

Red Hat Enterprise Linux 4

Introduction à l'administration système



Red Hat Enterprise Linux 4: Introduction à l'administration système

Copyright © 2005 par Red Hat, Inc.



Red Hat, Inc.

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

rhel-isa(FR)-4-Impression-RHI (2004-08-25T17:11)

Copyright © 2005 par Red Hat, Inc. Ce produit ne peut être distribué qu'aux termes et conditions stipulés dans la licence Open Publication License, V1.0 ou successive (la dernière version est actuellement disponible à l'adresse suivante : <http://www.opencontent.org/openpub/>).

Toute distribution de versions modifiées du contenu du présent document est interdite sans l'autorisation explicite du détenteur du copyright.

Toute distribution du contenu du document ou d'un dérivé de ce contenu sous la forme d'un ouvrage imprimé standard quel qu'il soit, à des fins commerciales, est interdite sans l'autorisation préalable du détenteur du copyright.

Red Hat et le logo "Shadow Man" de Red Hat sont des marques déposées de Red Hat, Inc. aux États-Unis et dans d'autres pays.

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

Le code GPG de la clé security@redhat.com est :

CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Table des matières

Introduction	i
1. Informations spécifiques aux architectures.....	i
2. Conventions de documentation.....	ii
3. Activation de votre abonnement.....	iv
3.1. Saisie d'un nom de connexion Red Hat.....	v
3.2. Saisie d'un numéro d'abonnement.....	v
3.3. Connexion de votre système.....	v
4. Prochainement.....	vi
4.1. Faites-nous part de vos commentaires !.....	vi
1. Philosophie de l'administration système	1
1.1. Automatisez toute activité.....	1
1.2. Documentez de toute activité.....	2
1.3. Communiquez autant que possible.....	3
1.3.1. Dites à vos utilisateurs ce que vous allez faire.....	4
1.3.2. Dites à vos utilisateurs ce que vous faites.....	5
1.3.3. Dites à vos utilisateurs ce que vous avez fait.....	5
1.4. Connaissez vos ressources.....	6
1.5. Connaissez vos utilisateurs.....	6
1.6. Connaissez votre entreprise.....	7
1.7. Ne considérez pas la sécurité comme une mesure après coup.....	7
1.7.1. Dangers de l'ingénierie sociale.....	8
1.8. Planifiez à l'avance.....	8
1.9. Attendez-vous à l'inattendu.....	9
1.10. Informations spécifiques à Red Hat Enterprise Linux.....	9
1.10.1. Automatisation.....	9
1.10.2. Documentation et communication.....	10
1.10.3. Sécurité.....	11
1.11. Ressources supplémentaires.....	12
1.11.1. Documentation installée.....	12
1.11.2. Sites Web utiles.....	12
1.11.3. Livres sur le sujet.....	13
2. Contrôle des ressources	15
2.1. Concepts de base.....	15
2.2. Contrôle de la performance du système.....	15
2.3. Contrôle de la capacité du système.....	16
2.4. Que contrôler ?.....	16
2.4.1. Contrôle de la puissance de CPU.....	17
2.4.2. Contrôle de la largeur de bande.....	18
2.4.3. Contrôle de la mémoire.....	19
2.4.4. Contrôle du stockage.....	20
2.5. Informations spécifiques à Red Hat Enterprise Linux.....	20
2.5.1. free.....	21
2.5.2. top.....	22
2.5.3. vmstat.....	23
2.5.4. Sysstat, la suite d'outils de contrôle des ressources.....	25
2.5.5. OProfile.....	28
2.6. Ressources supplémentaires.....	32
2.6.1. Documentation Installée.....	32
2.6.2. Sites Web utiles.....	33
2.6.3. Livres sur le sujet.....	33

3. Puissance de traitement et largeur de bande.....	35
3.1. Largeur de bande.....	35
3.1.1. Bus	35
3.1.2. Chemins des données.....	36
3.1.3. Problèmes potentiels liés à la largeur de bande	36
3.1.4. Solutions potentielles à des problèmes liés à la largeur de bande	37
3.1.5. En résumé	38
3.2. Puissance de traitement.....	38
3.2.1. Informations sur la puissance de traitement.....	38
3.2.2. Consommateurs de puissance de traitement	39
3.2.3. Réponse à une insuffisance de CPU.....	40
3.3. Informations spécifiques à Red Hat Enterprise Linux	42
3.3.1. Contrôle de la largeur de bande sur Red Hat Enterprise Linux	42
3.3.2. Contrôle de l'utilisation CPU sur Red Hat Enterprise Linux	45
3.4. Ressources supplémentaires.....	49
3.4.1. Documentation installée.....	49
3.4.2. Sites Web utiles.....	49
3.4.3. Livres sur le sujet.....	49
4. Mémoire physique et mémoire virtuelle	51
4.1. Modes d'accès au stockage	51
4.2. Éventail des options de stockage	51
4.2.1. Registres du CPU.....	52
4.2.2. Mémoire cache.....	52
4.2.3. Mémoire principale — RAM.....	54
4.2.4. Disques durs.....	54
4.2.5. Stockage de sauvegarde hors ligne	55
4.3. Concepts élémentaires de la mémoire virtuelle	56
4.3.1. Mémoire virtuelle expliquée simplement	56
4.3.2. Mémoire auxiliaire — la pierre angulaire de la mémoire virtuelle	57
4.4. Mémoire virtuelle : informations détaillées.....	57
4.4.1. Défauts de pages	58
4.4.2. Jeu de pages de travail	58
4.4.3. Échange (ou swapping).....	59
4.5. Implications de la mémoire virtuelle au niveau de la performance	59
4.5.1. Pire scénario de performance.....	60
4.5.2. Meilleur scénario de performance	60
4.6. Informations spécifiques à Red Hat Enterprise Linux	61
4.7. Ressources supplémentaires.....	64
4.7.1. Documentation installée.....	64
4.7.2. Sites Web utiles.....	64
4.7.3. Livres sur le sujet.....	64
5. Gestion du stockage	67
5.1. Bref aperçu du matériel de stockage.....	67
5.1.1. Plateaux de disque.....	67
5.1.2. Périphérique de lecture/écriture des données.....	68
5.1.3. Bras d'accès	68
5.2. Concepts d'adressage en matière de stockage	69
5.2.1. Adressage basé sur la géométrie.....	69
5.2.2. Adressage basé sur les blocs	71
5.3. Interfaces des périphériques de stockage de masse	71
5.3.1. Aperçu historique.....	71
5.3.2. Interfaces actuelles aux normes de l'industrie	72
5.4. Caractéristiques de performance des disques durs.....	75
5.4.1. Limitations mécaniques/électriques	76
5.4.2. Charges des E/S et performance	77

5.5. Mise en utilisation du stockage.....	79
5.5.1. Partitions/Tranches.....	79
5.5.2. Systèmes de fichiers.....	80
5.5.3. Structure de répertoire.....	83
5.5.4. Activation de l'accès au stockage.....	84
5.6. Technologies avancées de stockage.....	84
5.6.1. Stockage accessible en réseau.....	84
5.6.2. Stockage basé sur RAID.....	85
5.6.3. Gestionnaire de volumes logiques (LVM).....	91
5.7. Gestion quotidienne du stockage.....	92
5.7.1. Contrôle de l'espace libre.....	92
5.7.2. Problèmes liés aux quotas de disque.....	95
5.7.3. Problèmes liés aux fichiers.....	96
5.7.4. Ajout/Suppression de stockage.....	98
5.8. Commentaires sur les sauvegardes.....	104
5.9. Informations spécifiques à Red Hat Enterprise Linux.....	104
5.9.1. Conventions de nommage des périphériques.....	104
5.9.2. Éléments de base des systèmes de fichiers.....	107
5.9.3. Montage de systèmes de fichiers.....	109
5.9.4. Stockage réseau sous Red Hat Enterprise Linux.....	112
5.9.5. Montage automatique de systèmes de fichiers avec <code>/etc/fstab</code>	113
5.9.6. Ajout/Suppression de stockage.....	114
5.9.7. Implémentation de quotas de disque.....	118
5.9.8. Création de matrices RAID.....	122
5.9.9. Gestion quotidienne des matrices RAID.....	124
5.9.10. Gestionnaire de volumes logiques (LVM).....	125
5.10. Ressources supplémentaires.....	125
5.10.1. Documentation installée.....	125
5.10.2. Sites Web utiles.....	126
5.10.3. Livres sur le sujet.....	126
6. Gestion des comptes utilisateur et de l'accès aux ressources.....	129
6.1. Gestion des comptes utilisateur.....	129
6.1.1. Nom d'utilisateur.....	129
6.1.2. Mots de passe.....	132
6.1.3. Informations relatives au contrôle d'accès.....	137
6.1.4. Gestion quotidienne des comptes et de l'accès aux ressources.....	138
6.2. Gestion des ressources de l'utilisateur.....	140
6.2.1. Qui peut avoir accès aux données partagées ?.....	140
6.2.2. Où les utilisateurs peuvent-ils avoir accès aux données partagées ?.....	141
6.2.3. Quelles barrières sont mises en place afin d'éviter la mauvaise utilisation des ressources ?.....	142
6.3. Informations spécifiques à Red Hat Enterprise Linux.....	143
6.3.1. Comptes utilisateur, groupes et permissions.....	143
6.3.2. Fichiers contrôlant les comptes utilisateur et groupes.....	145
6.3.3. Applications pour les comptes utilisateur et groupes.....	148
6.4. Ressources supplémentaires.....	150
6.4.1. Documentation installée.....	150
6.4.2. Sites Web utiles.....	151
6.4.3. Livres sur le sujet.....	151

7. Imprimantes et impression.....	153
7.1. Types d'imprimantes.....	153
7.1.1. Considérations en matière d'impression.....	153
7.2. Imprimantes à impact.....	155
7.2.1. Imprimantes matricielles à aiguilles.....	155
7.2.2. Imprimantes à marguerite.....	155
7.2.3. Imprimantes ligne.....	156
7.2.4. Consommables des imprimantes à impact.....	156
7.3. Imprimantes à jet d'encre.....	156
7.3.1. Consommables des imprimantes à jet d'encre.....	156
7.4. Imprimantes laser.....	157
7.4.1. Imprimantes couleur laser.....	158
7.4.2. Consommables des imprimantes laser.....	158
7.5. Autres types d'imprimantes.....	158
7.6. Langages et technologies d'imprimante.....	159
7.7. Imprimantes locales contre imprimantes réseau.....	160
7.8. Informations spécifiques à Red Hat Enterprise Linux.....	160
7.9. Ressources supplémentaires.....	162
7.9.1. Documentation installée.....	162
7.9.2. Sites Web utiles.....	162
7.9.3. Livres sur le sujet.....	162
8. Préparation à un sinistre.....	165
8.1. Types de sinistres.....	165
8.1.1. Pannes matérielles.....	165
8.1.2. Pannes logicielles.....	171
8.1.3. Pannes environnementales.....	174
8.1.4. Erreurs d'origine humaine.....	181
8.2. Sauvegardes.....	186
8.2.1. À données de types différents, besoins de sauvegarde différents.....	186
8.2.2. Logiciels de sauvegarde : acheter ou construire ?.....	187
8.2.3. Types de sauvegardes.....	188
8.2.4. Support de sauvegarde.....	190
8.2.5. Stockage des sauvegardes.....	192
8.2.6. Problèmes de restauration.....	192
8.3. Récupération suite à un sinistre.....	193
8.3.1. Élaboration, test et mise en oeuvre d'un plan de récupération après sinistre.....	194
8.3.2. Centres de secours : froids, doux et chauds.....	195
8.3.3. Disponibilité matérielle et logicielle.....	196
8.3.4. Disponibilité des sauvegardes.....	196
8.3.5. Connectivité réseau au centre de secours.....	197
8.3.6. Personnel du centre de secours.....	197
8.3.7. Retour à la normale.....	197
8.4. Informations spécifiques à Red Hat Enterprise Linux.....	198
8.4.1. Assistance logicielle.....	198
8.4.2. Technologies de sauvegarde.....	198
8.5. Ressources supplémentaires.....	202
8.5.1. Documentation installée.....	202
8.5.2. Sites Web utiles.....	202
8.5.3. Livres sur le sujet.....	203
Index.....	205
Colophon.....	213

Introduction

Bienvenue au manuel d'*Introduction à l'administration système de Red Hat Enterprise Linux*.

Ce guide d'*Introduction à l'administration système de Red Hat Enterprise Linux* contient des informations de base à l'intention des nouveaux administrateurs de systèmes Red Hat Enterprise Linux. L'intention de ce guide n'est *pas* de vous apprendre à effectuer une tâche particulière sous Red Hat Enterprise Linux, mais plutôt de vous transmettre les connaissances générales que les administrateurs système plus expérimentés ont acquises au fil des années avec l'expérience.

Ce guide part de la supposition que vous disposez d'une expérience limitée en tant qu'utilisateur de Linux mais n'avez aucune expérience quant à l'administration de systèmes Linux. Si vous êtes un nouveau venu au monde de Linux en général (et de Red Hat Enterprise Linux en particulier), nous vous conseillons de vous procurer d'abord un livre d'introduction au monde de Linux.

Chaque chapitre de ce manuel d'*Introduction à l'administration système de Red Hat Enterprise Linux* observe la structure suivante :

- Aperçu générique du matériel — Cette section aborde le sujet du chapitre sans entrer dans les détails quant à un système d'exploitation, une technologie ou une méthodologie spécifiques.
- Matériel spécifique à Red Hat Enterprise Linux — Cette section aborde certains aspects du sujet qui sont en relation avec Linux en général et avec Red Hat Enterprise Linux en particulier.
- Ressources supplémentaires pour un approfondissement des connaissances — Cette section inclut des pointeurs vers d'autres manuels traitant de Red Hat Enterprise Linux, des sites Web utiles et des livres contenant des informations applicables au sujet abordé.

Grâce à une structure homogène, les lecteurs peuvent lire plus facilement le guide d'*Introduction à l'administration système de Red Hat Enterprise Linux* en fonction de leurs besoins. Un administrateur système ayant une certaine expérience avec Red Hat Enterprise Linux pourrait par exemple se contenter de survoler les sections dédiées spécifiquement à Red Hat Enterprise Linux, alors qu'un nouvel administrateur système pourrait lui commencer en lisant seulement les sections donnant un aperçu générique et pourrait se servir des sections spécifiques à Red Hat Enterprise Linux comme une introduction fournissant des ressources plus détaillées.

Au niveau des ressources plus détaillées, le *Guide d'administration système de Red Hat Enterprise Linux* constitue une excellente source d'informations sur la manière d'effectuer certaines tâches spécifiques dans un environnement Red Hat Enterprise Linux. Les administrateurs nécessitant des informations factuelles plus détaillées devraient se reporter au *Guide de référence de Red Hat Enterprise Linux*.

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



Remarque

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

1. Informations spécifiques aux architectures

À moins que cela ne soit indiqué différemment, toutes les informations contenues dans ce manuel s'appliquent uniquement au processeur x86 et aux processeurs comprenant les technologies Intel®

Extended Memory 64 Technology (Intel® EM64T) et AMD64. Afin d'obtenir des informations spécifiques aux architectures, reportez-vous au *Guide d'installation de Red Hat Enterprise Linux* correspondant à votre architecture.

2. Conventions de documentation

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

`commande`

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

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

`nom de fichier`

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

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

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

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

application

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

Utilisez **Mozilla** pour parcourir le Web.

[touche]

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

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

[combinaison]-[touche]

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

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

texte trouvé sur une interface GUI

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

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

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

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

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

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

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

bouton dans un écran ou une fenêtre GUI

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

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

sortie d'ordinateur

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

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

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

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

invite

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

```
$
#
[stephen@maturin stephen]$
leopard login:
```

saisie de l'utilisateur

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

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

remplaçable

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

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

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



Remarque

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



Astuce

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



Important

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



Attention

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



Avertissement

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

3. Activation de votre abonnement

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

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

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

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

3.1. Saisie d'un nom de connexion Red Hat

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

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

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

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

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

```
https://rhn.redhat.com/help/forgot\_password.pxt
```

3.2. Saisie d'un numéro d'abonnement

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

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

3.3. Connexion de votre système

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

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

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

4. Prochainement

Ce manuel d'*Introduction à l'administration système de Red Hat Enterprise Linux* fait partie de l'engagement croissant de Red Hat à fournir une assistance utile et opportune aux utilisateurs de Red Hat Enterprise Linux. Au fur et à mesure que de nouvelles versions de Red Hat Enterprise Linux seront disponibles, nous nous efforçons autant que possible d'inclure aussi bien la nouvelle documentation que la documentation révisée à l'intention des utilisateurs.

4.1. Faites-nous part de vos commentaires !

Si vous remarquez une faute de frappe dans ce manuel d'*Introduction à l'administration système de Red Hat Enterprise Linux* ou si vous avez des suggestions pour améliorer ce manuel, n'hésitez pas à nous en faire part. Veuillez soumettre votre rapport par l'entremise de Bugzilla (<http://bugzilla.redhat.com/bugzilla>) dans la partie `rhel-isa`.

Prenez soin de bien mentionner les références du manuel :

```
rhel-isa(FR)-4-Improvement-RHI (2004-08-25T17:11)
```

En mentionnant précisément les références de ce manuel, vous nous permettez d'identifier exactement la version du manuel dont vous disposez.

Si vous avez des suggestions pour améliorer la documentation, essayez d'être aussi précis que possible. Si vous avez trouvé une erreur, veuillez inclure le numéro de la section et un extrait du texte l'entourant afin que nous puissions facilement la retrouver.

Chapitre 1.

Philosophie de l'administration système

Bien que les caractéristiques de la fonction d'administrateur système puissent varier d'une plateforme à une autre, un certain nombre d'aspects demeurent néanmoins identiques. Ces aspects mêmes constituent la philosophie de l'administration système.

Parmi ces derniers figurent :

- Automatisez de toute activité
- Documentez toute activité
- Communiquez autant que possible
- Connaissez vos ressources
- Connaissez vos utilisateurs
- Connaissez votre entreprise
- Ne considérez pas la sécurité comme une mesure après coup
- Planifiez à l'avance
- Attendez-vous à l'inattendu

Les sections suivantes examinent chacun de ces aspects de manière détaillée.

1.1. Automatisez toute activité

La plupart des administrateurs système sont dépassés par le nombre — de leurs utilisateurs ou de leurs systèmes, voire des deux. Dans bien des cas, l'automatisation est le seul moyen de garder le contrôle de la situation. D'une manière générale, toute tâche devant être effectuée plusieurs fois devrait être perçue comme une possibilité d'automatisation.

Ci-dessous figure une liste de certaines tâches couramment automatisées :

- Vérification et rapportage de l'espace disque disponible
- Création de sauvegardes
- Recueil de données sur les performances du système
- Maintenance des comptes utilisateur (création, suppression, etc.)
- Fonctions spécifiques à l'activité de l'entreprise (transmission de nouvelles données au serveur Web, création de rapports mensuels/trimestriels/annuels, etc.)

Cette liste n'est en aucun cas exhaustive ; les fonctions automatisées par les administrateurs système ne sont en fait limitées que par la volonté de ces derniers à rédiger les scripts appropriés. Dans ce cas, être fainéant (et demander à l'ordinateur d'effectuer la plupart des tâches banales) est en fait une très bonne chose.

En outre, l'automatisation offre aux utilisateurs l'avantage supplémentaire d'un service plus prévisible et uniforme.



Astuce

Rappelez-vous que si vous devez automatiser une tâche, il est fort probable que vous ne soyez pas le premier administrateur système à devoir le faire. Ce cas de figure illustre la situation dans laquelle les avantages des logiciels Open Source sont les plus explicites — vous pourrez peut-être réutiliser le travail d'une autre personne afin d'automatiser la procédure manuelle qui monopolise actuellement tout votre temps. Dans de telles circonstances, assurez-vous bien de toujours effectuer des recherches sur le Web avant de vous embarquer dans l'écriture de tout script d'une complexité supérieure à un petit script en Perl.

1.2. Documentez de toute activité

Si un administrateur système moyen avait le choix entre l'installation d'un tout nouveau serveur et l'écriture d'un document de procédure sur la manière d'effectuer des sauvegardes système, il choisirait à chaque fois la première option. Dans tous les cas de figure, vous *devez* documenter vos activités. De nombreux administrateurs système reportent à plus tard la mise à jour des documents nécessaires pour un certain nombre de raisons :

"Je pourrai toujours le faire plus tard."

Malheureusement, ce n'est généralement pas le cas. Même si l'administrateur système pense vraiment être en mesure de faire la mise à jour ultérieurement, la nature du travail d'administrateur système est telle que les tâches quotidiennes sont généralement trop chaotiques pour "le faire plus tard." Pis encore, plus cette tâche est reportée, plus le nombre d'informations oubliées augmente et moins le document final sera détaillé (est par conséquent, moins il sera utile).

"Pourquoi tout mettre par écrit, je m'en rappellerai bien."

À moins que vous ne fassiez partie de ces rares personnes dotées d'une incroyable mémoire photographique, vous ne pourrez pas vous rappeler des informations nécessaires. Pis encore, vous ne vous rappellerez que de la moitié des faits, sans même vous rendre compte qu'il vous manque une bonne partie de la situation. Dans de telles circonstances, vous perdrez un temps considérable à essayer soit de réapprendre ce que vous avez oublié, soit de réparer ce que vous aurez endommagé à cause de votre compréhension incomplète de la situation.

"Si je m'en rappelle, je ne serai pas licencié — Je bénéficierai de la sécurité de l'emploi !"

Alors que cette approche pourra vraisemblablement fonctionner pendant un certain temps, elle se traduira au long terme par une sécurité de l'emploi réduite — et non — accrue. Imaginez un instant ce qui pourrait se produire en cas d'urgence. Il se peut que vous ne soyez pas disponible ; les documents que vous aurez rédigés permettront peut-être d'éviter une catastrophe en donnant à une autre personne les moyens de résoudre la situation en votre absence. De plus, n'oubliez jamais que c'est dans les cas d'urgence que la direction a tendance à analyser les choses de manière détaillée. Dans de telles conditions, il est préférable que votre travail de documentation fasse partie de la solution plutôt que de voir votre absence faire partie du problème.

De plus, si vous faites partie d'une petite entreprise en expansion, il y a de fortes chances qu'un autre poste d'administrateur système soit créé dans le futur. Comment cette personne pourra-t-elle vous assister si toutes les informations sont dans votre tête ? Pis encore, toute absence de documentation de votre part pourrait vous rendre si indispensable que toute promotion pourrait être pour cette raison même, considérée avec réticence. Vous pourriez même finir par travailler pour la personne recrutée à l'origine pour vous épauler.

Dans de telles circonstances, vous verrez certainement les avantages de maintenir la documentation relative aux systèmes. Ce point nous amène à la question suivante. Que devriez-vous documenter ? Ci-après figure une liste partielle des aspects devant faire l'objet de documentation :

Politiques

Les politiques sont rédigées pour établir de façon claire et formelle la relation que vous entretenez avec votre communauté d'utilisateurs. Elles définissent clairement à vos utilisateurs, la manière selon laquelle leurs requêtes de ressources et/ou d'assistance sont traitées. La nature, le style et la méthode selon lesquels ces politiques sont disséminées parmi votre communauté varient de société à société.

Procédures

Les procédures décrivent, étape par étape, les différentes actions devant être effectuées afin d'accomplir une certaine tâche. Parmi les procédures à documenter peuvent figurer entre autres, les procédures de sauvegarde, les procédures de gestion des comptes utilisateur, les procédures de rapportage de problèmes. Tout comme pour l'automatisation, si une procédure est suivie plus d'une fois, il est toujours bon de la documenter.

Changements

Une grande partie de la carrière d'un administrateur système évolue autour de changements devant être effectués — comme la configuration du système visant à maximiser les performances, l'amélioration des scripts, la modification de fichiers de configuration, etc. Tout ces changements devraient faire l'objet de documentation sous une forme ou sous une autre. Dans le cas contraire, vous pourriez avoir une idée très confuse quant à une modification que vous avez effectuée il y a quelques mois.

Bien que certaines sociétés utilisent des méthodes plus complexes pour effectuer un suivi des changements, dans bien des cas, il est suffisant d'inclure un simple historique de révision au début du fichier faisant l'objet de modifications. Toute entrée faisant partie de l'historique de révision devrait comporter au strict minimum les éléments suivants :

- Le nom ou les initiales de la personne effectuant les modifications
- La date à laquelle la modification a été effectuée
- La raison pour laquelle la modification a été effectuée

Ces éléments, spécifiés dans des entrées concises mais informatives, pourraient ressembler à l'extrait ci-dessous :

ECB, 12-Juin-2002 — Entrée mise à jour pour la nouvelle imprimante du service comptabilité (pour permettre la prise en charge de la capacité d'impression en duplex de l'imprimante de remplacement)

1.3. Communiquez autant que possible

Lorsqu'il s'agit de vos utilisateurs, il n'y a jamais trop de communication. N'oubliez pas que de petits changements qui pour vous, sont à peine remarquables, pourraient en revanche être à l'origine d'une confusion totale pour le/la secrétaire des Ressources Humaines.

La méthode selon laquelle vous communiquez avec vos utilisateurs peut varier en fonction de votre entreprise. Certaines entreprises utilisent l'email, d'autres utilisent un site Web interne. D'autres peuvent décider de recourir à Usenet ou IRC. (de l'anglais Internet Relay Chat) pour faire circuler les informations. Dans certaines entreprises, une note écrite sur un morceau de papier placé sur le tableau d'affichage de la salle de pause pourra même suffire. Dans tous les cas, il est important d'utiliser la ou les méthodes qui fonctionnent le mieux dans votre environnement spécifique.

D'une manière générale, il est bon de suivre l'approche utilisée dans la rédaction d'articles de presse, à savoir :

1. Dites à vos utilisateurs ce que vous allez faire

2. Dites à vos utilisateurs ce que vous faites
3. Dites à vos utilisateurs ce que vous avez fait

Les sections suivantes examinent toutes ces étapes en détail.

1.3.1. Dites à vos utilisateurs ce que vous allez faire

Avant d'apporter quelque modification que ce soit, assurez-vous de bien en avertir vos utilisateurs suffisamment longtemps à l'avance. La durée de la période nécessaire pour prévenir vos utilisateurs varie non seulement en fonction du type de modification à apporter (la mise à niveau d'un système d'exploitation nécessite une mise en garde plus longue que le simple changement de la couleur par défaut de l'écran de connexion du système) mais également en fonction de la nature de la communauté de vos utilisateurs (des utilisateurs plus expérimentés au niveau technique seront probablement plus à même de faire face à des changements que des utilisateurs disposant d'un minimum de connaissances techniques).

Au minimum, vous devriez décrire les éléments suivants :

- La nature du changement
- Le moment où il aura lieu
- La raison pour laquelle il doit être effectué
- La durée estimée de l'opération
- L'impact (le cas échéant) que ce changement aura sur les utilisateurs
- Les coordonnées des personnes à contacter pour toute question ou inquiétude

Imaginez la situation hypothétique suivante. Depuis un certain temps, le service des finances rencontre des problèmes avec son serveur de base de données qui, de temps à autre, est très lent. Vous allez mettre le serveur hors service, mettre son module CPU à niveau en le remplaçant par un module plus rapide puis le redémarrer. Une fois ces opérations effectuées, vous allez déplacer la base de données elle-même vers un stockage plus rapide basé sur une matrice RAID. Dans une situation de ce genre, vous pourriez communiquer la message suivant à votre communauté d'utilisateurs :

Temps d'indisponibilité du système prévu pour vendredi soir

Ce vendredi à partir de 18:00 heure, heure locale (24:00 heure pour notre bureau de Berlin), aucune application financière ne sera disponible pour une durée d'environ quatre heures.

Pendant cette période, des modifications seront apportées aussi bien au matériel qu'au logiciel du serveur de base de données du Service des Finances. Grâce à ces modifications, l'obtention des comptes de crédit et des comptes de débit sera beaucoup plus rapide, de même que la création du bilan hebdomadaire.

Outre la différence au niveau de la durée d'exécution, la plupart d'entre vous ne devraient remarquer aucun autre changement. Toutefois, pour ceux et celles d'entre vous qui ont écrit leurs propres requêtes SQL, sachez que le format de certains indices changera. Cet aspect est documenté sur le site Internet à la page Service des Finances.

Pour toute question, commentaire ou inquiétude, veuillez contacter l'Administration Système au poste 4321.

Un certain nombre de points méritent une attention toute particulière :

- Communiquez clairement le début et la durée de la période d'indisponibilité due au changement.
- Assurez-vous de bien donner l'heure à laquelle le changement commencera de manière à inclure *tous* les utilisateurs, quel que soit leur emplacement géographique.

- Utilisez des termes que vos utilisateurs comprendront. Les personnes touchées par ce changement se moquent de savoir que le nouveau module CPU est une unité de 2GHz avec deux fois plus de cache L2 ou que la base de données sera placée sur un volume logique RAID 5.

1.3.2. Dites à vos utilisateurs ce que vous faites

Cette étape est essentiellement un avertissement de dernière minute pour rappeler aux utilisateurs que le changement est désormais imminent ; cet avertissement devrait se présenter sous la forme d'un bref rappel du message précédent mais en soulignant cette fois-ci de manière explicite, l'aspect imminent du changement. ("La mise à niveau du système aura lieu CE SOIR."). Ce rappel offre également l'opportunité de répondre publiquement à toute question reçue suite au premier message.

Toujours selon notre exemple hypothétique, un avertissement de dernière minute pourrait ressembler à l'extrait suivant :

période d'indisponibilité du système prévue pour *CE soir*

Rappel : La période d'indisponibilité du système annoncée lundi dernier aura lieu comme prévu ce soir à 18:00 heure, heure locale (24:00 heure pour notre bureau de Berlin). La première annonce relative à ce changement est disponible sur notre site intranet à la page Administration Système.

De nombreuses personnes ont demandé si elles devaient finir leur journée plus tôt ce soir afin de s'assurer que leur travail puisse être sauvegardé avant que la période d'indisponibilité du système ne commence. Les changements effectués ce soir ne touchant aucune opération faite sur les postes de travail individuels, il ne sera pas nécessaire de finir plus tôt que d'habitude.

Il convient ici de rappeler à ceux et celles d'entre vous qui ont rédigé leurs propres requêtes SQL que le format de certains indices changera. Cet aspect est documenté sur le site intranet à la page Service des Finances.

Vos utilisateurs ont été avertis, vous êtes désormais prêt à effectuer le travail nécessaire.

1.3.3. Dites à vos utilisateurs ce que vous avez fait

Après avoir effectué les changements nécessaires, vous *devez* expliquer à vos utilisateurs ce que vous avez fait. Là encore, il ne devrait s'agir que d'un résumé des messages précédents (il est indiscutable que certaines personnes ne les auront pas lus.)¹

Toutefois, il reste encore une opération importante à effectuer. Il est important d'informer vos utilisateurs sur l'état actuel du système. La mise à niveau s'est-elle passée sans problème ? Le nouveau serveur de stockage était-il fonctionné pour le service d'ingénierie mais pas pour celui des Finances ? Ces aspects associés au changement doivent être mentionnés ici.

Il va de soi que si l'état est différent de celui communiqué précédemment, ce point devra non seulement être souligné de manière claire et explicite mais il sera également important d'informer les utilisateurs sur les mesures prises (le cas échéant) afin d'arriver à la solution finale.

Dans notre situation hypothétique, la durée d'indisponibilité était source de problème. Le nouveau module CPU ne fonctionnait pas ; en téléphonant au fabricant du système il s'est avéré qu'une version spéciale du module était nécessaire afin de pouvoir effectuer les mises à niveau appropriées. Du bon côté des choses, la migration de la base de données sur le volume RAID s'est passée sans problème (même si elle a pris plus de temps qu'escompté en raison des problèmes associés au module CPU).

Pour une telle situation, l'annonce reproduite ci-dessous pourrait être communiquée aux utilisateurs :

1. Assurez-vous de bien envoyer ce message dès que le travail a été effectué et *avant* de quitter le bureau. En effet, une fois parti, il est beaucoup trop facile d'oublier d'informer vos utilisateurs et de les laisser dans l'obscurité quant à la possibilité d'utiliser ou non le système.

Fin de la durée d'indisponibilité du système

La durée d'indisponibilité totale du système prévue pour vendredi (reportez-vous à la page Administration Système de notre site intranet) est désormais terminée. Malheureusement, en raison de problèmes matériels une des tâches n'a pas pu être effectuée. Dans de telles circonstances, les tâches restantes ont pris plus longtemps que la durée prévue de quatre heures. Malgré ce petit problème, tous les systèmes étaient à nouveau en production avant minuit, heure locale (06:00 heure du matin pour notre bureau de Berlin).

En raison des problèmes matériels persistants, la performance des comptes de crédits et des comptes de débits ainsi que celle du rapport de bilan ne sera accrue que légèrement par rapport à la prévision d'origine. Il sera donc nécessaire de prévoir une deuxième période d'indisponibilité qui sera annoncée dès que les problèmes ayant entravés l'achèvement des opérations seront résolus.

Veillez noter que la période d'indisponibilité a entraîné le changement de certains indices de base de données ; ceux et celles d'entre vous qui ont écrit leurs propres requêtes SQL devraient se reporter à la page Service des Finances disponible sur notre site intranet.

Pour toute question, veuillez contacter l'Administration Système au poste 4321.

Grâce à ce type d'informations, vos utilisateurs disposeront de connaissances suffisantes pour d'une part, pouvoir poursuivre leur travail et d'autre part, être en mesure de comprendre l'impact que les changements auront sur leur activité.

1.4. Connaissez vos ressources

L'administration système consiste essentiellement à équilibrer les ressources disponibles en fonction des personnes et des programmes qui les utilisent. Dans de telles circonstances et à moins que vous n'ayez une excellente connaissance des ressources dont vous disposez, votre carrière d'administrateur système sera courte et stressante.

Certaines de ces ressources sont assez évidentes :

- Les ressources système, telles que la puissance de traitement disponible, la mémoire et l'espace disque
- La largeur de bande du réseau
- Le montant du budget IT disponible

Mais d'autres ne seront pas forcément aussi évidentes :

- Le personnel des services d'opérations, les autres administrateurs système et même un(e) secrétaire
- L'heure (souvent d'une importance vitale lorsque cette dernière doit tenir compte de la durée pendant laquelle le système effectue des opérations de sauvegarde)
- La base de connaissances (qu'elles se présentent sous la forme de livres, documentation système ou le cerveau d'une personne employée par la société depuis une vingtaine d'années)

Il convient de souligner ici l'importance non seulement de faire un inventaire détaillé des ressources disponibles auxquelles vous avez accès mais également de *le tenir à jour* — en matière de ressources disponibles, un manque de "connaissances de la situation" (ou Situational Awareness) peut s'avérer pire encore qu'une *absence totale* de connaissances en la matière.

1.5. Connaissez vos utilisateurs

Bien que certaines personnes se hérissent à la mention du terme "utilisateurs" (peut-être en raison de l'emploi du terme de manière dérogatoire par certains administrateurs système), il est utilisé dans ce manuel sans connotation aucune. Ainsi, les utilisateurs représentent les personnes qui utilisent les

systèmes et ressources dont vous êtes responsables — rien de plus, rien de moins. En tant que tel, les utilisateurs jouent un rôle central dans votre capacité à administrer vos systèmes avec succès ; sans une bonne connaissance de vos utilisateurs, comment pouvez-vous espérer comprendre les ressources système dont ils ont besoin ?

Prenez l'exemple d'un caissier dans une banque. Dans le cadre de son travail, ce dernier utilise un nombre bien défini d'applications et ne nécessite que peu de ressources système. Un ingénieur de développement logiciel en revanche utilisera probablement de nombreuses applications différentes et recevra toujours avec enthousiasme des ressources système supplémentaires (permettant un temps de construction plus rapide). Deux utilisateurs complètement différents avec des besoins complètement différents.

Assurez-vous donc de connaître vos utilisateurs aussi précisément que possible.

1.6. Connaissez votre entreprise

Que vous soyez employé par une grande multinationale ou le collègue d'une petite communauté, il est essentiel que vous compreniez la nature de l'environnement professionnel dans lequel vous travaillez. Cette connaissance peut se résumer en une seule question :

Quel est le but des systèmes que vous administrez ?

À cet égard, il est essentiel de comprendre le but de vos systèmes dans un sens plus global :

- Les applications devant être exécutées dans un cadre temporel particulier, comme à la fin d'une année, d'un mois ou d'un trimestre
- Les moments pendant lesquels les opérations de maintenance du système peuvent avoir lieu
- Les nouvelles technologies pouvant être utilisées afin de résoudre des problèmes dont l'entreprise souffre depuis longtemps

En prenant compte de l'activité de votre entreprise, les décisions que vous prendrez quotidiennement créeront une meilleure situation pour vos utilisateurs et pour vous-même.

1.7. Ne considérez pas la sécurité comme une mesure après coup

Indépendamment de votre perception de l'environnement dans lequel vos systèmes tournent, l'aspect sécurité ne doit jamais être sous-estimé. Même les systèmes autonomes, pourtant pas connectés à l'Internet, ne sont pas à l'abri de dangers (bien que les dangers encourus diffèrent évidemment de ceux auxquels un système connecté au monde extérieur est exposé).

Il est par conséquent extrêmement important, lors de toute action ou décision, de prendre en compte les implications au niveau de la sécurité. La liste suivante illustre les différents aspects que vous devriez toujours prendre en considération :

- La nature des menaces possibles sur chacun des systèmes dont vous avez la charge
- L'emplacement, le type et la valeur des données disponibles sur ces systèmes
- Le type et la fréquence de l'accès autorisé à ces systèmes

Lors de considérations de sécurité, ne commettez pas l'erreur de supposer que les agresseurs potentiels n'attaqueront vos systèmes que de l'extérieur. Dans bien des cas, l'agresseur vient de l'entreprise elle-même. La prochaine fois que vous passerez dans les bureaux, observez les gens autour de vous et posez-vous la question suivante :

Que se passerait-il si *cette* personne essayait de compromettre notre sécurité ?



Remarque

Ceci dit, nous n'insinuons *en aucun cas* ici que vous deviez traiter vos collègues comme s'ils étaient des criminels. Néanmoins, en adoptant cette approche consistant à examiner le type de travail que chaque personne effectue, vous serez à même de mieux déterminer le type de brèche de sécurité qu'une personne occupant un poste donné pourrait ouvrir, si telle était son intention.

1.7.1. Dangers de l'ingénierie sociale

Alors qu'au niveau de la sécurité, la première réaction de la plupart des administrateurs système est de se concentrer sur les aspects technologiques, il est important de mettre la situation en perspective. Bien souvent, les brèches de sécurité ne trouvent pas leur origine dans la technologie mais plutôt dans la nature humaine.

Les personnes qui s'intéressent aux infractions de sécurité utilisent souvent les vulnérabilités de la nature humaine pour contourner complètement les accès de contrôle basés sur la technologie. Ce phénomène est connu sous le terme d'*ingénierie sociale* (ou SE de l'anglais social engineering). Ci-après figure un exemple d'ingénierie sociale :

Le/la standardiste de la deuxième tournée reçoit un appel de l'extérieur. L'interlocuteur prétend être le directeur des finances de votre entreprise (le nom et d'autres informations sur ce dernier ont été obtenus à partir du site Web de l'entreprise, sur la page "Équipe de direction").

L'interlocuteur prétend téléphoner d'un endroit à l'autre bout du monde (cette information est peut-être une invention de toutes pièces ou il se peut que le site Web de votre entreprise contienne un communiqué de presse précisant que votre directeur des finances participe à un salon international).

L'interlocuteur se plaint ; son ordinateur portable a été volé à l'aéroport, il est en ce moment avec un client important et a besoin de l'accès à l'Internet de l'entreprise afin de vérifier l'état du compte de ce client. Le/la standardiste aurait-il/elle l'amabilité de lui fournir les informations nécessaires à l'autorisation de son accès ?

Savez-vous comment le/la standardiste de l'entreprise réagira ? À moins que le/la standardiste en question ne dispose de directives (sous la forme de politiques et procédures), vous ne savez pas vraiment quelles informations seront données.

Tout comme les feux de circulation, le but des politiques et procédures est de fournir des directives claires sur ce qui définit un comportement acceptable ou inacceptable. Toutefois, comme pour les feux de circulation, les politiques et procédures ne servent que si tout le monde les suit. Là est bien le cœur du problème — il est peu probable que tout le monde adhèrera à vos politiques et procédures. En fait, selon la nature de votre entreprise, vous ne disposez peut-être même pas de l'autorité nécessaire pour définir des politiques, est encore moins pour forcer leur application. Que faire dans ce cas-là ?

Malheureusement, il n'a pas de solutions faciles. L'éducation des utilisateurs peut aider à résoudre le problème ; faites tout ce qui est en votre pouvoir pour attirer l'attention de la communauté de vos utilisateurs sur les aspects de sécurité et sur l'ingénierie sociale. Faites des présentations sur la sécurité pendant le déjeuner. Disséminez les références d'articles liés à la sécurité grâce aux listes de diffusion de votre entreprise. Assurez-vous d'être disponible afin de pouvoir répondre aux utilisateurs ayant des questions à propos de choses qui leur semblent étranges.

En bref, disséminez le message parmi vos utilisateurs de toutes les manières possibles.

1.8. Planifiez à l'avance

Les administrateurs système qui ont compris l'importance de tous nos conseils et ont fait le maximum pour les suivre seront de remarquables professionnels — pour un jour. En effet, petit à petit, l'environnement change et un jour ou l'autre notre remarquable administrateur système se trouvera

pris au dépourvu. Pourquoi ? Parce que notre remarquable administrateur système n'a pas réussi à planifier à l'avance.

Certes, personne ne peut prédire l'avenir avec 100% d'exactitude. Toutefois, en ayant conscience de l'évolution de l'environnement informatique, il est relativement facile de lire les signes annonciateurs de changements :

- Lors d'une réunion hebdomadaire ennuyante, la mention à la volée d'un nouveau projet en cours d'articulation est le signe indiquant que vous devrez certainement prendre en charge de nouveaux utilisateurs dans l'avenir proche
- Des discussions autour d'une acquisition imminente signifie que vous serez peut-être responsable d'autres systèmes (qui ne seront pas forcément compatibles) implantés dans un ou plusieurs sites distants

La capacité à lire ces signes annonciateurs de changements (et à pouvoir prendre les mesures appropriées de manière efficace) peut grandement simplifier votre vie et celle des utilisateurs.

1.9. Attendez-vous à l'inattendu

Bien que l'expression "Attendez-vous à l'inattendu" soit quelque peu banale, elle reflète une réalité sous-jacente que tout administrateur système doit comprendre.

Il y a *aura* indubitablement des situations dans lesquelles vous serez pris au dépourvu.

Une fois cette réalité acceptée, que peut faire un administrateur système inquiet ? La réponse réside dans une certaine flexibilité, consistant à effectuer votre travail de telle sorte que vous donniez à vous-même et à vos utilisateurs, le maximum d'options possibles. Prenez par exemple les problèmes liés à l'espace disque. Étant donné que le manque permanent d'espace disque semble être une loi physique tout autant que celle de la gravité, il est raisonnable de supposer qu'à un moment donné, vous devrez faire face à un besoin désespéré d'espace disque supplémentaire *immédiat*.

Dans un tel cas, que ferait un administrateur système prêt à affronter l'inattendu ? Il est peut-être possible de garder quelques disques durs de secours sur les étagères juste au cas où il faudrait faire face à des problèmes matériels². Un tel disque de secours pourrait être déployé rapidement³ et temporairement afin de répondre à un besoin à court terme de disque dur, permettant ainsi de résoudre le problème de manière permanente (par exemple, en suivant la procédure normale pour fournir des disques durs supplémentaires).

En essayant d'anticiper les problèmes avant qu'ils ne se produisent, vous serez à même de répondre plus rapidement et de manière plus efficace qu'en vous laissant surprendre par les événements.

1.10. Informations spécifiques à Red Hat Enterprise Linux

Cette section fournit des informations relatives à la philosophie de l'administration système qui s'appliquent spécifiquement à Red Hat Enterprise Linux.

1.10.1. Automatisation

Pour être en mesure d'automatiser des tâches fréquemment effectuées sous Red Hat Enterprise Linux, il est nécessaire de connaître différents types de technologies. Tout d'abord, il y a les commandes qui

2. Il va de soi qu'un administrateur système qui s'attend à l'inattendu utiliserait RAID (ou des technologies similaires) pour réduire l'impact d'une panne de disque dur pendant la production.

3. Là encore, tout administrateur système prévoyant configure ses systèmes de telle sorte qu'il puisse ajouter aussi rapidement que possible un nouveau disque dur au système.

contrôlent le moment choisi de l'exécution de la commande ou du script. Pour ce genre de tâche, les commandes `cron` et `at` sont le plus souvent utilisées.

Pour incorporer un système de spécification temporel facile à comprendre mais en même temps très flexible, la commande `cron` est très utile car elle permet d'orchestrer l'exécution de commandes ou de scripts à intervalles récurrents, allant de quelques minutes à plusieurs mois. La commande `crontab` quant à elle, est utilisée pour manipuler les fichiers contrôlant le démon `cron` qui programme le moment de l'exécution de chaque tâche `cron`.

La commande `at` et la commande `batch` qui lui est étroitement liée, sont tout à fait appropriées pour programmer l'exécution unique de commandes et de scripts. Ces deux commandes implémentent un sous-système de traitement par lots, composé de files d'attente multiples ayant des priorités de programmation variées. On fait référence à ces priorités en tant que valeur de *níceness* (en raison du nom de la commande — *nice*). Les commandes `at` et `batch` sont toutes les deux idéales pour des tâches qui doivent absolument commencer à un moment donné, mais dont la fin n'a pas vraiment une importance vitale.

Il y a ensuite les différents langages de script, c'est-à-dire les "langages de programmation" que tout administrateur système moyen utilise afin d'automatiser des opérations manuelles. Il existe certes de nombreux scripts (et chaque administrateur système a tendance à avoir une préférence personnelle en la matière) mais nous nous contenterons d'énumérer ci-dessous seulement ceux qui sont les plus couramment utilisés :

- Le shell de commande `bash`
- Le langage de script `perl`
- Le langage de script `python`

Outre les différences évidentes existant entre ces langages, le point sur lequel ils diffèrent le plus est la manière dont ils interagissent avec d'autres programmes utilitaires sur un système Red Hat Enterprise Linux. Les scripts rédigés avec le shell `bash` ont tendance à utiliser de nombreux petits programmes utilitaires (comme par exemple, pour effectuer la manipulation de chaînes de caractères) alors que les scripts `perl` eux recourent à des fonctionnalités incorporées dans le langage lui-même pour effectuer ce type d'opérations. Le langage `python` quant à lui peut exploiter totalement les capacités orientées objet du langage permettant par là même d'allonger plus facilement des scripts complexes.

Dans de telles circonstances, il est nécessaire de bien connaître les nombreux programmes utilitaires (tels que `grep` et `sed`) qui font partie de Red Hat Enterprise Linux, afin de pouvoir vraiment maîtriser la création de scripts shell. L'apprentissage du langage `perl` (et `python`), d'autre part, tend à être un processus plus "autonome". Toutefois, de nombreux éléments du langage `perl` reposent sur la syntaxe de différents programmes utilitaires UNIX traditionnels, et en tant que tel, sont bien connus des administrateurs de systèmes Red Hat Enterprise Linux expérimentés en matière de création de scripts shell.

1.10.2. Documentation et communication

En matière de documentation et communication, peu de choses sont spécifiques à Red Hat Enterprise Linux. Étant donné que les activités de documentation et communication prennent des formes très diverses allant de l'ajout de commentaires dans un fichier de configuration de type texte à la mise à jour d'une page Web ou à l'envoi d'un email, un administrateur système utilisant Red Hat Enterprise Linux doit avoir accès à des éditeurs de texte, des éditeurs HTML et des clients de messagerie.

Ci-après figure une sélection limitée des nombreux éditeurs de texte disponibles sous Red Hat Enterprise Linux :

- L'éditeur de texte **gedit**
- L'éditeur de texte **Emacs**

- L'éditeur de texte `Vim`

L'éditeur de texte **gedit** est une application exclusivement graphique (en d'autres termes, elle nécessite un environnement actif du système X Window) alors que `vim` et **Emacs** eux sont par nature des applications de type texte.

Des discussions centrées sur le meilleur choix en matière d'éditeurs de texte sont en cours depuis la naissance des ordinateurs et ne s'arrêteront jamais. Dans de telles circonstances, la meilleure approche consiste à expérimenter avec chaque éditeur de texte pour finalement utiliser celui qui correspond le mieux à vos besoins.

Pour ce qui est des éditeurs HTML, les administrateurs système peuvent utiliser la fonction Composer du navigateur Web **Mozilla**. Bien sûr, certains administrateurs système préfèrent codifier manuellement leur page en HTML, et dans ce cas aussi, un éditeur de texte normal est un outil tout à fait acceptable.

Pour ce qui est des emails, Red Hat Enterprise Linux inclut le client de messagerie graphique **Evolution**, le client de messagerie **Mozilla** (qui est lui aussi graphique) et **mutt**, qui est lui de type texte. De même que pour le choix d'un éditeur de texte, celui d'un client de messagerie tend à se faire en fonction de préférences personnelles ; il est donc suggéré d'expérimenter avec chacun d'eux afin de choisir celui qui répond le mieux à vos besoins.

1.10.3. Sécurité

Comme nous l'avons mentionné précédemment dans ce chapitre, la sécurité ne peut pas être une mesure d'après coup et sous Red Hat Enterprise Linux, son approche n'est pas du tout superficielle. L'authentification et les contrôles de l'accès sont profondément intégrés dans le système d'exploitation et reposent sur différentes conceptions obtenues au cours d'une longue expérience dans la communauté UNIX.

Pour l'authentification, Red Hat Enterprise Linux utilise des modules d'authentification enfichables — aussi appelés PAM (de l'anglais Pluggable Authentication Modules). PAM permet de raffiner l'authentification des utilisateurs grâce à la configuration de bibliothèques partagées qui sont utilisées par toutes les applications prenant en charge PAM et ce, sans devoir apporter de changements quelconques aux applications elles-mêmes.

Le contrôle de l'accès sous Red Hat Enterprise Linux se fait en fonction des permissions traditionnelles de type UNIX (à savoir lecture, écriture et exécution ou `read`, `write`, `execute`) accordées aux catégories utilisateur, groupe ou "tout autre personne". Tout comme UNIX, Red Hat Enterprise Linux utilise également les bits `setuid` et `setgid` pour octroyer temporairement des droits d'accès étendus à des processus tournant sur un programme particulier et ce, en fonction de la propriété du fichier programme. Bien sûr il est essentiel que tout programme devant être exécuté avec des privilèges `setuid` ou `setgid` puisse être contrôlé afin de s'assurer qu'il n'existe aucune vulnérabilité exploitable.

Red Hat Enterprise Linux prend également en charge des listes de contrôle d'accès ou ACL (de l'anglais *access control lists*). Une ACL est un élément restrictif permettant d'exercer un contrôle minutieux sur des utilisateurs ou groupes pouvant accéder à un fichier ou répertoire. Par exemple, il est possible que les permissions d'un fichier interdisent tout accès aux personnes autres que le propriétaire du fichier mais qu'en même temps, l'ACL du fichier puisse être configurée de sorte que seul l'utilisateur `bob` puisse modifier le fichier (ou `write`) et que le groupe `finance` puisse le lire.

Un autre aspect important de la sécurité consiste à être capable d'effectuer un suivi de l'activité du système. Pour ce faire, Red Hat Enterprise Linux utilise énormément la journalisation, aussi bien au niveau du noyau qu'au niveau des applications. Cette activité est contrôlée par le démon de journalisation du système nommé `syslogd`, qui peut enregistrer des informations sur le système aussi bien localement (normalement dans des fichiers placés dans le répertoire `/var/log/`) que sur un système distant (qui sert de serveur de log attiré pour de multiples ordinateurs).

Les systèmes de détection d'intrusions (ou IDS, de l'anglais Intrusion Detection Systems) constituent un outil performant pour tout administrateur de systèmes Red Hat Enterprise Linux. Un IDS per-

met aux administrateurs système de déterminer si des changements non autorisés ont été effectués sur un ou plusieurs systèmes. La conception globale du système d'exploitation lui-même inclut des fonctionnalités de type IDS.

Étant donné que Red Hat Enterprise Linux est installé à l'aide du gestionnaire de paquetages RPM (appelé RPM), il est possible d'utiliser RPM pour contrôler si des changements ont été apportés aux paquetages incluant le système d'exploitation. Néanmoins, RPM étant essentiellement un outil de gestion de paquetages, ses capacités en tant qu'IDS sont quelque peu limitées. Ceci étant, il peut néanmoins constituer un bon point de départ dans le processus de détection de changements non autorisés effectués sur un système Red Hat Enterprise Linux.

1.11. Ressources supplémentaires

Cette section inclut un certain nombre de ressources pouvant être utilisées afin d'approfondir ses connaissances sur la philosophie de l'administration système et sur les thèmes spécifiques à Red Hat Enterprise Linux que nous avons abordés dans ce chapitre.

1.11.1. Documentation installée

Les ressources suivantes sont installées au cours d'une installation typique de Red Hat Enterprise Linux et peuvent vous aider à approfondir vos connaissances sur les thèmes examinés dans ce chapitre.

- Pages de manuel de `crontab(1)` et `crontab(5)` — Pour apprendre comment programmer l'exécution automatique de commandes et de scripts à intervalles réguliers.
- Page de manuel de `at(1)` — Pour apprendre comment programmer l'exécution automatique unique de commandes et de scripts à un moment ultérieur.
- Page de manuel de `bash(1)` — Pour en savoir plus sur le shell par défaut et la création de scripts shell.
- Page de manuel de `perl(1)` — Pour passer en revue la liste des pointeurs vers les nombreuses pages de manuel qui constituent la documentation en ligne de perl.
- Page de manuel de `python(1)` — Pour approfondir ses connaissances sur les options, fichiers et variables d'environnement qui contrôlent l'interpréteur Python.
- Page de manuel de `gedit(1)` et entrée du menu **Help** — Pour apprendre comment éditer des fichiers texte à l'aide de l'éditeur de texte graphique.
- Page de manuel de `emacs(1)` — Pour en savoir plus sur cet éditeur de texte hautement adaptable, y compris comment exécuter son tutoriel en ligne.
- Page de manuel de `vim(1)` — Pour apprendre comment utiliser cet éditeur de type texte performant.
- Entrée de menu **Contenu de l'aide de Mozilla** — Pour apprendre comment éditer des fichiers HTML, lire du courrier and naviguer le Web.
- Page de manuel de `evolution(1)` et entrée du menu **Help** — Pour apprendre comment gérer votre courrier à l'aide du client de messagerie graphique.
- Page de manuel de `mutt(1)` et fichiers contenus dans `/usr/share/doc/mutt-<version>` — Pour apprendre comment gérer votre courrier à l'aide de ce client de messagerie de type texte.
- Page de manuel de `pam(8)` et fichiers contenus dans `/usr/share/doc/pam-<version>` — Pour découvrir comment s'effectue l'authentification sous Red Hat Enterprise Linux.

1.11.2. Sites Web utiles

- <http://www.kernel.org/pub/linux/libs/pam/> — La page d'accueil du projet Linux-PAM.
- <http://www.usenix.org/> — La page d'accueil de USENIX, une organisation professionnelle se consacrant au rassemblement de professionnels de l'informatique venant de tous horizons et à la promotion d'une meilleure communication et innovation.
- <http://www.sage.org/> — Page d'accueil de System Administrators Guild, un groupe technique de USENIX particulier représentant une bonne ressource pour tous les administrateurs de systèmes responsables de systèmes d'exploitation Linux (ou de type Linux).
- <http://www.python.org/> — Le site Web du langage Python. Un excellent site pour approfondir ses connaissances du langage Python.
- <http://www.perl.org/> — Le site Web des Perl Mongers. Un excellent point de départ pour acquérir des connaissances sur Perl et se connecter à la communauté Perl.
- <http://www.rpm.org/> — La page d'accueil du gestionnaire de paquetages RPM. Le site Web le plus complet pour acquérir des connaissances sur RPM.

1.11.3. Livres sur le sujet

La plupart des livres sur l'administration système ne couvrent pas vraiment la philosophie sous-jacente de ce poste. Ils contiennent toutefois des sections fournissant des informations un peu plus détaillées sur les thèmes traités ici :

- *Guide de référence de Red Hat Enterprise Linux*; Red Hat, Inc. — Fournit un aperçu des endroits où se trouvent les fichiers système clés, les paramètres concernant les utilisateurs et groupes et la configuration des PAM.
- *Guide de sécurité de Red Hat Enterprise Linux*; Red Hat, Inc. — Examine en détail de nombreux thèmes en relation avec la sécurité qui concernent les administrateurs de systèmes Red Hat Enterprise Linux.
- *Guide d'administration système de Red Hat Enterprise Linux*; Red Hat, Inc. — Inclut des chapitres traitant de la gestion des utilisateurs et des groupes, de l'automatisation des tâches et de la gestion des fichiers journaux.
- *Linux Administration Handbook* (Guide de l'administration Linux) de Evi Nemeth, Garth Snyder et Trent R. Hein ; Prentice Hall — Fournit une section intéressante sur les politiques et la politique de l'administration système, y compris plusieurs discussions du type "que se passerait-il si" à propos de l'éthique.
- *Linux System Administration : A User's Guide* (Administration de systèmes Linux : Guide utilisateur) de Marcel Gagne ; Addison Wesley Professional — Contient un chapitre intéressant sur l'automatisation de différentes tâches.
- *Solaris System Management* (Management de Systèmes Solaris) de John Philcox ; New Riders Publishing — Bien que ce livre ne soit pas écrit spécifiquement pour Red Hat Enterprise Linux (ou même pour Linux en général) et utilise le terme "manager de systèmes" au lieu "d'administrateur système", ce livre offre au long de ses 70 pages une vue d'ensemble des rôles multiples que les administrateurs système jouent dans une entreprise traditionnelle.

Chapitre 2.

Contrôle des ressources

Comme nous l'avons mentionné précédemment, une grande partie de l'administration système est axée sur les ressources et leur utilisation de manière efficace. En comparant les différentes ressources avec les personnes et programmes qui les utilisent, il est possible non seulement d'économiser de l'argent mais également de satisfaire les utilisateurs autant que possible. Ceci étant, deux questions se posent :

Qu'entend-on par ressources ?

Et :

Comment peut-on savoir quelles ressources sont utilisées (et dans quelle mesure) ?

L'objectif de ce chapitre est de vous fournir les moyens nécessaires pour répondre à ces questions et ce, en vous aidant à approfondir vos connaissances sur les ressources et la manière de les contrôler.

2.1. Concepts de base

Avant d'être en mesure de contrôler les ressources, il est évidemment essentiel de savoir quelles ressources doivent être contrôlées. Dans tous les systèmes, les ressources suivantes sont disponibles :

- Puissance de CPU
- Largeur de bande
- Mémoire
- Stockage

Ces ressources sont traitées de manière plus détaillée dans les chapitres suivants. Toutefois, il suffit pour le moment de garder à l'esprit que ces ressources ont un impact direct sur les performances du système et par conséquent, sur la productivité et sur la satisfaction des utilisateurs.

De manière relativement simpliste, le contrôle des ressources n'est rien d'autre que l'obtention d'informations sur l'utilisation d'une ou plusieurs ressources système.

Ceci étant, le contrôle des ressources est rarement aussi simple. Il faut tout d'abord prendre en compte les ressources devant être contrôlées. Il est ensuite nécessaire d'examiner chaque système devant être contrôlé en prêtant une attention toute particulière à la situation spécifique de chaque système.

Les systèmes que vous surveillez se divisent en deux catégories selon la situation :

- Le système connaît de temps à autre des problèmes de performance et vous aimeriez améliorer la situation.
- Le système fonctionne parfaitement et vous souhaitez que la situation demeure ainsi.

Dans le premier cas, il est nécessaire de contrôler le système dans une perspective de performance système, alors que dans le deuxième cas, il faut contrôler les ressources système dans une perspective de planification de la capacité.

Étant donné que chaque perspective a des besoins propres et spécifiques, les sections suivantes examinent chaque catégorie de manière détaillée.

2.2. Contrôle de la performance du système

Comme nous l'avons mentionné ci-dessus, le contrôle de la performance du système est généralement effectué pour répondre à des problèmes de performance. Soit le système tourne trop lentement, soit les programmes (et parfois même le système entier) ne réussit pas à tourner du tout. Dans les deux cas, le contrôle de la performance est normalement effectué en tant que première ou dernière étape d'un processus en trois étapes :

1. Contrôle du système pour identifier la nature et l'envergure du manque de ressources à l'origine des problèmes de performance
2. Analyse des données obtenues lors de la phase de contrôle et évidement, prise de mesures (généralement réglage de performance et/ou obtention de matériel supplémentaire) pour résoudre le problème
3. Contrôle du système pour confirmer que le problème de performance a bien été résolu

Dans de telles circonstances, le contrôle de performance a tendance à être de courte durée et de portée plus précise.



Remarque

Le contrôle de la performance du système est souvent un processus interactif, dont les étapes sont répétées plusieurs fois afin d'obtenir la meilleure performance possible du système. En effet, étant donné qu'il existe une relation d'interdépendance entre les ressources système et leur utilisation, l'élimination d'un goulet d'étranglement au niveau des ressources en expose souvent un autre.

2.3. Contrôle de la capacité du système

Le contrôle de la capacité du système est effectué en tant que composante d'un programme permanent de planification de la capacité. La planification de la capacité utilise un contrôle des ressources à long terme pour déterminer des taux de changement dans l'utilisation des ressources système. Une fois que ces taux de changement sont connus, il est alors possible d'effectuer une planification plus précise et à long terme, quant à l'obtention de ressources supplémentaires.

Le contrôle effectué à des fins de planification de capacité est différent du contrôle de performance et ce, à deux niveaux :

- Le contrôle a lieu de manière plus ou moins continue
- Le contrôle est généralement moins détaillé

L'origine de ces différences réside dans les objectifs d'un programme de planification de capacité. Pour effectuer une bonne planification de capacité il est nécessaire d'avoir une perspective "d'ensemble à long terme" ; l'utilisation anormale ou à court terme de ressources n'a que peu d'importance. Les données sont plutôt recueillies au cours d'une certaine durée, ce qui permet de catégoriser l'utilisation des ressources en fonction des variations de la charge de travail. Dans des environnements plus limités (dans lesquels tourne par exemple une seule application), il est possible de transposer l'impact de l'application sur les ressources système. Cette transposition peut être effectuée avec suffisamment de précision pour pouvoir déterminer par exemple, l'impact causée par cinq agents d'un service clientèle utilisant l'application du service pendant la période la plus active de la journée.

2.4. Que contrôler ?

Comme nous l'avons mentionné précédemment, les ressources de tout système se composent de la puissance de CPU, de la largeur de bande, de la mémoire et du stockage. Au premier abord, le contrôle ne semble porter que sur ces quatre éléments différents.

Malheureusement, ce n'est pas aussi simple. Prenez par exemple un disque dur. Quel genre d'informations aimeriez-vous connaître au niveau de sa performance ?

- Quelle est la quantité d'espace disque libre ?
- Combien d'opérations d'E/S par seconde effectue-t-il en moyenne ?
- Combien de temps faut-il en moyenne pour que chaque opération d'E/S soit effectuée ?
- Combien de ces opérations d'E/S sont des opérations de lecture ? Combien sont des opérations d'écriture ?
- Quelle est la quantité moyenne de données lues/écrites lors de chaque opération d'E/S ?

Il existe bien d'autres manières d'examiner la performance du disque dur ; les éléments précédents ne renseignent que très superficiellement sur le sujet. Le concept essentiel qu'il convient de garder à l'esprit est que les données de chaque ressource se présentent sous différents types.

Les sections suivantes examinent les différents types d'informations sur l'utilisation des ressources permettant de comprendre le comportement de chacun des principaux types de ressources.

2.4.1. Contrôle de la puissance de CPU

Le contrôle de la puissance de CPU dans sa forme la plus élémentaire peut en fait être une activité plus difficile à effectuer que de déterminer la possibilité que l'utilisation du CPU atteigne 100%. Si l'utilisation du CPU reste inférieure à 100%, quelle que soit l'activité du système, une puissance de traitement supplémentaire est toujours disponible pour faire face à une activité supérieure.

Toutefois, rares sont les systèmes n'atteignant pas, à un moment ou à un autre, une utilisation à 100% du CPU. À ce stade, il est important d'examiner des données plus détaillées sur l'utilisation du CPU. Ce faisant, il est alors possible de commencer à identifier là où la majorité de la puissance de traitement est utilisée. Ci-après figurent certaines des statistiques les plus couramment consultées en matière d'utilisation du CPU :

Utilisateur contre système

Une comparaison du pourcentage de temps passé à effectuer des opérations de traitement au niveau de l'utilisateur par rapport à celui dédié aux opérations de traitement au niveau du système, peut indiquer si une charge de travail est essentiellement due à l'exécution d'applications ou au temps de gestion du système d'exploitation. Des pourcentages élevés au niveau des utilisateurs ont tendance à être positifs (à condition que les utilisateurs ne connaissent pas de performance insatisfaisante) alors que des pourcentages élevés au niveau du système tendent à indiquer qu'il existe des problèmes nécessitant un examen plus détaillé.

Changements de contexte

Un changement de contexte se produit lorsque le CPU arrête d'exécuter un processus particulier et en lance un autre. Étant donné que tout changement de contexte demande que le système d'exploitation prenne contrôle du CPU, des changements de contexte excessifs semblent aller de paire avec des degrés élevés de consommation de CPU au niveau du système.

Interruptions

Comme le nom l'indique, les interruptions correspondent à des situations dans lesquelles un changement soudain intervient au niveau du traitement effectué par le CPU. Des interruptions ont généralement lieu en raison d'une activité matérielle (telle qu'un périphérique d'E/S finissant une

opération d'E/S) ou en raison d'un logiciel (tel que des interruptions logicielles qui contrôlent le traitement d'applications). Étant donné que les interruptions doivent s'effectuer au niveau du système, un taux élevé d'interruptions entraîne une consommation de CPU accrue au niveau du système.

Processus exécutables

Un processus peut être dans différents états. Il peut, par exemple :

- En attente qu'une opération d'E/S soit terminée
- En attente que le sous-système de gestion de mémoire traite un défaut de page

Dans ces cas-là, le processus n'a pas besoin du CPU.

Toutefois, après un certain temps, l'état du processus change et ce dernier devient alors exécutable. Comme le nom l'indique, un processus exécutable est un processus capable d'effectuer un travail dès qu'il est programmé pour recevoir du temps CPU. Ceci étant, si plusieurs processus sont exécutables à un moment donné, tous les processus exécutables sauf un¹ doivent attendre leur tour pour être traité par le CPU. En contrôlant le nombre de processus exécutables, il est possible de déterminer le degré de dépendance de votre système par rapport au CPU.

