⟨*hostname*⟩, le nom ou l'adresse IP du serveur de proximité à utiliser et comme ⟨*type*⟩, *parent*. Indiquez dans ⟨*proxy-port*⟩ le numéro de port que le gestionnaire du serveur parent demande d'utiliser dans le navigateur, en général `8080`. Vous pouvez définir ⟨*icp-port*⟩ à `7` ou `0` si vous ne connaissez pas le port ICP du parent ou si l'utilisation de celui-ci n'a pas été convenue avec le fournisseur d'accès. Vous devez encore préciser `default` et `no-query` après le numéro de port pour empêcher complètement l'utilisation du protocole ICP. Squid se comporte alors vis-à-vis du serveur de proximité du fournisseur d'accès comme un navigateur normal.

`cache_mem 8 MB` Cet élément indique la taille maximale de la mémoire de travail utilisée par Squid pour le cache. La valeur par défaut est `8 Mo`.

`cache_dir ufs /var/cache/squid 100 16 256`
L'élément *cache_dir* indique le répertoire dans lequel tous les objets sont stockés sur le disque. Les nombres derrière indiquent l'espace disque maximal à utiliser en "Mo" et le nombre des répertoires dans les premier et deuxième niveaux. Ne modifiez pas le paramètre `ufs`. L'espace disque

défini par défaut est de `100 Mo` dans le répertoire `/var/cache/squid`, soit 16 sous-répertoires contenant chacun environ 256 répertoires. Lorsque l'on indique l'espace disque à utiliser, il faut prévoir suffisamment de marge. Des valeurs comprises entre 50 et 80 pour cent du disque disponible sont raisonnables, 80 pour cent étant un maximum. N'augmentez les deux derniers valeurs c'est-à-dire le nombre de répertoires qu'avec la plus grande précaution, dans la mesure où trop de répertoires peuvent également avoir des répercussions sur la performance. Si vous disposez de plusieurs disques sur lesquels répartir le cache, insérez autant de lignes *cache_dir* que nécessaire.

`cache_access_log /var/log/squid/access.log`
Chemin des fichiers journaux

`cache_log /var/log/squid/cache.log`
Chemin des fichiers journaux

`cache_store_log /var/log/squid/store.log`
Chemin des fichiers journaux. Ces trois éléments indiquent le chemin d'accès aux fichiers journaux de Squid. Ils ne doivent normalement pas être modifiés. Si Squid doit être fortement sollicité, il peut être judicieux de répartir le cache et les fichiers journaux sur différents disques.

`emulate_httpd_log off` Si vous réglez ce paramètre à *on*, vous obtiendrez des fichiers journaux lisibles. Certains programmes n'arrivent toutefois pas à les exploiter.

`client_netmask 255.255.255.255`
Cet élément permet de masquer les adresses IP enregistrées dans les fichiers journaux et ainsi de dissimuler l'identité des clients. Si vous indiquez `255.255.255.0` ici, le dernier chiffre de l'adresse IP est mis à zéro.

`ftp_user Squid@` Vous pouvez définir ici le mot de passe que Squid doit utiliser pour une connexion FTP anonyme. Il peut être intelligent d'indiquer une adresse électronique valable dans son propre domaine car certains serveurs FTP en vérifient la validité.

`cache_mgr webmaster` Une adresse électronique à laquelle Squid envoie un message lorsqu'il s'arrête de manière inattendue. L'adresse par défaut est celle du *webmestre*.

`logfile_rotate 0` Squid peut effectuer une rotation des fichiers journaux sécurisés si vous lancez la commande `squid -k rotate`. Les fichiers sont à cet effet numérotés et lorsque la valeur spécifiée est atteinte, les fichiers les plus anciens sont écrasés. Cette valeur est par défaut fixée à

`0`, car l'archivage et la suppression des fichiers journaux dans SUSE LINUX est effectué par une tâche cron propre configurée dans le fichier `/etc/logrotate/squid`.

`append_domain` ⟨***`domain`***⟩ Avec *append_domain*, vous pouvez indiquer quel domaine doit être automatiquement ajouté lorsqu'aucun n'est spécifié. On indique ici la plupart du temps son propre domaine et il suffit alors de saisir *www* dans le navigateur pour accéder à son propre serveur Web.

`forwarded_for on` Si vous réglez ce paramètre à *off*, Squid retire des requêtes HTTP les adresses IP ou les noms de machine des clients.

`negative_ttl 5 minutes; negative_dns_ttl 5 minutes`
Vous n'avez normalement pas besoin de modifier cette valeur. Si toutefois vous disposez d'une liaison commutée, il se peut que l'Internet ne puisse parfois pas être joint. Squid retient alors les demandes qui ont échoué et refuse de procéder à de nouvelles requêtes même si la connexion Internet est rétablie. Pour ce cas, vous devez remplacer *minutes* par *seconds* pour que l'utilisateur demandant à *recharger* la page dans le navigateur obtienne satisfaction juste quelques secondes après le rétablissement de la connexion.

`never_direct allow` ⟨***`acl_name`***⟩
Si vous souhaitez empêcher que Squid n'interroge directement l'Internet, vous pouvez forcer ici l'utilisation d'un autre serveur de proximité. Vous devez avoir au préalable saisi celui-ci sous *cache_peer*. Si vous indiquez *all* en tant que <*acl_name*> , vous forcez le transfert de toutes les demandes au *parent*. Cela peut, par exemple, être utile si vous passez par un fournisseur d'accès qui exige que vous utilisiez son serveur de proximité ou si le pare-feu n'autorise aucun accès direct à l'Internet.

Options liées au contrôle d'accès

Squid propose un système détaillé pour gérer l'accès au serveur de proximité. L'utilisation d'ACL (listes de contrôle d'accès) permet de le configurer facilement et de manière polyvalente. Il s'agit de listes de règles élaborées point par point. Vous devez commencer par définir des ACL pour pouvoir les utiliser. Quelques ACL usuelles telles que *all* et *localhost* sont déjà disponibles. La définition d'une ACL en soi n'a cependant aucun effet. Ce n'est qu'une fois réellement installée par exemple en relation avec *http_access* qu'une règle définie fonctionne.

`acl` ⟨***`acl_name`***⟩ ⟨***`type`***⟩ ⟨***`data`***⟩ Pour définir une ACL, vous avez besoin d'au moins trois informations. Vous pouvez choisir son nom <*acl_name*> librement. Pour le <*type*>, vous pouvez choisir parmi un large éventail de

possibilités que vous pouvez consulter dans la section *ACCESS CONTROLS* du fichier `/etc/squid/squid.conf`. Les données, <*data*>, dépendent du type de l'ACL et sont également disponibles dans un fichier, il peut par exemple s'agir de noms d'ordinateur, d'adresses IP ou d'URL. En voici quelques exemples simples :

```
acl monsurfeur srcdomain .mon-domaine.com
acl professeur src 192.168.1.0/255.255.255.0
acl etudiants src 192.168.7.0-192.168.9.0/255.255.255.0
acl midi time MTWHF 12:00-15:00
```

`http_access allow` ⟨***`acl_name`***⟩ Utilisez *http_access* pour définir qui est autorisé à utiliser le serveur de proximité et à quoi il peut accéder sur l'Internet. Pour ce faire, saisissez des ACL qui interdiront l'accès avec *deny* ou l'autoriseront avec *allow* ; *localhost* et *all* ont déjà été définis plus haut. Vous pouvez créer ici une liste comprenant plusieurs déclarations *http_access* ; ainsi, selon ce qui se produit en premier, l'accès à l'URL demandé sera ou non autorisé. Le dernier élément doit toujours être *http_access deny all*. Dans l'exemple suivant, *localhost*, c'est-à-dire l'ordinateur local a un accès libre à tout, tandis que tout est complètement bloqué pour tous les autres :

```
http_access allow localhost
http_access deny all
```

Encore un exemple dans lequel sont utilisées les ACL définies précédemment : le groupe `professeurs` a tout le temps accès à l'Internet, tandis que le groupe `etudiants` n'y a accès que du lundi au vendredi et seulement pendant la pause de midi :

```
http_access deny localhost
http_access allow professeurs
http_access allow etudiants midi
http_access deny all
```

Pour des raisons de clarté, n'insérez dans la liste vos propres éléments *http_access* qu'à l'endroit prévu à cet effet dans le fichier `/etc/squid/squid.conf`. Cela signifie entre le texte

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

et la déclaration finale

```
http_access deny all final.
```

redirect_program /usr/bin/squidGuard
Vous pouvez utiliser cette option pour indiquer un "redirecteur", comme squidGuard qui est en mesure de bloquer l'accès aux URL indésirables. Il est donc possible de gérer très finement l'accès à l'Internet de différents groupes d'utilisateurs à l'aide de l'authentification sur le serveur de proximité et des ACL adaptées. squidGuard est un paquetage indépendant qui s'installe et qui se configure séparément.

auth_param basic program /usr/sbin/pam_auth
Si les utilisateurs doivent s'authentifier auprès du serveur de proximité, vous pouvez indiquer ici un programme responsable de l'authentification comme par exemple pam_auth. Lorsque pam_auth est utilisé, une fenêtre de login dans laquelle l'utilisateur doit saisir son nom et son mot de passe s'ouvre lors de sa première tentative de connexion. Vous disposez, en outre, d'une ACL supplémentaire pour n'autoriser à naviguer que les clients disposant d'un login valable :

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

Vous pouvez aussi remplacer le mot-clé *REQUIRED* après *proxy_auth* par une liste de noms d'utilisateurs autorisés ou par le chemin d'accès à cette liste.

ident_lookup_access allow ⟨***acl_name***⟩
Cette option permet qu'une demande d'identification soit adressée à tous les clients définis à l'aide d'ACL pour vérifier l'identité de chaque utilisateur. Si vous attribuez à <*acl_name*> la valeur *all*, cela s'applique de manière générale à tous les clients. Un démon ident doit fonctionner pour ce faire sur tous les clients ; sous Linux, vous pouvez installer le paquetage pidentd, et sous Windows, il existe un logiciel gratuit pouvant être téléchargé

sur l'Internet. Pour que seuls soient autorisés les clients dont la recherche d'identité est réussie, il faut ici encore définir une ACL correspondante :

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

Vous pouvez ici aussi remplacer le terme *REQUIRED* par une liste de noms d'utilisateurs autorisés. L'utilisation d'*ident* peut considérablement ralentir l'accès dans la mesure où la recherche d'identité est répétée en entier à chaque demande.

26.3.6 Configuration d'un serveur de proximité transparent

Normalement, le navigateur Web envoie les demandes à un port donné du serveur de proximité et le serveur de proximité fournit les objets demandés, qu'ils soient ou non en cache. Dans un vrai réseau, différentes situations peuvent se présenter :

- Pour des raisons de sécurité, il vaut mieux que tous les clients utilisent un serveur de proximité pour naviguer sur l'Internet.
- Il est indispensable que tous les clients utilisent un serveur de proximité qu'ils en soient ou non informés.
- Si le serveur de proximité d'un réseau déménage, les clients existants doivent quand même conserver leur ancienne configuration.

Vous pouvez utiliser un serveur de proximité transparent dans chacun des cas mentionnés ci-dessus. Le principe est très simple : le serveur de proximité accepte les demandes du navigateur Web et les traite de manière à ce que le navigateur Web obtienne les pages demandées sans savoir d'où elles proviennent. Le processus complet s'exécute de manière transparente, d'où son nom.

Configuration du noyau

Vous devez commencer par vous assurer que le noyau du serveur de proximité prend en charge un serveur de proximité transparent. Le noyau livré avec SUSE LINUX Enterprise Server est configuré de façon à assurer cette prise en charge. Dans le cas contraire, vous devez ajouter ces options au noyau et le recompiler. Vous trouverez des informations précises à ce sujet dans le chapitre *Le noyau Linux* page 227.

Options de configuration de /etc/squid/squid.conf

Vous devez activer les options suivantes dans le fichier `/etc/squid/squid.conf` pour définir un serveur de proximité transparent :

- `httpd_accel_host` virtual
- `httpd_accel_port` 80 # Port, sur lequel se trouve le véritable serveur HTTP.
- `httpd_accel_with_proxy` on
- `httpd_accel_uses_host_header` on

Configuration du pare-feu avec SuSEfirewall2

Toutes les demandes qui passent au travers du pare-feu doivent être redirigées vers le port de Squid à l'aide d'une règle de redirection de port. Utilisez pour ce faire l'outil proposé par SuSE, SuSEfirewall2. Il se configure à l'emplacement `/etc/sysconfig/SuSEfirewall2`. Le fichier de configuration, se compose encore une fois d'éléments bien documentés. Même si vous ne souhaitez qu'installer un serveur de proximité transparent, il vous faut configurer quelques options de pare-feu :

- L'interface est du côté de l'Internet : `FW_DEV_EXT`="eth1"
- L'interface est du côté du réseau interne : `FW_DEV_INT`="eth0"

Il est impossible d'accéder aux ports et aux services (voir `/etc/services`) du pare-feu à partir de réseaux non dignes de confiance, c'est-à-dire de l'Internet. Dans cette exemple, nous n'offrons à l'extérieur comme service que le Web.

`FW_SERVICES_EXT_TCP`="www"

Il est possible d'accéder aux ports et services (voir `/etc/services`) dans le pare-feu à partir d'un réseau sécurisé, que ce soit en TCP ou en UDP.

`FW_SERVICES_INT_TCP`="domain www 3128"

`FW_SERVICES_INT_UDP`="domain"

Nous accédons au Web et à Squid (dont le port par défaut est `3128`). Le service décrit ci-dessus "Domain" signifie DNS ou Domain Name Service. Il s'agit d'un service utilisé fréquemment. Sinon, vous devez simplement supprimer l'élément ci-dessus et définir l'option suivante à `no` :

`FW_SERVICE_DNS`="yes"

L'option la plus importante est le nombre `15` :

Exemple 26.1: *L'option 15 de la configuration du pare-feu*

```
#
# 15.)
# Quel accès aux différents services doit être redirigé vers un
# port local de l'ordinateur pare-feu ?
#
# Cette option permet d'obliger tous les utilisateurs internes à
# utiliser le serveur de proximité pour naviguer ou de transférer
# tout le trafic Web entrant à un serveur Web sécurisé.
#
# Choix : n'insérer aucun nouvel élément ou utiliser la syntaxe
# de règle de redirection suivante séparée par des espaces.
# Une règle de redirection se compose de : 1) IP/réseau source,
# 2) IP/ réseau cible, 3) port cible précédent et 4) port local
# vers lequel le trafic doit être redirigé, séparés par des
# virgules, par exemple :
# "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"
#
```

La syntaxe à respecter est indiquée dans le commentaire ci-dessus. D'abord, les adresses IP et le masque réseau du "réseau interne" accèdent au pare-feu du serveur de proximité. Ensuite, les adresses IP et le masque réseau auxquels sont "envoyées" les demandes des clients. Pour les navigateurs Web, on choisit les réseaux `0/0`. Il s'agit d'un joker qui signifie "dans toutes les directions". Vient ensuite le port "d'origine" auquel ces demandes ont été envoyées et enfin le port vers lequel les demandes sont "redirigées".

Comme Squid prend en charge d'autres protocoles que le seul HTTP, il est aussi possible de rediriger des demandes provenant d'autres ports au serveur de proximité, comme par exemple FTP (port 21), HTTPS ou SSL (port 443).

Concrètement, les services Web (port `80`) sont redirigés vers le port du serveur de proximité (ici `3128`. Si plusieurs réseaux ou services doivent être ajoutés, ils doivent être séparés par un espace dans la ligne correspondante.

`FW_REDIRECT_TCP`="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"

`FW_REDIRECT_UDP`="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"

Pour démarrer le pare-feu et la nouvelle configuration, vous devez modifier une ligne du fichier `/etc/sysconfig/SuSEfirewall2`. Le paramètre `START_FW` doit être défini à "yes" :

Démarrez Squid comme décrit dans la section *Démarrer Squid* page 638. Vous pouvez utiliser les fichiers journaux dans `/var/log/squid/access.log` pour vérifier que tout fonctionne correctement. Pour vérifier que tous les ports sont correctement configurés, vous pouvez exécuter une analyse des ports de l'ordinateur à partir de n'importe quel ordinateur extérieur au réseau. Seul le port du service Web (80) doit être ouvert. Pour analyser les ports, saisissez :`nmap -O` ⟨*adresses IP*⟩.

26.3.7 cachemgr.cgi

Le gestionnaire de cache (cachemgr.cgi) est un programme CGI utilisé pour générer des statistiques au sujet de la place nécessaire pour les processus Squid en cours. Contrairement à la journalisation, il facilite la gestion du cache et l'affichage des statistiques.

Mise en place

Vous avez tout d'abord besoin d'un serveur Web en état de marche sur le système. En tant qu'utilisateur `root` saisissez les informations suivantes pour savoir si Apache fonctionne déjà : `rcapache status`.

Si un message comme celui ci-dessous s'affiche, Apache fonctionne sur l'ordinateur :

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

Dans le cas contraire, vous devez saisir la commande suivante : `rcapache start`. Cela vous permet de démarrer Apache avec les paramètres par défaut de SUSE LINUX.

Enfin, il faut copier le fichier `cachemgr.cgi` du répertoire `/usr/share/doc/packages/squid/scripts/` dans le répertoire `/srv/www/cgi-bin` d'Apache.

Les ACL du gestionnaire de cache dans /etc/squid/squid.conf

Vous disposez des paramètres par défaut suivants pour le gestionnaire de cache :

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Les règles suivantes doivent être incluses :

```
http_access allow manager localhost
http_access deny manager
```

La première ACL est la plus importante car le gestionnaire de cache essaie de communiquer avec Squid avec le protocole cach_object. Les règles qui suivent précisent que le serveur Web et Squid tournent sur la même machine. La communication entre le gestionnaire de cache et Squid se passe au niveau du serveur Web et pas du navigateur. Ainsi, si le serveur Web se trouve sur un autre ordinateur, vous devez ajouter de manière expresse une ACL comme dans l'exemple 26.2.

Exemple 26.2: *Règles d'accès*

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # IP Webserver
```

Vous avez ensuite encore besoin des règles suivantes 26.3.

Exemple 26.3: *Règles d'accès*

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Il est également possible de configurer un mot de passe pour le gestionnaire s'il faut accéder à des options comme par exemple la fermeture du cache à distance ou l'affichage d'informations étendues sur le cache. Vous devez alors configurer le paramètre `cachemgr_passwd` et la liste des options qui s'affichent avec un mot de passe du gestionnaire. Cette liste apparaît en tant que partie des commentaires dans `/etc/squid/squid.conf`.

Vous devez redémarrer Squid à chaque fois que vous avez modifié le fichier de configuration. Pour ce faire, le plus simple est d'utiliser la commande suivante : `rcsquid reload`.

Affichage des statistiques

Rendez-vous sur la page Web correspondante, par exemple `http://webserver.example.org/cgi-bin/cachemgr.cgi`. Cliquez sur 'Continuer' pour afficher les différentes statistiques. Vous trouverez des informations supplémentaires au sujet des différents éléments fournis par le gestionnaire de cache dans la FAQ de Squid : `http://www.squid-cache.org/Doc/FAQ/FAQ-9.html`

26.3.8 squidGuard

Ce chapitre ne présente que la configuration de squidGuard et donne quelques conseils relatifs à son utilisation. L'objectif n'est pas ici d'en donner une explication complète. Vous trouverez des informations plus détaillées à ce sujet sur les pages Web de squidGuard : `http://www.squidguard.org`

squidGuard est un filtre libre (sous GPL), flexible et ultra-rapide, un redirecteur et un "module enfichable" pour les contrôles d'accès de Squid. Il permet de définir un grand nombre de règles d'accès à un cache Squid avec des limitations différentes en fonction des différents groupes d'utilisateurs. squidGuard utilise l'interface standard de Squid pour la redirection. Vous pouvez utiliser squidGuard, entre autres, pour :

- Limiter l'accès à l'Internet de certains utilisateurs à des serveurs Web et/ou des URL acceptés/connus.
- Refuser l'accès à certains serveurs Web et/ou URL à certains utilisateurs.
- Refuser l'accès aux URL qui contiennent des expressions ou des mots particuliers à certains utilisateurs.
- Rediriger les URL bloqués vers une page d'informations CGI "intelligente".
- Rediriger les utilisateurs non enregistrés vers un formulaire d'enregistrement.
- Remplacer les bannières par un GIF vide.
- Différentes règles d'accès en fonction de l'heure, du jour de la semaine, de la date, etc.
- Différentes règles pour les différents groupes d'utilisateurs.

Vous pouvez effectuer les opérations suivantes, que ce soit avec squidGuard ou avec Squid :

- Filtrer, censurer ou modifier le texte à l'intérieur de documents.
- Filtrer, censurer ou modifier le langage de script intégré dans du HTML, tel que JavaScript ou VBscript.

Installez `squidGuard`. Modifiez le fichier de configuration `/etc/squidguard.conf`. Vous disposez de nombreux autres exemples de configuration à l'adresse

`http://www.squidguard.org/config/`. Vous pourrez apprendre plus tard à effectuer des paramétrages plus compliqués.

L'étape suivante consiste à créer une page factice "Accès refusé" ou une page CGI plus ou moins convenable pour rediriger Squid lorsque le client demande une page Web interdite. Nous vous recommandons ici aussi l'utilisation d'Apache.

Il faut à présent configurer Squid de façon à ce qu'il utilise squidGuard. Utilisez pour ce faire les déclarations suivantes dans le fichier `/etc/squid/squid.conf` :

```
redirect_program /usr/bin/squidGuard
```

Une autre option appelée `redirect_children` permet de configurer le nombre des différents processus "redirect" exécutés, c'est-à-dire des processus de redirection (dans ce cas,squidGuard). squidGuard est suffisamment rapide pour traiter un grand nombre de demandes.(squidGuard est vraiment rapide : 100 000 demandes en 10 secondes sur un Pentium 500 MHz avec 5 900 domaines, 7 880 URL, soit 13 780 au total). Il est donc préférable de ne pas définir plus de 4 processus car l'attribution de ces processus consomme inutilement trop de mémoire.