D'autres métriques de performance reflétant un impact sur l'utilisation du CPU ont tendance à inclure différents services fournis par le système d'exploitation aux processus. Ces dernières peuvent inclure des statistiques relatives à la gestion de la mémoire, au traitement des E/S etc. Ces statistiques révèlent également que, lorsqu'un système est sous surveillance, les informations fournies se recoupent. En d'autres termes, il se peut que les statistiques d'utilisation du CPU identifient un problème au niveau du sous-système d'E/S ou que les statistiques d'utilisation de la mémoire révèlent un défaut de conception au niveau d'une application.

Par conséquent, lors du contrôle de la performance du système, il n'est pas possible d'examiner une statistique particulière de manière entièrement indépendante ; seulement en prenant en compte la situation globale est-il possible d'extraire des informations utiles de statistiques quelconques sur la performance.

2.4.2. Contrôle de la largeur de bande

Le contrôle de la largeur de bande est une opération plus difficile que celui des autres ressources décrites ici. En effet, les statistiques de performance ont tendance à être basées sur les périphériques alors que la plupart des endroits où la largeur de bande est importante ont tendance à se trouver au niveau des bus reliant les périphériques. Dans les cas où plusieurs périphériques partagent un bus commun, les statistiques fournies sur chaque périphérique sembleront peut-être acceptables, mais la charge totale que ces périphériques placent sur le bus est en réalité beaucoup plus importante.

Il peut se poser un autre déficit au niveau du contrôle de la largeur de bande, lorsque les statistiques relatives aux périphériques eux-mêmes ne sont pas disponibles. C'est précisément le cas pour des bus d'extension du système et pour les chemins des données². Toutefois, bien que des statistiques 100% précises sur la largeur de bande ne soient pas toujours disponibles, il existe souvent suffisamment d'informations pour permettre un certain niveau d'analyse, en particulier lorsque d'autres statistiques sur le sujet sont prises en compte.

Parmi certaines des statistiques les plus courantes sur la largeur de bande figurent :

1. Dans le cas d'un système informatique doté d'un seul processeur.
 2. De plus amples informations sur les bus, sur les chemins des données et sur la largeur de bande sont disponibles dans le Chapitre 3.

Nombre d'octets reçus/envoyés

Les statistiques relatives aux interfaces réseau fournissent une indication sur l'utilisation de la largeur de bande d'un des bus les plus visibles — le réseau.

Décomptes des interfaces et taux

Ces statistiques en relation avec le réseau peuvent fournir entre autres des indications sur des collisions excessives, des erreurs de transmission et de réception. En utilisant ces statistiques (en particulier si elles sont disponibles pour plus d'un système du réseau), il est possible de résoudre un certain nombre de problèmes en relation avec le réseau, avant même d'utiliser les outils de diagnostic du réseau les plus courants.

Transferts par seconde

Généralement recueilli pour les périphériques blocs d'E/S, tels que des lecteurs de disques durs et des lecteurs de bandes haute performance, ce type de statistiques est un bon moyen de déterminer si la limite de la largeur de bande d'un périphérique particulier est atteinte. En raison de leur nature électromagnétique, les lecteurs de disques et de bandes peuvent seulement effectuer un nombre déterminé d'opérations d'E/S par seconde ; leur performance se détériore rapidement au fur et à mesure que le nombre d'opérations se rapproche de la limite.

2.4.3. Contrôle de la mémoire

S'il existe un domaine dans lequel les statistiques de performance abondent, c'est bien celui du contrôle de l'utilisation de la mémoire. En raison de la complexité inhérente aux systèmes d'exploitation dotés de mémoire virtuelle paginée à la demande, les statistiques relatives à l'utilisation de la mémoire prennent de nombreuses formes différentes. C'est à ce niveau qu'à lieu la plupart du travail d'un administrateur de système effectuant la gestion des ressources.

Les statistiques énumérées ci-dessous donnent un bref aperçu des statistiques de gestion de mémoire couramment disponibles :

Pages reçues (In)/Pages transmises (Out)

Ces statistiques permettent d'estimer le flux de pages entre la mémoire du système et les périphériques de stockage de masse qui y sont reliés (généralement les disques durs). Des taux élevés pour ces deux types de statistiques indiquent généralement que le système est à court de mémoire physique et effectue des opérations d'*écroulement* (ou thrashing) ou qu'il utilise plus de ressources système pour charger des pages en mémoire et pour les décharger, que pour exécuter des applications.,

Pages actives/Pages Inactives

Ces statistiques indiquent le degré d'utilisation des pages mises en mémoire. L'absence de pages inactives peut être le signe d'un manque de mémoire physique imminent.

Pages libres, partagées, tamponnées et mises en cache

Ces statistiques fournissent de informations supplémentaire plus détaillées que celles relatives aux pages actives/inactives. Grâce à ces statistiques, il est possible d'obtenir une vue globale de l'utilisation variée de la mémoire.

Swap Entrants/Swap sortants

Ces statistiques expliquent le comportement générale de l'échange de mémoire (ou swapping) du système. Des taux excessivement élevés indiquent ici qu'il existe peut-être des problèmes liés à un manque de mémoire.

Pour bien contrôler l'utilisation de la mémoire, il est nécessaire de disposer d'une bonne compréhension du fonctionnement des systèmes d'exploitation dotés de mémoire virtuelle paginée à la demande. Bien qu'un tel sujet pourrait faire l'objet d'un livre entier, nous nous contenterons d'aborder les concepts de base dans le Chapitre 4. En lisant ce chapitre et en passant du temps à effectivement contrôler un système, vous disposerez des bases nécessaires pour ensuite approfondir vos connaissances sur le sujet.

2.4.4. Contrôle du stockage

En matière de stockage, il existe généralement deux types de contrôle différents :

- Contrôle pour garantir un espace disque suffisant
- Contrôle pour identifier des problèmes en relation avec la performance

Il est nécessaire d'effectuer un contrôle aussi bien au niveau du disque qu'au niveau de la performance car il est tout à fait possible d'avoir de sérieux problèmes à un niveau et absolument aucun à l'autre. Par exemple, il est possible qu'un disque dur soit à court d'espace sans pour autant entraîner de problème de performance. De même, il est possible qu'un disque dur, bien que disposant de 99% d'espace libre, fonctionne au-delà de sa capacité en terme de performance.

Toutefois, il est plus probable qu'un système moyen doive faire face à un manque de ressources aussi bien au niveau de l'espace disque qu'au niveau de la performance. Dans de telles circonstances, il y a également de grandes chances que — jusqu'à un certain point — des problèmes à un niveau aient un impact sur l'autre niveau. Très souvent ce type d'interaction entraîne une performance d'E/S de plus en plus mauvaise au fur et à mesure qu'un disque dur approche de la barre des 0% d'espace libre néanmoins, dans des cas où la charge d'E/S est extrême, il est tout à fait possible de ralentir la capacité de traitement des E/S à tel point que les applications ne puissent plus tourner correctement.

Dans tous les cas de figure, les statistiques suivantes sont utiles pour le contrôle du stockage :

Espace libre

L'espace libre est probablement la ressource que les administrateurs de système surveillent le plus étroitement ; un administrateur ne contrôlant jamais l'espace libre sera un cas rarissime (ou alors, il dispose d'un certain processus de contrôle automatisé).

Statistiques sur les systèmes de fichiers

Ces statistiques (telles que le nombre de fichiers par répertoire, la taille moyenne des fichiers, etc.) fournissent des informations supplémentaires plus utiles que le simple pourcentage d'espace libre. Grâce à ces informations détaillées, les administrateurs peuvent configurer le système de manière à optimiser la performance car la charge d'E/S imposée par un système de fichiers peuplé de petits fichiers n'est pas la même que celle correspondant à un système de fichiers composé d'un seul fichier énorme.

Transferts par seconde

Ce genre de statistique constitue un bon moyen de déterminer si les limites de la largeur de bande d'un périphérique particulier ont été atteintes.

Opérations de lecture/écriture par seconde

Ces statistiques sous forme d'une ventilation légèrement plus détaillée des transferts par seconde permettent à un administrateur de système de mieux comprendre la nature des charges d'E/S auxquelles un périphérique peut être soumis. Cet aspect peut être critique dans la mesure où certaines technologies de stockage ont des caractéristiques de performance très différentes selon qu'elles traitent des opérations de lecture ou des opérations d'écriture.

2.5. Informations spécifiques à Red Hat Enterprise Linux

Red Hat Enterprise Linux offre une variété d'outils de contrôle des ressources. Bien que la liste ci-après n'englobe pas tous les outils disponibles, ceux énumérés se distinguent en raison de leur fonctionnalité respective. Parmi ces outils figurent :

- `free`
- `top` (et le **Moniteur système** de GNOME, une version plus graphique de `top`)
- `vmstat`
- Sysstat, la suite d'outils de contrôle des ressources
- OProfile, le profileur de tout le système

Examinons chacun de ces outils de manière plus détaillée.

2.5.1. `free`

La commande `free` affiche l'utilisation de la mémoire du système. Ci-dessous figure un exemple de cette sortie :

	total	used	free	shared	buffers	cached
Mem:	255508	240268	15240	0	7592	86188
-/+ buffers/cache:		146488	109020			
Swap:	530136	26268	503868			

La rangée `Mem:` correspond à l'utilisation de la mémoire physique alors que la rangée `Swap:` représente l'utilisation de l'espace swap du système et que la rangée `-/+ buffers/cache:` donne elle la quantité de mémoire physique actuellement consacrée aux tampons du système.

Étant donné que, par défaut, `free` ne fournit qu'une seule fois des informations sur l'utilisation de la mémoire, cette commande n'est vraiment utile que pour un contrôle à très court terme ou pour déterminer s'il existe actuellement un problème au niveau de la mémoire. Bien que la commande `free` puisse, au moyen de l'option `-s`, afficher des informations chiffrées sur l'utilisation de mémoire, ces dernières défilent si rapidement qu'il est assez difficile de remarquer tout changement dans l'utilisation de la mémoire.



Astuce

Une meilleure alternative à `free -s` consisterait à exécuter `free` à l'aide de la commande `watch`. Par exemple, afin d'obtenir l'affichage de l'utilisation de mémoire toutes les deux secondes (l'intervalle d'affichage par défaut de `watch`), utilisez la commande suivante :

```
watch free
```

La commande `watch` exécute `free` toutes les deux secondes, mettant ainsi l'écran à jour en l'effaçant avant d'y afficher la nouvelle sortie. Ainsi, il est beaucoup plus facile de déterminer la manière selon laquelle l'utilisation de la mémoire change au fil du temps dans la mesure où `watch` crée un seul affichage mis à jour sans défilement. Il est de plus possible de contrôler l'intervalle entre les mises à jour en utilisant l'option `-n` et grâce à l'option `-d`, il est même possible de modifier l'affichage de manière à ce que toute différence entre les mises à jour apparaisse en caractères gras, comme le ferait la commande suivante :

```
watch -n 1 -d free
```

Pour obtenir de plus amples informations sur le sujet, reportez-vous à la page de manuel de `watch`.

La commande `watch` tourne jusqu'à ce qu'elle soit interrompue par la combinaison de touches [Ctrl]-[C]. Il est bon de garder à l'esprit la commande `watch`, car elle peut être très utile dans de nombreuses situations.

2.5.2. `top`

Alors que `free` affiche seulement des informations relatives à la mémoire, la commande `top` elle fournit des informations très variées. Qu'il s'agisse de l'utilisation du CPU, des statistiques sur les processus ou de l'utilisation de la mémoire — `top` contrôle le tout. De plus, contrairement à la commande `free`, le comportement par défaut de `top` fait qu'elle est exécutée en permanence si bien qu'il n'y a pas lieu d'utiliser la commande `watch`. Ci-après figure un exemple d'affichage fourni par cette commande :

```
14:06:32 up 4 days, 21:20, 4 users, load average: 0.00, 0.00, 0.00
77 processes: 76 sleeping, 1 running, 0 zombie, 0 stopped
CPU states:  cpu  user  nice  system  irq  softirq  iowait  idle
              total 19.6%  0.0%  0.0%  0.0%  0.0%  0.0%  180.2%
              cpu00 0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  100.0%
              cpu01 19.6%  0.0%  0.0%  0.0%  0.0%  0.0%  80.3%
Mem:  1028548k av, 716604k used, 311944k free, 0k shrd, 131056k buff
Swap: 1020116k av, 5276k used, 1014840k free 382228k cached

  PID USER      PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME CPU COMMAND
 17578 root        15   0 13456  13M  9020 S   18.5  1.3  26:35 1 rhn-applet-gu
 19154 root        20   0  1176  1176   892 R    0.9  0.1   0:00 1 top
     1 root        15   0   168   160   108 S    0.0  0.0   0:09 0 init
     2 root        RT   0    0    0    0 SW    0.0  0.0   0:00 0 migration/0
     3 root        RT   0    0    0    0 SW    0.0  0.0   0:00 1 migration/1
     4 root        15   0    0    0    0 SW    0.0  0.0   0:00 0 keventd
     5 root        34  19    0    0    0 SWN   0.0  0.0   0:00 0 ksoftirqd/0
     6 root        35  19    0    0    0 SWN   0.0  0.0   0:00 1 ksoftirqd/1
     9 root        15   0    0    0    0 SW    0.0  0.0   0:07 1 bdflush
     7 root        15   0    0    0    0 SW    0.0  0.0   1:19 0 kswapd
     8 root        15   0    0    0    0 SW    0.0  0.0   0:14 1 kscand
    10 root        15   0    0    0    0 SW    0.0  0.0   0:03 1 kupdated
    11 root        25   0    0    0    0 SW    0.0  0.0   0:00 0 mdrecoveryd
```

Comme vous pouvez le voir, l'affichage est divisé en deux sections. La partie supérieure contient des informations relatives à l'état général du système — durée de fonctionnement, charge moyenne, décompte des processus, état du CPU et statistiques sur l'utilisation de la mémoire et de l'espace swap. La partie inférieure quant à elle fournit des statistiques au niveau des processus ; la nature de ces dernières peut être modifiée alors même que le commande `top` est en cours d'exécution. Par exemple, `top` affiche par défaut, aussi bien les processus actifs que les processus inactifs. Afin d'afficher seulement les processus actifs, appuyez sur la touche [i] ; en appuyant une deuxième fois sur cette touche, l'affichage retourne au mode d'affichage par défaut.



Avertissement

Bien que `top` apparaisse comme étant seulement un simple programme d'affichage, ce n'est pas le cas. Cette misconception s'explique par le fait que `top` utilise des commandes à caractère unique pour effectuer certaines opérations. Par exemple, si vous êtes connecté en tant que super-utilisateur, il est possible de changer la priorité et même de mettre fin à tout processus sur votre système. Il est par conséquent plus sûr de vous limiter à l'utilisation de [q] (pour quitter `top`) jusqu'à ce que vous ayez passé en revue l'écran d'assistance de la commande `top` (tapez [?] pour faire apparaître ce dernier).

2.5.2.1. Le Moniteur système de GNOME — Une commande `top` graphique

Si vous vous sentez plus à l'aise avec des interfaces utilisateur graphiques, le **Moniteur système** de GNOME vous conviendra peut-être mieux. Tout comme `top`, le **Moniteur système** de GNOME affiche des informations sur l'état général du système, les décomptes de processus, l'utilisation de la mémoire et du swap et les statistiques au niveau des processus.

Toutefois, le **Moniteur système** de GNOME va encore plus loin dans le sens où il inclut des représentations graphiques du CPU, de l'utilisation de la mémoire et du swap ainsi qu'un listage sous forme de tableau de l'utilisation de l'espace disque. Pour examiner un exemple de la **Liste des processus** dressée par le **Moniteur système** de GNOME, reportez-vous à la Figure 2-1.

Nom du processus	Utilisateur	Mémoire	% CPU	ID
bash	asimons	956 K	0	3540
gnome-system-monitor	asimons	9,4 Mo	5	6191
bash	asimons	384 K	0	3489
bash	asimons	384 K	0	2977
bash	asimons	380 K	0	2372
gnome-pty-helpe	asimons	252 K	0	2371
xchat	asimons	4,1 Mo	0	2316
python	asimons	9,7 Mo	0	2194
pam-panel-icon	asimons	2,2 Mo	0	2192
eggccups	asimons	2,1 Mo	0	2190
magicdev	asimons	1,3 Mo	0	2187
xscreensaver	asimons	1,0 Mo	0	2176
fam	asimons	764 K	0	2171

Figure 2-1. Affichage de la Liste des processus par le Moniteur système de GNOME

Il est possible d'afficher des informations supplémentaires pour un processus spécifique en cliquant d'abord sur le processus en question avant de sélectionner le bouton **Plus d'info**.

Pour afficher des statistiques relatives au CPU, à la mémoire et à l'utilisation du disque, cliquez sur l'onglet **Moniteur système**.

2.5.3. `vmstat`

Pour une meilleure compréhension de la performance du système, vous pouvez utiliser `vmstat`. Grâce à ce moniteur de ressources, il est possible d'obtenir un aperçu de l'activité des processus, de la

mémoire, du swap, des E/S et du CPU sous la forme d'une ligne de nombres, comme le montre l'extrait reproduit ci-dessous :

```
procs                memory                swap                io                system                cpu
 r  b  swpd  free  buff  cache  si  so  bi  bo  in  cs  us  sy  id  wa
 0  0  5276 315000 130744 380184  1  1  2  24  14  50  1  1  47  0
```

La première ligne subdivise le champ en six catégories à savoir : processus, mémoire, swap, E/S, système et CPU sur lesquelles elle donne des statistiques. La seconde ligne elle identifie de manière encore plus détaillée chacun des champs, permettant ainsi de parcourir simplement et rapidement l'ensemble des données lors de la recherche de statistiques spécifiques.

Les champs relatifs aux processus sont les suivants :

- `r` — Le nombre de processus exécutables attendant d'avoir accès au CPU
- `b` — Le nombre de processus exécutables dans un état de veille qui ne peut être interrompu

Les champs relatifs à la mémoire sont les suivants :

- `swpd` — La quantité de mémoire virtuelle utilisée
- `free` — La quantité de mémoire libre
- `buff` — La quantité de mémoire utilisée par les tampons (ou buffers)
- `cache` — La quantité de mémoire utilisée comme cache de pages

Les champs relatifs au swap sont les suivants :

- `si` — La quantité de mémoire chargée depuis le disque
- `so` — La quantité de mémoire déchargée sur le disque

Les champs relatifs aux Entrées/Sorties (E/S) sont les suivants :

- `bi` — Blocs envoyés vers un périphérique blocs
- `bo` — Blocs reçus d'un périphérique blocs

Les champs relatifs au système sont les suivants :

- `in` — Nombre d'interruptions par seconde
- `cs` — Nombre de changements de contexte par seconde

Les champs relatifs au CPU sont les suivants :

- `us` — Le pourcentage de temps pendant lequel le CPU exécute un code de niveau utilisateur
- `sy` — Le pourcentage de temps pendant lequel le CPU exécute un code de niveau système
- `id` — Le pourcentage de temps pendant lequel le CPU était inoccupé
- `wa` — Attente d'E/S

Lorsque la commande `vmstat` est utilisée sans aucune option, seule est affichée une ligne fournissant des moyennes calculées sur la base du moment auquel le dernier démarrage a eu lieu.

Toutefois, la plupart des administrateurs système ne se basent pas vraiment sur les données fournies sur cette ligne dans la mesure où la durée au cours de laquelle elles ont été recueillies varie. Ils préfèrent profiter de la capacité de `vmstat` à afficher de manière répétée et à intervalles définis des données sur l'utilisation des ressources. Par exemple, la commande `vmstat 1` affiche une nouvelle

ligne de données sur l'utilisation toutes les secondes, alors que la commande `vmstat 1 10` fournit elle aussi une nouvelle ligne par seconde mais seulement pour les dix secondes suivantes.

Entre les mains d'un administrateur expérimenté, la commande `vmstat` peut être utilisée pour cerner rapidement des problèmes d'utilisation de ressource ou de performance. Toutefois, afin d'obtenir une compréhension plus approfondie de ces problèmes, un type d'outil différent est nécessaire — un outil capable de recueillir et d'analyser des données de manière plus détaillée.

2.5.4. Sysstat, la suite d'outils de contrôle des ressources

Alors que les outils précédents peuvent se révéler utiles pour obtenir une certaine compréhension de la performance du système sur de courtes durées, ils ne fournissent qu'un bref aperçu de l'utilisation des ressources système. En outre, certains aspects de la performance du système ne peuvent pas être facilement contrôlés par ces outils relativement primaires.

Un outil plus sophistiqué est par conséquent nécessaire, d'où Sysstat.

Pour le recueil de statistiques sur les E/S et le CPU, Sysstat contient les outils suivants :

`iostat`

Affiche une vue d'ensemble de l'utilisation CPU ainsi que des statistiques d'E/S pour un ou plusieurs disque(s) dur(s).

`mpstat`

Affiche des statistiques plus détaillées sur le CPU.

Sysstat contient également des outils recueillant des données sur l'utilisation des ressources système et créant des rapports quotidiens basés sur les données recueillies. Parmi ces outils figurent :

`sadc`

Connu comme le collecteur de données sur l'activité du système, `sadc` recueille des informations relatives à l'utilisation des ressources système et les enregistre dans un fichier.

`sar`

Génère des rapports à partir des fichiers créés par `sadc` ; ces rapports `sar` peuvent être produits de manière interactive ou écrits dans un fichier qui fera l'objet d'une analyse plus approfondie.

Les sections suivantes examinent chacun des ces outils de manière plus détaillée.

2.5.4.1. La commande `iostat`

La commande `iostat` dans son utilisation la plus élémentaire fournit une vue d'ensemble des statistiques du CPU et des E/S de disque.

```
Linux 2.4.20-1.1931.2.231.2.10.ent (pigdog.example.com) 07/11/2003
```

```
avg-cpu:  %user   %nice   %sys   %idle
           6.11    2.56    2.15   89.18
```

```
Device:            tps    Blk_read/s    Blk_wrtn/s    Blk_read    Blk_wrtn
dev3-0              1.68          15.69          22.42    31175836    44543290
```

Au-dessous de la première ligne (indiquant la version du noyau du système et son nom d'hôte ainsi que la date actuelle) `iostat` affiche une vue d'ensemble de l'utilisation CPU moyenne du système depuis le dernier démarrage. Le rapport d'utilisation du CPU inclut les pourcentages suivants :

- Pourcentage de temps passé en mode utilisateur (exécutant des applications, etc.)
- Pourcentage de temps passé en mode utilisateur (pour les processus qui ont modifié leur priorité de programmation à l'aide de la commande `nice(2)`)
- Pourcentage de temps passé en mode noyau
- Pourcentage de temps passé en inactivité

Au-dessous du rapport d'utilisation du CPU figure le rapport d'utilisation des périphériques. Ce dernier contient une ligne pour chaque périphérique disque du système et inclut les informations suivantes :

- La spécification du périphérique, apparaissant sous la forme `dev<major-number>-sequence-number` où `<major-number>` correspond au nombre majeur du périphérique³ et `<sequence-number>` correspond à un numéro de séquence commençant par zéro.
- Le nombre de transferts (ou opérations d'E/S) par seconde.
- Le nombre de blocs de 512 octets lus par seconde.
- Le nombre de blocs de 512 octets écrits par seconde.
- Le nombre total de blocs de 512 octets lus par seconde.
- Le nombre total de blocs de 512 octets écrits par seconde.

Ces exemples ne représentent qu'un échantillon des informations pouvant être obtenues à l'aide de `iostat`. Pour de plus amples informations sur le sujet, reportez-vous à la page de manuel de `iostat(1)`.

2.5.4.2. La commande `mpstat`

Au premier abord, la commande `mpstat` semble fournir des informations semblables à celles incluses dans le rapport d'utilisation du CPU produit par `iostat`, comme le montre l'extrait ci-dessous :

```
Linux 2.4.20-1.1931.2.231.2.10.ent (pigdog.example.com) 07/11/2003
07:09:26 PM CPU %user %nice %system %idle intr/s
07:09:26 PM all 6.40 5.84 3.29 84.47 542.47
```

En fait, à l'exception d'une colonne supplémentaire fournissant des informations sur les interruptions traitées par le CPU toutes les secondes, il n'existe pas vraiment de différence entre les deux commandes. Toutefois, si l'option `-P ALL` est utilisée avec la commande `mpstat`, la situation est alors différente, comme le montre l'extrait suivant :

```
Linux 2.4.20-1.1931.2.231.2.10.ent (pigdog.example.com) 07/11/2003
07:13:03 PM CPU %user %nice %system %idle intr/s
07:13:03 PM all 6.40 5.84 3.29 84.47 542.47
07:13:03 PM 0 6.36 5.80 3.29 84.54 542.47
07:13:03 PM 1 6.43 5.87 3.29 84.40 542.47
```

3. Les nombres majeurs des périphériques peuvent être obtenus en utilisant `ls -l` pour afficher le fichier de périphérique souhaité se trouvant dans `/dev/`. Le nombre majeur apparaît après la spécification du groupe du périphérique.

Sur des systèmes à processeurs multiples, `mpstat` permet d'afficher l'utilisation de chaque CPU de manière individuelle, si bien qu'il est alors possible de déterminer le degré d'efficacité avec lequel chaque CPU est utilisé.

2.5.4.3. La commande `sadc`

Comme nous l'avons mentionné précédemment, la commande `sadc` recueille des données sur l'utilisation du système et les enregistre ensuite dans un fichier pour une analyse ultérieure. Par défaut, les données sont écrites dans des fichiers faisant partie du répertoire `/var/log/sa/`. Ces derniers se nomment `sa<dd>` où `<dd>` correspond au jour actuel dont la date est exprimée en fonction de deux caractères.

La commande `sadc` est normalement exécutée par le script `sa1`. Ce dernier est invoqué périodiquement par `cron` par le biais du fichier `sysstat` qui se trouve dans `/etc/cron.d/`. Le script `sa1` invoque `sadc` pour un seul intervalle d'évaluation durant une seconde. Par défaut, `cron` exécute `sa1` toutes les 10 minutes et ajoute les données recueillies lors de chaque intervalle au fichier courant nommé `/var/log/sa/sa<dd>`.

2.5.4.4. La commande `sar`

La commande `sar` crée des rapports sur l'utilisation du système en fonction des données recueillies par `sadc`. Conformément à la manière dont elle a été configurée dans Red Hat Enterprise Linux, la commande `sar` est automatiquement exécutée pour traiter les fichiers recueillis automatiquement par `sadc`. Les fichiers du rapport qui sont écrits dans `/var/log/sa/` se nomment `sar<dd>` où `<dd>` correspond au jour précédent dont la date est exprimée en fonction de deux caractères.

La commande `sar` est normalement exécutée par le script `sa2`. Ce dernier est invoqué périodiquement par `cron` par le biais du fichier `sysstat` qui se trouve dans `/etc/cron.d/`. Par défaut, `cron` exécute `sa2` une fois par jour à 23:53, ce qui lui permet de créer un rapport prenant en compte les données recueillies au cours de la journée entière.

2.5.4.4.1. Lecture des rapports `sar`

Le format d'un rapport `sar` créé selon la configuration par défaut de Red Hat Enterprise Linux se présente en plusieurs sections. Chacune d'elles contient un type spécifique de données, classées en fonction du moment auquel elles ont été recueillies pendant la journée. Étant donné que la commande `sadc` est configurée de manière à effectuer un intervalle d'évaluation d'une durée fixée à une seconde toutes les dix minutes, le rapport par défaut de `sar` contient des données par incréments de 10 minutes, commençant à 00:00 et finissant à 23:50⁴.

Chaque section de ce rapport commence par une en-tête spécifiant le type de données qu'elle contient. Cette en-tête est répétée à différents intervalles dans cette section, permettant ainsi d'examiner facilement les données tout en parcourant le rapport. Chaque section se termine par une ligne exprimant la moyenne des données rapportées dans cette section.

Ci-après figure l'exemple d'une section provenant d'un rapport créé par `sar`, dans lequel les données recueillies entre 00:30 et 23:40 ont été supprimées afin d'économiser de la place :

00:00:01	CPU	%user	%nice	%system	%idle
00:10:00	all	6.39	1.96	0.66	90.98
00:20:01	all	1.61	3.16	1.09	94.14
...					
23:50:01	all	44.07	0.02	0.77	55.14
Average:	all	5.80	4.99	2.87	86.34

4. En raison des variations des charges du système, il se peut que l'heure exacte à laquelle les données sont recueillies varie d'une ou deux secondes.

Dans cette section figurent les informations relatives à l'utilisation du CPU. Le contenu est en fait très proche des données fournies par la commande `iostat`.

Il est possible que d'autres sections comportent plus d'une ligne de données à la fois, comme le montre la section suivante générée d'après les données relatives à l'utilisation du CPU, recueillies sur un systèmes à double processeur :

```
00:00:01      CPU      %user      %nice      %system      %idle
00:10:00          0      4.19      1.75      0.70      93.37
00:10:00          1      8.59      2.18      0.63      88.60
00:20:01          0      1.87      3.21      1.14      93.78
00:20:01          1      1.35      3.12      1.04      94.49
...
23:50:01          0      42.84      0.03      0.80      56.33
23:50:01          1      45.29      0.01      0.74      53.95
Average:          0      6.00      5.01      2.74      86.25
Average:          1      5.61      4.97      2.99      86.43
```

Les rapports générés selon la configuration par défaut de `sar` sous Red Hat Enterprise Linux incluent au total dix-sept sections différentes, dont certaines seront examinées dans des chapitres ultérieurs. Pour de plus amples informations sur les données contenues dans chaque section, reportez-vous à la page de manuel de `sar` (1).

2.5.5. OProfile

OProfile, le profileur de tout le système, est un outil de contrôle fonctionnant avec un temps de gestion court. Il utilise le matériel de contrôle de performance du processeur⁵.

Le matériel de contrôle de la performance fait partie du processeur lui-même. Il se présente sous la forme d'un compteur spécial incrémenté après chaque événement (comme lorsque le processeur est occupé ou que les données ne sont pas stockées dans un cache). Certains processeurs sont dotés de plusieurs compteurs de ce type et permettent donc de réserver chaque compteur pour un type d'événement particulier.

Les compteurs peuvent être initialisés avec une certaine valeur de départ et une interruption est engendrée quand un compteur atteint sa limite. En donnant à un compteur des valeurs initiales différentes, il est possible d'obtenir une variation du taux auquel les interruptions sont produites. De cette manière, il est également possible de contrôler la fréquence d'échantillonnage et par conséquent le degré de détail obtenu à partir des données recueillies.

Un cas extrême consistant à initialiser le compteur de sorte qu'il engendre une interruption de dépassement après chaque événement, fournirait des données de performance extrêmement détaillées (mais au prix d'un temps de gestion très long). Le cas extrême inverse consistant à initialiser le compteur de sorte qu'il engendre aussi peu d'interruptions que possible, ne donnerait lui en revanche qu'une vue d'ensemble très générale de la performance du système (mais avec un temps système quasiment inexistant). Le secret d'un contrôle efficace réside dans le choix d'une fréquence d'échantillonnage suffisamment élevée pour saisir les données requises, mais sans toutefois être élevée, au point de surcharger le système avec un temps de gestion excessif nécessaire pour pouvoir effectuer le contrôle de la performance.

5. OProfile peut également utiliser un autre mécanisme (appelé `TIMER_INT`) pouvant être utilisé pour les architectures de systèmes qui ne disposent pas de matériel pour le contrôle de la performance.



Avertissement

La configuration de OProfile peut être effectuée de telle sorte que le profileur impose un temps de gestion suffisant pour que le système soit inutilisable. Il est par conséquent important de choisir les valeurs du compteur avec beaucoup de prudence. C'est la raison pour laquelle la commande `opcontrol` prend en charge l'option `--list-events` qui permet d'afficher les différents types d'événements disponibles pour le processeur actuellement installé, ainsi que les valeurs du compteur recommandées pour chacun d'eux.

Lors de l'utilisation de OProfile, il est important de garder à l'esprit le compromis nécessaire entre la fréquence d'échantillonnage et le temps de gestion du système.

2.5.5.1. Composants de OProfile

OProfile est constitué des composants suivants :

- Logiciel de recueil de données
- Logiciel d'analyse de données
- Logiciel de l'interface administrative

Le logiciel de recueil de données est composé du module de noyau `oprofile.o` et du démon `oprofiled`.

Le logiciel d'analyse des données quant à lui inclut les programmes suivants :

`op_time`

Affiche le nombre et les pourcentages relatifs des échantillons pris pour chaque fichier exécutable

`oprofpp`

Affiche le nombre et les pourcentages relatifs des échantillons pris par fonction, instruction individuelle ou en sortie de type `gprof`

`op_to_source`

Affiche des listes de codes sources annotés et/ou d'assemblages

`op_visualise`

Affiche sous forme graphique les données recueillies

Grâce à ces programmes, il est possible d'afficher les données recueillies de plusieurs manières différentes.

Le logiciel de l'interface administrative contrôle tous les aspects liés au recueil de données, de la spécification des événements à contrôler au commencement et à l'arrêt des opérations de recueil elles-mêmes. La commande `opcontrol` permet de déterminer ces différents aspects.

2.5.5.2. Exemple d'une session de OProfile

Cette section illustre une session de contrôle et d'analyse des données avec OProfile, allant de la configuration initiale à l'analyse finale des données. Cet exemple n'est autre qu'un bref aperçu fourni à titre d'introduction ; pour obtenir des informations plus détaillées, consultez le *Guide d'administration système de Red Hat Enterprise Linux*.

Utilisez `opcontrol` pour configurer le type de données à recueillir à l'aide de la commande suivante :

```
opcontrol \
  --vmlinux=/boot/vmlinux-`uname -r` \
  --ctr0-event=CPU_CLK_UNHALTED \
  --ctr0-count=6000
```

Les options utilisées ici instruisent `opcontrol` de :

- Diriger OProfile vers une copie du noyau actuellement en cours d'exécution (`--vmlinux=/boot/vmlinux-`uname -r``)
- Spécifier que le compteur 0 du processeur doit être utilisé et que l'événement à contrôler est le moment où le CPU exécute des instructions (`--ctr0-event=CPU_CLK_UNHALTED`)
- Spécifier que OProfile doit recueillir des échantillons chaque fois que l'évènement spécifié a été effectué 6000 fois (`--ctr0-count=6000`)

Vérifiez en suite que le module noyau de `oprofile` est bien chargé à l'aide de la commande `lsmod` dont la sortie figure ci-dessous :

```
Module                Size Used by    Not tainted
oprofile              75616  1
...
```

Vérifiez que le système de fichiers de OProfile (situé dans `/dev/oprofile/`) est bien monté avec la commande `ls /dev/oprofile/` dont la sortie figure ci-dessous :

```
0 buffer      buffer_watershed  cpu_type  enable    stats
1 buffer_size cpu_buffer_size  dump      kernel_only
```

(Le nombre exact de fichiers varie selon le type de processeur).

À ce stade, le fichier `/root/.oprofile/daemonrc` contient les paramètres dont le logiciel de recueil de données a besoin, comme le montre l'extrait ci-dessous :

```
CTR_EVENT[0]=CPU_CLK_UNHALTED
CTR_COUNT[0]=6000
CTR_KERNEL[0]=1
CTR_USER[0]=1
CTR_UM[0]=0
CTR_EVENT_VAL[0]=121
CTR_EVENT[1]=
CTR_COUNT[1]=
CTR_KERNEL[1]=1
CTR_USER[1]=1
CTR_UM[1]=0
CTR_EVENT_VAL[1]=
one_enabled=1
SEPARATE_LIB_SAMPLES=0
SEPARATE_KERNEL_SAMPLES=0
VMLINUX=/boot/vmlinux-2.4.21-1.1931.2.349.2.2.ent.smp
```

Utilisez ensuite `opcontrol` pour effectivement commencer à recueillir des données à l'aide de la commande `opcontrol --start` dont la sortie figure ci-dessous :

```
Using log file /var/lib/oprofile/oprofiled.log
Daemon started.
Profiler running.
```

Vérifiez que le démon `oprofiled` est bien en cours d'exécution à l'aide de la commande `ps x | grep -i oprofiled` dont la sortie figure ci-dessous :

```
32019 ?      S      0:00 /usr/bin/oprofiled --separate-lib-samples=0 ...
32021 pts/0  S      0:00 grep -i oprofiled
```

(La ligne de commande `oprofiled` que `ps` affiche est en réalité beaucoup plus longue mais elle a dû être tronquée ici pour des raisons de formatage.)

Le système est désormais sous surveillance et des données sont recueillies sur tous les exécutable figurant sur le système. Ces données sont ensuite stockées dans le répertoire `/var/lib/oprofile/samples/`. Les fichiers contenus dans ce dernier font l'objet d'une convention de nommage quelque peu inhabituelle, comme l'illustre l'exemple ci-dessous :

```
}usr}bin}less#0
```

La convention de nommage utilise certes le chemin d'accès absolu pour chaque fichier contenant un code exécutable, mais la barre oblique avant (`/`) est remplacée par des accolades de fermeture (`}`) et il se finit avec le symbole dièse (`#`) suivi d'un nombre (0 dans le cas présent). Par conséquent, le fichier utilisé dans notre exemple correspond à des données qui ont été recueillies alors que `/usr/bin/less` était en cours d'exécution.

Une fois les données recueillies, utilisez un de ces outils d'analyse pour les afficher. En matière de contrôle, OProfile est dotée d'une excellente fonctionnalité à savoir, il n'est pas nécessaire d'interrompre le recueil des données avant de pouvoir effectuer une analyse de données. Il faut toutefois attendre qu'au moins un groupe d'échantillons soit écrit sur le disque mais il est tout à fait possible de forcer le transfert des échantillons sur disque à l'aide de la commande `opcontrol --dump`.

Dans l'exemple suivant, la commande `op_time` est utilisée pour afficher (dans l'ordre inverse — du nombre le plus élevé d'échantillons au nombre le plus bas) les échantillons qui ont été recueillis :

```
3321080  48.8021  0.0000 /boot/vmlinuz-2.4.21-1.1931.2.349.2.2.entsmp
761776   11.1940  0.0000 /usr/bin/oprofiled
368933   5.4213  0.0000 /lib/tls/libc-2.3.2.so
293570   4.3139  0.0000 /usr/lib/libgobject-2.0.so.0.200.2
205231   3.0158  0.0000 /usr/lib/libgdk-x11-2.0.so.0.200.2
167575   2.4625  0.0000 /usr/lib/libglib-2.0.so.0.200.2
123095   1.8088  0.0000 /lib/libcrypto.so.0.9.7a
105677   1.5529  0.0000 /usr/X11R6/bin/XFree86
...
```

Étant donné que les rapports peuvent s'étendre sur plusieurs centaines de lignes, il est judicieux d'utiliser l'option `less` lorsqu'un rapport est créé de manière interactive. Le rapport reproduit dans notre exemple a d'ailleurs été tronqué pour cette raison.

Le format ce rapport spécifique consiste à créer une ligne chaque fichier exécutable pour lequel des échantillons ont été recueillis. Chaque ligne suit ce format particulier, comme le montre l'extrait suivant :

```
<sample-count> <sample-percent> <unused-field> <executable-name>
```

où :

- `<sample-count>` correspond au nombre d'échantillons recueillies
- `<sample-percent>` correspond au pourcentage de tous les échantillons recueillis pour cet exécutable spécifique
- `<unused-field>` représente un champ qui n'est pas utilisé
- `<executable-name>` correspond au nom du fichier contenant le code de l'exécutable pour lequel des échantillons ont été recueillis.

Ce rapport (créé sur un système essentiellement inoccupé) montre que presque la moitié de tous les échantillons ont été recueillis alors que le CPU exécutait des codes au sein du noyau lui-même. Le démon de recueil de données OProfile était le premier élément mis en attente, suivi par une variété de bibliothèques et le serveur du Système X Window, XFree86. Il est important de noter ici que pour le système exécutant cette session, la valeur de 6000 utilisée pour le compteur correspond à la valeur minimale recommandée par `opcontrol --list-events`. Dans de telles conditions — au moins pour ce système particulier — le temps de gestion de OProfile à son niveau le plus élevé, consomme environ 11% du CPU.

2.6. Ressources supplémentaires

Cette section inclut un certain nombre de ressources pouvant être utilisées pour développer vos connaissances sur le contrôle des ressources et sur des sujets spécifiques à Red Hat Enterprise Linux qui ont été discutés dans ce chapitre.

2.6.1. Documentation Installée

Les ressources suivantes sont installées lors d'une installation traditionnelle de Red Hat Enterprise Linux.

- Page de manuel de `free(1)` — Pour apprendre comment afficher des statistiques relatives à la mémoire aussi bien libre qu'utilisée.
- Page de manuel de `top(1)` — Pour apprendre comment afficher des statistiques relatives à l'utilisation du CPU et des statistiques au niveau des processus.
- Page de manuel de `watch(1)` — Pour apprendre comment exécuter périodiquement le programme spécifié par l'utilisateur, affichant la sortie dans la totalité de l'écran.
- Entrée de menu **Aide du Moniteur système** de GNOME — Pour apprendre comment afficher de manière graphique, des statistiques relatives aux processus, au CPU, à la mémoire et à l'utilisation de l'espace disque.
- Page de manuel de `vmstat(8)` — Pour apprendre comment afficher une vue d'ensemble concise des processus, de la mémoire, du swap, des E/S, du système et de l'utilisation du CPU.
- Page de manuel de `iostat(1)` — Pour apprendre comment afficher des statistiques relatives au CPU et aux E/S.
- Page de manuel de `mpstat(1)` — Pour apprendre comment afficher des statistiques relatives aux processeurs individuels de systèmes dotés de processeurs multiples.
- Page de manuel de `sadc(8)` — Pour apprendre comment recueillir des données sur l'utilisation du système.
- Page de manuel de `sa1(8)` — Pour en savoir plus sur un script exécutant `sadc` périodiquement.
- Page de manuel de `sar(1)` — Pour apprendre comment créer des rapports sur l'utilisation des ressources système.
- Page de manuel de `sa2(8)` — Pour apprendre comment créer des fichiers quotidiens de rapports sur l'utilisation des ressources du système.
- Page de manuel de `nice(1)` — Pour apprendre comment changer la priorité de la programmation des processus.
- Page de manuel de `oprofile(1)` — Pour apprendre comment profiler la performance du système.
- Page de manuel de `op_visualise(1)` — Pour apprendre comment afficher des données de OProfile sous forme graphique.

2.6.2. Sites Web utiles

- http://people.redhat.com/alikins/system_tuning.html — Informations sur le réglage du système pour les serveurs Linux. Une approche peu conventionnelle du réglage de la performance et du contrôle des ressources pour les serveurs.
- <http://www.linuxjournal.com/article.php?sid=2396> — Outils de contrôle de performance pour Linux. Cette page de Linux Journal s'adresse surtout à l'administrateur souhaitant écrire une solution personnalisée sous forme de graphiques de performance. Cette page datant d'il y a quelques années, il se peut que certaines des informations ne soient plus courantes mais l'idée et l'exécution générales sont toujours valables.
- <http://oprofile.sourceforge.net/> — Site Web du projet OProfile. Cette page inclut des ressources utiles sur OProfile y compris des pointeurs vers les listes de diffusion et le canal IRC #oprofile.

2.6.3. Livres sur le sujet

Les ressources suivantes traitent de différents sujets en relation avec le contrôle des ressources et constituent de bonnes sources d'informations pour les administrateurs de systèmes Red Hat Enterprise Linux :

- *Guide d'administration système de Red Hat Enterprise Linux* ; Red Hat, Inc. — Inclut un chapitre sur de nombreux outils de contrôle des ressources abordés dans ce guide, y compris OProfile.
- *Linux Performance Tuning and Capacity Planning* de Jason R. Fink et Matthew D. Sherer ; Sams — Fournit un horizon plus détaillé des outils de contrôle des ressources examinés dans ce guide et en inclut d'autres qui pourraient être appropriés pour des besoins plus spécifiques quant au contrôle des ressources.
- *Red Hat Linux Security and Optimization* de Mohammed J. Kabir ; Red Hat Press — Les 150 premières pages de ce livre examinent les problèmes liés à la performance et inclut des chapitres consacrés aux problèmes de performance rencontrés en particulier au niveau du réseau, du Web, de la messagerie et des serveurs de fichiers.
- *Linux Administration Handbook* de Evi Nemeth, Garth Snyder et Trent R. Hein ; Prentice Hall — Fournit un petit chapitre d'une portée semblable à celle de ce guide, mais inclut également une section intéressante sur la manière d'effectuer un diagnostic d'un système qui a soudainement ralenti. (Livre en anglais)
- *Linux System Administration: A User's Guide* de Marcel Gagne ; Addison Wesley Professional — Contient un petit chapitre sur le réglage et le contrôle de la performance.

Chapitre 3.

Puissance de traitement et largeur de bande

Des deux ressources examinées dans ce chapitre, la largeur de bande est souvent de compréhension difficile pour les administrateurs alors que la puissance de traitement est un concept beaucoup plus simple à saisir.

De plus, ces deux ressources ne semblent pas vraiment étroitement liées — alors pourquoi les regrouper ?

Ces deux ressources sont examinées ensemble car elles sont toutes les deux basées sur le matériel responsable de la capacité d'un ordinateur à déplacer et traiter des données. Dans ce sens, ces deux ressources entretiennent souvent une relation d'interdépendance.

3.1. Largeur de bande

Au niveau le plus élémentaire, la largeur de bande représente la capacité de transfert de données — en d'autres termes, la quantité de données pouvant être transférée d'un point à un autre au cours d'une durée déterminée. Toute communication de données point à point nécessite deux éléments :

- Un ensemble de conducteurs électriques permettant d'établir une communication à deux niveaux
- Un protocole pour faciliter la communication efficace et fiable des données

À ce titre, deux types de composants système satisfont ces obligations :

- Bus
- Chemins des données

Les sections suivantes abordent chacun des deux composants de manière détaillée.

3.1.1. Bus

Comme nous l'avons mentionné précédemment, les bus permettent une communication point à point et utilisent un certain type de protocole pour garantir que toutes les communications aient lieu de manière contrôlée. Ceci étant, les bus affichent d'autres caractéristiques particulières :

- Des caractéristiques électriques normalisées (telles que le nombre de conducteurs, les niveaux de tension, les vitesses de signalisation, etc.)
- Des caractéristiques mécaniques normalisées (telles que le type de conducteurs, la taille de la carte, la disposition physique, etc.)
- Protocol normalisé

Le terme "normalisé" est important car les bus représentent le moyen de base par lequel les différents composants du système sont reliés entre eux.

Dans bien des cas, les bus permettent l'interconnexion du matériel conçu par de multiples fabricants, une opération qui s'avérerait impossible en l'absence de normalisation. Toutefois, même dans les situations où un bus est la propriété d'un fabricant particulier, la normalisation est importante car elle permet à ce dernier d'implémenter plus facilement différents composants grâce à une interface commune — le bus lui-même.

3.1.1.1. Exemples de bus

Où que vous regardiez dans un ordinateur, vous remarquerez la présence de bus. Parmi les plus courants figurent :

- Les bus de stockage de masse (ATA et SCSI)
- Les réseaux¹ (Ethernet et Token Ring aussi appelé anneau à jetons)
- Les bus mémoire (PCI33 et Rambus®)
- Les bus d'expansion (PCI, ISA, USB)

3.1.2. Chemins des données

Les chemins des données eux peuvent être plus difficiles à identifier mais, tout comme les bus, ils sont présents partout dans un ordinateur. De même que les bus, les chemins des données permettent également une communication point à point. Toutefois, à la différence des bus, les chemins aux données :

- utilisent un protocole plus simple (s'ils en utilisent un)
- ne respectent que peu (voire pas du tout) la normalisation mécanique

Ces différences s'expliquent par le fait que les chemins des données sont généralement internes à certains composants système et ne sont pas utilisés pour faciliter l'interconnexion improvisée de différents composants. En tant que tels, les chemins des données sont particulièrement adaptés pour des situations où une vitesse élevée et un coût moindre représentent une priorité importante par rapport à des situations disposant d'une souplesse générale obtenue grâce à une vitesse basse et un coût élevé.

3.1.2.1. Exemples de chemins des données

Ci-après figurent certains chemins des données typiques :

- CPU vers le chemin des données d'un cache sur puce
- Processeur graphique vers le chemin des données de la mémoire vidéo

3.1.3. Problèmes potentiels liés à la largeur de bande

Les problèmes en relation avec la largeur de bande peuvent se produire de deux manières (aussi bien pour les bus que pour les chemins des données) :

1. Les bus et les chemins des données peuvent constituer une ressource partagée. Dans ce cas, un haut degré de contention pour le bus réduit l'efficacité de la largeur de bande disponible pour tous les périphériques sur le bus.

Un bus SCSI doté de plusieurs disques durs très actifs illustre bien cette situation. Les disques durs très actifs saturent le bus SCSI, ne laissant disponible qu'une largeur de bande très faible pour tout autre périphérique sur le même bus. En conséquence, toutes les activités d'E/S vers tout autre périphérique seront lentes, et ce, même si aucun périphérique du bus n'est extrêmement actif.

2. Il est possible que le bus ou le chemin des données représentent une ressource attitrée à laquelle un nombre fixe de périphériques sont reliés. Dans ce cas, les caractéristiques électriques du

1. Les réseaux sont plus comparables à un bus *inter*-système qu'à un bus *intra*-système

bus (et dans une certaine mesure, la nature du protocole utilisé) limitent la largeur de bande disponible. Cette situation est toutefois plus courante avec les chemins d'accès qu'avec les bus. C'est d'ailleurs une des raisons pour lesquelles les adaptateurs graphiques ont tendance à être plus lents lorsqu'ils fonctionnent à des degrés élevés de résolution et/ou d'intensité de couleur — pour tout rafraîchissement d'écran, davantage de données doivent être transmises le long du chemin des données reliant la mémoire vidéo et le processeur de graphiques.

3.1.4. Solutions potentielles à des problèmes liés à la largeur de bande

Heureusement, il existe des solutions aux problèmes liés à la largeur de bande. En fait, il est possible d'adopter plusieurs approches :

- Distribution de la charge
- Réduction de la charge
- Augmentation de la capacité

Les sections suivantes abordent chacune de ces approches de manière plus détaillée.

3.1.4.1. Répartition de la charge

La première approche consiste à répartir l'activité du bus de manière plus équilibrée. En d'autres termes, si un bus particulier est surchargé et qu'un autre est inactif, peut-être que la situation pourrait être améliorée en transférant une partie de la charge sur le bus inactif.

En tant qu'administrateur système, cette approche devrait être la première à considérer, particulièrement lorsque de nombreux bus supplémentaires existent déjà sur le système. Par exemple, la plupart des ordinateurs comportent au moins deux *canaux* ATA (juste un autre nom pour un bus). Si vous disposez de deux disques durs ATA et de deux canaux ATA, pourquoi les deux disques durs devraient-ils se trouver sur le même canal ?

Même si votre configuration système n'inclut pas de bus supplémentaires, la répartition de la charge peut toujours représenter une approche valable. Les coûts au niveau matériel associés à une telle approche seraient moins élevés que de remplacer un bus existant par un matériel à capacité supérieure.

3.1.4.2. Réduction de la charge

Au premier abord, la réduction et la répartition de la charge semblent représenter différents aspects du même problème. Après tout, la répartition de la charge ne permet-elle pas aussi de la réduire (du moins sur le bus surchargé) ?

Alors que ce point de vue est tout à fait correct, répartir la charge ne revient toutefois pas à réduire la charge *globalement*. La clé ici consiste à déterminer si un certain aspect de la charge du système est à l'origine de la surcharge d'un bus particulier. Par exemple, est-ce qu'un réseau doit faire face à une lourde charge à cause d'activités qui ne sont pas vraiment nécessaires ? Ou peut-être un petit fichier temporaire est-il le destinataire d'activités d'E/S intenses. Si ce fichier temporaire figure sur un serveur de fichiers réseau, une grande partie du trafic réseau pourrait être éliminée simplement en travaillant localement avec ce fichier.

3.1.4.3. Augmentation de la capacité

La solution la plus évidente au problème de largeur de bande insuffisante consiste à augmenter cette dernière d'une manière ou d'une autre. Cette approche est néanmoins souvent assez coûteuse. Imaginez par exemple un contrôleur SCSI avec un bus surchargé. Afin d'augmenter sa largeur de bande, il faudrait remplacer le contrôleur SCSI (et vraisemblablement tous les périphériques connectés à ce dernier) par du matériel plus puissant. Dans le cas où le contrôleur SCSI est une carte indépendante,

le processus est relativement simple ; en revanche, si le contrôleur SCSI fait partie de la carte mère du système, il est beaucoup plus difficile de justifier le coût d'une telle opération.

3.1.5. En résumé...

Tous les administrateurs de système devraient disposer de connaissances sur la largeur de bande et sur l'impact que la configuration et l'utilisation du système ont sur la largeur de bande disponible. Malheureusement, la distinction existant entre un problème lié à la largeur de bande et un autre problème n'est pas toujours très claire. Quelquefois, le problème n'est pas le bus lui-même mais plutôt les composants qui sont reliés au bus.

Par exemple, imaginez un adaptateur SCSI relié à un bus PCI. S'il existe des problèmes de performance au niveau des E/S du disque SCSI, peut-être qu'un adaptateur SCSI à faible performance en est la cause, même si les bus SCSI et PCI eux-mêmes sont bien loin de leur capacité au niveau de leur largeur de bande.

3.2. Puissance de traitement

Souvent appelée puissance CPU, la puissance de traitement des cycles CPU (qui portent parfois d'autres noms) représente la capacité d'un ordinateur à manipuler des données. La puissance de traitement varie en fonction de l'architecture (et de la vitesse d'horloge) du CPU — généralement, des CPU à vitesses d'horloge élevées et des CPU prenant en charge des longueurs de mots plus importantes ont une puissance de traitement supérieure aux CPU plus lents supportant des mots de tailles inférieures.

3.2.1. Informations sur la puissance de traitement

Il est important de garder à l'esprit deux points principaux concernant la puissance de traitement, à savoir :

- La puissance de traitement est fixe
- La puissance de traitement ne peut être stockée

La puissance de traitement est fixe dans le sens où la vitesse du CPU est déterminée. Par exemple, si vous devez ajouter deux nombres (une opération qui, sur la plupart des ordinateurs, ne nécessite qu'une seule instruction pour la machine), un CPU spécifique peut effectuer la tâche à une vitesse déterminée et seulement à cette vitesse spécifique. Mises à part quelques rares exceptions, il n'est même pas possible de *ralentir* le taux auquel le CPU traite les instructions, alors pour ce qui est de l'augmenter, il ne faut même pas y songer.

La puissance de traitement est également fixe à un autre niveau : elle est limitée. C'est à dire qu'il existe des limites quant aux CPU pouvant être branchés dans un ordinateur donné. Certains systèmes sont à même de prendre en charge une vaste gamme de CPU à vitesses variées, alors que d'autres ne pourront peut-être même pas faire l'objet d'une mise à niveau².

La puissance de traitement ne peut pas être mise en réserve pour une utilisation ultérieure. En d'autres termes, si un CPU peut traiter 100 millions d'instructions en une seconde, une seconde d'inactivité se traduit par une perte de traitement équivalent à 100 millions d'instructions.

En prenant ces informations et en les examinant sous une optique légèrement différente, un CPU peut être considéré comme "produisant" un flux d'instructions exécutées à un taux fixe. Si le CPU "pro-

2. Cette situation mène à ce que l'on appelle de manière humoristique une *mise à niveau massive*, qui correspond en fait au remplacement complet d'un ordinateur

duit" des instructions exécutées, un autre élément doit indubitablement les "consommer". La section suivante se concentre sur ces consommateurs d'instructions.

3.2.2. Consommateurs de puissance de traitement

Les deux principaux consommateurs de puissance de traitement sont :

- Les applications
- Le système d'exploitation lui-même

3.2.2.1. Les applications

Les consommateurs de puissance de traitement les plus évidents sont les applications et les programmes que vous souhaitez voir exécuter par l'ordinateur. Qu'il s'agisse d'un tableur ou d'une base de données, ces outils sont les raisons pour lesquelles vous avez un ordinateur.

Un système à CPU unique ne peut effectuer qu'une seule tâche à un moment donné. Par conséquent, si votre application est en cours d'exécution, aucun autre élément de votre système ne peut être exécuté. Et bien évidemment, il en va de même pour la relation inverse — si tout élément autre que votre application est en cours d'exécution, cette dernière ne pourra être exécutée.

Dans de telles conditions, comment se fait-il que de nombreuses applications différentes puissent en apparence tourner sous un système d'exploitation moderne ? La réponse est simple ; ces systèmes d'exploitation sont des systèmes multitâche. En d'autres termes, ils créent l'illusion que de nombreux éléments sont exécutés simultanément alors que c'est en fait impossible. L'astuce consiste à donner à chaque processus une durée d'exécution sur le CPU d'une fraction de seconde avant d'accorder le même traitement à un autre processus qui lui, disposera de la fraction de seconde suivante. À condition que ces *changements de contexte* se produisent suffisamment rapidement, il est possible de créer l'illusion que de multiples applications sont exécutées de manière simultanée.

Bien sûr, les applications effectuent des tâches autres que la seule manipulation de données par le biais du CPU. Elles peuvent aussi bien attendre des entrées de l'utilisateur qu'effectuer des activités d'E/S vers des périphériques comme les disques durs ou des affichages de graphiques. Lorsque ces événements se produisent, l'application n'a plus besoin du CPU. Dans ces cas-là, le CPU peut être utilisé pour d'autres processus exécutant d'autres applications sans pour autant ralentir du tout l'application en attente.

En outre, le CPU peut être utilisé par un autre consommateur de puissance de traitement : le système d'exploitation lui-même.

3.2.2.2. Le système d'exploitation

Il est difficile de déterminer le degré de puissance de traitement consommé par le système d'exploitation. En effet, pour effectuer leur travail, les systèmes d'exploitation utilisent une combinaison de codes au niveau des processus et au niveau du système. Alors qu'il est facile d'utiliser par exemple, un contrôleur de processus pour déterminer ce que fait le processus exécutant un *démon* ou *service*, il est plus difficile de déterminer la puissance de traitement consommée par le traitement d'activités en relation avec les E/S au niveau du système (ce qui est normalement effectué dans le contexte du processus demandant les E/S).

En général, il est possible de diviser ce genre de temps de gestion du système d'exploitation en deux types :

- Gestion interne du système d'exploitation
- Activités en relation avec les processus

La gestion interne du système d'exploitation inclut des activités telles que la programmation des processus et la gestion de la mémoire alors que les activités associées aux processus incluent tout processus supportant le système d'exploitation lui-même, tels que des processus traitant la journalisation des événements dans tout le système ou effectuant le vidage du cache des E/S (cache flushing).

3.2.3. Réponse à une insuffisance de CPU

Lorsque la puissance de traitement disponible est insuffisante pour faire face au travail devant être effectué, deux options sont disponibles :

- Réduction de la charge
- Augmentation de la capacité

3.2.3.1. Réduction de la charge

La réduction de la charge CPU est une opération ne nécessitant aucun coût supplémentaire. L'astuce consiste à identifier les aspects de la charge du système qui sont sous votre contrôle et qui peuvent être réduits. À cet égard, trois aspects ont une importance particulière :

- La réduction du temps de gestion du système d'exploitation
- La réduction du temps de gestion des applications
- L'élimination totale des applications

3.2.3.1.1. La réduction du temps de gestion du système d'exploitation

Afin de réduire le temps de gestion du système d'exploitation, il est nécessaire d'examiner la charge actuelle de votre système afin d'identifier les aspects précis entraînant des temps de gestion excessifs. Parmi ces derniers pourraient figurer :

- La réduction du besoin de programmation fréquente de processus
- La réduction de la quantité d'E/S effectuées

Ceci dit, il ne faut pas s'attendre à des miracles ; dans un système raisonnablement bien configuré, il y a peu de chances que la seule réduction du temps de gestion du système d'exploitation entraîne une amélioration considérable de la performance. En effet, un système raisonnablement bien configuré n'a, par définition, qu'un temps de gestion minimal. Toutefois, si votre système tourne par exemple avec une quantité de RAM insuffisante, vous serez peut-être en mesure de réduire le temps de gestion en résolvant le problème d'une mémoire vive trop petite.

3.2.3.1.2. Réduction du temps de gestion des applications

Pour réduire le temps de gestion d'une application, il est nécessaire de s'assurer que cette dernière dispose bien de tout ce dont elle a besoin pour fonctionner correctement. Certaines applications ont des comportements extrêmement différents selon les environnements — une application peut par exemple voir ses capacités fortement limitées par le traitement de certains types de données, mais pas par le traitement d'autres.

À ce stade, il est important de garder à l'esprit qu'une bonne compréhension des applications exécutées sur votre système est nécessaire pour pouvoir leur permettre de tourner aussi efficacement que possible. Pour ce faire, vous devrez souvent travailler avec vos utilisateurs et/ou les développeurs de votre entreprise afin de pouvoir découvrir des moyens permettant aux applications de tourner plus efficacement.

3.2.3.1.3. Élimination complète des applications

Selon l'environnement de votre entreprise, il est possible que cette approche ne puisse pas être utilisée, car il n'est souvent pas du ressort de l'administrateur système d'imposer une liste des applications qui peuvent ou ne peuvent pas tourner. Toutefois, si vous pouvez identifier des applications qui sont connues pour leur "monopole de CPU", vous serez peut-être en mesure d'influencer les personnes responsables de ce genre de décision, afin que les applications en question soient supprimées.

À cet égard, vous ne serez vraisemblablement pas la seule personne impliquée. Les utilisateurs concernés devraient certainement faire partie de ce processus ; dans bien des cas, ils disposeront probablement des connaissances et du pouvoir politique nécessaires pour apporter les changements nécessaires à la liste des applications.



Astuce

Gardez bien à l'esprit qu'il ne sera peut-être pas nécessaire de retirer une application donnée de tout les systèmes de votre entreprise. Vous pourrez peut-être déplacer une application particulièrement gourmande en CPU d'un système surchargé vers un autre système quasiment inoccupé.

3.2.3.2. Augmentation de la capacité

Bien sûr, s'il n'est pas possible de réduire la demande de puissance de traitement, vous devez trouver des moyens d'augmenter la puissance de traitement disponible. Cette option est certes tout à fait possible, mais elle entraînera des dépenses.

3.2.3.2.1. Mise à niveau du CPU

L'approche la plus simple consiste à déterminer s'il est possible de mettre à niveau le CPU de votre système. Pour ce faire, la première étape consiste à voir si le CPU actuel peut être retiré. Certains systèmes (essentiellement les ordinateurs portables) dotés de CPU soudés ne permettent pas une mise à niveau. Sur les autres en revanche, les CPU sont branchés et rendent donc les mises à niveau possibles — tout du moins en théorie.

Il convient ensuite de faire un peu de recherche afin de déterminer si un CPU plus rapide existe pour la configuration de votre système. Par exemple, si vous disposez actuellement d'un CPU de 1GHz et qu'il existe une unité de 2GHz du même type, une mise à jour sera peut-être possible.

Finalement, il est essentiel de déterminer la vitesse d'horloge maximale prise en charge par votre système. Toujours sur la base de l'exemple précédent, même s'il existe un CPU de 2GHz d'un type approprié, un simple échange de CPU n'est pas vraiment une option si votre système ne prend en charge que des processeurs tournant à une vitesse égale ou inférieure à 1GHz.

Dans le cas où vous ne pourriez pas installer un CPU plus rapide dans votre système, l'étendue de vos options se limitera peut-être au remplacement des cartes mères ou à la mise à niveau massive dont nous avons parlé précédemment.

Toutefois, certaines configurations système permettent une approche légèrement différente. Au lieu de remplacer le CPU actuel, pourquoi ne pas tout simplement en ajouter un autre ?

3.2.3.2.2. Le traitement multitâche symétrique est-il adapté à votre situation ?

Le traitement multitâche symétrique (aussi appelé multitraitement symétrique ou SMP de l'anglais Symmetric multiprocessing) permet à un ordinateur d'avoir plus d'un CPU partageant toutes les res-

sources système. Ainsi, contrairement à un système doté d'un seul processeur, un système SMP peut, lui, faire tourner plus d'un processus à la fois.

Au premier abord, cette situation semble représenter le rêve d'un administrateur de système. SMP permet avant tout d'augmenter la puissance de CPU d'un système, même s'il existe des CPU avec une vitesse d'horloge plus rapide — simplement en ajoutant un autre CPU. Cette souplesse s'accompagne néanmoins d'un certain nombre de contraintes.

La première d'entre elles est que tous les systèmes ne sont pas en mesure de fonctionner en traitement multitâche symétrique (SMP). La carte mère de votre système doit être conçue pour prendre en charge de multiples processeurs. Si ce n'est pas le cas, la mise à niveau de la carte mère (au strict minimum) sera nécessaire.

Le deuxième d'entre elles est que SMP augmente le temps de gestion du système. En y réfléchissant bien, l'augmentation du nombre de CPU pour lesquels la programmation de tâches doit être effectuée se traduit logiquement, pour le système d'exploitation, en un plus grand nombre de cycles CPU au niveau de la gestion. En outre, un plus grand nombre de CPU peut entraîner une contention accrue pour les ressources système. En raison de ces facteurs, la mise à niveau d'un système à double processeur vers une unité à quadruple processeur n'entraîne pas une augmentation à 100% de la puissance CPU disponible. En fait, en fonction du matériel même, de la charge de travail et de l'architecture du processeur, il est possible d'arriver à un stade où l'ajout d'un autre processeur pourrait en fait *réduire* la performance du système.

Il est aussi important de se souvenir que SMP ne permet pas d'influencer des charges de travail composées d'une application monolithique avec un seul flux d'exécution. En d'autres termes, si un grand programme de simulation nécessitant une activité de calcul intense tourne en tant qu'un processus et n'a pas de fils (ou thread), il ne sera pas exécuté plus rapidement sur un système SMP que sur un ordinateur à processeur unique. En fait, il tournera même peut-être un peu plus lentement à cause de la gestion supplémentaire engendrée par SMP. Ainsi, de nombreux administrateurs de système estiment qu'en matière de CPU, une puissance de traitement à flux unique est l'option à retenir. Elle offre une puissance CPU optimale avec des restrictions minimales au niveau de son utilisation.

Même si ces informations semblent indiquer que SMP n'est jamais une bonne option, il existe certaines situations dans lesquelles un tel choix est tout à fait approprié. Des environnements faisant tourner de multiples applications à calculs intensifs représentent, par exemple, un environnement tout à fait approprié pour SMP. En effet, des applications dont la tâche n'est autre que d'effectuer des calculs pendant de longues périodes de temps maintiennent la contention entre les processus actifs (et par conséquent, le temps de gestion du système d'exploitation) à un minimum, alors que les processus eux-mêmes utilisent chaque CPU.

Il est important de se rappeler également que la performance d'un système SMP a tendance à se dégrader plus progressivement au fur et à mesure que la charge du système augmente. C'est précisément une des raisons pour lesquelles les systèmes SMP sont populaires dans des environnements de serveurs ou dans des environnements à utilisateurs multiples, car l'impact qu'un mélange de processus changeant constamment a sur la charge du système entier est moindre sur un ordinateur à processeurs multiples.