```
redirect_children 4
```

Enfin, faites lire à Squid le nouveau fichier de configuration : `rcsquid reload`. Vous pouvez à présent tester vos réglages dans un navigateur.

26.3.9 Génération de rapports de cache avec Calamaris

Calamaris est un script Perl utilisé pour générer des rapports d'activité du cache au format ASCII ou HTML. Il utilise pour ce faire les journaux d'accès de Squid. Voici l'adresse de la page Web de Calamaris `http://Calamaris.Cord.de/`. Il s'agit d'un programme simple d'utilisation. Identifiez-vous en tant qu'utilisateur `root` et lancez la commande suivante : `cat access.log.files | calamaris` ⟨*options*⟩ `> reportfile`.

Lorsque vous utilisez plusieurs fichiers journaux, il est important de respecter l'ordre chronologique, c'est-à-dire que les fichiers les plus anciens viennent en premier. Voici les différentes options disponibles :

-a tous les rapports disponibles

-w rapport HTML

-l message ou logo dans l'en-tête du rapport

Pour plus d'informations sur les différentes options, consultez la page de manuel de Calamaris : `man calamaris`.

SARG (Squid Analysis Report Generator) est un autre outil puissant utilisé pour générer des rapports de cache. . Pour plus d'informations à son sujet, consultez la page Internet correspondante à l'adresse `http://web.onda.com.br/orso/`

26.3.10 Pour plus d'informations sur Squid

Consultez le site Internet de Squid à l'adresse `http://www.squid-cache.org/`. Vous y trouverez le guide de l'utilisateur de Squid ("Squid User Guide") et une FAQ complète au sujet de Squid. Le paquetage `howtoen`, que vous trouverez sous `/usr/share/doc/howto/en/mini/TransparentProxy.gz` après l'installation, propose un mini-descriptif (howto) des serveurs de proximité.

Enfin vous trouverez des listes de diffusion concernant Squid à l'adresse `squid-users@squid-cache.org`. L'archive correspondante se trouve à l'adresse `http://www.squid-cache.org/mail-archive/squid-users/`.

Sécurité sous Linux

Le masquage et les pare-feux fournissent les fondations d'un réseau sécurisé en contrôlant le trafic et l'échange des données. L'interpréteur de commandes sécurisé (Secure Shell, SSH) permet à l'utilisateur de se connecter à une machine distante via une liaison chiffrée. Le chiffrement des fichiers ou de partitions entières sécurise vos données lorsque des tiers ont accès à votre système. Outre ces instructions purement techniques, vous trouverez, en conclusion, une section traitant de différents aspects de la sécurité dans les réseaux Linux.

27.1 Mascarade et pare-feu

Lorsque Linux est mis en œuvre dans un environnement réseau découpé en différents secteurs internes et externes, on utilise les fonctionnalités de gestion des paquets réseau du noyau Linux. L'infrastructure Netfilter offre tous les moyens permettant d'utiliser un système Linux en tant que pare-feu efficace entre différents réseaux. Grâce à iptables – une structure de tables génériques permettant de définir des ensembles de règles – on peut contrôler avec précision quels sont les paquets du flux de données qui peuvent passer et ceux qui ne peuvent pas. SuSEfirewall2 et le module YaST correspondant vous facilitent l'installation d'un filtre de paquets.

27.1.1 Filtrage de paquets avec iptables

Netfilter et iptables sont chargés de filtrer, de modifier les paquets réseau. Ils peuvent aussi traduire les adresses réseau (NAT, *Network Address Translation*) de ces paquets. Les critères de filtrage ainsi que les actions correspondantes sont enregistrés dans des chaînes et traités dans l'ordre dès qu'un paquet réseau arrive. Les chaînes de règles à traiter sont enregistrées dans des tables. La commande `iptables` a pour mission de traiter ces tables et ces chaînes de règles.

Linux dispose de trois tables pour les différentes fonctions d'un filtre de paquets :

filter La plupart des règles se trouvent dans cette table puisque le *filtrage de paquets* proprement dit y est défini. Les règles concernant l'admission (`ACCEPT`) et l'abandon (`DROP`) des paquets y figurent.

nat La modification des adresses sources et cibles des paquets est définie ici. La *mascarade* dont vous vous servez pour la connexion d'un petit réseau privé à l'Internet est un cas particulier de NAT.

mangle Les valeurs contenues dans l'en-tête IP peuvent être manipulées à l'aide des règles fixées ici (le *Type de Service*).

Dans les tables citées, il y a plusieurs chaînes prédéfinies par lesquelles les paquets doivent passer :

`PREROUTING` Cette chaîne concerne les paquets qui viennent d'arriver au système.

`INPUT` Cette chaîne concerne les paquets qui sont destinés à des processus propres au système.

`FORWARD` Cette chaîne concerne les paquets qui sont simplement routés à travers le système.

`OUTPUT` Cette chaîne concerne les paquets qui ont été générés dans le système lui-même.

`POSTROUTING` Cette chaîne concerne tous les paquets qui quittent le système.

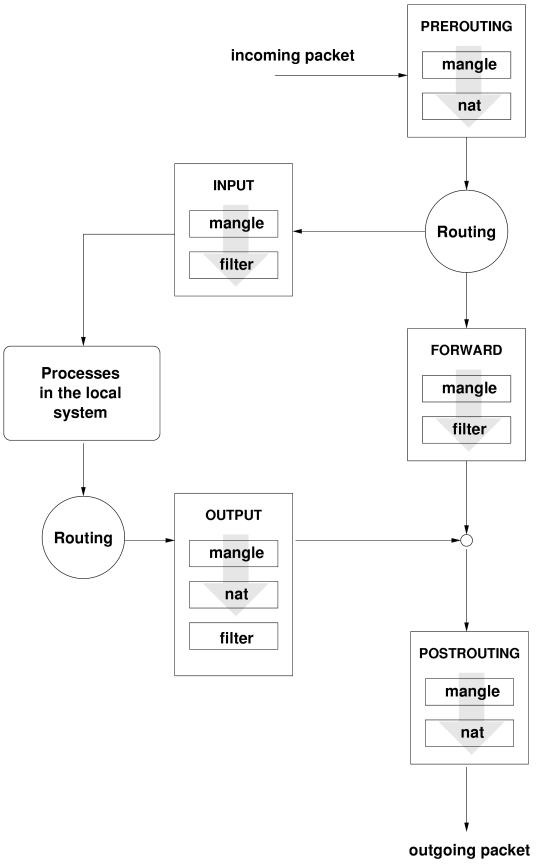


FIG. 27.1: *iptables : cheminement d'un paquet à travers le système*

La figure 27.1 page précédente illustre le cheminement d'un paquet réseau à travers le système. Pour la clarté de l'exposé, les tables sont groupées par chaînes, bien que dans la réalité les chaînes soient organisées à l'intérieur des tables.

Dans le cas le plus simple, un paquet qui est destiné au système lui-même arrive sur l'interface `eth0` du système. Ce paquet est d'abord dirigé dans la chaîne `PREROUTING` de la table `mangle`, puis dans la chaîne `PREROUTING` de la table `nat`. L'étape de routage correspondante permet d'établir que le paquet est destiné à un processus dans le système lui-même. Après être passé par la chaîne `INPUT` dans les deux tables `mangle` et `filter`, le paquet arrive à son lieu de destination, en supposant que les règles de filtrage dans la table ne l'en empêchent pas.

27.1.2 Principes de base de la mascarade

La mascarade est le cas particulier sous Linux de NAT *Network Address Translation*, la traduction des adresses réseau. Elle est mise en œuvre quand un petit réseau local ayant es adresses IP du domaine privé (voir section *Masques réseau et routage* page 443) est connecté à l'Internet avec ses adresses IP officielles. Pour que les ordinateurs du réseau local puissent établir des connexions à l'Internet, une correspondance entre les adresses privées et les adresses officielles s'impose. Ce processus a lieu sur le routeur, qui sert de commutateur entre le réseau local et l'Internet. Le principe sous-jacent est simple : votre routeur possède plusieurs interfaces réseau, généralement une carte réseau et une interface d'accès à l'Internet. Une de ces interfaces vous raccorde à l'extérieur, une ou plusieurs autres raccordent votre ordinateur aux autres ordinateurs de votre réseau. Vous disposez de plusieurs ordinateurs sur le réseau local, dont la carte réseau raccordée à votre routeur Linux s'appelle, dans cet exemple, `eth0`. Les machines du réseau envoient au routeur par défaut (default-router) ou à la passerelle (default-gateway) par défaut toutes les paquets qui ne sont pas destinés au réseau proprement dit.

Remarque

Masques réseau uniformes

Lorsque vous configurez votre réseau, veillez toujours à la concordance entre les adresses de diffusion et les masques réseau. Autrement, votre réseau ne fonctionnera pas correctement, puisque les paquets réseau ne pourront pas être routés.

Remarque

Si à présent un des ordinateurs de votre réseau envoie un paquet destiné à l'Internet, ce paquet arrive sur le routeur par défaut. Ce dernier doit être configuré de manière à transmettre aussi ce type de paquets. Pour des raisons de sécurité, un système SUSE LINUXne les transmettra pas par défaut ! Modifiez la variable `IP_FORWARD` dans le fichier `/etc/sysconfig/sysctl` et attribuez-lui la valeur `IP_FORWARD=yes`.

L'ordinateur cible de la connexion ne connaît que votre routeur, et non l'ordinateur expéditeur de votre réseau interne proprement dit. Celui-ci se cache derrière votre routeur. C'est de là que vient le terme de mascarade. Du fait de la traduction d'adresses, l'adresse cible pour les paquets reçus est à nouveau notre routeur. Ce dernier doit reconnaître les paquets et réécrire l'adresse cible de manière à ce qu'ils arrivent sur l'ordinateur qui convient dans le réseau local.

Comme le chemin parcouru par les paquets de l'extérieur vers l'intérieur dépend du tableau de mascarade, il n'est pas possible d'ouvrir une connexion de l'extérieur vers l'intérieur. Il n'y aurait pour cette connexion aucun élément dans le tableau. Une connexion établie possède ainsi un état particulier dans ce tableau, de manière à ce que cet élément de tableau ne puisse être utilisé par une deuxième connexion.

En conséquence, on rencontre à présent des problèmes avec certaines applications, ICQ, CU-SeeMe, IRC (DCC, CTCP) et FTP (en mode PORT). Netscape, le programme FTP standard et beaucoup d'autres applications utilisent le mode PASV qui, en ce qui concerne le filtrage des paquets et la mascarade, rencontre beaucoup moins de problèmes.

27.1.3 Principes de base du pare-feu

Le terme pare-feu recouvre la notion très répandue d'un mécanisme qui relie deux réseaux entre eux, mais en contrôlant le trafic autant que possible. Pour le pare-feu type que nous présentons ici, il serait en fait plus correct de parler de filtre de paquets. Un filtre de paquets régule le passage au moyen de critères tels que le protocole, le port et l'adresse IP. De cette manière, vous pouvez intercepter des paquets qui, en raison de leur adressage, ne devraient pas s'infiltrer dans votre réseau. Si vous souhaitez autoriser les accès à votre serveur web, vous devez ouvrir le port correspondant. Le contenu de ces paquets, s'ils sont adressés correctement (donc avec votre serveur web comme cible), n'est pas contrôlé. Le paquet pourrait très bien contenir une attaque contre un programme CGI de votre serveur web et votre filtre de paquets le laissera passer.

Une structure plus efficace — mais aussi plus complexe — consiste à combiner plusieurs types, un filtre de paquets avec des passerelles applicatives ou des serveurs mandataires supplémentaires. Le filtre de paquets rejette les paquets qui sont envoyés vers des ports non ouverts. Seuls les paquets destinés à une passerelle applicative doivent pouvoir être autorisés à passer. Ce serveur mandataire fonctionne alors comme s'il s'agissait du propre interlocuteur du serveur qui établit une connexion avec nous. En ce sens, un tel serveur mandataire peut être considéré comme une machine de mascarade au niveau du protocole de chaque application. Un exemple de ce type de serveur mandataire est Squid, un serveur mandataire HTTP, pour lequel vous devez configurer votre navigateur de manière à ce que les demandes de pages HTML soient d'abord enregistrées dans la mémoire du serveur mandataire et que, seulement si la page en question n'a pas à y être trouvée, ces demandes soient envoyées sur l'Internet. SuSE proxy-suite (paquetage `proxy-suite`) contient en outre un serveur mandataire pour le protocole FTP.

Nous souhaitons à présent nous concentrer sur le paquetage "filtre de paquets" de SUSE LINUX. Pour obtenir plus d'informations ainsi que d'autres liens à propos des pare-feu, consultez le document Firewall-HOWTO (en anglais) contenu dans le paquetage `howto`. Pour le lire, utilisez la commande `less /usr/share/doc/howto/en/Firewall-HOWTO.gz` si ce paquetage est installé.

27.1.4 SuSEfirewall2

SuSEfirewall2 est un script qui convertit les variables configurées dans `/etc/sysconfig/SuSEfirewall2` en un ensemble de règles iptables. SuSEfirewall2 connaît trois zones de sécurité (cependant, on ne prendra en considération que les deux premières dans l'exemple de configuration suivant) :

Réseau externe L'ordinateur doit être protégé du réseau externe, puisque ce dernier n'est pas sous contrôle à proprement parler. Il est généralement question ici de l'Internet, mais il peut tout aussi bien s'agir d'autres réseaux non protégés (un réseau étendu).

Réseau interne Ici, il est question du véritable réseau, plus généralement dénommé réseau local. Si l'on utilise dans ce réseau des adresses IP du secteur privé (voir section *Masques réseau et routage* page 443), la mise en œuvre de la traduction d'adresses réseau (NAT) s'impose pour pouvoir accéder du le réseau interne vers l'extérieur.

Zone démilitarisée (DMZ) Les ordinateurs qui se trouvent dans cette zone sont accessibles du réseau externe comme du réseau interne mais n'ont aucun accès à l'intranet. Ce type de configuration protège de plus le réseau interne du réseau externe, puisqu'il n'y a aucune possibilité d'accès disponible sur les machines internes à partir des machines de la zone démilitarisée.

Tout trafic réseau qui n'a pas fait l'objet d'une autorisation explicite est interrompu par iptables grâce à l'ensemble de règles. Par conséquent, chaque interface donnée doit être affectée à une des trois zones et il faut définir pour chaque zone donnée quels services ou protocoles doivent être autorisés. L'ensemble de règles ne contrôle toutefois que les paquets créés à l'extérieur. Les paquets générés localement peuvent toujours être envoyés.

La configuration se fait soit avec YaST (voir section *Configuration avec YaST* de la présente page), soit directement dans le fichier `/etc/sysconfig/SuSEfirewall2` qui contient des commentaires détaillés en anglais. Vous trouverez de plus quelques exemples de scénarios dans `/usr/share/doc/SuSEfirewall2/EXAMPLES`

Configuration avec YaST

Remarque

Configuration automatique du pare-feu

YaST démarre automatiquement un pare-feu sur toutes vos interfaces configurées. Dès qu'un service est configuré et activé sur votre serveur, YaST permet d'adapter, au travers des options 'Ouvrir le pare-feu sur les ports sélectionnés' ou 'Ouvrir port sur pare-feu' du module de configuration du serveur, la configuration générée automatiquement. Si un bouton 'Détails du pare-feu' apparaît dans la boîte de dialogue du module du serveur, vous pouvez activer d'autres services ou ports. Le module YaST pour la configuration du pare-feu sert juste à activer ou désactiver le pare-feu ou pour les configurations autonomes.

Remarque

Utilisez le centre de contrôle YaST pour accéder à la configuration en mode graphique. Choisissez dans la catégorie 'Sécurité et utilisateurs' l'option 'Pare-feu'. La configuration se divise en cinq sous-sections :

Reconfiguration/Arrêt Si un SuSEfirewall2 tourne déjà sur votre système parce que vous n'avez pas désactivé la configuration et l'initialisation automatique du pare-feu pendant l'installation, cette boîte de dialogue apparaît.

Vous y décidez si vous voulez commencer à modifier à la main la configuration du pare-feu générée automatiquement par YaST avec ‘Reconfigurer les paramètres du pare-feu’ ou si vous vous voulez arrêter le pare-feu avec ‘Arrêter le pare-feu et le supprimer du processus d’amorçage’ et l’ignorer complètement lors de l’initialisation du système. Si aucun pare-feu ne tourne sur votre système, cette boîte de dialogue n’apparaît pas et la configuration commence avec ‘Paramètres de base’.

Paramètres de base Définissez les interfaces à sécuriser. Si vous devez sécuriser un ordinateur sans réseau interne, n’indiquez que les interfaces avec l’extérieur dans l’Internet. Il est également possible d’indiquer ici plusieurs interfaces par le biais d’une liste dont les éléments sont séparés par des virgules. Si un réseau interne est connecté derrière votre système, vous devez également indiquer les interfaces avec l’intérieur pour vous protéger de ce réseau. Votre système se trouverait alors dans une DMZ. La configuration d’une DMZ ne s’applique généralement que dans des réseaux d’entreprise. Fermez cette boîte de dialogue en cliquant sur ‘Suivant’.

FIG. 27.2: *YaST : SuSEfirewall2 –– Choix des interfaces à sécuriser*

Services Cette option n’a de sens que si vous souhaitez utiliser votre système pour proposer des services qui doivent pouvoir être accessibles par l’Internet (serveur web, serveur de messagerie, etc.). Cochez les cases corres-

pondantes et/ou utilisez l'icône 'Expert...' pour autoriser certains services en fonction de leur numéro de port (pour plus d'informations à ce sujet, reportez-vous au fichier `/etc/services`). Si vous ne souhaitez pas utiliser votre ordinateur en tant que serveur, ne changez rien et fermez cette boîte de dialogue en cliquant sur 'Suivant'.

Fonctionnalités Sélectionnez ici les fonctionnalités les plus importantes que votre pare-feu doit offrir :

'Transmettre des données et mettre en œuvre le mécanisme de mascarade'
Cette option protège les ordinateurs du réseau interne contre l'Internet — tous les services Internet sembleront être utilisés par votre pare-feu, tandis que les ordinateurs internes demeureront invisibles.

'Protéger du réseau interne' Seuls les services autorisés du pare-feu sont disponibles pour les ordinateurs *internes*. Comme il n'est pas possible d'autoriser des services ici, décochez plutôt cette option si vous souhaitez pouvoir accéder au réseau interne.

'Protéger tous les services actifs' Cette option signifie que chaque accès réseau externe aux services TCP et UDP du pare-feu est empêché, à l'exclusion des services que vous avez autorisés de manière explicite au cours de l'étape précédente.

'Autoriser traceroute' Cette option permet de vérifier le routage vers votre pare-feu.

'Gérer le transfert des paquets IPsec comme s'il s'agissait de paquets internes'
Les paquets IPsec cryptés qui ont été déchiffrés avec succès sont traités exactement de la même manière que les paquets provenant de votre réseau interne.

Lorsque vous avez terminé la configuration des fonctionnalités, quittez ce formulaire en cliquant sur 'Suivant'.

Journalisation Définissez ici la portée de la journalisation de votre pare-feu. Avant d'activer les 'Options de débogage', n'oubliez pas que ces fichiers journaux génèrent des quantités de données volumineuses. Une fois la configuration de la journalisation terminée, la configuration de votre pare-feu est terminée. Fermez la boîte de dialogue en cliquant sur 'Suivant' et confirmez le message qui s'affiche à présent pour activer le pare-feu.

Configuration manuelle

Voyons à présent étape par étape une configuration réussie. Nous préciserons, pour chaque point, s'il s'agit de mascarade ou de pare-feu. Dans le fichier de configuration, il est aussi question d'une zone démilitarisée (DMZ, en anglais *demilitarized zone*), que nous n'étudierons pas en détail pour l'instant.

Activez d'abord SuSEfirewall2 avec YaST Runlevel Editor pour votre niveau d'exécution (probablement 3 ou 5). Vous trouverez à cet effet des liens symboliques pour les scripts SuSEfirewall2_* dans les répertoires `/etc/init.d/rc?.d/`.

`FW_DEV_EXT` (pare-feu, mascarade) Il s'agit de l'interface qui conduit à l'Internet. Pour les connexions par modem et à haut débit (ADSL), faites appel au protocole `ppp0` approprié, à `ippp0` pour les connexions RNIS et pour `auto`, ce sera l'interface de la route par défaut (Defaultroute).

`FW_DEV_INT` (pare-feu, mascarade) Indiquez ici l'interface qui pointe sur le réseau "privé" interne (`eth0`). S'il n'existe aucun réseau interne, contentez-vous de laisser ce champ vide.

`FW_ROUTE` (pare-feu, mascarade) Si vous avez besoin de la mascarade, vous devez impérativement indiquer `yes` ici. Vos machines internes ne sont pas visibles de l'extérieur, car elles possèdent des adresses réseau privées (`192.168.x.x`) qui ne sont pas routées sur l'Internet.

Dans le cas d'un pare-feu sans mascarade, ne choisissez ici `yes` que si vous souhaitez autoriser l'accès à votre réseau interne.Vous devez pour cela avoir affecté officiellement des adresses IP aux machines internes. Vous ne devriez normalement *pas* autoriser l'accès de l'extérieur à vos machines internes !

`FW_MASQUERADE` (mascarade) Si vous avez besoin de la mascarade, vous devez indiquer `yes` ici. Notez qu'il s'agit de l'option la plus sûre si les ordinateurs du réseau interne accèdent à l'Internet par l'intermédiaire d'un serveur mandataire.

`FW_MASQ_NETS` (mascarade) Indiquez ici les ordinateurs ou les réseaux pour lesquels il faut faire de la mascarade. Séparez chaque saisie par un espace. Par exemple :

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

`FW_PROTECT_FROM_INTERNAL` (pare-feu)
Saisissez `yes` ici si vous souhaitez aussi protéger l'ordinateur utilisé comme

pare-feu contre les tentatives d'accès en provenance du réseau interne. Vous devez alors autoriser les services disponibles pour le réseau interne. Voir également FW_SERVICES_INTERNAL_TCP et FW_SERVICES_-INTERNAL_UDP.

FW_AUTOPROTECT_SERVICES (pare-feu)
Laissez en principe cette option sur yes, pour générer automatiquement des règles explicites pour les services actuels.

FW_SERVICES_EXT_TCP (pare-feu) Indiquez ici les ports TCP auxquels on doit pouvoir accéder. Pour un simple ordinateur domestique qui n'a pas à proposer de services, vous n'avez la plupart du temps rien à indiquer.

FW_SERVICES_EXT_UDP (pare-feu) Si vous n'utilisez pas de serveur de noms auquel on doit pouvoir accéder de l'extérieur, ne renseignez pas ce champ. Sinon, ajoutez ici les ports UDP requis.

FW_SERVICES_INT_TCP (pare-feu) C'est ici que sont déclarés les services disponibles pour le réseau interne. Les indications sont analogues à celles qui se trouvent sous FW_SERVICES_EXT_TCP, mais font cette fois référence au réseau *interne*. Cette variable ne doit alors être configurée que si FW_-PROTECT_FROM_INTERNAL a été activée.

FW_SERVICES_INT_UDP (pare-feu) Voir ci-dessus.

FW_STOP_KEEP_ROUTING_STATE (pare-feu)
Si vous accédez automatiquement à l'Internet par diald ou par le RNIS (connexion à la demande), indiquez yes ici.

La configuration est à présent terminée. N'oubliez pas de tester le pare-feu. En tant qu'utilisateur root, appelez la commande SuSEfirewall2 start pour créer les règles. Avec un telnet de l'extérieur, vérifiez si cette connexion est aussi refusée *de facto* : vous devriez alors voir dans le fichier /var/log/messages des lignes similaires à celles-ci :

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFLT IN=eth0 OUT=
MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF
PROTO=TCP SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0 OPT
(020405B40402080A061AFEBC0000000001030300)
```

27.1.5 Informations complémentaires

Vous trouverez de la documentation appropriée et à jour concernant le paquetage SuSEfirewall2 dans /usr/share/doc/packages/SuSEfirewall2.

Les livres, articles et sites web suivants vous aideront à mieux appréhenderiptables et netfilter :

Das Firewall-Buch Barth, Wolfgang: *Das Firewall-Buch* 2., überarbeitete Auflage SUSE PRESS, 2003 - (ISBN 3-899900-44-8)

`http://www.netfilter.org` La page d'accueil des projets netfilter/iptables. Vous y trouverez de la documentation en abondance en différentes langues.

27.2 SSH – travailler en réseau en toute sécurité

Lorsque l'on travaille en réseau, il est fréquemment nécessaire d'accéder à des systèmes distants. L'utilisateur doit alors s'identifier à l'aide de son login et d'un mot de passe. Ces données sensibles étant transmises en clair, sans être chiffrées, elles risquent d'être interceptées à tout moment par des tiers et d'être utilisées dans l'intérêt de ces derniers, par exemple en exploitant l'accès de l'utilisateur à son insu. Indépendamment du fait que les attaquants peuvent ainsi prendre connaissance de l'ensemble des données privées de l'utilisateur, ils peuvent utiliser l'accès ainsi obtenu pour attaquer à partir de là d'autres systèmes ou pour usurper les comptes administrateur ou root sur le système visé. Avant cela, c'était le programme telnet, dépourvu de mécanisme de chiffrement ou de sécurité contre l'écoute des liaisons, qui était utilisé pour connecter deux machines distantes. De même, ni les connexions FTP simples ni les copies entre machines distantes ne sont protégées.

Le programme SSH apporte la protection requise. L'authentification complète, assurée généralement par un nom d'utilisateur et un mot de passe, ainsi que la communication sont chiffrées. Même s'il reste possible, pour un tiers, d'intercepter les données transmises, leur contenu ne peut pas être déchiffré, faute de disposer de la clé appropriée. Cette méthode permet ainsi des communications sécurisées sur des réseaux non sécurisés tels que le réseau Internet. SUSE LINUX propose pour cela le paquetage OpenSSH.

27.2.1 Le paquetage OpenSSH

Le paquetage OpenSSH est installé par défaut sous SUSE LINUX. Vous disposez ainsi des programmes ssh, scp et sftp, afin de remplacer telnet, rlogin, rsh, rcp et ftp.

27.2.2 Le programme ssh

Le programme ssh permet de se connecter à un système distant et d'y travailler de façon interactive. Il constitue ainsi une alternative à telnet et à rlogin. Inspiré du programme rlogin, le lien symbolique supplémentaire slogin fait également référence à ssh. Ainsi, la commande `ssh soleil` permet de se connecter sur la machine soleil. La demande de connexion doit ensuite être autorisée par un mot de passe validé par le système soleil.

Une fois authentifié, vous pouvez alors y travailler soit à partir de la ligne de commande soit en mode graphique, par exemple avec YaST. Dans le cas où votre nom d'utilisateur sur la machine locale et celui sur le système distant sont différents, vous pouvez spécifier un autre nom, par exemple `ssh -l august soleil` ou `ssh august@soleil`.

D'autre part, le programme ssh offre une possibilité connue avec rsh et consistant à exécuter des commandes sur un autre système. Dans l'exemple suivant, la commande `uptime` est exécutée sur la machine soleil et un répertoire nommé `tmp` est créé. Le programme affiche sur le terminal local de la machine terre.

```
ssh soleil "uptime; mkdir tmp"
tux@soleil's password:
1:21pm  up  2:17,  9 users,  load average: 0.15, 0.04, 0.02
```

Dans cette commande, les guillemets sont requis afin de regrouper les deux instructions en une commande unique. C'est nécessaire pour permettre l'exécution de la seconde commande sur la machine soleil.

27.2.3 scp – Copie sécurisée

Le programme scp vous permet de copier des fichiers sur une machine distante. scp constitue une alternative sécurisée et chiffrée au programme rcp. Ainsi, la commande `scp MonCourrier.tex soleil:` copie le fichier `MonCourrier.tex` de la machine terre sur la machine soleil. Dans le cas où le nom d'utilisateur sur terre est différent de celui sur soleil, utilisez pour la commande scp la notation `NomUtilisateur@NomMachine`. L'option `-l` n'est pas disponible.

Après avoir saisi votre mot de passe, le programme scp commence à transférer les données en affichant l'avancement à l'aide d'une jauge formée d'astérisques et progressant de gauche à droite. Dans le même temps, la durée estimée restant jusqu'à la fin de la transmission (*estimated time of arrival*) est affichée sur la droite. Il est également possible d'inhiber l'affichage à l'aide de l'option `-q`.

La copie de fichiers individuels n'est pas la seule opération que scp permet d'effectuer. En effet, il est également possible de transférer récursivement des répertoires entiers : ainsi, la commande `scp -r src/ soleil:backup/` copie la totalité du répertoire `src/`, y compris les sous-répertoires présents sur la machine soleil, dans le sous-répertoire `backup/`. Ce dernier est créé automatiquement s'il n'existe pas encore.

L'option `-p` permet à scp de conserver l'horodatage des fichiers. L'option `-C` permet de compresser les fichiers à transférer, ce qui, d'un côté, permet de réduire le volume de données à transférer, mais de l'autre, impose une charge supérieure au système.

27.2.4 sftp - Transfert de fichiers sécurisé

On peut aussi utiliser le programme sftp pour transférer les données de façon sécurisée. sftp propose une session à l'intérieur de laquelle on peut utiliser plusieurs des commandes ftp bien connues. Par rapport à scp, le principal avantage est de pouvoir transférer des données lorsqu'on ne connaît pas le nom de fichier.

27.2.5 Le démon SSH (sshd) – côté serveur

Pour pouvoir fonctionner, ssh et scp, les programmes clients du paquetage SSH ont besoin que le démon SSH qui est un serveur s'exécute en arrière-plan. Celui-ci attend les connexions sur le `port TCP/IP numéro 22`.

La première fois qu'il est démarré, le démon génère trois paires de clés. Celles-ci comportent une partie privée et une partie publique (*public*). il s'agit donc d'une méthode à clé publique. Pour assurer la sécurité de l'application à l'aide de SSH, seul l'administrateur doit pouvoir voir les fichiers de la clé privée. Les privilèges correspondant sont définis par défaut de manière restrictive. Les clés privées sont utilisées en local uniquement par le démon SSH et ne doivent être communiquées à personne. En revanche, la partie publique de la clé (identifiable par l'extension de fichier `.pub`) peut être communiquée à vos correspondants et peut être lue par tous les utilisateurs.

Une connexion est créée par le client SSH. Le démon SSH en attente et le client SSH à l'origine de la demande échangent des données d'identification en vue de comparer la version du protocole et du logiciel et d'éviter une connexion sur un mauvais port. La réponse étant apportée par un processus fils du démon SSH initial, il est possible d'avoir plusieurs connexions SSH simultanément.

Afin d'assurer la communication entre le serveur SSH et le client SSH, le programme OpenSSH prend en charge les versions 1 et 2 du protocole SSH. Après avoir réinstallé SUSE LINUX, c'est la version 2 actuelle du protocole qui est automatiquement utilisée. Si vous souhaitez continuer à utiliser SSH1 après une mise à jour, veuillez suivre les instructions données dans `/usr/share/doc/packages/openssh/README.SuSE`. Vous y trouverez également la marche à suivre pour passer d'un environnement SSH 1 à un environnement SSH 2 opérationnel.

Si vous utilisez le protocole SSH version 1, le serveur envoie sa clé d'hôte (`host key`) publique ainsi qu'une clé de serveur (`server key`) générée toutes les heures par le démon SSH. Grâce à ces deux clés, le client SSH chiffre (*encrypts*) une clé de session (*session key*) et l'envoie au serveur SSH.Il communique par ailleurs au serveur la méthode de chiffrement (*cipher*) choisie.

Le protocole SSH version 2 fonctionne sans la clé de serveur (`server key`). Ce dispositif est remplacé par un algorithme de Diffie-Hellman destiné à l'échange des clés.

Il n'est pas possible de déduire les clés privées de l'hôte et du serveur, indispensables pour déchiffrer la clé de session, à partir des parties publiques de la clé. Ainsi, seul le démon SSH contacté est en mesure de déchiffrer la clé de session à l'aide de ses clés privées (voir `man /usr/share/doc/packages/openssh/RFC.nroff`). Cette phase préparatoire de la connexion peut être aisément tracée à l'aide de l'option de débogage `-v` du programme client SSH. Par défaut, c'est la version 2 du protocole SSH qui est utilisée, même si le paramètre `-1` permet d'imposer la version 1 du protocole SSH. En stockant après le premier contact toutes les clés publiques dans `~/.ssh/known_hosts`, il est possible de contrer les attaques de type interception (*man-in-the-middle*). Les serveurs SSH tentant d'usurper le nom et l'adresse IP d'un autre sont démasqués avec un avertissement sans ambiguïté. Ils sont identifiés par leur clé d'hôte différente de `~/.ssh/known_hosts` ou sont dans l'impossibilité de déchiffrer la clé de session convenue, faute de connaître la partie privée adéquate.

Il est recommandé d'archiver sur un support externe et en les protégeant comme il se doit les clés privées et publiques de `/etc/ssh/`. Vous pouvez ainsi constater d'éventuelles modifications apportées aux clés et récupérer les anciennes clés dans le cas où vous auriez à réinstaller votre système. Cette précaution épargnera aux utilisateurs l'inquiétude que peuvent causer des messages d'avertissement. Dans le cas où vous avez la certitude d'avoir à faire au bon serveur SSH en dépit de l'avertissement, la ligne correspondante doit être retirée du fichier `~/.ssh/known_hosts`.

27.2.6 Mécanismes d'authentification de SSH

L'authentification proprement dite intervient à cet instant. Sous sa forme la plus simple, elle consiste à saisir un mot de passe, de manière analogue à la procédure illustrée dans les exemples précédents. L'objet de SSH était de mettre en place un logiciel sécurisé tout en restant simple à utiliser. De manière analogue aux programmes rsh et rlogin à remplacer, il importe donc que SSH offre une méthode d'authentification simple à utiliser au quotidien. Cet objectif est réalisé par SSH à l'aide d'une autre paire de clés générée ici par l'utilisateur. Le paquetage SSH offre pour cela l'utilitaire ssh-keygen. La paire de clés est générée après avoir saisi `ssh-keygen -t rsa` ou `ssh-keygen -t dsa` et vous devez indiquer un nom pour le fichier de base destiné à stocker les clés :

```
Enter file in which to save the key (/home/tux/.ssh/id_rsa):
```

Validez la valeur par défaut et lorsque l'on vous demande une phrase de passe, donnez-en une. Même si le logiciel accepte une phrase de passe vide, nous conseillons de choisir un texte de 10 à 30 signes. Dans la mesure du possible, évitez d'utiliser des mots ou phrases courts et simples. Après la saisie, vous devez vérifier la première saisie en effectuant une seconde saisie. Vous devez ensuite indiquer l'emplacement de la clé privée et publique, en l'occurrence les fichiers `id_rsa` et `id_rsa.pub`.

```
Enter same passphrase again:
Your identification has been saved in /home/tux/.ssh/id_rsa
Your public key has been saved in /home/tux/.ssh/id_rsa.pub.
The key fingerprint is:
79:c1:79:b2:e1:c8:20:c1:89:0f:99:94:a8:4e:da:e8 tux@soleil
```

Utilisez la commande `ssh-keygen -p -t rsa` ou `ssh-keygen -p -t dsa` pour modifier votre ancienne phrase de passe. Copiez la partie publique de la clé (dans notre exemple `id_rsa.pub`) sur la machine distante et enregistrez-la sous `~/.ssh/authorized_keys`. Lors de la prochaine connexion, vous devrez saisir votre phrase de passe. Dans le cas contraire, vérifiez l'emplacement et le contenu des fichiers dont il vient d'être question.

Cette procédure s'avère plus lourde, à la longue, que celle consistant à saisir un mot de passe. Le paquetage SSH s'accompagne d'un utilitaire supplémentaire, ssh-agent, proposant des clés privées valables pour la durée d'une session X. Pour cela, le programme X est démarré comme processus fils de ssh-agent. La méthode la plus simple pour mettre cette fonctionnalité en place consiste à placer

au début du fichier `.xsession` la variable `usessh` en fixant sa valeur à `yes` et à vous connecter à partir d'un gestionnaire de connexions tel que KDM ou XDM. Autre possibilité : utiliser ssh-agent startx.

Vous pouvez à présent utiliser ssh ou scp comme à l'accoutumée. Si vous avez partagé votre clé publique comme indiqué précédemment, vous devriez être dispensé de donner votre mot de passe. Lorsque vous vous éloignez de votre ordinateur, prenez toutefois la précaution de terminer votre session X ou de la verrouiller à l'aide d'un économiseur d'écran protégé par mot de passe, par exemple xlock.

Toutes les modifications importantes résultant de l'utilisation du protocole SSH version 2 sont également récapitulées dans le fichier `/usr/share/doc/packages/openssh/README.SuSE`.

27.2.7 Redirections : de X, de l'authentification, etc.

Indépendamment des améliorations en matière de sécurité dont il vient d'être question, le programme ssh facilite également l'utilisation d'applications X distantes. Lorsque vous appelez `ssh` avec l'option `-X`, la variable DISPLAY est automatiquement définie sur le système distant et toutes les sorties X sont redirigées vers la machine source à travers la connexion ssh existante. Cette fonctionnalité pratique interdit dans le même temps les possibilités d'écoute qui existaient auparavant, lorsque l'on appelait à distance des applications X pour les afficher en local.

En définissant l'option `-A`, le mécanisme d'authentification de l'agent ssh-agent est repris sur la machine suivante. Vous pouvez ainsi passer d'une machine à l'autre sans être obligé de saisir de mot de passe. Ceci n'est toutefois possible que si vous avez préalablement copié et convenablement enregistré votre clé publique sur les machines cibles concernées.

Par précaution, les deux mécanismes sont désactivés par défaut, même s'ils peuvent être activés de manière permanente dans le fichier de configuration système `/etc/ssh/ssh_config` ou dans le fichier utilisateur `~/.ssh/config`.

Le programme ssh peut également être utilisé afin de permettre des redirections de connexions TCP/IP. Exemple d'application : la redirection des ports SMTP et POP3 :

```
ssh -L 25:soleil:25 terre
```

Dans cet exemple, toutes les connexions vers terre port 25 SMTP sont redirigées vers le port SMTP de soleil via le canal chiffré. Cette possibilité est particulièrement utile pour les utilisateurs de serveurs SMTP dépourvus de fonctions SMTP-AUTH ou POP-before-SMTP. Ainsi, le courrier peut être transmis de n'importe quel endroit disposant d'une connexion réseau afin d'être acheminé par le serveur de messagerie domestique. De manière analogue, la commande suivante permet de rediriger toutes les requêtes POP3 (port 110) adressées à terre vers le port POP3 de soleil :

```
ssh -L 110:soleil:110 terre
```

Vous devez exécuter ces deux exemples en tant qu'utilisateur `root` ; la connexion s'effectuant sur des ports locaux privilégiés. Lorsque la connexion SSH est établie, l'utilisateur envoie et reçoit les messages à partir de son compte habituel. L'hôte SMTP et POP3 doit être configuré à `localhost`. Vous trouverez des informations complémentaires dans les pages de manuels des différents programmes et dans les fichiers sous `/usr/share/doc/packages/openssh`.

27.3 Chiffrer les partitions et les fichiers

27.3.1 Scénarios d'utilisation

Chaque utilisateur possède des données sensibles qu'un tiers non autorisé ne doit pas pouvoir consulter. Plus vous travaillez en réseau et plus vous vous déplacez souvent, plus vous devriez être méfiant à propos de vos données. Le chiffrement des fichiers ou de toute la partition se justifie toujours lorsque un tiers a accès au système, que ce soit au moyen d'une connexion réseau ou en y accédant physiquement. La liste suivante décrit des scénarios d'utilisation envisageables.

Ordinateurs portables Si vous vous déplacez souvent lorsque vous travaillez et si vous transportez sur votre ordinateur portable des données sensibles, chiffrez la partition correspondante sur le disque dur. Si vous perdez votre ordinateur portable ou si on vous le vole, vos données sont protégée contre les tiers lorsqu'elles se trouvent sur une partition chiffrée ou dans un fichier sur un système de fichiers chiffré.

Medias d'échange Les clés USB ou les disques durs externes risquent d'être volées de la même manière que les ordinateurs portables. Un système de fichiers chiffré vous protège aussi contre les tiers.

27.3.2 Installation avec YaST

YaST vous permet de chiffrer vos fichiers ou vos partitions aussi bien durant l'installation que sur un système installé. On peut toujours chiffrer un fichier, car les fichiers s'intègrent sans problèmes dans le schéma de partitions existant ; une partition chiffrée ne peut être mise en place que si vous avez à votre disposition dans votre schéma de partitions une partition dédiée. Le partitionnement par défaut que YaST propose à l'installation ne prévoit pas de partition chiffrée. Vous devez donc modifier le partitionnement à la main pour pouvoir mettre en place une partition chiffrée.

Mise en place d'une partition chiffrée au cours de l'installation

Dans la boîte de dialogue pour le partitionnement expert ('Partitionnement en mode expert') décrite dans la section *Partitionnement pour experts avec YaST* page 21 choisissez 'Créer' pour créer une partition chiffrée, comme vous le feriez pour une partition normale. Dans la boîte de dialogue suivant l'enregistrement des partitions, indiquez le type de formatage souhaité et le point de montage de la nouvelle partition et cliquez sur 'Système de fichiers crypté'. Indiquez dans la boîte de dialogue suivante le mot de passe utilisé et répétez-le pour des raisons de sécurité. Dès que vous quittez la boîte de dialogue de partitionnement avec 'OK', la nouvelle partition chiffrée est créée. Au prochaine amorçage du système, le mot de passe vous sera demandé avant le montage de la partition. Si la première demande de mot de passe échoue, le mot de passe vous sera à nouveau demandé.

Attention

Indiquer le mot de passe

Lorsque vous saisissez le mot de passe, lisez attentivement les avertissements au sujet de la sécurité des mots de passe et retenez bien le mot de passe. Si vous oubliez le mot de passe, il vous sera impossible d'accéder à vos données chiffrées.

Attention

Si vous ne désirez pas monter la partition à l'amorçage, laissez la zone de mot de passe vide. Répondez par la négative lorsque le système vous demande si vous voulez à nouveau saisir un mot de passe. Votre système de données chiffré ne sera alors pas monté et le reste du système sera néanmoins amorcé. Le montage automatique d'une partition à l'amorçage affaiblit la stratégie de sécurité sous-jacente, car la partition est disponible pour tous les utilisateurs dès que l'amorçage du système est terminé si elle n'est pas démontée à nouveau immédiatement

après y avoir accédé. Il en découle que cette option ne se justifie que si vous voulez assurer contre le vol un appareil mobile sur lequel vous êtes sûr d'être le seul à travailler et dont le système était arrêté au moment du vol.

Si vous ne voulez pas donner le mot de passe à chaque amorçage du système et si la partition chiffrée ne doit être montée qu'à la demande, choisissez dans la boîte de dialogue 'Options Fstab' l'option 'Ne pas monter au démarrage du système'. La partition correspondante ne sera pas prise en compte lors de L'amorçage du système. Pour y donner accès, vous devez la monter explicitement : `mount <nom-de-la-partition> <point-de-montage>`. La partition est montée après la saisie du mot de passe et elle est à votre disposition. Si vous démontez la partition après y avoir accédé avec `umount nom-de-la-partition`, vous évitez que d'autres utilisateurs puissent y obtenir accès.

Installation d'une partition chiffrée en cours de fonctionnement

Attention

Activer le chiffrement pendant le fonctionnement

Vous pouvez créer une partition chiffrée pendant le fonctionnement de la même manière que pendant l'installation. Soyez toutefois conscient que lors du chiffrement sur une partition déjà existante, les données existantes sont perdues.

Attention

Lancez dans le système en fonctionnement le module de YaST 'Partitionnement' dans le menu 'Système' du centre de contrôle de YaST. Vous devez répondre 'Oui' à la demande de confirmation sur le partitionnement d'un système en cours de fonctionnement. Vous accédez alors à une vue d'ensemble de toutes les partitions disponibles. Au lieu de cliquer sur 'Créer' comme auparavant, cliquez sur 'Modifier'. La suite se déroule comme décrit précédemment. Le montage de la partition lors de l'amorçage ou à part à la demande est également paramétré dans la suite comme décrit précédemment.

Mise en place de fichiers chiffrés

Au lieu d'une partition entière vous pouvez aussi créer des systèmes de fichiers chiffrés contenus dans des fichiers. Ils peuvent alors contenir vos données sensibles. Le point de départ est comme pour les partitions chiffrées la boîte de dialogue de YaST 'Partitionnement en mode expert'. Choisissez 'Fichier chiffrement' et saisissez dans la boîte de dialogue suivante le chemin vers ce fichier. Réglez-y

également les besoins en espace disque du fichier. Acceptez les réglages prédéfinis pour le formatage et le système de fichiers. Indiquez finalement si et où le système de fichier doit être monté au démarrage du système ou s'il doit être monté et démonté à part.

27.3.3 Chiffrer le contenu de médias d'échange

Les médias d'échange comme les disques dur amovibles ou les clés USB sont reconnus par YaST de la même manière que les autres disques durs. Si vous voulez chiffrer des fichiers ou des partitions sur de tels médias, procédez sur le modèle de ce qui précède. Il faut absolument activer dans les 'Options Fstab' l'option 'Ne pas monter au démarrage du système' afin que de tels médias ne soient pas mis à disposition comme il est d'usage à l'amorçage du système, mais soient mis en ligne en cours de fonctionnement.

27.4 La sécurité est une affaire de confiance

27.4.1 Principes fondamentaux

L'une des caractéristiques principales d'un système Linux/Unix est que plusieurs utilisateurs (*multiuser*) peuvent effectuer plusieurs tâches simultanément sur le même ordinateur (*multitasking*). Le réseau est de plus transparent au système d'exploitation, si bien que, très souvent, les utilisateurs ne savent pas précisément si les données ou les applications qu'ils utilisent se trouvent en local sur leur ordinateur ou leur sont fournies par le réseau.

Pour que plusieurs utilisateurs puissent travailler sur un même système, leurs données doivent pouvoir être gérées de manière séparée. Il s'agit ici, entre autres, de considérations relatives à la sécurité et à la protection de la vie privée. La sûreté des données avait déjà un sens quand les ordinateurs n'étaient pas mis en réseau. En cas de perte ou de défaillance des supports de données (généralement, des disques durs), les données les plus importantes devaient pouvoir toujours être disponibles, même si ce type de défaillance pouvait avoir pour conséquence la panne passagère d'une infrastructure plus importante.

Même si ce chapitre du manuel SUSE concerne principalement la confidentialité des données et la protection de la vie privée de l'utilisateur, il faut insister

sur le fait qu'une politique de sécurité globale doit toujours comprendre, en tant que partie intégrante du système, un système de sauvegarde régulier, éprouvé et qui fonctionne correctement. Sans cette sauvegarde des données, on serait en difficulté pour accéder à nouveau aux données non seulement dans le cas d'une défaillance du matériel, mais également quand on soupçonne que quelqu'un a réussi à accéder aux données de manière illégale.

27.4.2 Sécurité locale et sécurité du réseau

Il existe plusieurs possibilités pour accéder aux données :

- La communication avec quelqu'un qui a accès aux informations souhaitées ou qui a accès à des données particulières sur un ordinateur,
- directement sur le clavier et l'écran d'un ordinateur (accès physique),
- par une interface série ou
- en réseau.

Tous ces cas ont un point commun : vous devez vous identifier en tant qu'utilisateur avant d'obtenir l'accès aux ressources ou aux données. Un serveur Web peut être envisagé différemment, mais vous ne souhaitez très certainement pas que le serveur Web révèle vos informations personnelles à n'importe quel internaute.

Le premier des cas mentionnés ci-dessus est celui qui fait le plus appel au facteur humain : comme dans une banque, vous devez fournir à un employé autorisé à accéder à votre compte une signature, un numéro d'identification personnel ou un mot de passe, pour prouver que vous êtes bien la personne que vous affirmez être. La plupart du temps, cela peut se faire en mentionnant certaines connaissances ou en obtenant, par la ruse ou en faisant preuve de rhétorique, la confiance d'une personne détenant les connaissances nécessaires, pour que cette personne communique d'autres informations, parfois à l'insu de la victime. Dans le monde des pirates, on parle de Social Engineering (ingénierie sociale). Contre ce type d'attaque, la seule solution consiste à faire attention, à manipuler avec précaution vos informations et à tenir votre langue. Les effractions dans les systèmes informatiques sont souvent précédées d'une variante d'attaque d'ingénierie sociale dirigée contre le personnel d'accueil, les prestataires de service de la société ou les membres de la famille et qui n'est décelée, la plupart du temps, que beaucoup plus tard.

Quelqu'un qui souhaite accéder aux données de manière illégale pourrait très bien aussi utiliser la méthode la plus traditionnelle qui soit, puisque le matériel lui-même est un point d'attaque. L'ordinateur doit être protégé contre les vols, les

échanges et les sabotages partiels ou totaux (ainsi que la sauvegarde des données !) – sans oublier une éventuelle connexion réseau disponible ou un câble électrique. En outre, le démarrage doit être sécurisé car des combinaisons de touches connues peuvent entraîner des réactions spéciales de l'ordinateur. Le fait de définir des mots de passe pour le BIOS et le gestionnaire d'amorçage protège contre de telles tentatives.

Les interfaces série avec des terminaux série sont certes toujours utiles de nos jours, mais ne sont pratiquement plus installées sur les nouveaux postes de travail. Un terminal série représente un type d'accès particulier : il ne s'agit pas d'une interface réseau dans la mesure où aucun protocole réseau n'est utilisé pour la communication entre les unités système. Un simple câble (ou une interface infrarouge) est utilisé comme moyen de transmission pour les signaux simples.Le câble même est ainsi le point d'attaque le plus simple à utiliser : il suffit d'y connecter une vieille imprimante pour enregistrer la communication. L'exploitation de cette imprimante ne se fait naturellement pas sans efforts.

Comme l'ouverture d'un fichier sur un ordinateur implique d'autres limitations d'accès que l'ouverture d'une connexion réseau à un service sur un ordinateur, il est nécessaire de bien distinguer entre sécurité locale et sécurité réseau. La ligne de séparation est le point où les données doivent être mises en paquets pour pouvoir être envoyées et utilisées.

Sécurité locale

Il s'agit de la sécurité locale avec les éléments physiques sur lesquels l'ordinateur est installé. Nous partons du principe que vous avez construit votre ordinateur de manière à ce que son niveau de sécurité suffise à vos exigences. Lorsque l'on parle de sécurité locale, cela consiste à séparer les différents utilisateurs les uns des autres de manière à ce qu'aucun utilisateur ne puisse s'accaparer les droits ou l'identité d'un autre utilisateur. Cela s'applique dans tous les cas, et en particulier, naturellement, aux droits de l'utilisateur `root` en effet, cet utilisateur possède les pleins pouvoirs dans le système ; il peut notamment, sans mot de passe, prendre l'identité de n'importe quel utilisateur local et lire chaque fichier local.

Mots de passe

Votre système Linux n'enregistre pas les mots de passe en texte clair pour ensuite comparer le mot de passe saisi avec celui qui est enregistré. En cas de vol du fichier dans lequel sont enregistrés les mots de passe, tous les comptes de votre système seraient compromis. Au contraire, votre mot de passe est enregistré sous sa forme chiffrée et à chaque fois que vous saisissez votre mot de passe, il est à

nouveau chiffré et le résultat est comparé avec ce qui est enregistré en tant que mot de passe chiffré. Cela n'a naturellement un sens que s'il n'est pas possible de calculer le mot de passe en clair à partir du mot de passe chiffré. On utilise à cet effet des algorithmes à trappe qui ne fonctionnent qu'à sens unique. Un attaquant ayant pris possession du mot de passe chiffré ne peut pas simplement calculer et obtenir le mot de passe, il doit en revanche essayer toutes les combinaisons de lettres possibles pour un mot de passe pour trouver lequel, une fois codé, ressemble à celui qu'il détient. Avec des mots de passe de huit lettres, il existe un nombre considérable de combinaisons possibles.