3.3. Informations spécifiques à Red Hat Enterprise Linux

Sous Red Hat Enterprise Linux, le contrôle de l'utilisation de la largeur de bande et du CPU se fait grâce à l'utilisation des outils examinés dans le Chapitre 2 ; il est par conséquent recommandé de lire ce chapitre (si ce n'est pas déjà fait) avant de poursuivre.

3.3.1. Contrôle de la largeur de bande sur Red Hat Enterprise Linux

Comme nous l'avons mentionné dans la Section 2.4.2, il est difficile de contrôler directement l'utilisation de la largeur de bande. Néanmoins, en analysant les statistiques au niveau des périphériques, il est possible d'évaluer grossièrement si une largeur de bande insuffisante pose un problème quelconque pour votre système.

Avec `vmstat`, il est possible de déterminer si l'activité générale des périphériques est excessive, en examinant les champs `bi` et `bo` ; en outre, les champs `si` et `so` fournissent des informations un peu plus précises sur le degré d'activité du disque résultant des activités d'E/S associées au swap.

```

procs
r  b  w      swpd   free   buff  cache   si  so      bi   bo   in   cs  us  sy  id
1  0  0          0 248088 158636 480804  0  0      2    6  120  120 10   3  87

```

Dans l'extrait ci-dessus, le champ `bi` montre que deux blocs par seconde sont écrits sur les périphériques blocs (essentiellement les disques durs), alors que le champ `bo` indique lui que six blocs par seconde sont lus depuis les périphériques blocs. Il est également possible de voir qu'aucune partie de cette activité n'est due à un échange de mémoire (aussi appelé swapping) car les champs `si` et `so` montrent tous les deux un taux d'activités d'E/S associé au swap équivalent à zéro kilo-octet/seconde.

En utilisant `iostat`, il est possible d'obtenir des informations plus précises sur l'activité associée au disque :

```

Linux 2.4.21-1.1931.2.349.2.2.entsmp (raptor.example.com)      07/21/2003

avg-cpu:  %user   %nice    %sys    %idle
           5.34    4.60    2.83   87.24

Device:            tps    Blk_read/s    Blk_wrtn/s    Blk_read    Blk_wrtn
dev8-0              1.10         6.21         25.08      961342     3881610
dev8-1              0.00         0.00         0.00         16           0

```

Cette sortie montre que le périphérique dont le nombre majeur est 8 (correspondant à `/dev/sda`, le premier disque SCSI) avait une moyenne légèrement supérieure à une opération d'E/S par seconde (le champ `tps`). La plupart de l'activité d'E/S de ce périphérique était constituée par des opérations d'écriture (le champ `Blk_wrtn`), avec un peu plus de 25 blocs écrits par seconde (le champ `Blk_wrtn/s`).

Dans le cas où des informations encore plus détaillées seraient nécessaires, utilisez l'option `-x` de `iostat` :

```

Linux 2.4.21-1.1931.2.349.2.2.entsmp (raptor.example.com)      07/21/2003

avg-cpu:  %user   %nice    %sys    %idle
           5.37    4.54    2.81   87.27

Device:    rrqm/s  wrqm/s    r/s    w/s    rsec/s    wsec/s    rkB/s    kB/s  avgrq-sz
/dev/sda   13.57    2.86    0.36  0.77   32.20    29.05    16.10    14.53   54.52
/dev/sda1  0.17    0.00    0.00  0.00    0.34     0.00     0.17     0.00  133.40
/dev/sda2  0.00    0.00    0.00  0.00    0.00     0.00     0.00     0.00  11.56
/dev/sda3  0.31    2.11    0.29  0.62    4.74    21.80     2.37    10.90  29.42
/dev/sda4  0.09    0.75    0.04  0.15    1.06     7.24     0.53     3.62  43.01

```

Outre le fait que les lignes plus longues contiennent plus de champs, la première chose dont il faut se souvenir est que cette sortie d'`iostat` affiche désormais des statistiques sur les partitions de manière individuelle. En utilisant `df` pour associer les points de montage aux noms de périphériques, il est

possible d'utiliser ce rapport pour déterminer par exemple si la partition `/home` est soumise à une charge excessive.

En fait, la sortie renvoyée par la commande `iostat -x` est composée de lignes plus longues contenant plus d'informations que l'extrait ci-dessus, comme le montre le reste de chaque ligne reproduit ci-après (notez que la colonne relative aux périphériques faisant partie de l'extrait d'origine a été rajoutée ici pour permettre une lecture plus facile):

```
Device:   avgqu-sz   await   svctm   %util
/dev/sda      0.24    20.86    3.80    0.43
/dev/sda1     0.00   141.18  122.73    0.03
/dev/sda2     0.00     6.00    6.00    0.00
/dev/sda3     0.12   12.84    2.68    0.24
/dev/sda4     0.11   57.47    8.94    0.17
```

Dans cet exemple, il est intéressant de remarquer que `/dev/sda2` est la partition swap du système ; étant donné les nombreux champs affichant `0.00`, il est évident que le swapping ne pose aucun problème pour le système.

Le deuxième élément de la colonne de périphériques, `/dev/sda1`, est un autre élément intéressant en raison des statistiques inhabituelles de cette partition ; en effet, l'activité globale semble faible et pourtant, la taille moyenne des requêtes d'E/S (le champ `avgqrq-sz`), le temps d'attente moyen (le champ `await`) et le temps de service moyen (le champ `svctm`) sont beaucoup plus importants que pour les autres partitions ; pourquoi ? Parce que cette partition contient le répertoire `/boot/`, qui est l'endroit où le noyau et le disque de mémoire vive initiale (ramdisk) sont stockés. Lorsque le système démarre, les E/S des opérations de lecture (notez bien que seuls les champs relatifs à `rsec/s` et `rkB/s` n'affichent pas de zéros ; d'une manière générale, aucune opération d'écriture n'est effectuée ici) utilisées lors de ce processus se font pour de nombreux blocs, entraînant des temps d'attente et de service relativement longs, comme l'affiche la sortie d'`iostat`.

Il est possible d'utiliser `sar` pour un affichage à plus long terme des statistiques d'E/S ; la commande `sar -b` affiche par exemple, un rapport d'E/S général comme le montre l'extrait ci-dessous :

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (raptor.example.com) 07/21/2003

12:00:00 AM      tps      rtps      wtps      bread/s      bwrtn/s
12:10:00 AM      0.51      0.01      0.50      0.25      14.32
12:20:01 AM      0.48      0.00      0.48      0.00      13.32
...
06:00:02 PM      1.24      0.00      1.24      0.01      36.23
Average:         1.11      0.31      0.80      68.14      34.79
```

Ici, comme dans l'affichage initial d'`iostat`, les statistiques sont regroupées pour tous les périphériques blocs.

Un autre rapport sur les E/S peut être créé grâce à `sar -d`, comme le montre l'extrait suivant :

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (raptor.example.com) 07/21/2003

12:00:00 AM      DEV      tps      sect/s
12:10:00 AM      dev8-0   0.51     14.57
12:10:00 AM      dev8-1   0.00     0.00
12:20:01 AM      dev8-0   0.48     13.32
12:20:01 AM      dev8-1   0.00     0.00
...
06:00:02 PM      dev8-0   1.24     36.25
06:00:02 PM      dev8-1   0.00     0.00
Average:         dev8-0   1.11     102.93
Average:         dev8-1   0.00     0.00
```


Ce rapport fournit certes des informations périphérique par périphérique, mais de manière relativement superficielle.

Malgré l'absence de statistiques explicites montrant l'utilisation de la largeur de bande pour un chemin des données ou un bus spécifique, il est au moins possible d'une part de voir l'activité des périphériques et d'autre part, d'utiliser cette dernière afin de déterminer indirectement le chargement du bus.

3.3.2. Contrôle de l'utilisation CPU sur Red Hat Enterprise Linux

Contrairement à la largeur de bande, le contrôle de l'utilisation CPU est une tâche relativement simple. Que ce soit grâce à un simple pourcentage d'utilisation CPU dans le **Moniteur système** de GNOME ou aux statistiques plus détaillées rapportées par la commande `sar`, il est possible de déterminer d'une part combien de puissance CPU est consommée et d'autre part, quel élément la consomme.

Au-delà du **Moniteur système** de GNOME, il existe un autre outil de contrôle des ressources à savoir, `top`, le premier outil abordé dans le Chapitre 2, qui fournit lui, une représentation plus détaillée de l'utilisation CPU. Ci-après figure un rapport établi par la commande `top` depuis un poste de travail à double processeur :

```

9:44pm up 2 days, 2 min,  1 user,  load average: 0.14, 0.12, 0.09
90 processes: 82 sleeping, 1 running, 7 zombie, 0 stopped
CPU0 states:  0.4% user,   1.1% system,   0.0% nice, 97.4% idle
CPU1 states:  0.5% user,   1.3% system,   0.0% nice, 97.1% idle
Mem:  1288720K av, 1056260K used,  232460K free,        0K shrd,  145644K buff
Swap: 522104K av,        0K used,  522104K free                469764K cached
    
```

PID	USER	PRI	NI	SIZE	RSS	SHARE	STAT	%CPU	%MEM	TIME	COMMAND
30997	ed	16	0	1100	1100	840	R	1.7	0.0	0:00	top
1120	root	5	-10	249M	174M	71508	S<	0.9	13.8	254:59	X
1260	ed	15	0	54408	53M	6864	S	0.7	4.2	12:09	gnome-terminal
888	root	15	0	2428	2428	1796	S	0.1	0.1	0:06	sendmail
1264	ed	15	0	16336	15M	9480	S	0.1	1.2	1:58	rhn-applet-gui
1	root	15	0	476	476	424	S	0.0	0.0	0:05	init
2	root	0K	0	0	0	0	SW	0.0	0.0	0:00	migration_CPU0
3	root	0K	0	0	0	0	SW	0.0	0.0	0:00	migration_CPU1
4	root	15	0	0	0	0	SW	0.0	0.0	0:01	keventd
5	root	34	19	0	0	0	SWN	0.0	0.0	0:00	ksoftirqd_CPU0
6	root	34	19	0	0	0	SWN	0.0	0.0	0:00	ksoftirqd_CPU1
7	root	15	0	0	0	0	SW	0.0	0.0	0:05	kswapd
8	root	15	0	0	0	0	SW	0.0	0.0	0:00	bdflush
9	root	15	0	0	0	0	SW	0.0	0.0	0:01	kupdated
10	root	25	0	0	0	0	SW	0.0	0.0	0:00	mdrecoveryd

La première information relative au CPU se trouve sur la toute première ligne : la moyenne de charge. Cette dernière est représentée par un chiffre correspondant au nombre moyen de processus exécutables sur le système. La moyenne de charge est souvent exprimée sous forme de trois groupes de chiffres (de la même manière que `top`) qui correspondent respectivement à la moyenne de charge de la dernière minute et des 5, 15 dernières minutes ; dans notre exemple, le système n'était pas très occupé.

La ligne suivante, bien que n'étant pas étroitement liée à l'utilisation CPU a tout de même une relation indirecte avec cette dernière, dans la mesure où elle affiche le nombre de processus exécutables (un seul dans le cas présent -- souvenez-vous de ce chiffre car il a une signification particulière dans cet exemple). Le nombre de processus exécutables représente un bon indicateur du degré de limitation dicté par le CPU.

Viennent ensuite deux lignes affichant l'utilisation courante de chacun des deux CPU sur le système. Les statistiques d'utilisation montrent si l'augmentation des cycles CPU étaient le résultat d'un traitement intense au niveau de l'utilisateur ou au niveau du système ; apparaît également ici une statistique indiquant le degré selon lequel les processus aux priorités de programmation modifiées sont la cause d'une augmentation du temps CPU. Finalement, apparaît une statistique relative au temps d'inactivité.

Plus bas dans la section de l'affichage relative aux processus figurent des statistiques montrant que `top` lui-même est le processus utilisant le plus de puissance CPU ; en d'autres termes, le seul processus sur ce système qui autrement serait exécutable est `top` prenant une "image" de lui-même.



Astuce

Il est important de ne pas oublier que l'opération consistant à exécuter un moniteur de système a un impact sur les statistiques d'utilisation des ressources que vous obtenez. Tel est le cas, jusqu'à un certain point, pour tous les moniteurs basés sur des logiciels.

Afin d'obtenir de plus amples informations sur l'utilisation CPU, il est nécessaire de changer d'outil. En examinant la sortie de `vmstat`, la vue d'ensemble du système de notre exemple est légèrement différente, comme le montre l'extrait suivant :

procs			memory				swap		io		system			cpu	
r	b	w	swpd	free	buff	cache	si	so	bi	bo	in	cs	us	sy	id
1	0	0	0	233276	146636	469808	0	0	7	7	14	27	10	3	87
0	0	0	0	233276	146636	469808	0	0	0	0	523	138	3	0	96
0	0	0	0	233276	146636	469808	0	0	0	0	557	385	2	1	97
0	0	0	0	233276	146636	469808	0	0	0	0	544	343	2	0	97
0	0	0	0	233276	146636	469808	0	0	0	0	517	89	2	0	98
0	0	0	0	233276	146636	469808	0	0	0	32	518	102	2	0	98
0	0	0	0	233276	146636	469808	0	0	0	0	516	91	2	1	98
0	0	0	0	233276	146636	469808	0	0	0	0	516	72	2	0	98
0	0	0	0	233276	146636	469808	0	0	0	0	516	88	2	0	97
0	0	0	0	233276	146636	469808	0	0	0	0	516	81	2	0	97

Les informations ci-dessus ont été obtenues grâce à la commande `vmstat 1 10` qui recueille des échantillons sur le système toutes les secondes, dix fois de suite. Au premier abord, les statistiques relatives au CPU (à savoir les champs `us`, `sy` et `id`) semblent similaires à celles affichées par `top`, ou peut-être même légèrement moins détaillées. Néanmoins, contrairement à `top`, il est possible d'obtenir ici un certain nombre d'informations sur la manière dont le CPU est utilisé.

En examinant les champs `system`, on peut voir que le CPU traite en moyenne environ 500 interruptions par seconde et qu'il alterne entre les processus de 80 à presque 400 fois par seconde. Si vous pensez que ces chiffres représentent une activité intense, détrompez-vous car les opérations de traitement au niveau de l'utilisateur (le champ `us`) atteignent seulement 2% en moyenne, alors que celles effectuées au niveau du système (le champ `sy`) sont généralement inférieures à 1%. Dans cet exemple, il s'agit également d'un système inactif.

En examinant les outils offerts par Sysstat, on peut voir que `iostat` et `mpstat` n'offrent que peu d'informations supplémentaires par rapport aux sorties obtenues avec `top` et `vmstat`. Toutefois, `sar` crée un certain nombre de rapports pouvant se révéler utiles lors du contrôle de l'utilisation CPU.

Le premier rapport est obtenu grâce à la commande `sar -q` qui affiche la longueur de la file d'attente des processus exécutables (`run`), le nombre total des processus et les moyennes de charge enregistrés lors de la dernière minute et au cours des 5 dernières minutes. Ci-après figure un exemple de ce rapport :

```

12:00:01 AM   runq-sz   plist-sz   ldavg-1   ldavg-5
12:10:00 AM           3         122       0.07     0.28
12:20:01 AM           5         123       0.00     0.03
...
09:50:00 AM           5         124       0.67     0.65
Average:         4         123       0.26     0.26

```

Dans cet exemple, le système est certes toujours occupé (puisque plus d'un processus est exécutable à tout moment donné), mais il n'est pas excessivement chargé (car ce système précis est doté de plus d'un processeur).

Le rapport `sar` ci-dessous qui fournit des informations sur le CPU est produit par la commande `sar -u` :

```

Linux 2.4.21-1.1931.2.349.2.2.entsmp (falcon.example.com)    07/21/2003

12:00:01 AM      CPU   %user   %nice   %system   %idle
12:10:00 AM      all   3.69    20.10    1.06     75.15
12:20:01 AM      all   1.73    0.22    0.80     97.25
...
10:00:00 AM      all   35.17   0.83    1.06     62.93
Average:         all   7.47    4.85    3.87     83.81

```

Les statistiques contenues dans ce rapport ne sont pas vraiment différentes de celles fournies par de nombreux autres outils. Toutefois, le gros avantage dans le cas présent est que `sar` fournit ces données de manière constante et par là même, représente une commande beaucoup plus utile pour obtenir des moyennes à long terme ou pour créer des graphiques sur l'utilisation CPU.

Sur des systèmes à processeurs multiples, la commande `sar -U` permet de fournir des statistiques aussi bien pour un processeur particulier que pour l'ensemble des processeurs. Ci-après figure un exemple de sortie renvoyée par `sar -U ALL` :

```

Linux 2.4.21-1.1931.2.349.2.2.entsmp (falcon.example.com)    07/21/2003

12:00:01 AM      CPU   %user   %nice   %system   %idle
12:10:00 AM      0     3.46    21.47    1.09     73.98
12:10:00 AM      1     3.91    18.73    1.03     76.33
12:20:01 AM      0     1.63    0.25    0.78     97.34
12:20:01 AM      1     1.82    0.20    0.81     97.17
...
10:00:00 AM      0     39.12   0.75    1.04     59.09
10:00:00 AM      1     31.22   0.92    1.09     66.77
Average:         0     7.61    4.91    3.86     83.61
Average:         1     7.33    4.78    3.88     84.02

```

La commande `sar -w` établit un rapport sur le nombre de changements de contextes par seconde et permet par là même, d'obtenir des informations supplémentaires sur les endroits monopolisant les cycles CPU :

```

Linux 2.4.21-1.1931.2.349.2.2.entsmp (falcon.example.com)    07/21/2003

12:00:01 AM      cswch/s
12:10:00 AM           537.97
12:20:01 AM           339.43
...
10:10:00 AM           319.42
Average:         1158.25

```

Il est également possible de créer deux rapports `sar` différents fournissant des informations sur l'activité d'interruption. Le premier (produit à l'aide de la commande `sar -I SUM`) affiche une seule statistique sur les "interruptions par seconde" :

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (falcon.example.com)      07/21/2003

12:00:01 AM      INTR      intr/s
12:10:00 AM      sum      539.15
12:20:01 AM      sum      539.49
...
10:40:01 AM      sum      539.10
Average:         sum      541.00
```

À l'aide de la commande `sar -I PROC`, il est possible de ventiler les données relatives à l'activité d'interruption par processeur (sur des systèmes à processeurs multiples) *et* par niveau d'interruption (de 0 à 15) comme le montre l'extrait ci-dessous :

```
Linux 2.4.21-1.1931.2.349.2.2.entsmp (pigdog.example.com)    07/21/2003

12:00:00 AM CPU i000/s i001/s i002/s i008/s i009/s i011/s i012/s
12:10:01 AM 0 512.01 0.00 0.00 0.00 3.44 0.00 0.00

12:10:01 AM CPU i000/s i001/s i002/s i008/s i009/s i011/s i012/s
12:20:01 AM 0 512.00 0.00 0.00 0.00 3.73 0.00 0.00
...
10:30:01 AM CPU i000/s i001/s i002/s i003/s i008/s i009/s i010/s
10:40:02 AM 0 512.00 1.67 0.00 0.00 0.00 15.08 0.00
Average:    0 512.00 0.42 0.00 N/A 0.00 6.03 N/A
```

Ce rapport (tronqué afin de tenir sur la page) comprend une colonne par niveau d'interruption (le champ `i002/s` illustrant le taux pour le niveau 2 d'interruption). Si ce système était doté de processeurs multiples, la sortie comprendrait une ligne par période d'échantillonnage et ce, pour chaque CPU.

Un autre point important à noter concernant ce rapport est que `sar` ajoute ou retire des champs d'interruption spécifiques, si aucune information n'est recueillie pour le champ en question. Comme le montre l'exemple ci-dessus, la fin du rapport inclut des niveaux d'interruption (à savoir 3 et 10) qui n'apparaissent pas au début de la période d'échantillonnage.



Remarque

Il existe deux autres rapports `sar` fournissant des informations sur les interruptions — `sar -I ALL` et `sar -I XALL`. Toutefois, la configuration par défaut de l'utilitaire de recueil de données `sadc` ne récolte pas les informations nécessaires pour ces rapports. Pour permettre la création de tels rapports, il suffit de modifier le fichier `/etc/cron.d/sysstat` en modifiant la ligne suivante :

```
*/10 * * * * root /usr/lib/sa/sa1 1 1
```

de sorte à qu'elle ressemble à la ligne ci-dessous :

```
*/10 * * * * root /usr/lib/sa/sa1 -I 1 1
```

Notez bien que cette modification donne à `sadc` l'instruction de recueillir des données supplémentaires et que par conséquent, elle entraîne la création de fichiers de données plus volumineux. Il

est donc essentiel de vous assurez que la configuration de votre système permet bien prendre en charge une consommation d'espace supplémentaire.

3.4. Ressources supplémentaires

Cette section contient de nombreuses ressources pouvant être utilisées pour approfondir vos connaissances sur des sujets spécifiques à Red Hat Enterprise Linux, qui ont été abordés dans ce chapitre.

3.4.1. Documentation installée

Les ressources suivantes sont installées au cours d'une installation normale de Red Hat Enterprise Linux et peuvent vous aider à étendre vos connaissances sur les thèmes abordés dans ce chapitre.

- Page de manuel de `vmstat(8)` — Pour apprendre comment afficher un aperçu concis de l'utilisation des processus, de la mémoire, du swap, des E/S, du système et du CPU.
- Page de manuel de `iostat(1)` — Pour apprendre comment afficher des statistiques relatives au CPU et aux E/S.
- Page de manuel de `sar(1)` — Pour apprendre comment créer des rapports sur l'utilisation des ressources du système.
- Page de manuel de `sadc(8)` — Pour apprendre comment recueillir des données sur l'utilisation du système.
- Page de manuel de `sa1(8)` — Pour obtenir des informations sur un script qui exécute périodiquement la commande `sadc`.
- Page de manuel de `top(1)` — Pour apprendre comment afficher des statistiques sur l'utilisation du CPU et sur l'activité au niveau des processus.

3.4.2. Sites Web utiles

- http://people.redhat.com/alikins/system_tuning.html — Informations sur le réglage du système pour les serveurs Linux. Une approche peu conventionnelle du réglage de la performance et du contrôle des ressources pour les serveurs.
- <http://www.linuxjournal.com/article.php?sid=2396> — Outils de contrôle de performance pour Linux. Cette page de Linux Journal s'adresse plutôt à l'administrateur souhaitant écrire une solution personnalisée sous forme de graphiques de performance. Cette page datant d'il y a quelques années, il se peut que certaines des informations ne soient plus courantes mais l'idée et l'exécution générales n'en demeurent pas moins valables.

3.4.3. Livres sur le sujet

Les ressources suivantes traitent de différents sujets en relation avec le contrôle des ressources et constituent de bonnes sources d'informations pour les administrateurs de systèmes Red Hat Enterprise Linux :

- *Guide d'administration système de Red Hat Enterprise Linux*; Red Hat, Inc. — Inclut un chapitre sur de nombreux outils de contrôle des ressources abordés dans ce guide.

- *Linux Performance Tuning and Capacity Planning* de Jason R. Fink et Matthew D. Sherer ; Sams — Fournit un horizon plus détaillé des outils de contrôle des ressources examinés dans ce guide et en inclut d'autres qui pourraient être appropriés pour des besoins plus spécifiques lors du contrôle des ressources.
- *Linux Administration Handbook* de Evi Nemeth, Garth Snyder et Trent R. Hein ; Prentice Hall — Fournit un petit chapitre d'une portée semblable à celle de ce guide, mais inclut également une section intéressante sur la manière d'effectuer un diagnostic d'un système qui a soudainement ralenti.
- *Linux System Administration: A User's Guide* de Marcel Gagne ; Addison Wesley Professional — Contient un petit chapitre sur le réglage et le contrôle de la performance.

Chapitre 4.

Mémoire physique et mémoire virtuelle

De nos jours, tous les ordinateurs universels font partie de la catégorie intitulée *ordinateurs à programmes stockés*. Comme ce terme l'indique, les ordinateurs à programmes stockés chargent les instructions (les éléments de base des programmes) dans un type de mémoire interne où ils les exécutent par la suite.

Les ordinateurs à programmes stockés utilisent également ce même stockage pour les données. Outre ce type d'ordinateurs, il existe aussi ceux qui utilisent leur configuration matérielle pour contrôler leur fonctionnement (comme les anciens ordinateurs basés sur un tableau de connexions).

Sur les premiers ordinateurs à programmes stockés, l'endroit où les programmes étaient conservés a porté de nombreux noms et utilisait un grand nombre de technologies différentes qui allaient de points sur un tube à rayons cathodiques à des impulsions de pression dans une colonne de mercure. Heureusement, les ordinateurs modernes ont désormais recours à des technologies dotées de capacités de stockage largement supérieures et de taille bien moindre qu'auparavant.

4.1. Modes d'accès au stockage

Il est important de garder à l'esprit tout au long de ce chapitre, que les ordinateurs ont tendance à accéder au stockage de certaines manières. En fait, la plupart des modes d'accès au stockage ont généralement un des attributs suivants (voire les deux) :

- L'accès a tendance à être séquentiel
- L'accès a tendance à être localisé

En mode d'accès séquentiel, si le CPU accède à une adresse N , il est très probable que $N+1$ sera l'adresse suivante à laquelle le CPU accédera. Un tel mode d'accès est logique dans la mesure où la plupart des programmes se composent de grandes sections d'instructions qui sont exécutées — dans l'ordre — les unes après les autres.

Selon le mode d'accès localisé, si le CPU accède à une adresse X , il est très probable que dans le futur, le CPU accédera à d'autres adresses voisines de X .

Ces attributs sont essentiels car ils permettent à du stockage plus petit et plus rapide de tamponner efficacement du stockage plus grand et plus lent. Ce principe constitue la base de l'implémentation de la mémoire virtuelle. Avant de passer à la mémoire virtuelle, il convient d'examiner d'abord les différentes technologies de stockage actuellement utilisées.

4.2. Éventail des options de stockage

De nos jours, les ordinateurs modernes ont recours à une variété de technologies de stockage. Chaque technologie sert à remplir une fonction spécifique et pour ce faire, dispose de vitesses et de capacités appropriées.

Parmi ces technologies figurent :

- Les registres du CPU
- La mémoire cache
- RAM
- Les disques durs

- Le stockage de sauvegarde hors-ligne (bande, disque optique, etc.)

En termes de possibilités et de coût, ces technologies constituent un large éventail. Par exemple, les registres du CPU affichent les caractéristiques suivantes :

- Rapidité considérable (temps d'accès de quelques nanosecondes)
- Capacité faible (généralement moins de 200 octets)
- Possibilités de développement très limitées (un changement de l'architecture CPU serait nécessaire)
- Coûts élevés (plus d'un dollar par octet)

Toutefois, à l'autre extrémité de l'éventail, le stockage hors-ligne affiche lui, les caractéristiques suivantes :

- Lenteur considérable (les temps d'accès peuvent se mesurer en jours si le support de sauvegarde doit être acheminé sur de longues distances)
- Capacité élevée (dizaines - centaines de giga-octets)
- Possibilités de développement quasiment illimitées (la seule limitation se situe au niveau de l'espace physique nécessaire pour héberger les supports de sauvegarde)
- Coûts très élevés (de l'ordre du centime par octet)

En utilisant différentes technologies avec des capacités différentes, il est possible de raffiner la conception des systèmes afin de maximiser la performance, tout en réduisant les coûts au minimum. La section suivante examine chacune des technologies composant l'éventail des options de stockage.

4.2.1. Registres du CPU

Toute conception de CPU moderne inclut des registres et ce, pour une variété de raisons allant du stockage de l'adresse de l'instruction en cours d'exécution au stockage et aux manipulations de données à des fins plus générales. Les registres du CPU tournent à la même vitesse que celle du CPU ; dans le cas contraire, il existerait un sérieux goulet d'étranglement pour la performance générale du système. En effet, les registres jouent un rôle dans presque toutes les opérations effectuées par le CPU.

Le nombre de registres du CPU (et leurs utilisations) dépend strictement de la conception de l'architecture du CPU lui-même. Il n'existe aucun moyen de modifier le nombre de registres du CPU, sauf en migrant vers un CPU avec une architecture différente. Dans de telles conditions, le nombre de registres du CPU peut être considéré comme fixe dans la mesure où son changement nécessite non seulement de grands efforts mais également de lourdes dépenses.

4.2.2. Mémoire cache

Le but de la mémoire cache est de jouer le rôle d'un tampon entre les registres très limités du CPU à vitesse élevée d'une part, et la mémoire du système principal — à laquelle on fait généralement référence sous l'acronyme RAM¹ — d'une capacité beaucoup plus élevée et relativement lente d'autre part. La mémoire cache a une vitesse de fonctionnement semblable à celle du CPU lui-même, si bien que lorsque le CPU accède à des données mises en cache, il ne doit pas attendre avant d'obtenir les données souhaitées.

La mémoire cache est configurée de telle sorte que, lorsque des données doivent être lues depuis la RAM, le matériel du système vérifie d'abord si les données requises sont en cache. Si tel est le cas, les données sont rapidement obtenues et utilisées par le CPU. En revanche, si les données ne sont pas

1. Alors que l'acronyme "RAM" signifie "Random Access Memory" et pourrait tout à fait être utilisé pour toute technologie de stockage permettant l'accès non séquentiel aux données stockées, lorsque les administrateurs système parlent de RAM, ils ne font référence à rien d'autre que la mémoire principale du système.

en cache, elles sont lues depuis la mémoire vive (ou RAM) et, tout en étant transmises au CPU, sont également mises en cache (juste au cas où elles seraient nécessaires ultérieurement). Pour le CPU, tout le processus est effectué de manière transparente si bien que la seule différence entre l'accès aux données en cache et l'accès aux données en mémoire vive réside au niveau de la durée nécessaire à l'obtention des données souhaitées.

En termes de capacité de stockage, le cache a une taille beaucoup plus petite que la RAM. Par conséquent, tous les octets en mémoire vive ne peuvent pas bénéficier de leur propre emplacement unique en cache. Dans de telles circonstances, il est nécessaire de subdiviser le cache en sections qui peuvent alors être utilisées pour stocker différentes parties de la RAM d'une part, et d'autre part, pour disposer d'un mécanisme permettant à chaque partie du cache d'accueillir différentes parties de la RAM et ce, à différents moments. Malgré la différence de taille entre le cache et la RAM, et étant donnée la nature séquentielle ou localisée de l'accès au stockage, une toute petite quantité de cache peut vraiment accélérer l'accès à une grande quantité de mémoire vive.

Lors de l'écriture de données depuis le CPU, les choses se compliquent quelque peu. Pour une telle opération, deux approches différentes peuvent être adoptées. Dans les deux cas, les données sont tout d'abord mises en cache. Toutefois, étant donné que le but du cache est de jouer le rôle d'une copie très rapide du contenu de certaines parties choisies de la mémoire vive, chaque fois que la valeur d'une donnée change, la nouvelle valeur doit être enregistrée aussi bien dans le cache que dans la mémoire vive. Dans le cas contraire, les données mises en cache et celles stockées dans la mémoire vive ne seraient plus identiques.

Les deux approches diffèrent au niveau de la manière selon laquelle elles effectuent cette opération. Selon une approche de mise en cache dite *write-through* (ou en double écriture), l'écriture des données modifiées se fait immédiatement dans la mémoire vive. Selon l'autre approche de mise en cache dite *Write-back* (ou réécriture), l'écriture des données modifiées dans la mémoire vive est en revanche différée. Cette méthode permet de réduire la fréquence selon laquelle les opérations de réécriture en mémoire vive devront être effectuées pour mettre à jour les données fréquemment modifiées.

Un cache en double-écriture étant plus facile à implémenter, il représente le choix le plus courant. Un cache en réécriture est d'une implémentation plus complexe ; en plus du stockage des données elles-mêmes, il est nécessaire de maintenir un certain mécanisme capable d'identifier les données mises en cache comme étant des données propres (ou clean, signifiant que les données en cache sont identiques à celles figurant dans la RAM) ou des données sales (ou dirty, indiquant que les données en cache ont été modifiées et que celles de la RAM ne sont par conséquent plus actuelles). Il est également nécessaire de mettre en place un moyen permettant de transférer périodiquement des entrées sales du cache vers la RAM.

4.2.2.1. Niveaux de cache

Les sous-systèmes de cache des ordinateurs modernes peuvent avoir de multiples niveaux ; c'est-à-dire qu'il peut exister plus d'un niveau de cache entre le CPU et la mémoire principale. Les niveaux de cache sont souvent numérotés et les numéros les plus bas représentent généralement les niveaux de cache les plus proches du CPU. De nombreux systèmes ont deux niveaux de cache :

- Le cache de niveau 1 (ou L1), placé directement sur la puce même du CPU et tournant à la même vitesse que ce dernier
- Le cache de niveau 2 (ou L2), souvent partie intégrante du module CPU et tournant aux mêmes vitesses (ou presque) que celles du CPU, qui est généralement un peu plus grand et moins rapide que le cache L1

Certains systèmes (d'habitude les serveurs haute performance) ont aussi un cache de niveau 3 (ou L3) qui fait généralement partie de la carte mère du système. Comme on pourrait s'y attendre, le cache L3 est plus grand (est vraisemblablement plus lent) que le cache L2.

Dans tous les cas, le but de tous les sous-systèmes de cache — qu'ils aient un seul niveau ou des niveaux multiples — est de réduire le temps d'accès moyen à la mémoire vive (RAM).

4.2.3. Mémoire principale — RAM

La mémoire principale (aussi appelée mémoire vive ou RAM de l'anglais Random Access Memory) constitue l'essentiel du stockage électronique présent dans les ordinateurs modernes. Elle est utilisée comme stockage aussi bien pour des données que pour des programmes lors de leur utilisation. La vitesse de la mémoire vive dont la plupart des ordinateurs modernes sont dotés, se situe entre celle de la mémoire cache et celle des disques durs et se rapproche généralement plus de la vitesse du premier que de celle du dernier.

Le fonctionnement de base de la RAM est en fait très simple. Au niveau le plus bas figurent les puces de la RAM — des circuits intégrés qui sont responsables de la "mémorisation." Ces puces sont dotées de quatre types de connexions avec l'extérieur :

- Des connexions électriques (pour faire fonctionner la circuitrie au sein de la puce)
- Les connexions aux données (pour permettre le transfert de données depuis la puce et vers la puce)
- Des connexions de lecture/écriture (pour contrôler si les données doivent être stockées sur la puce, ou au contraire doivent être extraites de cette dernière)
- Des connexions d'adresse (pour déterminer l'endroit dans la puce où les données devraient être lues/écrites)

Ci-après figurent les étapes effectuées pour stocker des données dans la RAM :

1. Les données à stocker sont envoyées aux connexions de données.
2. L'adresse à laquelle les données doivent être stockées est transmise aux connexions d'adresse.
3. La connexion de lecture/écriture est paramétrée sur le mode d'écriture.

L'obtention de données est un processus tout aussi simple :

1. L'adresse des données recherchées est transmise aux connexions d'adresse.
2. La connexion de lecture/écriture est paramétrée sur le mode de lecture.
3. Les données recherchées sont lues à partir des connexions de données.

Ces étapes, qui semblent relativement simples, se déroulent à des vitesses très élevées ; la durée de chacune des étapes se mesure en effet en nanosecondes.

Presque toutes les puces de RAM fabriquées de nos jours sont vendues en tant que *modules*. Chaque module se compose d'un nombre de puces de RAM individuelles reliées à une petite carte à circuit intégré. La présentation mécanique et électrique du module est conforme aux normes de l'industrie informatique si bien que l'achat de mémoire peut se faire auprès d'un vaste éventail de revendeurs.



Remarque

L'avantage principal d'un système utilisant des modules de RAM conformes aux normes de l'industrie informatique se situe au niveau du coût de la mémoire qui a tendance à rester faible puisque le fabricant du système n'est pas la source exclusive pour l'achat de modules.

Bien que la plupart des ordinateurs utilisent des modules de RAM conformes aux normes de l'industrie informatique, il existe tout de même des exceptions. Parmi les plus importantes figurent les ordinateurs portables (et à ce niveau également, un certain degré de normalisation a lieu) et les serveurs de haut niveau. Toutefois, même dans ces cas-là, il est possible que des modules de RAM d'autres fabricants soient disponibles, à condition que le système soit assez populaire et ne soit pas d'une conception complètement nouvelle.

4.2.4. Disques durs

Toutes les technologies examinées jusqu'à présent sont de nature *volatile*. En d'autres termes, toutes les données contenues dans un stockage volatil sont perdues lors d'une mise hors tension.

Les disques durs en revanche, ne sont pas de nature *volatile* — en effet, les données qu'ils contiennent sont conservées même lors d'une mise hors tension. C'est la raison pour laquelle les disques durs occupent une place spéciale dans la gamme des options de stockage. En raison de leur nature non volatile, ils représentent une option idéale en matière de stockage de programmes et de données pour une utilisation à plus long terme. Ceci étant, contrairement à la RAM et à la mémoire cache, il n'est pas possible d'exécuter des programmes directement lorsqu'ils sont stockés sur des disques durs ; ils doivent être lus en mémoire vive avant d'être exécutés.

La vitesse à laquelle les données sont stockées et extraites est également différente de celle caractérisant le cache et la RAM ; la vitesse des disques durs est généralement une mesure de grandeur inférieure à celle des technologies entièrement électroniques utilisées pour le cache ou la RAM. Cette différence de vitesse s'explique essentiellement par la nature électromécanique de ces derniers. Tout transfert de données depuis ou vers un disque dur se déroule selon un processus composé de quatre étapes distinctes. La liste figurant ci-dessous illustre non seulement ces étapes, mais fournit également le temps moyen nécessaire à un disque dur haute performance normal pour effectuer chacune d'elles :

- Déplacement du bras d'accès (5,5 millisecondes)
- Rotation du disque (0,1 millisecondes)
- Lecture/écriture de données par les têtes (0,00014 millisecondes)
- Transfert de données vers/ depuis les composants électroniques du disque (0,003 millisecondes)

Parmi toutes ces étapes, seule la dernière ne dépend pas d'un fonctionnement mécanique quelconque.



Remarque

Nous n'avons couvert ici que certains aspects des disques durs, mais les technologies de stockage disque sont examinées de manière détaillée dans le Chapitre 5. À ce stade, il suffit de garder à l'esprit d'une part qu'il existe une différence de vitesse considérable entre la RAM et les technologies à base de disques et d'autre part, que leur capacité de stockage est souvent plus de 10 fois, voire souvent 100 fois, supérieure à celle de la RAM.

4.2.5. Stockage de sauvegarde hors ligne

Le stockage de sauvegarde hors ligne va encore plus loin que le stockage sur disque dur en termes de capacité (supérieure) et de vitesse (inférieure). À ce niveau en effet, les possibilités ne sont vraiment limitées que par votre capacité à obtenir et à stocker des supports amovibles.

Les technologies utilisées dans ces périphériques peuvent être très variées. Ci-après figurent les types les plus couramment utilisés :

- Bande magnétique
- Disque optique

Il va de soi que le fait d'avoir des supports amovibles rallonge souvent encore plus le temps d'accès, en particulier lorsque les données recherchées ne sont pas chargées sur le périphérique de stockage au moment de la demande. L'utilisation de dispositifs robotisés capables de monter et démonter automatiquement des supports améliore quelque peu la situation, mais les capacités de stockage de tels périphériques demeurent toutefois limitées. Même dans le meilleur des cas, les temps d'accès sont

mesurés en secondes, ce qui est bien plus long que les temps d'accès relativement lents mesurés en millisecondes qui sont typiques des disques durs haute performance.

Après avoir brièvement examiné les différentes technologies de stockage utilisées à l'heure actuelle, il convient maintenant d'aborder les concepts élémentaires de la mémoire virtuelle.

4.3. Concepts élémentaires de la mémoire virtuelle

Alors que la technologie soutenant la construction des différentes technologies de stockage modernes soit vraiment impressionnante, il n'est pas nécessaire que l'administrateur système moyen en connaisse tous les détails. En fait, il suffit de garder à l'esprit un seul point, à savoir :

la RAM n'est jamais assez grande.

Alors que ce truisme puisse au premier abord paraître humoristique, de nombreux concepteurs de systèmes d'exploitation ont passé énormément de temps à essayer de réduire l'impact de ce manque réel de mémoire. Ils y sont parvenus grâce à la *mémoire virtuelle* — une manière d'associer de la RAM à un stockage lent, afin de donner à un système une mémoire vive plus grande que celle effectivement installée.

4.3.1. Mémoire virtuelle expliquée simplement

Commençons avec une application hypothétique. Le code de l'ordinateur composant cette application a une taille de 10000 octets. Il a également besoin de 5000 octets pour le stockage des données et les tampons d'E/S. Dans de telles conditions, l'application ne peut fonctionner que si la RAM dispose d'au moins 15000 octets ; même si sa taille est inférieure de juste un octet, l'application ne pourra pas tourner.

On fait référence à ce besoin de 15000 octets sous le terme d'*espace d'adressage* de l'application. Il correspond au nombre d'adresses uniques nécessaires pour contenir aussi bien l'application que ses données. Dans les tout premiers ordinateurs, la quantité de RAM disponible devait être supérieure à l'espace d'adressage nécessaire pour faire tourner la plus grande application ; dans le cas contraire, l'exécution de l'application était vouée à l'échec et un message d'erreur apparaissait signalant une "quantité de mémoire insuffisante".

Une autre approche connue sous le terme d'*écrasement* (ou *overlaying* en anglais) a essayé de résoudre le problème en permettant aux programmeurs de spécifier les parties de leur application devant être en mémoire à tout moment donné. De la sorte, un code nécessaire une fois seulement pour les tâches d'initialisation pouvait être écrasé (par superposition) par le code utilisé ultérieurement. Alors que ce processus a permis de minimiser l'importance des problèmes liés au manque de mémoire, sa mise en oeuvre était complexe et donnait lieu à de nombreuses erreurs. De plus, ce processus de superposition n'a pas réussi à résoudre le problème du manque de mémoire du système en général lors de l'exploitation (runtime). En d'autres termes, il est possible qu'au niveau de son exécution, un programme aux codes superposés nécessite moins de mémoire qu'un programme qui ne l'est pas ; mais si le système ne dispose pas d'une mémoire suffisante pour le programme aux codes superposés, le résultat final demeure le même, à savoir un message d'erreur signalant une quantité de mémoire insuffisante.

La notion de mémoire virtuelle chamboule quelque peu le concept de l'espace d'adressage d'une application. Au lieu de se concentrer sur la *quantité maximale* nécessaire au bon fonctionnement d'une application, un système doté d'une mémoire virtuelle essaie en permanence d'obtenir une réponse à la question inverse : "quelle est la *quantité minimale* de mémoire nécessaire au bon fonctionnement d'une application ?"

Alors qu'au premier abord, notre application hypothétique semble avoir besoin de 15000 octets pour fonctionner correctement, revenez un instant à nos propos de la Section 4.1 — l'accès à la mémoire a tendance à s'effectuer de manière séquentielle et localisée. Dans de telles conditions, la quantité de mémoire nécessaire pour exécuter l'application à tout moment donné est inférieure à 15000 octets

— et bien souvent largement inférieure. Prenez par exemple, les types d'accès à la mémoire qui sont nécessaires pour exécuter une instruction sur un seul ordinateur :

- La lecture de l'instruction se fait depuis la mémoire.
- Les données dont l'instruction a besoin sont lues depuis la mémoire.
- Une fois l'instruction exécutée, les résultats de cette dernière sont envoyés vers la mémoire pour y être enregistrés.

Le nombre spécifique d'octets nécessaires pour chaque accès à la mémoire varie selon l'architecture du CPU, l'instruction elle-même et le type de données. Toutefois, même si une instruction avait besoin de 100 octets de mémoire pour chaque type d'accès à la mémoire, les 300 octets nécessaires sont bien loin du total de 15000 octets requis pour l'espace d'adressage de l'application. S'il existait un moyen d'effectuer un suivi des besoins en mémoire d'une application lors de son exécution, il serait possible de la faire tourner en utilisant moins de mémoire que la quantité exigée par l'espace d'adressage.

Une question demeure néanmoins :

Si une partie seulement de l'application est en mémoire à un moment donné, où se trouve le reste ?

4.3.2. Mémoire auxiliaire — la pierre angulaire de la mémoire virtuelle

La réponse à cette question est courte : le reste de l'application demeure sur le disque. En d'autres termes, le disque sert de *mémoire auxiliaire* pour la RAM ; un support de stockage plus lent et plus grand servant de "stockage auxiliaire" pour un support plus rapide et plus petit. Au premier abord, une telle situation pourrait entraîner un très grand problème au niveau de la performance — après tout, les disques durs sont tellement plus lents que la RAM.

Cette remarque est certes valable, mais il est tout à fait possible de maximiser les avantages liés au comportement d'accès séquentiel et localisé des applications afin d'éliminer la plupart des implications négatives associées à l'utilisation des disques durs comme mémoire auxiliaire. Pour ce faire, le sous-système de mémoire virtuelle est structuré de telle sorte qu'il essaie de garantir le stockage en mémoire des parties de l'application actuellement requises — ou susceptibles de l'être dans le futur proche — seulement pour la durée pendant laquelle ces dernières sont effectivement nécessaires.

À bien des égards, cette situation est semblable à la relation existant entre le cache et la RAM : la combinaison d'une petite quantité de stockage rapide avec une grande quantité de stockage lent revient en fait à avoir une grande quantité de stockage rapide.

Dans cet état d'esprit, examinons maintenant en détail le processus même.

4.4. Mémoire virtuelle : informations détaillées

Il convient tout d'abord d'examiner un nouveau concept, celui de l'*espace d'adressage virtuel*. Ce dernier correspond à la quantité maximale d'espace d'adressage disponible pour une application. Il varie en fonction de l'architecture du système et du système d'exploitation lui-même. L'espace d'adressage virtuel dépend de l'architecture car c'est elle qui définit la quantité de bits disponibles à des fins d'adressage. L'espace d'adressage virtuel dépend aussi du système d'exploitation car il est possible que la manière selon laquelle il a été implémenté fasse intervenir des limites supplémentaires allant au-delà de celles imposées par l'architecture elle-même.

Le mot "virtuel" dans l'expression espace d'adressage virtuel fait référence au nombre total d'emplacements de mémoire dotés d'une adresse unique qui sont disponibles pour une application mais il *ne fait pas* référence à la quantité de mémoire physique, quelle soit installée dans le système ou dédiée à l'application à tout moment donné.

Dans notre exemple, l'espace d'adressage virtuel de notre application est de 15000 octets.

Afin d'implémenter la mémoire virtuelle, il est nécessaire que le système informatique dispose de matériel spécifique pour la gestion de mémoire. Ce dernier est souvent connu sous l'acronyme *MMU* (de l'anglais Memory Management Unit ou unité de gestion de mémoire). Sans MMU, lorsque le CPU accède à la RAM, les emplacements de cette dernière ne changent jamais — l'adresse mémoire 123 correspond toujours au même emplacement physique au sein de la mémoire vive.

Cependant, avec une MMU, les adresses mémoire font l'objet d'une étape de traduction avant tout accès à la mémoire. Ainsi, l'adresse mémoire 123 se verra peut-être mise en correspondance avec l'adresse physique 82043 à un moment donné et avec l'adresse physique 20468 à un autre. Dans une telle situation néanmoins, le temps de gestion du système nécessaire pour effectuer le suivi individuel de la correspondance entre les adresses virtuelles et les adresses physiques pour des millions d'octets de mémoire serait beaucoup trop long. Ainsi, au lieu de ce processus, la MMU découpe la mémoire vive en *pages* — des sections de mémoire contiguës d'une taille déterminée qui sont traitées par la MMU comme des entités indépendantes.

Effectuer le suivi des pages et des traductions de leurs adresses peut sembler être une étape quelque peu inutile et compliquée. Toutefois, elle représente en fait un élément crucial à l'implémentation de mémoire virtuelle. C'est la raison pour laquelle il est important de prendre l'élément suivant en considération.

Revenant à notre application hypothétique dotée d'un espace d'adressage de 15000 octets, imaginez que la première instruction de l'application accède à des données stockées à l'adresse 12374. Supposez également que notre ordinateur ne dispose que de 12288 octets de RAM physique. Que se passe-t-il lorsque le CPU tente d'accéder à l'adresse 12374 ?

Le processus ayant lieu dans ce cas est appelé *défaut de page*.

4.4.1. Défauts de pages

Un défaut de page correspond à une série d'événements se déroulant lorsqu'un programme essaie d'accéder à des données (ou à un code) qui se trouvent dans son espace d'adressage mais ne sont pas actuellement placées dans la mémoire vive (ou RAM) du système. Le système d'exploitation doit traiter les défauts de pages en permettant, d'une manière ou d'une autre, l'accès à la mémoire des données recherchées afin que le programme puisse continuer ses opérations, comme si le défaut de page ne s'était jamais produit.

Dans le cas de notre application hypothétique, le CPU transmet d'abord l'adresse recherchée (12374) à la MMU. Toutefois, ne disposant d'aucune traduction pour cette adresse, la MMU interrompt le CPU et engendre l'exécution du logiciel appelé gestionnaire de défauts de pages. Ce dernier détermine alors les mesures à prendre pour résoudre le défaut de page en question. À cet égard, il peut :

- Trouver l'emplacement de la page recherchée sur le disque et la lire (c'est généralement le cas si le défaut de page se situe au niveau d'une page de code)
- Confirmer que la page recherchée se trouve déjà dans la mémoire vive (mais n'est pas allouée au processus en cours) et reconfigurer la MMU de manière à ce qu'elle renvoie bien à cette page
- Pointer vers une page spéciale ne contenant rien d'autre que des zéros et allouer ensuite une page au processus seulement si le processus tente d'enregistrer des données sur la page spéciale (on parle alors d'une page *copiée par écriture* ou copy on write ; cette technique est souvent utilisée pour des pages de données initialisées avec des zéros)
- Obtenir la page souhaitée depuis un autre emplacement (un point que nous traiterons ultérieurement de manière plus détaillée)

Alors que les trois premières mesures sont relativement simples, la dernière elle, ne l'est pas du tout. Pour bien comprendre ce dernier point, il est nécessaire d'aborder d'autres sujets.

4.4.2. Jeu de pages de travail

L'ensemble des pages de mémoire physique actuellement dédiées à un processus spécifique est connu sous le terme de *jeu de pages de travail* (ou *working set*) de ce processus. Le nombre de pages faisant partie de ce jeu de pages de travail peut augmenter ou diminuer selon la quantité globale de pages disponibles sur l'ensemble du système.

La taille du jeu de pages de travail augmente lorsqu'une page du processus fait défaut. En revanche sa taille diminue au fur et à mesure que le nombre des pages libres baisse. Afin d'éviter d'être complètement à cours de mémoire, il est nécessaire de retirer des pages des jeux de pages de travail des processus et de les transformer en pages libres qui pourront être utilisées ultérieurement. Le système d'exploitation réduit les jeux de pages de travail des processus de plusieurs manières :

- En enregistrant des pages modifiées dans un endroit particulier du périphérique de stockage de masse (auquel on fait généralement référence sous le terme d'espace d'*échange* ou de *pagination*, parfois aussi appelé *swapping* ou *paging space*)
- En identifiant des pages non modifiées comme étant des pages libres (il n'est pas nécessaire d'enregistrer ces pages sur un disque étant donné qu'elles n'ont pas été modifiées)

Afin de déterminer des jeux de pages de travail pour tous les processus, le système d'exploitation doit effectuer un suivi des informations relatives à l'utilisation de toutes les pages. De cette manière, il est à même de déterminer les pages précises qui sont activement utilisées (et doivent donc demeurer en mémoire) et celles qui ne le sont pas (et peuvent par conséquent être supprimées de la mémoire). Dans la plupart des cas, un genre d'algorithme basé sur les pages utilisées le moins récemment permet de déterminer les pages spécifiques pouvant être supprimées des jeux de pages de travail des processus.

4.4.3. Échange (ou swapping)

Alors que l'échange ou *swapping* (c'est-à-dire l'écriture de pages modifiées dans l'espace de pagination du système) fait partie des opérations normales d'un système, il est possible que le *swapping* devienne trop important. Il est important de prêter une attention toute particulière à un *swapping* excessif car la situation décrite ci-dessous peut facilement se produire de façon répétée :

- Des pages d'un processus sont échangées
- Le processus est en mesure d'être exécuté et tente d'accéder à une page échangée
- La page est remise en mémoire (forçant probablement le déchargement des pages d'autres processus)
- Un peu plus tard cette page est échangée à nouveau

Si cette série d'événements est généralisée (on parle alors d'écroulement ou de *thrashing*), elle indique que la quantité de mémoire vive est insuffisante pour faire face à la charge de travail actuelle. L'écroulement a un impact extrêmement négatif sur la performance du système dans la mesure où le CPU et les charges d'E/S qui peuvent résulter d'une telle situation dépassent rapidement la charge imposée par le travail réel d'un système. Dans des cas extrêmes, il est possible que le système n'effectue aucun travail utile et monopolise toutes ses ressources pour le déplacement de pages de et vers la mémoire.

4.5. Implications de la mémoire virtuelle au niveau de la performance

Alors que la mémoire virtuelle permet aux ordinateurs de traiter plus facilement des applications plus grandes et plus complexes, il faut — comme c'est le cas avec tout outil puissant — en payer le prix. Dans le cas présent, le prix à payer se situe au niveau de la performance — un système d'exploitation

doté d'une mémoire virtuelle effectue beaucoup plus de tâches qu'un système d'exploitation ne pouvant pas prendre en charge de mémoire virtuelle. Ainsi, en recourant à la mémoire virtuelle, la performance n'est jamais aussi bonne que lorsque l'application est stockée à 100% en mémoire.

Toutefois, il n'y a pas lieu de baisser les bras et d'abandonner. Les avantages liés à la mémoire virtuelle sont trop grands pour agir de la sorte. De plus, avec un peu d'effort, il est possible d'obtenir une bonne performance. Dans ce contexte, il est important d'examiner les ressources du système sur lesquelles se fait ressentir l'impact d'une utilisation importante du sous-système de mémoire.

4.5.1. Pire scénario de performance

Avec les connaissances que vous avez acquises dans ce chapitre, examinez pour un instant les ressources du système qui sont utilisées pour de très lourdes activités de défaut de page et de swapping :

- Mémoire vive ou RAM — Il va de soi que la quantité de mémoire vive est faible (sinon, il ne serait pas nécessaire d'effectuer des opérations de défaut de page ou d'échange de pages)
- Disque — Alors qu'aucun impact ne sera peut-être ressenti au niveau du disque, la largeur de bande des E/S (en raison d'une pagination et d'un échange de pages importants) sera elle, affectée.
- CPU — Le CPU rallonge le cycle effectuant le traitement requis pour prendre en charge la gestion de mémoire et établir les opérations d'E/S nécessaires pour la pagination et l'échange de pages (swapping).

Étant donné l'interdépendance de ces charges, il est facile de comprendre comment un manque de ressources peut entraîner de graves problèmes de performance.

Pour se trouver dans une telle situation, il suffit d'un système doté d'une mémoire vive trop petite, d'une activité de défaut de page intense et d'un système tournant quasiment à capacité en termes de CPU ou d'E/S de disque. À ce stade, le système effectue des opérations d'écroulement (ou thrashing) entraînant inévitablement une réduction de performance.

4.5.2. Meilleur scénario de performance

Dans le meilleur des cas, le temps de gestion système résultant de la prise en charge de mémoire virtuelle se traduit, dans un système bien configuré, par une faible charge supplémentaire :

- Mémoire vive ou RAM — Suffisamment de mémoire vive pour tous les jeux de pages de travail et suffisamment de mémoire libre pour traiter tout défaut de page²
- Disque — En raison d'une activité de défaut de page limitée, l'impact sur la largeur de bande des E/S de disque ne serait que minimal
- CPU — La majorité des cycles CPU se concentrent sur l'exécution même des applications, plutôt que sur l'exécution du code de gestion mémoire du système d'exploitation

Dans de telles circonstances, il est important de se rappeler que l'impact de la mémoire virtuelle sur la performance est minimal, lorsqu'elle est utilisée aussi peu que possible. En d'autres termes, l'élément vital pour obtenir une bonne performance du sous-système de mémoire virtuelle est une quantité de mémoire vive (ou RAM) suffisante.

Également d'une extrême importance (bien que moindre dans notre contexte) sont des capacités suffisantes en matière d'E/S disque et de CPU. Rappelez-vous toutefois que ces ressources aident seulement la performance du système à dégrader plus progressivement lors d'activités importantes de défaut de page et de swapping ; elles n'apportent pas vraiment d'aide en ce qui concerne la performance

2. Un système relativement actif doit *toujours* effectuer une certaine activité de défaut de page en raison des défauts de page engendrés par des applications récemment lancées et mises en mémoire.

du sous-système de mémoire virtuelle (bien qu'elles jouent évidemment un rôle important au niveau de la performance du système en général).

4.6. Informations spécifiques à Red Hat Enterprise Linux

En raison de la complexité inhérente à un système d'exploitation doté d'une mémoire virtuelle paginée à la demande, le contrôle des ressources associées à la mémoire peut être quelque peu déroutant sous Red Hat Enterprise Linux. Il est par conséquent préférable de commencer avec les outils simples et d'avancer progressivement.

À l'aide de la commande `free`, il est possible d'obtenir un aperçu concis (bien qu'élémentaire) de l'utilisation de la mémoire et du swap, comme le montre l'extrait ci-dessous :

```

                total      used      free      shared    buffers    cached
Mem:           1288720    361448    927272         0       27844    187632
-/+ buffers/cache:    145972    1142748
Swap:           522104         0      522104

```

Notez que ce système ne dispose que de 1,2 Go de mémoire vive (RAM) dont seulement 350 Mo sont réellement utilisés. Comme on peut le supposer avec un système doté d'une telle quantité de RAM libre, aucune partie des 500 Mo de la partition swap n'est utilisée.

Comparez maintenant l'exemple ci-dessus avec celui qui suit :

```

                total      used      free      shared    buffers    cached
Mem:           255088    246604     8484         0       6492    111320
-/+ buffers/cache:    128792    126296
Swap:           530136    111308    418828

```

Ce système dispose d'environ 256 Mo de RAM dont la majorité est utilisée, ne laissant qu'environ 8 Mo de libre. Plus de 100 Mo des 512 Mo de la partition swap sont utilisés. Bien que le système en question soit certainement plus limité en termes de mémoire que le système de notre premier exemple, il est nécessaire d'examiner la situation plus en profondeur afin de déterminer si la limitation de mémoire entraîne des problèmes de performance.

Bien que la commande `vmstat` soit plus énigmatique que `free`, elle a l'avantage de fournir plus d'informations que les seules statistiques sur l'utilisation de la mémoire. Ci-après figure la sortie de la commande `vmstat 1 10` :

```

procs          memory      swap          io          system          cpu
r  b  w  swpd  free  buff  cache  si  so  bi  bo  in  cs  us  sy  id
2  0  0  111304  9728  7036  107204  0  0  6  10  120  24  10  2  89
2  0  0  111304  9728  7036  107204  0  0  0  0  526  1653  96  4  0
1  0  0  111304  9616  7036  107204  0  0  0  0  552  2219  94  5  1
1  0  0  111304  9616  7036  107204  0  0  0  0  624  699  98  2  0
2  0  0  111304  9616  7052  107204  0  0  0  48  603  1466  95  5  0
3  0  0  111304  9620  7052  107204  0  0  0  0  768  932  90  4  6
3  0  0  111304  9440  7076  107360  92  0  244  0  820  1230  85  9  6
2  0  0  111304  9276  7076  107368  0  0  0  0  832  1060  87  6  7
3  0  0  111304  9624  7092  107372  0  0  16  0  813  1655  93  5  2
2  0  2  111304  9624  7108  107372  0  0  0  972  1189  1165  68  9  23

```

Dans cet extrait de 10 secondes, la quantité de mémoire libre (le champ `free`) change quelque peu et il y a une certaine activité d'E/S associée au swap (les champs `si` et `so`), mais d'une manière générale,

ce système fonctionne bien. Ceci étant, il est difficile de connaître l'importance de la charge de travail supplémentaire que le système pourrait accepter, étant donné l'utilisation actuelle de mémoire.

Lors de toute recherche de problème en relation avec la mémoire, il est souvent nécessaire de déterminer comment le sous-système de mémoire virtuelle de Red Hat Enterprise Linux utilise la mémoire du système. À l'aide de la commande `sar`, il est possible d'examiner cet aspect de la performance du système de manière plus détaillée.

En parcourant le rapport `sar -r` suivant, il est possible d'examiner en détail l'utilisation de la mémoire et du swap :

```
Linux 2.4.20-1.1931.2.231.2.10.ent (pigdog.example.com) 07/22/2003

12:00:01 AM kbmemfree kbmemused %memused kbmemshrd kbbuffers kbcached
12:10:00 AM 240468 1048252 81.34 0 133724 485772
12:20:00 AM 240508 1048212 81.34 0 134172 485600
...
08:40:00 PM 934132 354588 27.51 0 26080 185364
Average: 324346 964374 74.83 0 96072 467559
```

Les champs `kbmemfree` et `kbmemused` fournissent des statistiques typiques sur la mémoire libre et la mémoire utilisée, le pourcentage de la mémoire utilisée apparaissant dans le champ `%memused`. Les champs `kbbuffers` et `kbcached` quant à eux indiquent la quantité de kilo-octets de mémoire allouée aux tampons (ou buffers) et au cache de données de tout le système.

Le champ `kbmemshrd` affiche toujours un zéro pour des systèmes (tels que Red Hat Enterprise Linux) utilisant un noyau Linux 2.4.

Notez que les lignes de ce rapport ont été tronquées afin de tenir sur la page. Ci-après figure la partie restante de chaque ligne à laquelle l'horodatage a été ajouté, afin de faciliter la lecture :

```
12:00:01 AM kbswpfree kbswpused %swpused
12:10:00 AM 522104 0 0.00
12:20:00 AM 522104 0 0.00
...
08:40:00 PM 522104 0 0.00
Average: 522104 0 0.00
```

Pour l'utilisation du swap, les champs `kbswpfree` et `kbswpused` précisent en kilo-octets la quantité d'espace swap libre et utilisé, le champ `%swpused` lui, exprimant en pourcentage la quantité d'espace swap utilisé.

Pour en savoir plus sur l'activité d'échange de mémoire (ou swapping) se produisant, consultez le rapport `sar -w` dont un exemple figure ci-après :

```
Linux 2.4.20-1.1931.2.231.2.10.entsmp (raptor.example.com) 07/22/2003

12:00:01 AM pswpin/s pswpout/s
12:10:01 AM 0.15 2.56
12:20:00 AM 0.00 0.00
...
03:30:01 PM 0.42 2.56
Average: 0.11 0.37
```

Comme vous pouvez le remarquer, il y avait trois fois moins de pages provenant de swap (`pswpin/s`) qu'il n'y en avait allant vers swap (`pswpout/s`).

Pour mieux comprendre comment les pages sont utilisées, reportez-vous au rapport `sar -B` suivant :

```
Linux 2.4.20-1.1931.2.231.2.10.entsmp (raptor.example.com) 07/22/2003
```

```
12:00:01 AM ppggin/s ppggout/s activepg inadtypg inaclnpg inatargp
12:10:00 AM 0.03 8.61 195393 20654 30352 49279
12:20:00 AM 0.01 7.51 195385 20655 30336 49275
...
08:40:00 PM 0.00 7.79 71236 1371 6760 15873
Average: 201.54 201.54 169367 18999 35146 44702
```

Il est possible de déterminer ici le nombre de blocs paginés en mémoire par seconde depuis le disque (*ppggin/s*) et celui des blocs paginés sur le disque depuis la mémoire (*ppggout/s*). Ces statistiques sont utilisées comme baromètre de l'activité globale de la mémoire virtuelle.

Toutefois, il est possible d'obtenir plus d'informations en examinant les autres champs de ce rapport. Le noyau de Red Hat Enterprise Linux identifie toutes les pages comme étant soit actives, soit inactives. Comme le nom l'indique, des pages actives sont d'une manière ou d'une autre en cours d'utilisation (en temps que pages de processus ou tampon par exemple) alors que des pages inactives ne le sont pas. Notre exemple de rapport montre que la liste des pages actives (le champ *activepg*) est en moyenne de 660 Mo³.

Les autres champs figurant dans ce rapport se concentrent sur la liste des pages inactives — des pages qui pour une raison ou une autre n'ont pas été récemment utilisées. Le champ *inadtypg* indique le nombre de pages inactives qui sont *sales* (ou dirty, c'est-à-dire qui ont été modifiées) et peuvent être enregistrées sur le disque. Le champ *inaclnpg* d'autre part, spécifie le nombre de pages inactives qui sont *propres* (ou clean, c'est-à-dire qui n'ont pas été modifiées) et ne doivent par conséquent pas être enregistrées sur disque.

Le champ *inatargp* indique la taille souhaitée de la liste des pages inactives. Cette valeur, calculée par le noyau Linux, est déterminée de sorte que la liste des pages inactives demeure suffisamment grande pour servir de réserve en cas de remplacement de pages.

Pour obtenir des informations supplémentaires sur l'état (et plus particulièrement sur la fréquence à laquelle les pages changent d'état), consultez le rapport *sar -R* dont un exemple figure ci-après :

```
Linux 2.4.20-1.1931.2.231.2.10.entsmp (raptor.example.com) 07/22/2003
```

```
12:00:01 AM frmpg/s shmpg/s bufpg/s campg/s
12:10:00 AM -0.10 0.00 0.12 -0.07
12:20:00 AM 0.02 0.00 0.19 -0.07
...
08:50:01 PM -3.19 0.00 0.46 0.81
Average: 0.01 0.00 -0.00 -0.00
```

Les statistiques apparaissant dans le rapport *sar* ci-dessus sont uniques dans le sens où les valeurs sont positives, négatives ou équivalentes à zéro. Lorsque la valeur est positive, elle indique le taux selon lequel des pages de ce type augmentent. Lorsqu'elle est négative, elle indique le taux selon lequel des pages de ce type diminuent. Finalement, une valeur de zéro indique que des pages de ce type n'augmentent ni ne diminuent.

Dans cet exemple, le dernier échantillon montre qu'une quantité légèrement supérieure à trois pages par seconde est allouée dans la liste des pages libres (le champ *frmpg/s*) et que presque une page par seconde est ajoutée au cache de pages (le champ *campg/s*). La liste des pages utilisées comme tampons (le champ *bufpg/s*) a augmenté d'environ une page toutes les deux secondes, alors que la liste des pages de mémoire partagée (le champ *shmpg/s*) n'a elle, ni augmenté, ni diminué en nombre.

3. Sous Red Hat Enterprise Linux sur le système x86 qui est utilisé dans cet exemple, la taille de la page est de 4096 octets. Il est fort possible que des systèmes basés sur d'autres architectures aient des tailles de pages différentes.

4.7. Ressources supplémentaires

Cette section inclut un certain nombre de ressources pouvant être utilisées pour approfondir vos connaissances sur le contrôle des ressources et sur des sujets spécifiques à Red Hat Enterprise Linux qui ont été abordés dans ce chapitre.

4.7.1. Documentation installée

Les ressources suivantes sont installées lors d'une installation normale de Red Hat Enterprise Linux et peuvent vous aider à acquérir des connaissances plus étendues sur les sujets abordés dans ce chapitre.

- Page de manuel de `free(1)` — Pour apprendre comment afficher des statistiques sur la mémoire libre et sur la mémoire utilisée.
- Page de manuel de `vmstat(8)` — Pour apprendre comment afficher un aperçu concis de l'utilisation des processus, de la mémoire, du swap, des E/S, du système et du CPU.
- Page de manuel de `sar(1)` — Pour apprendre comment créer des rapports sur l'utilisation des ressources du système.
- Page de manuel de `sa2(8)` — Pour apprendre comment crée des fichiers de rapports quotidiens sur l'utilisation des ressources du système.

4.7.2. Sites Web utiles

- http://people.redhat.com/alikins/system_tuning.html — Informations sur le réglage de la performance pour les utilisateurs de Linux. Une approche peu conventionnelle des réglages de la performance et du contrôle des ressources pour des serveurs.
- <http://www.linuxjournal.com/article.php?sid=2396> — Outils de contrôle de la performance pour Linux. Cette page du Linux Journal s'adresse plus à l'administrateur souhaitant écrire une solution personnalisée sous forme de graphiques de performance. Cette page datant d'il y a quelques années, il est fort possible que certaines des informations ne soient plus courantes, mais l'idée et l'exécution générales n'en demeurent pas moins valables.

4.7.3. Livres sur le sujet

Les ressources suivantes traitent de différents sujets en relation avec le contrôle des ressources et constituent de bonnes sources d'informations pour les administrateurs de systèmes Red Hat Enterprise Linux:

- *Guide d'administration système de Red Hat Enterprise Linux* ; Red Hat, Inc. — Inclut un chapitre sur de nombreux outils de contrôle des ressources abordés dans ce guide.
- *Linux Performance Tuning and Capacity Planning* de Jason R. Fink et Matthew D. Sherer ; Sams — Fournit un horizon plus détaillé des outils de contrôle des ressources examinés dans ce guide et en inclut d'autres qui pourraient être appropriés pour des besoins plus spécifiques lors du contrôle des ressources.
- *Red Hat Linux Security and Optimization* de Mohammed J. Kabir ; Red Hat Press — Les 150 premières pages de ce livre examinent les problèmes liés à la performance et comptent des chapitres consacrés aux problèmes de performance rencontrés en particulier au niveau du réseau, du Web, de la messagerie et des serveurs de fichiers.
- *Linux Administration Handbook* de Evi Nemeth, Garth Snyder et Trent R. Hein ; Prentice Hall — Fournit un petit chapitre d'une portée semblable à celle de ce guide, mais inclut également

une section intéressante sur la manière d'effectuer un diagnostic d'un système qui a soudainement ralenti.

- *Linux System Administration : A User's Guide* de Marcel Gagne ; Addison Wesley Professional — Contient un petit chapitre sur le réglage et le contrôle de la performance.
- *Essential System Administration* (3ème Édition) de Aeleen Frisch ; O'Reilly & Associates — Ce chapitre sur la gestion des ressources du système contient de bonnes informations générales, y compris certains aspects spécifiques à Linux.
- *System Performance Tuning* (2ème Édition) de Gian-Paolo D. Musumeci et Mike Loukides ; O'Reilly & Associates — Bien que l'accent soit mis essentiellement sur des implémentations UNIX plus traditionnelles, ce livre inclut néanmoins de nombreuses références spécifiques à Linux.

Chapitre 5.

Gestion du stockage

S'il y a un aspect du travail de l'administrateur système qui monopolise la plupart de son temps, c'est bien la gestion du stockage. On a l'impression que les disques sont toujours à cours de mémoire, qu'ils sont surchargés par une activité d'entrée sorties trop intense ou qu'ils tombent en panne de façon inattendue. Ainsi, pour être un bon administrateur système, il est primordial de disposer de solides connaissances en matière de stockage disque.

5.1. Bref aperçu du matériel de stockage

Avant de pouvoir gérer le stockage, il est essentiel de comprendre le matériel sur lequel les données sont stockées. À moins que vous ne disposiez d'un minimum de connaissances sur le fonctionnement des périphériques de stockage de masse, vous courez le risque de vous trouver un jour dans une situation où vous devrez faire face à un problème lié au stockage mais ne disposerez malheureusement pas des connaissances de base nécessaires pour interpréter le problème en question. En acquérant une compréhension élémentaire du fonctionnement du matériel sous-jacent, vous devriez être en mesure de déterminer plus facilement si le sous-système de stockage de votre ordinateur fonctionnent correctement.

La grande majorité des périphériques de stockage de masse utilisent un support rotatif d'un type ou d'un autre et prennent en charge l'accès aléatoire aux données sur ce support. Ainsi, les composants suivants seront présents sous une forme ou sous une autre, dans presque tous les périphériques de stockage de masse :

- Plateau de disque
- Périphérique de lecture/écriture des données
- Bras d'accès

Les sections suivantes examinent en détail chacun de ces composants.

5.1.1. Plateaux de disque

Les supports rotatifs utilisés par presque tous les périphériques de stockage se présentent sous la forme d'un ou plusieurs plateaux plats et ronds. Le plateau peut être composé de matériaux très variés, tels que l'aluminium, le verre et le polycarbonate.

La surface de chaque plateau est traitée de telle sorte qu'elle puisse permettre le stockage de données. La nature exacte du traitement dépend de la technologie de stockage de données utilisée. La technologie de stockage de données la plus courante repose sur la propriété du magnétisme ; dans ce cas, les plateaux sont couverts d'un composé montrant de bonnes caractéristiques magnétiques.

Une autre technologie courante de stockage de données repose sur des principes optiques ; dans ces cas-là, les plateaux sont couverts de matériaux dont les propriétés optiques peuvent être modifiées, permettant par là-même le stockage de données de manière optique¹.

Indépendamment du type de technologie de stockage de données utilisée, les plateaux de disque tournent, permettant à la totalité de leur surface de passer à proximité d'un autre composant — le périphérique de lecture/écriture des données.

1. Certains périphériques optiques — particulièrement les lecteurs des CD-ROM — ont recours à des approches quelque peu différentes en matière de stockage de données ; ces différences seront soulignées plus tard dans ce chapitre, lorsque les sujets y faisant référence seront abordés.

5.1.2. Périphérique de lecture/écriture des données

Le périphérique de lecture/écriture des données est le composant qui prend les bits et octets qu'un système informatique utilise pour son fonctionnement et les convertit ensuite en variations magnétiques ou optiques nécessaires pour interagir avec les matériaux recouvrant la surface des plateaux de disque.

Parfois, les conditions dans lesquelles ces périphériques doivent fonctionner relèvent du défi. Dans le cas du stockage de masse effectué de manière magnétique par exemple, les périphériques de lecture/écriture (appelés *têtes*) doivent être positionnés très près de la surface du plateau. Toutefois, si la tête et la surface du plateau de disque venaient à entrer en contact, la friction produite endommagerait très sérieusement aussi bien la tête que le plateau. En conséquence, la surface de la tête et celle du plateau sont minutieusement polies, permettant à la tête d'utiliser un coussin l'air générée par la rotation des plateaux pour rester juste au-dessus de la surface du plateau sans le toucher, "survolant" ainsi ce dernier à une altitude inférieure à l'épaisseur d'un cheveu. C'est d'ailleurs la raison pour laquelle les disques durs risquent être endommagés par les chocs, les changements soudains de température et toute contamination transmissible par l'air.

Les défis auxquels les têtes optiques doivent faire face sont quelque peu différents de ceux auxquels les têtes magnétiques sont confrontées — dans le cas des têtes optiques, l'assemblage de la tête doit rester à une distance relativement constante par rapport à la surface du plateau, sinon, les lentilles utilisées pour la mise au point sur le plateau ne produiront pas une image d'une qualité suffisante.

Ceci dit, pour le stockage de données, les têtes utilisent dans les deux cas une toute petite partie de la surface du plateau. Lors de la rotation de ce dernier sous les têtes, la surface se transforme en un cercle concentrique très fin.

Si telle était vraiment le fonctionnement des périphériques de stockage de masse, 99% de la surface du plateau serait gaspillée. Certes des têtes supplémentaires pourraient être installées, mais pour pouvoir utiliser toute la surface du plateau, des milliers de têtes seraient nécessaires. Une approche plus pratique consiste donc à déplacer la tête sur la surface du plateau.

5.1.3. Bras d'accès

En utilisant une tête montée sur un bras capable de balayer toute la surface du plateau, il est possible d'utiliser le plateau entièrement pour le stockage de données. Toutefois, le bras d'accès doit pouvoir faire deux choses :

- Bouger avec une grande rapidité
- Bouger avec une grande précision

Le bras d'accès doit se déplacer aussi rapidement que possible, car le temps nécessaire à son déplacement d'un point à un autre est du temps de perdu. En effet, aucune donnée ne peut être lue tant que le bras d'accès n'est pas immobile².

Le bras d'accès doit pouvoir se déplacer avec une grande précision parce que, comme nous l'avons mentionné précédemment, la superficie utilisée par la tête est infime. Par conséquent, afin d'utiliser la capacité de stockage du plateau de manière efficace, il est nécessaire de pouvoir déplacer la tête juste assez pour s'assurer que toute donnée enregistrée au nouvel emplacement n'écrase pas les données écrites juste avant. À un niveau conceptuel, ce processus divise la surface du plateau en une ou plusieurs centaines "d'anneaux" ou *pistes*. Le déplacement du bras d'accès d'une piste à une autre est

2. Dans certains périphériques optiques (tels que les lecteurs de CD-ROM) le bras d'accès bouge en permanence si bien que l'assemblage de la tête effectue un déplacement en spirale au-dessus de la surface du plateau. Ce point représente une différence fondamentale au niveau de l'utilisation du support de stockage et reflète les origines du CD-ROM en tant que support de stockage pour la musique, où la recherche continue de l'information est une opération plus commune que la recherche d'un point particulier où se trouve des données.

souvent appelé processus de *recherche* et on fait référence à la durée nécessaire au bras d'accès pour passer d'une piste à une autre sous le terme de *temps de recherche*.

Lorsqu'il y a plusieurs plateaux (ou un seul plateau utilisant les deux faces pour le stockage de données), les bras des deux côtés sont montés de manière solidaire, permettant ainsi l'accès simultané à chaque piste sur chaque plateau. Si on pouvait visualiser les pistes de chaque face avec un accès fixe au-dessus d'une piste donnée, elles apparaîtraient comme étant empilées les unes au-dessus des autres, formant une sorte de cylindre ; c'est la raison pour laquelle l'ensemble des pistes accessibles depuis un emplacement précis des bras d'accès porte le nom de *cylindre*.

5.2. Concepts d'adressage en matière de stockage

La configuration de plateaux de disque, têtes et bras d'accès permet de positionner la tête à un endroit quelconque sur la surface quelconque d'un plateau quelconque appartenant au périphérique de stockage de masse. Ceci n'est néanmoins pas suffisant ; afin de pouvoir utiliser la capacité de stockage, il est nécessaire de disposer d'une méthode permettant de donner des adresses à des parties d'une taille uniforme, faisant partie du stockage disponible.

Mais ce n'est pas tout. Un dernier aspect est encore nécessaire pour que ce processus fonctionne bien. Prenez toutes les pistes des nombreux cylindres présents dans un périphérique de stockage de masse typique. Étant donné que les pistes ont des diamètres différents, leur circonférence varie en conséquence. Ainsi, si le stockage recevait une adresse seulement au niveau de la piste, chaque piste contiendrait des quantités différentes de données — la piste #0 (se trouvant vers le centre du plateau) contiendrait peut-être 10,827 octets, alors que la piste #1,258 elle (se trouvant proche de la bordure extérieure du plateau) contiendrait peut-être 15,382 octets.

La solution consiste à subdiviser chaque piste en *secteurs* ou *blocs* de segments de stockage de taille homogène (souvent 512 octets). De cette manière, chaque piste contient un nombre fixe³ de secteurs.

Une conséquence secondaire de cette approche est que chaque piste contient de l'espace inutilisé — l'espace entre les secteurs. Malgré le nombre constant de secteurs sur chaque piste, la quantité d'espace inutilisé varie — relativement peu d'espace inutilisé sur les pistes au centre du plateau contre beaucoup d'espace inutilisé sur les pistes se trouvant en bordure du plateau. Dans les deux cas, l'espace inutilisé représente une perte d'espace dans la mesure où aucune donnée ne peut y être stockée.

Toutefois, l'avantage de cette approche faisant de l'espace perdu un sacrifice acceptable, est que l'adressage efficace du stockage sur un périphérique de stockage de masse est désormais possible. En fait, il existe deux méthodes d'adressage — l'une basée sur la géométrie et l'autre sur les blocs.

5.2.1. Adressage basé sur la géométrie

Le terme d'*adressage basé sur la géométrie* fait référence au fait que les périphériques de stockage de masse stockent effectivement les données à un endroit physique bien spécifique sur le support de stockage. Dans le cas des périphériques décrits ici, ce terme fait référence à trois éléments définissant un point spécifique sur les plateaux de disque des périphériques :

- Cylindre
- Tête

3. Alors que les premiers périphériques de stockage de masse utilisaient le même nombre de secteurs pour chaque piste, les périphériques plus récents divisent la gamme de cylindres en "zones" différentes, chacune d'elles ayant un nombre de secteurs différents par piste. Cette approche est utilisée afin d'exploiter l'espace supplémentaire entre les secteurs des cylindres extérieurs où l'espace inutilisé entre les secteurs est plus grand

- Secteur

La section suivante décrit la manière selon laquelle une adresse hypothétique peut renvoyer à un emplacement physique précis sur le support de stockage.

5.2.1.1. Cylindre

Comme nous l'avons mentionné précédemment, le cylindre indique un emplacement spécifique où le bras d'accès se positionne (et par conséquent, les têtes de lecture/écriture). En spécifiant un cylindre particulier, on fait abstraction de tous les autres cylindres, réduisant ainsi notre recherche à seulement une piste sur chaque surface du périphérique de stockage de masse.

Cylindre	Tête	Secteur
1014	X	X

Tableau 5-1. Adressage du stockage

Dans le Tableau 5-1, la première partie de l'adresse basée sur la géométrie du disque a été complétée. Deux éléments de cette adresse — la tête et le secteur — n'ont pas encore été définis.

5.2.1.2. Tête

Bien qu'au sens strict nous choissions un plateau de disque précis, il est plus simple de concevoir le processus en tant qu'interaction avec une tête particulière, étant donné que chaque surface a une tête de lecture/écriture qui lui est propre. En fait, les composants électroniques sous-jacents du périphérique sélectionnent une tête et — dé-sélectionnant les autres — interagissent seulement avec la tête choisie pour toute la durée des opérations d'E/S. Toutes les autres pistes qui constituent le cylindre actuel ne sont alors plus prises en compte.

Cylindre	Tête	Secteur
1014	2	X

Tableau 5-2. Adressage du stockage

Dans le Tableau 5-2, les deux premiers éléments constituant une adresse basée sur la géométrie du disque ont été complétés. Un dernier élément de cette adresse — le secteur — reste encore à être défini.

5.2.1.3. Secteur

En précisant un secteur particulier, nous avons terminé l'adressage et avons identifié de manière unique le bloc de données choisi.

Cylindre	Tête	Secteur
1014	2	12

Tableau 5-3. Adressage du stockage

Dans le Tableau 5-3, la totalité de l'adresse basée sur la géographie a été définie. L'adresse identifie l'emplacement d'un bloc précis parmi les autres blocs figurant sur le périphérique.

5.2.1.4. Problèmes liés à l'adressage basé sur la géométrie du disque

Alors que l'adressage basé sur la géométrie est relativement simple, il existe toutefois un domaine ambigu qui est source de problèmes. Cette ambiguïté réside dans le numérotage des cylindres, des têtes et des secteurs.

Chaque adresse établie en fonction de la géométrie du disque identifie certes de manière unique un bloc spécifique de données, mais cette méthode n'est applicable que si le système de numérotage des cylindres, des têtes et des secteurs ne change pas. Si le système de numérotage change (comme lors du changement de matériel ou de logiciels interagissant avec le périphérique de stockage), le mappage entre les adresses basées sur la géométrie et les blocs de données leur correspondant peut lui aussi changer, rendant ainsi impossible l'accès aux données souhaitées.

En raison de ce potentiel d'ambiguïté, une approche différente a été développée pour l'adressage. Cette dernière est traitée en détail dans la section suivante.

5.2.2. Adressage basé sur les blocs

L'*adressage basé sur les blocs* est beaucoup plus simple que l'adressage basé sur la géométrie du disque. Avec l'adressage basé sur les blocs, chaque bloc de données se voit attribuer un numéro unique. Ce numéro est passé de l'ordinateur au périphérique de stockage de masse qui lui, effectue de manière interne la conversion en une adresse basée sur la géométrie, dont la circuiterie de contrôle du périphérique a besoin.

Étant donné que la conversion en une adresse basée sur la géométrie est toujours effectuée par le périphérique lui-même, elle est toujours homogène, éliminant ainsi les problèmes survenant lorsque l'adressage du périphérique basé sur la géométrie est donné.

5.3. Interfaces des périphériques de stockage de masse

Tout périphérique utilisé dans un système informatique doit être relié d'une manière ou d'une autre à ce système informatique. On fait référence à ce point d'interconnexion sous le terme d'*interface*. Il en va de même des périphériques de stockage de masse — ils sont eux aussi considérés comme des interfaces. Il est importants de disposer d'un minimum de connaissances sur les interfaces pour deux raisons essentielles :

- Il existe de nombreuses interfaces différentes (généralement incompatibles)
- Les performances et caractéristiques au niveau des prix varient selon les types d'interfaces

Malheureusement, il n'existe ni interface de périphérique universelle, ni interface de périphérique de stockage de masse unique. Dans de telles circonstances, il est important que les administrateurs système connaissent l'interface ou les interfaces prise(s) en charge par les systèmes de leur entreprise. Sinon, il existe un risque réel d'acheter le mauvais matériel lors de la planification de la mise à niveau d'un système.

Les capacités au niveau des performances variant elles aussi en fonction des types d'interfaces, certaines d'entre elles sont plus appropriées que d'autres dans certains environnements. Par exemple, les interfaces à même de prendre en charge des périphériques rapides sont parfaitement appropriées pour des environnements serveur, alors que des interfaces lentes sont elles tout à fait suffisantes pour un bureau peu utilisé. De telles différences au niveau des performances se traduisent par des différences au niveau des prix dans le sens où — comme toujours — les performances sont une fonction du prix. La haute performance en informatique n'est pas bon marché.

5.3.1. Aperçu historique

Au fil des années, de nombreuses interfaces différentes ont été développées pour les périphériques de stockage de masse. Certaines ont été abandonnées alors que d'autres sont toujours utilisées à l'heure actuelle. Dans cette optique, la liste ci-dessous n'a pour autre but que de donner des informations sur l'envergure du développement des interfaces au cours des trente dernières années et de fournir une certaine perspective sur les interfaces utilisées de nos jours.

FD-400

Une interface conçue dans les années '70, à l'origine pour les lecteurs de disquettes 8 pouces. Elle utilisait un câble conducteur 44 broches avec un connecteur en bordure de la carte du circuit intégré, qui fournissait aussi bien l'électricité que les données.

SA-400

Une autre interface de lecteur de disquettes (développée cette fois-ci à l'origine, à la fin des années '70, pour le lecteur de nouvelles disquettes 5,25 pouces de l'époque). Elle utilisait un câble conducteur 34 broches avec un connecteur socket standard. Une version légèrement modifiée de cette interface est encore utilisée de nos jours pour les lecteurs de disquettes 5,25 pouces et 3,5 pouces.

IPI

Cette interface, dont l'acronyme signifie Intelligent Peripheral Interface, était utilisée sur les lecteurs de disques 8 pouces et 14 pouces déployés dans les miniordinateurs des années '70.

SMD

Succédant à l'interface IPI, l'interface SMD (de l'anglais Storage Module Device) était utilisée sur les disques durs 8 pouces et 14 pouces des miniordinateurs des années '70 et '80.

ST506/412

Une interface de disque dur remontant aux années '80. Utilisée dans de nombreux ordinateurs personnels de l'époque, cette interface utilisait deux câbles — un câble conducteur 34 broches et un câble conducteur 20 broches.

ESDI

Cette interface dont l'acronyme signifie Enhanced Small Device Interface, était considérée comme un successeur de l'interface ST506/412 avec un taux de transfert plus rapide et une prise en charge de disques d'une taille supérieure. Remontant au milieu des années '80, l'interface ESDI utilisait le même schéma de connexion à deux câbles que l'interface qui la précédait.

Parallèlement à ces interfaces, existaient aussi les interfaces des systèmes propriétaires, créées par les plus grands revendeurs informatiques de l'époque (essentiellement IBM et DEC). La création de ces interfaces était en fait une tentative pour protéger le marché très lucratif des périphériques de leurs ordinateurs. Toutefois, à cause de la nature des produits propriétaires, les périphériques compatibles avec ces interfaces étaient plus coûteux que leurs équivalents libres. Telle est la raison pour laquelle ces interfaces n'ont pas réussi à jouir d'une popularité à long terme.

Bien que les interfaces propriétaires aient pour la plupart disparu et que celles décrites au début de cette section ne représentent désormais qu'une partie infime (voire nulle) du marché, il est bon de connaître l'existence de ces interfaces oubliées car elles démontrent un aspect important de l'informatique — dans l'industrie, rien n'est constant pour bien longtemps. Dans de telles circonstances, il est important de toujours être attentif à l'émergence de nouvelles technologies en matière d'interfaces ; il se peut qu'un jour vous tombiez sur une interface qui en fait réponde mieux à vos besoins que le produit plus traditionnel que vous utilisez actuellement.

5.3.2. Interfaces actuelles aux normes de l'industrie

Contrairement aux interfaces propriétaires mentionnées dans la section précédente, certaines interfaces ont été adoptées plus d'autres et ont été adaptées aux normes de l'industrie. Deux interfaces en particulier ont effectué cette transition et sont désormais au coeur de l'industrie de stockage actuelle :

- IDE/ATA
- SCSI

5.3.2.1. IDE/ATA

L'acronyme IDE signifie Integrated Drive Electronics. Cette interface a vu le jour à la fin des années '80 et utilise un connecteur 40 broches.



Remarque

En fait, le vrai nom de cette interface est interface "AT Attachment" (ou ATA) mais le terme "IDE" (faisant référence à un périphérique de stockage de masse compatible avec ATA) est encore parfois utilisé. Ceci étant, le reste de cette section utilisera le vrai nom de cette interface — ATA.

ATA implémente une topologie en bus, chaque bus prenant en charge deux périphériques de stockage de masse. Les deux périphériques portent respectivement les noms de *maître* et d'*esclave*. Ces termes prêtent quelque peu à confusion dans la mesure où ils impliquent une relation entre les deux périphériques, qui en fait n'existe pas. Le choix du périphérique devant être le maître et de celui devant être l'esclave est normalement effectué via l'utilisation de blocs de cavaliers sur chaque périphérique.



Remarque

Une innovation plus récente est l'introduction de capacités *cable select* (ou sélection par le câble) pour l'interface ATA. Cette innovation nécessite l'utilisation d'un câble spécial, d'un contrôleur ATA et de périphériques de stockage de masse qui prennent en charge cable select (normalement au moyen du paramètre "cable select" du cavalier). Lorsque le paramètre cable select est configuré correctement, il permet d'éliminer le besoin de changer les cavaliers lorsque des périphériques sont déplacés ; au lieu d'une telle situation, l'emplacement du périphérique sur le câble ATA indique s'il s'agit du maître ou de l'esclave.

Une variation de cette interface illustre les différentes manières uniques selon lesquelles les technologies peuvent être mélangées et nous permet de présenter une autre interface aux normes de l'industrie informatique. *ATAPI*, qui est une variation de l'interface ATA, correspond à l'acronyme de AT Attachment Packet Interface. Utilisée essentiellement pour les lecteurs de CD-ROM, *ATAPI* respecte les caractéristiques électriques et mécaniques de l'interface ATA, mais utilise le protocole de communication de l'interface que nous allons maintenant examiner — SCSI.

5.3.2.2. SCSI

Précédemment connue sous le nom Small Computer System Interface, ou SCSI comme elle est appelée à l'heure actuelle, a vu le jour au début des années '80 et a été déclarée comme norme en 1986. Tout comme ATA, SCSI utilise la topologie en bus. Ceci dit, les similarités s'arrêtent ici.

L'utilisation d'une topologie en bus suppose que chaque périphérique du bus soit identifié d'une manière ou d'une autre et ce, de façon unique. Alors que l'interface ATA prend en charge seulement deux

périphériques différents pour chaque bus et donne à chacun d'eux un nom spécifique, SCSI effectue cette opération en attribuant à chaque périphérique du bus SCSI une adresse numérique unique ou *ID SCSI*. Chaque périphérique d'un bus SCSI doit être configuré (généralement avec des cavaliers ou commutateurs³) pour répondre à son ID SCSI.

Avant de poursuivre cette discussion, il est important de remarquer ici que la norme SCSI ne représente pas une interface particulière, mais plutôt une famille d'interfaces. À ce titre, SCSI affiche des différences dans de nombreux domaines, parmi lesquels figurent :

- Largeur de bus
- Vitesse de bus
- Caractéristiques électriques

La norme SCSI d'origine décrivait une topologie en bus dans laquelle huit lignes du bus étaient utilisées pour le transfert de données. Dans de telles conditions, les périphériques SCSI pouvaient transférer des données, un octet à la fois. Quelques années plus tard, la norme a été étendue afin de permettre des implémentations dans lesquelles seize lignes pouvaient être utilisées, doublant ainsi la quantité de données transférables par les périphériques. Les premières implémentations SCSI "8 bits" ont alors pris le nom de SCSI *étroit* (ou *narrow*) alors que les nouvelles implémentations SCSI 16 bits ont elles été baptisées SCSI *large* (ou *wide*) .

Au départ, la vitesse de bus pour SCSI était de 5 MHz, permettant un taux de transfert de 5 Mo/seconde sur l'ancien bus SCSI 8 bit. Toutefois, plus tard des révisions de la norme ont permis de doubler cette vitesse à 10 MHz, faisant passer le taux de transfert à 10 Mo/seconde pour SCSI étroit et à 20 Mo/seconde pour SCSI large. Tout comme c'était le cas lors du changement de largeur de bus, l'augmentation de la vitesse de bus a elle aussi donné lieu à une nouvelle terminologie, le bus d'une vitesse de 10 MHz étant désormais qualifié de *rapide*. Les améliorations ultérieures qui ont permis d'augmenter la vitesse des bus ont également entraîné l'utilisation de nouveaux qualificatifs : *ultra* (20 MHz), *fast-40* (40 MHz), et *fast-80*⁵. Des augmentations encore plus importantes des taux de transfert sont à l'origine de plusieurs versions différentes de la vitesse de bus *ultra160*.

Grâce à une combinaison de tous ces termes, les différentes configurations SCSI peuvent être qualifiées de manière concise. Par exemple, "SCSI ultra large " (ou SCSI ultra-wide) fait référence à un bus SCSI 16 bits tournant à une vitesse de 20MHz.

La norme SCSI utilisait à l'origine un système de signalisation asymétrique aussi appelé *single-ended* ; il s'agit d'une configuration électrique dans laquelle un seul conducteur est utilisé pour transmettre un signal électrique. Des implémentations plus récentes ont permis l'utilisation d'une signalisation *différentielle* dans laquelle deux conducteurs sont utilisés pour transmettre un signal. Bien qu'ayant l'avantage d'être moins sensible aux interférences et de permettre l'utilisation de câbles plus longs, un SCSI différentiel (portant désormais le nom de SCSI *high voltage differential* ou HVD), n'a jamais été vraiment populaire sur le marché informatique traditionnel. Une implémentation plus récente portant le nom de *low voltage differential* (LVD), a finalement percé pour être maintenant couramment utilisée et figure même parmi les pré-requis pour les vitesses de bus plus élevées.

La largeur d'un bus SCSI ne détermine pas seulement la quantité de données pouvant être transmise à chaque cycle d'horloge, mais détermine également le nombre de périphériques pouvant être connectés à un bus. Les SCSI courants prennent en charge 8 périphériques à adresse unique, alors que les SCSI larges eux en supportent 16. Dans les deux cas, vous devez vous assurer que tous les périphériques sont bien configurés de manière à utiliser un ID SCSI unique. Une situation dans laquelle

4. Il existe du matériel de stockage (incorporant généralement des "supports" — ou carriers — de disques amovibles) conçu de sorte que le branchement d'un module donne automatiquement à l'ID SCSI sa valeur appropriée.

5. Fast-80 ne correspond pas techniquement parlant à une augmentation de vitesse de bus ; en effet, le bus 40 MHz est toujours utilisé mais les données sont cadencées aussi bien au sommet qu'au bas de chaque impulsion d'horloge, permettant ainsi de doubler la capacité de traitement.

deux périphériques partageant un même ID est une source de problèmes qui pourraient entraîner la corruption des données.

Il est également important de garder à l'esprit que *chaque* périphérique sur un bus utilise un ID, y compris le contrôleur SCSI. Assez souvent, les administrateurs système oublient ce point important et accidentellement configurent un périphérique pour qu'il utilise le même ID SCSI que le contrôleur de bus. Ainsi, en pratique, seulement 7 périphériques (ou 15 dans le cas d'un SCSI large) peuvent être présents sur un seul bus, puisque chaque bus doit réserver un ID pour le contrôleur.



Astuce

La plupart des implémentations SCSI incluent un processus de balayage du bus SCSI qui est souvent utilisé pour confirmer que tous les périphériques sont correctement configurés. Si le balayage d'un bus établit que chaque ID SCSI est associé au même périphérique, ce dernier a été incorrectement configuré pour utiliser le même ID SCSI que le contrôleur SCSI. Pour résoudre le problème, reconfigurez le périphérique de sorte qu'il utilise cette fois-ci un ID SCSI différent (et unique).

Étant donné que l'architecture SCSI est orientée vers les bus, il est nécessaire de *terminer* les deux extrémités de manière appropriée. La terminaison est effectuée en plaçant une charge d'une impédance adéquate sur chaque conducteur composant le bus SCSI. La terminaison est une nécessité électrique ; sans terminaison, les différents signaux présents sur le bus seraient réfléchis aux extrémités des bus, corrompant par là même toute communication.

De nombreux périphériques SCSI (mais pas tous) sont vendus avec des terminateurs (aussi appelés bouchons) internes qui peuvent être activés ou désactivés à l'aide de cavaliers ou de commutateurs. Des terminateurs externes sont également disponibles.

Un dernier point important à garder à l'esprit en ce qui concerne SCSI — ce n'est pas seulement un standard d'interface pour les périphériques de stockage de masse. De nombreux autres périphériques (tels que les scanners, imprimantes et périphériques de communication) utilisent SCSI. Bien que d'une utilisation beaucoup moins courante que les périphériques de stockage de masse SCSI, il ne faut pas les oublier. De plus, avec l'apparition des interfaces USB et IEEE-1394 (souvent appelées Firewire), ces interfaces seront à l'avenir, utilisées davantage pour ce type de périphériques.



Astuce

Les interfaces USB et IEEE-1394 commencent également à percer dans le monde du stockage de masse ; toutefois, aucun périphérique de stockage de masse USB ou IEEE-1394 natif n'existe encore à l'heure actuelle. Les produits disponibles de nos jours sont plutôt basés sur des périphériques ATA ou SCSI dotés d'une circuitrie externe pour la conversion.

Indépendamment de l'interface utilisée par le périphérique de stockage de masse, le principe de fonctionnement interne du périphérique a une influence sur sa performance. La section suivante examine ce point important.

5.4. Caractéristiques de performance des disques durs

Les caractéristiques de performance des disques durs ont déjà été abordées très brièvement dans la Section 4.2.4 ; la présente section examine elle le sujet de manière beaucoup plus approfondie. Il est

important que les administrateurs système disposent de bonnes connaissances de base sur le fonctionnement des disques durs, afin d'éviter toute modification accidentelle de la configuration du système qui pourrait avoir un impact négatif sur la performance du système.

La durée nécessaire à un disque dur pour répondre à une requête d'E/S et la traiter dépend des deux éléments suivants :

- Les limitations électriques et mécaniques du disque dur
- La charge d'E/S imposée par le système

Les sections suivantes examinent ces aspects de la performance du disque dur de manière plus détaillée.

5.4.1. Limitations mécaniques/électriques

Étant donné que les disques durs sont des périphériques électromécaniques, ils sont soumis à des limitations au niveau de leur vitesse et de leur performance. Chaque requête E/S a besoin que les différents composants du disque dur fonctionnent de concert afin de répondre à la requête. Puisque chacun de ces composants a des caractéristiques de performance différentes, la performance générale du disque dur est déterminée par la somme des performances des composants individuels.

Cependant, au niveau de la rapidité, les composants électroniques sont au moins d'un ordre de grandeur supérieur, par rapport aux composants mécaniques. Par conséquent, ce sont les composants mécaniques qui ont le plus grand impact sur la performance générale du disque dur.



Astuce

La meilleure manière d'améliorer la performance du disque dur consiste à réduire autant que possible, son activité mécanique.

Le temps d'accès moyen d'un disque dur typique est d'environ 8,5 millisecondes. Les sections suivantes subdivisent ce chiffre de manière plus détaillée, montrant ainsi la manière selon laquelle chaque composant impacte sur la performance générale du disque dur.

5.4.1.1. Durée de traitement des commandes

Tous les disques durs fabriqués de nos jours sont dotés de systèmes informatiques sophistiqués qui contrôlent leur fonctionnement. Ces systèmes informatiques effectuent les tâches suivantes :

- Ils interagissent avec l'extérieur au moyen de l'interface du disque dur
- Ils contrôlent le fonctionnement des autres composants du disque dur et effectuent la récupération nécessaire suite à toute situation d'erreur pouvant survenir
- Ils traitent les données brutes lues et écrites sur le support de stockage même

Malgré la puissance des microprocesseurs utilisés dans les disques durs, les tâches qui leur sont assignées prennent du temps pour être effectuées. En moyenne, cette durée est de l'ordre de 0,003 millisecondes.

5.4.1.2. Lecture/écriture de données par les têtes

Les têtes de lecture/écriture du disque dur ne fonctionnent que lorsque les plateaux de disques qu'elles "survolent" sont en rotation. Étant donné que c'est le mouvement du support placé sous les têtes qui permet aux données d'être lues ou écrites, le temps qu'il faut au support contenant le secteur recherché pour passer entièrement sous la tête, constitue en fait le seul élément influençant l'impact de la tête sur la durée totale d'accès aux données. Cette opération est en moyenne de 0,0086 millisecondes pour un disque d'une vitesse de 10.000 RPM, contenant 700 secteurs par piste.

5.4.1.3. Latence rotationnelle

Étant donné que les plateaux d'un disque dur tournent en permanence, lorsque la requête d'E/S arrive, il est très peu probable que le plateau dans sa rotation se trouve exactement à l'endroit à partir duquel il est possible d'accéder au secteur souhaité. Par conséquent, même si le reste du disque dur est prêt à accéder à ce secteur, tous les différents composants doivent attendre que le plateau tourne suffisamment pour que le secteur recherché se trouve exactement sous la tête de lecture/écriture.

C'est précisément la raison pour laquelle les disques durs à performance élevée font tourner leur plateau à une vitesse supérieure. De nos jours, des vitesses de l'ordre de 15.000 RPM sont réservées aux disques durs les plus performants, alors qu'une vitesse de 5.400 RPM est seulement considérée comme acceptable pour des disques de base. La durée moyenne est de 3 millisecondes pour un disque d'une vitesse de 10.000 RPM.

5.4.1.4. Mouvement du bras d'accès

Au niveau des disques durs, le bras d'accès est considéré comme le talon d'Achille du matériel. En effet, ce bras d'accès doit se déplacer de manière très rapide et précise sur de longues distances. En outre, le mouvement du bras d'accès est continu — il doit accélérer rapidement en approchant le cylindre recherché et doit ensuite ralentir tout aussi rapidement afin d'éviter tout dépassement. Le bras d'accès doit donc être très solide (afin de faire face aux forces violentes engendrées par le besoin de mouvement rapide) tout en restant léger (afin de réduire la masse à accélérer/ralentir).

Il est très difficile d'atteindre ces buts opposés, comme le montre le temps relativement long qu'il faut au bras d'accès pour se déplacer, par rapport au temps nécessaire aux autres composants pour effectuer leur tâche. La rapidité de mouvement du bras d'accès représente par conséquent l'élément essentiel influençant la performance générale d'un disque dur ; cette dernière est en moyenne de 5,5 millisecondes.

5.4.2. Charges des E/S et performance

La charge des E/S à laquelle un disque dur est soumis représente un autre élément ayant une influence sur la performance des disques durs. Parmi les aspects spécifiques de la charge des E/S figurent :

- La quantité d'opérations de lecture par rapport à la quantité d'opérations d'écriture
- Le nombre actuel de lecteurs/scripteurs
- L'endroit où les opérations de lecture/écriture sont effectuées

Ces points sont traités de manière plus détaillée dans les sections suivantes.

5.4.2.1. Opérations de lecture contre opérations d'écriture

Pour un disque dur moyen utilisant des supports magnétiques pour le stockage de données, le nombre d'opérations d'E/S de lecture par rapport à celui des opérations d'E/S d'écriture n'est pas vraiment source d'inquiétude dans la mesure où les opérations de lecture et les opérations d'écriture prennent

autant de temps pour être effectuées⁶. Ceci étant, le temps nécessaire au traitement des opérations de lecture et celui des opérations d'écriture est différent pour d'autres technologies de stockage de masse⁷.

En conséquence, les périphériques prenant plus de temps pour traiter les opérations d'E/S d'écriture (par exemple) sont capables de traiter moins d'opérations d'E/S d'écriture que d'opérations d'E/S de lecture. Dans une optique différente, par rapport à une opération d'E/S de lecture, une opération d'E/S d'écriture utilise une plus grande partie de la capacité du périphérique à traiter des requêtes d'E/S.

5.4.2.2. Lecteurs/Scripteurs multiples

Un disque dur qui traite des requêtes d'E/S provenant de sources multiples doit faire face à une charge différente qu'un disque dur traitant des requêtes d'E/S provenant d'une seule source. Une telle situation s'explique essentiellement par le fait que de multiples demandeurs d'E/S ont le potentiel de faire peser une charge d'E/S plus élevée sur un disque dur, que ne peut le faire un seul demandeur d'E/S.

En effet, le demandeur d'E/S doit effectuer un certain degré de traitement avant qu'une E/S puisse être effectuée. Après tout, le demandeur doit établir la nature de la requête d'E/S avant qu'elle ne puisse être effectuée. Étant donné que le traitement nécessaire pour déterminer la nature de la requête prend un certain temps, il existe une limite supérieure à la charge d'E/S pouvant être engendrée par tout demandeur — seul un CPU plus rapide peut augmenter cette limite. Cette limitation est plus prononcée si, avant d'effectuer une opération d'E/S, le demandeur a besoin d'une intervention de la part de l'utilisateur.

Toutefois, lorsqu'il existe des demandeurs multiples, il est possible de maintenir des charges d'E/S supérieures. Dès lors que la puissance de CPU disponible est suffisante pour assurer le traitement nécessaire à la création de requêtes d'E/S, l'ajout de demandeurs d'E/S supplémentaires se traduit en une augmentation de la charge d'E/S.

À cet égard cependant, un autre aspect influence la charge d'E/S produite. Ce dernier sera abordé dans la section suivante.

5.4.2.3. Emplacement des opérations de lecture/écriture

Bien que cet aspect des performances du disque dur ne se limite pas seulement à un environnement ayant de multiples demandeurs, il a tendance à se manifester de manière plus prononcée dans un tel environnement. Le problème est de savoir si les demandes de données d'E/S venant d'un disque dur concernent des données physiquement proches des autres données qui sont également demandées.

La raison pour laquelle cet aspect est important devient plus clair lorsqu'on garde à l'esprit la nature électromécanique du disque dur. Le composant le plus lent de tout disque dur est le bras d'accès. Par conséquent, si les données auxquelles les requêtes d'E/S entrantes ont accès ne nécessitent aucun mouvement du bras d'accès, le disque dur est à même de répondre à un nombre bien plus élevé de requêtes de données d'E/S, que si les données auxquelles l'accès est nécessaire se trouvent éparpillées sur tout le disque et demandent donc au bras d'accès de bouger énormément.

Pour illustrer ce point, il suffit d'examiner les caractéristiques de performance des disques durs. Ces caractéristiques incluent souvent le *temps d'accès au cylindre adjacent* (lorsque le bras d'accès ne

6. Strictement parlant, ce n'est pas vraiment le cas. Tous les disques durs disposent, sur la carte mère, d'une certaine quantité de mémoire cache qui est utilisée pour améliorer les performances en écriture. Cependant, toute requête d'E/S demandant la lecture de données doit à un moment ou à un autre, être satisfaite en lisant physiquement les données sur le support de stockage. Dans de telles conditions, même si le cache peut permettre de réduire les problèmes de performance liés à la lecture des E/S, il ne peut en aucun cas éliminer totalement le temps nécessaire à la lecture physique des données sur le support de stockage.

7. Certains disques durs optiques ont ce comportement en raison des limitations physiques dues aux technologies utilisées pour implémenter un stockage optique des données.

bouge qu'un tout petit peu — seulement jusqu'au cylindre placé juste à côté) et le *temps d'accès pour une course complète* (lorsque le bras d'accès se déplace du tout premier cylindre au tout dernier). Par exemple, ci-dessous figurent les temps d'accès d'un disque dur à haute performance :

Cylindre adjacent	Full-Stroke
0,6	8,2

Tableau 5-4. Temps d'accès au cylindre adjacent et temps d'accès full-stroke (en millisecondes)

5.5. Mise en utilisation du stockage

Une fois qu'un périphérique de stockage de masse est en place, de lui même, il ne sert pas à grand chose. En effet, il peut certes servir à lire et écrire des données, mais sans structure sous-jacente, l'accès aux données n'est possible qu'en utilisant des adresses de secteurs (soit géométriques, soit logiques).

Il faut des méthodes permettant d'utiliser beaucoup plus facilement le stockage brut fourni par le disque dur. Les sections suivantes examinent certaines des techniques les plus couramment utilisées pour ce faire.

5.5.1. Partitions/Tranches

Un administrateur système est toujours frappé par le fait que la taille d'un disque dur peut être bien supérieure aux besoins de la tâche à effectuer. En effet, de nombreux systèmes d'exploitation sont en mesure de découper l'espace de leur disque dur en différentes *partitions* ou *tranches*.

Étant donné que les partitions sont séparées les unes des autres, elles peuvent utiliser des quantités d'espace différentes sans que cet espace n'affecte d'une manière ou d'une autre celui utilisé par les autres partitions. Par exemple, même si la partition contenant les fichiers de l'utilisateur approche sa capacité, la partition contenant les fichiers qui composent le système d'exploitation n'est pas du tout affectée. Le système d'exploitation dispose toujours d'espace libre pour sa propre utilisation.

Bien qu'une telle perception soit un peu simpliste, vous pouvez plus ou moins comparer les partitions à des disques durs. En fait, certains systèmes d'exploitation font référence aux partitions en tant que "disques". Toutefois, ce point de vue n'est pas tout à fait exact ; il est donc important d'examiner les partitions de manière plus détaillée.

5.5.1.1. Attributs des partitions

Les partitions sont définies en fonctions des attributs suivants :

- Géométrie de la partition
- Type de partition
- Champ du type de partiton

Ces attributs sont examinés de manière plus détaillée dans les sections suivantes.

5.5.1.1.1. Géométrie

La géométrie d'une partition fait référence à son emplacement sur un disque dur. Elle peut être définie en terme de têtes, secteurs, cylindres de début et de fin, bien que les partitions commencent et finissent

le plus souvent à la limite d'un cylindre. La taille d'une partition est alors définie comme étant la quantité de stockage existant entre les cylindres de début et de fin.

5.5.1.1.2. Type de partition

Le type de partition fait référence à la relation existant entre une certaine partition et les autres partitions du disque dur. Il existe trois types différents de partitions :

- Partitions primaires
- Partitions étendues
- Partitions logiques

Les sections suivantes décrivent en détail chacun des types de partitions.

5.5.1.1.2.1. Partitions primaires

Les partitions primaires sont des partitions qui peuvent prendre un des quatre emplacements des partitions primaires dans la table des partitions du disque dur.

5.5.1.1.2.2. Partitions étendues

Les partitions étendues ont été développées pour répondre à un besoin en partition allant au-delà des quatre partitions disponibles sur chaque disque dur. Une partition étendue peut elle-même contenir de multiples partitions, permettant ainsi d'augmenter considérablement le nombre de partitions possibles sur un seul disque dur. L'apparition des partitions étendues a été motivée par les capacités croissantes des nouveaux disques durs.

5.5.1.1.2.3. Partitions logiques

Les partitions logiques correspondent aux partitions contenues à l'intérieur d'une partition étendue ; du point de vue de leur utilisation, elles ne sont en aucun cas différentes d'une partition primaire non étendue.

5.5.1.1.3. Champ du type de partition

Chaque partition a un champ consacré au type contenant un code pour indiquer l'utilisation prévue de la partition. Ce champ de type peut (ou non) correspondre au système d'exploitation de l'ordinateur. Mais il peut aussi correspondre à la manière dont les données seront stockées au sein de la partition. La section suivante fournit de plus amples informations sur cet aspect important.

5.5.2. Systèmes de fichiers

Même en disposant du périphérique de stockage de masse approprié, configuré correctement et partitionné de manière adéquate, il n'est toujours pas possible de stocker et rechercher des informations facilement — il manque une manière permettant de structurer et d'organiser ces informations. En fait, il faut un *système de fichiers*.

La notion de système de fichiers est tellement fondamentale pour l'utilisation des périphériques de stockage de masse que l'utilisateur d'ordinateur moyen ne distingue même plus entre les deux éléments. Ceci étant, les administrateurs système ne peuvent pas se permettre d'être ignorants quant aux systèmes de fichiers et quant à l'impact qu'ils ont sur le travail quotidien.

Un système de fichiers est une méthode permettant de représenter des données sur un périphérique de stockage de masse. Les systèmes de fichiers ont généralement les caractéristiques suivantes :

- Stockage de données basé sur des fichiers
- Structure de répertoire (parfois appelé "dossiers") hiérarchique
- Suivi de la création de fichiers, de l'accès et des moments de modification
- Degré de contrôle du type d'accès autorisé pour un fichier particulier
- Notion de propriété de fichier
- Comptabilisation de l'espace utilisé

Tous les systèmes de fichiers ne possèdent pas forcément chacune de ces caractéristiques. Par exemple, un système de fichiers construit pour un système d'exploitation mono-utilisateur pourrait tout à fait utiliser une méthode de contrôle d'accès beaucoup plus simplifiée et pourrait vraisemblablement se passer d'une prise en charge pour la propriété de fichiers.

Il est important de garder à l'esprit que le système de fichiers utilisé peut avoir un impact considérable sur la nature de votre charge de travail quotidienne. Ainsi, en vous assurant que le système de fichiers utilisé dans votre entreprise correspond étroitement aux besoins fonctionnels de cette dernière, vous pourrez non seulement garantir qu'il sera tout à fait approprié aux besoins de votre environnement, mais qu'il pourra également être maintenu facilement et efficacement.

C'est dans cet état d'esprit que les sections suivantes examinent ces caractéristiques en détail.

5.5.2.1. Stockage à base de fichiers

Alors que de nos jours les systèmes de fichiers qui utilisent la métaphore du fichier pour le stockage de données sont si universels qu'on n'y prête même plus attention, il convient néanmoins ici d'examiner certains points.

Tout d'abord, il est important de connaître toute restriction existant au niveau des noms des fichiers. Par exemple, quels caractères sont acceptés dans un nom de fichier ? Quelle est la longueur maximale d'un nom de fichier ? Ces questions sont importantes dans la mesure où elles dictent les règles à suivre en matière de noms de fichiers acceptables ou inacceptables. Les systèmes d'exploitation plus anciens utilisant des systèmes de fichiers plus élémentaires n'acceptaient souvent que des caractères alphanumériques (et seulement majuscules) et des noms de fichiers traditionnels de type 8.3 (c'est-à-dire un nom de fichier composé de huit caractères suivi d'une extension de fichier de trois caractères).

5.5.2.2. Structure de répertoire hiérarchique

Alors que les systèmes de fichiers utilisés dans certains anciens systèmes d'exploitation ne fonctionnaient pas selon le concept des répertoires, tous les systèmes de fichiers couramment utilisés de nos jours incluent cette caractéristique. Les répertoires sont eux-mêmes souvent implémentés en tant que fichiers, ce qui veut dire qu'aucun utilitaire particulier n'est nécessaire pour les maintenir.

De plus, étant donné que les répertoires sont eux-mêmes des fichiers et qu'ils contiennent des fichiers, ils peuvent contenir d'autres répertoires, permettant ainsi la construction d'une hiérarchie de répertoires à plusieurs niveaux. Ce concept étant essentiel, tous les administrateurs système devraient en avoir une très bonne compréhension. L'utilisation d'une hiérarchie de répertoires à plusieurs niveaux peut simplifier considérablement la gestion de fichiers, aussi bien par vos utilisateurs que par vous-même.

5.5.2.3. Suivi des dates de création, d'accès, de modification des fichiers

La plupart des systèmes de fichiers effectuent un suivi des dates auxquelles un fichier a été créé ; certains gardent même un historique des dates auxquelles les fichiers ont été modifiés ou lus. Outre la possibilité de pouvoir déterminer lorsqu'un fichier donné a été créé, utilisé ou modifié, ces dates sont essentielles pour le bon déroulement des opérations de sauvegardes incrémentielles.

Pour de plus amples informations sur la manière dont les sauvegardes utilisent ces caractéristiques des système de fichiers, reportez-vous à la Section 8.2.

5.5.2.4. Contrôle d'accès

Le contrôle d'accès représente un domaine dans lequel les systèmes de fichiers diffèrent considérablement. Certains systèmes de fichiers n'ont aucun modèle de contrôle d'accès clair, alors que d'autres sont beaucoup plus sophistiqués. D'une manière générale, la plupart des systèmes de fichiers modernes utilisent l'association de deux composants comme base d'une même méthodologie de contrôle d'accès, à savoir :

- Identification de l'utilisateur
- Liste des opérations permises

Le principe de l'identification de l'utilisateur suppose que le système de fichiers (et le système d'exploitation sous-jacent) puisse d'abord être capable d'identifier l'utilisateur individuel de manière unique. Il est alors possible d'attribuer une responsabilité totale pour toute opération effectuée au niveau du système de fichiers. Une autre caractéristique souvent utile est celle des *groupes* d'utilisateurs— permettant de regrouper au coup par coup des utilisateurs. Les groupes sont la plupart du temps utilisés par des entreprises au sein desquelles des membres peuvent être associés à un ou plusieurs projet(s). Une autre caractéristique prise en charge par certains systèmes de fichiers est la création d'identifiants génériques pouvant être attribués à un ou plusieurs utilisateur(s).

Le système de fichiers doit ensuite être capable de maintenir des listes d'opérations qui sont permises (ou interdites) sur chaque fichier. Les opérations pour lesquelles un suivi est le plus couramment effectué sont les suivantes :

- La lecture de fichiers
- L'écriture de fichiers
- L'exécution de fichiers

Différents systèmes de fichiers peuvent étendre la liste des opérations pour inclure la possibilité de supprimer des fichiers ou même la possibilité d'effectuer des modifications liées au contrôle d'accès d'un fichier.

5.5.2.5. Comptabilisation de l'espace utilisé

Un aspect constant de la vie d'un administrateur système est le fait qu'il n'y a jamais assez d'espace libre, et même s'il y en a assez, ce ne sera pas la cas pour bien longtemps. Par conséquent, un administrateur système devrait, au minimum, être en mesure de déterminer facilement la proportion d'espace disponible pour chaque système de fichiers. En outre, des systèmes de fichiers dotés de fonctionnalités bien définies en matière d'identification des utilisateurs incluent souvent la possibilité d'afficher la quantité d'espace consommée par un utilisateur.

Cette fonctionnalité est essentielle dans de vastes environnements à utilisateurs multiples, car regrettamment, la règle des 80/20 est souvent en vigueur en matière d'espace disque — 20% des utilisateurs seront responsables pour 80% de la consommation de votre espace disque disponible. En facilitant l'identification des utilisateurs inclus dans ces 20%, il est possible de gérer de manière plus efficace les éléments liés au stockage.

En allant encore plus loin dans ce sens, certains systèmes de fichiers incluent la possibilité d'établir des limites individuelles pour les utilisateurs (souvent appelés *quotas de disque*) en ce qui concerne la quantité d'espace disque que chacun d'eux peut utiliser. Bien que les caractéristiques varient en fonction des systèmes de fichiers, d'une manière générale, il est possible d'allouer à chaque utilisateur une certaine quantité d'espace disque pour sa propre utilisation. Mis à part cet aspect commun, les systèmes de fichiers varient les uns par rapport aux autres. En effet, certains d'entre eux autorisent l'utilisateur à dépasser une seule fois la limite qui lui est propre, alors que d'autre recourent à une "période de grâce" pendant laquelle une deuxième limite plus élevée est appliquée.

5.5.3. Structure de répertoire

De nombreux administrateurs système ne se préoccupent pas vraiment de la manière selon laquelle le stockage mis aujourd'hui à la disposition des utilisateurs, sera en fait utilisé demain. Pourtant, en réfléchissant un peu au sujet avant même de permettre aux utilisateurs de se servir du stockage, peut vous épargner de nombreux efforts superflus plus tard.

Dans ce sens, les administrateurs système peuvent utiliser les répertoires et sous-répertoires pour structurer le stockage disponible de manière compréhensible. Cette approche offre de nombreux avantages :

- Une compréhension plus aisée
- Une flexibilité accrue dans le futur

En soumettant votre stockage à une certaine structure, il est plus facile de comprendre son fonctionnement. Par exemple, prenez un vaste système à utilisateurs multiples. Au lieu de placer tous les répertoires des utilisateurs dans un grand répertoire, il sera peut-être plus approprié d'utiliser des sous-répertoires qui reflètent la structure de votre entreprise. Dans ce cadre, les personnes travaillant dans le service de comptabilité ont leurs propres répertoires sous le répertoire nommé *comptabilité*, alors que les membres du service d'ingénierie eux verront leurs répertoires regroupés sous le répertoire portant le nom *ingénierie* et ainsi de suite.

Une telle approche offre l'avantage de pouvoir effectuer plus facilement et de manière quotidienne, un suivi des besoins (et de l'utilisation) de stockage de chaque service de votre entreprise. L'obtention d'une liste des fichiers utilisés par les membres du service des ressources humaines devient alors une opération relativement simple. De même, il est alors facile de sauvegarder tous les fichiers utilisés par les services juridiques.

Avec une structure adéquate, il est possible d'augmenter la flexibilité. Toujours selon l'exemple précédent, supposez pour un instant que le service d'ingénierie soit sur le point de commencer plusieurs nouveaux projets de grande envergure. Dans ce cadre, de nombreux nouveaux ingénieurs seront recrutés. Malheureusement, il n'y a pas à l'heure actuelle, suffisamment de stockage libre utilisable pour satisfaire les besoins accrus du service d'ingénierie qui accueillera sous peu de nouveaux membres.

Toutefois, étant donné que chaque membre du service d'ingénierie stocke ses fichiers sous le répertoire *ingénierie*, il est relativement simple d'effectuer les opérations suivantes :

- Fournir du stockage supplémentaire pour faire face aux besoins du service d'ingénierie
- Sauvegarder tous les documents sous le répertoire *ingénierie*
- Restaurer la sauvegarde sur le nouveau stockage
- Changer le nom du répertoire *ingénierie* sur le stockage d'origine en quelque chose comme *archives-ingénierie* (avant de le supprimer entièrement, une fois que les opérations fonctionnent sans problème avec la nouvelle configuration et ce, pendant un mois)
- Effectuer les modifications nécessaires afin que tous les membres du service d'ingénierie puissent avoir accès à leurs fichiers sur le nouveau stockage

Bien sûr, une telle approche a également ses inconvénients. Par exemple, si du personnel est transféré fréquemment d'un service à un autre, il est nécessaire de disposer d'un système vous permettant d'en être averti, afin que vous puissiez modifier la structure de répertoire de manière appropriée. Sinon, la structure ne reflétera plus la réalité de votre environnement, ce qui entraînera au long terme, plus — et non moins — de travail pour vous.

5.5.4. Activation de l'accès au stockage

Une fois que le périphérique de stockage de masse a été correctement partitionné et qu'un système de fichiers y a été enregistré, le stockage peut être mis à la disposition des utilisateurs.

Pour certains systèmes d'exploitation, tel est en effet le scénario ; dès que le système d'exploitation a détecté le nouveau périphérique de stockage de masse, l'administrateur système peut le formater et il est alors possible d'y avoir accès immédiatement, sans aucun effort supplémentaire.

D'autres systèmes d'exploitation en revanche, nécessitent une étape supplémentaire. Cette dernière — à laquelle on fait souvent référence sous le terme de *montage* — indique au système d'exploitation la manière selon laquelle il peut accéder au périphérique de stockage. Le montage du stockage, qui est généralement effectué au moyen d'une commande particulière ou d'un programme utilitaire spécial, nécessite que le périphérique de stockage de masse (et parfois également la partition) soit explicitement identifié.

5.6. Technologies avancées de stockage

Bien que toutes les informations fournies dans ce chapitre n'aient fait référence jusqu'à présent qu'aux disques durs uniques reliés directement à un système, vous pouvez explorer d'autres options plus avancées. Les sections suivantes abordent certaines des approches les plus couramment utilisées pour élargir l'éventail des options disponibles en matière de stockage de masse.

5.6.1. Stockage accessible en réseau

En associant les technologies de réseau aux technologies de stockage, les administrateurs système peuvent disposer d'une plus grande flexibilité. Ce type de configuration offre deux avantages :

- La consolidation du stockage
- La simplification de l'administration

Le stockage peut être consolidé en déployant des serveurs haute performance dotés d'une connectivité réseau rapide et configurés avec de grandes quantités de stockage rapide. En disposant de la configuration appropriée, il est tout à fait possible de fournir un accès au stockage à des vitesses semblables à celles des stockages branchés localement. En outre, la nature même d'une telle configuration basée sur le partage, permet souvent de réduire les coûts ; en effet, les frais associés à la mise à disposition de stockage centralisé et partagé peuvent se révéler être inférieurs à ceux engendrés par la mise à disposition de stockage équivalent pour chacun des clients. De plus, l'espace libre est consolidé au lieu d'être réparti (et donc pas utilisable en tant qu'une seule entité) à travers de nombreux clients.

Des serveurs de stockage centralisés peuvent également simplifier de nombreuses tâches administratives. Par exemple, le contrôle de l'espace disque libre est une opération beaucoup plus simple lorsque le stockage devant être contrôlé se trouve sur un serveur de stockage centralisé. Les sauvegardes peuvent être considérablement simplifiées grâce à un serveur de stockage centralisé. Les sauvegardes prises en charge par un réseau pour de multiples clients sont possibles mais demandent plus de travail au niveau de la configuration et de la maintenance.

De nos jours, il existe une grande variété de technologies de stockage réseau et le choix d'une technologie particulière peut se révéler être une tâche relativement difficile. Presque tous les systèmes

d'exploitation disponibles sur le marché à l'heure actuelle incluent des moyens d'accéder à un stockage réseau, mais il est important de noter ici que certaines technologies ne sont pas compatibles les unes avec les autres. Dans ce telles conditions, quelle est la meilleure manière de déterminer la bonne technologie à déployer ?

L'approche produisant généralement les meilleurs résultats consiste à laisser les fonctionnalités intégrées du client décider en la matière, et ce pour les raisons suivantes :

- Réduction du nombre de problèmes liés à l'intégration du client
- Réduction de la quantité de travail à effectuer sur chaque système client
- Réduction du coût d'entrée de chaque client

Gardez bien à l'esprit que tout problème associé à un client est multiplié par le nombre total de clients dans votre entreprise. En utilisant les fonctionnalités intégrées des clients, vous n'avez pas à installer de logiciels supplémentaires sur chaque client (n'entraînant donc aucune dépense pour l'obtention de logiciels). Qui plus est, la certitude d'avoir une bonne prise en charge et intégration avec le système d'exploitation client est largement supérieure.

Il y a cependant un inconvénient. En effet, une telle approche suppose que l'environnement du serveur soit en mesure de fournir une bonne prise en charge des technologies de stockage réseau dont les clients ont besoin. Dans les situations où le système d'exploitation serveur et le système d'exploitation client sont un seul et même système, il n'y a généralement aucun problème. Dans le cas contraire, il sera nécessaire de passer du temps à "convertir" le serveur au langage des clients. Ceci étant, cet aspect négatif est mineur par rapport aux avantages qui en découlent.

5.6.2. Stockage basé sur RAID

Une des compétences qu'un administrateur système devrait cultiver, est son habilité à examiner des configurations de systèmes complexes et à remarquer les différents inconvénients inhérents à chaque configuration. Bien que cette opinion soit, au premier abord, quelque peu déprimante, elle peut en fait représenter une excellente manière d'extrapoler la situation au-delà du bel emballage flambant neuf et de visualiser l'envers du décor que pourrait représenter un certain samedi soir dans le futur, où la production sera arrêtée à cause d'une panne qui aurait facilement pu être évitée avec un minimum de prévoyance.

Dans cet état d'esprit, et en utilisant les connaissances dont nous disposons au sujet du stockage sur disque, essayons de voir si nous pouvons déterminer les manières selon lesquelles les disques durs peuvent créer des problèmes. Prenons tout d'abord une panne complète de matériel :

Un disque dur contenant quatre partitions tombe complètement en panne ; qu'advient-il des données stockées sur ces partitions ?

D'une manière immédiate, elles ne sont plus disponibles (au moins jusqu'à ce que l'élément défaillant puisse être remplacé et que les données puissent être récupérées à partir d'une sauvegarde récente).

Un disque dur ne contenant qu'une seule partition fonctionne à la limite de ses capacités en raison de charges d'Entrées/Sorties importantes : qu'advient-il des applications devant avoir accès aux données stockées sur cette partition ?

Les applications sont ralenties car le disque dur ne peut pas traiter plus rapidement les opérations de lecture et d'écriture.

Vous avez un grand fichier de données qui petit à petit grandit en taille ; il sera bientôt plus volumineux que le plus grand disque dur disponible sur votre système. Que se passe-t-il alors ?

Le disque dur se remplit au maximum, la taille du fichier de données est gelée et les applications qui l'utilisent arrêtent de tourner.

Un seul de ces problèmes suffirait à paralyser tout un centre de données, et pourtant, les administrateurs système sont confrontés à ce genre de problèmes de manière quotidienne. Que faire ?

Heureusement, une technologie permet de faire face à chacun de ces problèmes. *RAID* est le nom de cette dernière.

5.6.2.1. Concepts de base

RAID est l'acronyme de Redundant Array of Independent Disks⁸. Comme son nom l'indique, RAID est le moyen par lequel de multiples disques durs peuvent agir comme s'ils ne constituaient qu'un seul disque.

Les techniques RAID ont à l'origine été développées par les chercheurs de l'Université de Californie à Berkeley au milieu des années '80. À l'époque, il existait une différence de prix considérable entre les disques durs haute performance utilisés dans de grandes installations informatiques et les plus petits disques durs à vitesse inférieure employés dans l'industrie de l'informatique personnelle qui n'en était encore qu'à ses débuts. La matrice RAID était considérée comme un moyen d'utiliser plusieurs disques durs moins coûteux pour remplacer une unité au prix plus élevé.

Plus important encore, les matrices RAID pouvant être construites de diverses manières, elle peuvent afficher des caractéristiques différentes selon la configuration finale retenue. Examinons les différentes configurations (auxquelles ont fait référence sous le terme de *niveaux RAID*) disponibles de manière plus détaillée.

5.6.2.1.1. Niveaux RAID

À l'origine, les chercheurs de Berkeley avaient défini cinq niveaux RAID différents et les avaient numérotés de "1" à "5". Au cours des années, des niveaux supplémentaires ont été introduits par d'autres chercheurs et membres de l'industrie de stockage. Ceci dit, tous les niveaux RAID n'étaient pas utiles au même titre ; certains n'avaient d'intérêt que pour la recherche, alors que d'autres ne pouvaient pas être implémentés pour des raisons économiques.

En fin de compte, seulement trois niveaux RAID ont fini par être largement utilisés :

- Niveau 0
- Niveau 1
- Niveau 5

Les sections suivantes examinent chacun de ces niveaux de manière plus détaillée.

5.6.2.1.1.1. RAID 0

La configuration de disque connue sous le terme de RAID niveau 0 prête quelque peu à confusion dans le sens où ce niveau RAID est le seul n'utilisant absolument aucune redondance. Toutefois, même si RAID 0 n'offre pas grand chose d'un point de vue de la fiabilité, il offre d'autres avantages.

Une matrice RAID 0 est composée de deux disques durs ou plus. La capacité de stockage disponible sur chaque disque est découpée en *morceaux* qui correspondent à des copies de la taille d'origine (ou natives) des blocs natifs des disques. Les données enregistrées sur la matrice doivent être inscrites morceau par morceau, sur chacun des disques la composant. Les morceaux peuvent être perçus comme des bandes présentes sur chaque disque de la matrice, d'où l'autre terme utilisé pour RAID 0 : *striping* (aussi appelé agrégat par bandes).

8. Au tout début de la recherche sur RAID, l'acronyme correspondait à Redundant Array of *Inexpensive* Disks (Matrice de disques redondants bon marché), mais au fil des années, le prix des disques "standalone" (ou autonomes) que RAID avait pour vocation de remplacer a tellement baissé que la différence de prix est devenue insignifiante.

Par exemple, avec une matrice composée de deux disques et un morceau d'une taille de 4 Ko, l'écriture de 12 Ko de données sur cette matrice serait effectuée par répartition sur trois morceaux de 4 Ko chacun, sur les disques suivants :

- Les 4 premiers Ko seraient écrits sur le premier disque dur, sur le premier morceau
- Les 4 deuxièmes Ko seraient écrits sur le deuxième disque dur, sur le premier morceau
- Les 4 derniers Ko seraient écrits sur le premier disque dur, sur le second morceau

Par rapport à un disque dur unique, RAID 0 offre les avantages suivants :

- Taille globale supérieure — Il est possible de construire des matrices RAID 0 d'une taille supérieure à un disque dur unique, rendant le stockage de grands fichiers de données beaucoup plus facile
- Meilleure performance des opérations de lecture/écriture — La charge des Entrées/Sorties sur une matrice RAID 0 est répartie de manière uniforme sur l'ensemble des disques composant la matrice (à condition que toutes les E/S ne soient pas concentrées sur un seul morceau)
- Aucun espace perdu — Tout l'espace de stockage disponible sur l'ensemble des disques de la matrice est utilisable pour stocker des données

Par rapport à un disque dur unique, RAID 0 offre l'inconvénient suivant :

- Fiabilité inférieure — Chacun des disques d'une matrice RAID 0 doit être opérationnel pour que la matrice soit utilisable ; la défaillance d'un seul disque d'une matrice RAID 0 composé de N disques entraînera la suppression d' $1/N$ ème des données, rendant par là-même la matrice inutile.



Astuce

Si vous avez des problèmes pour maintenir l'uniformité des différents niveaux RAID, rappelez-vous que RAID 0 a zéro pour cent de redondance.

5.6.2.1.1.2. RAID 1

RAID 1 utilise deux disques durs identiques (bien que certaines implémentations en prennent en charge davantage). Toutes les données sont enregistrées sur chacun des deux disques, faisant par là-même de ces derniers des copies identiques. C'est la raison pour laquelle on parle souvent de RAID 1 en tant qu'agencement de disques en mode *miroir* (ou mirroring).

Lors de toute opération d'écriture sur une matrice RAID 1, deux opérations d'écriture doivent physiquement avoir lieu : une sur le premier disque et une sur le second disque. La lecture de données en revanche, est une opération unique à partir de l'un ou l'autre des disques de la matrice.

Par rapport à un disque dur unique, RAID 1 offre les avantages suivants :

- Redondance supérieure — Même en cas de défaillance d'un des disques de la matrice, il est toujours possible d'avoir accès aux données
- Performance supérieure des opérations de lecture — Étant donné que les deux disques durs sont opérationnels, les opérations de lecture peuvent être réparties de manière uniforme entre eux, réduisant ainsi les charge d'E/S individuelles

Par rapport à un disque dur unique, RAID 1 offre certains inconvénients parmi lesquels figurent :

- Taille maximale de la matrice limitée au plus grand disque dur disponible

- Performance réduite des opérations d'écriture — Étant donné que chacun des deux disques durs doit toujours être à jour, toutes les opérations d'écriture d'E/S doivent être effectuées par chacun des deux disques, une double opération qui ralentit le processus général des opérations d'écriture de données sur la matrice
- Rentabilité inférieure — Étant donné qu'un disque entier est dédié à la redondance, le coût d'une matrice RAID 1 est deux fois plus élevé que celui d'un disque dur unique



Astuce

Si vous avez des problèmes pour maintenir l'uniformité des différents niveaux RAID, rappelez-vous que RAID 1 a *un* pour cent de redondance.

5.6.2.1.1.3. RAID 5

RAID 5 essaie d'associer les avantages de RAID 0 à ceux de RAID 1, tout en minimisant leurs inconvénients respectifs.