L'un des arguments pour la sécurité de cette méthode dans les années 70 était que l'algorithme utilisé était particulièrement lent et qu'il fallait un temps de l'ordre de la seconde pour chiffrer un mot de passe. Les ordinateurs actuels peuvent sans effort réaliser de plusieurs milliers à plusieurs millions de chiffrements par seconde. C'est pour cette raison que les mots de passe chiffrés ne doivent pas être visibles de tous les utilisateurs (un utilisateur normal ne peut pas lire `/etc/shadow`) et les mots de passe ne doivent pas être faciles à deviner dans le cas où les mots de passe chiffrés deviendraient lisibles suite à une erreur. Un mot de passe tel que fantaisie écrit sous la forme de f@nt@is13 n'est pas très utile : ce type de règles d'échange peut facilement être déchiffré par des programmes de craquage qui utilisent des dictionnaires. Il est préférable d'utiliser des combinaisons de lettres qui ne constituent pas un mot connu et qui n'ont une signification personnelle que pour l'utilisateur, comme les premières lettres des mots d'une phrase ou par exemple un titre de livre comme Le nom de la rose d'Umberto Eco. Vous pourriez ainsi obtenir un bon mot de passe : LNdlRdUE9. Un mot de passe tel que bonvin ou Jasmin76 pourrait facilement être deviné par quelqu'un vous connaissant ne serait-ce que superficiellement.

Le processus d'amorçage

Interdisez tout démarrage à partir d'une disquette ou d'un cédérom en démontant les lecteurs correspondants ou en définissant un mot de passe du BIOS et en n'autorisant dans le BIOS que l'amorçage à partir du disque dur.

Généralement, les systèmes Linux démarrent avec un gestionnaire de démarrage qui permet de passer des options supplémentaires au noyau à démarrer. Ces options sont périlleuses en termes de sécurité car non seulement le noyau s'exécute avec les droits de l'utilisateur `root` mais il offre, dès le début, les droits de l'utilisateur `root`. Si vous utilisez GRUB comme chargeur d'amorçage, vous pouvez l'éviter en saisissant un mot de passe supplémentaire dans `/boot/grub/menu.lst` (voir *Créer un mot de passe d'amorçage* page 218).

Droits d'accès

Un principe consiste à toujours travailler avec les privilèges les plus bas possibles pour une tâche donnée. Il n'est effectivement absolument pas nécessaire de lire et d'écrire son courrier en tant que super-utilisateur. Quand le programme de messagerie (MUA, Mail User Agent) que vous utilisez comporte une erreur, cette erreur se répercute avec exactement les droits que vous aviez au moment de l'accès. Cela permet aussi de limiter les dégâts.

Les droits individuels des plus de 200 000 fichiers d'une distribution SUSE sont attribués avec soin. L'administrateur d'un système ne doit installer de logiciels supplémentaires ou d'autres fichiers qu'avec la plus grande précaution et faire particulièrement attention aux droits attribués aux fichiers. Les administrateurs expérimentés et soucieux de la sécurité utilisent toujours l'option `-l` de la commande `ls` pour obtenir une liste complète des fichiers et de leurs droits d'accès afin de pouvoir reconnaître immédiatement les droits de fichiers mal définis. Un attribut mal défini ne signifie pas seulement que les fichiers peuvent être modifiés ou supprimés, mais également que les fichiers modifiés peuvent être exécutés par l'utilisateur `root` ou, dans le cas de fichiers de configuration de programmes, utilisés en tant qu'utilisateur `root`. Cela permettrait à un attaquant d'augmenter ses droits de façon considérable. On appelle ce genre d'attaque des œufs de coucou parce que le programme (l'œuf) est exécuté (couvé) par un utilisateur étranger (l'oiseau), un peu comme un coucou se débrouille pour faire couver ses œufs par d'autres oiseaux.

Les systèmes SUSE disposent des fichiers `permissions`, `permissions.easy`, `permissions.secure` et `permissions.paranoid` dans le répertoire `/etc`. Dans ces fichiers sont définis des droits importants tels que les répertoires dans lesquels tout utilisateur a des droits d'écriture, ou les bits "setuser-ID" des fichiers. Ces bits de changement d'identité font qu'un programme ne s'exécute pas avec les droits du propriétaire du processus qui l'a démarré mais avec les droits du propriétaire du fichier, et c'est généralement l'utilisateur `root`. L'administrateur dispose du fichier `/etc/permissions.local` dans lequel il peut procéder à ses propres modifications.

Vous pouvez également choisir confortablement avec YaST dans l'option de menu 'Sécurité' lequel de ces fichiers sera utilisé par les programmes de configuration de SUSE pour l'attribution des droits. Vous trouverez plus d'informations à ce sujet directement dans le fichier `/etc/permissions` et la page de manuel de la commande `chmod` (`man chmod`).

Débordements de tampon, bogues dans des chaînes de format

À chaque fois qu'un programme traite des données qui se trouvent ou se trouvaient sous le contrôle d'un utilisateur dans un format donné, nous vous recommandons la plus grande vigilance. Le programmeur de l'application aussi doit faire preuve de vigilance : il doit s'assurer que les données sont correctement interprétées par le programme, qu'elles n'ont à aucun moment été écrites dans un espace mémoire trop petit et qu'il transmet les données d'une manière cohérente à l'aide de son propre programme et des interfaces définies à cet effet.

Il y a débordement de tampon (*buffer overflow*) quand, lors de l'écriture à l'intérieur d'une mémoire tampon, on ne fait pas attention à la taille réelle du tampon. Il se peut que les données (qui proviennent de l'utilisateur) nécessitent un peu plus de place que disponible dans le tampon. Avec ce débordement de tampon au delà de ses capacités, il se peut qu'un programme, du fait des données qu'il doit en théorie seulement traiter, exécute des morceaux de code choisis par l'utilisateur et non par le programmeur. Il s'agit d'une erreur grave notamment quand le programme fonctionne avec des droits particuliers (reportez-vous à la section *Droits d'accès* page précédente). Les bogues dans les chaînes de format fonctionnent quelque peu différemment mais à nouveau les données saisies par l'utilisateur peuvent détourner le programme de sa vocation d'origine.

Ces erreurs de programmation sont normalement exploitées par les programmes exécutés avec des privilèges élevés, comme par exemple les programmes setuid et setgid. Vous pouvez donc vous protéger ainsi que votre système contre ce type d'erreurs en éliminant les droits d'exécution particuliers des programmes. Ici aussi s'applique donc le principe des privilèges les plus restreints possibles (reportez-vous à la section *Droits d'accès* page précédente).

Comme les débordements de tampon et les bogues dans les chaînes de format sont des erreurs qui se présentent lors du traitement des données utilisateur, elles ne sont pas nécessairement exploitables uniquement quand on dispose déjà d'un accès à un login local. Beaucoup des erreurs connues peuvent être exploitées par l'intermédiaire d'une connexion réseau. C'est pour cette raison que l'on ne peut pas associer les débordements de tampon et les bogues dans les chaînes de format directement à l'ordinateur local ou au réseau.

Virus

Contrairement à ce que l'on croit généralement, il existe aussi des virus pour Linux. Les virus connus sont décrits par leurs auteurs en tant que proof-of-concept, à savoir une démonstration du bien-fondé d'un principe. Cependant, aucun de ces virus n'a encore été observé dans la nature.

Pour se propager, les virus ont besoin d'un hôte sans lequel ils ne peuvent survivre. Cet hôte est un programme ou un emplacement sur le disque important pour le système, comme par exemple l'enregistrement d'amorçage maître et le code de programme du virus doit pouvoir y écrire. Linux, du fait de ses fonctionnalités multi-utilisateurs, peut limiter l'accès en écriture aux fichiers et notamment aux fichiers système. Si vous travaillez en tant qu'utilisateur `root` vous augmentez la probabilité d'infecter votre système avec ce type de virus. Si vous observez cependant la règle des privilèges les plus restreints possibles, il devient difficile d'être infecté par un virus sous Linux. En outre, vous ne devriez jamais exécuter à la légère un programme que vous avez récupéré sur l'Internet et dont vous ne connaissez pas l'origine. Les paquetages SUSE-rpm portent une signature cryptographique et témoignent avec cette signature numérique du soin apporté par SUSE lors de l'élaboration de ses paquetages. Les virus sont l'un des symptômes classiques d'un système hautement sécurisé devenu non sûr lorsque l'administrateur ou même l'utilisateur n'ont pas une parfaite conscience de la sécurité.

Il ne faut pas confondre les virus avec les vers qui sont également des phénomènes de la sécurité réseau mais qui n'ont en revanche pas besoin d'hôte pour se propager.

Sécurité réseau

Dans le domaine de la sécurité locale il fallait séparer les utilisateurs travaillant sur le même ordinateur, notamment l'utilisateur `root`. En matière de sécurité réseau, en revanche, c'est l'intégralité du système qu'il faut protéger contre les attaques en provenance du réseau. L'authentification des utilisateurs dans le cas de la connexion classique avec un nom d'utilisateur et un mot de passe relève de la sécurité locale. En cas de connexion par le réseau, il faut différencier les deux aspects de la sécurité : avant la réussite de l'authentification, on parle de sécurité réseau, après le login, il s'agit de sécurité locale.

X-Window (authentification X11)

Comme déjà mentionné précédemment, la transparence du réseau est une caractéristique fondamentale d'un système Unix. Avec X11, le système de fenêtrage d'Unix, cela l'est au plus haut point ! Vous pouvez ainsi simplement vous connecter à un ordinateur distant et y démarrer un programme qui s'affichera alors via le réseau sur votre ordinateur.

Si un client X doit être affiché via le réseau sur notre serveur X, alors le serveur doit protéger la ressource qu'il gère (l'affichage) contre les accès non autorisés.

Concrètement, cela signifie ici que le programme client doit obtenir des droits. Pour X-Windows, cela se passe de deux manières différentes : un contrôle d'accès fondé sur un ordinateur ou sur un cookie. Le premier se fonde sur l'adresse IP de l'ordinateur sur lequel le programme client doit être exécuté et est contrôlé avec le programme `xhost`. Le programme `xhost` inscrit une adresse IP d'un client légitime dans une mini-base de données sur le serveur X. Une authentification uniquement fondée sur une adresse IP n'est cependant pas considérée comme sûre. Il pourrait très bien y avoir un deuxième utilisateur actif sur l'ordinateur avec le programme client et celui-ci aurait, comme quiconque qui déroberait l'adresse IP, accès au serveur X. C'est pour cette raison qu'il est inutile d'aller plus loin au sujet de ces méthodes. Les pages du manuel de la commande `xhost` donnent davantage d'explications sur leur fonctionnement (ainsi qu'un avertissement !).

Dans le cas d'un contrôle d'accès fondé sur un cookie, une chaîne de caractères connue uniquement par le serveur X et l'utilisateur connecté de manière légitime est utilisée comme preuve d'identité, un peu à l'instar d'un mot de passe. Ce cookie (le mot anglais cookie signifie biscuit et désigne ici les biscuits porte-bonheur chinois qui contiennent une maxime) est enregistré dans le fichier `.Xauthority` dans le répertoire personnel de l'utilisateur lors du login et est ainsi à la disposition de chaque client X-Window qui souhaite afficher une fenêtre sur le serveur X. Le programme `xauth` fournit à l'utilisateur l'outil pour analyser le fichier `.Xauthority`. Si vous supprimez ou renommez le fichier `.Xauthority` de votre répertoire personnel, vous ne pourrez plus ouvrir d'autres fenêtres de nouveaux clients X. Vous trouverez plus d'informations sur les aspects liés à la sécurité de X-Window dans la page de manuel de `Xsecurity` (`man Xsecurity`).

`ssh` (secure shell) peut acheminer pour un utilisateur, de manière transparente, une connexion à un serveur X via une connexion réseau complètement chiffrée (du moins pas directement visible). On parle de redirection X11. Dans ce cas, un serveur X est simulé du côté du serveur et la variable DISPLAY de l'interpréteur de commandes du côté distant réglée en conséquence.

Attention

Si vous pensez que l'ordinateur auquel vous vous connectez n'est pas sûr, vous ne devez alors pas autoriser de transmission de connexions X-Window. Lorsque la redirection X11 est activée, des attaquants peuvent aussi se connecter en s'authentifiant auprès de votre serveur X via votre connexion ssh et, par exemple, épier votre clavier.

Attention

Débordements de tampon et bogues dans les chaînes de format

Sans pouvoir être directement classés en local et distant, les termes débordement de tampon et bogues dans les chaînes de format évoqués à la section Sécurité locale sont également employés en sécurité réseau. Comme pour les variantes locales de ces erreurs de programmation, les débordements de tampon des services réseau portent la plupart du temps sur les droits de l'utilisateur `root`. Si tel n'est pas le cas, l'attaquant peut alors au moins réussir à accéder à un compte local sans privilèges dont il pourrait par la suite exploiter les éventuels problèmes de sécurité locale.

Les débordements de tampon et les bogues dans les chaînes de format sont probablement les variantes les plus fréquentes d'attaques distantes exploitables sur le réseau. On trouve sur les listes de diffusion relatives à la sécurité des exploits, c'est-à-dire des programmes qui utilisent les brèches qui viennent d'être découvertes. Même une personne ne connaissant pas les détails précis de la faille de sécurité peut l'exploiter. On a découvert, dans le courant de l'année, que la libre disposition des codes d'exploit (*exploit codes*) a, de manière générale, amélioré la sécurité des systèmes d'exploitation, ce qui est probablement dû au fait que les éditeurs de systèmes d'exploitation ont été obligés de régler les problèmes de leurs logiciels. Comme dans le cas des logiciels libres le code source est à la disposition de tous, (SUSE LINUX fournit toutes les sources disponibles), quelqu'un qui découvre une brèche à l'aide d'un *exploit code* peut aussitôt faire une proposition de réparation pour le problème en question.

DoS — déni de service (Denial of Service)

Le but de ce type d'attaques est d'interrompre un service (voire le système tout entier). Cela peut être provoqué par différentes méthodes : en provoquant une surcharge, en envoyant au système, pour l'occuper, des paquets dont le contenu n'a pas de signification, ou en exploitant les débordements de tampon distants, qui ne sont pas directement exploitables du côté distant pour exécuter des programmes.

L'objectif d'un déni de service peut souvent tout simplement être que le service ne soit plus disponible. L'absence d'un service peut toutefois avoir d'autres conséquences. Voir man in the middle (l'homme au milieu) : sniffing (reniflage de paquets), TCP connection hijacking (détournement de connexion TCP), spoofing (usurpation) et DNS poisoning (corruption de DNS).

man in the middle (l'homme au milieu) : sniffing (reniflage de paquets), tcp connection hijacking (détournement de connexion TCP), spoofing (usurpation)

De manière générale, une attaque du réseau, dans laquelle un attaquant prend une position entre deux partenaires de communication s'appelle une attaque de type man in the middle (l'homme au milieu). Elles ont toutes un point commun : la victime ne se doute de rien. L'attaquant prend la main sur la connexion et établit, sans que la victime ne remarque quoi que ce soit, une connexion avec la cible. La victime a donc sans le savoir établi une connexion avec le mauvais ordinateur parce que ce dernier s'identifie comme étant la cible. L'attaque de type man in the middle la plus simple est un sniffer (renifleur de paquets). Elle épie simplement les connexions réseau qui lui sont adressées (en anglais, sniffing = flairer). Cela devient plus complexe quand l'attaquant au milieu essaie de prendre la main sur une connexion établie existante (en anglais, hijacking = détournement). L'attaquant doit, pour ce faire, analyser pendant un moment les paquets qui lui sont adressés pour pouvoir pronostiquer les numéros de séquence TCP corrects de la connexion TCP. Quand il prend ensuite le rôle de la cible de la connexion, la victime s'en aperçoit car du côté du destinataire, la connexion apparaît comme ayant été interrompue brutalement.

L'attaquant peut tout particulièrement tirer profit de cette technique pour les protocoles non protégés contre le détournement et dans lesquels une authentification se produit au début de la connexion. On parle d'usurpation lors de l'envoi de paquets avec modification des données de l'expéditeur, c'est-à-dire principalement de l'adresse IP. La plupart dse variantes d'attaques actives impliquent l'envoi de paquets falsifiés ce qui sous Unix/Linux n'est autorisé que pour le super utilisateur (l'utilisateur `root`).

La plupart des possibilités d'attaques sont souvent combinées avec un déni de service. S'il y a une possibilité pour séparer l'ordinateur brusquement du réseau (même si ce n'est que pour une courte période), cela entraîne une attaque active car aucune autre perturbation n'est attendue.

Corruption de DNS (DNS poisoning)

L'attaquant essaie d'empoisonner (*poisoning*) avec des paquets de réponse DNS falsifiés le cache d'un serveur DNS pour que celui-ci transmette les informations souhaitées à une victime les demandant. Pour passer ce type de fausses informations de manière crédible à un serveur DNS, l'attaquant doit normalement obtenir quelques paquets du serveur et les analyser. Comme de nombreux serveurs ont établi un rapport de confiance vis-à-vis des autres ordinateurs basé sur

leur adresse IP ou leur nom d'ordinateur, une telle attaque peut très rapidement porter ses fruits, même si les précautions nécessaires ont été prises. La condition essentielle est une bonne connaissance des relations de confiance entre les ordinateurs. Du point de vue de l'attaquant, il est la plupart du temps inévitable de programmer précisément dans le temps un déni de service contre un serveur DNS dont les données doivent être falsifiées.

Pour y remédier, il convient à nouveau d'utiliser une connexion chiffrée avec une technique cryptographique capable de vérifier l'identité de la cible de la connexion.

Vers

On fait souvent l'amalgame entre les vers et les virus. Il existe cependant une différence sensible entre ces deux parasites : un vers n'a nullement besoin d'infecter un programme hôte et il est conçu pour se propager le plus rapidement possible sur le réseau. Les vers les plus connus comme Ramen, Lion ou Adore utilisent les brèches de sécurité de programmes serveur tels que `bind8` ou `lprNG`. Il est relativement facile de se protéger contre les vers, car entre le moment de la découverte des brèches utilisées et le moment de la naissance du vers, il s'écoule généralement quelques jours qui laissent suffisamment de temps pour développer des paquetages de mise à jour ; en partant du principe, naturellement, que l'administrateur applique aussi les mises à jour de sécurité à son système.

27.4.3 Conseils et astuces : renseignements d'ordre général

Informations : pour traiter le domaine de la sécurité de manière efficace, il est nécessaire de bien suivre les développements en la matière et de connaître tout ce qui concerne les derniers problèmes de sécurité. Une très bonne méthode de protection contre les erreurs de tous types consiste à appliquer le plus rapidement possible les paquetages de mise à jour signalés lors d'une annonce de sécurité. Les annonces de sécurité de SUSE sont diffusées par liste de diffusion à laquelle vous pouvez vous inscrire à l'adresse suivante : `http://www.suse.de/security`. `suse-security-announce@suse.de` est la meilleure source d'informations récentes sur les paquetages de mise à jour fournis par l'équipe de sécurité.

La liste de diffusion `suse-security@suse.de` est un forum de discussion instructif en ce qui concerne le domaine de la sécurité. Vous pouvez vous y inscrire sur la même URL `suse-security-announce@suse.de` que pour la liste.

L'une des listes de diffusion les plus connues en terme de sécurité est la liste `bugtraq@securityfocus.com`. Nous vous recommandons la lecture attentive de cette liste dans la mesure où il y passe en moyenne 15 à 20 nouveaux messages chaque jour. Pour plus d'informations, consultez : `http://www.securityfocus.com`.

Voici quelques règles de base à connaître :

- Évitez de travailler en tant qu'utilisateur `root`, et respectez le principe d'utiliser des privilèges minimaux pour effectuer une tâche. Cela permet de réduire les risques d'œuf de coucou ou d'infection par un virus et, de surcroît, les erreurs de votre part.
- Utilisez, dans la mesure du possible, toujours des connexions chiffrées pour effectuer des tâches à distance. `ssh` (secure shell) est le standard pour ce genre de tâches, évitez `telnet`, `ftp`, `rsh` et `rlogin`.
- N'utilisez aucune méthode d'authentification qui serait uniquement fondée sur une adresse IP.
- Tenez vos paquetages réseau les plus importants toujours à jour et abonnez-vous aux listes de diffusion pour recevoir les annonces des différents logiciels (par exemple : `bind`, `sendmail`, `ssh`). Cela s'applique également aux logiciels qui ne concernent que la sécurité locale.
- Optimisez les droits d'accès aux fichiers critiques en terme de sécurité dans le système en adaptant le fichier `/etc/permissions` en fonction de vos besoins. Un programme setuid qui n'a plus de bit setuid peut certes ne plus remplir sa fonction correctement mais ne représente, en règle générale, aucun problème de sécurité. Vous pouvez utiliser le même processus pour les fichiers et les répertoires pour lesquels tout utilisateur possède les droits d'écriture.
- Désactivez les services réseau dont vous n'avez pas absolument besoin sur votre serveur. Cela permet de rendre votre système plus sûr et cela évite que vos utilisateurs ne s'habituent à un service que vous n'avez jamais activé à dessein (problème d'héritage). Utilisez le programme `netstat` pour identifier les ports ouverts (ceux dont l'état est LISTEN). Vous disposez des options `netstat -ap` ou `netstat -anp`. L'option `-p` vous permet de voir immédiatement quel processus occupe quel port et sous quel nom.
  Comparez les résultats que vous obtenez avec une analyse complète des ports de votre ordinateur de l'extérieur. Le programme `nmap` est particulièrement adapté à cet effet. Il interroge chacun des ports et peut, à l'aide de la réponse de votre ordinateur, tirer des conclusions au sujet d'un service en attente derrière le port correspondant. Ne procédez jamais à l'analyse d'un ordinateur sans en avoir averti directement l'administrateur car ce dernier pourrait l'interpréter comme un acte agressif. N'oubliez pas que vous devez non seulement analyser

les ports TCP, mais également les ports UDP (options `-sS` et `-sU`).

- Utilisez `tripwire` pour vérifier, de manière fiable, l'intégrité des fichiers dans votre système et chiffrer la base de données pour la protéger contre toute manipulation. Vous devez, en outre, toujours effectuer une sauvegarde de cette base de données que vous conserverez en dehors de la machine, sur un support de données indépendant non connecté par l'intermédiaire d'un ordinateur au réseau.
- Faites toujours attention lorsque vous installez des logiciels inconnus. On a déjà vu des cas où l'attaquant avait intégré un cheval de Troie dans l'archive tar d'un logiciel de sécurité. Cela a heureusement rapidement été détecté. Si vous installez un paquetage binaire, vous devez être sûr de sa provenance.
  Les paquetages RPM SUSE livrés sont signés avec une signature GPG. La clé que nous utilisons pour le chiffrement est
  ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>
  Empreinte de la clé = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA
  La commande `rpm -checksig paquetage.rpm` indique si la somme de contrôle et la signature du paquetage (non installé !) correspondent. Vous trouverez la clé sur le premier cédérom ou DVD de SUSE LINUX et sur les principaux serveurs de clés du monde.
- Vérifiez régulièrement la sauvegarde de vos données et de votre système. Sans connaissance fiable de la fonction de sauvegarde, une sauvegarde n'a aucune valeur.
- Surveillez vos fichiers journaux. Si vous le pouvez, écrivez un petit script qui recherche dans vos fichiers journaux les éléments inhabituels. Cette tâche n'est vraiment pas triviale car vous êtes le seul à savoir ce qui est habituel ou non.
- Utilisez `tcp_wrapper` pour limiter l'accès aux différents services de votre ordinateur aux adresses IP auxquelles un accès à des services donnés a été accordé. Vous trouverez des informations plus précises au sujet des `tcp_wrapper` dans `tcpd(8)` et `hosts_access`.
- Vous pouvez aussi utiliser comme protection supplémentaire, outre `tcpd` (tcp_-wrapper), le pare-feu SuSEfirewall.
- N'ayez pas peur d'être redondant quand il s'agit de sécurité : un message qui s'affiche deux fois est préférable à un que vous ne verriez jamais, ce qui vaut aussi pour les discussions avec vos collaborateurs.

27.4.4 Publication centralisée des nouveaux problèmes de sécurité

Lorsque vous découvrez un problème de sécurité (vérifiez tout d'abord les paquetages de mise à jour disponibles), vous pouvez alors vous adresser en toute confiance à l'adresse électronique suivante : `security@suse.de`. N'oubliez pas de joindre une description précise du problème ainsi que le numéro de version du paquetage utilisé. Nous ferons tout notre possible pour vous répondre le plus rapidement possible. Nous vous recommandons de chiffrer votre message avec pgp. Notre clé pgp est :

```
ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>
```

Empreinte de la clé = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5

Vous pouvez aussi télécharger cette clé à l'adresse suivante : `http://www.suse.de/security`.

Quatrième partie

Administration

Listes de contrôle d'accès sous Linux

Ce chapitre présente brièvement les tenants et les aboutissants ainsi que le fonctionnement des ACL POSIX pour les systèmes de fichiers Linux. Vous allez découvrir comment les listes de contrôle d'accès (*Access Control Lists*, ACL) ont permis d'améliorer le système traditionnel de droits sur les objets du système de fichiers et les avantages qu'elles apportent.