Tout comme RAID 0, une matrice RAID 5 est composée de multiples disques durs, chacun d'eux étant divisé en morceaux. Cette méthode permet à une matrice RAID 5 d'avoir une taille supérieure à tout disque dur unique. Tout comme une matrice RAID 1, RAID 5 utilise une partie de son espace disque de manière redondante, augmentant ainsi le degré de fiabilité.

Ci étant, le principe de fonctionnement de RAID 5 est différent aussi bien de RAID 0 que de RAID 1.

Une matrice RAID 4 doit être composée au minimum de trois disques durs de taille identique (un plus grand nombre de disques durs peut cependant être utilisé). Chaque disque est découpé en morceaux sur lesquels les données sont enregistrées dans l'ordre. Chaque morceau n'est toutefois pas dédié au stockage de données comme c'est le cas avec RAID 0. En effet, dans une matrice composée de n disques durs, tout n ième morceau est dédié à la *parité*.

Les morceaux contenant la parité permettent la récupération de données en cas de défaillance d'un des disques durs de la matrice. La parité du morceau x est calculée mathématiquement selon une combinaison de chaque morceau x stocké sur tous les autres disques composant la matrice. Si les données d'un morceau sont mises à jour, la parité correspondante doit elle aussi être recalculée et mise à jour.

Selon cette méthode, chaque fois que des données sont enregistrées sur la matrice, au moins *deux* disques font l'objet d'opérations d'écriture : le disque stockant les données et le disque sur lequel figure le morceau contenant la parité.

Il est important de garder à l'esprit que les morceaux contenant les données de parité ne sont pas concentrés sur un seul disque de la matrice. Au contraire, ils sont répartis de manière uniforme sur tous les disques. Bien qu'il soit tout à fait possible de réserver un disque particulier au stockage exclusif des données de parité (en fait, on fait référence à ce type de configuration sous le terme de RAID 4), la mise à jour constante de ces dernières suite à l'enregistrement de nouvelles données sur la matrice, pourrait transformer le disque stockant ces données de parité en un goulet d'étranglement pour la performance. La répartition des données de parité sur l'ensemble de la matrice permet quant à elle de limiter cet impact.

Il est toutefois important de se rappeler que la parité a un impact sur les capacités globales de stockage de la matrice. Bien que les données de parité soient réparties sur l'ensemble des disques de la matrice, la quantité de stockage disponible n'est pas égale à l'ensemble des disques, dans la mesure où la taille d'un disque est dédiée à la parité.

Par rapport à un disque dur unique, RAID 5 offre les avantages suivants :

- Redondance accrue — En cas de défaillance de l'un des disques de la matrice, les informations de parité peuvent être utilisées pour reconstruire les morceaux de données manquants, sans perturber l'utilisation de la matrice⁹
- Performance accrue des opérations de lecture — En raison de la manière selon laquelle les données sont réparties entre les disques de la matrice (manière semblable à RAID 0), les opérations de lecture des E/S sont distribuées de manière uniforme entre les disques durs
- Rentabilité relativement bonne — Pour une matrice RAID 5 composée de n disques, seul $1/n$ ième du stockage global disponible est dédié à la redondance

Par rapport à un disque dur unique, RAID 5 offre l'inconvénient suivant :

- Performance réduite des opérations d'écriture — Étant donné que chaque opération d'écriture effectuée sur la matrice implique au moins deux activités d'écriture sur les disques physiques (une opération d'écriture pour les données et une pour la parité), la performance en écriture est inférieure à celle d'un disque unique¹⁰.

5.6.2.1.1.4. Combinaison de niveaux RAID

Suite à notre présentation des différents niveaux RAID, il devrait sembler évident que chaque niveau à des avantages et des inconvénients spécifiques. Peu après l'apparition du stockage basé sur des matrices RAID, un intérêt particulier s'est développé au niveau de la possibilité de combiner les différents niveaux RAID, afin de produire des matrices affichant tous les avantages et aucun des inconvénients des niveaux créés à l'origine.

Par exemple, que se passerait-il si les disques durs d'une matrice RAID 0 étaient en fait, eux-mêmes, des matrices RAID 1 ? Une telle situation offrirait les avantages de RAID 0 au niveau vitesse, alliés à la fiabilité de RAID 1.

Cette combinaison est exactement le genre de chose que les matrices RAID permettent de faire. Ci-dessous figurent les imbrications de niveaux RAID les plus courantes :

- RAID 1+0
- RAID 5+0
- RAID 5+1

Étant donné que les imbrications de niveaux RAID sont utilisées dans des environnements spécialisés, nous ne nous étendrons pas sur le sujet de manière plus détaillée. Toutefois, en ce qui concerne l'imbrication de niveaux RAID, il est important de garder à l'esprit les deux points suivants :

- Importance de l'ordre — L'ordre selon lequel les niveaux RAID sont combinés peut avoir un impact considérable sur la fiabilité. En d'autres termes, RAID 1+0 et RAID 0+1 *ne correspondent pas* à la même matrice.
- Coûts potentiellement élevés — Toutes les implémentations de RAID imbriqués partagent le même inconvénient, à savoir le coût de l'imbrication ; par exemple, RAID 5+1, la plus petite matrice possible, est composée de six disques durs (et un nombre encore plus élevé de disques durs est nécessaire pour des matrices plus grandes).

Après avoir examiné les concepts soutenant RAID, passons à la manière d'implémenter la matrice.

9. Lorsque la matrice fonctionne et qu'un disque n'est pas disponible, la performance des E/S est réduite en raison de la surcharge engendrée par la reconstruction des données manquantes.

10. Les calculs de parité engendrés par chaque activité d'écriture ont également un impact sur les opérations. Toutefois, selon l'implémentation particulière de RAID 5 (et en particulier selon l'endroit dans le système où les calculs de parité sont effectués), l'ampleur de cet impact peut être considérable ou presque inexistant.

5.6.2.1.2. Implémentations de RAID

Il est évident, d'après les sections précédentes, que RAID nécessite une "intelligence" supérieure à celle requise pour le traitement habituel des E/S de disque effectuées sur des disques individuels. Au strict minimum, les tâches suivantes doivent être effectuées :

- Répartition des requêtes d'E/S entrantes sur les disques individuels de la matrice.
- Calcul de la parité et enregistrement sur le disque approprié de la matrice, dans le cas de RAID 5
- Contrôle des disques individuels de la matrice et prise de mesures appropriées en cas de défaillance d'un disque
- Contrôle de la reconstruction d'un disque individuel de la matrice, lorsque ce disque a été remplacé ou réparé
- Mise à disposition d'un moyen permettant aux administrateurs d'effectuer des opérations de maintenance de la matrice (retrait et ajout de disques, initialisation et arrêt de reconstructions, etc.)

Il est possible d'utiliser deux méthodes pour accomplir ces tâches. Les deux sections suivantes les décrivent en détail.

5.6.2.1.2.1. RAID matériel

Une implémentation de RAID matériel prend généralement la forme d'une carte contrôleur de disque spécialisée. La carte effectue toutes les fonctions associées au RAID et contrôle directement les disques individuels des matrices auxquelles elle est connectée. Avec le pilote approprié, les matrices gérées par une carte RAID matériel sont considérées par le système d'exploitation hôte exactement comme des disques durs normaux.

La plupart des cartes contrôleurs RAID fonctionnent avec des disques SCSI, bien qu'il existe également d'autres contrôleurs RAID basés sur ATA. Dans tous les cas, l'interface d'administration est généralement implémentée selon une des trois manières suivantes :

- Des programmes utilitaires spécialisés qui sont exécutés comme des applications sous le système d'exploitation hôte, offrant une interface logicielle à la carte contrôleur
- Une interface intégrée à une carte utilisant un port série auquel l'accès se fait par le biais d'un émulateur de terminal
- Une interface de type BIOS à laquelle l'accès n'est possible que lors du test de mise sous tension du système

Certains contrôleurs RAID ont plus d'une seule interface d'administration. Pour des raisons évidentes, une interface logicielle offre le plus haut degré de souplesse, dans la mesure où elle permet d'effectuer des tâches administratives alors même que le système d'exploitation est en cours d'exécution. Toutefois, si vous démarrez un système d'exploitation à partir d'un contrôleur RAID, il est nécessaire d'utiliser une interface qui ne nécessite pas un système d'exploitation en cours d'exécution.

La gamme des différentes cartes contrôleurs RAID actuellement disponibles sur le marché est telle qu'il nous est impossible de toutes les examiner ici de manière détaillée. Pour obtenir de plus amples informations sur le sujet, il est recommandé de lire les brochures de documentation fournies par le fabricant.

5.6.2.1.2.2. RAID logiciel

Le RAID logiciel représente une matrice RAID implémentée en tant que logiciel au niveau du noyau ou du lecteur pour un système d'exploitation particulier. En tant que tel, il offre plus de souplesse en terme de prise en charge du matériel — dès lors que le matériel est pris en charge par le système

d'exploitation, il est possible de configurer et déployer des matrices RAID. Ce faisant, les coûts associés au déploiement d'une matrice RAID peuvent être considérablement réduits dans la mesure où l'acquisition de matériel RAID spécialisé et onéreux n'est pas nécessaire.

Souvent, la puissance CPU excédentaire qui est disponible pour les calculs de parité de RAID logiciel dépasse largement la puissance de traitement existant sur la carte contrôleur RAID. Par conséquent, certaines implémentations de RAID logiciels disposent en fait d'une capacité permettant des performances supérieures à celles des implémentations de RAID matériels.

Toutefois, RAID logiciel est soumis à certaines limitations qui n'apparaissent pas dans un RAID matériel. La plus importante qu'il convient de prendre en compte est la prise en charge lors du démarrage depuis une matrice RAID logicielle. Dans la plupart des cas, seules des matrices RAID 1 peuvent être utilisées au démarrage car le BIOS de l'ordinateur ne reconnaît pas RAID. Étant donné que le disque unique d'une matrice RAID 1 est reconnu de la même manière qu'un périphérique de démarrage non RAID, le BIOS peut engendrer le processus de démarrage sans problème ; le système d'exploitation peut alors passer à un fonctionnement RAID logiciel une fois qu'il s'est approprié le contrôle du système.

5.6.3. Gestionnaire de volumes logiques (LVM)

Parmi les autres technologies avancées de stockage figurent le *gestionnaire de volumes logiques* (ou LVM de l'anglais Logical Volume Management). Cette technologie permet de considérer les périphériques physiques de stockage de masse comme des éléments de base sur lesquels différentes configurations de stockage peuvent être construites. Les capacités exactes, qui varient selon l'implémentation spécifique, peuvent inclure le groupement physique du stockage, le redimensionnement de volumes logiques et la migration de données.

5.6.3.1. Groupement physique du stockage

Bien que cette capacité porte des noms différents, le groupement physique du stockage représente la base de toutes les implémentations du LVM. Comme son nom l'indique, les périphériques physiques de stockage de masse peuvent être groupés de manière à créer un ou plusieurs périphériques logiques de stockage. Les périphériques logiques de stockage (ou volumes logiques) peuvent avoir une capacité supérieure à celle de tout périphérique de stockage de masse sous-jacent.

Par exemple, avec deux disques de 100 Go, il est possible de créer un volume logique de 200 Go. Mais il est également possible de créer deux volumes logiques, un de 150 Go et un de 50 Go. En fait, toute combinaison de volumes logiques inférieure ou égale à la capacité totale (soit 200 Go dans notre exemple) est possible. Les choix possibles ne sont en fait limités que par les besoins de votre entreprise.

Un administrateur système peut ainsi considérer tout le stockage comme une entité globale dont il peut utiliser toute quantité souhaitée. En outre, des disques supplémentaires pouvant être ajoutés ultérieurement au stockage, il est relativement facile de toujours disposer d'une quantité de stockage supérieure à celle requise par les utilisateurs.

5.6.3.2. Redimensionnement de volumes logiques

Une des fonctions du LVM très appréciée par la plupart des administrateurs système est sa capacité à attribuer du stockage rapidement, là où il est nécessaire. Dans une configuration de système autre que le LVM, lorsque la mémoire devient insuffisante — dans le meilleur cas de figure — il est nécessaire de transférer des fichiers du périphérique manquant de mémoire vers un autre périphérique disposant d'espace libre. Très souvent, il est nécessaire de changer la configuration elle-même des périphériques

de stockage de masse de votre système ; une tâche qui devra avoir lieu après les heures de bureau normales.

Avec le LVM cependant, il est possible d'augmenter facilement la taille d'un volume logique. Supposons pour un instant que notre groupement de stockage de 200 Go ait été utilisé pour créer un volume logique de 150 Go, laissant ainsi 50 Go en réserve. Dans le cas où le volume logique de 150 Go se remplirait à capacité, le LVM pourrait être utilisé pour agrandir sa taille (disons de 10 Go) sans pour ce faire, changer physiquement la configuration. Selon l'environnement du système d'exploitation, il sera peut-être possible d'effectuer cette opération de manière dynamique ; dans le cas contraire, une courte période d'indisponibilité sera peut être nécessaire afin de pouvoir effectuer le redimensionnement.

5.6.3.3. Migration de données

La plupart des administrateurs système chevronnés seront certes impressionnés par notre présentation de certaines des possibilités offertes par le LVM, mais ils se poseront également la question suivante :

Que se passera-t-il si les disques composant un volume logique tombent en panne ?

Heureusement, la plupart des implémentations du LVM offrent la possibilité de *migrer* des données d'un disque physique particulier vers un autre. Afin que cette opération puisse fonctionner, une capacité de réserve suffisante doit être disponible pour absorber la perte de capacité liée au disque défaillant. Une fois la migration terminée, le disque défaillant peut alors être remplacé, avant d'être rajouté au groupement de stockage disponible.

5.6.3.4. Pourquoi utiliser RAID avec le LVM ?

Étant donné que le LVM a des caractéristiques semblables à celles de RAID (comme la possibilité de remplacer des disques défaillants) et qu'il a certaines caractéristiques lui donnant des capacités que la plupart des implémentations de RAID ne peuvent égaler (comme la capacité à ajouter dynamiquement du stockage supplémentaire à un groupement central de stockage), nombreux sont ceux s'interrogeant sur l'importance actuelle de RAID.

En fait, cette interrogation n'a pas vraiment lieu d'être. RAID et LVM sont en effet, des technologies complémentaires qui, utilisées de concert (de manière semblable aux niveaux RAID imbriqués), permettent de profiter des avantages offerts par les deux technologies.

5.7. Gestion quotidienne du stockage

Au cours de leur activité quotidienne, les administrateurs système doivent surveiller le stockage. À cet égard, il est important de garder à l'esprit les points suivants :

- Contrôle de l'espace libre
- Problèmes des quotas de disque
- Problèmes liés aux fichiers
- Problèmes liés aux répertoires
- Problèmes liés aux sauvegardes
- Problèmes liés à la performance
- Ajout/Suppression de stockage

Les sections suivantes examinent en profondeur chacun de ces points.

5.7.1. Contrôle de l'espace libre

Tout en haut de la liste des tâches qu'un administrateur système doit effectuer quotidiennement devrait se trouver le contrôle du stockage ; en effet, cette tâche est essentielle afin de garantir qu'une quantité suffisante d'espace libre est toujours disponible. En outre, l'espace disque étant une entité très dynamique, il est essentiel de le contrôler fréquemment et régulièrement ; en effet, à un moment donné il peut y avoir plus d'espace disponible que ce dont on a besoin, et peu après, l'espace libre peut être quasiment inexistant.

D'une manière générale, trois raisons peuvent expliquer le manque d'espace libre :

- Consommation excessive par un utilisateur
- Consommation excessive par une application
- Croissance normale de la consommation d'espace

Les sections suivantes examinent chacune de ces raisons de manière plus détaillée.

5.7.1.1. Consommation excessive par un utilisateur

Le degré de propreté varie de personne à personne. Certaines sont horrifiées à la vue d'un grain de poussière sur une table, alors que d'autres trouvent tout à fait normal d'avoir à côté du divan une pile de boîtes d'emballage de pizza datant de l'an dernier. Pour ce qui est du stockage, la situation est similaire :

- Certains utilisateurs sont très économes dans leur consommation de stockage et ne conservent aucun fichier qui n'est pas nécessaire
- D'autres ne semblent jamais pouvoir trouver le temps de supprimer des fichiers dont ils n'ont plus besoin.

Très souvent, lorsqu'un utilisateur est responsable d'une grande utilisation de stockage, la deuxième situation mentionnée ci-dessus en est la raison.

5.7.1.1.1. Approche pour répondre à une consommation excessive par un utilisateur

Pour faire face à une telle situation, un administrateur système doit recourir à ses talents de diplomate d'une part, et à ses compétences au niveau social d'autre part. En effet, les discussions au sujet de l'espace disque ont souvent lieu à un niveau émotionnel pour un certain nombre de raisons : les individus considèrent que l'imposition de restrictions au niveau de l'utilisation du disque rend leur travail plus difficile à effectuer (voire impossible), ils estiment que ces restrictions sont bien trop strictes ou qu'ils n'ont tout simplement pas le temps de nettoyer leurs fichiers.

Dans une telle situation, les meilleurs administrateurs système prennent en considération de nombreux facteurs. Les restrictions sont-elles justes et acceptables pour le type de travail effectué par cette personne ? Est-ce que cette personne utilise son espace disque de manière appropriée ? Existe-t-il un moyen quelconque d'aider cette personne à réduire son utilisation d'espace disque (par exemple, en créant un CD-ROM de sauvegarde de tous les emails datant d'il y a plus d'un an) ? Votre objectif lors de cette conversation est d'essayer de déterminer si une personne quelconque nécessite réellement beaucoup d'espace disque, tout en essayant de vous assurer qu'une personne n'ayant pas vraiment besoin d'une grande quantité de stockage, l'utilise en fait raisonnablement.

Dans tous les cas, il est important que la conversation reste à un niveau professionnel et factuel. Essayez de faire face à la situation de manière polie ("Je comprends tout à fait que tu aies beaucoup de travail, mais il est important que tous les membres du service s'efforcent de ne pas consommer plus de stockage que nécessaire et en fait, la consommation moyenne des employés est à peu près la moitié de la tienne") tout en déplaçant la conversation vers le sujet en question. Assurez-vous de bien offrir de l'aide lorsqu'un manque de connaissances ou d'expérience semble être à l'origine du problème.

Dans une telle situation, une approche sensible mais ferme est souvent plus productive et plus susceptible de produire le résultat souhaité, que le recours à votre autorité en tant qu'administrateur système. Vous trouverez par exemple, qu'il est parfois nécessaire d'établir un compromis entre l'utilisateur et vous-même. Ce compromis peut se présenter sous trois formes :

- Fournir de l'espace temporaire
- Effectuer des sauvegardes pour l'archivage
- Capituler

Il se peut que l'utilisateur soit en mesure de réduire son utilisation s'il dispose d'une certaine quantité d'espace temporaire, utilisable sans aucune restriction. Les individus qui profitent souvent de cette situation estiment qu'une telle mesure leur permet de travailler sans se soucier de l'espace qu'ils utilisent, jusqu'au moment où ils doivent logiquement mettre fin à une telle situation et jugent opportun de faire du nettoyage et de déterminer parmi les fichiers en stockage temporaire, ceux qui sont encore nécessaires et ceux qui ne le sont plus.



Avertissement

Si vous proposez cette solution à un utilisateur, *évit*ez de tomber dans le piège consistant à laisser l'espace temporaire se transformer en espace permanent. Expliquez clairement et fermement que l'espace offert est strictement temporaire et qu'aucune garantie ne peut être offerte quant à la rétention des données ; dans l'espace temporaire, absolument aucune sauvegarde de quelque données que ce soit n'est effectuée.

En fait, de nombreux administrateurs soulignent souvent ce point dans la pratique en supprimant automatiquement tout fichier existant dans le stockage temporaire pour une durée supérieure à une valeur qu'ils définissent (une semaine par exemple).

En d'autres occasions, il se peut que l'utilisateur conserve des fichiers si anciens, qu'il est très peu probable qu'un accès continu à ces derniers soit nécessaire. Assurez-vous d'obtenir la confirmation que tel est bien le cas. Parfois, les utilisateurs eux-mêmes sont responsables du maintien des archives de données anciennes ; dans ce cas, vous devriez, autant que possible, les aider dans leur tâche en fournissant des sauvegardes multiples qui sont alors traitées de la même manière que les sauvegardes d'archive de votre centre de données.

Toutefois, il y a des cas dans lesquels la valeur des données soit discutable. Dans de tels cas, vous estimerez peut-être qu'il est préférable de proposer de faire une sauvegarde spéciale à la place des utilisateurs. Vous effectuerez alors la sauvegarde des données anciennes et remettrez aux utilisateurs les supports de sauvegarde en leur expliquant bien qu'ils en sont responsables et que s'ils ont besoin, à un moment ou à un autre, d'accéder à ces données, ils devront vous demander (ou demander au personnel d'opérations de votre entreprise — selon la procédure appropriée dans votre environnement) de restituer le contenu.

Afin d'éviter que la situation ne se retourne contre vous, il est toutefois nécessaire de garder à l'esprit un certain nombre de points. Tout d'abord, assurez-vous de ne pas inclure des fichiers qui devront très certainement être restaurés ; ne retenez pas des fichiers qui sont *trop* récents. Ensuite, soyez tout à fait certain que vous serez en mesure d'effectuer une restauration, dans le cas où elle serait nécessaire. Une telle approche suppose donc que le type de support de sauvegarde que vous avez choisi sera (autant que vous sachiez) toujours utilisé dans votre centre de données utilisera dans un avenir prévisible.



Astuce

Votre choix de supports de sauvegarde devrait également prendre en compte les technologies permettant à l'utilisateur d'effectuer lui-même la restauration des données. Par exemple, bien que la sauvegarde de plusieurs giga-octets sur un support CD-R demande plus de travail que l'exécution

d'une simple commande les envoyant sur une cartouche à bande de 20 Go, rappelez-vous que dans ce cas, l'utilisateur pourra alors lui-même accéder aux informations sauvegardées sur CD-R à tout moment — et ce sans demander une quelconque intervention de votre part.

5.7.1.2. Utilisation excessive d'espace par une application

Parfois une application est responsable d'une utilisation excessive d'espace. De nombreuses raisons peuvent expliquer une consommation excessive d'espace, y compris :

- Des améliorations au niveau de la fonctionnalité de l'application nécessitent un stockage accru
- Une augmentation du nombre d'utilisateurs employant l'application
- L'application ne réussit pas à nettoyer l'espace après son utilisation, laissant donc sur le disque, des fichiers temporaires qui ne sont plus nécessaires
- L'application a un problème et le bogue entraîne une utilisation anormalement élevée du stockage

Votre tâche consiste à identifier la raison figurant dans cette liste qui s'applique à votre situation. Pour ce faire, la connaissance du statut des applications utilisées dans votre centre de données d'une part, et celle des habitudes de traitement de vos utilisateurs d'autre part, devraient vous permettre d'éliminer un certain nombre de raisons. Il ne reste alors qu'à effectuer un certain travail de détective afin de déterminer comment le stockage a été utilisé. Cette approche devrait réduire considérablement l'envergne de vos recherches.

À ce stade, il est nécessaire de prendre les mesures appropriées pour faire face à la situation : qu'il s'agisse d'ajouter du stockage afin de prendre en charge une application de plus en plus demandée, de contacter les développeurs de l'application afin d'examiner ces caractéristiques de traitement de fichiers ou de créer des scripts pour nettoyer le stockage après l'utilisation de l'application.

5.7.1.3. Croissance normale de l'utilisation

Au long terme, la plupart des entreprises connaissent un certain niveau de croissance. Pour cette raison, il est normal d'anticiper une croissance de l'utilisation du stockage au même rythme. Dans presque toutes les circonstances, un contrôle constant peut révéler le taux d'utilisation moyen du stockage de votre entreprise ; grâce à ce taux d'utilisation, vous devriez être en mesure de déterminer le moment où il sera nécessaire de fournir du stockage supplémentaire, avant d'être vraiment à cours d'espace libre.

Si vous vous trouvez dans la situation où, suite à une croissance normale, vous êtes soudainement à cours d'espace libre, vous n'avez pas fait votre travail.

Toutefois, il arrive que de larges demandes supplémentaires de stockage soient reçues de manière tout à fait imprévue. Peut-être que votre entreprise a fusionné avec une autre entreprise, entraînant des modifications rapides au niveau de l'infrastructure IT (est par conséquent, au niveau du stockage). Peut-être qu'un nouveau projet à haute priorité est apparu soudainement. Des modifications apportées à une application existante ont peut-être entraîné des besoins de stockage beaucoup plus importants.

Quelle que soit la raison, il y aura des situations dans lesquelles vous serez pris au dépourvu. Pour vous préparer à ces situations, essayez de configurer votre architecture de stockage dans un esprit de souplesse maximale. En gardant du stockage de secours à portée de la main (dans la mesure du possible), il est possible de limiter considérablement l'impact de tels événements imprévus.

5.7.2. Problèmes liés aux quotas de disque

Dans bien des cas, la première chose qui vient à l'esprit lorsqu'on parle de quotas de disque, est l'emploi de ces derniers pour forcer les utilisateurs à nettoyer leurs répertoires. Bien qu'ils puissent être en effet utilisés dans ce sens dans certains sites, les quotas de disque permettent avant tout d'examiner le problème de l'utilisation de l'espace disque sous un autre angle. Comment expliquer que des applications, pour une raison ou une autre, consomment trop d'espace disque ? Il n'est pas rare en effet que des applications rencontrent des problèmes se traduisant par une consommation de tout l'espace disque disponible. Dans de tels cas, les quotas de disque peuvent aider à limiter les dégâts causés par de telles applications au comportement anormal, en les forçant à s'arrêter *avant* qu'elles ne monopolisent tout l'espace libre du disque.

En ce qui concerne l'implémentation et de la gestion des quotas de disque l'aspect le plus difficile se situe au niveau des limites elles-mêmes. Quelle devrait être leur valeur ? Une approche quelque peu simpliste consisterait à diviser l'espace disque par le nombre d'utilisateurs et/ou de groupes qui l'utilisent et à se servir du résultat obtenu pour déterminer le quota applicable à chaque utilisateur. Par exemple, si le système dispose d'un disque dur de 100 Go qui est utilisé par 20 personnes, chacune d'elles devrait se voir attribuer un quota de disque d'une taille inférieure ou égale à 5 Go. De cette manière, chaque utilisateur aura la garantie de pouvoir utiliser 5 Go (bien que le disque serait à ce stade rempli à 100%).

Pour les systèmes d'exploitation qui prennent en charge le principe des quotas temporaires, il est possible d'utiliser, en plus du quota permanent, un quota temporaire d'une limite légèrement supérieure — disons 7,5 Go, tout en maintenant un quota permanent à 5 Go. Cette approche offre l'avantage de restreindre la consommation permanente des utilisateurs à leur pourcentage de disque, tout en leur offrant une certaine souplesse lorsqu'ils atteignent (ou dépassent) leur limite. En utilisant les quotas de disque de la sorte, vous allouez plus d'espace que la quantité réellement disponible. En effet, le quota temporaire est de 7,5 Go. Si tous les utilisateurs venaient à dépasser en même temps, leur quota permanent et essaieraient d'atteindre leur quota temporaire, ce disque de 100 Go devrait en fait avoir une taille de 150 Go afin de permettre à tous les utilisateurs d'atteindre leur quota temporaire en même temps.

Ceci étant, dans la pratique tous les utilisateurs ne dépassent pas leur quota permanent en même temps, de sorte qu'il est tout à fait raisonnable d'utiliser une approche basée sur une quantité de disque légèrement supérieure à la quantité réellement disponible. Il va de soi que le choix de ces quotas permanents et temporaires dépend de l'administrateur système, dans la mesure où la situation de chaque site et de chaque communauté d'utilisateurs est différente.

5.7.3. Problèmes liés aux fichiers

Les administrateurs système doivent souvent faire face à des problèmes liés aux fichiers. Parmi ces problèmes figurent :

- Accès aux fichiers
- Partage de fichiers

5.7.3.1. Accès aux fichiers

Les problèmes liés à l'accès aux fichiers font en général tous partie d'un même scénario — un utilisateur se voit refuser l'accès à un fichier mais estime qu'il devrait être autorisé à y accéder.

Souvent, il s'agit d'une situation dans laquelle l'utilisateur #1 souhaite donner la copie d'un fichier à l'utilisateur #2. Dans la plupart des entreprises, la capacité d'un utilisateur à accéder aux fichiers d'un autre utilisateur est strictement réduite, d'où ce genre de problème.

Dans une telle situation, il est possible d'adopter une des trois approches suivantes :

- L'utilisateur #1 apporte les modifications nécessaires afin que l'utilisateur #2 puisse avoir accès au fichier, quel que soit son emplacement actuel.
- Une zone d'échange de fichier est créée pour cet usage précis ; l'utilisateur #1 y place une copie du fichier qui peut à son tour être copiée par l'utilisateur #2.
- L'utilisateur #1 envoie par email une copie du fichier à l'utilisateur #2 .

Il existe un problème avec la première approche — selon la manière dont l'accès est donné, l'utilisateur #2 aura peut-être un accès total à tous les fichiers de l'utilisateur #1. Même pire, il se peut que l'opération ait été effectuée de telle sorte que *tous* les utilisateurs de votre entreprise ont désormais accès aux fichiers de l'utilisateur #1. Et pis encore, il se peut que ce droit d'accès ne soit pas rétablie à sa valeur d'origine, une fois que l'utilisateur #2 n'a plus besoin des privilèges ; si tel est le cas, tous les autres utilisateurs continuent à avoir un accès permanent aux fichiers de l'utilisateur #1. Regrettablement, lorsque les utilisateurs sont responsables de ce type de situation, la sécurité n'est que très rarement leur première préoccupation.

La deuxième approche permet d'éliminer le problème lié au fait que tous les autres utilisateurs peuvent avoir accès à l'ensemble des fichiers de l'utilisateur #1. Cependant, une fois que le fichier se trouve dans la zone d'échange de fichiers, il est lisible (et selon les permissions, il peut même être écrit) par tous les autres utilisateurs. Cette approche pose également le problème du remplissage à capacité de la zone d'échange, causé par l'oubli courant des utilisateurs de supprimer leurs fichiers une fois utilisés.

Finalement, bien que la troisième approche apparaisse au premier abord comme une solution délicate, elle s'avère être dans bien des cas la meilleure solution. Avec l'apparition de protocoles aux normes de l'industrie permettant d'envoyer de pièces jointes par email et celle de programmes de messagerie plus intelligents, l'envoi par email de toute sorte de fichiers est désormais une opération quasiment sans risque qui ne nécessite aucune intervention de la part d'un administrateur système. Bien sûr, il y a toujours le risque qu'un utilisateur essaie d'envoyer un fichier de base de données de 1 Go aux 150 membres du service des finances, et dans ce sens, il serait probablement prudent d'éduquer les utilisateurs sur le sujet (et peut-être même d'imposer des limites au niveau de la taille des pièces jointes envoyées électroniquement). Aucune de ces approches n'examine néanmoins la situation dans laquelle deux utilisateurs ou plus nécessitent un accès continu à un seul fichier. Dans ces cas particuliers, il est nécessaire de recourir à d'autres méthodes.

5.7.3.2. Partage de fichiers

Lorsque de multiples utilisateurs doivent partager une copie unique d'un fichier, autoriser l'accès au fichier en modifiant les permissions n'est pas la meilleure approche. Il est plutôt recommandé de formaliser le statut partagé du fichier, et ce, pour plusieurs raisons :

- Les fichiers partagés depuis le répertoire d'un utilisateur risquent de disparaître de manière inattendue lorsque l'utilisateur quitte l'entreprise ou effectue tout simplement une réorganisation de ses fichiers.
- Le maintien d'un accès partagé pour plus d'un ou deux utilisateurs supplémentaires devient une opération difficile, entraînant au long terme le problème de tâches inutiles à effectuer, chaque fois que les utilisateurs du partage changent de responsabilités.

Dans de telles conditions, la meilleure approche consiste à :

- Demander à l'utilisateur d'origine d'abandonner la propriété directe du fichier
- Créer un groupe qui sera propriétaire du fichier
- Placer le fichier dans un répertoire partagé qui est la propriété du groupe
- Inclure dans le groupe, tous les utilisateurs nécessitant l'accès au fichier

Cette approche qui fonctionne aussi bien pour des fichiers multiples que pour des fichiers uniques, peut être utilisée pour implémenter du stockage partagé lors de projets complexes et de grande envergure.

5.7.4. Ajout/Suppression de stockage

Étant donné que le besoin d'espace disque supplémentaire est constant, il est souvent nécessaire pour un administrateur système d'ajouter de l'espace disque, tout en supprimant d'anciens disques plus petits. Cette section fournit un aperçu du processus de base lié à l'ajout et à la suppression de stockage.



Remarque

Sur de nombreux systèmes d'exploitation, les périphériques de stockage de masse sont désignés en fonction de leur connexion au système. Par conséquent, l'ajout ou la suppression de périphériques de stockage de masse peut entraîner des changements inattendus au niveau des noms de périphériques. Ainsi, lors de telles opérations, assurez-vous de toujours bien passer en revue (et de mettre à jour le cas échéant) les références aux noms de périphériques que votre système d'exploitation utilise.

5.7.4.1. Ajout de stockage

Le processus consistant à ajouter du stockage à un système informatique est relativement simple. Tels en sont les étapes élémentaires :

1. Installation du matériel
2. Partitionnement
3. Formatage d'une ou plusieurs partition(s)
4. Mise à jour de la configuration du système
5. Modification du programme de sauvegarde

Les sections suivantes examinent chacune de ces étapes en détails.

5.7.4.1.1. Installation du matériel

Avant que toute opération ne puisse être effectuée, le nouveau disque dur doit être installé et accessible. Bien que de nombreuses configurations matérielles différentes soient possibles, les sections suivantes n'aborderont que les deux situations les plus courantes — l'ajout d'un disque dur ATA ou d'un disque dur SCSI. Même avec d'autres configurations, les étapes élémentaires décrites ci-dessous demeurent applicables.



Astuce

Indépendamment du matériel de stockage utilisé, vous devriez toujours prendre en considération la charge qu'un nouveau disque dur ajoute au sous-système d'E/S de votre ordinateur. D'une manière générale, il est recommandé d'essayer de répartir la charge des E/S du disque sur tous les canaux/bus disponibles. Du point de vue des performances, les résultats obtenus en procédant de la sorte sont largement supérieurs à ceux obtenus en mettant tous les disques durs sur un canal et en laissant un autre canal vide et inactif.

5.7.4.1.1.1. Ajout de disques dur ATA

Les disques durs ATA sont essentiellement utilisés dans les bureaux et les systèmes serveurs de bas niveau. Presque tous les systèmes appartenant à ces classes ont des contrôleurs ATA intégrés avec des canaux ATA multiples — généralement deux ou quatre.

Chaque canal peut prendre en charge deux périphériques — un maître et un esclave. Les deux périphériques sont branchés au canal à l'aide d'un seul câble. La première étape consiste donc à identifier les canaux ayant de l'espace disponible pour accueillir le disque dur supplémentaire. Trois situations différentes sont possibles :

- Il existe un canal auquel un seul disque dur est connecté
- Il existe un canal auquel aucun disque dur n'est connecté
- Il n'y a pas d'espace disponible

La première situation est généralement la plus simple, dans la mesure où il est fort possible que le câble déjà en place dispose d'un connecteur non utilisé sur lequel le nouveau disque dur peut être branché. Toutefois, si le câble en place dispose seulement de deux connecteurs (un pour le canal et un pour le disque dur déjà installé) il est nécessaire de remplacer le câble existant par un modèle à trois connecteurs.

Avant d'installer le nouveau disque dur, assurez-vous que les deux disques partageant le canal sont configurés de manière adéquate (un en tant que maître et l'autre en tant qu'esclave).

La deuxième situation est légèrement plus compliquée car il faut un câble pour pouvoir connecter le disque dur au canal. Le nouveau disque dur peut être configuré en tant que maître ou esclave (bien que traditionnellement, le premier disque dur sur un canal soit configuré comme le maître).

Dans la troisième situation, il ne reste aucun espace disponible pour accueillir un disque dur supplémentaire. Il est alors nécessaire de prendre une décision. Que décidez-vous de faire ?

- Vous vous procurez une carte contrôleur ATA et vous l'installez ?
- Vous remplacez un des disques durs installés par un nouveau disque d'une capacité supérieure ?

L'ajout d'une carte contrôleur suppose que vous vérifiez préalablement la compatibilité matérielle, la capacité physique et la compatibilité logicielle. En d'autres termes, il faut que la carte soit non seulement compatible avec les fentes (aussi appelées slots) du bus de votre ordinateur mais il faut également qu'une fente existe pour son insertion et que votre système d'exploitation d'exploitation la prenne en charge. Le remplacement d'un disque dur installé soulève un problème unique : que faire des données stockées sur le disque ? Pour résoudre ce problème, une des approches suivantes peut être adoptée :

- Vous pouvez enregistrer les données sur un périphérique de sauvegarde et les restaurer ultérieurement, une fois le nouveau disque dur installé ;
- Vous pouvez utiliser le réseau pour copier les données sur un autre système disposant d'une quantité d'espace libre suffisante et les restaurer ensuite une fois le nouveau disque dur installé ;
- Vous pouvez utiliser l'espace physique occupé par un troisième disque dur en :
 1. Retirant temporairement le troisième disque dur
 2. Installant temporairement le nouveau disque dur à sa place
 3. Copiant les données sur le nouveau disque dur
 4. Retirant l'ancien disque dur
 5. Remplaçant l'ancien disque dur par le nouveau disque
 6. Réinstallant le troisième disque dur temporairement retiré

- Vous pouvez temporairement installer le disque dur d'origine ainsi que le nouveau disque dur dans un autre ordinateur, copier les données sur le nouveau disque dur et ensuite installer ce dernier dans l'ordinateur d'origine.

Comme vous pouvez le constater, de nombreuses opérations sont parfois nécessaires afin de placer les données (et le nouveau matériel) là où elles sont supposées se trouver.

5.7.4.1.1.2. Ajout de disques durs SCSI

Les disques durs SCSI sont généralement utilisés dans les postes de travail ou systèmes serveur de haut niveau. Contrairement aux systèmes ATA, les systèmes SCSI peuvent ou non disposer de contrôleurs SCSI intégrés ; certains en sont dotés alors que d'autres utilisent une carte contrôleur SCSI indépendante.

Les capacités des contrôleurs SCSI (qu'ils soient intégrés ou non) diffèrent grandement. Ils peuvent fournir un bus SCSI large ou étroit. La vitesse de bus peut être normale, rapide, ultra, ultra2 ou même ultra160.

Si vous ne connaissez pas bien ces termes (ils ont été examinés brièvement dans la Section 5.3.2.2), vous devez déterminer les capacités de votre configuration matérielle et choisir un nouveau disque dur en conséquence. À cet égard, la documentation de votre système et/ou de l'adaptateur SCSI représente la meilleure ressource pour obtenir de genre d'information.

Vous devez alors non seulement déterminer le nombre de bus SCSI disponibles sur votre système mais également identifier ceux disposant d'espace libre pour accueillir un nouveau disque dur. Le nombre de périphériques pris en charge par un bus SCSI varie en fonction de sa largeur :

- Bus SCSI étroit (8 bit) — 7 périphériques (plus contrôleur)
- Bus SCSI large (16 bit) — 15 périphériques (plus contrôleur)

La première étape consiste à déterminer quels bus ont de l'espace disponible pour accueillir un disque dur supplémentaire. Une des trois situations suivantes est possible :

- Il y a un bus avec un nombre de disques durs inférieur au nombre qu'il peut accueillir
- Il y a un bus qui n'est connecté à aucun disque dur
- Il n'y a pas d'espace disponible sur quel que bus que ce soit

La première situation est généralement la plus simple, dans la mesure où il est fort possible que le câble déjà en place dispose d'un connecteur non utilisé sur lequel le nouveau disque dur peut être branché. Toutefois, si le câble en place ne dispose pas d'un connecteur libre, il est alors nécessaire de remplacer le câble existant par un modèle ayant au moins un connecteur supplémentaire.

La deuxième situation est légèrement plus compliquée pour la simple raison qu'un câble doit être présent afin de pouvoir connecter le disque dur au bus.

S'il ne reste aucun espace disponible pour un disque dur supplémentaire, il est alors nécessaire de prendre une décision. Laquelle prenez-vous ?

- Vous vous procurez une carte contrôleur SCSI et l'installez
- Vous remplacez un des disques durs installés par un nouveau disque à capacité supérieure

L'ajout d'une carte contrôleur suppose que vous vérifiez préalablement la compatibilité matérielle, la capacité physique et la compatibilité logicielle. En d'autres termes, il faut que la carte soit non seulement compatible avec les fentes (aussi appelées slots) du bus de votre ordinateur mais il faut également qu'une fente existe pour son insertion et que votre système d'exploitation d'exploitation la prenne en charge.

Le remplacement d'un disque dur installé soulève un problème unique : que faire des données stockées sur le disque ? Pour résoudre ce problème, une des approches suivantes peut être adoptée :

- Vous pouvez enregistrer les données sur un périphérique de sauvegarde et les restaurer ensuite une fois le nouveau disque dur installé ;
- Vous pouvez utiliser le réseau pour copier les données sur un autre système disposant d'une quantité d'espace libre suffisante et les restaurer ensuite une fois le nouveau disque dur installé ;
- Vous pouvez utiliser l'espace physique occupé par un troisième disque dur en :
 1. Retirant temporairement le troisième disque dur
 2. Installant temporairement le nouveau disque dur à sa place
 3. Copiant les données sur le nouveau disque dur
 4. Retirant l'ancien disque dur
 5. Remplaçant l'ancien disque dur par le nouveau disque
 6. Réinstallant le troisième disque dur temporairement retiré
- Vous pouvez temporairement installer le disque dur d'origine ainsi que le nouveau disque dur dans un autre ordinateur, copier les données sur le nouveau disque dur et ensuite installer ce dernier dans l'ordinateur d'origine.

Une fois que vous disposez d'un connecteur libre sur lequel brancher le nouveau disque dur, vous devez vous assurer que l'ID SCSI du périphérique est réglé sur la valeur adéquate. Pour ce faire, il est nécessaire de connaître la valeur que tous les autres périphériques sur le bus (y compris le contrôleur) utilisent pour leur ID SCSI. La meilleure manière de procéder consiste à avoir accès au BIOS du contrôleur SCSI. Il est généralement possible de le faire en pressant une combinaison spécifique de touches lors de la séquence de mise sous tension du système. Il est alors possible de voir la configuration du contrôleur SCSI ainsi que tous les périphériques qui sont reliés à l'ensemble de ses bus.

Ensuite, vous devez vous assurer que la terminaison des bus est correcte. Lors de l'ajout d'un nouveau disque dur, la règle est en fait assez simple — si le nouveau disque dur est le dernier (ou le seul) périphérique du bus, sa terminaison doit être activée. Dans le cas contraire, la terminaison doit être désactivée.

Vous pouvez maintenant passer à l'étape suivante du processus — le partitionnement de votre nouveau disque dur.

5.7.4.1.2. Partitionnement

Une fois que le disque dur a été installé, c'est le moment de créer une ou plusieurs partitions pour mettre l'espace disponible à la disposition de votre système d'exploitation. Bien que les outils pour ce faire diffèrent selon les systèmes d'exploitation, les étapes de base décrites ci-après restent les mêmes :

1. Sélectionnez le nouveau disque dur
2. Affichez la table actuelle des partitions du disque dur pour vous assurer que le disque dur choisi pour le partitionnement est bien le disque approprié
3. Supprimez toute partition non souhaitée qui pourrait déjà se trouver sur le nouveau disque dur
4. Créez la ou les nouvelle(s) partition(s) en vous assurant de bien préciser la taille et le type de partition souhaités

5. Enregistrez vos modifications et quittez le programme de partitionnement



Avertissement

Lors du partitionnement d'un nouveau disque dur, il est *primordial* d'être absolument certain que le disque sur le point d'être partitionné est bien celui que vous souhaitez utiliser pour cette opération. Dans le cas contraire, vous risqueriez de partitionner par erreur un disque dur qui est déjà utilisé, entraînant par là-même la perte des données contenues.

Assurez-vous également de bien avoir choisi la meilleure taille de partition possible. Réfléchissez bien à ce point avant de prendre une décision car il est beaucoup plus difficile de modifier ultérieurement la taille d'une partition, que de passer un peu de temps maintenant à considérer la chose.

5.7.4.1.3. Formatage d'une ou plusieurs partition(s)

À ce stade, une ou plusieurs partitions ont été créées sur le nouveau disque dur. Toutefois, avant de vraiment pouvoir utiliser l'espace contenu sur cette/ces partition(s), il est nécessaire de la/les formater. Avec le formatage, vous choisissez le système de fichiers spécifiques qui sera utilisé au sien de chaque partition. En tant que tel, ce moment est crucial dans la vie de tout disque dur ; en effet, les choix que vous ferez maintenant ne pourront pas être modifiés plus tard, sans devoir effectuer de nombreuses opérations.

Le processus de formatage lui-même est effectué en exécutant un programme utilitaire ; les étapes qui composent ce processus varient selon le système d'exploitation utilisé. Une fois le formatage terminé, le disque dur est alors configuré de manière adéquate pour son utilisation.

Avant de poursuivre, il est toujours préférable de vérifier le résultat des opérations en ayant accès à la partition (ou aux partitions) pour vous assurez que les opérations effectuées ont bien produit le résultat souhaité.

5.7.4.1.4. Mise à jour de la configuration du système

Dans le cas où vous devriez modifier la configuration de votre système d'exploitation afin de pouvoir utiliser le nouveau stockage qui vient d'être ajouté, maintenant est le moment de le faire.

Vous pouvez désormais avoir la quasi certitude que le système d'exploitation est correctement configuré pour permettre l'accès au nouveau stockage chaque fois que le système démarrera (ceci étant, il est toujours prudent d'effectuer un redémarrage rapide, si vous pouvez vous le permettre — juste pour jouer la carte de la sécurité).

La section suivante examine une des étapes les plus communément oubliées dans le processus d'ajout d'un nouveau stockage.

5.7.4.1.5. Modification du programme de sauvegarde

À condition que le nouveau stockage soit utilisé pour contenir des données dignes d'être sauvegardées, c'est maintenant le moment opportun d'effectuer les changements nécessaires à vos procédures de sauvegarde et de vous assurer que le nouveau stockage sera effectivement sauvegardé. La nature exacte des opérations à effectuer pour permettre une telle situation dépend de la manière dont les sauvegardes sont créées sur votre système. Toutefois, lorsque vous apportez les modifications nécessaires, gardez bien à l'esprit les points suivants :

- Prenez en compte la fréquence maximale à laquelle les sauvegardes devraient être effectuées

- Déterminez le type de sauvegarde le plus approprié à votre situation (seulement des sauvegardes complètes, des sauvegardes incrémentielles complètes, des sauvegardes différentielles complètes, etc.)
- Prenez en compte l'impact du stockage supplémentaire sur l'utilisation du support de sauvegarde, particulièrement au fur et à mesure qu'il se remplit
- Estimez si le stockage supplémentaire pourrait entraîner un rallongement des opérations de sauvegarde allant au-delà du temps qui leur est alloué
- Assurez-vous que toutes les personnes concernées sont bien averties de ces modifications (d'autres administrateurs système, le personnel d'opérations, etc.)

Une fois que toutes ces tâches ont été effectuées, votre stockage est prêt à l'emploi.

5.7.4.2. Suppression de stockage

La suppression d'espace disque d'un système est une opération relativement simple dont la plupart des étapes correspondent plus ou moins à la séquence d'installation (mais cette fois-ci, dans le sens inverse cela va de soi) :

1. Retirez du disque dur, toute donnée devant être enregistrée
2. Modifiez le programme de sauvegarde afin que le disque dur ne soit plus sauvegardé
3. Mettez à jour la configuration du système
4. Effacez le contenu du disque dur
5. Retirez le disque dur

Comme vous pouvez le constater, par rapport au processus d'installation, le processus de suppression de stockage comporte un certain nombre d'étapes supplémentaires. Ces dernières sont examinées dans les sections suivantes.

5.7.4.2.1. Transfert des données du disque dur

Dans le cas où des données stockées sur le disque dur devraient être enregistrées, la première tâche à effectuer consiste à déterminer l'endroit vers lequel ces données devraient être transférées. Cette décision dépend en grande partie de l'utilisation future de ces dernières. Par exemple, si les données ne seront plus vraiment utilisées de manière active, elles devraient être archivées, probablement de la même manière que vos sauvegardes système. Maintenant est donc le moment opportun de penser aux durées de rétention adéquates des données de cette dernière sauvegarde.



Astuce

Prenez bien en considération, outre toutes les directives concernant la rétention de données en vigueur dans votre entreprise, les obligations juridiques imposant la rétention de données pour une certaine durée. Dans de telles circonstances, n'oubliez pas de consulter les membres du service responsable des données lorsqu'elles étaient encore utilisées ; ces derniers devraient en effet connaître la durée de rétention appropriée.

D'autre part, si les données sont encore utilisées, elles devraient se trouver sur le système approprié afin de toujours pouvoir être utilisées. Bien sûr, si tel est le cas, il serait peut-être plus simple de déplacer les données en réinstallant le disque dur sur le nouveau système. Si vous choisissez cette option, vous devriez effectuer auparavant une sauvegarde complète des données — il s'est déjà produit des situations où des personnes ont laissé tomber des disques durs contenant de nombreuses données

importantes (entraînant par là même la perte totale des données) alors qu'elles les déplaçaient tout simplement d'un endroit à un autre dans le centre de données.

5.7.4.2.2. Effacement du contenu du disque dur

Que le disque dur contienne des données importantes ou non, il est toujours recommandé d'effacer le contenu du disque dur avant de le réutiliser ou de l'abandonner. Outre le fait que cette mesure est évidemment nécessaire pour garantir la disparition totale de toute information confidentielle stockée sur le disque, elle offre également l'opportunité de vérifier l'état du disque dur en recherchant, grâce à un test de lecture-écriture, les blocs endommagés présents sur l'ensemble du disque dur.



Important

De nombreuses entreprises (et ministères) disposent de méthodes spécifiques pour effacer des données contenues sur des disques durs et autres supports de stockage d'informations. Assurez-vous de *toujours* comprendre et respecter ces obligations ; dans bien des cas, leur non respect a des conséquences juridiques. L'exemple décrit ci-dessus ne devraient en aucun cas être considéré comme la méthode absolue pour effacer un disque dur.

En outre, dans le cas d'entreprises traitant des informations confidentielles, il est possible que la disposition finale du disque dur soit soumise à certaines procédures d'ordre juridique (telles que la destruction physique du disque). Dans de tels cas, le service responsable de la sécurité au sein de votre entreprise devrait pouvoir vous aider en la matière.

5.8. Commentaires sur les sauvegardes...

Un des éléments les plus importants à prendre en compte en ce qui concerne le stockage disque est la sauvegarde. Ce sujet n'a pas été abordé ici, car une section détaillée (la Section 8.2) y a été consacré.

5.9. Informations spécifiques à Red Hat Enterprise Linux

Selon votre expérience en matière d'administration système, la gestion du stockage sous Red Hat Enterprise Linux représente une opération dont vous avez l'habitude ou au contraire, une opération entièrement nouvelle. Cette section aborde différents aspects de l'administration du stockage qui sont spécifiques à Red Hat Enterprise Linux.

5.9.1. Conventions de nommage des périphériques

Comme c'est le cas avec tous les systèmes d'exploitation de type Linux, Red Hat Enterprise Linux utilise des fichiers de périphérique afin d'accéder à tout élément matériel (y compris les disques durs). Il est important de noter ici que les conventions de nommage des périphériques de stockage connectés varient quelque peu selon qu'il s'agisse d'une implémentation Linux ou d'une implémentation autre que Linux. Sous Red Hat Enterprise Linux, le nommage des périphériques s'effectue selon les informations fournies ci-dessous.



Remarque

Sous Red Hat Enterprise Linux, les noms de périphériques sont déterminés au démarrage.

Par conséquent, toute modification apportée à la configuration matérielle du système peuvent entraîner un changement du nom de périphérique lorsque le système redémarre. Pour cette raison, des problèmes peuvent surgir si les références à un nom de périphérique contenues dans les fichiers de configuration ne sont pas mises à jour de manière adéquate.

5.9.1.1. Fichiers de périphérique

Sous Red Hat Enterprise Linux, les fichiers de périphérique des disques durs se trouvent dans le répertoire `/dev/`. Le format de chaque nom de fichier dépend de certains éléments du matériel lui-même et de la manière dont il est configuré. À ce niveau, les éléments suivants ont une grande importance :

- Type de périphérique
- Unité
- Partition

5.9.1.1.1. Type de périphérique

Les deux premières lettres du nom du fichier de périphérique font référence au type spécifique de périphérique. Pour les disques durs, les deux types de périphériques les plus courants sont les suivants :

- `sd` — Le périphérique est basé sur SCSI
- `hd` — Le périphérique est basé sur ATA

De plus amples informations sur ATA et SCSI sont disponibles dans la Section 5.3.2.

5.9.1.1.2. Unité

Après les deux lettres représentant le type de périphérique figurent une ou deux lettres identifiant l'unité particulière. L'identifiant d'unité commence avec la lettre "a" pour la première unité, ensuite la lettre "b" pour la seconde et ainsi de suite. Le premier disque dur de votre système sera peut-être par conséquent identifié en tant que `hda` ou `sda`.



Astuce

En raison de la capacité de SCSI à traiter un grand nombre de périphériques, un deuxième caractère a dû être ajouté à l'unité, afin de prendre en charge des systèmes auxquels sont reliés plus de 26 périphériques SCSI. Par conséquent, les 26 premiers disques durs SCSI d'un système seront identifiés en tant que `sda` jusqu'à `sdz`, les 26 disques suivants eux en tant que `sdaa` jusqu'à `sdaz` et ainsi de suite.

5.9.1.1.3. Partition

La dernière partie du nom de fichier d'un périphérique consiste en un nombre représentant une partition spécifique du périphérique. Ce nombre, commençant par "1," peut être composé d'un ou deux chiffres, en fonction du nombre de partitions enregistrées sur le périphérique. Après avoir compris le format des noms de fichiers de périphérique, il est facile d'identifier le périphérique auquel chaque nom de fichier correspond. Ci-dessous figurent quelques exemples :

- `/dev/hda1` — La première partition existant sur le premier disque ATA
- `/dev/sdb12` — La douzième partition existant sur le second disque SCSI
- `/dev/sdad4` — La quatrième partition existant sur le trentième disque SCSI

5.9.1.1.4. Accès au périphérique entier

Il y a des situations dans lesquelles il est nécessaire d'avoir accès au périphérique tout entier et pas seulement à une partition spécifique. C'est généralement le cas lorsque le périphérique n'est pas partitionné ou lorsqu'il ne prend pas en charge les partitions standard (comme un lecteur de CD-ROM). Dans ces cas précis, le numéro de la partition est omis :

- `/dev/hdc` — Le troisième périphérique ATA tout entier
- `/dev/sdb` — Le deuxième périphérique SCSI tout entier

Toutefois, la plupart des disques durs utilisent des partitions (de plus amples informations sur le partitionnement sous Red Hat Enterprise Linux sont disponibles dans la Section 5.9.6.1).

5.9.1.2. Alternatives aux noms de fichiers de périphérique

Étant donné que l'ajout ou la suppression de périphériques de stockage de masse peuvent entraîner des modifications au niveau des noms de fichier de périphérique associés aux périphériques existants, le stockage risque de ne pas être disponible lorsque le système redémarre. Ci-après figure l'exemple d'une séquence d'événements entraînant ce genre de problème :

1. L'administrateur système ajoute un nouveau contrôleur SCSI afin que deux nouveaux disques SCSI puissent être ajoutés au système (le bus SCSI est complètement rempli)
2. Les disques SCSI d'origine (y compris le premier disque du bus `/dev/sda`) ne sont modifiés d'aucune manière
3. Le système est redémarré
4. Le disque SCSI précédemment identifié comme `/dev/sda` porte désormais un nouveau nom, car le premier disque SCSI sur le nouveau contrôleur s'appelle maintenant `/dev/sda`

En théorie, cette situation semble représenter un véritable problème. En pratique, ce n'est toutefois que très rarement un problème et ce, pour un certain nombre de raisons. Premièrement, des reconfigurations matérielles de ce type se produisent rarement. Deuxièmement, il est probable que l'administrateur système ait programmé des temps d'arrêt du système afin d'effectuer les changements nécessaires ; les temps d'arrêt nécessitent une planification rigoureuse afin de garantir que le travail en cours ne prendra pas plus longtemps que le temps imparti. La planification a aussi pour avantage indirect de mettre à jour tout problème lié au changement de nom des périphériques.

Ceci étant, certaines entreprises et configurations de système risquent de rencontrer ce genre de problème plus que d'autres. Les entreprises nécessitant de fréquentes reconfigurations de stockage afin de satisfaire leurs besoins, utilisent souvent du matériel permettant une reconfiguration sans temps d'arrêt. Ce genre de matériel *enfichable à chaud* (aussi appelé hotpluggable) permet d'ajouter ou de

supprimer le stockage. Mais dans de telles circonstances, certains aspects du nommage de périphérique peuvent poser un problème. Heureusement, Red Hat Enterprise Linux inclut des fonctionnalités qui limitent les problèmes liés au changement de nom des périphériques.

5.9.1.2.1. Étiquettes de système de fichiers

Certains systèmes de fichiers (qui seront examinés de manière plus détaillée dans la Section 5.9.2) ont la capacité de stocker une *étiquette* (aussi appelée *label*) — une chaîne de caractères qui peut être utilisée pour identifier de manière unique les données que le système de fichiers contient. Les étiquettes peuvent alors être utilisées lors du montage du système de fichiers, éliminant par là-même, le besoin d'utiliser le nom de périphérique.

Les étiquettes des systèmes de fichiers fonctionnent bien ; toutefois, elles doivent être absolument uniques dans tout le système. Si, à un moment ou à un autre, plus d'un système de fichiers ont la même étiquette, vous ne pourrez peut-être pas avoir accès au système de fichiers que vous essayiez d'utiliser. Notez également que les configurations de système n'utilisant pas les systèmes de fichiers (certaines bases de données, par exemple) ne peuvent pas profiter des avantages associés à l'utilisation des étiquettes de systèmes de fichiers.

5.9.1.2.2. Utilisation de `devlabel`

Le logiciel `devlabel` tente de résoudre le problème du nommage des périphériques, mais d'une manière différente de celle basée sur les étiquettes de systèmes de fichiers. Le logiciel `devlabel` est exécuté par Red Hat Enterprise Linux lors de chaque redémarrage du système (et chaque fois que des périphériques enfichables à chaud sont insérés ou retirés).

Lorsque `devlabel` tourne, il lit son fichier de configuration (`/etc/sysconfig/devlabel`) afin d'obtenir la liste des périphériques dont il est responsable. Pour chaque périphérique figurant dans la liste, il existe un lien symbolique (choisi par l'administrateur système) et un identifiant universel unique, UUID (de l'anglais Universal Unique Identifier).

La commande `devlabel` garantit que le lien symbolique renvoie toujours au périphérique spécifié à l'origine — et ce, même si le nom du périphérique a changé. De cette manière, un administrateur système peut configurer un système de sorte qu'il renvoie à `/dev/projdisk` plutôt qu'à `/dev/sda12`, par exemple.

Étant donné que l'UUID est obtenu directement du périphérique, il suffit à `devlabel` de rechercher dans le système l'UUID correspondant et de mettre à jour le lien symbolique en conséquence.

Pour de plus amples informations sur `devlabel`, reportez-vous au *Guide d'administration système de Red Hat Enterprise Linux*.

5.9.2. Éléments de base des systèmes de fichiers

Étant donné que Red Hat Enterprise Linux inclut la prise en charge de nombreux systèmes de fichiers très utilisés, il est possible d'accéder facilement aux systèmes de fichiers d'autres systèmes d'exploitation.

Cette prise en charge est particulièrement utile lors de scénarios impliquant des systèmes à double démarrage et lors de la migration de fichiers d'un système d'exploitation à un autre.

Parmi les systèmes de fichiers pris en charge figurent (entre autres) :

- EXT2
- EXT3

- NFS
- ISO 9660
- MSDOS
- VFAT

Les sections suivantes examinent de manière plus détaillée les systèmes de fichiers les plus utilisés.

5.9.2.1. EXT2

Jusqu'à récemment, le système de fichiers ext2 était le système de fichiers standard pour Linux. En tant que tel, il a fait l'objet de si nombreux tests qu'il est désormais considéré comme l'un des systèmes de fichiers les plus robustes qu'il soit à l'heure actuelle.

Ceci étant, il n'existe pas de système de fichiers parfait et ext2 ne fait pas exception à la règle. Un problème souvent mentionné en ce qui concerne le système de fichiers ext2, est le fait qu'il doit faire l'objet de longues vérifications d'intégrité de système de fichiers lorsque le système n'a pas été éteint selon la procédure normale. Alors que cette obligation n'est pas particulière à ext2, la popularité de ce système de fichiers et l'arrivée de disques durs plus grands ont entraîné un rallongement grandissant des vérifications d'intégrité des systèmes de fichiers. Un changement devenait donc absolument nécessaire.

La section suivante examine l'approche adoptée pour résoudre ce problème sous Red Hat Enterprise Linux.

5.9.2.2. EXT3

Le système de fichiers ext3 est une version améliorée du système de fichiers ext2 qui a été obtenue en ajoutant des capacités de journalisation au code initial de ext2, qui a lui déjà fait ses preuves. En tant que système de fichiers doté de capacités de journalisation, ext3 maintient en permanence le système de fichiers dans un état homogène, éliminant ainsi le besoin d'effectuer de longues opérations de vérification d'intégrité du système de fichiers.

Pour ce faire, toutes les modifications apportées au système de fichiers sont enregistrées sur le disque dans un journal qui est ensuite régulièrement purgé. Suite à un événement de système inattendu (comme une coupure de courant ou un plantage du système), la seule opération devant avoir lieu avant que le système de fichiers ne soit disponible, est le traitement du contenu du journal ; dans la plupart des cas, cette opération dure environ une seconde.

Étant donné que le système de fichiers ext3 utilise un format basé sur ext2 pour le stockage des données sur disque, l'accès à un système de fichiers ext3 est possible sur tout système pouvant lire et écrire un système de fichiers ext2 (toutefois sans avoir l'avantage de la journalisation). Cette caractéristique peut représenter un avantage considérable dans des entreprises où certains systèmes utilisent ext3 alors que d'autres utilisent toujours ext2.

5.9.2.3. ISO 9660

En 1987, l'organisation internationale de normalisation (plus connue sous l'acronyme anglais ISO, International Organization for Standardization) a publié la norme 9660. ISO 9660 définit la manière selon laquelle les fichiers sont représentés sur CD-ROM. Les administrateurs de systèmes Red Hat Enterprise Linux rencontreront des données au format ISO 9660 avec :

- Les CD-ROM
- Les fichiers contenant des systèmes de fichiers ISO 9660 complets (fichiers auxquels on fait généralement référence sous le terme d'*images ISO*), destinés à être enregistrés sur des supports CD-R ou CD-RW

La norme ISO 9660 de base est assez limitée au niveau de la fonctionnalité, particulièrement par rapport à des systèmes de fichiers plus récents. En effet, la longueur maximale des noms de fichiers ne peut dépasser huit caractères, alors que celle d'une extension ne peut aller au-delà de trois caractères. Toutefois, différentes extensions apportées à la norme ont connu une popularité croissante au cours des années ; parmi celles-ci figurent :

- Rock Ridge — Une extension utilisant des champs qui ne sont pas définis dans la norme ISO 9660, afin de fournir une prise en charge pour des fonctions telles que la possibilité d'utiliser des noms de fichiers composés d'un mélange de lettres majuscules et minuscules, des liens symboliques et des répertoires imbriqués (en d'autres termes, des répertoires pouvant contenir eux-mêmes des répertoires)
- Joliet — Une extension de la norme ISO 9660 (développée par Microsoft afin de permettre aux CD-ROM de contenir de longs noms de fichiers) utilisant un jeu de caractères Unicode

Red Hat Enterprise Linux peut interpréter correctement les systèmes de fichiers ISO 9660 à l'aide des extensions Rock Ridge et Joliet.

5.9.2.4. MSDOS

Red Hat Enterprise Linux prend également en charge les systèmes de fichiers d'autres systèmes d'exploitation. Comme l'indique le nom même du système de fichiers `msdos`, MS-DOS de Microsoft était le système d'exploitation prenant en charge à l'origine ce système de fichiers. Comme dans MS-DOS, un système Red Hat Enterprise Linux accédant à un système de fichiers `msdos` est restreint à une utilisation de noms de fichiers au format 8.3. De même, d'autres attributs de fichiers, tels que les permissions et la propriété, ne peuvent être modifiés. Toutefois, pour ce qui est de l'interéchange de fichiers, le système de fichiers `msdos` est tout à fait approprié.

5.9.2.5. VFAT

Le système de fichiers `vfat` était à l'origine utilisé par le système d'exploitation Windows® 95 de Microsoft. Grâce à une amélioration du système de fichiers `msdos`, le nom des fichiers d'un système de fichiers `vfat` peut désormais être plus long que le format `msdos` 8.3. Ceci étant, les permissions et la propriété ne peuvent toujours pas être modifiées.

5.9.3. Montage de systèmes de fichiers

Afin de pouvoir accéder à un système de fichiers quel qu'il soit, il est nécessaire de le *monter*. Grâce au montage d'un système de fichiers, vous demandez à Red Hat Enterprise Linux de mettre une partition spécifique (existant sur un périphérique particulier) à disposition du système de fichiers. De même, lorsque l'accès à un système de fichiers spécifique n'est plus nécessaire, il doit être *démonté*.

Pour monter tout système de fichiers, il est nécessaire de préciser les deux éléments suivants :

- Un moyen d'identifier de manière unique, le disque dur et la partition choisis, comme le nom du fichier de périphérique, l'étiquette du système de fichiers ou le lien symbolique géré par `devlabel`.
- Un répertoire sous lequel le système de fichiers monté doit être mis à disposition (auquel on fait aussi référence sous le terme de *point de montage*)

La section suivante aborde le sujet des points de montage de manière plus détaillée.

5.9.3.1. Points de montage

À moins que vous n'ayez l'habitude des systèmes d'exploitation Linux (ou de type Linux), le concept d'un point de montage paraîtra certainement étrange au premier abord. Ce dernier représente toutefois l'une des méthodes les plus performantes et souples qui ait été développée en matière de gestion de systèmes de fichiers. Avec de nombreux autres systèmes d'exploitation, la spécification complète d'un fichier inclut le nom du fichier, un moyen d'identifier le répertoire précis dans lequel le fichier se trouve et un moyen d'identifier le périphérique physique sur lequel le fichier se trouve.

Avec Red Hat Enterprise Linux cependant, une approche légèrement différente est adoptée. Tout comme c'est le cas avec d'autres systèmes d'exploitation, une spécification complète du fichier inclut le nom du fichier et le nom du répertoire dans lequel il se trouve. Ceci étant, aucun identifiant explicite n'est utilisé.

La raison expliquant cet inconvénient apparent est l'existence du point de montage. Sur d'autres systèmes d'exploitation, il existe une hiérarchie des répertoires pour chaque partition. Cependant, sur des systèmes de type Linux, il n'existe qu'une *seule* hiérarchie des répertoires pour tout le système et cette dernière peut même couvrir plusieurs partitions. La clé d'une telle structure est le point de montage. Lorsqu'un système de fichiers est monté, il est mis à disposition en tant qu'un ensemble de sous-répertoires, sous le point de montage spécifié.

Cet inconvénient apparent est en fait un véritable avantage. En effet, grâce au point de montage, il est possible d'étendre le système Linux de manière transparente dans la mesure où chaque répertoire peut servir de point de montage pour de l'espace disque supplémentaire.

À titre d'exemple, supposez qu'un système Red Hat Enterprise Linux contienne un répertoire `foo` dans son répertoire root (parfois aussi appelé racine) et que son chemin d'accès complet au répertoire soit `/foo/`. Supposez ensuite que ce système ait une partition devant être montée et que le point de montage de cette dernière soit `/foo/`. Si cette partition contenait un fichier portant le nom `bar.txt` placé au niveau supérieur de son répertoire, une fois la partition montée, vous pourriez avoir accès au fichier à l'aide de sa spécification complète, à savoir :

```
/foo/bar.txt
```

En d'autres termes, une fois cette partition montée, tout fichier lu ou écrit à un endroit quelconque sous le répertoire `/foo/` sera lu depuis ou écrit sur cette partition.

`/home/` est un point de montage couramment utilisé sur de nombreux systèmes — la raison étant que les répertoires de connexion des comptes de tous les utilisateurs se trouvent généralement sous ce répertoire `/home/`. Si `/home/` est utilisé comme point de montage, les fichiers de tous les utilisateurs sont enregistrés sur une partition attitrée, afin d'éviter que le système de fichiers du système d'exploitation ne se remplisse.



Astuce

Étant donné qu'un point de montage n'est rien de plus qu'un autre répertoire, il est tout à fait possible d'écrire des fichiers dans un répertoire qui sera plus tard utilisé comme point de montage. Dans une telle situation, qu'advient-il des fichiers qui se trouvaient à l'origine dans le répertoire ?

Tant que la partition n'est pas montée sur le répertoire, il est impossible d'avoir accès aux fichiers (le système de fichiers monté apparaît à la place du contenu du répertoire). Toutefois, les fichiers ne seront pas endommagés et il sera possible d'y accéder une fois la partition montée.

5.9.3.2. Affichage de ce qui est monté

Outre le montage et démontage d'espace disque, il est possible de voir ce qui est monté. Pour ce faire, il est possible de procéder de différentes manières :

- Affichage de `/etc/mtab`
- Affichage de `/proc/mounts`
- Exécution de la commande `df`

5.9.3.2.1. Affichage de `/etc/mtab`

Le fichier `/etc/mtab` est un fichier normal qui est mis à jour par le programme `mount` chaque fois que des systèmes de fichiers sont montés ou démontés. Ci-dessous figure un fichier `/etc/mtab` type :

```
/dev/sda3 / ext3 rw 0 0
none /proc proc rw 0 0
usbdevfs /proc/bus/usb usbdevfs rw 0 0
/dev/sda1 /boot ext3 rw 0 0
none /dev/pts devpts rw,gid=5,mode=620 0 0
/dev/sda4 /home ext3 rw 0 0
none /dev/shm tmpfs rw 0 0
none /proc/sys/fs/binfmt_misc binfmt_misc rw 0 0
```



Remarque

Le fichier `/etc/mtab` est supposé être utilisé pour afficher seulement le statut des systèmes de fichiers actuellement montés. Il ne devrait en aucun cas être modifié manuellement.

Chaque ligne représente un système de fichiers actuellement monté et contient les champs suivants (de gauche à droite) :

- La spécification du périphérique
- Le point de montage
- Le type de système de fichiers
- Une indication précisant si le système de fichiers est monté en lecture-seule (`ro`) ou en lecture-écriture (`rw`), avec toute autre option de montage
- Deux champs non utilisés contenant des zéros (pour la compatibilité avec `/etc/fstab`¹¹).

5.9.3.2.2. Affichage de `/proc/mounts`

Le fichier `/proc/mounts` fait partie du système de fichiers virtuels `proc`. Comme c'est le cas avec les autres fichiers sous `/proc/`, le "fichier" `mounts` n'existe sur aucun disque dur de votre système Red Hat Enterprise Linux.

En fait, ce n'est même pas un fichier ; c'est plutôt une représentation du statut des systèmes qui sont mis à disposition (par le noyau Linux) sous forme de fichiers.

En utilisant la commande `cat /proc/mounts`, il est possible d'examiner le statut de tous les systèmes de fichiers montés :

```
rootfs / rootfs rw 0 0
/dev/root / ext3 rw 0 0
/proc /proc proc rw 0 0
usbdevfs /proc/bus/usb usbdevfs rw 0 0
```

11. Pour de plus amples informations sur `/etc/fstab` reportez-vous à la Section 5.9.5.