28.1 À quoi servent les ACL ?

Remarque

ACL POSIX

L'expression *ACL POSIX* suggère qu'il s'agit d'un véritable standard de la famille POSIX (*Portable Operating System Interface* - Interface de Système d'Exploitation Portable). Pour différentes raisons, les projets de standards correspondants, POSIX 1003.1e et POSIX 1003.2c, ont été abandonnés. Ces documents sont pourtant la base des ACL dans de nombreux systèmes d'exploitation UNIX. L'implémentation des ACL de système de fichiers décrite dans ce chapitre respecte le contenu de ces deux documents, que vous pouvez consulter à l'adresse `http://wt.xpilot.org/publications/posix.1e/`

Remarque

Traditionnellement, sous Linux, un fichier est associé à trois ensembles de droits. Ces ensembles représentent les droits de lecture (`r`), d'écriture (`w`) et d'exécution (`x`) pour les trois classes d'utilisateurs propriétaire du fichier (*owner*), groupe (*group*) et "reste du monde" (*other*). Vous pouvez en outre définir les bits *set user id*, *set group id* et *sticky*. Pour plus d'informations à ce sujet, consultez le *manuel de l'utilisateur*, à la section *Utilisateurs et droits d'accès*.

Dans la pratique, ce système simple suffit amplement la plupart du temps. Pour les scénarios plus complexes ou les applications plus avancées, les administrateurs système devaient autrefois avoir recours à un grand nombre d'astuces pour contourner les limites des systèmes de droits traditionnels.

Les ACL sont utiles pour les situations dans lesquelles le système traditionnel de droits d'accès aux fichiers ne suffit pas. Elles permettent d'attribuer des droits à des utilisateurs ou des groupes particuliers même si ces derniers ne correspondent pas au propriétaire ou au groupe d'un fichier.

Les ACL sont une fonctionnalité du noyau Linux et sont actuellement prises en charge par ReiserFS, Ext2, Ext3, JFS et XFS. Vous pouvez vous en servir pour mettre en œuvre des scénarios complexes sans avoir à implémenter des modèles de droits complexes au niveau des applications.

Un exemple de premier plan des avantages des ACL est le remplacement d'un serveur Windows par un serveur Linux. Plusieurs des stations de travail connectées pourront, même après le changement, toujours être exploitées sous Windows. Le système Linux propose aux clients Windows des services de serveur de fichiers et d'impression grâce à Samba.

Comme Samba prend en charge les ACL, les droits d'accès des utilisateurs peuvent être définis aussi bien au niveau du serveur Linux que par l'intermédiaire d'une interface utilisateur graphique sous Windows (uniquement sous Windows NT et versions ultérieures). winbindd permet également d'accorder des droits utilisateur qui n'existent que dans le domaine Windows et qui ne disposent d'aucun compte sur le serveur Linux. Vous pouvez modifier les ACL du côté du serveur à l'aide des applications getfacl et setfacl.

28.2 Définitions

Classes d'utilisateurs Le système de droits traditionnel POSIX connaît trois *classes* d'utilisateurs pour l'attribution de droits dans le système de fichiers : propriétaire (en anglais, *owner*), groupe (en anglais, *group*) et autres utilisateurs ou le "reste du monde" (en anglais, *other*). Les trois bits de droits d'accès (en anglais, *permission bits*) pour l'accès en lecture (`r`), l'accès en écriture (`w`) et l'accès en exécution (`x`) sont définis pour chaque classe d'utilisateur. Vous trouverez une présentation du concept d'utilisateur sous Linux dans le *manuel de l'utilisateur*, dans la section *Utilisateurs et droits d'accès*.

ACL d'accès Les droits d'accès, pour les utilisateurs et les groupes, aux différents objets du système de fichiers (fichiers et répertoires) se définissent à l'aide des ACL d'accès.

ACL par défaut Les ACL par défaut ne peuvent être appliquées qu'aux répertoires et définissent de quels droits un objet de système de fichiers hérite de son répertoire parent lors de sa création.

Élément d'ACL Chaque liste ACL est composée d'éléments (en anglais, *ACL entries*). Un élément d'ACL possède un type (voir le tableau 28.1 page suivante), un descripteur de l'utilisateur ou du groupe concerné par cet élément et des droits. Le descripteur pour le groupe ou l'utilisateur reste vide pour certains types d'éléments.

28.3 Utilisation des ACL

Vous allez apprendre à connaître, dans la section suivante, la structure de base d'une ACL et ses différentes caractéristiques. La relation entre les ACL et le système traditionnel de droits d'accès dans le système de fichiers Linux traditionnel

est brièvement expliquée à l'aide de plusieurs graphiques. Deux exemples vous permettent d'apprendre comment créer des ACL et de faire attention à ce que leur syntaxe soit correcte. Vous découvrirez enfin les modèles utilisés par le système d'exploitation pour mettre en pratique les ACL.

28.3.1 Structure des éléments d'ACL

Les ACL se divisent principalement en deux classes. Une ACL *minimale* est exclusivement composée d'éléments de type *owner* (propriétaire), *owning group* (groupe propriétaire) et *other* (autres) et correspond aux bits de droits d'accès traditionnels pour les fichiers et les répertoires. Une ACL *étendue* (*extended*) prolonge ce système. Elle doit contenir un élément *mask* (masque) et peut contenir plusieurs éléments de type *named user* (utilisateur nommé) et *named group* (groupe nommé). Le tableau 28.1 résume les différents types d'éléments d'ACL disponibles.

TAB. 28.1: *Aperçu : types d'éléments d'ACL*

Type	Forme du texte
owner	`user::rwx`
named user	`user:name:rwx`
owning group	`group::rwx`
named group	`group:name:rwx`
mask	`mask::rwx`
other	`other::rwx`

Les droits définis dans les éléments *owner* et *other* sont toujours actifs. À part l'élément *mask*, tous les autres éléments (*named user*, *owning group* et *named group*) peuvent être soit actifs soit masqués. Si des droits sont disponibles aussi bien dans les éléments ci-dessus que dans le masque, ils deviennent actifs. Les droits qui ne sont disponibles que dans le masque ou que dans leur propre élément ne sont pas actifs. L'exemple suivant explique ce mécanisme (voir tableau 28.2 page suivante) :

TAB. 28.2: *Masquage de droits d'accès*

Type	Forme du texte	Droits
named user	`user:jane:r-x`	`r-x`
mask	`mask::rw-`	`rw-`
	Droits actifs	`r--`

28.3.2 Éléments d'ACL et bits de droits d'accès

Les deux illustrations présentent les deux cas d'une ACL minimale et d'une ACL étendue (voir les illustrations 28.1 et 28.2 page suivante). Les illustrations se divisent en trois blocs. À gauche, l'indication de type des éléments d'ACL, au milieu un exemple d'ACL et à droite les bits de droits d'accès correspondants, tels que `ls -l` les indique également.

Dans les deux cas, les droits d'accès *owner class* sont associés à l'élément d'ACL *owner*. Les droits d'accès *other class* sont aussi toujours associés à l'élément d'ACL correspondant. L'association des droits *group class* dépend :

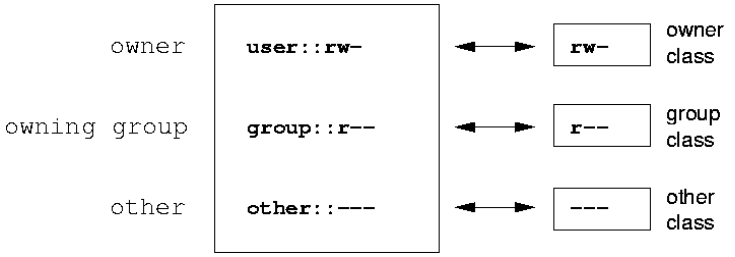


FIG. 28.1: *ACL minimale : éléments d'ACL et bits de droits d'accès*

- Dans le cas d'une ACL minimale — sans élément *mask* — les droits d'accès *group class* sont associés à l'élément *owning group* (voir l'illustration 28.1).
- Dans le cas d'une ACL étendue — avec un élément *mask* — les droits d'accès *group class* sont associés à l'élément *mask* (voir l'illustration 28.2 page suivante).

Ce type d'associations garantit une interaction harmonieuse entre les applications avec et sans prise en charge des ACL. Les droits d'accès définis à l'aide des bits

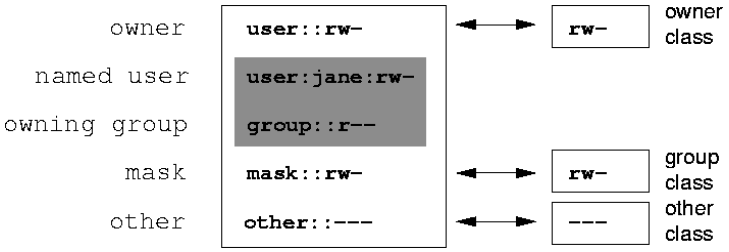


FIG. 28.2: *ACL étendue : éléments d'ACL et bits de droits d'accès*

de droits d'accès sont les plus "fins" de ce que l'on peut régler à l'aide des ACL. Tous les droits qui ne sont pas reflétés ici n'ont pas été définis dans l'ACL ou ne sont pas en vigueur. Si des bits de droits d'accès sont modifiés, cela se reflète dans l'ACL correspondante et vice versa.

28.3.3 Un répertoire avec ACL d'accès

Vous allez apprendre, en trois étapes, l'utilisation d'une ACL d'accès à l'aide de l'exemple suivant :

- Création d'un objet de système de fichiers (ici un répertoire)
- Modifications de l'ACL
- Utilisation de masques

1. Avant de créer le répertoire, vous pouvez définir à l'aide de la commande `umask` quels droits d'accès doivent être masqués aussitôt qu'ils sont mis en place :

   ```
   umask 027
   ```

   `umask 027` limite les droits des différents groupes d'utilisateurs de la manière suivante : le propriétaire du fichier conserve tous les droits (`0`), le groupe d'utilisateurs n'a pas d'accès en écriture au fichier (`2`) et tous les autres utilisateurs n'ont aucun accès (`7`). Ces nombres doivent être lus en tant que masques de bits. Vous trouverez plus de détails sur la commande umask à la page de manuel correspondante (`man umask`).

```
mkdir monrep
```

Le répertoire `monrep` est créé et possède les droits définis à l'aide de la commande `umask`. Avec

```
ls -dl monrep
```

```
drwxr-x--- ... tux projet3 ... monrep
```

vous pouvez vérifier si tous les droits ont correctement été attribués.

2. Après vous être informé du nouvel état de l'ACL, vous pouvez lui ajouter au choix un nouvel élément utilisateur ou groupe.

```
getfacl monrep
```

```
# file: monrep
# owner: tux
# group: projet3
user::rwx
group::r-x
other::---
```

L'affichage de `getfacl` reflète exactement l'association des bits de droits d'accès aux éléments d'ACL décrite à la section *Éléments d'ACL et bits de droits d'accès* page 695. Les trois premières lignes de l'affichage indiquent le nom, le propriétaire et le groupe correspondant du répertoire. Les trois lignes suivantes contiennent les trois éléments d'ACL *owner*, *owning group* et *other*. Au final, la commande `getfacl`, dans le cas de cette ACL simple ("minimale"), ne vous communique aucune information que vous ne puissiez obtenir à l'aide de la commande `ls`.
Votre première intervention sur cette ACL consiste à accorder à un utilisateur supplémentaire `jane` et un groupe supplémentaire `jungle`, les droits en lecture, écriture et exécution.

```
setfacl -m user:jane:rwx,group:jungle:rwx monrep
```

L'option `-m` ordonne à `setfacl` de modifier l'ACL existante. L'argument suivant indique quels éléments d'ACL modifier (utilisez des virgules pour séparer plusieurs éléments à modifier). Indiquez enfin le nom du répertoire auquel les modifications doivent s'appliquer.
Utilisez la commande `getfacl` pour obtenir l'affichage de l'ACL en résultant.

```
# file: monrep
# owner: tux
# group: projet3
user::rwx
user:jane:rwx
group::r-x
group:jungle:rwx
mask::rwx
other::---
```

En plus des éléments que vous avez créés pour l'utilisateur `jane` et le groupe `jungle`, un élément *mask* a été créé. Cet élément *mask* est automatiquement défini pour ramener au même dénominateur tous les éléments dans la *classe du groupe* (*group class*). En outre, la commande `setfacl` adapte automatiquement tous les éléments *mask* existants aux réglages que vous avez modifiés, tant que vous ne désactivez pas ce comportement avec `-n`. *mask* définit les droits d'accès actifs maximum pour tous les éléments se trouvant dans la *classe du groupe* (*class group*). Cela comprend : les *utilisateurs nommés*, les *groupes nommés* et le *groupe propriétaire*. Les bits de droits d'accès *classe de groupe* qui permettraient d'obtenir un `ls -dl monrep` correspondent à présent à l'élément `mask`.

```
ls -dl monrep

drwxrwx---+ ... tux projet3 ... monrep
```

Un + apparaît dans la première colonne de l'affichage. Il signale que l'on est en présence d'une ACL *étendue*.

3. Selon l'affichage obtenu à l'aide de la commande `ls`, les droits de l'élément *mask* comprennent aussi un accès en écriture. Traditionnellement, ces bits de droits d'accès devraient également indiquer que le *owning group* (ici : `projet3`) devraient également avoir un accès en écriture au répertoire `monrep`. En fait les droits d'accès effectivement valables pour le *owning group* sont définis en tant qu'intersection des droits définis pour *owning group* et *mask*, c'est-à-dire dans notre exemple `r-x` (voir le tableau 28.2 page 695). Rien n'a été modifié dans les droits du *owning group* après l'ajout des éléments d'ACL.
   Vous pouvez modifier l'élément *mask* à l'aide des commandes `setfacl` ou `chmod`.

```
chmod g-w monrep
ls -dl monrep

drwxr-x---+ ... tux projet3 ... monrep

getfacl monrep

# file: monrep
# owner: tux
# group: projet3
user::rwx
user:jane:rwx          # effective: r-x
group::r-x
group:jungle:rwx       # effective: r-x
mask::r-x
other::---
```

Une fois que vous avez utilisé `chmod` pour limiter les bits *group class* aux droits en écriture, l'affichage de la commande `ls` vous indique déjà que les bits *mask* ont été adaptés en conséquence à l'aide de la commande `chmod`. On reconnaît que seul le propriétaire possède des droits d'écriture dans le répertoire `monrep`. Cela est encore plus évident dans l'affichage obtenu avec la commande `getfacl`. `getfacl` fournit des commentaires pour tous les éléments dont les bits de droits d'accès véritablement actifs ne correspondent pas à ceux définis précédemment parce qu'ils ont été filtrés par l'élément *mask*. Vous pouvez reproduire l'état d'arrivée à l'aide de la commande `chmod` correspondante :

```
chmod g+w monrep
ls -dl monrep

drwxrwx---+ ... tux projet3 ... monrep

getfacl monrep

# file: monrep
# owner: tux
# group: projet3
user::rwx
user:jane:rwx
group::r-x
group:jungle:rwx
```

```
mask::rwx
other::---
```

28.3.4 Un répertoire avec une ACL par défaut

Les répertoires peuvent être pourvus d'un type bien particulier d'ACL : une ACL par défaut (*default ACL*). Cette ACL par défaut définit les droits d'accès dont les différents sous-objets de ce répertoire héritent lorsqu'ils sont créés. Une ACL par défaut agit aussi bien sur les sous-répertoires que sur les fichiers.

Conséquences d'une ACL par défaut

Les droits d'accès dans une ACL par défaut se transmettent différemment aux fichiers et aux sous-répertoires :

- Un sous-répertoire hérite de l'ACL par défaut de son répertoire parent aussi bien pour sa propre ACL par défaut que pour son ACL d'accès.
- Un fichier hérite de l'ACL par défaut pour sa propre ACL d'accès.

Tous les appels système (en anglais, *system calls*), qui créent des objets de système de fichiers utilisent un paramètre `mode`. Ce paramètre `mode` définit les droits d'accès au nouvel objet de système de fichiers à créer :

- Si le répertoire parent ne possède aucune ACL par défaut, sont appliqués les droits définis dans le paramètre `mode`, desquels sont tirés les droits définis dans la commande `umask`.
- S'il existe une ACL par défaut pour le répertoire parent, les bits de droits d'accès sont composés de l'intersection de la valeur du paramètre `mode` et des droits définis dans l'ACL par défaut et attribués à l'objet. On ne tient alors pas compte de `umask`.

ACL par défaut en pratique

Les trois exemples suivants sont destinés à vous initier aux opérations les plus importantes effectuées sur les répertoires et les ACL par défaut :

- Création d'une ACL par défaut pour un répertoire existant
- Création d'un sous-répertoire dans un répertoire avec une ACL par défaut
- Création d'un fichier dans un répertoire avec une ACL par défaut

1. Ajoutez au répertoire existant `monrep` une ACL par défaut :

```
setfacl -d -m group:jungle:r-x monrep
```

L'option `-d` de la commande `setfacl` indique à `setfacl` d'effectuer les modifications suivantes (option `-m`) sur l'ACL par défaut.
Observez un peu plus précisément le résultat de cette commande :

```
getfacl monrep

# file: monrep
# owner: tux
# group: projet3
user::rwx
user:jane:rwx
group::r-x
group:jungle:rwx
mask::rwx
other::---
default:user::rwx
default:group::r-x
default:group:jungle:r-x
default:mask::r-x
default:other::---
```

`getfacl` fournit aussi bien l'ACL d'accès que l'ACL par défaut. Toutes les lignes qui commencent par `default` constituent l'ACL par défaut. Même si vous aviez passé à la commande `setfacl` uniquement un élément pour le groupe `jungle` dans l'ACL par défaut, `setfacl` a automatiquement copié tous les autres éléments de l'ACL d'accès pour construire ainsi une ACL par défaut valable. Les ACL par défaut n'ont pas d'influence directe sur les droits d'accès et n'ont des conséquences que lors de la création des objets de système de fichiers. Lors de l'héritage, seule l'ACL par défaut du répertoire parent est prise en compte.

2. Dans l'exemple suivant, créez dans `monrep` avec la commande `mkdir` un sous-répertoire qui devra "hériter" de l'ACL par défaut.

```
mkdir monrep/monsousrep
getfacl monrep/monsousrep

# file: monrep/monsousrep
# owner: tux
# group: projet3
user::rwx
group::r-x
group:jungle:r-x
```

```
mask::r-x
other::---
default:user::rwx
default:group::r-x
default:group:jungle:r-x
default:mask::r-x
default:other::---
```

Comme on pouvait le prévoir, le sous-répertoire nouvellement créé `monsousrep` possède les droits de l'ACL par défaut du répertoire parent. L'ACL d'accès de `monsousrep` est un reflet exact de l'ACL par défaut de `monrep`, de même pour l'ACL par défaut qui transmettra de nouveau ce répertoire à ses sous-objets.

3. Créez dans le répertoire `monrep` un fichier avec la commande `touch` :

```
touch monrep/monfichier
ls -l monrep/monfichier

-rw-r-----+ ... tux projet3 ... monrep/monfichier

getfacl monrep/monfichier

# file: monrep/monfichier
# owner: tux
# group: projet3
user::rw-
group::r-x          # effective:r--
group:jungle:r-x    # effective:r--
mask::r--
other::---
```

Important dans cet exemple : `touch` met `mode` à la valeur `0666`, ce qui signifie que les nouveaux fichiers sont créés avec des droits en lecture et en écriture pour toutes les classes d'utilisateurs, tant que d'autres restrictions provenant soit de la commande `umask` soit de l'ACL par défaut n'existent pas (reportez-vous à la section *Conséquences d'une ACL par défaut* page 700). Concrètement, cela signifie que tous les droits d'accès qui ne sont pas compris dans la valeur `mode` ont été supprimés des éléments d'ACL correspondants. Aucun droit n'a été supprimé de l'élément d'ACL de la *classe du groupe*, mais l'élément *mask* a été adapté de manière à ce que les bits de droits d'accès définis par `mode` ne soient pas masqués.

On garantit ainsi que les compilateurs par exemple peuvent interagir sans problème avec les ACL. Vous pouvez créer des fichiers avec des droits d'accès limités et marquer ceux-ci par la suite comme étant exécutables. Le mécanisme `mask` garantit que les utilisateurs et les groupes corrects obtiennent au final les droits qui leur reviennent dans l'ACL par défaut.

28.3.5 Exploitation d'une ACL

Maintenant que vous avez compris comment utiliser les outils les plus importants pour la configuration des ACL, nous allons vous présenter brièvement l'algorithme d'évaluation que chaque processus ou chaque application doit réussir avant qu'on ne puisse lui accorder l'accès à un objet du système de fichiers protégé par une ACL.

En principe, les éléments d'ACL sont étudiées dans l'ordre suivant : *owner*, *named user*, *owning group* ou *named group* et *other*. L'accès est, au final, réglé sur l'élément le mieux adapté au processus.

Las situation se complique quand un processus appartient à plusieurs groupes et peut donc potentiellement être adapté à plusieurs éléments *group*. On cherche n'importe quel élément adapté dont les droits conviennent. Il est naturellement important de savoir lequel de ces éléments a été décisif pour obtenir le résultat final "accès accordé". Si aucun élément *group* adapté ne contient les droits corrects, on prend à nouveau n'importe quel élément pour décider du résultat final "accès refusé".

28.4 Prise en charge par les applications

Comme vous l'avez vu dans les sections précédentes, on peut mettre en œuvre des scénarios très complexes de droits d'accès avec les ACL, qui correspondent aux applications modernes. Le système traditionnel de droits et les ACL sont parfaitement compatibles entre eux.

Pourtant, certaines applications importantes ne prennent pas encore en charge les ACL. C'est notamment le cas des applications de sauvegarde, pour lesquelles, à l'exception de l'archiveur `star`, il n'existe aucun programme qui garantit la prise en charge complète des ACL.

Les principales commandes de manipulation de fichiers (`cp`, `mv`, `ls`, ...) prennent en charge les ACL. De nombreux éditeurs et gestionnaires de fichiers (par

exemple Konqueror) ne prennent pourtant pas en charge les ACL. Lors de la copie de fichiers avec Konqueror, les ACL sont, même encore maintenant, perdues. Lorsque vous éditez un fichier possédant une ACL d'accès avec un éditeur, c'est le mode de sauvegarde de l'éditeur utilisé qui détermine si l'ACL d'accès sera toujours présente une fois la modification terminée :

- Si l'éditeur écrit les modifications dans le fichier d'origine, l'ACL d'accès est conservée.
- Si l'éditeur crée un nouveau fichier qui prend le nom de l'ancien une fois les modifications effectuées, les ACL seront probablement égarées, même si l'éditeur prend en charge les ACL.

Remarque

Pour plus d'informations

Vous trouverez des informations détaillées au sujet des ACL aux adresses suivantes :
`http://sdb.suse.de/de/sdb/html/81_acl.html` `http://acl.bestbits.at/`
et sur les pages de manuel consacrées à `getfacl`, `acl` et `setfacl`.

Remarque

Utilitaires pour la surveillance du système

Dans ce chapitre vous sont présentés plusieurs programmes et mécanismes différents avec lesquels vous pouvez surveiller l'état de votre système. Vous trouverez ensuite la description de quelques utilitaires intéressants pour votre travail au quotidien avec leurs options les plus importantes.

29.1 Conventions

Vous trouverez des exemples de sorties pour les commandes qui vous sont présentées. La première ligne représente la commande elle-même (après un signe Dollar en tant qu'invite). Les omissions sont représentées par `[...]` et les longues lignes peuvent être coupées si nécessaire. Les lignes coupées sont indiquées par un backslash (\) :

```
$ command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
    we have to break it
output line 3
[...]
output line 98
output line 99
```

Afin de pouvoir mentionner le plus possible d'utilitaires, leur présentation est faite brièvement. Vous trouverez plus d'informations sur chaque commande à leur page de manuel respective. La plupart des commandes comprennent également l'option `--help`, si bien qu'on obtient une brève liste des options possibles.

29.2 Liste des fichiers ouverts : lsof

Afin d'indiquer la liste de tous les fichiers, qui a ouvert la processus avec l'ID de processus ⟨*PID*⟩, on utilise l'option `-p`. Par exemple, pour indiquer tous les fichiers utilisés par le shell en cours :

```
$ lsof -p $$
COMMAND  PID USER   FD   TYPE DEVICE    SIZE     NODE NAME
zsh     4694   jj  cwd    DIR   0,18     144 25487368 /suse/jj/t (totan:/real-home/jj)
zsh     4694   jj  rtd    DIR    3,2     608        2 /
zsh     4694   jj  txt    REG    3,2  441296    20414 /bin/zsh
zsh     4694   jj  mem    REG    3,2  104484    10882 /lib/ld-2.3.3.so
zsh     4694   jj  mem    REG    3,2   11648    20610 /usr/lib/zsh/4.2.0/zsh/rlimits.so
[...]
zsh     4694   jj  mem    REG    3,2   13647    10891 /lib/libdl.so.2
zsh     4694   jj  mem    REG    3,2   88036    10894 /lib/libnsl.so.1
zsh     4694   jj  mem    REG    3,2  316410   147725 /lib/libncurses.so.5.4
zsh     4694   jj  mem    REG    3,2  170563    10909 /lib/tls/libm.so.6
zsh     4694   jj  mem    REG    3,2 1349081    10908 /lib/tls/libc.so.6
zsh     4694   jj  mem    REG    3,2      56    12410 /usr/lib/locale/de_DE.utf8/LC_TELEPHONE
[...]
zsh     4694   jj  mem    REG    3,2      59    14393 /usr/lib/locale/en_US/LC_NUMERIC
zsh     4694   jj  mem    REG    3,2  178476    14565 /usr/lib/locale/en_US/LC_CTYPE
zsh     4694   jj  mem    REG    3,2   56444    20598 /usr/lib/zsh/4.2.0/zsh/computil.so
```

```
zsh     4694   jj    0u   CHR 136,48              50 /dev/pts/48
zsh     4694   jj    1u   CHR 136,48              50 /dev/pts/48
zsh     4694   jj    2u   CHR 136,48              50 /dev/pts/48
zsh     4694   jj   10u   CHR 136,48              50 /dev/pts/48
```

La variable shell spéciale $$, ayant comme valeur l'ID de processus du shell, a été utilisée.

Sans option, `lsof` énumère tous les fichiers ouverts actuellement, il y en a en règle générale une grande quantité. Nous comptons :

```
$ lsof | wc -l
3749
```

Enumération de tous les périphériques caractère utilisés :

```
$ lsof | grep CHR
sshd       4685    root  mem    CHR    1,5             45833 /dev/zero
sshd       4685    root  mem    CHR    1,5             45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5             45833 /dev/zero
sshd       4693      jj  mem    CHR    1,5             45833 /dev/zero
zsh        4694      jj    0u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    1u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj    2u   CHR 136,48               50 /dev/pts/48
zsh        4694      jj   10u   CHR 136,48               50 /dev/pts/48
X          6476    root  mem    CHR    1,1             38042 /dev/mem
lsof      13478      jj    0u   CHR 136,48               50 /dev/pts/48
lsof      13478      jj    2u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    1u   CHR 136,48               50 /dev/pts/48
grep      13480      jj    2u   CHR 136,48               50 /dev/pts/48
```

29.3 Qui accède au fichiers : fuser

Un système de fichiers est monté sous `/mnt` :

```
$ mount -l | grep /mnt
/dev/sda on /mnt type ext2 (rw,noexec,nosuid,nodev,noatime,user=jj)
```

La tentative de le démonter échoue :

```
$ umount /mnt
umount: /mnt: device is busy
```

Nous examinons quels processus accèdent aux fichiers dans le répertoire `/mnt` :

```
$ fuser -v /mnt/*

                     USER        PID ACCESS COMMAND
/mnt/notes.txt
                     jj        26597 f....  less
```

Après la fin du processus `less` qui fonctionnait dans un autre terminal, le sytème de fichiers se laisse démonter.

29.4 Caractéristiques d'un fichier : stat

On utilise la commande `stat` pour afficher les caractéristiques d'un fichier :

```
$ stat xml-doc.txt
  File: 'xml-doc.txt'
  Size: 632             Blocks: 8          IO Block: 4096   regular file
Device: eh/14d  Inode: 5938009     Links: 1
Access: (0644/-rw-r--r--)  Uid: (11994/      jj)   Gid: (   50/    suse)
Access: 2004-04-27 20:08:58.000000000 +0200
Modify: 2003-06-03 15:29:34.000000000 +0200
Change: 2003-07-23 17:48:27.000000000 +0200
```

Avec l'option `--filesystem`, les caractéristiques du système de fichiers, sur lequel se trouve le fichier indiqué, sont affichées :

```
$ stat  . --filesystem
  File: "."
    ID: 0        Namelen: 255     Type: ext2/ext3
Blocks: Total: 19347388   Free: 17831731   Available: 16848938   Size: 4096
Inodes: Total: 9830400    Free: 9663967
```

Si vous utilisez le terminal z-shell (`zsh`), saisissez `/usr/bin/stat`, car ce terminal a un shell-builtin `stat` avec d'autres options et un format de sortie diffétent :

```
% type stat
stat is a shell builtin
% stat .
device  769
inode   4554808
mode    16877
nlink   12
uid     11994
gid     50
```

```
rdev    0
size    4096
atime   1091536882
mtime   1091535740
ctime   1091535740
blksize 4096
blocks  8
link
```

29.5 Processus : top

Avec la commande `top` (pour : *table of processes*), une liste des processus qui est actualisée toutes les 2 secondes apparaît. On quitte le programme avec la touche ⓠ. Avec l'option `-n 1`, on arrive à terminer le programme après un seul affichage de la liste de processus :

```
$ top -n 1
top - 14:19:53 up 62 days,  3:35, 14 users,  load average: 0.01, 0.02, 0.00
Tasks: 102 total,   7 running,  93 sleeping,   0 stopped,   2 zombie
Cpu(s):   0.3% user,   0.1% system,   0.0% nice,  99.6% idle
Mem:    514736k total,   497232k used,    17504k free,    56024k buffers
Swap:  1794736k total,   104544k used,  1690192k free,   235872k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  Command
 1426 root      15   0  116m  41m  18m S  1.0  8.2  82:30.34 X
20836 jj        15   0   820  820  612 R  1.0  0.2   0:00.03 top
    1 root      15   0   100   96   72 S  0.0  0.0   0:08.43 init
    2 root      15   0     0    0    0 S  0.0  0.0   0:04.96 keventd
    3 root      34  19     0    0    0 S  0.0  0.0   0:00.99 ksoftirqd_CPU0
    4 root      15   0     0    0    0 S  0.0  0.0   0:33.63 kswapd
    5 root      15   0     0    0    0 S  0.0  0.0   0:00.71 bdflush
       [...]
 1362 root      15   0   488  452  404 S  0.0  0.1   0:00.02 nscd
 1363 root      15   0   488  452  404 S  0.0  0.1   0:00.04 nscd
 1377 root      17   0    56    4    4 S  0.0  0.0   0:00.00 mingetty
 1379 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
 1380 root      18   0    56    4    4 S  0.0  0.0   0:00.01 mingetty
```

Pendant que `top` est en marche, on arrive, en appuyant sur la touche ⓕ, à un menu dans lequel le format de la sortie peut être modifié de façon importante.

Afin de surveiller les processus d'un utilisateur défini, l'option `-U` ⟨*UID*⟩ peut être utilisée, ⟨*UID*⟩ représentant alors l'ID de l'utilisateur. Avec la commande suivante, l'UID de l'utilisateur est recherché à l'aide du nom d'utilisateur et ses processus sont affichés :

```
$ top -U $(id -u <username>)
```

29.6 Liste de processus : ps

La commande `ps` créé une liste de processsus. Avec l'option `r`, seuls les processus utilisant des ressources sont affichés :

```
$ ps r
  PID TTY      STAT   TIME COMMAND
22163 pts/7    R      0:01 -zsh
 3396 pts/3    R      0:03 emacs new-makedoc.txt
20027 pts/7    R      0:25 emacs xml/common/utilities.xml
20974 pts/7    R      0:01 emacs jj.xml
27454 pts/7    R      0:00 ps r
```

L'option doit effectivement être entrée *sans* moins. Les mutliples options sont entrées en partie avec, en partie sans moins. La page de manuel est susceptible de faire fuire l'utilisateur potentiel. Heureusement, `ps --help` propose une brève page d'assistance.

Nous contrôlons le nombre de processus `emacs` en marche :

```
$ ps x | grep emacs
 1288 ?        S      0:07 emacs
 3396 pts/3    S      0:04 emacs new-makedoc.txt
 3475 ?        S      0:03 emacs .Xresources
20027 pts/7    S      0:40 emacs xml/common/utilities.xml
20974 pts/7    S      0:02 emacs jj.xml

$ pidof emacs
20974 20027 3475 3396 1288
```

Avec l'option `-p`, les processus sont sélectionnés par l'intermédiaire de l'ID de processus :

```
$ ps www -p $(pidof xterm)
  PID TTY      STAT   TIME COMMAND
 9025 ?        S      0:01 xterm -g 100x45+0+200
 9176 ?        S      0:00 xterm -g 100x45+0+200
25543 ?        S      0:02 xterm -g 100x45+0+200
22161 ?        R      0:14 xterm -g 100x45+0+200
16832 ?        S      0:01 xterm -bg MistyRose1 -T root -e su -l
16912 ?        S      0:00 xterm -g 100x45+0+200
17861 ?        S      0:00 xterm -g 120x45+40+300
19930 ?        S      0:13 xterm -bg LightCyan
21686 ?        S      0:04 xterm -g 100x45+0+200
23104 ?        S      0:00 xterm -g 100x45+0+200
23334 ?        S      0:00 xterm -g 100x45+0+200
26547 ?        S      0:00 xterm -g 100x45+0+200
```

La liste de processus peut également être formatées selon les besoins. L'option `-L` donne une liste de tous les mots-clés. Si vous souhaitez une liste de tous les processus ordonnés selon l'utilisation qu'ils font des ressources, utilisez la commande suivante :

```
$ ps ax --format pid,rss,cmd --sort rss
  PID  RSS CMD
    2    0 [ksoftirqd/0]
    3    0 [events/0]
   17    0 [kblockd/0]
[...]
10164 5260 xterm
31110 5300 xterm
17010 5356 xterm
 3896 29292 /usr/X11R6/bin/X -nolisten tcp -br vt7 -auth /var/lib/xdm/authdir/au
```

29.7 Arborescence de processus : pstree

La commande `pstree` délivre une liste de processus :

```
$ pstree
init-+-atd
     |-3*[automount]
     |-bdflush
     |-cron
  [...]
     |-usb-storage-1
     |-usb-storage-2
     |-10*[xterm---zsh]
     |-xterm---zsh---mutt
     |-2*[xterm---su---zsh]
     |-xterm---zsh---ssh
     |-xterm---zsh---pstree
     |-ypbind---ypbind---2*[ypbind]
     `-zsh---startx---xinit4-+-X
                             `-ctwm-+-xclock
                                    |-xload
                                    `-xosview.bin
```

Avec l'option `-p`, les noms sont complétés par l'ID de processus. Afin de faire apparaître les lignes de commande, on utilise l'option `-a` :

```
$ pstree -pa
init,1
```

```
  |-atd,1255
[...]
  ‘-zsh,1404
      ‘-startx,1407 /usr/X11R6/bin/startx
          ‘-xinit4,1419 /suse/jj/.xinitrc [...]
              |-X,1426 :0 -auth /suse/jj/.Xauthority
              ‘-ctwm,1440
                  |-xclock,1449 -d -geometry -0+0 -bg grey
                  |-xload,1450 -scale 2
                  ‘-xosview.bin,1451 +net -bat +net
```

29.8 Qui fait quoi : w

Avec la commande `w`, vous pouvez constater qui est connecté au système et ce qu'il fait. Exemple :

```
$ w
 15:17:26 up 62 days,  4:33, 14 users,  load average: 0.00, 0.04, 0.01
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
jj       pts/0     30Mar04  4days  0.50s  0.54s xterm -bg MistyRose1 -e su -l
jj       pts/1     23Mar04  5days  0.20s  0.20s -zsh
jj       pts/2     23Mar04  5days  1.28s  1.28s -zsh
jj       pts/3     23Mar04  3:28m  3.21s  0.50s -zsh
[...]
jj       pts/7     07Apr04  0.00s  9.02s  0.01s w
jj       pts/9     25Mar04  3:24m  7.70s  7.38s mutt
[...]
jj       pts/14    12:49   37:34   0.20s  0.13s ssh totan
```

La dernière ligne révèle que l'utilisateur jj a créé une liaison secure shell (`ssh`)vers l'ordinateur `totan`. Si des utilisateurs d'autres systèmes se sont connectés à distance, on peut alors faire afficher, à l'aide de l'option `-f`, à partir de quel ordinateur il a créé cette liaison.

29.9 Utilisation de la mémoire : free

L'utilisation de la RAM est examinée à l'aide de l'utilitaire `free`. Il indique la mémoire libre et la mémoire occupée (et Swap) :

```
$ free
             total       used       free     shared    buffers     cached
```

```
Mem:        514736     273964     240772          0      35920      42328
-/+ buffers/cache:     195716     319020
Swap:      1794736     104096    1690640
```

L'option `-m`, qui a pour effet que toutes les tailles sont indiquées en Megaoctets, est utile :

```
$ free -m
             total       used       free     shared    buffers     cached
Mem:           502        267        235          0         35         41
-/+ buffers/cache:        191        311
Swap:         1752        101       1651
```

La donnée réellement intéressante se trouve à la ligne suivante :

```
-/+ buffers/cache:        191        311
```

Ici, l'utilisation par Buffer et Cache est calculée. Avec l'option `-d` ⟨*delay*⟩, la sortie est renouvelée toutes les ⟨*delay*⟩ secondes : `free -d 1.5` émet toutes les 1,5 secondes les valeurs actuelles.

29.10 Tampon circulaire du noyau : dmesg

Le noyau Linux conserve une certaine quantité de messages dans un tampon circulaire. Ces messages sont publiés à l'aide de la commande `dmesg` :

```
$ dmesg
[...]
sdc : READ CAPACITY failed.
sdc : status = 1, message = 00, host = 0, driver = 08
Info fld=0xa00 (nonstd), Current sd00:00: sense key Not Ready
sdc : block size assumed to be 512 bytes, disk size 1GB.
sdc: test WP failed, assume Write Enabled
 sdc: I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 2097144
 I/O error: dev 08:20, sector 0
 I/O error: dev 08:20, sector 0
 unable to read partition table
 I/O error: dev 08:20, sector 0
nfs: server totan not responding, still trying
nfs: server totan OK
```

L'avant-dernière ligne indique un problème temporaire du serveur NFS `totan`. Les lignes avant celle-ci sont déclenchées par le branchement d'un flash drive USB.

Les événements remontant à plus loin sont notifiés dans les fichiers `/var/log/messages` et `/var/log/warn`.

29.11 Systèmes de fichiers : mount, df et du

On constate à l'aide de `mount` quel système de fichier (périphérique et type) est monté et à quel endroit (point de montage) :

```
$ mount
/dev/hdb2 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/hda1 on /data type ext2 (rw)
shmfs on /dev/shm type shm (rw)
usbdevfs on /proc/bus/usb type usbdevfs (rw)
automount(pid1012) on /suse type autofs \
    (rw,fd=5,pgrp=1012,minproto=2,maxproto=3)
totan:/real-home/jj on /suse/jj type nfs \
    (rw,nosuid,rsize=8192,wsize=8192,hard,intr,nolock,addr=10.10.0.1)
```

L'utilisation caractéristique générale des systèmes fichiers peut être interrogée avec `df`. L'option `-h` (alias `--human-readable`) rend l'information lisible pour tout un chacun :

```
$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hdb2             7.4G  5.1G  2.0G  73% /
/dev/hda1              74G  5.8G   65G   9% /data
shmfs                 252M     0  252M   0% /dev/shm
totan:/real-home/jj   350G  324G   27G  93% /suse/jj
```

Il est préférable que les utilisateurs du serveur de fichiers NFS `totan` mettent de l'ordre dans leurs répertoires personnels le plus vite possible. On peut connaître la taille globale de tous les fichiers à l'intérieur d'un répertoire à l'aide de la commande `du`. L'option `-s` empêche la sortie détaillée, `-h` améliore également la lisibilité pour tout un chacun.

Par l'intermédiaire de

```
$ du -sh ~
361M    /suse/jj,
```

on peut estimer la place nécessaire à son propre répertoire personnel.

29.12 Le système de fichiers /proc

Le système de fichiers `/proc` est un pseudo système de fichiers dans lequel le noyau détient des informations importantes sous forme de fichiers virtuels. Par exemple, le type de CPU peut être défini simplement comme suit :

```
$ cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 6
model           : 8
model name      : AMD Athlon(tm) XP 2400+
stepping        : 1
cpu MHz         : 2009.343
cache size      : 256 KB
fdiv_bug        : no
[...]
```

On retrouve l'affectation et l'utilisation des interruptions avec :

```
$ cat /proc/interrupts
           CPU0
  0:  537544462          XT-PIC  timer
  1:     820082          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          2          XT-PIC  rtc
  9:          0          XT-PIC  acpi
 10:      13970          XT-PIC  usb-uhci, usb-uhci
 11:  146467509          XT-PIC  ehci_hcd, usb-uhci, eth0
 12:    8061393          XT-PIC  PS/2 Mouse
 14:    2465743          XT-PIC  ide0
 15:       1355          XT-PIC  ide1
NMI:          0
LOC:          0
ERR:          0
MIS:          0
```

Voici une liste de certains fichiers importants et des informations qu'ils comportent :

- `/proc/devices` : périphériques disponibles
- `/proc/modules` : modules du noyau chargés
- `/proc/cmdline` : ligne de commande du noyau
- `/proc/meminfo` : informations détaillées sur l'utilisation de la mémoire
- `/proc/config.gz` : fichier de configuration `gzip` comprimé du noyau fonctionnant actuellement.

Vous trouverez des informations supplémentaires dans le fichier de texte : `/usr/src/linux/Documentation/filesystems/proc.txt`. Des informations sur les processus en cours se trouvent dans les répertoires `/proc/` ⟨*NNN*⟩, ⟨*NNN*⟩ étant l'ID de processus (PID) de chaque processus. Sous `/proc/self/`, un processus trouve toujours ses propres caractéristiques :

```
$ ls -l /proc/self
lrwxrwxrwx  1 root root 64 Apr 29 13:52 /proc/self -> 27585

$ ls -l /proc/self/
total 0
dr-xr-xr-x  2 jj suse 0 Apr 29 13:52 attr
-r--------  1 jj suse 0 Apr 29 13:52 auxv
-r--r--r--  1 jj suse 0 Apr 29 13:52 cmdline
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 cwd -> /suse/jj/t
-r--r--r--  1 jj suse 0 Apr 29 13:52 delay
-r--------  1 jj suse 0 Apr 29 13:52 environ
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 exe -> /bin/ls
dr-x------  2 jj suse 0 Apr 29 13:52 fd
-rw-------  1 jj suse 0 Apr 29 13:52 mapped_base
-r--r--r--  1 jj suse 0 Apr 29 13:52 maps
-rw-------  1 jj suse 0 Apr 29 13:52 mem
-r--r--r--  1 jj suse 0 Apr 29 13:52 mounts
lrwxrwxrwx  1 jj suse 0 Apr 29 13:52 root -> /
-r--r--r--  1 jj suse 0 Apr 29 13:52 stat
-r--r--r--  1 jj suse 0 Apr 29 13:52 statm
-r--r--r--  1 jj suse 0 Apr 29 13:52 status
dr-xr-xr-x  3 jj suse 0 Apr 29 13:52 task
-r--r--r--  1 jj suse 0 Apr 29 13:52 wchan
```

Dans le fichier `maps`, on trouve le classement des adresses des exécutables et des bibliothèques :

```
$ cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:02 22890      /bin/cat
0804c000-0804d000 rw-p 00003000 03:02 22890      /bin/cat
0804d000-0806e000 rwxp 0804d000 00:00 0
40000000-40016000 r-xp 00000000 03:02 10882      /lib/ld-2.3.3.so
40016000-40017000 rw-p 00015000 03:02 10882      /lib/ld-2.3.3.so
40017000-40018000 rw-p 40017000 00:00 0
4002b000-40135000 r-xp 00000000 03:02 10908      /lib/tls/libc.so.6
40135000-4013d000 rw-p 0010a000 03:02 10908      /lib/tls/libc.so.6
4013d000-40141000 rw-p 4013d000 00:00 0
bfffe000-c0000000 rw-p bfffe000 00:00 0
ffffe000-fffff000 ---p 00000000 00:00 0
```

29.13 procinfo

Les informations importantes provenant du système de fichiers `/proc` sont récapitulées par le programme `procinfo` :

```
$ procinfo
Linux 2.6.4-54.5-default (geeko@buildhost) (gcc 3.3.3 ) #1 1CPU [roth.suse.de]

Memory:      Total        Used        Free      Shared     Buffers
Mem:        516696      513200        3496           0       43284
Swap:       530136        1352      528784

Bootup: Wed Jul  7 14:29:08 2004    Load average: 0.07 0.04 0.01 1/126 5302

user  :       2:42:28.08   1.3%  page in :        0
nice  :       0:31:57.13   0.2%  page out:        0
system:       0:38:32.23   0.3%  swap in :        0
idle  :   3d 19:26:05.93  97.7%  swap out:        0
uptime:   4d  0:22:25.84         context :207939498

irq  0: 776561217 timer                 irq  8:         2 rtc
irq  1:    276048 i8042                 irq  9:     24300 VIA8233
irq  2:         0 cascade [4]           irq 11:  38610118 acpi, eth0, uhci_hcd
irq  3:         3                       irq 12:   3435071 i8042
irq  4:         3                       irq 14:   2236471 ide0
irq  6:         2                       irq 15:       251 ide1
```

Pour voir "toutes" les informations, utilisez l'option `-a`. Avec l'option `-n`⟨*N*⟩ , les informations seront consultées toutes les ⟨*N*⟩ secondes. Dans ce cas, vous devez quitter le programme avec la touche ⓠ.

Les valeurs cumulées sont affichées par défaut ; on indique les valeurs différentielles avec l'option `-d` : `procinfo -dn5` indique les valeurs apparues en 5 secondes :

```
Memory:      Total        Used        Free      Shared     Buffers      Cached
Mem:             0           2          -2           0           0           0
Swap:            0           0           0

Bootup: Wed Feb 25 09:44:17 2004    Load average: 0.00 0.00 0.00 1/106 31902

user  :       0:00:00.02   0.4%  page in :        0  disk 1:        0r       0w
nice  :       0:00:00.00   0.0%  page out:        0  disk 2:        0r       0w
system:       0:00:00.00   0.0%  swap in :        0  disk 3:        0r       0w
idle  :       0:00:04.99  99.6%  swap out:        0  disk 4:        0r       0w
uptime:  64d  3:59:12.62         context :     1087

irq  0:       501 timer               irq 10:         0 usb-uhci, usb-uhci
irq  1:         1 keyboard            irq 11:        32 ehci_hcd, usb-uhci,
irq  2:         0 cascade [4]         irq 12:       132 PS/2 Mouse
irq  6:         0                     irq 14:         0 ide0
irq  8:         0 rtc                 irq 15:         0 ide1
irq  9:         0 acpi
```

29.14 Ressources PCI : lspci

La commande `lspci` énumère les ressources PCI :

```
$ lspci
00:00.0 Host bridge: VIA Technologies, Inc. \
    VT8366/A/7 [Apollo KT266/A/333]
00:01.0 PCI bridge: VIA Technologies, Inc. \
    VT8366/A/7 [Apollo KT266/A/333 AGP]
00:0b.0 Ethernet controller: Digital Equipment Corporation \
    DECchip 21140 [FasterNet] (rev 22)
00:10.0 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.1 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.2 USB Controller: VIA Technologies, Inc. USB (rev 80)
00:10.3 USB Controller: VIA Technologies, Inc. USB 2.0 (rev 82)
00:11.0 ISA bridge: VIA Technologies, Inc. VT8235 ISA Bridge
00:11.1 IDE interface: VIA Technologies, Inc. VT82C586/B/686A/B \
    PIPC Bus Master IDE (rev 06)
00:11.5 Multimedia audio controller: VIA Technologies, Inc. \
    VT8233 AC97 Audio Controller (rev 50)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. \
    MGA G550 AGP (rev 01)
```

Avec l'option `-v`, le listage est plus détaillé :

```
$ lspci -v
[...]
01:00.0 \
 VGA compatible controller: Matrox Graphics, Inc. MGA G550 AGP (rev 01) \
    (prog-if 00 [VGA])
 Subsystem: Matrox Graphics, Inc. Millennium G550 Dual Head DDR 32Mb
 Flags: bus master, medium devsel, latency 32, IRQ 10
 Memory at d8000000 (32-bit, prefetchable) [size=32M]
 Memory at da000000 (32-bit, non-prefetchable) [size=16K]
 Memory at db000000 (32-bit, non-prefetchable) [size=8M]
 Expansion ROM at <unassigned> [disabled] [size=128K]
 Capabilities: <available only to root>
```

La résolution des noms des périphériques est effectuée avec le fichier `/usr/share/pci.ids`. Les ID PCI n'apparaissant pas dans ce fichier sont indiquées comme "Unknown device".