```

/dev/sda1 /boot ext3 rw 0 0
none /dev/pts devpts rw 0 0
/dev/sda4 /home ext3 rw 0 0
none /dev/shm tmpfs rw 0 0
none /proc/sys/fs/binfmt_misc binfmt_misc rw 0 0

```

Comme le montre l'exemple ci-dessus, le format de `/proc/mounts` est très semblable à celui de `/etc/mtab`. Un certain nombre de systèmes de fichiers montés n'ont rien à voir avec les disques durs. Parmi ces derniers figure le système de fichiers `/proc/` lui-même (ainsi que deux autres systèmes de fichiers montés sous `/proc/`), les pseudo-ttys et la mémoire partagée.

Bien que le format ne soit certes pas très facile à comprendre, un examen de `/proc/mounts` représente la meilleure façon de déterminer à 100% ce qui est monté sur votre système Red Hat Enterprise Linux, dans la mesure où ces informations sont fournies directement par le noyau. D'autres méthodes peuvent, dans de rares circonstances, être inexactes.

Ceci étant, il est probable que vous utiliserez la plupart du temps une commande dont la sortie est plus facile à comprendre (et plus utiles). La section suivante examine cette commande.

5.9.3.2.3. Exécution de la commande `df`

Alors que `/etc/mtab` ou `/proc/mounts` vous permettent de savoir quels systèmes de fichiers sont actuellement montés, ils n'offrent pas beaucoup plus d'informations. La plupart du temps cependant, vous souhaitez obtenir des informations sur un aspect précis des systèmes de fichiers actuellement montés — la quantité d'espace libre dont ils disposent.

Pour obtenir une telle information, il est possible d'utiliser la commande `df`. Ci-dessous figure un extrait de sortie renvoyée par `df` :

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/sda3	8428196	4280980	3719084	54%	/
/dev/sda1	124427	18815	99188	16%	/boot
/dev/sda4	8428196	4094232	3905832	52%	/home
none	644600	0	644600	0%	/dev/shm

Par rapport à `/etc/mtablet` / `/proc/mount` un certain nombre de différences sautent aux yeux :

- Affichage d'une en-tête facile à lire
- Affichage seulement des systèmes de fichiers basé sur un disque, à l'exception des systèmes de fichiers de mémoire partagée
- Affichage de la taille totale, de l'espace utilisé, de l'espace libre et du pourcentage utilisé

Ce dernier point est probablement le plus important car tout administrateur système se voit, à un moment ou à un autre, confronté au problème d'un système sur le point de manquer d'espace disque. Avec `df`, il est facile de voir où le problème se situe.

5.9.4. Stockage réseau sous Red Hat Enterprise Linux

Sous Red Hat Enterprise Linux, il existe deux technologies principales pour l'implémentation de stockage réseau :

- NFS
- SMB

Les sections suivantes examinent ces technologies.

5.9.4.1. NFS

Comme son nom l'indique, Network File System (ou NFS) est un système de fichiers auquel l'accès se fait par le biais d'une connexion réseau. Avec d'autres systèmes de fichiers, le périphérique de stockage doit être branché directement au système local. Avec NFS cependant, ce n'est pas une obligation ; ainsi, de nombreuses configurations différentes sont alors possibles et la gamme s'étend des serveurs de systèmes de fichiers centralisés aux systèmes informatiques n'utilisant absolument aucun disque dur (aussi appelés diskless).

Contrairement à d'autres systèmes de fichiers, NFS ne dicte pas un format spécifique pour le stockage sur disque. Pour le contrôle des E/S vers un ou plusieurs disques durs locaux, il s'en remet plutôt à la prise en charge native du système de fichiers du système d'exploitation serveur. NFS met alors le système de fichiers à disposition de tout système d'exploitation exécutant un client NFS compatible.

Bien qu'étant au départ une technologie Linux et UNIX, il convient de noter ici que des implémentations clients NFS existent pour d'autres systèmes d'exploitation, si bien que NFS représente en fait une technique viable pour le partage de fichiers avec de nombreuses plates-formes différentes.

Le système de fichiers mis à la disposition des clients par le serveur NFS est contrôlé par le fichier de configuration `/etc/exports`. Pour de plus amples informations, reportez-vous à la page de manuel relative à `exports` (5) et au *Guide d'administration système de Red Hat Enterprise Linux*.

5.9.4.2. SMB

SMB, l'acronyme de *Server Message Block*, correspond au nom du protocole de communication utilisé par différents systèmes d'exploitation produits par Microsoft au cours des années. SMB permet de partager le stockage sur un réseau. Des implémentations actuelles utilisent souvent TCP/IP comme les moyens de transport sous-jacents ; auparavant, NetBEUI était le moyen de transport.

Red Hat Enterprise Linux prend en charge SMB via le programme du serveur Samba. Le *Guide d'administration système de Red Hat Enterprise Linux* inclut des informations sur la configuration de Samba.

5.9.5. Montage automatique de systèmes de fichiers avec `/etc/fstab`

Lorsqu'un système Red Hat Enterprise Linux vient d'être installé, toutes les partitions de disque définies et/ou créées lors de l'installation sont automatiquement montées lors de chaque démarrage du système. Mais que se passe-t-il lorsque des disques durs supplémentaires sont ajoutés à un système, une fois l'installation terminée ? La réponse est "rien du tout" car le système n'était pas configuré pour effectuer un montage automatique de ces derniers. Toutefois, il est possible de changer cette situation.

Pour ce faire, il suffit d'utiliser le fichier `/etc/fstab`. Ce dernier est utilisé pour contrôler les systèmes de fichiers qui seront montés lors du démarrage et pour fournir les valeurs par défaut aux autres systèmes de fichiers qui seront peut-être montés manuellement de temps à autre. Ci-après figure l'extrait d'un fichier `/etc/fstab` type :

```

LABEL=/                /                ext3    defaults    1 1
/dev/sda1              /boot           ext3    defaults    1 2
/dev/cdrom             /mnt/cdrom     iso9660 noauto,owner,kudzu,ro 0 0
/dev/homedisk         /home          ext3    defaults    1 2
/dev/sda2              swap           swap    defaults    0 0

```

Chaque ligne représente un système de fichiers et contient les champs suivants :

- Identifiant des systèmes de fichiers — Pour les systèmes de fichiers sur disque, il peut s'agir d'un nom de fichier de périphérique (`/dev/sda1`), de la spécification d'une étiquette de système de fichiers (`LABEL=`) ou d'un lien symbolique géré par `devlabel` (`/dev/homedisk`)
- Point de montage — À l'exception des partitions swap, ce champ précise le point de montage à utiliser lorsque le système de fichiers est monté (`/boot`)
- Type de système de fichiers — Le type de système de fichiers existant sur le périphérique spécifié (notez bien qu'il est possible de préciser `auto` afin de choisir une détection automatique du système de fichiers à monter ; cette option est très utile dans le cas d'unités de support amovibles telles que des unités de disquettes)
- Options de montage — Une liste d'options séparées par des virgules pouvant être utilisées pour contrôler le comportement de `mount` (`noauto, owner, kudzu`)
- Fréquence de vidage — Si l'utilitaire de sauvegarde `dump` est utilisé, le nombre inséré dans ce champ contrôle la manière dont `dump` traitera le système de fichiers spécifié
- Ordre de vérification des systèmes de fichiers — Détermine l'ordre selon lequel le contrôleur de systèmes de fichiers `fsck` effectue la vérification de l'intégrité des systèmes de fichiers

5.9.6. Ajout/Suppression de stockage

Bien que la plupart des étapes nécessaires à l'ajout ou à la suppression de stockage dépendent plus du matériel du système que du logiciel du système, certains aspects de la procédure sont toutefois spécifiques à votre environnement d'exploitation. Cette section examine les étapes spécifiques à Red Hat Enterprise Linux qui doivent être suivies pour ajouter ou supprimer du stockage.

5.9.6.1. Ajout de stockage

Le processus permettant d'ajouter du stockage à un système Red Hat Enterprise Linux est relativement simple. Ci-après figurent les étapes spécifiques à Red Hat Enterprise Linux :

- Partitionnement
- Formatage d'une ou plusieurs partition(s)
- Mise à jour de `/etc/fstab`

La section suivante examine chacune de ces étapes de manière plus détaillée.

5.9.6.1.1. Partitionnement

Une fois le disque dur installé, il est nécessaire de créer une ou plusieurs partitions afin que Red Hat Enterprise Linux puisse utiliser cet espace.

Pour ce faire, il est possible de procéder de plusieurs manières :

- Utilisation du programme utilitaire en ligne de commande `fdisk`
- Utilisation de `parted`, un autre programme utilitaire en ligne de commande

Bien que les outils puissent être différents, les étapes de base restent les mêmes. L'exemple ci-dessous inclut les commandes nécessaires pour effectuer ces étapes à l'aide de `fdisk` :

1. Sélectionnez le nouveau disque dur (le nom du périphérique peut être déterminé en suivant les conventions de nommage de périphérique soulignées dans la Section 5.9.1). Avec `fdisk`, cette opération est effectuée en incluant le nom du périphérique lorsque vous lancez `fdisk` :

```
fdisk /dev/hda
```

2. Consultez la table des partitions du disque dur pour vous assurez que les informations relatives au disque dur devant être partitionné sont bien correctes. Dans notre exemple, `fdisk` affiche la table des partitions à l'aide de la commande `p` :

```
Command (m for help): p

Disk /dev/hda: 255 heads, 63 sectors, 1244 cylinders
Units = cylinders of 16065 * 512 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hda1 *          1          17       136521   83   Linux
/dev/hda2            18          83       530145   82   Linux swap
/dev/hda3            84         475      3148740   83   Linux
/dev/hda4           476        1244      6176992+  83   Linux
```

3. Supprimez toute partition inutile qui pourrait déjà exister sur le nouveau disque dur. Pour ce faire, utilisez la commande `d` dans `fdisk` :

```
Command (m for help): d
Partition number (1-4): 1
```

Ce processus devrait être répété pour toutes les partitions inutiles présentes sur le disque dur.

4. Créez la (ou les) nouvelle(s) partition(s), en vous assurant bien de préciser la taille souhaitée ainsi que la type de système de fichiers. En utilisant la commande `fdisk`, ce processus comportera deux étapes — d'une part la création de la partition (avec la commande `n`) :

```
Command (m for help): n
Command action
  e   extended
  p   primary partition (1-4)
```

P

```
Partition number (1-4): 1
First cylinder (1-767): 1
Last cylinder or +size or +sizeM or +sizeK: +512M
```

D'autre part, le choix du type de système de fichiers (avec la commande `t`) :

```
Command (m for help): t
Partition number (1-4): 1
Hex code (type L to list codes): 82
```

Une partition de type 82 correspond à une partition swap Linux .

5. Enregistrez vos modifications et quittez le programme de partitionnement. Dans `fdisk`, il suffit d'utiliser la commande `w` :

```
Command (m for help): w
```



Avertissement

Lors du partitionnement d'un nouveau disque dur, il est *primordial* d'être absolument certain que le disque sur le point d'être partitionné est bien celui que vous souhaitez utiliser pour cette opération. Dans le cas contraire, vous risqueriez de partitionner par erreur un disque dur qui est déjà utilisé, entraînant par là-même la perte des données contenues.

Assurez-vous également de bien avoir choisi la meilleure taille de partition possible. Réfléchissez bien à ce point avant de prendre une décision car il est beaucoup plus difficile de modifier ultérieurement la taille d'une partition, que de passer un peu de temps maintenant à considérer la chose.

5.9.6.1.2. Formatage d'une ou plusieurs partition(s)

Sous Red Hat Enterprise Linux, le formatage des partitions est effectué à l'aide du programme utilitaire `mkfs`. Toutefois, `mkfs` n'effectue pas l'enregistrement des informations spécifiques au système de fichiers sur le disque dur ; il s'en remet à un des nombreux autres programmes qui lui effectivement crée le système de fichiers.

Il convient maintenant d'examiner la page de manuel de `mkfs.<fstype>` traitant du système de fichiers que vous avez choisi. Par exemple, consultez la page de manuel de `mkfs.ext3` pour obtenir la liste des options s'offrant à vous lors de la création d'un nouveau système de fichiers ext3. En général, le programme `mkfs.<fstype>` fournit des valeurs par défaut pouvant être utilisées pour la plupart des configurations ; ci-après figurent certaines des options que les administrateurs systèmes changent le plus souvent :

- Détermination d'une étiquette de volume dans `/etc/fstab` afin de l'utiliser plus tard
- Réduction du pourcentage d'espace réservé au super-utilisateur (sur de grands disques durs)
- Détermination d'une taille de bloc et/ou d'un nombre d'octets par inode non standard, dans le cas de configurations devant prendre en charge des fichiers soit très volumineux, soit très petits
- Recherche des blocs défectueux avant le formatage

Une fois que tous les systèmes de fichiers ont été créés sur les partitions appropriées, le disque dur est alors configuré de manière adéquate pour son utilisation.

Ensuite, il est toujours recommandé de vérifier votre travail en montant la (ou les) partition(s) manuellement et en vous assurant que tout est bien correct. Une fois cette opération effectuée avec succès, il est alors possible de configurer votre système Red Hat Enterprise Linux de sorte qu'il monte automatiquement le (ou les) nouveau(x) système(s) de fichiers lors de chaque démarrage.

5.9.6.1.3. Mise à jour de `/etc/fstab`

Comme il l'a été souligné dans la Section 5.9.5, vous devez ajouter la (ou les) ligne(s) nécessaire(s) dans `/etc/fstab`, afin de garantir le montage du (ou des) nouveau(x) système(s) de fichiers lors de chaque démarrage. Une fois `/etc/fstab` mis à jour, testez votre travail en exécutant une commande `mount` "incomplète", c'est-à-dire en ne précisant que le périphérique ou le point de montage. Pour ce faire, une des commandes semblables à celles figurant ci-dessous suffira :

```
mount /home
mount /dev/hda3
```

(En remplaçant bien sûr `/home` ou `/dev/hda3` par le point de montage ou le périphérique correspondant à votre situation particulière.)

Si l'entrée ajoutée dans `/etc/fstab` est correcte, la commande `mount` obtiendra les informations manquantes de ce fichier et effectuera l'opération de montage.

À ce stade, vous pouvez être plus ou moins certain que `/etc/fstab` est configuré de manière à monter automatiquement le nouveau stockage lors de tout démarrage (ceci étant, si vous pouvez vous permettre d'effectuer une redémarrage rapide, c'est encore mieux — juste pour vous assurer que tout fonctionne bien comme vous le souhaitez).

5.9.6.2. Suppression de stockage

Le processus consistant à supprimer du stockage d'un système Red Hat Enterprise Linux est relativement simple. Ci-après figurent les étapes spécifiques à Red Hat Enterprise Linux :

- Supprimez les partitions du disque dur dans le fichier `/etc/fstab`
- Démontez les partitions actives du disque dur
- Effacez le contenu du disque dur

Les sections suivantes abordent ces sujets de manière plus détaillée.

5.9.6.2.1. Suppression des partitions du disque dur dans `/etc/fstab`

À l'aide de l'éditeur de texte de votre choix, supprimez la (ou les) ligne(s) correspondant à la (ou aux) partition(s) présente(s) dans le fichier `/etc/fstab`. Il est possible d'identifier les lignes appropriées en suivant l'une des méthodes suivantes :

- En établissant la correspondance entre le point de montage de la partition et les répertoires figurant dans la deuxième colonne du fichier `/etc/fstab`
- En établissant la correspondance entre le nom du fichier de périphérique et les noms de fichiers figurant dans la première colonne du fichier `/etc/fstab`



Astuce

Assurez-vous de bien rechercher dans le fichier `/etc/fstab` toute ligne identifiant les partitions swap qui sont présentes sur le disque dur devant être supprimé ; il est très facile de les oublier.

5.9.6.2.2. Fermeture de l'accès avec `umount`

Ensuite, il est nécessaire de mettre fin à tout accès au disque dur. Dans le cas de partitions contenant des systèmes de fichiers actifs, cette opération peut être effectuée à l'aide de la commande `umount`. Si une partition swap est présente sur le disque dur, il y a deux possibilités : soit la partition est désactivée avec la commande `swapoff`, soit le système est redémarré.

Pour permettre le démontage de partitions avec la commande `umount`, il est nécessaire de spécifier soit le nom de fichier de périphérique, soit le point de montage de la partition :

```
umount /dev/hda2
umount /home
```

Une partition ne peut être montée que si elle n'est pas déjà montée. Dans le cas où la partition ne pourrait pas être montée bien qu'étant au niveau d'exécution normal, démarrez en mode de secours et supprimez l'entrée dans `/etc/fstab` qui concerne la partition.

Lors de l'utilisation de `swapoff` pour désactiver l'échange de mémoire (ou swapping) sur une partition, il est nécessaire de préciser le nom du fichier de périphérique correspondant à la partition swap :

```
swapoff /dev/hda4
```

S'il n'est pas possible de désactiver l'échange de mémoire sur une partition swap à l'aide de la commande `swapoff`, démarrez en mode de secours et supprimez l'entrée de la partition dans `/etc/fstab`.

5.9.6.2.3. Effacement du contenu du disque dur

L'effacement du contenu d'un disque dur sous Red Hat Enterprise Linux est une procédure relativement simple.

Après avoir démonté toutes les partitions du disque dur, exécutez la commande suivante (en étant connecté en tant que super-utilisateur) :

```
badblocks -ws <device-name>
```

où *<device-name>* correspond au nom de fichier du disque dur que vous souhaitez effacer, en excluant le numéro de partition. Par exemple, */dev/hdb* pour identifier le deuxième disque dur ATA.

Lorsque `badblocks` est en cours d'exécution, la sortie suivante apparaît à l'écran :

```
Writing pattern 0xaaaaaaaa: done
Reading and comparing: done
Writing pattern 0x55555555: done
Reading and comparing: done
Writing pattern 0xffffffff: done
Reading and comparing: done
Writing pattern 0x00000000: done
Reading and comparing: done
```

Gardez bien à l'esprit que `badblocks` enregistre en fait quatre arrangements différents de données sur chaque bloc du disque dur. Dans le cas de grands disques durs, le processus peut prendre beaucoup de temps — souvent plusieurs heures.



Important

De nombreuses entreprises (et ministères) disposent de méthodes spécifiques pour effacer des données contenues sur des disques durs et autres supports de stockage d'informations. Assurez-vous de *toujours* comprendre et respecter ces obligations ; dans bien des cas, leur non respect a des conséquences juridiques. L'exemple décrit ci-dessus ne devraient en aucun cas être considéré comme la méthode absolue pour effacer un disque dur.

Toutefois, cette méthode est beaucoup plus efficace que l'utilisation de la commande `rm`. En effet, lorsqu'un fichier est effacé à l'aide de la commande `rm`, cette dernière ne fait qu'identifier le fichier comme étant effacé — elle *n'efface pas* le contenu du fichier.

5.9.7. Implémentation de quotas de disque

Grâce à l'utilisation de quotas de disque, Red Hat Enterprise Linux est en mesure d'effectuer un suivi de l'utilisation d'espace disque sur une base individuelle au niveau de l'utilisateur et du groupe. La section suivante fournit un aperçu des caractéristiques associées aux quotas de disque sous Red Hat Enterprise Linux.

5.9.7.1. Informations de base sur les quotas de disque

Sous Red Hat Enterprise Linux, les quotas de disque ont les caractéristiques suivantes :

- Implémentation par système de fichiers individuel
- Comptabilisation de l'espace par utilisateur individuel

- Comptabilisation de l'espace par groupe individuel
- Suivi de l'utilisation des blocs du disque
- Suivi de l'utilisation des inodes du disque
- Limites dures (hard)
- Limites douces (soft)
- Périodes de grâce

Les sections suivantes examinent chacune de ces caractéristiques de manière plus détaillée.

5.9.7.1.1. Implémentation par système de fichiers individuel

Sous Red Hat Enterprise Linux, les quotas de disques peuvent être utilisés sur la base de systèmes de fichiers individuels. En d'autres termes, les quotas de disque peuvent être activés ou désactivés de manière individuelle pour chaque système de fichiers.

Cette caractéristique offre à l'administrateur système une très grande flexibilité. Par exemple, si le répertoire `/home/` était présent sur son propre système de fichiers, il serait possible d'activer les quotas de disque à ce niveau, afin d'instaurer une utilisation équitable du disque par tous les utilisateurs. Toutefois, le système de fichiers `root` (parfois appelé racine) n'a pas à être soumis à des quotas de disque, éliminant ainsi la complexité associée au maintien de quotas de disque pour un système de fichiers sur lequel seul le système d'exploitation lui-même est présent.

5.9.7.1.2. Comptabilisation de l'espace par utilisateur individuel

Les quotas de disque permettent d'effectuer la comptabilisation de l'espace utilisé par chaque individu sur une base individuelle. Ce faisant, l'espace de chaque utilisateur est non seulement comptabilisé de manière individuelle, mais toute restriction d'utilisation (un sujet abordé plus tard) est également imposée de manière individuelle, utilisateur par utilisateur.

Grâce à cette souplesse au niveau du suivi et de l'application de directives d'utilisation du disque pour chaque utilisateur de manière individuelle, un administrateur système peut, en fonction des responsabilités et besoins de stockage des individus, déterminer des restrictions différentes.

5.9.7.1.3. Comptabilisation de l'espace par groupe

Les quotas de disque peuvent également effectuer le suivi de l'utilisation du disque sur une base individuelle, groupe par groupe. Cette fonctionnalité est par conséquent idéale pour les entreprises qui recourent à la notion de groupes pour rassembler différents utilisateurs en une seule ressource pour toute la durée d'un projet.

En établissant des quotas de disque sur l'ensemble du groupe, l'administrateur système est à même de gérer plus étroitement l'utilisation du stockage ; en effet, il peut attribuer aux utilisateurs individuels seulement le quota de disque dont ils ont besoin pour leur utilisation personnelle, tout en établissant des quotas de disque plus grands et plus adéquats dans le cas de projets regroupant plusieurs utilisateurs. Cette méthode peut se révéler être très utile pour les entreprises qui fonctionnent selon un principe de "facturation après service" ; en effet, elle permet d'établir le montant des dépenses du centre de données qui est associé à l'utilisation des ressources du centre de données par des services et équipes qui devront être facturés ultérieurement.

5.9.7.1.4. Suivi de l'utilisation de blocs du disque

Les quotas de disque permettent d'effectuer le suivi de l'utilisation des blocs du disque. Étant donné que le stockage de toutes les données sur un système de fichiers se fait en blocs, les quotas de disque

peuvent mettre en corrélation les fichiers créés et effacés sur un système de fichiers avec la quantité de mémoire que ces fichiers occupent.

5.9.7.1.5. *Suivi de l'utilisation des inodes du disque*

Outre le suivi effectué au niveau de l'utilisation des blocs du disque, les quotas de disque peuvent également effectuer celui de l'utilisation des inodes. Sous Red Hat Enterprise Linux, les inodes servent à stocker différentes parties du système de fichiers, mais surtout, elles contiennent des informations sur chaque fichier. Par conséquent, en effectuant le suivi (et en contrôlant) l'utilisation des inodes, il est possible de contrôler la création de nouveaux fichiers.

5.9.7.1.6. *Limites dures*

Une limite dure correspond au nombre absolument maximal de blocs de disque (ou d'inodes) pouvant être utilisé de manière temporaire par un utilisateur (ou par un groupe). Toute tentative d'utilisation d'un bloc ou d'une inode au-dessus de la limite dure sera vouée à l'échec.

5.9.7.1.7. *Limites douces*

Une limite douce correspond au nombre maximal de blocs de disque (ou d'inodes) pouvant être utilisé de manière temporaire par un utilisateur (ou par un groupe).

La limite douce se situe logiquement au-dessous de la limite dure. Ainsi, étant donné que les utilisateurs peuvent temporairement dépasser leur limite douce, ils sont non seulement en mesure de finir toute tâche commencée mais il ont également le temps de naviguer parmi leurs fichiers afin de réduire leur utilisation de sorte qu'elle soit à nouveau en dessous de leur limite douce.

5.9.7.1.8. *Périodes de grâce*

Comme mentionné précédemment, toute utilisation de disque au-dessus de la limite douce est une mesure temporaire. C'est la période de grâce qui détermine la durée pendant laquelle un utilisateur (ou un groupe) peut pousser son utilisation au-delà de la limite douce et proche de la limite dure.

Si un utilisateur continue à consommer plus d'espace que la limite douce et que la période de grâce est dépassée, aucune utilisation supplémentaire de disque ne sera permise tant que l'utilisateur (ou le groupe) n'aura pas réduit son utilisation au-dessous de la limite douce.

La période de grâce pouvant être exprimée en secondes, minutes, heures, jours, semaines ou mois, l'administrateur système dispose d'une grande liberté au niveau de la détermination de la durée qui sera accordée aux utilisateurs afin de leur permettre de ramener leur consommation au-dessous de leur limite douce.

5.9.7.2. **Activation des quotas de disque**



Remarque

Les sections suivantes fournissent un bref aperçu des étapes nécessaires pour activer les quotas de disque sous Red Hat Enterprise Linux. Pour obtenir des informations plus détaillées sur ce sujet, consultez le chapitre consacré aux quotas de disque dans le *Guide d'administration système de Red Hat Enterprise Linux*.

Afin de pouvoir utiliser les quotas de disque, ils doivent tout d'abord être activés. Ce processus comporte les étapes suivantes :

1. Modification de `/etc/fstab`
2. Remontage du (ou des) système(s) de fichiers
3. Exécution de `quotacheck`
4. Attribution de quotas

Le fichier `/etc/fstab` contrôle le montage du système de fichiers sous Red Hat Enterprise Linux. Étant donné que les quotas de disque sont implémentés de manière individuelle pour chaque système de fichiers, il est nécessaire d'ajouter deux options — `usrquota` et `grpquota` — pour activer les quotas de disque.

L'option `usrquota` permet d'activer des quotas de disque sur la base des utilisateurs alors que `grpquota` permet leur activation sur la base des groupes. L'activation d'une ou des deux options peut être effectuée en `la/les` spécifiant dans le champ d'options correspondant au système de fichiers sur lequel les quotas doivent être appliqués.

Il est alors nécessaire de démonter le (ou les) système(s) de fichiers en question pour le (ou les) remonter ensuite de sorte que les options relatives aux quotas de disque puissent prendre effet.

Ensuite, la commande `quotacheck` est utilisée pour créer les fichiers quotas de disque et pour recueillir les informations sur l'utilisation actuelle qui sont stockées dans des fichiers qui existent déjà. Les fichiers quotas de disque (nommés `aquota.user` pour les quotas imposés aux utilisateurs et `aquota.group` pour ceux des groupes) qui contiennent les informations nécessaires sur les quotas se trouvent dans le répertoire `root` (ou racine) du système de fichiers.

L'attribution des quotas de disque se fait à l'aide de la commande `edquota`.

Le programme utilitaire utilise un éditeur de texte pour afficher les informations sur les quotas qui s'appliquent à l'utilisateur ou au groupe spécifiés dans la commande `edquota`. Ci-après figure un exemple de sortie renvoyée par cette commande :

```
Disk quotas for user matt (uid 500):
Filesystem      blocks      soft      hard    inodes      soft      hard
/dev/md3        6618000    0         0       17397       0         0
```

Selon cet exemple, l'utilisateur `matt` utilise actuellement plus de 6 Go d'espace disque et plus de 17.000 inodes. Aucun quota (à limite douce ou dure) n'ayant encore été établi que ce soit pour les blocs de disque ou pour les inodes, aucune limite n'existe quant à la quantité d'espace disque ou au nombre d'inodes que l'utilisateur peut actuellement utiliser.

En utilisant l'éditeur de texte permettant d'afficher les informations relatives aux quotas de disque, l'administrateur système peut modifier les limites douces et dures comme il le souhaite :

```
Disk quotas for user matt (uid 500):
Filesystem      blocks      soft      hard    inodes      soft      hard
/dev/md3        6618000    6900000  7000000  17397       0         0
```

Dans cet exemple, on a octroyé à l'utilisateur `matt` une limite douce de 6,9 Go et une limite dure de 7 Go. Pour cette utilisateur, aucune limite douce ou dure, n'a été fixée au niveau des inodes.



Astuce

À l'aide de l'option `-t`, le programme `edquota` peut également servir à déterminer de manière individuelle, la période de grâce s'appliquant à chaque système de fichiers.

5.9.7.3. Gestion des quotas de disque

Sous Red Hat Enterprise Linux, les tâches de gestion nécessaires pour prendre en charge les quotas de disque sont en fait très limitées et se limitent essentiellement à :

- Création de rapports d'utilisation de disque à intervalles réguliers (et la prise de mesures appropriées par rapport aux utilisateurs qui semblent avoir des difficultés à gérer de manière efficace, l'espace disque qui leur est attribué)
- Contrôle pour s'assurer que les quotas de disque sont toujours justes

La création de rapports sur l'utilisation du disque passe par l'exécution du programme utilitaire `repquota`. L'utilisation de la commande `repquota /home` fournit la sortie suivante :

```
*** Report for user quotas on device /dev/md3
Block grace time: 7days; Inode grace time: 7days
User                used      Block limits      File limits
                   soft    hard  grace    used    soft  hard  grace
-----
root                --  32836      0      0      4      0    0
matt                -- 6618000 6900000 7000000 17397   0    0
```

De plus amples informations sur `repquota` sont disponibles dans le chapitre consacré aux quotas de disque du *Guide d'administration système de Red Hat Enterprise Linux*.

Dés lors qu'un système de fichiers n'est pas démonté correctement (par exemple, suite à un plantage), il est nécessaire d'exécuter `quotacheck`. Toutefois, de nombreux administrateurs recommandent d'exécuter `quotacheck` de manière régulière et ce, même en l'absence de plantage du système.

Le processus est semblable à l'utilisation initiale de `quotacheck` lors de l'activation des quotas de disque.

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

```
quotacheck -avug
```

La manière la plus simple d'exécuter `quotacheck` de façon régulière, consiste à utiliser `cron`. Bien que la plupart des administrateurs système exécutent `quotacheck` une fois par semaine, il y a parfois de bonnes raisons justifiant l'allongement ou le raccourcissement de l'intervalle en fonction de circonstances particulières.

5.9.8. Création de matrices RAID

Outre la prise en charge de solutions de type RAID matériel, Red Hat Enterprise Linux supporte RAID logiciel. Les matrices RAID peuvent être créées de deux manières :

- Lors de l'installation de Red Hat Enterprise Linux
- Après l'installation de Red Hat Enterprise Linux

Les sections suivantes examinent chacune des deux méthodes.

5.9.8.1. Lors de l'installation de Red Hat Enterprise Linux

Lors du processus d'installation normal de Red Hat Enterprise Linux, il est possible de créer des matrices RAID. Cette opération a lieu pendant l'étape de partitionnement du processus d'installation.

Pour commencer, vous devez partitionner manuellement vos disques durs à l'aide de **Disk Druid**. Vous devez tout d'abord créer une nouvelle partition de type "RAID logiciel" (software RAID). Ensuite,

dans le champ **Allowable Drives** (Disques disponibles), choisissez les disques durs que vous souhaitez inclure dans la matrice RAID. Poursuivez en sélectionnant la taille voulue et en précisant si vous souhaitez que la partition soit une partition primaire.

Une fois que vous avez créé toutes les partitions nécessaires pour la (ou les) matrice(s) RAID que vous voulez réaliser, vous devez utiliser le bouton **RAID** pour que la création de la ou des matrice(s) ait effectivement lieu. Une boîte de dialogue s'affiche alors, dans laquelle vous pouvez choisir le point de montage de la ou des matrice(s), le type de système de fichiers, le nom du périphérique RAID, le niveau RAID et la partition de type "RAID logiciel" (ou software RAID) sur laquelle la matrice sera présente.

Une fois les différentes matrices créées, le processus d'installation se poursuit normalement.



Astuce

Pour obtenir de plus amples informations sur la création de matrices RAID logicielles lors du processus d'installation de Red Hat Enterprise Linux, reportez-vous au *Guide d'administration système de Red Hat Enterprise Linux*.

5.9.8.2. Après l'installation de Red Hat Enterprise Linux

La création d'une matrice RAID une fois l'installation terminée est un processus légèrement plus compliqué. Comme c'est le cas lors de l'ajout de tout type de stockage disque, le matériel nécessaire doit être préalablement installé et correctement configuré.

Le partitionnement de RAID est légèrement différent de celui de disques durs individuels. Au lieu de choisir un type de partition "Linux" (type 83) ou "Linux swap" (type 82), toutes les partitions destinées à faire partie d'une matrice RAID doivent être de type "Linux raid auto" (type fd).

Il est ensuite nécessaire de créer le fichier `/etc/raidtab`. Ce dernier est responsable de la configuration correcte de toutes les matrices RAID du système. Le format du fichier (expliqué dans la page de manuel relative à `raidtab(5)`) est relativement simple. Ci-après figure un exemple d'entrée du fichier `/etc/raidtab` pour une matrice RAID 1 :

```
raiddev          /dev/md0
raid-level       1
nr-raid-disks   2
chunk-size      64k
persistent-superblock 1
nr-spare-disks  0
  device        /dev/hda2
  raid-disk     0
  device        /dev/hdc2
  raid-disk     1
```

Parmi les sections les plus importantes de cette entrée figurent :

- `raiddev` — Affiche le nom du fichier de périphérique correspondant à la matrice RAID¹²
- `raid-level` — Détermine le niveau RAID à utiliser dans cette matrice RAID
- `nr-raid-disks` — Indique le nombre de partitions physiques de disque composant la matrice

12. Notez bien que la matrice RAID étant composée d'espace disque partitionné, le nom du fichier de périphérique d'une matrice RAID ne fournit pas d'informations au niveau de la partition.

- `nr-spare-disks` — Sous Red Hat Enterprise Linux, le RAID logiciel permet de définir une ou plusieurs partition(s) de disque ; ces partitions peuvent automatiquement remplacer un disque défaillant
- `device,raid-disk` — Ensemble, ces deux éléments définissent les partitions physiques de disque composant la matrice RAID

Il est ensuite nécessaire de créer effectivement la matrice RAID. Cette opération est effectuée à l'aide du programme `mkraid`. Toujours en utilisant le fichier de notre exemple, `/etc/raidtab`, la matrice RAID `/dev/md0` pourrait être créée à l'aide de la commande suivante :

```
mkraid /dev/md0
```

La matrice RAID `/dev/md0` est désormais prête à être formatée et montée. À ce stade, le processus n'est pas différent de celui utilisé pour le formatage et le montage d'un disque dur individuel.

5.9.9. Gestion quotidienne des matrices RAID

Pour maintenir le bon fonctionnement d'une matrice RAID, il n'y a pas grand chose à faire. Dès lors qu'aucun problème matériel ne survient, la matrice devrait fonctionner comme s'il s'agissait d'un seul disque dur physique. Toutefois, tout comme un administrateur système se doit de vérifier de temps à autre l'état de tous les disques durs du système, il est important de vérifier également l'état des matrices RAID.

5.9.9.1. Vérification de l'état des matrices avec `/proc/mdstat`

Le fichier `/proc/mdstat` est le moyen le plus simple de vérifier l'état de toutes les matrices RAID d'un système particulier. Ci-après figure un exemple de fichier `mdstat` (pour l'afficher, utiliser la commande `cat /proc/mdstat`):

```
Personalities : [raid1]
read_ahead 1024 sectors
md1 : active raid1 hda3[0] hdc3[1]
      522048 blocks [2/2] [UU]

md0 : active raid1 hda2[0] hdc2[1]
      4192896 blocks [2/2] [UU]

md2 : active raid1 hda1[0] hdc1[1]
      128384 blocks [2/2] [UU]

unused devices: <none>
```

Ce système dispose de trois matrices RAID (toutes RAID 1). Dans `/proc/mdstat`, chacune des matrices a sa propre section contenant les informations suivantes :

- Le nom de périphérique de la matrice RAID (n'incluant pas la partie `/dev/`)
- L'état de la matrice RAID
- Le niveau RAID de la matrice RAID
- Les partitions physiques qui composent actuellement la matrice (suivies du numéro d'unité de la matrice de la partition)
- La taille de la matrice
- Le nombre de périphériques configurés par rapport au nombre de périphériques employés dans la matrice

- L'état de chacun des périphériques configurés dans la matrice (U indiquant que le périphérique fonctionne et _ indiquant au contraire, que le périphérique ne fonctionne pas)

5.9.9.2. Reconstruction d'une matrice RAID avec `raidhotadd`

Dans le cas où `/proc/mdstat` indiquerait qu'il y a un problème avec une des matrices RAID, le programme utilitaire `raidhotadd` devrait être utilisé afin de reconstruire la matrice. Dans ce cadre, il faudra suivre les étapes suivantes :

1. Déterminer le disque contenant la partition défaillante
2. Résoudre le problème à l'origine de la défaillance (très probablement en remplaçant le disque)
3. Partitionner le nouveau disque afin que les partitions qu'il héberge soient *identiques* à celles présentes sur le ou les autre(s) disque(s) de la matrice
4. Exécuter la commande suivante :
`raidhotadd <raid-device> <disk-partition>`
5. Surveiller `/proc/mdstat` pour examiner la reconstruction en cours



Astuce

La commande suivante peut être utilisée afin de surveiller la reconstruction en cours d'exécution :