On reçoit avec `-vv` toutes les informations pouvant être appelées par le programme. Les valeurs purement numériques sont indiquées à l'aide de l'option `-n`.

29.15 strace

On peut suivre tous les appels système d'un processus en cours à l'aide de l'utilitaire `strace`. On entre la commande comme à l'habitude, complétée d'un `strace` au début de la ligne :

```
$ strace ls

execve("/bin/ls", ["ls"], [/* 88 vars */]) = 0
uname({sys="Linux", node="edison", ...}) = 0
brk(0)                                  = 0x805b000
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
        = 0x40017000
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=76333, ...}) = 0
old_mmap(NULL, 76333, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40018000
[...]
ioctl(1, SNDCTL_TMR_TIMEBASE or TCGETS, {B38400 opost isig icanon echo ...}) = 0
ioctl(1, TIOCGWINSZ, {ws_row=53, ws_col=110, ws_xpixel=897, ws_ypixel=693}) = 0
open(".", O_RDONLY|O_NONBLOCK|O_LARGEFILE|O_DIRECTORY) = 3
fstat64(3, {st_mode=S_IFDIR|0755, st_size=144, ...}) = 0
fcntl64(3, F_SETFD, FD_CLOEXEC)         = 0
getdents64(3, /* 5 entries */, 4096)    = 160
getdents64(3, /* 0 entries */, 4096)    = 0
close(3)                                = 0
fstat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 48), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
        = 0x40018000
write(1, "ltrace-ls.txt  myfile.txt  strac"..., 41) = 41
munmap(0x40018000, 4096)                = 0
exit_group(0)                           = ?
```

Par exemple, pour suivre toutes les tentatives d'ouverture d'un fichier, on procède comme suit :

```
$ strace -e open ls myfile.txt

open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
open("/lib/tls/librt.so.1", O_RDONLY)   = 3
open("/lib/libacl.so.1", O_RDONLY)      = 3
open("/lib/libselinux.so.1", O_RDONLY)  = 3
open("/lib/tls/libc.so.6", O_RDONLY)    = 3
open("/lib/tls/libpthread.so.0", O_RDONLY) = 3
open("/lib/libattr.so.1", O_RDONLY)     = 3
open("/proc/mounts", O_RDONLY)          = 3
[...]
open("/proc/filesystems", O_RDONLY)     = 3
open("/proc/self/attr/current", O_RDONLY) = 4
```

Pour suivre également tous les processus enfants, on utilise l'option `-f`. On peut largement contrôler le comportement et le format de sortie de strace, voir à ce sujet `man strace`.

29.16 ltrace

Les appels bibliothèque d'un processus peuvent être suivis à l'aide de la commande `ltrace`. Le principe d'utilisation est le même que pour `strace`. Avec l'option `-c`, le nombre et la durée des appels bibliothèque effectués est affiché :

```
$ ltrace -c find /usr/share/doc
% time     seconds  usecs/call     calls    errors syscall
------ ----------- ----------- --------- --------- ----------------
 86.27    1.071814          30     35327           write
 10.15    0.126092          38      3297           getdents64
  2.33    0.028931           3     10208           lstat64
  0.55    0.006861           2      3122         1 chdir
  0.39    0.004890           3      1567         2 open
[...]
  0.00    0.000003           3         1           uname
  0.00    0.000001           1         1           time
------ ----------- ----------- --------- --------- ----------------
100.00    1.242403                 58269         3 total
```

29.17 De quelle bibliothèque a-t-on besoin : ldd

A l'aide de `ldd` on reconnaît quelles bibliothèques seraient chargées par le programme dynamique exécutable donné en argument :

```
$ ldd /bin/ls
linux-gate.so.1 =>  (0xffffe000)
librt.so.1 => /lib/tls/librt.so.1 (0x4002b000)
libacl.so.1 => /lib/libacl.so.1 (0x40033000)
libselinux.so.1 => /lib/libselinux.so.1 (0x40039000)
libc.so.6 => /lib/tls/libc.so.6 (0x40048000)
libpthread.so.0 => /lib/tls/libpthread.so.0 (0x4015d000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
libattr.so.1 => /lib/libattr.so.1 (0x4016d000)
```

Les exécutables statiques n'ont besoin d'aucune bibliothèque dynamique :

```
$ ldd /bin/sash
        not a dynamic executable
$ file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
for GNU/Linux 2.2.5, statically linked, stripped
```

29.18 Informations sur les fichiers binaires ELF

Le contenu des fichiers binaires peut être lu à l'aide du programme `readelf`. Ceci fonctionne aussi avec les fichiers ELF qui sont conçus pour d'autres architectures :

```
$ readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x8049b40
  Start of program headers:          52 (bytes into file)
  Start of section headers:          76192 (bytes into file)
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         9
  Size of section headers:           40 (bytes)
  Number of section headers:         29
  Section header string table index: 26
```

29.19 Communication inter-processus : ipcs

Avec la commande `ipcs`, on reçoit une énumération des ressources IPC utilisées :

```
$ ipcs
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status
0x000027d9 5734403    toms       660        64528      2
0x00000000 5767172    toms       666        37044      2
0x00000000 5799941    toms       666        37044      2

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
0x000027d9 0          toms       660        1

------ Message Queues --------
key        msqid      owner      perms      used-bytes   messages
```

29.20 Mesure du temps avec time

Le besoin en temps des commandes peut être retrouvé grâce au programme d'aide `time`. Ce programme est disponible en deux versions : d'une part en tant que shell-builtin et d'autre part en tant que programme sous `/usr/bin/time`.

```
$ time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

Cinquième partie

Appendices

Sources d'information et documentations

Ce chapitre vous montre à quel endroit vous pouvez trouver des informations et de la documentation concernant votre système.

Documentation SUSE

Vous trouverez d'amples informations sur ce sujet dans nos manuels au format HTML ou PDF dans les paquetages RPM `suselinux-adminguide_fr` et `suselinux-adminguide_fr-pdf`).

Dans le cas d'une installation standard, les manuels sont installés dans le répertoire `/usr/share/doc/manual/`. A l'aide du SUSEHelpCenter, vous avez accès à ces informations.

Le projet de documentation Linux (TLDP)

Le projet de documentation Linux (voir `http://www.tldp.org/`) est une équipe de volontaires qui créent une documentation sur Linux. TLDP comporte des HOWTO, FAQ et ce qu'on appelle des guides (manuels), tous publiés sous une licence libre.

Les HOWTO ("Comment faire ?") sont des modes d'emploi pas à pas et s'adressent à l'utilisateur final, aux administrateurs de système ou aux programmeurs. Par exemple, l'installation d'un serveur DHCP ainsi que ce à quoi il faut

veiller est décrit dans un HOWTO, mais pas la façon d'installer Linux en tant que tel. En règle générale, de telles documentations sont assez générales afin de pouvoir être utilisées pour chaque distribution. Le paquetage `howto` comporte des "Comment faire..." au format ASCII. Les utilisateurs préférant HTML installeront `howtoenh`.

Les FAQ (en angl. *Frequently Asked Questions*) sont un ensemble de questions et réponses concernant des domaines de problèmes définis, fréquemment posées dans les listes de diffusion. Par exemple, "Qu'est-ce que LDAP ?", "Qu'est-ce que RAID ?", etc. Les textes de cette catégorie sont en général très courts.

Les *guides* sont des manuels qui peuvent traiter un thème de manière beaucoup plus détaillée que les "Comment faire..." et les FAQ. Par exemple la programmation du noyau, l'administration du réseau, entre autres. L'objectif est de transmettre une connaissance solide au lecteur.

Beaucoup de documentations du TLDP sont également disponibles en d'autres formats, comme par exemple PDF, des pages HTLML isolées ou multiples, PostScript et sous forme de sources SGML/XML. Il existe également parfois des traductions dans différentes langues.

Pages de manuel et d'information

Une page de manuel (en angl. *Manual page*) est un texte d'aide relatif à une commande, un appel système, un format de fichier, entre autres. Habituellement, une page de manuel est subdivisée en différentes sections, comme Nom, Syntaxe, Description, Options, Fichiers, etc.

Pour afficher une page de manuel, entrez :

```
man ls
```

L'entrée précédente affiche le texte d'aide relatif à la commande `ls`. Avec les touches curseur, vous pouvez déplacer la partie visible, avec (q) vous quittez `man`. Pour imprimer une page de manuel (par exemple pour la commande `ls`), entrez :

```
card ls
```

Vous trouverez plus d'aide concernant la commande `card` (paquetage `a2ps`) avec l'option `--help`.

Beaucoup de documentations sont également disponibles dans le format Info, par exemple `grep`. On l'appelle de cette façon :

`info grep`

Contrairement aux pages de manuel, les pages d'info sont plus détaillées et divisées en plusieurs "points". Un point représente alors une page pouvant être lue avec un Info Reader (comparable à un navigateur HTML). Pour naviguer dans une page d'info, on utilise les touches ⓟ (previous, page précédente) et ⓝ (next, page suivante). Avec ⓠ, vous quittez `info`. Vous trouverez d'autres informations sur les autres touches dans la documentation relative à `info` (appelez `info info`).

On peut appeler aussi bien les pages de manuel que les pages d'info dans Konqueror en entrant `man:`⟨*Commande*⟩ ou `info:`⟨*Commande*⟩ dans la ligne d'URL.

Standards et spécifications

Si vous avez besoin d'informations sur les standards ou les spécifications, il existe pour cela différentes possibilités d'information :

`www.linuxbase.org` Le "Free Standards Group" est un organisme indépendant sans but lucratif dont l'objectif est d'assister la diffusion de logiciels libres et gratuits. Ceci doit être réalisé grâce à la définition de standards communs aux distributions. Sous la direction de cette organisation, la maintenance de plusieurs standards, entre autres le très important LSB (Linux Standard Base) pour Linux, doit être exécutée.

`http://www.w3.org` Le *World Wide Web Consortium* (W3C) est l'une des organisations la plus connue. Elle a été créée en octobre 1994 par TIM BERNERS-LEE et se concentre sur la standardisation de technologies Web. Il encourage la diffusion de spécifications libres, sans licence et indépendantes du fabricant comme par exemple HTML, XHTML, XML et plus encore. Ces "standards web" sont développés dans un processus à 4 niveaux dans ce qu'on appelle des *Working Groups* et présentés au public comme des *recommandations W3C (REC).*

`http://www.oasis-open.org` OASIS (*Organization for the Advancement of Structured Information Standards*) est un consortium international spécialisé dans le développement de standards relatifs à la sécurité Web, le commerce électronique, les transactions commerciales, la logistique et l'interopérabilité entre différents marchés.

`http://www.ietf.org` L'*Internet Engineering Task Force* (IETF) est une communauté, agissant au niveau international, de chercheurs, designers de réseau, fournisseurs et utilisateurs. Elle se concentre sur le développement de l'architecture internet et le bon fonctionnement d'internet par l'intermédiaire de protocoles.

Chaque standard IETF est publié en tant que RFC (*Request for Comments*, cf. `http://www.ietf.org/rfc.html`) et est gratuit. Il existe six sortes de RFC : propsed standards, draft standards, Internet standards, experimental protocols, Informational documents et historic standards. Seules les trois premières (proposed, draft, et full) sont des standards IETF au sens strict du terme (cf. également un résumé à ce sujet sous `http://www.ietf.org/rfc/rfc1796.txt`).

`http://www.ieee.org` L'*Institute of Electrical and Electronics Engineers* (IEEE) est une organisation qui crée les standards dans les domaines de la technologie d'information, des télécommunications, de la médecine et de la santé, du transport, entre autres. Les standards IEEE sont payants.

`http://www.iso.org` Le comité ISO (*Internationl Organization for Standards*) est le plus grand développeur de standards et gère un réseau d'instituts de standardisation nationaux dans plus de 140 pays. Les standards ISO sont payants.

`http://www.din.de`, `http://www.din.com`
Le Deutsches Institut für Normung (DIN) est une association technico-scientifique déclarée et fut fondé en 1917. DIN se définit comme "l'institution responsable en Allemagne des travaux de normalisation et le représentant des intérêts allemands dans les organisations de normalisation internationales et européeennes".

L'association est un regroupement de fabricants, consommateurs, artisans, entreprises de prestation de services, scientifiques et autres personnes qui sont intéressés par la création de normes. Les normes sont payantes et peuvent être commandées sur le site de DIN.

Page de manuel de reiserfsck

```
REISERFSCK(8)                                                REISERFSCK(8)

NAME
       reiserfsck - check a Linux Reiserfs file system

SYNOPSIS
       reiserfsck  [  -afprVy ] [ --rebuild-sb | --check | --fix-
       fixable | --rebuild-tree | --clean-attributes  ]  [  -j  |
       --journal device ] [ -z | --adjust-size ] [ -n | --nolog ]
       [ -l | --logfile file ] [ -q | --quiet ] [ -y | --yes ]  [
       -S  |  --scan-whole-partition ] [ --no-journal-available ]
       device

DESCRIPTION
       Reiserfsck searches for a Reiserfs filesystem on a device,
       replays  any  necessary transactions, and either checks or
       repairs the file system.

       device is the special file corresponding to the device  or
              partition  (e.g /dev/hdXX for IDE disk partition or
              /dev/sdXX for SCSI disk partition).

OPTIONS
       --rebuild-sb
              This option recovers the superblock on  a  Reiserfs
              partition.   Normally  you only need this option if
              mount reports "read_super_block: can't find a reis
              erfs  file system" and you are sure that a Reiserfs
              file system is there.
```

--check
This default action checks file system consistency and reports but does not repair any corruption that it finds. This option may be used on a read-only file system mount.

--fix-fixable
This option recovers certain kinds of corruption that do not require rebuilding the entire file sys tem tree (--rebuild-tree). Normally you only need this option if the --check option reports "corrup tion that can be fixed with --fix-fixable". This includes: zeroing invalid data-block pointers, cor recting st_size and st_blocks for directories, and deleting invalid directory entries.

--rebuild-tree
This option rebuilds the entire file system tree using leaf nodes found on the device. Normally you only need this option if the --check option reports "corruption that can be fixed only during --rebuild-tree". You are strongly encouraged to make a backup copy of the whole partition before attempting the --rebuild-tree option.

--clean-attributes
This option cleans reserved fields of Stat-Data items.

--journal device , -j device
This option supplies the device name of the current file system journal. This option is required when the journal resides on a separate device from the main data device (although it can be avoided with the expert option --no-journal-available).

--adjust-size, -z
This option causes reiserfsck to correct file sizes that are larger than the offset of the last discov ered byte. This implies that holes at the end of a file will be removed. File sizes that are smaller than the offset of the last discovered byte are corrected by --fix-fixable.

```
       --logfile file, -l  file
              This option causes reiserfsck to report any corrup
              tion it finds to the specified log file rather than
              stderr.

       --nolog, -n
              This option prevents reiserfsck from reporting  any
              kinds of corruption.

       --quiet, -q
              This  option prevents reiserfsck from reporting its
              rate of progress.

       --yes, -y
              This option inhibits reiserfsck from asking you for
              confirmation  after telling you what it is going to
              do, assuming yes. For safety, it does not work with
              the --rebuild-tree option.

       -a, -p These  options are usually passed by fsck -A during
              the automatic checking of those  partitions  listed
              in  /etc/fstab.  These  options cause reiserfsck to
              print some information  about  the  specified  file
              system,  check if error flags in the superblock are
              set and  do  some  light-weight  checks.  If  these
              checks reveal a corruption or the flag indicating a
              (possibly fixable) corruption is found set  in  the
              superblock,  then  reiserfsck  switches to the fix-
              fixable mode. If the flag indicating a  fatal  cor
              ruption  is found set in the superblock, then reis
              erfsck finishes with an error.

       -V     This option prints the  reiserfsprogs  version  and
              exit.

       -r, -f These options are ignored.

EXPERT OPTIONS
       DO  NOT  USE  THESE  OPTIONS  UNLESS YOU KNOW WHAT YOU ARE
       DOING.  WE ARE NOT RESPONSIBLE  IF  YOU  LOSE  DATA  AS  A
       RESULT OF THESE OPTIONS.
```

--no-journal-available
This option allows reiserfsck to proceed when the journal device is not available. This option has no effect when the journal is located on the main data device. NOTE: after this operation you must use reiserfstune to specify a new journal device.

--scan-whole-partition, -S
This option causes --rebuild-tree to scan the whole partition, not only used space on the partition.

EXAMPLE OF USING

1. You think something may be wrong with a reiserfs parti tion on /dev/hda1 or you would just like to perform a periodic disk check.

2. Run reiserfsck --check --logfile check.log /dev/hda1. If reiserfsck --check exits with status 0 it means no errors were discovered.

3. If reiserfsck --check exits with status 1 (and reports about fixable corruptions) it means that you should run reiserfsck --fix-fixable --logfile fixable.log /dev/hda1.

4. If reiserfsck --check exits with status 2 (and reports about fatal corruptions) it means that you need to run reiserfsck --rebuild-tree. If reiserfsck --check fails in some way you should also run reiserfsck --rebuild-tree, but we also encourage you to submit this as a bug report.

5. Before running reiserfsck --rebuild-tree, please make a backup of the whole partition before proceeding. Then run reiserfsck --rebuild-tree --logfile rebuild.log /dev/hda1.

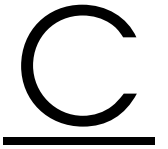
6. If the --rebuild-tree step fails or does not recover what you expected, please submit this as a bug report. Try to provide as much information as possible and we will try to help solve the problem.

EXIT CODES

reiserfsck uses the following exit codes:

0 - No errors.
1 - File system errors corrected.

```
          4 - File system fatal errors left uncorrected,
              reiserfsck --rebuild-tree needs to be launched.
          6 - File system fixable errors left uncorrected,
              reiserfsck --fix-fixable needs to be launched.
          8 - Operational error.
          16 - Usage or syntax error.

AUTHOR
       This version of reiserfsck  has  been  written  by  Vitaly
       Fertman <vitaly@namesys.com>.

BUGS
       There  are  likely  to be some bugs. Please report bugs to
       the ReiserFS mail-list <reiserfs-list@namesys.com>.

TODO
       Faster recovering, signal handling,  i/o  error  handling,
       etc.

SEE ALSO
       mkreiserfs(8),  reiserfstune(8)  resize_reiserfs(8), debu
       greiserfs(8),

Reiserfsprogs-3.6.9         April 2003              REISERFSCK(8)
```



Page de manuel-de e2fsck

NAME

e2fsck - check a Linux second extended file system

SYNOPSIS

e2fsck [-pacnyrdfvstDFSV] [-b superblock] [-B block size] [-l|-L bad_blocks_file] [-C fd] [-j external-journal] [-E extended_options] device

DESCRIPTION

e2fsck is used to check a Linux second extended file sys tem (ext2fs). E2fsck also supports ext2 filesystems coun taining a journal, which are also sometimes known as ext3 filesystems, by first applying the journal to the filesys tem before continuing with normal e2fsck processing. After the journal has been applied, a filesystem will nor mally be marked as clean. Hence, for ext3 filesystems, e2fsck will normally run the journal and exit, unless its superblock indicates that further checking is required.

device is the device file where the filesystem is stored (e.g. /dev/hdc1).

OPTIONS

-a This option does the same thing as the -p option. It is provided for backwards compatibility only; it is suggested that people use -p option whenever possible.

-b superblock
Instead of using the normal superblock, use an alternative superblock specified by superblock. This option is normally used when the primary superblock has been corrupted. The location of the backup superblock is dependent on the filesystem's blocksize. For filesystems with 1k blocksizes, a backup superblock can be found at block 8193; for filesystems with 2k blocksizes, at block 16384; and for 4k blocksizes, at block 32768.

Additional backup superblocks can be determined by using the mke2fs program using the -n option to print out where the superblocks were created. The -b option to mke2fs, which specifies blocksize of the filesystem must be specified in order for the superblock locations that are printed out to be accurate.

If an alternative superblock is specified and the filesystem is not opened read-only, e2fsck will make sure that the primary superblock is updated appropriately upon completion of the filesystem check.

-B blocksize
Normally, e2fsck will search for the superblock at various different block sizes in an attempt to find the appropriate block size. This search can be fooled in some cases. This option forces e2fsck to only try locating the superblock at a particular blocksize. If the superblock is not found, e2fsck will terminate with a fatal error.

-c This option causes e2fsck to run the badblocks(8) program to find any blocks which are bad on the filesystem, and then marks them as bad by adding them to the bad block inode. If this option is specified twice, then the bad block scan will be done using a non-destructive read-write test.

-C fd This option causes e2fsck to write completion

information to the specified file descriptor so that the progress of the filesystem check can be monitored. This option is typically used by pro grams which are running e2fsck. If the file descriptor specified is 0, e2fsck will print a com pletion bar as it goes about its business. This requires that e2fsck is running on a video console or terminal.

-d Print debugging output (useless unless you are debugging e2fsck).

-D Optimize directories in filesystem. This option causes e2fsck to try to optimize all directories, either by reindexing them if the filesystem sup ports directory indexing, or by sorting and com pressing directories for smaller directories, or for filesystems using traditional linear directo ries.

-E extended_options
Set e2fsck extended options. Extended options are comma separated, and may take an argument using the equals ('=') sign. The following options are sup ported:

ea_ver=extended_attribute_version
Assume the format of the extended attribute blocks in the filesystem is the specified version number. The ver sion number may be 1 or 2. The default extended attribute version format is 2.

-f Force checking even if the file system seems clean.

-F Flush the filesystem device's buffer caches before beginning. Only really useful for doing e2fsck time trials.

-j external-journal
Set the pathname where the external-journal for this filesystem can be found.

-l filename
Add the block numbers listed in the file specified by filename to the list of bad blocks. The format of this file is the same as the one generated by the badblocks(8) program. Note that the block num bers are based on the blocksize of the filesystem. Hence, badblocks(8) must be given the blocksize of the filesystem in order to obtain correct results. As a result, it is much simpler and safer to use the -c option to e2fsck, since it will assure that the correct parameters are passed to the badblocks program.

-L filename
Set the bad blocks list to be the list of blocks specified by filename. (This option is the same as the -l option, except the bad blocks list is cleared before the blocks listed in the file are added to the bad blocks list.)

-n Open the filesystem read-only, and assume an answer of ‘no’ to all questions. Allows e2fsck to be used non-interactively. (Note: if the -c, -l, or -L options are specified in addition to the -n option, then the filesystem will be opened read-write, to permit the bad-blocks list to be updated. However, no other changes will be made to the filesystem.)

-p Automatically repair ("preen") the file system without any questions.

-r This option does nothing at all; it is provided only for backwards compatibility.

-s This option will byte-swap the filesystem so that it is using the normalized, standard byte-order (which is i386 or little endian). If the filesys tem is already in the standard byte-order, e2fsck will take no action.

-S This option will byte-swap the filesystem, regard less of its current byte-order.

```
       -t     Print timing statistics for e2fsck.  If this option
              is  used  twice,  additional  timing statistics are
              printed on a pass by pass basis.

       -v     Verbose mode.

       -V     Print version information and exit.

       -y     Assume an answer of ‘yes’ to all questions;  allows
              e2fsck to be used non-interactively.

EXIT CODE
       The exit code returned by e2fsck is the sum of the follow
       ing conditions:
            0    - No errors
            1    - File system errors corrected
            2    - File system errors corrected, system should
                   be rebooted
            4    - File system errors left uncorrected
            8    - Operational error
            16   - Usage or syntax error
            32   - E2fsck canceled by user request
            128  - Shared library error

SIGNALS
       The following signals have the following effect when  sent
       to e2fsck.

       SIGUSR1
              This  signal  causes  e2fsck  to start displaying a
              completion bar.  (See discussion of the -C option.)

       SIGUSR2
              This signal causes e2fsck to stop displaying a com
              pletion bar.

REPORTING BUGS
       Almost any piece of  software  will  have  bugs.   If  you
       manage  to find a filesystem which causes e2fsck to crash,
       or which e2fsck is unable to repair, please report  it  to
       the author.
```

Please include as much information as possible in your bug report. Ideally, include a complete transcript of the e2fsck run, so I can see exactly what error messages are displayed. If you have a writeable filesystem where the transcript can be stored, the script(1) program is a handy way to save the output of e2fsck to a file.

It is also useful to send the output of dumpe2fs(8). If a specific inode or inodes seems to be giving e2fsck trou ble, try running the debugfs(8) command and send the out put of the stat(1u) command run on the relevant inode(s). If the inode is a directory, the debugfs dump command will allow you to extract the contents of the directory inode, which can sent to me after being first run through uuen code(1).

Always include the full version string which e2fsck dis plays when it is run, so I know which version you are run ning.

AUTHOR

This version of e2fsck was written by Theodore Ts'o <tytso@mit.edu>.

SEE ALSO

mke2fs(8), tune2fs(8), dumpe2fs(8), debugfs(8)

E2fsprogs version 1.34 July 2003 E2FSCK(8)

The GNU General Public License

GNU General Public License

Foreword

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the *GNU General Public License* is intended to guarantee your freedom to share and change free software — to make sure the software is free for all its users. This *General Public License* applies to most of the *Free Software Foundation's* software and to any other program whose authors commit to using it. (Some other *Free Software Foundation* software is covered by the *GNU Library General Public License* instead.) You can apply it to your programs, too.

When we speak of *"free" software*, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you

receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU General, Public License

Terms and Conditions for Copying, Distribution and Modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this *General Public License*. The "Program", below, refers to any such program or work, and a *work based on the Program* means either the Program or any derivative work

under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

1. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
2. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
3. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

1. Accompany it with the complete corresponding machine--readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
2. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
3. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, "complete source code" means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on

which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty--free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The *Free Software Foundation* may publish revised and/or new versions of the *General Public License* from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the *Free Software Foundation*. If the Program does not specify a version number of this License, you may choose any version ever published by the *Free Software Foundation*.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the *Free Software Foundation*, write to the *Free Software Foundation*; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

No Warranty

11. Because the program is licensed free of charge, there is no warranty for the program, to the extent permitted by applicable law. Except when otherwise stated in writing the copyright holders and/or other parties provide the program

"as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the program is with you. Should the program prove defective, you assume the cost of all necessary servicing, repair or correction.

12. In no event unless required by applicable law or agreed to in writing will any copyright holder, or any other party who may modify and/or redistribute the program as permitted above, be liable to you for damages, including any general, special, incidental or consequential damages arising out of the use or inability to use the program (including but not limited to loss of data or data being rendered inaccurate or losses sustained by you or third parties or a failure of the program to operate with any other programs), even if such holder or other party has been advised of the possibility of such damages.

End of Terms and Conditions

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
<one line to give the program's name and a brief
idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.
```

```
You should have received a copy of the GNU General Public
License along with this program; if not, write to the Free
Software Foundation, Inc., 59 Temple Place, Suite 330, Boston,
MA 02111-1307, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) <year> <name of author>

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type
'show w'. This is free software, and you  are welcome to
redistribute it under certain conditions; type 'show c' for
details.
```

The hypothetical commands `show w` and `show c` should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w` and `show c`; they could even be mouse-clicks or menu items—whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the
program 'Gnomovision' (which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1st April 1989 Ty Coon, President of Vice
```

This *General Public License* does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the *GNU Library General Public License* instead of this License.

Glossaire

Compte
voir ☞*Permissions d'accès*.

ACL (*Access Control List*)
Une extension du concept traditionnel de permission pour les fichiers et les répertoires.

ADSL (*Asymmetric Digital Subscriber Line*)
Procédé de transfert de données à travers le réseau téléphonique 100 fois plus rapide que RNIS (ISDN).

AGP (*Accelerated Graphics Port*)
Connecteur rapide pour cartes graphiques. Il est basé sur PCI mais offre une ☞*Largeur de bande* nettement plus importante que celui-ci. À la différence des modèles PCI, les cartes graphiques AGP peuvent accéder directement (sans passer par le processeur) à la ☞*mémoire de travail* et y stocker des données graphiques.

Mémoire de travail (*memory*)
Mémoire physique de capacité limitée à laquelle on peut accéder rapidement.

ATAPI (*Advance Technology Attachment Packet Interface*)
Généralement désigné aujourd'hui sous le nom de ☞*IDE* ou ☞*EIDE*. Le mot Advance remonte à une époque où les disques durs avaient une capacité de 10 Mo et étaient encore extrêmement lents.

Backup
Backup est le mot anglais pour les copies de sauvegarde. On devrait faire régulièrement des copies de sauvegarde, particulièrement pour les données importantes.

Largeur de bande
Capacité de transfert maximale d'un canal de données.

Compte d'utilisateur (*user account*)
Voir ☞*Compte*.

Répertoire d'utilisateur (*home directory*)
Voir ☞*Répertoire personnel*.

Système d'exploitation (*operating system*)
Le système d'exploitation est un programme qui tourne continuellement en arrière-plan sur une machine et qui constitue la base qui rend possible tout travail effectué avec la machine.

BIOS (*Basic Input Output System*)
Petit élément qui se charge de l'initialisation des composants matériels essentiels dans les premières secondes qui suivent le démarrage du système. Ce processus d'une importance primordiale ne s'achève, dans un système Linux, que lorsque ☞*LILO* apparaît.

Amorçage (*bootstrap = tirant de botte*)
L'amorçage (appelé aussi boot) désigne le processus de chargement d'un système, à partir de l'allumage de la machine jusqu'au moment où le système est à la disposition de l'utilisateur.

Navigateur
Programme pour l'affichage de documents et pour la recherche dans le contenu des documents. Aujourd'hui, le navigateur est principalement utilisé pour la représentation graphique des contenus de pages web (☞*World Wide Web*)

Cache
Mémoire temporaire, relativement petite par rapport à la ☞*mémoire de travail*, mais néanmoins très rapide. Le cache sert, par exemple, à stocker des fichiers qui ont déjà été ouverts. On peut ainsi gagner du temps lorsqu'on a de nouveau besoin de ces fichiers car il n'est pas nécessaire de les faire charger à partir du disque dur.

Client
Station de travail en réseau à laquelle le ☞*serveur* fournit des services.

CPU (*Central Processing Unit*)
☞*Processeur*.

Curseur
Petit élément graphique qui marque l'emplacement où se fait la saisie.

Daemon (*Disk and execution monitor*)
Programme qui veille en arrière-plan et entre en action en cas de besoin. Ces daemons (démons) répondent, par exemple, aux requêtes FTP ou HTTP et coordonnent aussi les activités dans les slots des cartes PCMCIA.

Système de fichiers (*filesystem*)
Méthode de structuration des fichiers. Il existe un très grand nombre de systèmes de fichiers dont les performances sont parfois très différentes.

DDC (*Direct Display Channel*)
Standard de communication entre le moniteur et la carte graphique servant à transmettre à la carte graphique différents paramètres tels que, par exemple, le nom du moniteur ou la résolution.

DNS (*Domain Name System*)
Système pour la conversion d'adresses ☞*WWW* en adresses ☞*TCP/IP* et vice versa.

E-Mail (*electronic mail*)
Méthode de transfert de courriers électroniques entre utilisateurs de machines intégrées dans un réseau local ou connectées à Internet.

EIDE (*Enhanced Integrated Drive Electronics*)
Standard ☞*IDE* amélioré qui permet l'utilisation de disques durs de plus de 512 Mo.

Invite (*prompt*)
Sous un ☞*Shell*, interpréteur de commandes en mode texte, l'emplacement où les commandes peuvent être transmises au ☞*système d'exploitation* est marqué par l'invite.

Ethernet
Standard courant pour ordinateur connectés à des réseaux peu étendus géographiquement.

EXT2 (*second extended Filesystem*)
Système de fichiers standard utilisé par Linux.

FAQ (*Frequently Asked Questions*)
Acronyme très répandu signifiant Questions fréquemment posées ou Foire Aux Questions. Il s'agit de documents qui apportent une réponse aux questions qui se posent le plus souvent.

Gestionnaire de fenêtres (*window manager*)
Couche au-dessus du ☞*système X-Window* qui est surtout garante de la prise en charge de la représentation du bureau. Il existe un très grand nombre de gestionnaires de fenêtres. L'un des plus populaires est kwm pour ☞*KDE*.

Logiciel libre
Voir ☞*GNU*.

Firewall
Pare feu qui relie un réseau local à Internet et en assure la sécurité avec différentes mesures.

FTP (*file transfer protocol*)
☞*Protocole* basé sur ☞*TCP/IP* pour le transfert de fichiers.

GNU (*GNU is Not Unix*)
GNU est un projet de la Free Software Foundation (FSF)™. L'objectif du projet GNU, auquel le nom de RICHARD STALLMAN (RMS) est étroitement lié, est la création d'un système d'exploitation libre compatible Unix ; le mot free étant employé ici beaucoup moins dans le sens de *gratuit* que de *libre freedom* pour ce qui concerne le droit d'accès aux programmes ainsi que le droit de les utiliser et de les modifier. Pour que la liberté du texte source, c'est-à-dire du code des programmes, soit respectée, toute modification doit également être *libre* : la liberté d'un logiciel ne doit donc pas être restreinte par la modification ou l'ajout d'un code de programme. Il est expliqué dans le manifeste GNU classique comment cela peut être garanti (`http://www.gnu.org/gnu/manifesto.html`) ; les logiciels GNU sont juridiquement protégés par la GNU General Public License, en abrégé GPL (`http://www.gnu.org/copyleft/gpl.html`, ou par la GNU Lesser General Public License, en abrégé LGPL (`http://www.gnu.org/copyleft/lgpl.html`).

Dans le cadre du projet GNU, tous les programmes auxiliaires Unix font l'objet d'un nouveau développement et sont en partie dotés d'une fonctionnalité plus complète ou améliorée. Mais certains systèmes logiciels complexes (par exemple Emacs ou la glibc) sont aussi au centre du projet.

Le noyau ☞*Linux*, soumis aux termes de la GPL, profite de ce développement (en particulier des outils) mais il ne doit pas être confondu avec le projet lui-même.

GNOME (*GNU Network Object Model Environment*)
Une interface graphique confortable supplémentaire pour Linux ; semblable à KDE.

GPL (*GNU GENERAL PUBLIC LICENSE*)
Voir ☞*GNU*.

Répertoire personnel (*home directory*)
Répertoire privé dans le système de fichiers Linux appartenant en propre à un utilisateur (généralement `/home/<nom_d'utilisateur>`). Cet utilisateur est le seul à avoir des droits d'accès complets à ce répertoire.

Nom d'hôte
Nom d'une machine Linux sous lequel elle est généralement accessible dans le réseau.

HTML (*Hypertext Markup Language*)
Le plus important langage utilisé sur le web (☞*World Wide Web*) pour l'affichage de documents. Les commandes de formatage mises à disposition par HTML déterminent l'aspect et la présentation du document qui sera affiché par un ☞*navigateur*.

HTTP (*Hypertext Transfer Protocol*)
Protocole utilisé entre les ☞*navigateurs* et les serveurs Internet pour le transfert de pages ☞*HTML* sur le web (☞*World Wide Web*).

IDE (*Integrated Drive Electronics*)
Standard de disques durs très répandu, particulièrement sur les PC d'entrée et de milieu de gamme.

IRQ (*Interrupt Request*)
Demande d'attribution de ressources CPU adressée par un programme ou un composant matériel au ☞*système d'exploitation*

Internet
Réseau mondial basé sur le protocole ☞*TCP/IP* et comptant un très grand nombre d'utilisateurs.

Adresse IP
Adresse numérique constituée de 4 blocs séparés par des points (par exemple 192.168.10.1) assignée à une machine dans un réseau ☞*TCP/IP*.

RNIS (ISDN, *Integrated Services Digital Network*)
Standard numérique pour le transfert rapide des données à travers le réseau téléphonique.

Caractère joker
Caractère de substitution tenant la place d'un (symbole : ?) ou de plusieurs (symbole : *) caractères inconnus. Les caractères jokers sont fréquemment utilisés dans les commandes, particulièrement dans les commandes de recherche.

KDE (*K Desktop Environment*)
Confortable Interface graphique pour Linux, semblable à GNOME.

Noyau
Cœur du système d'exploitation Linux sur lequel sont basés tous les programmes et la majeure partie des pilotes.

Console (*console*, *terminal*)
Autrefois, la console était assimilée au ☞*terminal*. Sous Linux il existe ce que l'on appelle les *consoles virtuelles*. Elles permettent d'utiliser un seul écran pour plusieurs sessions de travail indépendantes mais simultanées.

LAN (*local area network*)
Réseau informatique s'étendant sur un rayon très limité.

Signet (*bookmark*)
Collection, généralement personnelle, de liens que l'on insère dans le navigateur. Les signets permettent d'accéder directement aux pages web jugées intéressantes.

LILO (*Linux Loader*)
Petit programme qui s'installe dans le secteur d'amorçage du disque dur. LILO peut lancer aussi bien Linux que d'autres systèmes d'exploitation.

Lien
Référence croisée vers d'autres fichiers, utilisée aussi couramment sur Internet que dans le système de fichiers Linux. Dans ce dernier cas on distingue cependant les liens durs et les liens symboliques. Alors que les liens durs font référence à un emplacement dans le système de fichiers, les liens symboliques ne font référence qu'au nom du fichier.

Linux
Système d'exploitation similaire à UNIX, librement distribué aux termes de la GPL (☞*GNU*). Son nom (Linus' uniX) est dérivé du nom de son créateur Linus Torvalds. Bien qu'à proprement parler ce terme ne s'applique qu'au noyau, on entend généralement par Linux l'ensemble du système d'exploitation, y compris les applications.

Login
Procédure de connexion effectuée par un utilisateur pour accéder à un système ou à un réseau.

Logout
Procédure de déconnexion effectuée par l'utilisateur qui quitte le système.

Pages de manuel
La documentation des systèmes Unix se trouve traditionnellement dans les pages de manuel (ou pages de man) que l'on peut faire afficher avec la commande `man`.

MBR (*master boot record*)
Secteur maître d'amorçage. C'est le premier secteur physique d'un disque dur dont le contenu est chargé dans la mémoire de travail par le ☞*BIOS* lors du démarrage du système. Ce code charge soit le système d'exploitation à partir d'une partition de disque dur amorçable, soit un chargeur d'amorçage complexe tel que ☞*LILO* par exemple.

MD5
Un algorithme générant des sommes de contrôle.

Monter
Rattacher des systèmes de fichiers dans l'arborescence des répertoires du système.

Multitâche
Les systèmes d'exploitation pouvant exécuter simultanément plusieurs programmes sont appelés systèmes multitâches.

MP3
Procédé de compression très efficace pour fichiers audio. La taille d'un fichier compressé est réduite à environ un dixième de la taille du même fichier non compressé.

Multiulisateur
Un système multiutilisateur est un système sur lequel plusieurs personnes peuvent travailler simultanément.

Réseau (*net*, *network*)
Interconnexion de plusieurs machines réalisée généralement au moyen de ☞*serveurs* et de ☞*clients*.

NFS (*network file system*)
☞*Protocole* pour l'accès aux ☞*systèmes de fichiers* des machines en réseau.

NIS (*Network Information Service*)
Système pour la gestion centrale des informations d'administration du réseau. NIS permet tout particulièrement de gérer et de synchroniser les noms d'utilisateurs dans l'ensemble du réseau.

Partition
Unités logiques d'un disque dur indépendantes les unes des autres et pouvant contenir différents systèmes de fichiers. Sous Windows, les partitions sont aussi appelées unités de disque (*drives*).

Chemin d'accès (*path*)
Le chemin d'accès définit sans aucune ambiguïté l'emplacement d'un fichier à l'intérieur d'un système de fichiers.

Plug and Play
Technologie pour la configuration automatique de composants matériels. Les ressources telles que, par exemple, IRQ, DMA ou autres sont configurées et gérées par le système de manière autonome.

Prompt
Voir ☞*Invite*.

Protocole (*protocol*)
Standard spécifique défini qui règle la communication au niveau matériel et logiciel ainsi qu'au niveau du réseau. Il existe un très grand nombre de protocoles. Les plus courants sont ☞*HTTP* et ☞*FTP*.

Proxy
Serveur fonctionnant souvent chez les fournisseurs d'accès Internet comme mémoire temporaire (cache). Il sert à stocker des contenus de pages dans une base de données à partir de laquelle ces pages peuvent être fournies

directement aux machines qui les demandent. Ce procédé permet non seulement de réduire le temps nécessaire au téléchargement mais aussi d'économiser de la bande passante.

Processus (*process*)
Les programmes ou les fichiers exécutables tournent en tant que processus et peuvent être observés dans un ☞*shell*, par exemple avec `top`. Ce terme est souvent employé comme synonyme de tâche.

Processeur
Le processeur est le cerveau d'un ordinateur. Il traduit en langage machine les commandes de l'utilisateur ou des programmes et il les exécute. Le processeur exerce un contrôle sur l'ensemble du système et réalise les performances de calcul proprement dites.

RAM (*Random Access Memory*)
Voir ☞*Mémoire de travail*.

ReiserFS
Un système de fichiers qui enregistre ses modifications dans un journal. Ainsi, contrairement à Ext2, le système de fichiers peut être reconstitué très rapidement. ReiserFS est optimisé pour des petits fichiers.

Racine (*root*)
C'est la personne qui, dans un système complexe ou un réseau, se charge des configurations et de la maintenance. L'administrateur système (root) est le seul à avoir accès à toutes les ressources d'un système (il possède les droits root).

SCSI (*Small Computer Systems Interface*)
Standard de disques durs qui, en raison de sa grande rapidité, est surtout utilisé pour les ☞*serveurs* et pour les ordinateurs de haut de gamme.

Serveur
Le serveur est le plus souvent une machine très puissante qui fournit des données et des services à d'autres machines (☞*clients*) connectées au réseau. Il existe en outre des programmes qui, en raison de leur disponibilité et des services qu'ils fournissent, sont aussi désignés sous le nom de serveurs.

Shell
Ligne de saisie de commandes extrêmement flexible qui dispose très souvent d'un propre langage de programmation. Quelques exemples pour le shell sont bash, sh et tcsh.

SMTP (*Simple Mail Transfer Protocol*)
☞*Protocole* pour le transfert des courriers électroniques (☞*E-Mails*).

SSL (*Secure Socket Layer*)
Procédé pour l'encryptage de données transférées par ☞*HTTP*.

Super utilisateur (*super user*)
Voir ☞*Racine*.

Administrateur système (*system administrator, root user*)
Voir ☞*Racine*.

Tâche
Voir ☞*Processus*.

TCP/IP
Protocole de communication Internet. Il est de plus en plus souvent utilisé dans les réseaux locaux que l'on désigne alors sous le nom d'Intranet.

Telnet
Telnet est le ☞*protocole* et la commande permettant de communiquer avec d'autres machines (*hosts*).

Terminal (*terminal*)
Ce terme désignait autrefois la combinaison clavier/écran reliée à un ordinateur central. Sur une machine multiutilisateur, c'est une combinaison clavier/écran sans propres ressources de calcul. Sur les stations de travail, ce terme désigne aussi des programmes qui émulent un véritable terminal.

Pilote (*driver*)
Programme situé entre le système d'exploitation et le matériel et qui traduit les communications entre ces deux couches.

Tux
Nom du pingouin Linux (voir `http://www.sjbaker.org/tux/`).

Environnement (*environment*)
Un ☞*shell* procure, en règle générale, un environnement dans lequel l'utilisateur peut temporairement effectuer certains paramétrages. Ceux-ci concernent, par exemple, les noms des chemins d'accès aux programmes, le nom de l'utilisateur, le chemin courant, l'aspect de l'invite, etc. Ces données sont insérées dans une ☞*variable d'environnement*. Ces variables d'environnement peuvent être positionnées, par exemple, dans les fichiers de configuration de l'interpréteur de commandes shell.

Variable d'environnement (*environment variable*)
Une place dans l'☞*environnement* du ☞*shell*. Chaque variable d'environnement a un nom, le plus souvent spécifié en majuscules. Il est assigné aux variables d'environnement des valeurs telles que, par exemple, des noms de chemins d'accès.

UNIX
Système d'exploitation très répandu surtout sur les stations de travail en réseau. Depuis le début des années 90, une version libre de UNIX est disponible aussi pour les PC.

URL (*Uniform Resource Locator*)
Adresses Internet précises qui indiquent le type de la page (par exemple `http://`) et le nom du serveur (par exemple `www.suse.de`).

Répertoire (*directory*)
Les répertoires constituent la structure hiérarchique d'un ☞*système de fichiers*. Le répertoire contient la liste des noms de fichiers ou de répertoires.

VESA (*Video Electronics Standard Association*)
Association des constructeurs de cartes graphiques et de moniteurs qui ont défini, entre autres, d'importants standards vidéo.

Wildcard
Voir ☞*Caractère joker*.

Windowmanager
Voir ☞*Gestionnaire de fenêtres*.

Répertoire racine (*root directory*)
C'est le répertoire situé au sommet du ☞*système de fichiers*. Contrairement à tous les autres répertoires du système de fichiers, le répertoire racine n'a pas de répertoire de niveau supérieur. Le répertoire racine est symbolisé par `/` sous UNIX.

WWW (*World Wide Web*)
Partie graphique de l'Internet basée sur le protocole ☞*HTTP* et que l'on peut parcourir avec un navigateur web.

X11
Voir ☞*Système X Window*.

Système X Window

Le système X Window s'est établi comme standard pour les interfaces graphiques sous Linux. À la différence d'autres systèmes, il ne pose que les bases, par exemple la communication avec le matériel, qui permettent au ☞*gestionnaire de fenêtres*, par exemple ☞*KDE*, de fournir des interfaces individuelles.

YaST (*Yet another Setup Tool*)

L'assistant du système de SUSE LINUX.

YP (*yellow pages*)

Voir ☞*NIS*.

Permissions d'accès (*account*)

C'est l'ensemble constitué par le nom d'utilisateur *login name* et le mot de passe *password*. Le compte est en général créé par l'☞*administrateur système*. Il détermine également à quel groupe le nouvel utilisateur doit appartenir et quels droits lui sont attribués.

Bibliographie

[1] *SUSE LINUX* (Guide de l'utilisateur). SUSE, 10. Édition ©2004 .

[2] EDWARD C. BAILEY. *Maximum RPM*. ©1997 . ISBN 1-888172-78-9.

[3] BRYAN COSTALES, ERIC ALLMAN, NEIL RICKERT. *sendmail*. ©1993 . ISBN 1-56592-056-2.

[4] WERNER ALMESBERGER. *LILO User's guide [Guide de l'utilisateur de LILO]*. `file:///usr/share/doc/lilo/user.dvi`.

[5] OLAF KIRCH. *LINUX Network Administrator's Guide [Administration réseau sous Linux]*. ©1995 . ISBN 1-56592-087-2.

[6] CHIN FANG, BOB CROSSON, ERIC S. RAYMOND. *The Hitchhiker's Guide to X386/XFree86 Video Timing (or, Tweaking your Monitor for Fun and Profit)*. ©1993 .

[7] SEBASTIAN HETZE, DIRK HOHNDEL, MARTIN MÜLLER, OLAF KIRCH. *Linux Anwenderhandbuch [Le guide de l'utilisateur Linux]*. 6. Édition ©1996 . ISBN 3-929764-05-9.

[8] SIMON GARFINKEL, GENE SPAFFORD. *Practical UNIX Security [La sécurité UNIX en pratique]*. ©1993 . ISBN 0-937175-72-2.

[9] CRAIG HUNT. *TCP/IP Netzwerk Administration [L'administration réseau TCP/IP]*. ©1995 . ISBN 3-930673-02-9.

[10] TIM O'REILLY, GRACE TODINO. *Managing UUCP and Usenet [Gérer UUCP et Usenet]*. ©1992 . ISBN 0-937175-93-5.

[11] MATT WELSH. *Linux Installation and Getting Started [Installation et démarrage de Linux]*. 2. Édition ©1994 . ISBN 3-930419-03-3.

[12] LINDA LAMB. *Learning the vi Editor [Le guide vi]*. ©1990 . ISBN 0-937175-67-6.

[13] MATT WELSH, LARS KAUFMAN. *Running Linux [Le système Linux]*. ©1995 O'Reilly. ISBN 1-56592-100-3.

[14] JÜRGEN SCHNEIDERER. *Sicherheit Kostenlos – Firewall mit Linux [La sécurité gratuite – Pare-feu avec Linux]*. ©1998 iX.

[15] MICHAEL KIENLE. *TIS: Toolkit für anwendungsorientie Firewall-Systeme [TIS : Toolkit pour les systèmes de pare-feu orientés utilisateurs]*. ©1995 iX.

[16] WILLIAM R. CHESWICK, STEVEN M. BELLOVIN. *Firewalls und Sicherheit im Internet [Pare-feu et sécurité Internet]*. ©1996 Addison Wesley. ISBN 3-89319-875-x.

[17] BRENT CHAPMAN, ELISABETH D. ZWICKY. *Einrichten von Internet Firewalls [Mise en place de pare-feu Internet]* (*Sicherheit im Internet gewährleisten [Assurer la sécurité Internet]*). ©1996 O'Reilly. ISBN 3-930673312.

[18] CLIFFORD STOLL. *Kuckucksei. Die Jagd auf die deutschen hacker, die das Pentagon knackten [Le nid du coucou. La longue traque d'un espion dans le labyrinthe de l'espionage informatique]*. ©1998 Fischer-TB. Verlag. ISBN 3-596139848.

[19] BRIAN TUNG. *Kerberos: A Network Authentication System [Kerberos : un système d'authentification en réseau]*. ©1999 Fischer-TB. Verlag. ISBN 0-201-37924-4.

Index

Symboles

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Y

Z