```
watch -n1 cat /proc/mdstat
```

Cette commande permet d'afficher le contenu de `/proc/mdstat` qui est mis à jour toutes les deux secondes.

5.9.10. Gestionnaire de volumes logiques (LVM)

Red Hat Enterprise Linux inclut la prise en charge du LVM. Il est possible de configurer le LVM tout en installant Red Hat Enterprise Linux mais il peut également être configuré une fois l'installation terminée. Sous Red Hat Enterprise Linux, le LVM prend en charge le regroupement physique de stockage, le redimensionnement de volumes logiques et la migration de données à partir d'un volume physique spécifique.

Pour obtenir de plus amples informations sur le LVM, reportez-vous au *Guide d'administration système de Red Hat Enterprise Linux*.

5.10. Ressources supplémentaires

Cette section comprend un certain nombre de ressources pouvant être utilisées pour approfondir vos connaissances sur les technologies de stockage et sur des sujets spécifiques à Red Hat Enterprise Linux qui ont été abordés dans ce chapitre.

5.10.1. Documentation installée

Les ressources suivantes, installées lors d'une installation normale de Red Hat Enterprise Linux, peuvent vous aider à pour approfondir vos connaissances sur des sujets qui ont été abordés dans ce chapitre.

- Page de manuel de `exports(5)` — Pour en savoir plus sur le format du fichier de configuration de NFS.
- Page de manuel de `fstab(5)` — Pour en savoir plus sur le format du fichier de configuration contenant des informations relatives aux systèmes de fichiers.
- Page de manuel de `swapon(8)` — Pour apprendre à désactiver des partitions swap.
- Page de manuel de `df(1)` — Pour apprendre à afficher l'utilisation de l'espace disque sur les systèmes de fichiers montés.
- Page de manuel de `fdisk(8)` — Pour en savoir plus sur ce programme utilitaire permettant de maintenir la table des partitions.
- Pages de manuel de `mkfs(8)`, `mke2fs(8)` — Pour en savoir plus sur le programme utilitaire permettant de créer des systèmes de fichiers.
- Page de manuel de `badblocks(8)` — Pour apprendre comment sonder un périphérique pour détecter des blocs défectueux.
- Page de manuel de `quotacheck(8)` — Pour apprendre à contrôler l'utilisation des blocs et inodes par les utilisateurs et les groupes et, en option, pour créer les fichiers quotas de disque.
- Page de manuel de `edquota(8)` — Pour en savoir plus sur le programme utilitaire permettant de maintenir des quotas de disque.
- Page de manuel de `repquota(8)` — Pour en savoir plus sur le programme utilitaire permettant le rapportage des quotas de disque.
- Page de manuel de `raidtab(5)` — Pour en savoir plus sur le format du fichier de configuration d'un RAID logiciel.
- Page de manuel de `mkraid(8)` — Pour en savoir plus sur le programme utilitaire permettant la création d'une matrice RAID de type logiciel.
- Page de manuel de `mdadm(8)` — Pour en savoir plus sur le programme utilitaire permettant la gestion d'une matrice RAID de type logiciel.
- Page de manuel de `lvm(8)` — Pour en savoir plus sur LVM (ou Logical Volume Management).
- Page de manuel de `devlabel(8)` — Pour en savoir plus sur l'accès persistant aux périphériques de stockage.

5.10.2. Sites Web utiles

- <http://www.pcguides.com/> — Un bon site où obtenir toutes sortes d'informations sur les différentes technologies de stockage.
- <http://www.tldp.org/> — Le projet de documentation Linux (Linux Documentation Project) a des documents de type HOWTO et mini-HOWTO qui fournissent de bons aperçus sur les différentes technologies de stockage en relation avec Linux.

5.10.3. Livres sur le sujet

Les livres suivants abordent différents sujets en relation avec le stockage et constituent de bonnes ressources pour les administrateurs de systèmes Red Hat Enterprise Linux.

- *Guide d'installation de Red Hat Enterprise Linux* ; Red Hat, Inc. — Contient d'une part des instructions sur le partitionnement de disques durs lors du processus d'installation de Red Hat Enterprise Linux et, d'autre part, un aperçu des partitions de disque.
- *Guide de référence de Red Hat Enterprise Linux* ; Red Hat, Inc. — Contient des informations détaillées sur la structure de répertoire utilisée dans Red Hat Enterprise Linux, ainsi qu'un aperçu de NFS.
- *Guide d'administration système de Red Hat Enterprise Linux* ; Red Hat, Inc. — Inclut des chapitres sur les systèmes de fichiers, sur RAID, sur le LVM, sur `devlabel`, sur le partitionnement, sur les quotas de disque, sur NFS et sur Samba.
- *Linux System Administration : A User's Guide* (Administration de systèmes Linux : Guide d'utilisateur) de Marcel Gagne ; Addison Wesley Professional — Contient des informations sur les permissions accordées aux utilisateurs et aux groupes, sur les systèmes de fichiers et les quotas de disque, sur NFS et Samba.
- *Linux Performance Tuning and Capacity Planning* de Jason R. Fink et Matthew D. Sherer ; Sams — Contient des informations sur la performance des disques, de RAID et NFS.
- *Linux Administration Handbook* de Evi Nemeth, Garth Snyder et Trent R. Hein ; Prentice Hall — Contient des informations sur les systèmes de fichiers, le traitement des disques durs, NFS et Samba.

Chapitre 6.

Gestion des comptes utilisateur et de l'accès aux ressources

La gestion des *comptes utilisateur* et des *groupes* représente une partie essentielle de l'administration système au sein d'une entreprise. Mais pour que ce travail de gestion soit efficace, un bon administrateur système doit d'abord comprendre d'une part ce que sont les comptes utilisateur et les groupes et d'autre part, la manière dont ils fonctionnent.

La raison essentielle pour laquelle des comptes utilisateur existent est qu'ils permettent de vérifier l'identité de chaque personne utilisant un système informatique. La deuxième raison justifiant leur existence est qu'ils permettent d'attribuer des ressources et des privilèges d'accès sur une base individuelle, selon les besoins de chaque utilisateur ou groupe.

Les ressources peuvent comprendre des fichiers, des répertoires et des périphériques. Le contrôle de l'accès à ces ressources représente une grande partie du travail quotidien d'un administrateur système ; souvent l'accès à une ressource est contrôlé par des groupes. Ces derniers sont des entités logiques pouvant être utilisées pour regrouper des comptes utilisateur oeuvrant dans un même but. Par exemple, si une organisation dispose de plusieurs administrateurs système, il est possible de tous les regrouper au sein d'un même groupe d'administrateurs système. Il est alors possible d'attribuer au groupe la permission d'accéder à des ressources clé du système. Dans ce sens, les groupes peuvent représenter un outil performant en matière de gestion des ressources et de l'accès.

Les sections suivantes examinent les comptes utilisateur et les groupes de manière plus détaillée.

6.1. Gestion des comptes utilisateur

Comme nous l'avons mentionné précédemment, les comptes utilisateur représentent la méthode selon laquelle un individu est identifié et authentifié auprès du système. Un certain nombre d'éléments différents sont associés aux comptes utilisateur. Il y a tout d'abord le nom d'utilisateur (parfois appelé identifiant). Ensuite vient le mot de passe, suivi des informations de contrôle d'accès.

Les sections suivantes examinent chacun de ces éléments de manière plus détaillée.

6.1.1. Nom d'utilisateur

Du point de vue du système, le nom d'utilisateur (ou identifiant) est la réponse à la question "quelle est votre identité ?" En tant que tel, les noms d'utilisateur doivent satisfaire une obligation — ils doivent être absolument uniques. En d'autres termes, chaque utilisateur doit avoir un nom d'utilisateur qui est strictement différent de tous les autres identifiants de ce système.

En raison de cette obligation, il est essentiel de déterminer — à l'avance — la manière selon laquelle les noms d'utilisateur seront créés. Sinon, vous vous trouverez peut-être dans une situation où vous devrez intervenir chaque fois qu'un nouvel utilisateur effectuera une demande de compte.

Ce dont vous avez besoin est une convention de nommage pour les comptes utilisateur.

6.1.1.1. Convention de nommage

En créant une convention de nommage pour les noms d'utilisateur, vous vous épargnerez de nombreux problèmes. Plutôt que de créer des noms au fur et à mesure que les demandes de compte arrivent (et trouvant de plus en plus difficile de trouver des noms acceptables), il suffit de vous efforcer d'élaborer dès le départ, une convention qui sera ensuite adoptée pour tous les nouveaux comptes créés. Votre convention de nommage peut être très simple ou au contraire, sa description peut être documentée sur plusieurs pages.

La nature de votre convention de nommage devrait toutefois prendre en compte un certain nombre d'éléments dont :

- La taille de votre entreprise
- La structure de votre entreprise
- La nature de votre entreprise

La taille de votre entreprise est importante car elle dicte le nombre d'utilisateurs que votre convention de nommage doit prendre en charge. Par exemple, dans une toute petite entreprise il sera probablement possible d'utiliser le nom de famille de chaque personne. Pour une entreprise plus grande cependant, une telle convention de nommage ne fonctionnerait pas.

La structure d'une entreprise peut également influencer la convention de nommage la plus adéquate. Pour des entreprises dotées d'une structure définie de manière stricte, il peut être approprié d'inclure dans la convention de nommage des éléments de cette structure. Par exemple, vous pourriez inclure le code du service de votre entreprise dans tous les noms d'utilisateur.

Selon la nature globale de votre entreprise, certaines conventions de nommage seront plus appropriées que d'autres. Une entreprise traitant des données hautement confidentielles décidera peut-être d'opter pour une convention de nommage n'établissant aucun lien entre l'individu et son nom. Dans une telle entreprise, le nom d'utilisateur de Maggie McOmie sera peut-être LUH3417.

Ci-dessous figurent des exemples de conventions de nommage que d'autres entreprises ont déjà utilisées :

- Prénom (john, paul, george, etc.)
- Nom de famille (smith, jones, brown, etc.)
- Première initiale, suivie du nom de famille (jsmith, pjones, gbrown, etc.)
- Nom de famille suivi du code du service (smith029, jones454, brown191, etc.)



Astuce

Soyez conscient du fait que toute convention de nommage consistant à ajouter des données à d'autres afin d'obtenir un nom d'utilisateur a le potentiel de créer un identifiant qui pourrait être humoristique, voire offensif. Dans de telles circonstances, même si les noms d'utilisateur sont créés automatiquement, il est recommandé de disposer d'un certain processus de revue, juste au cas où.

Le point commun dans les conventions de nommage décrites ici est qu'il est tout à fait possible d'après ces conventions que deux utilisateurs puissent avoir le même identifiant. On parle dans ce cas-là de *collision*. Étant donné que chaque nom d'utilisateur doit être unique, il est très important de résoudre le problème des collisions, un thème abordé dans la section suivante.

6.1.1.1.1. Comment traiter les collisions

Les collisions sont des réalités inévitables — quelle que soit votre approche, vous devrez à un moment ou à un autre, faire face à une collision. Il est donc important d'inclure dans votre convention de nommage des dispositions à cet égard. Pour ce faire, vous pouvez recourir aux différentes possibilités énumérées ci-dessous :

- Ajout de chiffres au nom d'utilisateur en collision (smith, smith1, smith2, etc.)
- Ajout de données spécifiques à la personne dont le nom d'utilisateur est en collision (smith, esmith, eksmith, etc.)

- Ajout d'informations spécifiques à l'entreprise dont le nom d'utilisateur est en collision (smith, smith029, smith454, etc.)

Il est nécessaire que toute convention de nommage inclue une certaine méthode permettant de résoudre les collisions. Ce faisant, une personne extérieure à l'entreprise aura beaucoup plus de difficultés à déterminer de manière précise le nom d'utilisateur d'une personne. Par conséquent, l'inconvénient de la plupart des conventions de nommage est que l'email occasionnel envoyé au mauvais destinataire devient plus fréquent.

6.1.1.2. Comment traiter les changements de nom

Si votre organisation utilise une convention de nommage basée sur le nom de chaque utilisateur, vous serez inévitablement confronté à un moment ou à un autre au problème du changement de nom. Même si le nom même de la personne ne change pas, il se peut que de temps à autre, le changement du nom d'utilisateur soit nécessaire et ce pour une variété de raisons allant d'un individu n'aimant pas son nom d'utilisateur à un utilisateur au niveau de la direction de votre entreprise souhaitant utiliser son influence pour obtenir un nom d'utilisateur "plus approprié".

Lors du changement de nom d'utilisateur et quelle qu'en soit la raison, il est important de garder à l'esprit les points suivants :

- Le changement doit être effectué dans *tous* les systèmes concernés
- Les mêmes éléments permettant l'identification de l'utilisateur doivent être conservés
- La propriété de tous les fichiers et autres ressources spécifiques à l'utilisateur doit être changée
- Les problèmes liés aux emails doivent être résolus

Avant tout, il est important de vous assurer que le nouveau nom d'utilisateur est bien propagé sur tous les systèmes où le nom d'utilisateur original était utilisé. Si ce n'est pas le cas, toute fonction du système d'exploitation dépendant du nom d'utilisateur fonctionnera sur certains systèmes mais pas sur d'autres. Certains systèmes d'exploitation utilisent des techniques de contrôle d'accès basées sur les noms d'utilisateur ; de tels systèmes sont particulièrement vulnérables aux problèmes découlant de la modification d'un nom d'utilisateur.

De nombreux systèmes d'exploitation utilisent un numéro d'identification des utilisateurs pour la plupart des opérations de traitement effectuées par un utilisateur spécifique. Afin de minimiser le nombre de problèmes découlant du changement de nom d'utilisateur, essayez de conserver le même numéro d'identification pour l'ancien et le nouvel identifiant. En effet, suite au changement du numéro d'identification, il arrive souvent que l'utilisateur ne soit plus en mesure d'accéder à des fichiers et autres ressources dont il était propriétaire sous son ancien nom d'utilisateur.

Si le numéro d'identification de l'utilisateur doit être changé, il est nécessaire de changer la propriété de tous les fichiers et de toutes les ressources spécifiques à l'utilisateur afin de refléter cette nouvelle identification. Ce processus peut être source d'erreur dans la mesure où il y a toujours quelque chose, dans un endroit obscur du système, qui sera oublié.

Les problèmes liés aux emails représentent probablement l'aspect le plus délicat du changement de nom d'un utilisateur. En effet, à moins que des mesures ne soient prises pour assumer ce changement, les emails adressés à l'ancien nom d'utilisateur ne seront pas transférés au nouvel identifiant.

Regrettablement, l'impact des changements de noms d'utilisateur sur les activités de messagerie donne lieu à des problèmes d'ordre multidimensionnel. Au niveau le plus élémentaire, un changement de nom d'utilisateur peut se traduire par une incertitude au niveau du nom d'utilisateur correct de la personne en question. Au premier abord, la situation ne semble pas très problématique — il suffit de communiquer ce changement à tous les membres de l'entreprise. Mais qu'en est-il des individus extérieurs à l'entreprise ayant envoyé un email à cette personne ? Comment devraient-ils être notifiés

du changement ? Et qu'en est-il des listes de diffusion (aussi bien internes qu'externes) ? Comment peuvent-elles être mises à jour ?

Il n'y a pas de réponse simple à ces questions. La meilleure solution consiste peut-être à créer un alias d'email de sorte que tout message électronique envoyé à l'ancien nom d'utilisateur sera automatiquement redirigé vers le nouvel identifiant. Il est alors possible de demander à l'utilisateur d'informer toute personne envoyant un email que leur nom d'utilisateur a changé. Au fil du temps, de moins en moins d'emails seront redirigés par le biais de l'alias, qui pourra plus tard être supprimé.

Bien que l'utilisation d'alias perpétue, dans un sens, une supposition incorrecte (à savoir que l'utilisateur désormais connu sous le nom esmith est toujours connu en tant que ejones), cette méthode est la seule garantissant que l'utilisateur recevra bien les emails qui lui sont adressés.



Important

Si vous utilisez les alias d'email, assurez-vous de bien prendre les mesures adéquates pour protéger l'ancien nom d'utilisateur contre tout potentiel de réutilisation. Si vous n'avez pas pris les mesures nécessaires et qu'un nouvel utilisateur se voit attribuer un ancien nom d'utilisateur, la livraison de courrier (aussi bien pour l'utilisateur d'origine que pour le nouvel utilisateur) sera peut-être interrompue. La nature exacte de l'interruption dépend certes de la manière dont la livraison du courrier est implémentée sur votre système d'exploitation, mais les deux symptômes qui apparaîtront le plus vraisemblablement sont les suivants :

- Le nouvel utilisateur ne reçoit jamais d'emails — ils sont tous redirigés vers l'utilisateur original
- L'utilisateur original soudainement ne reçoit plus d'emails — ils sont tous redirigés vers le nouvel utilisateur

6.1.2. Mots de passe

Si le nom d'utilisateur fournit est la réponse à la question "quelle est votre identité ?", le mot de passe est lui, la réponse à la requête qui en découle logiquement :

"Prouvez votre identité !"

De manière plus formel, un mot de passe est le moyen selon lequel il est possible de confirmer l'authenticité d'une personne affirmant être l'utilisateur spécifié par le nom d'utilisateur. L'efficacité d'un processus d'authentification basé sur le mot de passe dépend énormément de différents aspects du mot de passe :

- Le secret du mot de passe
- La résistance du mot de passe à être deviné
- La résistance du mot de passe face à une attaque force brute

Les mots de passe qui satisfont les points ci-dessus sont dits *forts*, alors que ceux ne satisfaisant pas un ou plusieurs de ces éléments sont qualifiés de *faibles*. La création de mots de passe forts est importante pour une entreprise car ce type de mot de passe est moins susceptible d'être découvert ou deviné. Pour faire respecter l'utilisation de mots de passe forts, les deux options suivantes sont possibles :

- L'administrateur système peut créer des mots de passe pour les utilisateurs.
- L'administrateur système peut laisser les utilisateurs créer leurs mots de passe, mais en vérifiant bien que ces derniers sont suffisamment forts pour être acceptés.

La création de mots de passe pour tous les utilisateurs permet certes de garantir leur force mais, au fur et à mesure que l'entreprise s'agrandit, la tâche devient énorme. De plus, cette méthode augmente le risque que les utilisateurs conservent leurs mots de passe par écrit.

Pour ces raisons, la plupart des administrateurs système préfèrent que les utilisateurs créent eux-mêmes leurs mots de passe. Toutefois, un bon administrateur système prend des mesures pour vérifier la force des mots de passe.

Pour obtenir des instructions sur la création de mots de passe forts, consultez le chapitre intitulé *Sécurité du poste de travail* du *Guide de sécurité de Red Hat Enterprise Linux*.

La nécessité de garder les mots de passe secrets devrait représenter un élément essentiel de l'état d'esprit de tout administrateur système. Toutefois, cet aspect échappe souvent à de nombreux utilisateurs. En fait, nombreux sont ceux qui ne comprennent pas très bien la distinction existant entre les noms d'utilisateur et les mots de passe. Dans de telles circonstances, il est important d'éduquer quelque peu vos utilisateurs afin qu'ils comprennent bien l'importance de conserver leurs mots de passe aussi secrets que leur salaire.

Les mots de passe devraient être aussi difficiles que possible à deviner. Un mot de passe fort est un mot de passe qu'un agresseur ne pourrait pas deviner, même en connaissant bien l'utilisateur.

Une attaque force brute sur un mot de passe consiste à reproduire de manière méthodique (généralement par l'entremise d'un programme appelé *craqueur de mots de passe*) toute combinaison de caractères possibles en espérant à la longue trouver le bon mot de passe. Un mot de passe fort devrait être établi de telle sorte que le nombre de mots de passe potentiels devant être testés soit le plus élevé possible, forçant ainsi l'agresseur à passer beaucoup de temps à essayer de trouver le mot de passe en question.

La force et faiblesse des mots de passe sont des thèmes qui seront abordés de manière plus détaillée dans les sections suivantes.

6.1.2.1. Mots de passe faibles

Comme nous l'avons mentionné précédemment, un mot de passe dit faible ne passe pas l'un des trois tests suivants :

- Le test du secret
- Le test de la résistance du mot de passe à être deviné
- Le test de la résistance du mot de passe à faire face à une attaque force brute

Les sections suivantes montrent les éléments contribuant à la faiblesse des mots de passe.

6.1.2.1.1. Mots de passe courts

Un mot de passe court affiche des faiblesses en matière de sécurité car il est beaucoup plus vulnérable à une attaque force brute. Afin d'illustrer ce point, examinez le tableau ci-dessous dans lequel apparaît le nombre de mots de passe potentiels qui devraient être testés lors d'une attaque force brute. (Les mots de passe sont supposés n'être composés que de lettres minuscules).

Longueur de mot de passe	Mots de passe potentiels
1	26
2	676
3	17,576
4	456,976

Longueur de mot de passe	Mots de passe potentiels
5	11,881,376
6	308,915,776

Tableau 6-1. Longueur de mots de passe contre nombre de mots de passe potentiels

Comme le montre le tableau ci-dessus, le nombre de mots de passe possibles augmente de manière exponentielle avec la longueur du mot de passe.



Remarque

Bien que les exemples fournis dans ce tableau s'arrêtent à six caractères, il ne faut néanmoins pas conclure que des mots de passe de six caractères sont suffisamment longs pour garantir une bonne sécurité. D'une manière générale, plus le mot de passe est long, plus sa sécurité est élevée.

6.1.2.1.2. Jeu de caractères limité

Le nombre de caractères différents utilisés dans la composition d'un mot de passe a un impact considérable sur la capacité d'un agresseur à effectuer une attaque force brute. Par exemple, au lieu d'un choix de 26 caractères différents pouvant être utilisés dans un mot de passe basé seulement sur des lettres minuscules, pourquoi ne pas recourir également à des numéros ? Ce faisant, chaque caractère d'un mot de passe pourra être choisi parmi 36 caractères au lieu de 26. Dans le cas d'un mot de passe composé de six caractères, le nombre de possibilités passe alors de 308,915,776 à 2,176,782,336.

Telle n'est pas la limite des possibilités en matière de mots de passe. En incluant aussi des mots de passe alphanumériques mélangeant majuscules et minuscules (pour les systèmes d'exploitation prenant en charge une telle variété), le nombre de possibilités pour des mots de passe de six caractères augmente alors à 56,800,235,584. En ajoutant d'autres caractères (tels que des signes de ponctuation), l'éventail des possibilités devient encore plus grand, rendant ainsi une attaque force brute beaucoup plus difficile.

Toutefois, il est important de garder à l'esprit que toute attaque contre un mot de passe n'est pas forcément une attaque force brute. Les sections suivantes décrivent d'autres éléments contribuant à la faiblesse d'un mot de passe.

6.1.2.1.3. Mots reconnaissables

De nombreuses attaques contre des mots de passe reposent sur le fait que les gens sont le plus à l'aise avec des mots de passe dont ils peuvent se souvenir. Pour la plupart d'entre eux, les mots de passe le plus facilement mémorisables sont ceux contenant des mots. Par conséquent, la plupart des attaques contre des mots de passe recourent aux dictionnaires. En d'autres termes, l'agresseur utilise des dictionnaires de mots pour tenter de trouver le ou les mots composant le mot de passe.



Remarque

De nombreux programmes craqueurs de mots de passe reposant sur des dictionnaires utilisent les dictionnaires de langues multiples. Ne considérez donc pas que vous disposez d'un mot de passe fort, simplement parce qu'il est composé de mots tirés de langues étrangères.

6.1.2.1.4. Renseignements personnels

Les mots de passe contenant des renseignements personnels (comme le nom ou la date de naissance d'une personne qui vous est chère, un animal domestique ou un numéro d'identification personnel) pourront ou pas être devinés par une attaque de mots de passe basée sur un dictionnaire. Toutefois, si l'agresseur vous connaît personnellement (ou si la personne est suffisamment motivée pour effectuer des recherches sur votre vie personnelle), il sera peut-être en mesure de deviner votre mot de passe avec peu, voire aucune difficulté.

Outre les dictionnaires, de nombreux craqueurs de mots de passe incluent aussi des noms courants, dates et autres informations de ce genre dans leur recherche de mots de passe. Ainsi, même si l'agresseur ne sait pas que votre chien s'appelle Gracie, avec un craqueur de mots de passe puissant, il sera toutefois en mesure de deviner que votre mot de passe est "monchienestgracie".

6.1.2.1.5. Simples transformations de mots

Toute méthode consistant à utiliser comme base pour le mot de passe toute information fournie précédemment et à inverser ensuite l'ordre des caractères ne transformera pas un mot de passe faible en mot de passe fort. En effet, la plupart des craqueurs de mots de passe effectuent ce genre de manipulation élémentaire sur les mots de passe possibles. Parmi ces manipulations figurent aussi la substitution de certaines lettres par des chiffres dans des mots courants. Ci-dessous figurent deux exemples :

- 5AuC1550n pour saucisson
- 1Mp0551bl3 pour impossible

6.1.2.1.6. Mot de passe unique pour de multiples systèmes

Même si vous disposez d'un mot de passe fort, il est fortement déconseillé d'utiliser ce même mot de passe sur plus d'un système. Bien sûr, vous n'avez pas vraiment le choix si les systèmes sont configurés de manière à utiliser un serveur d'authentification central d'un type ou d'un autre, mais dans toute autre situation, il est vivement conseillé d'utiliser des mots de passe différents pour chaque système.

6.1.2.1.7. Mots de passe conservés sur papier

Une autre manière de transformer un mot de passe fort en mot de passe faible consiste à en garder une trace écrite. En écrivant un mot de passe, vous ne devez plus faire face à un problème de secret, vous êtes désormais confronté à un problème de sécurité physique — vous devez maintenant garantir la sécurité de votre morceau de papier. Il n'est par conséquent jamais recommandé de conserver une trace écrite de votre mot de passe.

Toutefois, certaines entreprises doivent légitimement conserver les mots de passe par écrit. Par exemple, dans certaines entreprises les mots de passe écrits font partie d'une procédure visant à faire face au départ de personnel clé (tel que des administrateurs système). Dans de telles situations, le morceau de papier contenant les mots de passe est conservé dans un endroit dont la sécurité physique est garantie et auquel l'accès ne peut avoir lieu qu'avec la coopération de plusieurs personnes. Des chambres fortes à verrous multiples ou la salle des coffres des banques sont souvent utilisés à cet effet.

Toute entreprise songeant à utiliser cette méthode de conservation des mots de passe en cas d'urgence devrait savoir que l'existence de mots de passe écrits ajoute un certain élément de risque quant à la sécurité de leurs systèmes, quel que soit le degré de sécurité selon lequel les mots de passe sont conservés. Les systèmes sont tout particulièrement en danger si tout le monde sait que les mots de passe sont conservés par écrit (et que l'endroit où ils sont conservés est connu).

Regrettablement, les mots de passe écrits ne sont pas souvent inclus dans les plans de secours et ne sont pas conservés dans une chambre forte ; lorsqu'il s'agit de simples utilisateurs, les mots de passe sont généralement conservés dans les endroits suivants :

- Dans le tiroir d'un bureau (verrouillé ou non)
- Sous un placard
- Dans un portefeuille
- Scotché sur le côté du moniteur

Aucun de ces endroits n'est approprié pour conserver un mot de passe écrit.

6.1.2.2. Mots de passe forts

Après avoir examiné les mots de passe faibles, il est temps d'aborder dans les sections suivantes, les caractéristiques que tous les mots de passe forts possèdent.

6.1.2.2.1. Mots de passe longs

Plus un mot de passe est long, moins il y a de chances qu'une attaque force brute réussisse à le deviner. Par conséquent, si votre système d'exploitation le permet, établissez des mots de passe d'une longueur minimale relativement grande pour vos utilisateurs.

6.1.2.2.2. Jeu de caractères étendu

Encouragez autant que possible la création de mots de passe alphanumériques utilisant aussi bien des lettres majuscules que minuscules et conseillez vivement qu'au moins un caractère non alphanumérique soit ajouté dans tout mot de passe, comme par exemple :

- t1Te-Bf,te
- Lb@lbhom

6.1.2.2.3. Mots de passe mémorisables

Un mot de passe est fort pour autant qu'il puisse être mémorisé. Toutefois, la facilité d'un mot de passe à être mémorisé va souvent de paire avec celle à être deviné. Dans de telles circonstances, il est fortement recommandé de donner à votre communauté d'utilisateurs un certain nombre d'astuces quant à la création de mots de passe qui soient certes mémorisables, mais ne puissent pas pour autant être devinés facilement.

Par exemple, prenez un diction ou une citation connus et gardez la première lettre de chaque mot comme base pour la création de votre nouveau mot de passe. Le résultat est mémorisable (étant donné que le diction sur lequel il est basé est lui-même mémorisable) et pourtant, le mot de passe ne contient aucun mot réel.



Remarque

Gardez toutefois bien à l'esprit que l'utilisation de la première lettre de chaque mot composant un diction ne constitue pas une stratégie suffisante pour rendre un mot de passe fort. Assurez-vous de toujours élargir le jeu de caractères utilisé dans les mots de passe en incluant non seulement des caractères alphanumériques en lettres majuscules et minuscules, mais également au moins un caractère spécial.

6.1.2.3. Expiration de mots de passe

Dans la mesure du possible, mettez en place dans votre entreprise une méthode d'expiration des mots de passe. L'expiration des mots de passe est une fonctionnalité (offerte dans de nombreux systèmes d'exploitation) permettant de définir des limites de temps quant à la validité d'un mot de passe donné. À la fin de la durée de vie d'un mot de passe, le système demandera à l'utilisateur de saisir un nouveau mot de passe, qui à son tour sera valide jusqu'à la date d'expiration qui lui est attribuée.

La question clé sur laquelle de nombreux administrateurs système s'interrogent en matière de mots de passe est celle de la durée de vie des mots de passe. Quelle devrait-elle sa valeur ?

En la matière, deux aspects diamétralement opposés sont en jeu, à savoir :

- Aspect pratique pour l'utilisateur
- Sécurité

À une extrême, un mot de passe d'une validité de 99 ans ne représenterait pour l'utilisateur que des désagréments mineurs (voire aucun inconvénient du tout). Toutefois, un tel choix ne se traduirait que par une amélioration mineure (voire nulle) au niveau de la sécurité.

À l'extrême inverse, une durée de vie de 99 minutes pour un mot de passe représenterait un désagrément majeur pour vos utilisateurs. Ceci étant, la sécurité se verrait considérablement renforcée.

Il s'agit en fait de trouver un compromis acceptable entre l'aspect pratique souhaité par vos utilisateurs et les besoins de votre entreprise en matière de sécurité. Pour la plupart des entreprises, les valeurs les plus courantes associées à la durée de vie des mots de passe se situent dans une fourchette allant de quelques semaines à quelques mois.

6.1.3. Informations relatives au contrôle d'accès

Parallèlement à un nom d'utilisateur et un mot de passe, les comptes utilisateurs contiennent aussi des informations relatives au contrôle d'accès. Ces dernières se présentent sous différentes formes selon le système d'exploitation utilisé. Ceci étant, ces informations incluent souvent les éléments suivants :

- Identification spécifique à l'utilisateur qui est valable sur l'ensemble du système
- Identification spécifique au groupe qui est valable sur l'ensemble du système
- Listes des groupes/ressources supplémentaires auxquels l'utilisateur appartient
- Informations relatives à l'accès par défaut devant s'appliquer à l'ensemble des fichiers et ressources créés par l'utilisateur

Dans certaines entreprises, les informations relatives à l'accès d'un utilisateur ne devront peut-être jamais être modifiées. C'est par exemple très souvent le cas avec les postes de travail individuels indépendants. D'autres entreprises, en particulier celles qui utilisent énormément le partage des ressources sur l'ensemble d'un réseau entre les différents groupes d'utilisateurs, nécessitent des modifications importantes au niveau des informations d'accès d'un utilisateur.

La charge de travail nécessaire pour maintenir correctement les informations relatives au contrôle d'accès de vos utilisateurs varie en fonction du degré d'utilisation par votre entreprise, des fonctionnalités de contrôle d'accès dont est doté votre système d'exploitation. Alors qu'il est bon de s'appuyer fortement sur ces fonctionnalités (en fait, c'est peut-être inévitable), une telle approche implique d'une

part que beaucoup plus d'efforts seront nécessaires pour maintenir l'environnement de votre système et d'autre part, que le risque de mal configurer chaque compte utilisateur sera également plus grand.

Par conséquent, si votre entreprise nécessite ce type d'environnement, il est fortement recommandé de documenter sérieusement les étapes précises qu'il faut suivre pour créer et configurer correctement un compte utilisateur. En fait, s'il existe différents types de comptes utilisateur, nous vous conseillons de documenter chacun d'eux (création d'un nouveau compte finances, d'un nouveau compte opérations, etc.).

6.1.4. Gestion quotidienne des comptes et de l'accès aux ressources

Comme on le dit souvent, le seul élément constant est le changement. Pour ce qui est de la communauté des utilisateurs, il en va de même. Les gens arrivent, partent et passent de certaines responsabilités à d'autres. Il est par conséquent essentiel que les administrateurs système soient en mesure de s'adapter aux changements normaux se produisant quotidiennement au sein d'une entreprise.

6.1.4.1. Nouveaux employés

Lorsqu'une nouvelle personne intègre votre entreprise, on lui donne généralement accès à un certain nombre de ressources (selon ses responsabilités). On lui donnera peut-être un emplacement où travailler, un téléphone et la clé de la porte d'entrée.

On lui donnera peut-être également accès à un ou plusieurs ordinateurs de votre entreprise. En tant qu'administrateur système, il vous incombe de vous assurer que tout le processus se déroule de façon adéquate au moment opportun. Comment pouvez-vous vous en assurer ?

Avant de pouvoir faire quoi que ce soit, vous devez être informé de l'arrivée de la nouvelle personne. Cet aspect est traité de manière différente selon les entreprises. Ci-après figurent certaines possibilités utilisées pour garantir le flux de ce type d'informations :

- Création d'une procédure selon laquelle le service du personnel de votre entreprise vous informe lorsqu'une nouvelle personne est recrutée
- Création d'un formulaire que le supérieur de la nouvelle personne employée peut remplir et utiliser pour effectuer une demande de compte au nom de cette dernière

Selon les entreprises, différentes approches sont nécessaires. Quelle que soit l'approche adoptée, il est vital de disposer d'un processus tout à fait fiable, grâce auquel vous pouvez être informé de tout travail nécessaire sur les comptes.

6.1.4.2. Licenciements

Le fait que du personnel quittera votre entreprise est inévitable. Parfois, les événements se dérouleront dans de joyeuses circonstances mais parfois, ces dernières ne seront pas aussi positives. Dans tous les cas, il est essentiel que vous soyez averti de la situation afin que vous puissiez prendre les mesures appropriées.

Au strict minimum, les mesures appropriées devraient inclure les points suivants :

- Désactivation de l'accès de l'utilisateur à tous les systèmes et ressources connexes (généralement en changeant/verrouillant le mot de passe de l'utilisateur)
- Sauvegarde des fichiers de l'utilisateur, juste au cas où ils contiendraient des informations requises dans le futur
- Coordination de l'accès aux fichiers de l'utilisateur par le directeur de l'employé en question

La plus haute priorité consiste à protéger votre système contre l'utilisateur récemment licencié. Cet aspect est particulièrement important lorsque les conditions du départ étaient telles que l'utilisateur

pourrait éprouver des sentiments hostiles envers votre entreprise. Toutefois, même si les circonstances ne sont pas aussi terribles, il est dans le plus grand intérêt de votre entreprise que vous puissiez rapidement et de manière fiable, désactiver l'accès de la personne récemment licenciée.

De telles situations soulignent la nécessité d'un processus vous informant de tout licenciement — préférablement avant même que le licenciement n'ait lieu. Dans ce sens, il est essentiel de travailler en étroite collaboration avec le service du personnel de votre entreprise afin de garantir que vous serez averti de tout licenciement imminent.



Astuce

Lors de "verrouillages" du système suite à des licenciements, le moment où l'opération a lieu est très important. Si le verrouillage a lieu seulement une fois le processus de licenciement achevé, il existe le risque que la personne qui vient d'être licenciée dispose toujours d'un accès non autorisé au sein de l'entreprise. En revanche, si l'opération de verrouillage est effectuée avant le commencement même du processus de licenciement, la personne concernée pourrait être avertie du licenciement imminent, ce qui rendrait le processus beaucoup plus difficile pour toutes les parties concernées.

Le processus de licenciement est généralement amorcé par un entretien entre la personne concernée, son directeur et un représentant du service du personnel de votre entreprise. Par conséquent, en mettant en place un processus vous avertissant du licenciement alors que l'entretien est sur le point de commencer garantit que le moment choisi pour le verrouillage sera tout à fait approprié.

Une fois l'accès désactivé, c'est le moment de faire une copie de sauvegarde des fichiers de l'employé venant d'être licencié. Cette copie des fichiers peut faire partie des sauvegardes standard de votre entreprise ou il peut s'agir d'une procédure de sauvegarde dédiée à la sauvegarde d'anciens comptes utilisateur. Certains aspects tels que les réglementations en matière de rétention de données, la conservation de preuves en cas de poursuites judiciaires pour licenciement injustifié et autres, joueront un rôle important au niveau du choix de la manière la plus appropriée de traiter les sauvegardes.

Dans tous les cas, effectuer une sauvegarde à ce stade est une bonne habitude dans la mesure où l'étape suivante (accès du directeur aux fichiers de la personne récemment licenciée) peut se transformer en l'effacement accidentel de fichiers. Dans de telles circonstances, l'accès à une sauvegarde courante permet de récupérer facilement toute information suite à de tels accidents, simplifiant ainsi le processus aussi bien pour le directeur que pour vous-même.

À ce stade, vous devez déterminer le type d'accès dont le directeur de la personne récemment licenciée a besoin pour l'utilisation des fichiers de cette dernière. Selon votre entreprise et selon la nature des responsabilités de la personne, il se peut qu'aucun accès ne soit nécessaire ou qu'au contraire, un accès total soit requis.

Si l'employé en question a utilisé votre système pour d'autres tâches que l'envoi d'emails peu importants, il est fort probable que le directeur devra examiner les fichiers afin de déterminer ceux devant être conservés et ceux devant être supprimés. À la fin de ce processus, il y a de grandes chances que certains des fichiers seront transmis à la personne assumant les responsabilités de l'employé récemment licencié. Lors des dernières étapes de ce processus, il se peut que votre assistance soit nécessaire mais le directeur sera peut-être en mesure d'effectuer les tâches appropriées lui-même. Tout dépend des fichiers et de la nature des opérations que votre entreprise effectue.

6.1.4.3. Changement d'emploi

Il est relativement simple de répondre à des demandes de création de comptes pour de nouveaux utilisateurs et de s'occuper de la série d'événements nécessaires pour verrouiller un compte lors du licenciement d'un employé. Toutefois, la situation n'est pas aussi claire lorsque les responsabilités d'une personne changent au sein d'une entreprise. Dans certains cas, le compte de la personne devra être modifié alors que dans d'autre, ce ne sera pas nécessaire.

Trois personnes au moins voudront s'assurer que le compte de l'utilisateur est bien reconfiguré de manière à répondre à ses nouvelles responsabilités :

- Vous-même
- L'ancien directeur de l'employé en question
- Le nouveau directeur de l'employé en question

Grâce à cette collaboration, il devrait être possible de déterminer d'une part les mesures à prendre afin de mettre fin aux anciennes responsabilités de l'employé et d'autre part, celles à prendre pour préparer le compte de l'utilisateur pour ses nouvelles responsabilités. À bien des égards, ce processus peut être comparé à la fermeture d'un compte utilisateur existant, suivi de la création d'un nouveau compte utilisateur. En fait, certaines entreprises procèdent de la sorte lors de tout changement de responsabilités.

Toutefois, il est plus probable que l'entreprise conservera le compte de l'utilisateur et le modifiera afin qu'il reflète les nouvelles responsabilités de l'employé en question. Selon cette approche, il est nécessaire de passer méticuleusement en revue le compte lui-même afin de vous assurer qu'il ne dispose que des ressources et privilèges correspondant aux nouvelles responsabilités de l'employé.

Le fait qu'il existe souvent une période de transition pendant laquelle l'utilisateur doit effectuer des tâches faisant partie parfois des anciennes responsabilités et parfois des nouvelles responsabilités, complique quelque peu la situation. À cet égard, l'ancien et le nouveau directeur de l'employé en question peuvent vous aider en vous fournissant la durée de cette période de transition.

6.2. Gestion des ressources de l'utilisateur

La création de comptes utilisateur représente seulement une des tâches faisant partie du travail d'un administrateur système. La gestion des ressources de l'utilisateur est également une tâche essentielle. À cet égard, trois aspects doivent être pris en considération :

- Qui peut avoir accès aux données partagées ?
- Où les utilisateurs peuvent-ils avoir accès à ces données ?
- Quelles barrières sont mises en place afin d'éviter l'abus des ressources ?

Les sections suivantes passent brièvement en revue chacun de ces aspects.

6.2.1. Qui peut avoir accès aux données partagées ?

L'accès d'un utilisateur à une application, fichier ou répertoire spécifiques est déterminé par les permissions données à l'application, au fichier ou au répertoire en question.

De plus, il est souvent utile de pouvoir appliquer des permissions différentes à des classes d'utilisateurs différentes. Par exemple, la mémoire temporaire partagée devrait permettre d'éviter la suppression accidentelle (ou malveillante) des fichiers d'un utilisateur par tout autre utilisateur que lui-même, tout en garantissant un accès complet au propriétaire des fichiers.

L'accès octroyé au répertoire personnel (parfois appelé home ou maison) d'un utilisateur constitue un autre exemple. Seul le propriétaire du répertoire personnel devrait être en mesure de créer ou examiner des fichiers dans cet emplacement. L'accès de tout autre utilisateur devrait être refusé (du moins sans l'autorisation du propriétaire). Cette différenciation au niveau de l'autorisation de l'accès permet non seulement d'augmenter la confidentialité de l'utilisateur mais permet également d'empêcher le détournement de fichiers personnels.

Ceci étant, de nombreuses situations nécessitent l'accès de multiples utilisateurs aux mêmes ressources d'un ordinateur. Dans ce cas précis, la création minutieuse de groupes partagés sera peut-être nécessaire.

6.2.1.1. Groupes et données partagées

Comme nous l'avons mentionné dans l'introduction, les groupes sont des entités logiques pouvant être utilisées pour regrouper des comptes utilisateurs oeuvrant dans un but précis.

Lors de la gestion des utilisateurs au sein d'une entreprise, il est sage d'identifier les données particulières auxquelles certains services devraient avoir accès, celles dont l'accès devrait être refusé à d'autres services et celles qui devraient être partagées par tout le personnel de l'entreprise. En déterminant préalablement ces points précis, il sera plus facile non seulement de créer une structure de groupe appropriée, mais également d'octroyer les permissions adéquates devant s'appliquer aux données partagées.

Par exemple, imaginez que le service des finances doivent tenir une liste des comptes des mauvais payeurs. Le service de recouvrement de dettes doit également avoir accès à cette liste. Si le personnel des deux services fait partie du même groupe appelé `comptes`, ces informations peuvent être placées dans le même répertoire (dont le groupe `comptes` est propriétaire) qui est a des permissions en lecture et écriture s'appliquant à l'ensemble du groupe.

6.2.1.2. Établissement d'une structure de groupe

Parmi les défis auxquels les administrateurs système doivent faire face lors de la création de groupes partagés figurent points suivants :

- Quels groupes créer
- Qui inclure dans un groupe donné
- Quel type de permissions donner à ces ressources partagées

Pour faire face à ces défis, il est utile d'adopter une approche basée sur le bon sens. Une possibilité consiste à copier la structure de votre organisation lors de la création de groupes. Par exemple, si votre entreprise a un service des finances, créez un groupe appelé `finances` auquel tous les membres du personnel de ce service appartiendront. Si les informations financières sont trop confidentielles pour être disponibles dans toute l'entreprise mais sont absolument essentielles pour les échelons supérieurs de la direction de l'entreprise, il suffit d'accorder à la direction des permissions de groupe afin que ses membres puissent avoir accès aux répertoires et données utilisés par le service des finances ; pour ce faire, ajoutez au groupe `finances` tous les membres des échelons supérieurs de la direction de l'entreprise.

Il est également bon d'être très prudent lors de l'octroi de permissions aux utilisateurs. De cette manière, il y a moins de risques que des informations confidentielles ne tombent dans de mauvaises mains.

En traitant la création de la structure des groupes de votre entreprise de la sorte, vous serez plus à même de satisfaire de manière sûre et efficace, les besoins d'accès aux données partagées au sein de votre entreprise.

6.2.2. Où les utilisateurs peuvent-ils avoir accès aux données partagées ?

Lors du partage de données parmi des utilisateurs, il est courant d'avoir un serveur central (ou un groupe de serveurs) mettant certains répertoires à disposition d'autres ordinateurs sur le réseau. De la sorte, les données sont stockées en un seul endroit et la synchronisation des données entre de multiples ordinateurs n'est par conséquent pas nécessaire.

Avant d'adopter cette approche, vous devez d'abord déterminer les systèmes qui devront avoir accès aux données stockées localement. Lors de ce processus, prenez note des systèmes d'exploitation utilisés par les différents systèmes. Ces informations influenceront la facilité avec laquelle vous implémenterez une telle approche étant donné que votre serveur de stockage doit être en mesure de transférer ses données à chacun des systèmes d'exploitation utilisés dans votre entreprise.

Malheureusement, dès l'instant où des données sont partagées entre de multiples ordinateurs d'un même réseau, des risques de conflit au niveau de la propriété des fichiers apparaissent.

6.2.2.1. Problèmes de propriété globale

Le stockage central de données auxquelles de multiples ordinateurs d'un réseau peuvent avoir accès offre un certain nombre d'avantages. Toutefois, supposez pour un instant que chacun de ces ordinateurs ait une liste de comptes utilisateur maintenue localement. Que se passe-t-il si la liste des utilisateurs maintenue sur chacun de ces systèmes n'est pas semblable à celle présente sur le serveur central ? Pis encore, que se passe-t-il si les différentes listes d'utilisateurs présentes sur chacun de ces systèmes ne sont pas homogènes entre elles ?

La situation dépend certes de la manière selon laquelle les utilisateurs et permissions d'accès sont implémentés sur chacun des systèmes, mais dans certains cas, il est fort possible que l'utilisateur A d'un système soit connu en tant qu'utilisateur B sur un autre système. Une telle situation devient vraiment problématique lorsque des données sont partagées entre ces systèmes, dans la mesure où celles auxquelles l'utilisateur A peut avoir accès depuis un système particulier peuvent également être lues par l'utilisateur B d'un autre système.

C'est la raison pour laquelle de nombreuses entreprises utilisent une base de données d'utilisateurs centrale. De cette manière, les listes d'utilisateurs ne se chevauchent pas sur différents systèmes.

6.2.2.2. Répertoires personnels

Un autre aspect auquel les administrateurs système sont confrontés est la possibilité offerte ou non aux utilisateurs d'avoir des répertoires personnels stockés localement.

L'avantage essentiel de la centralisation des répertoires personnels sur un serveur branché au réseau est que si un utilisateur se connecte à un ordinateur quelconque du réseau, il pourra avoir accès aux fichiers contenus dans son répertoire personnel.

L'inconvénient est que si le réseau tombe en panne, les utilisateurs de toute l'entreprise n'auront plus accès à leurs fichiers. Dans certains cas (par exemple dans des entreprises où l'utilisation des ordinateurs portables est très répandue), il n'est pas recommandé d'avoir des répertoires personnels centralisés. Ceci étant, si le déploiement de répertoires personnels centralisés est une option appropriée dans votre situation particulière, votre travail d'administrateur système n'en sera que simplifié.

6.2.3. Quelles barrières sont mises en place afin d'éviter la mauvaise utilisation des ressources ?

L'organisation minutieuse des groupes et l'attribution des permissions pour les ressources partagées représentent certaines des tâches les plus importantes qu'un administrateur système puisse effectuer afin d'éviter la mauvaise utilisation des ressources par les utilisateurs au sein d'une entreprise. Grâce à cette minutie, il est possible de cibler l'interdiction de l'accès aux ressources confidentielles et donc de refuser l'accès aux personnes non autorisées.

Quelle que soit l'approche adoptée par votre entreprise, la meilleure protection contre la mauvaise utilisation des ressources est toujours une vigilance soutenue de la part de l'administrateur système. En surveillant bien la situation, vous éviterez souvent d'être accueilli au bureau un beau matin par une pile de mauvaises surprises en attente de résolution.

6.3. Informations spécifiques à Red Hat Enterprise Linux

Les sections suivantes examinent certaines des caractéristiques spécifiques de Red Hat Enterprise Linux en relation avec l'administration des comptes utilisateur et des ressources connexes.

6.3.1. Comptes utilisateur, groupes et permissions

Sous Red Hat Enterprise Linux, un utilisateur peut se connecter au système et utiliser toutes les applications ou tous les fichiers auxquels il a accès une fois qu'un compte utilisateur normal a été créé. Red Hat Enterprise Linux décide lui-même si un utilisateur peut avoir accès ou non à ces ressources, en fonction des permissions qui lui sont assignées.

Trois permissions différentes peuvent être appliquées sur les fichiers, répertoires et applications. Ces permissions servent à contrôler les différents types d'accès autorisés. Dans une liste de répertoires, différentes lettres symbolisent différentes permissions. Les symboles suivants sont utilisés pour les différentes permissions :

- `r` — Indique qu'une certaine catégorie d'utilisateurs est autorisée à lire (ou read) le fichier.
- `w` — Indique qu'une certaine catégorie d'utilisateurs est autorisée à écrire (ou write) le fichier.
- `x` — Indique qu'une certaine catégorie d'utilisateurs est autorisée à exécuter (ou execute) le fichier.

Un quatrième symbole (`-`) indique qu'aucun accès n'est autorisé.

Chacune des trois permissions est assignée à trois catégories différentes d'utilisateurs, à savoir :

- *propriétaire* — Le propriétaire du fichier ou de l'application (ou owner en anglais).
- *groupe* — Le groupe propriétaire du fichier ou de l'application (ou group en anglais).
- *tout le monde* — Tous les utilisateurs ayant accès au système (ou all en anglais).

Comme nous l'avons mentionné précédemment, il est possible d'afficher les permissions d'un fichier en invoquant la commande `ls -l` pour obtenir un listage au format détaillé (ou long listing). Par exemple, si l'utilisateur `juan` crée un fichier exécutable portant le nom `foo`, la sortie de la commande `ls -l foo` ressemblerait à l'extrait ci-dessous :

```
-rwxrwxr-x 1 juan juan 0 Sep 26 12:25 foo
```

Les permissions données à ce fichier apparaissent au début de la ligne commençant par `rwx`. Cette première série de symboles détermine l'accès octroyé au propriétaire — dans cet exemple, le propriétaire `juan` a un accès total et peut donc effectuer des opérations de lecture, écriture et exécution sur le fichier. La deuxième série de symboles `rwx` définit elle, l'accès octroyé au groupe (dans notre exemple, un accès total), alors que la dernière série de symboles précise les types d'accès accordés à tous les autres utilisateurs. Dans notre exemple, ces derniers ont une permission de lecture et exécution sur le fichier mais ne sont pas en mesure de le modifier de quelque manière que ce soit.

Il faut garder un point important à l'esprit en matière de permissions et comptes utilisateur, à savoir que toute application lancée sur Red Hat Enterprise Linux tourne dans le contexte d'un utilisateur spécifique. En effet, si un utilisateur nommé `juan` exécute une application, cette dernière tourne en utilisant le contexte de `juan`. Toutefois, il se peut que dans certains cas, l'application ait besoin d'un niveau d'accès plus privilégié afin de pouvoir accomplir une tâche donnée. Parmi ces applications figurent celles permettant d'éditer les paramètres du système ou de connecter les utilisateurs. C'est la raison pour laquelle des permissions spéciales ont été créées.

Sous Red Hat Enterprise Linux, trois permissions spéciales sont disponibles, à savoir :

- *setuid* — Utilisée seulement pour les applications, cette permission indique que l'application en question est supposée être exécutée en tant que propriétaire du fichier et non pas en tant que l'utilisateur exécutant l'application. Cette permission spéciale est représentée par le caractère `s`

remplaçant le symbole `x` dans la catégorie propriétaire. Si le propriétaire du fichier n'a pas les permissions d'exécution, le caractère apparaît en majuscule en tant que `S` pour l'indiquer.

- *setgid* — Utilisée essentiellement pour les applications, cette permission indique que l'application doit être exécutée en tant que le groupe propriétaire du fichier et non pas en tant que le groupe exécutant l'application.

Lorsque cette permission spéciale s'applique à un répertoire, tous les fichiers créés au sein de ce répertoire sont la propriété du groupe propriétaire du répertoire, et non pas celle du groupe de l'utilisateur créant le fichier. La permission *setgid* est représentée par le caractère `s` à la place du caractère `x` dans la catégorie groupe. Si le groupe propriétaire du fichier n'a pas les permissions d'exécution, le caractère apparaît en majuscule en tant que `S` pour l'indiquer.

- *sticky bit* — Utilisée essentiellement sur les répertoires, ce bit stipule qu'un fichier créé dans le répertoire ne peut être supprimé que par l'utilisateur qui l'a créé. Le caractère `t` remplaçant le caractère `x` dans la catégorie tout le monde représente cette permission spéciale. Si la catégorie tout le monde n'a pas les permissions d'exécution, le caractère `T` apparaît en majuscule.

Sous Red Hat Enterprise Linux, la valeur par défaut de sticky bit est le répertoire `/tmp/` pour la même raison.

6.3.1.1. Noms d'utilisateur et UID, Groupes et GID

Dans Red Hat Enterprise Linux, un compte utilisateur et des noms de groupe existent essentiellement pour la commodité des utilisateurs. Dans le système même, des identifiants numériques sont utilisés. Pour les utilisateurs, cet identifiant est connu en tant que *UID*, alors que pour les groupes, il est connu en tant que *GID*. Des programmes qui fournissent des informations sur l'utilisateur ou le groupe convertissent les valeurs des UID/GID en équivalents plus lisibles par tout un chacun.



Important

Les UID et GID doivent être globalement uniques dans tout le système d'une organisation si des fichiers ou ressources sont destinés à être partagés sur un réseau. Dans le cas contraire, quels que soient les contrôles d'accès mis en place, il est possible qu'ils ne fonctionnent pas correctement dans la mesure où ils reposent sur les UID ou GID et non pas sur les noms d'utilisateur ou de groupe.

Plus précisément, si les fichiers `/etc/passwd` et `/etc/group` stockés sur un serveur de fichiers et sur le poste de travail d'un utilisateur contiennent des UID et GID différents, il est possible que des problèmes de sécurité résultent de la mauvaise application des permissions.

Par exemple, si l'utilisateur `juan` a un UID de 500 sur un ordinateur de bureau, les fichiers que `juan` crée sur un serveur de fichiers se verront attribuer l'UID propriétaire de 500. Toutefois, si l'utilisateur `bob` se connecte localement au serveur de fichiers (ou même à tout autre ordinateur) et que le compte de `bob` a lui aussi un UID de 500, `bob` aura un accès complet aux fichiers de `juan` et vice versa.

Il est par conséquent essentiel d'éviter à tout prix les collisions entre UID et GID.

Il existe deux cas dans lesquels la valeur numérique d'un UID ou d'un GID a une signification particulière. La valeur zéro (0) donnée à un UID et à un GID est utilisée pour le super-utilisateur ou `root` et, à ce titre, est traitée d'une manière particulière par Red Hat Enterprise Linux — en effet, un accès total est automatiquement accordé.

Le deuxième cas est celui dans lequel les UID et GID d'une valeur inférieure à 500 sont réservés exclusivement pour le système. Contrairement à un UID/GID de zéro (0), les UID et GID d'une valeur inférieure à 500 ne sont pas traités différemment par Red Hat Enterprise Linux. Toutefois, ces UID/GID ne sont jamais attribués à un utilisateur car il est fort possible qu'un certain composant du système les utilise actuellement ou qu'il les utilisera à un moment ou à un autre dans le futur. Pour obtenir de plus amples informations sur ces utilisateurs et groupes standard, reportez-vous au chapitre intitulé *Utilisateurs et groupes* du *Guide de référence de Red Hat Enterprise Linux*.

Lors de l'ajout de nouveaux utilisateurs à l'aide des outils standard de Red Hat Enterprise Linux pour la création de nouveaux utilisateurs, les nouveaux comptes utilisateur se voient attribuer le premier UID et GID disponible en commençant par 500. Le nouveau compte suivant recevra une valeur UID/GID de 501, celui d'après un UID/GID de 502 et ainsi de suite.

Les différents outils de création d'utilisateurs disponibles sous Red Hat Enterprise Linux seront examinés brièvement à la fin de ce chapitre. Avant de passer ces outils en revue, il convient d'examiner d'abord les fichiers utilisés par Red Hat Enterprise Linux pour définir les comptes et groupes du système.

6.3.2. Fichiers contrôlant les comptes utilisateur et groupes

Sur Red Hat Enterprise Linux, les informations relatives aux comptes utilisateur et groupes sont stockées dans divers fichiers texte contenus dans le répertoire `/etc/`. Lorsqu'un administrateur système crée de nouveaux comptes utilisateur, il doit soit modifier ces fichiers manuellement, soit utiliser des applications pour effectuer les modifications requises.

La section suivante examine les fichiers du répertoire `/etc/` qui, sous Red Hat Enterprise Linux, contiennent des informations sur les utilisateurs et les groupes.

6.3.2.1. `/etc/passwd`

Le fichier `/etc/passwd`, examinable par tout un chacun, contient une liste d'utilisateurs dans laquelle chacun d'eux apparaît sur une ligne différente. Sur chaque ligne figure une liste d'éléments séparés les uns des autres par deux points fournissant les informations suivantes :

- *Nom d'utilisateur* — Le nom ou identifiant que l'utilisateur saisit lorsqu'il se connecte au système.
- *Mot de passe* — Contient le mot de passe codé (ou le symbole `x` si des mots de passe masqués sont utilisés — ce point sera traité ultérieurement).
- *ID utilisateur (UID)* — L'équivalent numérique du nom d'utilisateur qui est référencé par le système et les applications lors de l'établissement des privilèges.
- *ID Groupe (GID)* — L'équivalent numérique du nom du groupe primaire qui est référencé par le système et les applications lors de l'établissement des privilèges.
- *GECOS* — Ainsi nommé pour des raisons historiques, le champ GECOS¹ qui est facultatif, sert à stocker des informations supplémentaires (telles que le nom complet de l'utilisateur). Il est possible de stocker dans ce champ de multiples entrées sous forme d'une liste dont les éléments sont séparés par des virgules. Des utilitaires tels que `finger` permettent d'accéder à ce champ afin de saisir des informations supplémentaires sur l'utilisateur.
- *Répertoire personnel* — Le chemin d'accès absolu au répertoire personnel (aussi appelé répertoire home ou maison) de l'utilisateur, comme par exemple, `/home/juan/`.
- *Shell* — Le programme lancé automatiquement lors de chaque connexion de l'utilisateur. Ce dernier est généralement un interpréteur de commandes (souvent appelé un *shell*). Sous Red Hat Enterprise Linux, la valeur par défaut est `/bin/bash`. Si ce champ est laissé blanc, `/bin/sh` sera la valeur utilisée. Si la valeur choisie correspond à un fichier qui n'existe pas, l'utilisateur ne sera pas en mesure de se connecter au système.

Ci-dessous figure l'exemple d'une entrée présente dans `/etc/passwd`:

1. L'acronyme GECOS signifie General Electric Comprehensive Operating Supervisor. Ce champ était utilisé dans le passé par Bell Labs dans l'implémentation UNIX d'origine. Le laboratoire avait de nombreux ordinateurs dont un exécutant GECOS. Ce champ était utilisé pour stocker des informations lorsque le système UNIX envoyait des lots et des travaux d'impression au système GECOS.

```
root:x:0:0:root:/root:/bin/bash
```

Cette ligne montre que le super-utilisateur (ou `root`) dispose d'un mot de passe masqué et que la valeur de UID et GID est 0. L'utilisateur `root` a `/root/` comme répertoire personnel et utilise `/bin/bash` comme shell.

Pour obtenir de plus amples informations sur `/etc/passwd`, consultez la page de manuel de `passwd(5)`.

6.3.2.2. `/etc/shadow`

Étant donné que le fichier `/etc/passwd` doit être examinable par tout utilisateur (la raison principale étant que ce fichier est utilisé pour effectuer la conversion de l'UID en nom d'utilisateur), il est risqué de stocker les mots de passe de tous les utilisateurs dans `/etc/passwd`. Certes, les mots de passe sont codés. Néanmoins, il est tout à fait possible d'effectuer une attaque contre des mots de passe si leur format codé est disponible.

Si un agresseur peut se procurer une copie du fichier `/etc/passwd`, il peut facilement orchestrer une attaque en secret. Au lieu de risquer d'être détecté en tentant de se connecter à l'aide de chacun des mots de passe potentiels générés par un programme craqueur de mots de passe, un agresseur peut utiliser un tel programme de la manière suivante :

- Un craqueur de mots de passe génère des mots de passe potentiels
- Chaque mot de passe potentiel est alors codé en utilisant le même algorithme que celui du système
- Le mot de passe potentiel ainsi codé est alors comparé à la liste des mots de passe cryptés présente dans `/etc/passwd`

L'aspect le plus dangereux d'une telle attaque est qu'elle peut avoir lieu sur un système très éloigné de votre entreprise. Ainsi, l'agresseur peut utiliser le matériel le plus puissant qu'il soit et peut traiter un nombre impressionnant de mots de passe en une très courte durée.

Telle est la raison pour laquelle le fichier `/etc/shadow` d'une part, ne peut être examiné que par le super-utilisateur et d'autre part contient des mots de passe (et en option, des informations sur l'expiration des mots de passe) pour chaque utilisateur. Comme dans le fichier `/etc/passwd`, les informations relatives à chaque utilisateur se trouvent sur une ligne différente. Chacune de ces lignes apparaît sous la forme d'une liste d'éléments séparés par deux points et inclut les informations suivantes :

- *Non d'utilisateur* — Le nom ou identifiant (Username en anglais) que l'utilisateur saisit lorsqu'il se connecte au système. Cet élément permet à l'application **login** d'extraire le mot de passe de l'utilisateur (et les informations connexes).
- *Mot de passe crypté* — Le mot de passe d'une longueur de 13 à 24 caractères. Ce dernier est codé soit à l'aide de la fonction de bibliothèque `crypt(3)`, soit à l'aide de l'algorithme de hashage md5. Dans ce champ, des valeurs autres qu'un mot de passe hashé ou codé selon un format valide sont utilisées pour contrôler les connexions de l'utilisateur et indiquer le statut du mot de passe. Par exemple, si la valeur est `!` ou `*`, le compte est verrouillé et l'utilisateur n'est pas autorisé à se connecter. Si la valeur est `!!`, un mot de passe n'a jamais été établi auparavant (et l'utilisateur, n'ayant pas de mot de passe, ne pourra pas se connecter).
- *Date du dernier changement du mot de passe* — Le nombre de jours s'étant écoulé entre le 1er janvier 1970 (date à laquelle ont fait aussi référence sous le terme *époque*) et la date du dernier changement de mot de passe. Cet élément est utilisé de concert avec les champs relatifs à l'expiration du mot de passe figurant ci-dessous.
- *Nombre de jours avant tout changement de mot de passe* — Le nombre minimum de jours devant s'écouler avant que le mot de passe ne puisse être changé.

- *Nombre de jours avant un changement de mot de passe nécessaire* — Le nombre minimum de jours devant s'écouler avant que le mot de passe ne doive être changé.
- *Nombre de jours avertissant d'un changement de mot de passe imminent* — Le nombre de jours précédent l'expiration d'un mot de passe pendant lesquels l'utilisateur est averti de l'expiration imminente du mot de passe.
- *Le nombre de jours précédant la désactivation du compte* — Le nombre de jours pouvant s'écouler avant que le compte ne soit désactivé.
- *Date de désactivation du compte* — La date (exprimée en tant que le nombre de jours écoulés depuis l'époque) à partir de laquelle le compte a été désactivé.
- *Un champ réservé* — Un champ qui n'est pas pris en compte dans Red Hat Enterprise Linux.

Ci-après figure l'exemple d'une ligne tirée du fichier `/etc/shadow` :

```
juan:$1$.QKDPc5E$SW1k.jRWexrXYgc98F.:12825:0:90:5:30:13096:
```

Cette ligne montre les informations suivantes s'appliquant à l'utilisateur `juan` :

- Le dernier changement de mot de passe date du 11 février 2005
- Le mot de passe peut être changé à tout moment puisqu'aucun délai n'existe
- Le mot de passe doit être changé tous les 90 jours
- L'utilisateur recevra un avertissement cinq jours avant la date d'expiration du mot de passe
- Le compte sera désactivé 30 jours après la date d'expiration du mot de passe si aucune tentative de connexion n'est effectuée
- La validité du compte viendra à échéance le 9 novembre 2005

Pour obtenir de plus amples informations sur le fichier `/etc/shadow`, consultez la page de manuel de `shadow(5)`.

6.3.2.3. `/etc/group`

Le fichier `/etc/group`, examinable par tout utilisateur, contient une liste de groupes où chacun d'eux figure sur une ligne différente. Chaque ligne, composée de quatre champs apparaissant sous forme de liste dont les éléments sont séparés par deux points, inclut les informations suivantes :

- *Nom du groupe* — Le nom du groupe qui est utilisé par différents programmes utilitaires comme identifiant lisible pour le groupe.
- *Mot de passe du groupe* — S'il existe, il permet aux utilisateurs qui ne font pas partie du groupe de le rejoindre en utilisant la commande `newgrp` et en saisissant le mot de passe défini. La présence d'un caractère `x` minuscule dans ce champ indique que des mots de passe masqués sont utilisés pour le groupe.
- *ID du groupe (GID)* — L'équivalent numérique du nom de groupe qui est utilisé par le système d'exploitation et par les applications lors de l'établissement des privilèges d'accès.
- *Liste des membres* — Une liste des utilisateurs appartenant au groupe dont les éléments sont séparés par une virgule.

Ci-après figure l'exemple d'une ligne tirée du fichier `/etc/group` :

```
general:x:502:juan,shelley,bob
```

Cette ligne montre que le groupe `general` utilise des mots de passe masqués, qu'il a un GID de 502 et que `juan`, `shelley` et `bob` sont des membres du groupe.

Pour obtenir de plus amples informations sur `/etc/group`, reportez-vous à la page de manuel de `group(5)`.

6.3.2.4. `/etc/gshadow`

Le fichier `/etc/gshadow`, examinable seulement par le super-utilisateur, contient un mot de passe codé pour chaque groupe ainsi que des informations sur les membres du groupe et sur les administrateurs. Tout comme dans le fichier `/etc/group`, les informations sur chaque groupe apparaissent sur une ligne différente. Sur chacune d'elles apparaît une liste dont les éléments séparés les uns de sautres par une virgule, fournissent les informations suivantes :

- *Nom du groupe* — Le nom du groupe qui est utilisé par différents programmes utilitaires comme identifiant lisible pour le groupe.
- *Mot de passe crypté* — Le mot de passe codé du groupe. S'il est établi, les membres qui n'appartiennent pas au groupe peuvent le rejoindre en saisissant le mot de passe de ce dernier à l'aide de la commande `newgrp`. Si la valeur de ce champ est `!`, aucun utilisateur n'est autorisé à accéder au groupe à l'aide de la commande `newgrp`. Une valeur correspondant à `!!` est traitée de la même manière que `!` — toutefois, elle indique en plus qu'un mot de passe n'a jamais été établi auparavant. Finalement, si la valeur est nulle, seuls les membres du groupe peuvent se connecter au groupe.
- *Administrateurs du groupe* — Les membres du groupe énumérés dans ce champ (dans une liste dont les éléments sont séparés les uns des autres par une virgule) peuvent ajouter ou retirer des membres à l'aide de la commande `gpasswd`.
- *Membres du groupe* — Les membres du groupe énumérés dans ce champ (dans une liste dont les éléments sont séparés les uns des autres par une virgule) sont des membres normaux du groupe ne pouvant pas effectuer de tâches d'administration.

Ci-après figure l'exemple d'une ligne tirée du fichier `/etc/gshadow` :

```
general:!!:shelley:juan,bob
```

Cette ligne montre que le groupe `general` n'a pas de mot de passe et ne permet pas aux utilisateurs n'en faisant pas partie de l'intégrer à l'aide de la commande `newgrp`. De plus, `shelley` est un administrateur du groupe alors que `juan` et `bob` eux, sont des membres normaux ne disposant pas de privilèges administratifs.

Étant donné que la modification manuelle de ces fichiers peut être la source d'erreurs de syntaxe, il est plutôt conseillé de recourir aux applications fournies avec Red Hat Enterprise Linux pour effectuer ce genre d'opérations. La section suivante passe en revue les outils permettant d'effectuer ces opérations.

6.3.3. Applications pour les comptes utilisateur et groupes

Sur des systèmes Red Hat Enterprise Linux, deux types d'applications élémentaires peuvent être utilisés lors de la gestion des comptes utilisateur et des groupes :

- L'application graphique **Gestionnaire d'utilisateurs**
- Une suite d'outils en ligne de commande

Pour obtenir des instructions détaillées sur l'utilisation du **Gestionnaire d'utilisateurs**, reportez-vous au chapitre intitulé *Configuration des utilisateurs et groupes* du *Guide d'administration système de Red Hat Enterprise Linux*.

Alors que l'application **Gestionnaire d'utilisateurs** et les utilitaires en ligne de commande effectuent tous plus ou moins la même tâche, les outils en ligne de commande ont l'avantage de pouvoir être scriptés et permettent par conséquent une automatisation plus facile de leurs tâches.

Le tableau ci-dessous passe en revue certains des outils en ligne de commande les plus couramment utilisés pour la création et la gestion des comptes utilisateur et des groupes :

Application	Fonction
<code>/usr/sbin/useradd</code>	Ajoute les comptes utilisateur. Cet outil est aussi utilisé pour préciser s'il s'agit d'une appartenance primaire ou secondaire au groupe.
<code>/usr/sbin/userdel</code>	Supprime des comptes utilisateur.
<code>/usr/sbin/usermod</code>	Modifie les attributs des comptes y compris certaines fonctions liées à l'expiration de mots de passe. Pour un contrôle plus minutieux, utilisez la commande <code>passwd</code> . Il est aussi possible d'utiliser <code>usermod</code> pour préciser s'il s'agit d'une appartenance primaire ou secondaire au groupe.
<code>passwd</code>	Permet d'établir les mots de passe. Bien que cette commande soit essentiellement utilisée pour changer le mot de passe d'un utilisateur, elle contrôle également toutes les facettes de l'expiration des mots de passe.
<code>/usr/sbin/chpasswd</code>	Lit le contenu d'un fichier composé de paires nom d'utilisateur/mot de passe et met à jour le mot de passe de chaque utilisateur en conséquence.
<code>chage</code>	Modifie les politiques d'expiration des mots de passe des utilisateurs. La commande <code>passwd</code> peut également remplir cette fonction.
<code>chfn</code>	Modifie les informations du champ GECOS de l'utilisateur.
<code>chsh</code>	Modifie le shell par défaut de l'utilisateur.

Tableau 6-2. Outils en ligne de commande pour la gestion des utilisateurs

Le tableau ci-dessous examine certains des outils de ligne de commande les plus couramment utilisés pour créer et gérer les groupes :

Application	Fonction
<code>/usr/sbin/groupadd</code>	Ajoute des groupes sans leur assigner de membres. Les programmes <code>useradd</code> et <code>usermod</code> doivent ensuite être utilisés pour assigner des utilisateurs à un groupe donné.
<code>/usr/sbin/groupdel</code>	Supprime des groupes.
<code>/usr/sbin/groupmod</code>	Modifie les noms des groupes ou GID sans changer les membres appartenant aux groupes. Les programmes <code>useradd</code> et <code>usermod</code> doivent ensuite être utilisés pour assigner des utilisateurs à un groupe donné.
<code>gpasswd</code>	Change les membres du groupe et établit des mots de passe afin que des utilisateurs extérieurs au groupe, mais connaissant le mot de passe de ce dernier, puissent l'intégrer. Cette commande permet également de spécifier les administrateurs du groupe.
<code>/usr/sbin/grpck</code>	Vérifie l'intégrité des fichiers <code>/etc/group</code> et <code>/etc/gshadow</code> .

Tableau 6-3. Outils de ligne de commande pour la gestion des groupes

Les outils énumérés jusqu'à présent fournissent aux administrateurs système une grande souplesse au niveau du contrôle de tous les aspects des comptes utilisateur et de appartenance à un groupe. Pour en savoir plus sur la manière dont ils fonctionnent, consultez la page de manuel de chacun d'eux.

Ces applications ne déterminent toutefois pas les ressources que les utilisateurs et groupes contrôlent. Pour contrôler cet aspect, un administrateur système doit recourir aux applications permettant l'établissement de permissions sur les fichiers.

6.3.3.1. Applications pour l'établissement de permissions sur les fichiers

L'établissement des permissions s'appliquant aux fichiers constitue une partie intégrante de la gestion des ressources au sein d'une entreprise. Le tableau ci-dessous examine certains des outils en ligne de commande les plus couramment utilisés à cet effet.

Application	Fonction
chgrp	Change l'identité du groupe propriétaire d'un fichier donné.
chmod	Change les permissions d'accès d'un fichier donné. Cette commande permet également d'assigner des permissions spéciales.
chown	Change la propriété d'un fichier (et peut également changer le groupe).

Tableau 6-4. Outils en ligne de commande pour la gestion des permissions

Il est également possible de modifier ces attributs dans des environnements graphiques GNOME et KDE. Pour ce faire, cliquez à l'aide du bouton droit de la souris sur l'icône du fichier (par exemple, alors que l'icône apparaît dans le gestionnaire de fichiers graphique ou sur le bureau) et sélectionnez **Propriétés**.

6.4. Ressources supplémentaires

Cette section inclut un certain nombre de sources d'informations différentes permettant d'étendre vos connaissances non seulement sur la gestion des comptes et ressources mais également sur les thèmes spécifiques à Red Hat Enterprise Linux qui viennent d'être abordés dans ce chapitre.

6.4.1. Documentation installée

Les ressources suivantes installées lors d'une installation normale de Red Hat Enterprise Linux, peuvent vous aider à développer vos connaissances sur les thèmes abordés dans ce chapitre.

- Entrée de menu **Aide** du **Gestionnaire d'utilisateurs** — Pour apprendre à gérer les comptes utilisateur et les groupes.
- Page de manuel de `passwd(5)` — Pour obtenir des informations supplémentaires sur le format du fichier s'appliquant au fichier `/etc/passwd`.
- Page de manuel de `group(5)` — Pour obtenir des informations sur le format du fichier s'appliquant au fichier `/etc/group`.
- Page de manuel de `shadow(5)` — Pour obtenir des informations sur le format du fichier s'appliquant au fichier `/etc/shadow`.

- Page de manuel de `useradd(8)` — Pour apprendre comment créer et mettre à jour les comptes utilisateur.
- Page de manuel de `userdel(8)` — Pour apprendre comment supprimer les comptes utilisateur.
- Page de manuel de `usermod(8)` — Pour apprendre comment modifier les comptes utilisateur.
- Page de manuel de `passwd(1)` — Pour apprendre comment mettre à jour le mot de passe d'un utilisateur.
- Page de manuel de `chpasswd(8)` — Pour apprendre comment mettre à jour en une seule opération, les mots de passe de plusieurs utilisateurs.
- Page de manuel de `chage(1)` — Pour apprendre comment modifier les informations relatives à l'expiration des mots de passe.
- Page de manuel de `chfn(1)` — Pour apprendre comment modifier les informations contenues dans le champ GECOS d'un utilisateur (*finger*).
- Page de manuel de `chsh(1)` — Pour apprendre comment changer le shell de connexion d'un utilisateur.
- Page de manuel de `groupadd(8)` — Pour apprendre comment créer un nouveau groupe.
- Page de manuel de `groupdel(8)` — Pour apprendre comment supprimer un groupe.
- Page de manuel de `groupmod(8)` — Pour apprendre comment modifier un groupe.
- Page de manuel de `gpasswd(1)` — Pour apprendre comment administrer les fichiers `/etc/group` et `/etc/gshadow`.
- Page de manuel de `grpck(1)` — Pour apprendre comment vérifier l'intégrité des fichiers `/etc/group` et `/etc/gshadow`.
- Page de manuel de `chgrp(1)` — Pour apprendre comment modifier la propriété au niveau du groupe.
- Page de manuel de `chmod(1)` — Pour apprendre comment changer les permissions d'accès sur les fichiers.
- Page de manuel de `chown(1)` — Pour apprendre comment changer le propriétaire et le groupe d'un fichier.

6.4.2. Sites Web utiles

- <http://www.bergen.org/ATC/Course/InfoTech/passwords.html> — Un bon exemple de document utilisé pour transmettre des informations sur la sécurité des mots, aux utilisateurs d'une entreprise.
- <http://www.crypticide.org/users/alecm/> — Page d'accueil de l'auteur d'un des programmes de craquage de mots de passe les plus populaires (Crack). Il est possible de télécharger Crack depuis cette page et de l'utiliser pour estimer le nombre de vos utilisateurs disposant de mots de passe faibles.
- <http://www.linuxpowered.com/html/editorials/file.html> — Un bon aperçu des permissions s'appliquant aux fichiers sous Linux.

6.4.3. Livres sur le sujet

Les livres suivants qui examinent différents problèmes liés à la gestion des comptes et des ressources, constituent de bonnes sources d'informations pour les administrateurs de systèmes Red Hat Enterprise Linux.

- *Guide de sécurité de Red Hat Enterprise Linux* ; Red Hat, Inc. — Ce guide fournit un aperçu de certains aspects liés à la sécurité des comptes utilisateur et examine tout particulièrement le moyen de choisir des mots de passe forts.
- *Guide de référence de Red Hat Enterprise Linux* ; Red Hat, Inc. — Contient des informations détaillées sur les utilisateurs et groupes tels qu'ils existent dans Red Hat Enterprise Linux.
- *Guide d'administration système de Red Hat Enterprise Linux* ; Red Hat, Inc. — Inclut un chapitre sur la configuration des utilisateurs et des groupes.
- *Linux Administration Handbook* (Guide d'administration Linux) de Evi Nemeth, Garth Snyder et Trent R. Hein ; Prentice Hall — Fournit un chapitre sur la maintenance des comptes utilisateur, une section sur la sécurité et sa relation avec les fichiers des comptes utilisateur et une section sur les attributs et permissions des fichiers.

Chapitre 7.

Imprimantes et impression

Les imprimantes représentent une ressource essentielle lors de la création d'une *copie papier* — comme son nom l'indique, une représentation physique des données sur papier — de documents variés pour une utilisation commerciale, universitaire ou personnelle. Les imprimantes sont devenues des périphériques indispensables à tous les niveaux de l'informatique commercial ou institutionnel.

Ce chapitre examine la variété d'imprimantes disponibles et compare leurs utilisations dans des environnements informatiques différents. Il décrit ensuite la manière selon laquelle Red Hat Enterprise Linux prend en charge les opérations d'impression.

7.1. Types d'imprimantes

Comme pour tout autre périphérique d'ordinateur, de nombreux types d'imprimantes sont disponibles. Certaines imprimantes emploient des technologies qui imitent des fonctionnalités manuelles de machines à écrire alors que d'autres vaporisent de l'encre sur du papier ou recourent même à un laser pour créer une image de la page à imprimer. Le matériel de l'imprimante interface avec un ordinateur ou un réseau à l'aide de protocoles parallèle, série ou de mise en réseau de données. Lors de l'évaluation des imprimantes qui seront acquises et déployées dans votre environnement informatique, il est important de prendre en compte un certain nombre de facteurs.

Les sections suivantes examinent les différents types d'imprimantes et les protocoles que ces dernières utilisent pour leur communication avec des ordinateurs.

7.1.1. Considérations en matière d'impression

Plusieurs aspects doivent être pris en compte lors de l'évaluation des fonctionnalités d'une imprimante. Ci-dessous figurent certains des critères les plus couramment utilisés lors de l'évaluation de vos besoins en matière d'impression.

7.1.1.1. Fonction

Afin de déterminer le type d'imprimante approprié à votre environnement, il est essentiel d'évaluer non seulement les besoins de votre entreprise mais également la manière selon laquelle une imprimante peut répondre à ces besoins. En la matière, la question la plus importante à poser est la suivante : "*Que doit-on imprimer ?*" Étant donné qu'il existe des imprimantes spécialisées dans l'impression de texte, d'images ou de toute combinaison des deux, il est important de s'assurer que votre choix fournira l'outil le plus approprié à vos besoins spécifiques.

Si par exemple, pour satisfaire vos besoins vous devez être en mesure d'imprimer des images en couleur de qualité supérieure sur du papier glacé de qualité professionnelle, il est recommandé d'utiliser une imprimante couleur à sublimation de teinture ou à transfert thermique (cire) plutôt qu'une imprimante laser ou à impact.

En revanche, les imprimantes laser et à jet d'encre sont tout à fait adaptées pour l'impression de brouillons ou de documents destinés à une circulation interne (on fait souvent référence à de telles imprimantes haut débit sous le terme d'imprimante pour *groupe de travail*). En déterminant les besoins des utilisateurs, les administrateurs seront en mesure de déterminer le type d'imprimante parfaitement approprié pour la fonction qu'elle devra remplir.

Parmi les autres éléments à prendre en compte figurent le *duplexage* — la capacité d'une imprimante à imprimer sur les deux côtés d'une même page. Dans le passé, les imprimantes ne pouvaient

imprimer que sur un seul côté (un processus aussi appelé impression *simplex*). La plupart des modèles d'imprimantes bas de gamme n'offrent pas les fonctions de duplexage par défaut (ils pourront peut-être néanmoins simuler une méthode manuelle de duplexage qui demandera aux utilisateurs de retourner eux-mêmes les pages). Certains modèles offrent la possibilité d'ajouter du matériel pour permettre le duplexage ; toutefois, cette option rend le montant total de l'investissement en équipement beaucoup plus élevé. Ceci étant, l'impression en duplex peut contribuer à la réduction des coûts à long terme en réduisant la quantité de papier utilisée pour l'impression de documents ; ce faisant, le coût des *consommables* est logiquement réduit — essentiellement le papier.

La taille du papier est un autre élément à prendre en considération. La plupart des imprimantes acceptent les tailles de papier les plus courantes, à savoir :

- *letter* — (8 1/2" x 11")
- *A4* — (210mm x 297mm)
- *JIS B5* — (182mm x 257mm)
- *legal* — (8 1/2" x 14")

Si certains services (tels que les services marketing ou design) ont des besoins particuliers pour la création de posters ou de bannières, il existe des imprimantes *format large* permettant l'impression sur du papier de format *A3* (297mm x 420mm) ou *tabloid* (11" x 17"). Certaines imprimantes permettent même l'impression sur des formats encore plus grands mais elles ne sont généralement utilisées qu'à des fins bien précises, telles que l'impression de bleus.

Lors de l'évaluation d'une imprimante, il est également important de prendre en considération des caractéristiques haut de gamme telles que les modules réseau pour l'impression de groupes de travail et depuis des endroits distants.

7.1.1.2. Coût

Le coût est un autre élément à prendre en considération lors de l'évaluation d'imprimantes. Il n'est toutefois pas suffisant de déterminer le seul coût lié à l'achat de l'imprimante elle-même. D'autres dépenses doivent également être prises en compte, telles que les consommables, les pièces de rechange, les frais de maintenance et tous les éléments devant être ajoutés à l'imprimante afin de répondre aux besoins de l'entreprise.

Comme le nom l'indique, le terme *consommables* est le collectif utilisé pour décrire les produits consommés lors du processus d'impression. Les consommables sont essentiellement les *supports* et *l'encre*.

Les supports correspondent aux matériaux sur lesquels le texte ou l'image sont imprimés. Le choix du support dépend en grande partie du type d'informations devant être imprimé.

Par exemple, pour créer une copie exacte d'une image numérique il est nécessaire d'utiliser un type de papier glacé spécial, capable non seulement de tolérer une exposition prolongée à la lumière naturelle ou artificielle, mais capable également de permettre la reproduction exacte des couleurs ; on fait référence à l'ensemble de ces qualités en tant que *solidité* des couleurs (ou *fastness*). Pour des documents dont une *qualité d'archive* est essentielle afin d'assurer leur durabilité et un niveau professionnel de lisibilité (dans le cas de contrats, résumés ou archives permanentes par exemple), un papier *mat* (ou non glacé) devrait être utilisé. *L'épaisseur* est également un élément important car le chemin-papier de certaines imprimantes n'est pas droit. Ainsi, l'utilisation de papier trop fin ou trop épais peut entraîner des bourrages de papier. Certaines imprimantes ont même la capacité d'imprimer sur *transparents* afin que les informations reproduites soient ensuite projetées sur un écran lors de présentations.

Étant donné que l'utilisation des supports spécialisés tels que ceux mentionnés précédemment peut avoir une influence non négligeable sur le coût des consommables, il est important de prendre ce facteur en considération lors de l'évaluation des besoins d'impression.

Encre est employé ici au sens large du terme car toutes les imprimantes n'utilisent pas de l'encre liquide pour l'impression. Les imprimantes laser utilisent par exemple, une poudre appelée *toner* (ou encre poudreuse) alors que les imprimantes à impact utilisent elles des rubans saturés d'encre. D'autre part, certaines imprimantes spécialisées chauffent l'encre avant de la transférer sur papier alors que d'autres vaporisent de l'encre sur un support d'impression. Les coûts associés au remplacement de l'encre varient considérablement et dépendent de la possibilité de *recharger* (remplir) le conteneur ou de la nécessité de remplacer la *cartouche* d'encre.

7.2. Imprimantes à impact

Les imprimantes à impact représentent les technologies d'impression les plus anciennes encore en production active de nos jours. Certains des plus grands vendeurs d'imprimantes continuent à fabriquer, commercialiser et fournir de l'assistance pour les imprimantes à impact, pièces détachées et fournitures. Ce type d'imprimante est le plus approprié dans des environnements spécialisés où l'impression à moindre coût est vitale. Les trois types d'imprimantes à impact les plus courants sont les imprimantes *matricielles à aiguilles*, *à marguerite* et *ligne*.

7.2.1. Imprimantes matricielles à aiguilles

La technologie derrière l'impression matricielle est assez simple. Le papier est pressé contre un *tambour* (un cylindre recouvert de caoutchouc) et de manière intermittente est tiré vers l'avant au fur et à mesure que le processus d'impression progresse. La *tête d'impression* au fonctionnement électromagnétique se déplace sur la surface du papier et appuie sur le ruban de l'imprimante se trouvant entre le papier et l'aiguille de la tête d'impression. L'impact de la tête d'impression sur le ruban de l'imprimante laisse sur le papier des points d'encre qui ensemble, créent des caractères lisibles par tout un chacun.

Les imprimantes matricielles à aiguilles affichent des différences au niveau de la résolution de l'impression et de la qualité générale, selon qu'elles utilisent des têtes d'impression à 9 ou 24 aiguilles. Plus le nombre d'aiguilles par pouce est important, plus la résolution est élevée. La plupart des imprimantes matricielles ont une résolution maximale d'environ 240 *ppp* (points par pouce, aussi appelé *dpi* de l'anglais *dots per inch*). Bien que la résolution de ce type d'imprimante ne soit pas aussi élevée que celle pouvant être obtenue avec des imprimantes laser ou à jet d'encre, les imprimantes matricielles (ou tout autre imprimante dont l'impression se fait par impact) ont un avantage distinct. Étant donné que la tête d'impression doit appuyer sur la surface du papier avec suffisamment de force pour permettre le transfert de l'encre du ruban sur la page de papier, les imprimantes matricielles sont idéales dans des environnements où des *copies carbonées* doivent être créées en utilisant des documents spéciaux en plusieurs parties. Une couche de carbone (ou tout autre substance permettant la reproduction par impact) recouvre le revers de ces documents permettant ainsi, suite à la pression appliquée, de créer une empreinte sur la feuille de papier qui se trouve au-dessous. Les commerçants et les petites entreprises utilisent souvent des copies carbonées comme reçus ou factures d'achat.

7.2.2. Imprimantes à marguerite

Si vous avez déjà utilisé une machine à écrire manuelle, vous comprendrez facilement le concept technologique derrière les imprimantes à marguerite. Ces dernières sont équipées de têtes d'impression composées de galettes métalliques ou plastiques découpées en *pétales*. Sur chacun d'eux figure la forme d'une lettre (minuscule ou majuscule), d'un nombre ou d'un signe de ponctuation. Le martellement du pétale sur le ruban de l'imprimante entraîne un transfert d'encre sur le papier où la forme précise du pétale est reproduite. Les imprimantes à marguerite sont lentes et bruyantes. Elles ne permettent ni l'impression de graphiques, ni le changement de police de caractères à moins que la galette d'impression ne soit physiquement remplacée. Depuis l'arrivée des imprimantes laser, les

imprimantes à marguerite ne sont généralement plus utilisées dans les environnements informatiques modernes.

7.2.3. Imprimantes ligne

Dans la catégorie des imprimantes à impact et fonctionnant d'une manière semblable à l'imprimante à marguerite figure l'*imprimante ligne*. Au lieu d'utiliser un jeu d'impression, les imprimantes ligne sont équipées d'un mécanisme leur permettant d'imprimer simultanément de multiples caractères sur la même ligne. La base de ce mécanisme peut être un grand *tambour d'impression* tournant ou une *chaîne d'impression* bouclée. Lors de la rotation du tambour ou de la chaîne d'impression au-dessus de la surface du papier, des marteaux électromagnétiques placés derrière le papier pressent ce dernier (et le ruban) sur la surface du tambour ou de la chaîne, imprimant par là même sur le papier, la forme du caractère du tambour ou de la chaîne.

En raison de la nature même du mécanisme d'impression, les imprimantes ligne sont beaucoup plus rapides que leurs homologues matricielles à aiguilles ou à marguerite. Toutefois, elles ont tendance à être bruyantes, ont des capacités multipolice limitées et leur qualité d'impression est souvent inférieure à celle des technologies d'impression plus récentes.

Étant donné que les imprimantes ligne sont utilisées pour leur vitesse, elles utilisent un papier spécial pré-perforé de chaque côté qui permet une *alimentation par tracteur*. Grâce à cette technologie, il est possible d'avoir un dispositif d'impression continu très rapide qui ne nécessite aucune supervision et qui s'arrête seulement lorsque l'imprimante est à cours de papier.

7.2.4. Consommables des imprimantes à impact

De tous les types d'imprimantes, celles à impact semblent le plus économiques car elles utilisent des consommables dont le coût est relativement faible. En effet, les rubans à encre et le papier constituent les coûts primaires récurrents des imprimantes à impact. Néanmoins, étant donné que certaines d'entre elles (généralement les imprimantes ligne ou matricielles à aiguilles) nécessitent du papier pré-perforé pour une alimentation par tracteur, les coûts de fonctionnement peuvent quelque peu augmenter.

7.3. Imprimantes à jet d'encre

Les imprimantes à *jet d'encre* utilisent une des technologies d'impression les plus populaires à l'heure actuelle. En raison de leur coût relativement faible et de leurs capacités d'impression tout usage, les imprimantes à jet d'encre constituent un choix idéal pour les petites entreprises et les bureaux à domicile.

Les imprimantes à jet d'encre utilisent des encres liquides à l'eau et des têtes d'impression avec une série des gicleurs qui vaporisent des gouttelettes d'encre sur la surface du papier. L'ensemble des têtes d'impression est actionné par un moteur à courroie qui les déplace à travers la feuille de papier.

Les imprimantes à jet d'encre étaient à l'origine fabriquées pour une impression en *monochrome* seulement (c'est-à-dire en noir et blanc). Toutefois, le développement de la tête d'impression et l'augmentation des gicleurs ont rendu possible l'utilisation de couleurs supplémentaires à savoir cyan, magenta, jaune et noir. Cette combinaison de couleurs (appelée CMJN ou *CMYK* de l'anglais Cyan, Magenta, Yellow and Black) permet d'imprimer des images avec une qualité très proche de celle obtenue dans un laboratoire de développement photographique (lors de l'utilisation de certains types de papier couché). Lorsque les imprimantes à jet d'encre sont utilisées avec une qualité d'impression de texte nette et très lisible, elles constituent un choix tout-en-un parfaitement adapté à des besoins d'impression aussi bien monochromes que couleur.

7.3.1. Consommables des imprimantes à jet d'encre

Les imprimantes à jet d'encre ont tendance à être peu onéreuses et augmentent en fonction de la qualité d'impression, des fonctions supplémentaires et de leur capacité à imprimer sur des formats supérieurs aux tailles de papier standard de type legal ou letter. Alors que le coût initial d'une imprimante à jet d'encre est inférieur à celui des autres types d'imprimantes, il est important de prendre en compte les coûts associés aux consommables de ce genre d'imprimante. En effet, la vaste demande des imprimantes à jet d'encre couvrant tous les niveaux du monde informatique, d'une utilisation personnelle à une utilisation en entreprise, l'obtention de consommables peut être une opération coûteuse.



Remarque

Lors de l'achat d'une imprimante à jet d'encre, assurez-vous de connaître exactement le genre de cartouche(s) d'encre que la machine utilise. Ce point est particulièrement critique pour des unités couleur. En effet, les imprimantes à jet d'encre CMJN ont besoin d'encre spécifique pour chaque couleur ; néanmoins, un élément important en la matière est de savoir si chaque couleur est conservée dans une cartouche séparée ou non.

Certaines imprimantes utilisent une cartouche à chambres multiples ; à moins qu'il ne soit possible de recharger la cartouche d'une manière ou d'une autre, dès que l'encre d'une couleur est vide, la cartouche entière doit être remplacée. D'autres imprimantes utilisent non seulement une cartouche à chambres multiples pour les couleurs cyan, magenta et jaune mais utilisent également une cartouche séparée pour le noir. Pour les environnements dans lesquels de grandes quantités de texte sont imprimées, le choix d'une telle option peut être avantageux. Ceci étant, la meilleure solution consiste à trouver une imprimante avec des cartouches séparées pour chaque couleur ; il est alors possible de remplacer toute couleur dès que la cartouche est vide.

Certains fabricants d'imprimantes à jet d'encre demandent également qu'un papier enduit spécialement soit utilisé pour l'impression d'images ou de documents de haute qualité. Ce type de papier utilise une pellicule de type semi-brillant à haut-brillant formulée pour l'absorption des encres couleur et permettant d'éviter un *amas d'encre* (ou *clumping*, c'est-à-dire la tendance des encres à eau à se concentrer dans certains endroits où les couleurs se mélangent et créent des bavures ou des tâches d'encre sèche) ou *banding* (lorsque la sortie d'impression contient des bandes horizontales superflues qui apparaissent sur la page imprimée). Reportez-vous à la documentation de votre imprimante pour obtenir des informations sur les types de papiers recommandés.

7.4. Imprimantes laser

Les imprimantes laser, une technologie plus ancienne que les imprimantes à jet d'encre, constituent une autre alternative à l'impression par impact basée sur des produits propriétaires. Les imprimantes laser sont connues pour leur rendement élevé et leur faible coût unitaire. Elles sont souvent déployées dans les entreprises en tant que centre d'impression pour les groupes de travail ou services, des environnements où les exigences en matière de performance, durabilité et rendement sont des critères importants. Étant donné que les imprimantes laser répondent parfaitement à ces exigences (et ce, à un coût modique par page), cette technologie est considérée par beaucoup comme étant le pilier de l'impression en entreprise.

Les imprimantes laser partagent plus ou moins les mêmes technologies que les photocopieuses. Des tambours tirent les feuilles de papier depuis un plateau d'alimentation et la passent à travers un *tambour ionisateur* qui donne au papier une charge électrostatique. En même temps, un tambour d'impression reçoit lui une charge opposée. La surface du tambour qui est alors balayée par un laser est déchargée à certains endroits afin que seuls ne soient chargés les points correspondant au texte ou à l'image devant être imprimée. Cette charge est alors utilisée pour forcer le toner à adhérer à la surface du tambour.

Le papier et le tambour entrent ensuite en contact ; en raison de leurs charges opposées, le toner adhère au papier. Finalement, le papier est acheminé entre des *tambours de fusion* qui chauffent le papier et font fondre le toner qui fusionne alors sur la surface du papier.

7.4.1. Imprimantes couleur laser

Les imprimantes couleur laser en associant les meilleures fonctionnalités de la technologie laser et de la technologie à jet d'encre créent un paquetage idéal pour des imprimantes polyvalentes. La technologie repose sur une impression laser monochrome traditionnelle mais utilise également des éléments supplémentaires pour créer des images et documents couleur. Au lieu d'utiliser seulement un toner noir, les imprimantes laser utilisent une combinaison de toners CMYK (ou CMJN selon l'acronyme français). Le tambour d'impression a deux options : soit il effectue une rotation des couleurs et les dépose une par une, soit il dépose les quatre couleurs sur une plaque et fait passer ensuite la feuille de papier sous le tambour, effectuant par là même le transfert de l'image complète sur le papier. Les imprimantes couleur laser utilisent également de l'*huile de fusion* (fuser oil) avec les tambours de fusion chauffés, ce qui permet non seulement une meilleure adhésion du toner de couleurs sur le papier mais permet également de donner des degrés différents de glaçage à l'image imprimée.

En raison de leurs fonctionnalités avancées, les imprimantes couleur laser sont en général deux fois plus chères (voire plus) que les imprimantes laser monochromes. Lors du calcul du coût total de la propriété en matière de ressources d'impression, certains administrateurs jugeront peut-être utile de séparer la fonctionnalité monochrome (texte) de la fonctionnalité couleur (image) en utilisant d'une part une imprimante laser monochrome dédiée à l'impression de texte et d'autre part, une imprimante laser (ou à jet d'encre) couleur dédiée à l'impression d'images.

7.4.2. Consommables des imprimantes laser

Selon le type d'imprimante laser déployé, les coûts associés aux consommables sont généralement proportionnels au volume des tâches d'impression. Le toner se vend sous forme de cartouches qui sont tout simplement remplacées une fois vides ; toutefois, certains modèles sont vendus avec des cartouches rechargeables. Les imprimantes couleur laser utilisent une cartouche de toner pour chacune des quatre couleurs. De plus, ce type d'imprimante a besoin d'une part, d'huiles de fusion pour faire adhérer le toner au papier et d'autre part, de bouteilles de récupération du toner usagé pour recueillir les excédents de toner. Bien que ces fournitures supplémentaires augmentent les coûts des consommables des imprimantes couleur laser, il est important de noter ici que ce type de consommables est suffisant pour produire en moyenne environ 6000 pages ; cette estimation est bien supérieure à celle de la durée de vie des consommables nécessaires pour les imprimantes à jet d'encre ou à impact. L'importance du type de papier à utilisé étant moins un problème pour les imprimantes laser, le papier standard pour photocopieuses ou copieurs xérogaphiques est tout à fait approprié pour la plupart des tâches d'impression et peut par conséquent être commandé en gros. Toutefois, si vous envisagez d'imprimer des images de haute qualité, vous devriez choisir du papier glacé afin d'obtenir un fini professionnel.

7.5. Autres types d'imprimantes

Il existe également d'autres types d'imprimantes qui sont surtout des imprimantes à fonctions spécifiques utilisées par des entreprises imprimant des graphiques professionnels ou par des entreprises d'édition. Ces imprimantes ne sont toutefois pas vouées à des fins d'impression générales. Étant donné que leur utilisation vise une niche particulière, leurs prix (incluant aussi bien le coût d'achat que les coûts associés aux consommables) ont tendance à être plus élevés que des unités plus courantes.

Imprimantes à cire thermique

Ce type d'imprimante est essentiellement utilisé pour les transparents de présentations commerciales et pour le *proofing* couleur (c'est-à-dire la création de documents et d'images test pour une inspection minutieuse de la qualité, avant que les originaux ne soient envoyés à l'impression sur des imprimantes industrielles offset quatre couleurs). Les imprimantes à cire thermique utilisent généralement des rubans CMJN de la taille d'une feuille qui sont entraînés par des courroies, ainsi que des transparents ou du papier enduit spécialement pour une telle utilisation. Les têtes d'impression contiennent des éléments chauffants qui font fondre chaque couleur de cire sur le papier lors de son passage dans l'imprimante.

Imprimantes à sublimation de teinture

Utilisées dans des entreprises telles que des services bureaux — dans lesquels la qualité professionnelle des documents, brochures et présentations est plus importante que les coûts des consommables — les imprimantes à sublimation de teinture (parfois appelées dye-sub) représentent les piliers de l'impression CMJN de qualité. Le concept derrière les imprimantes à sublimation de teinture est semblable à celui des imprimantes à cire thermique, sauf qu'elles utilisent un film de teinture plastique diffusif au lieu de cire de couleur. La tête d'impression chauffe la pellicule de couleur et vaporise l'image sur un papier traité spécialement à ces fins.

La sublimation de teinture est un procédé très courant dans le monde de l'édition et du design ainsi que dans les milieux de la recherche scientifique dans lesquels une extrême méticulosité et un haut niveau de détail sont nécessaires. Ceci étant, un tel niveau de détail et une telle qualité d'impression se payent et le coût se reflète dans les imprimantes à sublimation qui sont aussi connues pour leurs coûts d'impression par page très élevés.

imprimantes à encre solide

Les imprimantes à encre solide, surtout utilisées dans les industries de conditionnement de produits et de design industriel, sont prisées pour leur capacité à imprimer sur une grande variété de types de papier. Comme le nom l'indique, les imprimantes à encre solide utilisent des bâtonnets d'encre durcie qui sont fondus et dont l'encre à base de cire est vaporisée sur les têtes d'impression à travers de petits gicleurs. Le papier est ensuite enroulé autour d'un cylindre de transfert qui dépose l'encre sur le papier.

Les imprimantes à encre solide sont parfaites pour le prototypage et le proofing de nouveaux designs pour le conditionnement de produits ; ainsi, la plupart des entreprises dont l'activité tourne autour de l'offre de services n'auront pas vraiment besoin de ce type d'imprimante.

7.6. Langages et technologies d'imprimante

Avant l'arrivée de la technologie laser et à jet d'encre, les imprimantes à impact n'étaient capables d'imprimer que du texte standard et justifié, sans variation au niveau de la taille des lettres ou du style de la police. À l'heure actuelle en revanche, les imprimantes peuvent traiter des documents complexes composés non seulement d'images imbriquées, de diagrammes, de tableaux à cadres multiples mais également dans plusieurs langues et le tout, sur une même page. En raison d'une telle complexité, il est nécessaire d'adhérer à certaines conventions au niveau du format, d'où le développement d'un *langage de description de pages* — ou PDL de l'anglais printer description language, un langage spécialisé pour le formatage de documents, développé spécialement pour la communication informatique avec les imprimantes.

Au fil du temps, les fabricants d'imprimantes ont développé leurs propres langages propriétaires pour décrire les formats de documents. Toutefois, de tels langages propriétaires s'appliquent exclusivement aux imprimantes que les fabricants ont développées eux-mêmes. Si par exemple, vous deviez envoyer à l'imprimerie un fichier prêt à l'impression utilisant un LDP propriétaire, il n'y a aucune garantie que votre fichier sera compatible avec les machines reliées à l'imprimante. Le problème de la portabilité commence alors à être exploré.

Xerox® développe le protocole Interpress™ pour sa ligne d'imprimantes mais le reste de l'industrie d'édition n'adopte jamais compétement ce langage. Deux des développeurs à l'origine du protocole Interpress partent de Xerox et fondent Adobe®, une société de logiciels s'adressant essentiellement aux professionnels spécialisés dans les documents et graphiques électroniques. Chez Adobe on développe *PostScript*™, un PDL adopté par de nombreux professionnels. Ce protocole utilise un langage plus élaboré pour décrire le formatage de texte et les informations relatives aux images pouvant être traités par les imprimantes. Au même moment, la société Hewlett-Packard® met au point le protocole *Printer Control Language*™ (ou PCL) pour une utilisation sur sa ligne d'imprimantes laser et à jet d'encre. Les langages PostScript et PCL sont désormais des PDL largement adoptés et par conséquent pris en charge par la plupart des fabricants d'imprimantes.

Les PDL suivent le même principe que les langages de programmation informatique. Lorsqu'un document est prêt à être imprimé, le PC ou le poste de travail prend les images, les informations typographiques et le format du document et les utilisent comme des objets constituant les instructions que l'imprimante devra suivre. L'imprimante traduit ensuite ces objets en *trames* (ou rasters) c'est-à-dire une série de lignes scannées constituant une image du document (appelée processeur d'image tramée ou RIP de l'anglais *Raster Image Processing*) et imprime la sortie sur une page comme une image complète, incluant le texte et tout graphique. Ce flux de travail transforme l'impression de documents de toute complexité en une tâche uniforme et standard permettant de garantir un minimum de variation (voire aucune) lors de l'impression d'un même document sur des modèles d'imprimantes différents. Les PDL sont conçus de manière à être non seulement portables sur tout format mais également adaptables à différentes tailles de papier.

Afin de choisir l'imprimante appropriée, il est nécessaire de déterminer les standards adoptés par les différents services de votre entreprise pour répondre à leurs besoins. La plupart des services utilisent des machines à traitement de texte ou autres logiciels de productivité basés sur le langage PostScript pour transmettre les sorties aux imprimantes. Toutefois, si votre service d'arts graphiques nécessite PCL ou une forme d'impression propriétaire quelconque, vous devez évidemment en tenir compte.

7.7. Imprimantes locales contre imprimantes réseau

Selon les besoins de l'entreprise, il sera peut-être nécessaire d'assigner une imprimante à chaque membre de votre entreprise. Un tel chevauchement des dépenses peut grignoter une partie des budgets impartis et donc diminuer le capital pour d'autres nécessités. Bien que des imprimantes locales reliées par un câble parallèle ou USB à tous les postes de travail représentent une solution idéale pour l'utilisateur, une telle option n'est généralement pas réalisable sur un plan économique.

Les fabricants d'imprimantes ont pris ce besoin en considération en développant des imprimantes de *services* (ou groupe de travail). Ces machines sont généralement solides, rapides et utilisent des consommables dont la durée de vie est longue. Les imprimantes de groupes de travail sont généralement reliées à des serveurs d'impression, un périphérique indépendant (tel qu'un poste de travail reconfiguré) qui traite les travaux d'impression et envoie les sorties vers l'imprimante appropriée lorsque cette dernière est disponible. Parmi les imprimantes de services récentes figurent les interfaces réseau incorporées ou ajoutées, qui éliminent le besoin d'un serveur d'impression attitré.

7.8. Informations spécifiques à Red Hat Enterprise Linux

Les informations suivantes examinent les différentes fonctionnalités spécifiques à Red Hat Enterprise Linux qui ont trait aux imprimantes et à l'impression.

L'**Outil de configuration de l'imprimante** permet aux utilisateurs de configurer une imprimante. Il permet de maintenir le fichier de configuration de l'imprimante, d'imprimer des répertoires de spoule (ou spool) et des filtres.

Red Hat Enterprise Linux 4 utilise le système d'impression CUPS. Si le système a été mis à niveau à partir d'une version précédente de Red Hat Enterprise Linux qui utilisait CUPS, les files d'attente configurées ont été conservées lors du processus de mise à niveau.

Afin de pouvoir utiliser l'**Outil de configuration de l'imprimante** vous devez disposer des privilèges du super-utilisateur (ou root). Pour lancer l'application, sélectionnez le **Menu principal** (sur le panneau) => **Paramètres système** => **Impression** ou vous pouvez également taper la commande `system-config-printer`. Cette dernière détermine automatiquement si une version graphique ou texte doit être lancée selon si la commande a été exécutée à partir d'un environnement graphique X Window ou à partir d'une console en mode texte.

Pour forcer l'**Outil de configuration de l'imprimante** à démarrer en tant qu'application en mode texte, exécutez la commande `system-config-printer-tui` à une invite de shell.



Important

Ne modifiez ni le fichier `/etc/printcap` ni les fichiers du répertoire `/etc/cups/`. Chaque fois que le démon d'imprimante (que ce soit `lpd` ou `cups`) est lancé ou relancé, de nouveaux fichiers de configuration sont créés de façon dynamique. Ces fichiers sont également créés dynamiquement lorsque des modifications sont appliquées avec l'**Outil de configuration de l'imprimante**.

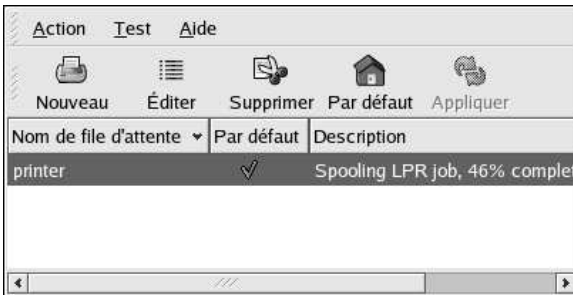


Figure 7-1. Outil de configuration de l'imprimante

Il est possible de configurer les types de files d'attente d'impression suivants :

- **Connectée-localement** — une imprimante directement reliée à votre ordinateur via un port parallèle ou USB.
- **CUPS (IPP) réseau** — une imprimante accessible sur un réseau TCP/IP par le biais du protocole d'impression Internet, également connu sous le nom IPP (de l'anglais Internet Printing Protocol) (par exemple, une imprimante reliée à un autre système Red Hat Enterprise Linux exécutant CUPS sur le réseau).
- **UNIX (LPD) réseau** — une imprimante reliée à un autre système d'impression UNIX auquel l'accès est possible par un réseau TCP/IP (par exemple, une imprimante reliée à un autre système Red Hat Enterprise Linux exécutant LPD sur le réseau).
- **Windows (SMB) réseau** — une imprimante reliée à un autre système qui partage une imprimante sur un réseau SMB (par exemple, une imprimante reliée à un ordinateur Microsoft Windows™).
- **Novell (NCP) réseau** — une imprimante reliée à un autre système qui utilise la technologie de réseau Novell NetWare.
- **JetDirect réseau** — une imprimante directement connectée au réseau par HP JetDirect au lieu d'être reliée à un ordinateur.

**Important**

Si vous ajoutez une nouvelle file d'attente d'impression ou si vous en modifiez une existante, vous devez appliquer les modifications afin qu'elles prennent effet.

Cliquez sur le bouton **Appliquer** afin d'enregistrer tous les changements effectués et de relancer le démon d'imprimante. Les changements ne sont enregistrés dans le fichier de configuration qu'après le redémarrage du démon d'impression. Vous pouvez également sélectionner **Action => Appliquer**.

Pour obtenir de plus amples informations sur la configuration des imprimantes sous Red Hat Enterprise Linux, reportez-vous au *Guide d'administration système de Red Hat Enterprise Linux*.

7.9. Ressources supplémentaires

La configuration de l'impression et l'impression réseau sont des sujets vastes demandant des connaissances et de l'expérience au niveau du matériel, de la mise en réseau et de l'administration système. Pour obtenir de plus amples informations sur le déploiement de services d'imprimantes dans vos environnements, reportez-vous aux ressources énumérées ci-dessous.

7.9.1. Documentation installée

- Page de manuel de `lpr` (1) — Pour apprendre comment imprimer des fichiers spécifiques sur l'imprimante de votre choix.
- Page de manuel de `lprm` (1) — Pour apprendre comment supprimer des travaux d'impression présents dans la file d'attente d'une imprimante.
- Page de manuel de `cupsd` (8) — Pour obtenir des informations sur le démon d'impression CUPS.
- Page de manuel de `cupsd.conf` (5) — Pour en savoir plus sur le format de fichier du fichier de configuration du démon d'impression CUPS.
- Page de manuel de `classes.conf` (5) — Pour en savoir plus sur le format de fichier du fichier de configuration de classe CUPS.
- Fichiers contenus dans `/usr/share/doc/cups-<version>` — Pour en savoir plus sur le système d'impression CUPS.

7.9.2. Sites Web utiles

- <http://www.webopedia.com/TERM/p/printer.html> — Définitions générales des imprimantes et descriptions des différents types d'imprimantes.
- <http://www.linuxprinting.org/> — Base de données de documents sur l'impression ainsi qu'une base de données regroupant environ 1000 imprimantes compatibles avec du matériel Linux.
- <http://www.cups.org/> — Documentation, FAQ et groupes de discussion à propos de CUPS.

7.9.3. Livres sur le sujet

- *Network Printing* de Matthew Gast et Todd Radermacher ; O'Reilly & Associates, Inc. — Ce livre sur l'impression réseau fournit des informations complètes sur l'utilisation de Linux comme serveur d'impression dans des environnements hétérogènes.

- *Guide d'administration système de Red Hat Enterprise Linux*; Red Hat, Inc. — Ce manuel inclut un chapitre sur la configuration de l'imprimante.

Chapitre 8.

Préparation à un sinistre

Il est relativement facile pour un administrateur système d'oublier de se préparer à un éventuel sinistre — ce n'est en effet pas une tâche plaisante et il semble toujours y avoir quelque chose de plus urgent à faire. Néanmoins, la négligence en matière de préparation à un sinistre est une des pires choses qu'un administrateur système puisse faire.

Bien que les terribles sinistres soient souvent ceux qui viennent à l'esprit en premier (tels que les incendies, les inondations ou les orages), les problèmes les plus banals (tels que la coupure accidentelle de câbles par des ouvriers du bâtiment ou même le débordement d'un évier) peuvent s'avérer tout aussi perturbateurs. Dans de telles circonstances, la définition du concept de sinistre qu'un administrateur système doit garder à l'esprit est la suivante : tout événement imprévu pouvant perturber le fonctionnement normal de l'entreprise.

Alors qu'il est absolument impossible de dresser la liste de tous les différents types de sinistres pouvant se produire, cette section examine les facteurs principaux faisant partie de chaque type de sinistre afin que toute confrontation possible à un sinistre puisse être analysée, non pas en termes de probabilité de la situation, mais en termes des facteurs réels qui pourraient entraîner un sinistre.

8.1. Types de sinistres

En général, quatre facteurs différents peuvent engendrer un sinistre, à savoir :

- des pannes matérielles
- des pannes logicielles
- des pannes environnementales
- des erreurs d'origine humaine

8.1.1. Pannes matérielles

Les pannes matérielles elles-mêmes sont faciles à comprendre — le matériel tombe en panne et arrête toute activité. Les aspects les plus difficiles à comprendre sont la nature des pannes et la manière de minimiser votre contact avec ces pannes. Ci-après figurent certaines des approches que vous pouvez utiliser pour limiter l'impact d'un éventuel sinistre.

8.1.1.1. Stockage de matériel de rechange

Dans le cas le plus simple, une exposition due à des problèmes matérielles peut être réduite en gardant du matériel de rechange. Évidemment, cette approche suppose deux choses :

- D'une part, qu'une personne sur place dispose des compétences nécessaires pour diagnostiquer le problème, identifier le matériel défaillant et le remplacer.
- D'autre part, que du matériel de rechange soit disponible pour le matériel défaillant.

Ces aspects sont abordés de manière plus détaillée dans les sections suivantes.

8.1.1.1.1. Compétences adéquates

Selon votre expérience passée et le matériel utilisé, le fait de disposer des connaissances nécessaires ne sera peut-être pas un problème. Toutefois, si vous n'avez pas travaillé avec du matériel dans le passé, vous souhaitez peut-être consulter des institutions d'enseignement de votre communauté locale pour explorer l'éventail des cours d'introduction consacrés à la réparation de PC. Bien qu'un tel cours ne soit pas en soi et par lui-même suffisant pour vous préparer à affronter des problèmes avec des serveurs de niveau entreprise, il représente néanmoins une excellente manière d'acquérir des connaissances de base en la matière (telles que la bonne manipulation des outils et composants, procédures élémentaires de diagnostic, etc.).



Astuce

Avant d'adopter une approche consistant à effectuer d'abord les réparations vous-même, assurez-vous que le matériel en question :

- n'est plus sous garantie
- n'est couvert par aucun contrat d'assistance/maintenance

Si vous tentez d'effectuer des réparations sur du matériel couvert par une garantie et/ou un contrat d'assistance, vous serez probablement en infraction avec les conditions de ces accords et risquerez par là-même de compromettre la couverture continue de votre matériel.

Toutefois, même en disposant d'un minimum de compétences, il sera peut-être possible de bien diagnostiquer et remplacer le matériel défaillant — à condition que vous choisissiez correctement votre stock de rechange

8.1.1.1.2. Que stocker ?

Cette question illustre la nature à facettes multiples de toute tâche en relation avec la récupération après un sinistre. Lorsque vous considérez le matériel à stocker, gardez à l'esprit les éléments suivants :

- La durée maximum du temps d'indisponibilité possible
- Les compétences nécessaires pour effectuer la réparation
- Le budget disponible pour des pièces de rechange
- L'espace nécessaire pour le stockage des pièces de rechange
- Tout autre matériel qui pourrait utiliser les mêmes pièces de rechange

Chacun de ces aspects a une influence sur les différents types de pièces de rechange qui devraient être stockés. Par exemple, le stockage de systèmes complets pourrait minimiser le temps d'indisponibilité et leur installation ne nécessite que des compétences minimales, mais une telle stratégie serait beaucoup plus coûteuse que le stockage d'un module CPU et RAM de rechange sur une étagère. Cette dépense est néanmoins peut-être justifiable si votre entreprise dispose de plusieurs dizaines de serveurs identiques qui pourraient profiter d'un seul système de rechange.

Indépendamment de la décision finale, la question suivante, abordée ci-après, est inévitable.

8.1.1.1.2.1. Quelle quantité de matériel doit être stockée ?

Cette question des niveaux de stock pour le matériel de rechange a également de multiples facettes. Toutefois, les principaux aspects sont les suivants :

- La durée maximum du temps d'indisponibilité possible

- L'estimation du taux de panne
- L'estimation de la durée nécessaire au réapprovisionnement du stock
- Le budget disponible pour des pièces de rechange
- L'espace nécessaire pour le stockage des pièces de rechange
- Tout autre matériel qui pourrait utiliser les mêmes pièces de rechange

Dans le cas extrême où un système peut être indisponible pour un maximum de deux jours et où une pièce de rechange ne serait probablement utilisée qu'une fois par an avec la possibilité de réapprovisionner le stock en un jour, il semblerait raisonnable de ne disposer que d'une pièce de rechange (voire aucune, dans le cas où vous auriez la certitude de pouvoir obtenir une pièce de rechange en 24 heures).

Dans le cas extrême inverse, si un système ne peut pas se permettre d'être indisponible pendant plus de quelques minutes et si une pièce de rechange sera peut-être utilisée une fois par mois (et qu'une nouvelle acquisition pourrait prendre plusieurs semaines), il serait judicieux de conserver sur les étagères une demi-douzaine de pièces de rechange (voire plus).

8.1.1.1.3. Pièces de rechange qui ne sont pas vraiment des pièces de rechange

Dans quel cas une pièce de rechange n'est pas vraiment une pièce de rechange ? Dans le cas de matériel qui est utilisé tous les jours mais sert également de pièce de rechange pour un système ayant une priorité supérieure, le cas échéant. Cette approche présente un certain nombre d'avantages, à savoir :

- Un budget moindre est alloué à des pièces de rechange "non-productives"
- Le matériel est considéré comme opérationnel

Il existe néanmoins certains inconvénient associés à cette approche, à savoir :

- Le déroulement normal de la tâche ayant la priorité la plus basse est interrompu
- Un risque de sinistre existe en cas de panne du matériel ayant la propriété la plus basse (et dans ce cas, le matériel doté de la propriété la plus haute est dépourvu de pièce de rechange)

Dans de telles conditions, il se peut que l'utilisation d'un autre système de production comme rechange soit possible, mais le succès de cette approche dépend d'une part de la charge de travail spécifique du système et d'autre part, de l'impact que l'absence du système a sur les opérations générales du centre de données.

8.1.1.2. Contrats d'assistance

Grâce aux contrats d'assistance, le problème des pannes matérielles est du ressort d'une autre personne. La seule chose à faire dans ce cas est de confirmer qu'une panne s'est bien produite et qu'elle ne semble pas être d'origine logicielle. Il vous suffit alors de passer un coup de fil et quelqu'un se rendra sur place pour résoudre le problème.

Cette situation semble tellement simple. Mais comme c'est le cas avec la plupart des choses dans la vie, ce n'est qu'un aspect de la situation. Ci-après figurent certaines des choses que vous devez prendre en considération lors de l'examen d'un contrat d'assistance :

- Heures de couverture
- Temps de réponse

- Disponibilité des pièces
- Budget disponible
- Matériel à couvrir

Chacun de ces points sera examiné de manière plus détaillée dans les sections suivantes.

8.1.1.2.1. Heures de couverture

Il existe différents contrats d'assistance répondant à différents besoins ; en la matière, les heures de couverture constituent un point essentiel sur lequel les différents contrats varient. À moins que vous ne soyez prêt à payer un supplément pour le privilège, vous ne pouvez pas prendre le téléphone à tout moment et espérer voir le technicien arriver dans votre entreprise aussitôt après.

En fait, selon votre contrat, vous ne pourrez peut-être même pas téléphoner à la société d'assistance avant un jour ou une heure spécifiques, ou si vous pouvez appeler la société, vous ne recevrez pas la visite du technicien avant le jour ou l'heure figurant dans votre contrat.

Dans la plupart des contrats, les heures de couverture sont définies en termes d'heures et de jours pendant lesquels un technicien peut être envoyé sur place. Les heures de couverture les plus courantes sont les suivantes :

- Du lundi au vendredi, de 09:00 à 17:00
- Du lundi au vendredi, tous les jours pendant 12/18/24 heures (avec une heure de commencement et de fin de couverture établie d'un commun accord)
- Du lundi au samedi (ou du lundi au dimanche), mêmes heures que ci-dessus

Comme vous vous en doutez, le coût d'un contrat augmente en fonction des heures de couverture. D'une manière générale, l'allongement des heures de couverture du lundi au vendredi coûte moins cher que l'inclusion du samedi et dimanche.

À ce niveau cependant, il est possible de réduire les coûts si vous êtes prêt à effectuer certaines tâches.

8.1.1.2.1.1. Assistance en atelier

Si dans votre situation vous ne nécessitez que la disponibilité d'un technicien pendant les heures de bureau normales et que vous avez suffisamment d'expérience pour pouvoir déterminer ce qui ne fonctionne pas, vous voudrez peut-être considérer l'*assistance en atelier*. Ce type d'assistance est connu sous de nombreux noms y compris *assistance walk-in* (assistance fournie lorsque la personne se déplace) et *assistance drop-off* (assistance fournie lorsque l'élément posant problème est amené à l'atelier) et le fabricant dispose peut-être d'ateliers d'assistance où les techniciens travaillent sur du matériel apporté par les clients.

L'assistance en atelier a l'avantage d'être aussi rapide que le temps qu'il vous faut pour vous rendre à l'atelier. Vous n'avez pas à attendre qu'un technicien soit disponible et se présente dans votre entreprise. Étant donné que les techniciens de l'atelier n'interviennent pas en dehors de l'atelier en réponse à l'appel d'un client, l'un d'eux sera toujours disponible pour travailler sur votre matériel et ce, dès que vous pourrez le déposer à l'atelier.

Étant donné que l'assistance en atelier est fournie en un seul endroit, il y a de grandes chances pour que toute pièce dont vous auriez besoin y soit disponible. Ainsi, il ne sera pas nécessaire d'envoyer cette pièce du jour au lendemain dans un autre atelier ou d'attendre que la pièce en question soit acheminée depuis un autre atelier qui l'a justement en stock et qui se trouve à plusieurs centaines de kilomètres de votre entreprise.

Ceci étant, il existe un certain nombre de contraintes. La plus évidente est que vous ne pouvez pas choisir les heures d'assistance — vous pouvez obtenir une assistance lorsque l'atelier est ouvert. De plus, les techniciens ne travaillant pas au-delà de leurs heures normales, si votre système tombe en

panne à 16.30 heures un vendredi et que vous arrivez à l'apporter à l'atelier juste avant 17.00 heures, les techniciens ne s'en occuperont pas avant de reprendre le travail le lundi suivant.

Une autre contrainte est que l'assistance en atelier dépend de l'existence d'un atelier à proximité. Si votre entreprise se trouve dans une zone métropolitaine, ce ne sera probablement pas un problème, En revanche, pour des entreprises se trouvant dans des zones plus rurales, l'atelier se trouvera peut-être à des centaines de kilomètres.



Astuce

Si vous envisagez d'utiliser une assistance en atelier, considérez bien la chose et prenez en considération les éléments logistiques associés à l'acheminement du matériel vers l'atelier. Utiliserez-vous une voiture de la société ou votre voiture personnelle ? Dans le cas où vous utiliseriez votre voiture, cette dernière est-elle suffisamment grande et peut-elle supporter le poids du système ? Quelles sont les implications au niveau de l'assurance ? Faudra-t-il plusieurs personnes pour charger et décharger le matériel ?

Bien que ces préoccupations soient quelque peu banales, elles devraient être considérées avant de prendre la décision de recourir à une assistance en atelier.

8.1.1.2.2. Temps de réponse

Outre les heures de couverture, de nombreux accords d'assistance stipulent un certain niveau de réponse. En d'autres termes, combien de temps s'écoulera-t-il entre le moment où vous téléphonez et l'arrivée du technicien ? Comme vous pouvez facilement vous en douter, plus le temps de réponse est court, plus l'accord d'assistance est cher.

Il y a des limites aux temps de réponse disponibles. Par exemple, le temps de transport pour aller des bureaux du fabricant à votre entreprise influence énormément l'éventail de temps de réponse possibles¹. Des temps de réponse se situant dans une fourchette de zéro à quatre heures sont généralement perçus comme faisant partie des offres les plus rapides. Des temps de réponse plus longs peuvent s'échelonner entre huit heures (qui en fait devient une assistance "le jour suivant" dans le cas d'un accord basé sur des heures de bureau normales) et 24 heures. Comme pour tous les autres aspects d'un accord d'assistance, même ces temps de réponse sont négociables — moyennant paiement cela va de soi.



Remarque

Bien qu'il ne s'agisse pas d'une situation fréquente, il est important de savoir que des accords d'assistance incluant des closes relatives au temps de réponse peuvent parfois engager la société d'assistance au-delà de sa capacité à répondre. Il n'est pas rare qu'une société d'assistance très demandée envoie quelqu'un — *n'importe qui* — lors d'un appel soumis à un temps de réponse court, rien que pour honorer son engagement quant au temps de réponse. Cette personne diagnostique apparemment le problème en téléphonant soi-disant "au bureau" afin que quelqu'un apporte la "pièce nécessaire."

En fait, la personne attend simplement qu'une personne vraiment capable de résoudre le problème arrive sur place.

1. Et cette durée serait très probablement considérée comme le temps de réponse donné dans le meilleur des cas, puisque les techniciens sont généralement responsables de régions qui s'étendent bien au-delà de leurs bureaux et ce, tous azimuts. Si vous vous trouvez à une des extrémités de leur territoire et que le seul technicien disponible se trouve lui à l'extrémité opposée, le temps de réponse sera évidemment beaucoup plus long

Alors qu'il est tout à fait compréhensible que cette situation se produise dans des circonstances extraordinaires (telles que lors de problèmes d'alimentation qui ont endommagés les systèmes dans tout le service d'assistance de la société), si cette situation correspond au service que vous recevez systématiquement, vous devriez contacter le directeur de l'assistance et exiger des explications.

Si vos temps de réponse sont peu flexibles (et que vous disposez en conséquence d'un gros budget), une certaine approche peut vous permettre de réduire considérablement votre temps de réponse— en fait, à zéro.

8.1.1.2.2.1. Temps de réponse nul — Disponibilité de techniciens sur place

En supposant que vous vous trouviez dans la situation appropriée (vous êtes un des plus grands clients de la région), que vos besoins soient très exigeants (un temps d'indisponibilité de *tout* ordre étant inacceptable) et que vos ressources financières soient adéquates (s'il est nécessaire de demander le prix, vous ne pouvez probablement pas vous le permettre), il se peut que la disponibilité d'un technicien sur place à plein temps soit une option. Les avantages de la présence d'un technicien toujours sur place sont évidents :

- Réponse immédiate à tout problème
- Approche plus proactive en matière de maintenance de système

Comme vous pouvez vous en douter, cette option peut être *très* coûteuse, particulièrement si vous avez besoin d'un technicien sur place 24 heures sur 24, 7 jours sur 7. Mais si cette approche est adéquate pour votre entreprise, vous devriez garder à l'esprit un certain nombre de points importants afin de maximiser les avantages.

Tout d'abord, des techniciens faisant partie de l'entreprise ont besoin d'une grande partie des ressources qu'un employé normal utilise, tel que de l'espace de travail, un téléphone, des cartes d'accès appropriées et/ou des clés etc.

Des techniciens travaillant dans l'entreprise ne sont pas très utiles s'ils ne disposent pas des pièces requises. Il est donc important de bien réserver un lieu de stockage sûr où entreposer les pièces de rechange des techniciens. De plus, assurez-vous que votre technicien dispose bien d'un stock de pièces appropriées à votre configuration et que ces pièces ne sont pas systématiquement "pillées" par d'autres techniciens subvenant aux besoins de leurs propres clients.

8.1.1.2.3. Disponibilité des pièces

Il va de soi que la disponibilité des pièces joue un rôle important dans l'exposition de votre entreprise à des pannes de matériel. Dans le cadre d'un accord d'assistance, la disponibilité des pièces prend une autre dimension dans la mesure où elle ne s'applique pas seulement à votre entreprise mais également à tout autre client faisant partie de la région du fabricant ayant aussi besoin de ces mêmes pièces. Il se peut qu'une autre entreprise ayant acheté plus de matériel que la votre se voie accorder un traitement préférentiel quant il s'agit d'obtenir des pièces (et même des techniciens).

Malheureusement, dans de telles circonstances, il n'y a pas grand chose à faire, mis à part résoudre le problème avec le directeur de l'assistance.

8.1.1.2.4. Budget disponible

Comme nous l'avons souligné précédemment, les contrats d'assistance varient au niveau des prix en fonction de la nature du service fourni. Rappelez-vous que les coûts associés à un contrat d'assistance représentent des dépenses récurrentes ; ainsi, chaque fois que le contrat arrive à échéance, vous devez en renégocier un autre et payer à nouveau.

8.1.1.2.5. Matériel à couvrir

C'est à ce niveau que vous pourrez peut-être réussir à réduire les dépenses au minimum. Imaginez un instant que vous ayez négocié un accord d'assistance offrant la présence d'un technicien sur place 24 heures sur 24, 7 jours sur 7 et le stockage de pièces de rechange sur place — bref, une assistance haut de gamme. Toute pièce de matériel achetée auprès de ce revendeur est couverte, y compris le PC que la secrétaire de l'entreprise utilise pour effectuer des tâches dont l'importance n'est pas critique.

Pour ce PC, est-il *vraiment* nécessaire d'avoir un technicien sur place 24 heures sur 24, 7 jours sur 7 ? Même dans le cas où ce PC serait d'une importance absolument vital pour le travail de la réceptionniste, elle ne travaille que de 09:00 heures à 17:00 heures ; il est donc très peu probable que :

- Le PC sera utilisé entre 17:00 heures et 09:00 heures le lendemain matin (sans parler des week-ends)
- Une panne de ce PC fera une différence quelconque, sauf entre 09:00 heures et 17:00 heures

Dans de telles circonstances, dépenser de l'argent en pensant à l'éventualité que ce PC puisse nécessiter une assistance au milieu de la nuit un samedi soir est en fait un véritable gaspillage d'argent.

La meilleure solution dans ce cas consiste à séparer l'accord d'assistance de manière à ce que le matériel qui n'a pas une importance critique soit regroupé séparément du matériel à fonction vitale. De cette manière, les coûts peuvent être réduits au minimum.



Remarque

Si vous avez vingt serveurs configurés de manière identique remplissant une fonction critique pour votre entreprise, vous serez peut-être tenté d'établir un accord offrant une assistance élevée seulement pour un ou deux serveurs, alors que les autres seront couverts par un accord beaucoup moins cher. L'idée étant ensuite de dire que le serveur défaillant pendant un week-end, quel qu'il soit, est en fait le serveur couvert par le contrat d'assistance élevée.

N'adoptez surtout pas cette approche. Elle est d'une part malhonnête et d'autre part, la plupart des fabricants utilisent les numéros de série pour identifier les éléments couverts par le contrat. Même si vous arrivez à contourner ces éléments de vérification, une fois votre malhonnêteté découverte, cette approche finira par coûter beaucoup plus cher que si vous aviez été honnête dès le départ et aviez payé le montant requis pour le type d'assistance dont vous avez besoin.

8.1.2. Pannes logicielles

Les pannes logicielles peuvent entraîner des temps d'indisponibilité plus longs. Par exemple, les propriétaires de systèmes informatiques d'une certaine marque, pourtant bien connue pour ses caractéristiques en matière de haute disponibilité, ont fait l'expérience d'une telle situation. En effet, un bogue dans le code de traitement du temps du système d'exploitation de l'ordinateur a entraîné un plantage des systèmes des clients à une certaine heure, un certain jour. Alors que cette situation précise correspond plus à un exemple concret de l'impact considérable d'une panne logicielle, d'autres pannes d'origine logicielle peuvent avoir des conséquences certes moins dramatiques, mais néanmoins dévastatrices.

Les pannes logicielles peuvent se produire à l'un des deux niveaux suivants :

- Système d'exploitation
- Applications

Chacun des deux types de pannes entraîne des conséquences spécifiques qui sont abordées en détails dans les sections suivantes.

8.1.2.1. Pannes du système d'exploitation

Dans ce type de panne, le système d'exploitation est à l'origine de l'interruption du service. Des pannes de système d'exploitation ont deux origines :

- Plantage du système (ou crash)
- Suspension du système (ou hang)

Le point essentiel à garder à l'esprit est que les pannes du système d'exploitation interrompent toutes les tâches que l'ordinateur effectuait au moment de la panne. Les pannes peuvent donc avoir des conséquences dévastatrices pour la production.

8.1.2.1.1. Plantage du système (ou crash)

Les plantages (ou crashes) se produisent lorsque le système d'exploitation doit faire face à un nombre d'erreurs tellement important qu'il ne peut faire face à la situation. Les causes des plantages peuvent aller d'une incapacité à résoudre les problèmes matériels sous-jacents, à un bogue dans le code au niveau du noyau qui compromet le système d'exploitation. Lors du plantage d'un système d'exploitation, il est nécessaire de le redémarrer afin de pouvoir poursuivre la production.

8.1.2.1.2. Suspension du système (ou hang)

Lorsque le système d'exploitation s'arrête de traiter les événements du système, le système est mis à l'arrêt. Cette situation est connue sous le terme de *hang* ou système suspendu. Ces situations peuvent se produire par des interblocages de type *deadlocks* (deux consommateurs de ressources essayant d'utiliser la ressource de l'autre) et *livelocks* (deux ou plusieurs processus répondant à leurs activités mutuelles, mais n'effectuant en fait aucun travail utile) produisant le même résultat final — un manque total de productivité.

8.1.2.2. Pannes des applications

Contrairement aux pannes du système d'exploitation, les défaillances d'applications peuvent avoir des conséquences plus limitées au niveau des dégâts causés. Selon la nature spécifique de l'application, sa défaillance n'affectera peut-être qu'une personne. En revanche, s'il s'agit d'une application serveur répondant aux besoins d'un vaste groupe d'applications clientes, les conséquences d'une panne seront beaucoup plus étendues.

Les pannes d'applications, comme les défaillances de systèmes d'exploitation, peuvent être causées par des plantages (ou crashes) ou des suspensions d'activité (hangs), la seule différence résidant dans le fait que cette fois-ci, c'est l'application et pas le système qui plante ou suspend son activité.

8.1.2.3. Obtention d'assistance — Assistance logicielle

De la même manière que les revendeurs de matériel offrent une assistance pour leurs produits, de nombreux revendeurs de logiciels mettent à la disposition de leurs clients des paquetages d'assistance. Hormis les différences évidentes (aucun matériel de rechange n'est requis et la plupart du travail nécessaire peut être effectué par téléphone par du personnel d'assistance) les contrats d'assistance logicielle peuvent être assez semblables à ceux d'assistance matérielle.

Tous les niveaux d'assistance fournis par un vendeur de logiciels ne sont pas identiques. Ci-après figurent certaines des stratégies d'assistance les plus couramment utilisées de nos jours :

- Documentation
- Auto-assistance
- Assistance Web ou email
- Assistance téléphonique
- Assistance sur place

Chacun de ces types d'assistance est décrit de manière plus détaillée dans les sections suivantes.

8.1.2.3.1. Documentation

Bien qu'étant un aspect souvent négligé, la documentation des logiciels peut servir d'outil d'assistance de premier niveau. Qu'elle soit disponible en ligne ou sous une forme écrite, cette documentation contient souvent les informations nécessaires à la résolution de nombreux problèmes.

8.1.2.3.2. Auto-assistance

L'auto-assistance suppose que le client utilise les ressources disponibles en ligne, afin de résoudre leurs propres problèmes d'origine logicielle. Très souvent ces ressources existent sous la forme de FAQ (Forum Aux Questions) ou de bases de connaissances utilisant le Web.

Les FAQ n'ont souvent que peu ou pas de fonctionnalités de recherche, demandant ainsi au client de parcourir toutes les questions, une à une, dans l'espoir de trouver celle qui répond au problème à résoudre. Les bases de connaissances ont tendance à être plus sophistiquées et permettent de faire des recherches en fonction d'un terme particulier. Ces dernières pouvant également couvrir des domaines plus vastes, elles constituent d'excellent outils pour résoudre des problèmes.

8.1.2.3.3. Assistance Web et email

Bien souvent, un site Web qui ressemble à un site d'auto-assistance inclut également des formulaires basés sur le Web ou des adresses email auxquelles envoyer des questions à l'intention du personnel d'assistance. Au premier abord, ce type de site constitue un véritable progrès par rapport à un simple site Web d'auto-assistance, mais en réalité, tout dépend des personnes répondant aux emails.

Si le personnel d'assistance est surchargé, il est difficile d'obtenir de leur part les informations nécessaires pour résoudre le problème car leur première préoccupation est de répondre rapidement à chaque email afin de pouvoir passer au suivant. Cette situation existe car presque tout personnel d'assistance est évalué en fonction du nombre de problèmes qu'il résout. L'escalade des problèmes à du personnel plus qualifié est également une opération très difficile car il n'est pas facile de forcer des réponses plus opportunes et utiles par le biais d'un email — particulièrement lorsque la principale préoccupation de la personne lisant votre email et d'y répondre aussi rapidement que possible afin de pouvoir traiter l'email suivant.

Le moyen d'obtenir la meilleure assistance possible consiste à aborder dans votre email, tous les aspects du problème dont un technicien d'assistance aurait besoin, tels que :

- Description claire et précise de la nature du problème
- Références à tous les numéros de versions pertinents
- Description de ce que vous avez déjà fait afin d'essayer de résoudre le problème (application des derniers correctifs, redémarrage avec une configuration minimale, etc.).

En fournissant au technicien d'assistance davantage d'informations, vous avez une meilleure chance d'obtenir l'assistance dont vous avez besoin.

8.1.2.3.4. Assistance téléphonique

Comme son nom l'indique, l'assistance téléphonique est offerte en téléphonant à un technicien d'assistance. Ce type d'assistance est très semblable à l'assistance matérielle dans le sens où différents niveaux d'assistance peuvent être disponibles (avec différentes heures de couverture, différents temps de réponse, etc.).

8.1.2.3.5. Assistance sur place

Aussi connue sous le terme de service conseils sur place, l'assistance logicielle sur place est normalement réservée à la résolution de problèmes spécifiques ou à l'apport de modifications critiques telles que l'installation et la configuration initiales de logiciels, des mises à niveau essentielles etc. Comme on pourrait s'y attendre, ce type d'assistance est l'option la plus coûteuse en matière d'assistance logicielle disponible .

Toutefois, il existe un certain nombre de situations dans lesquelles une assistance sur place est l'option adéquate. À titre d'exemple, imaginez une petite entreprise employant un seul administrateur système. Cette dernière est sur le point de déployer son premier serveur de bases de données, mais cette opération (et l'entreprise) n'est pas d'une envergure suffisante pour justifier l'emploi d'un administrateur de base de données attiré. Dans une telle situation, il est souvent meilleur marché de faire venir un spécialiste travaillant pour le vendeur de bases de données afin qu'il effectue le déploiement initial (et de temps à autre dans le futur, selon les besoins), plutôt que de former l'administrateur système pour une compétence qu'il n'utilisera que rarement.

8.1.3. Pannes environnementales

Bien que le matériel tourne parfaitement, et malgré une configuration logicielle adéquate et un fonctionnement normal, des problèmes peuvent toujours survenir. Les problèmes les plus courants qui se produisent en dehors du système lui-même ont un lien avec l'environnement physique dans lequel le système se trouve.

Les problèmes environnementaux peuvent être regroupés dans les quatre catégories principales suivantes :

- Intégrité du bâtiment
- Électricité
- Climatisation
- Climat et environnement extérieur

8.1.3.1. Intégrité du bâtiment

Pour une structure si simple en apparence, un bâtiment remplit de nombreuses fonctions. Il fournit un abri contre les éléments extérieurs (conditions climatiques). Il fournit le microclimat approprié pour le contenu qu'il renferme. Il héberge des mécanismes fournissant de l'électricité et protégeant contre les incendies, le vol et le vandalisme. Le bâtiment remplissant toutes ces fonctions, il n'est pas étonnant que de nombreux problèmes puissent survenir. Ci-dessous figurent certaines situations possibles qu'il convient de prendre en considération :

- Des fuites peuvent se produire dans le toit, laissant entrer de l'eau dans les centres de données.
- Dans le bâtiment, différents systèmes (tels que les l'alimentation en eau, l'épuration ou la ventilation) peuvent tomber en panne, rendant les lieux inhabitables.

- Les planchers n'ont peut-être pas une capacité porteuse suffisante pour supporter l'équipement que vous voulez mettre dans le centre de données.

Il est important d'être imaginatif lors de l'élaboration des différents scénarios selon lesquels le bâtiment pourrait être la cause de problèmes. La liste précédente n'a pour intention que de lancer la réflexion sur les bases appropriées.

8.1.3.2. Électricité

Étant donné que l'électricité représente l'élément vital de tout système informatique, les problèmes liés à l'électricité ont une importance essentielle dans l'esprit des administrateurs système, où qu'ils soient. Les problèmes liés à l'électricité prennent bien des aspects différents ; ces derniers sont couverts de manière plus détaillée dans les sections suivantes.

8.1.3.2.1. Sécurité de votre alimentation électrique

Il est tout d'abord nécessaire de déterminer le niveau de sécurité de votre alimentation électrique normale. Comme tout autre centre de données, votre électricité est probablement fournie par une société d'alimentation électrique locale au moyen de câbles électriques. Pour cette raison, il existe certaines limitations quant aux mesures que vous pouvez prendre pour assurer que votre source d'alimentation électrique primaire soit aussi sûre que possible.



Astuce

Les entreprises se trouvant à la limite de la région desservie par une société d'alimentation électrique seront peut-être en mesure de négocier des connexions à deux réseaux différents.

- Celui desservant votre région
- Celui de la société d'alimentation électrique voisine

Les coûts associés à l'installation de câbles électriques depuis le réseau voisin étant relativement élevés, cette option n'est vraiment possible que pour les grandes entreprises. Toutefois, ces entreprises estiment qu'à bien des égards, la redondance ainsi obtenue est bien supérieure aux coûts de l'installation.

Les éléments essentiels à vérifier sont les méthodes selon lesquelles l'électricité est acheminée sur la propriété de votre entreprise et ensuite dans le bâtiment. Les câbles électriques sont-ils souterrains ou non ? Les lignes non souterraines sont susceptibles d'être endommagées de différentes manières :

- par des conditions climatiques extrêmes (glace, vent, éclaires)
- par des accidents de la circulation qui peuvent causer des dégâts aux poteaux et/ou transformateurs
- par des animaux errant là où ils ne devraient pas ou raccourcissant les lignes

Ceci étant, les câbles électriques souterrains ont eux aussi des inconvénients qui leur sont propres :

- Endommagement par des ouvriers du bâtiment creusant au mauvais endroit
- Inondations
- Éclaires (bien que de manière plus rare que dans le cas des lignes électriques montées sur des poteaux)

Essayez de repérer les lignes électriques jusque dans votre bâtiment. Est-ce qu'elles vont d'abord dans un transformateur externe ? Existe-t-il une protection contre des accidents causés par une voiture

reculant dans le transformateur ou par un arbre tombant sur ce dernier ? Tous les interrupteurs de contrôle sont-ils protégés contre une utilisation non autorisée ?

Une fois ces lignes à l'intérieur de votre bâtiment, pourraient-elles (ou les panneaux auxquels elles sont branchées) être la cause d'autres problèmes ? Par exemple, un problème de plomberie pourrait-il inonder la chambre d'alimentation électrique ?

Continuez à suivre les lignes d'alimentation électrique jusqu'à l'intérieur du centre de données ; existe-t-il d'autres facteurs susceptibles d'interrompre votre alimentation en électricité ? Par exemple, le centre de données partage-t-il un ou plusieurs circuits avec des charges associées à des centres ne fournissant pas de données ? Si tel est le cas, il est fort possible qu'un jour, la charge externe déclenche le mécanisme de protection contre les surtensions électriques faisant partie du circuit et entraîne par là-même une interruption de l'activité du centre de données.

8.1.3.2.2. Qualité de l'électricité

Il n'est pas suffisant de s'assurer que la source d'alimentation électrique du centre de données est aussi sûre que possible. Il est également nécessaire d'examiner la qualité de l'électricité distribuée au sein du centre de données. À cet égard, un certain nombre de facteurs doivent être pris en considération, y compris :

Tension

La tension du courant arrivant doit être stable, sans aucune baisse (souvent appelées *chutes*) ou augmentation (souvent appelées *pointes de courant*) de tension.

Forme de l'onde

La forme de l'onde doit avoir l'aspect d'une onde sinusoïdale pure, avec une distorsion harmonique totale (ou *THD* de l'anglais Total Harmonic Distortion) minimale.

Fréquence

La fréquence doit être stable (la plupart des pays utilisent une fréquence électrique de 50Hz ou 60Hz).

Interférence

Le courant ne doit contenir aucune interférence radio (aussi appelée *RFI*, de l'anglais Radio Frequency Interference) et aucune interférence électromagnétique (ou *EMI*, de l'anglais Electro-Magnetic Interference).

Courant

L'électricité doit être fournie à une charge électrique suffisante pour faire fonctionner le centre de données.

L'électricité fournie directement par la société d'alimentation électrique ne satisfait généralement pas les normes nécessaires pour un centre de données. Un certain niveau de traitement de l'électricité est par conséquent généralement nécessaire. À cet égard, les différentes approches figurant ci-dessous peuvent être employées :

Protecteurs de surtension

Les protecteurs de surtension — comme le nom l'indique, ils filtrent les pointes de tension dans l'alimentation électrique. La plupart d'entre eux n'ont aucune autre fonction et ne diminuent donc en aucun cas la vulnérabilité du matériel par rapport à tout autre problème d'origine électrique.

Conditionneurs électriques

Les conditionneurs électriques eux ont une fonction plus étendue ; selon le degré de sophistication du dispositif, les conditionneurs électriques répondent à la plupart des types de problèmes soulevés ci-dessus.

Groupes électrogènes

Un groupe électrogène est essentiellement un gros moteur électrique alimenté par une source électrique normale. Le moteur est relié à un gros volant qui est lui relié à un générateur. Le moteur fait tourner le volant et le générateur, qui produit alors une quantité d'électricité suffisante pour faire fonctionner le centre de données. De cette manière, l'électricité du centre de données est, d'un point de vue électrique, séparée de l'électricité venant de l'extérieur, éliminant ainsi tout problème d'origine électrique. Le volant offre également la possibilité de maintenir l'alimentation lors de courtes pannes de courant étant donné qu'il faut quelque seconde avant que le volant ne ralentisse au point de ne plus pouvoir produire d'électricité.

Systèmes UPS

Certains types d'*UPS* (de l'anglais Uninterruptible Power Supplies) incluent la plupart (sinon toutes) des fonctionnalités de protection d'un conditionneur électrique ².

Avec les deux types de technologies mentionnés ci-dessus, nous avons commencé à aborder le sujet traversant l'esprit de la plupart des personnes lorsqu'elles pensent à l'alimentation électrique — alimentation électrique de secours. La section suivante examinera différentes approches utilisées pour fournir une alimentation électrique de secours.

8.1.3.2.3. Alimentation électrique de secours

Dans le cadre de l'alimentation électrique, tout le monde a déjà entendu le terme *coupure de courant* qui fait référence à une situation dans laquelle l'alimentation électrique est complètement interrompue pendant une certaine durée allant peut-être d'une fraction de seconde à plusieurs semaines.

Étant donné que la durée des coupures de courant peut varier énormément, il est nécessaire d'envisager une alimentation électrique de secours en utilisant différentes technologies, afin de répondre à des pannes de courant de différentes durées.



Astuce

Les pannes de courant les plus fréquentes durent en général moins de quelques secondes ; des coupures plus longues sont moins fréquentes. Dans de telles circonstances, il est recommandé de vous concentrer d'abord sur la protection contre des pannes de courant de quelques minutes et d'envisager ensuite, une stratégie pour réduire l'exposition à des pannes plus longues.

8.1.3.2.3.1. Alimentation en électricité pour les quelques secondes qui suivent

Étant donné que la majorité des pannes de courant ne durent que quelques secondes, votre solution pour une alimentation électrique de secours doit avoir les deux caractéristiques principales suivantes :

- Courte durée de transition vers l'alimentation électrique de secours (*durée de transfert*)
- Temps d'exécution (ou *runtime* c-à-d. la durée pendant laquelle l'alimentation électrique de secours devra être disponible) exprimée des secondes aux minutes

2. La technologie UPS est examinée de manière plus détaillée dans la Section 8.1.3.2.3.2.

Il existe deux solutions pour disposer d'une alimentation électrique de secours qui réponde à ces caractéristiques : les groupes électrogènes et les systèmes UPS. Le volant présent dans le groupe électrogène permet au générateur de continuer à produire de l'électricité pendant suffisamment de temps pour que les coupures de courant de quelques secondes ne soient pas remarquées. Étant donné que les groupes électrogènes ont tendance à être volumineux et coûteux, ils ne représentent une solution pratique que pour les centres de données de moyenne et grande taille.

Toutefois, une autre technologie — portant le nom de système UPS — représente une excellente alternative dans les situations où un groupe électrogène est trop onéreux. De plus, un système UPS peut faire face à des pannes de courant d'une plus longue durée.

8.1.3.2.3.2. Alimentation en électricité pour les quelques secondes qui suivent

Il est possible d'acheter des systèmes UPS de tailles variées — suffisamment petits pour alimenter un simple PC de base pendant cinq minutes ou suffisamment grands pour faire fonctionner tout un centre de données pendant une heure, voire plus.

Les systèmes UPS sont composés des éléments suivants :

- Un *commutateur de transfert* pour passer de la source d'alimentation primaire à la source d'alimentation de secours
- Une batterie pour assurer l'alimentation de secours
- Un *invertisseur* pour convertir le courant continu de la batterie en courant alternatif utilisé par l'équipement du centre de données

Sans parler de taille et de la capacité de la batterie du dispositif, il existe deux types de systèmes UPS de base :

- Le dispositif UPS *offline* utilise son invertisseur pour la gestion de l'électricité seulement lorsque la source d'alimentation primaire est défaillante.
- Le dispositif UPS *online* utilise son invertisseur pour la gestion de l'électricité en permanence, alimentant l'invertisseur au moyen de sa batterie seulement lorsque la source d'alimentation primaire est défaillante.

Chaque type de système a ses avantages et ses inconvénients. Le système UPS *offline* est généralement moins onéreux car l'invertisseur ne doit pas être construit pour un fonctionnement à plein temps. Toutefois, un problème au niveau de l'invertisseur d'un système UPS *offline* ne se remarquera pas (du moins, jusqu'à la prochaine panne de courant).

Les systèmes UPS *online* ont tendance à être plus à même de fournir une alimentation électrique pure à votre centre de données ; après tout, un système UPS *online* a pour fonction essentielle de fournir de l'électricité à plein temps.

Mais, indépendamment du type de système UPS choisi, vous devez d'une part estimer correctement la taille de votre système UPS en fonction de la charge anticipée (garantissant ainsi que le système UPS dispose d'une capacité suffisante pour produire de l'électricité à la tension et au courant nécessaires) et d'autre part, déterminer la durée pendant laquelle vous aimeriez pouvoir alimenter votre centre de données au moyen de la batterie.

Afin de déterminer ces informations, il est nécessaire d'identifier auparavant les charges qui devront être fournies par le système UPS. Prenez en considération chaque élément de l'équipement et déterminez la quantité d'électricité qu'il consomme (ces informations sont généralement mentionnées sur l'étiquette se trouvant à proximité du cordon électrique de l'appareil). Prenez note de la tension, du nombre de watts et/ou des ampères. Une fois que vous avez recueilli ces informations pour tous les appareils, vous devez les convertir en VA (Volt-Ampères). Si la consommation est exprimée en watts, vous pouvez utiliser le nombre mentionné comme VA ; si le nombre est donné en ampères, multipliez-le par le nombre de volts afin d'obtenir la valeur en VA. En additionnant les chiffres en VA,

vous obtiendrez une estimation en VA que vous pourrez alors utiliser pour choisir le type de système UPS nécessaire.



Remarque

D'un point de vue purement scientifique, cette méthode de calcul d'une valeur en VA n'est pas tout à fait correcte ; toutefois, afin d'obtenir la valeur scientifique en VA, il serait nécessaire de connaître le facteur de puissance de chaque appareil et cette information est rarement, voire jamais, fournie. Dans tous les cas, les valeurs en VA obtenues avec cette méthode peu scientifique reflètent les valeurs s'appliquant en fait aux pires situations et permettent par conséquent de disposer une marge d'erreur telle, que ces valeurs peuvent être considérées comme très sûres.

La détermination de la durée pendant laquelle l'alimentation électrique de secours devra être disponible (aussi appelée durée d'exécution ou runtime) est plus une considération d'ordre commerciale que d'ordre technique — contre quels types de pannes de courant souhaitez-vous vous protéger et quelle somme d'argent êtes-vous prêt à dépenser pour ce faire ? La plupart des sites choisissent des durées maximales qui sont inférieures à une ou deux heures car l'électricité fournie par une batterie devient très onéreuse au-delà de cette durée.

8.1.3.2.3.3. Alimentation en électricité pour les quelques heures qui suivent (et au-delà)

Lorsque les pannes de courant s'étendent sur plusieurs jours, ces choix deviennent encore plus coûteux. Les technologies permettant de faire face à des pannes de courant à long terme se limitent aux générateurs fonctionnant à l'aide d'un genre de moteur — essentiellement, moteur diesel et turbine à gaz.



Remarque

Gardez bien à l'esprit que des générateurs utilisant un moteur doivent être réapprovisionnés en carburant lorsqu'ils marchent. Il est donc important de connaître le taux de "consommation" de votre générateur lorsqu'il fonctionne à sa charge maximale, afin de pouvoir organiser un ravitaillement en conséquence.

À ce stade, de très nombreuses options s'offrent à vous si votre entreprise dispose de fonds suffisants. C'est à ce niveau que les experts devraient vous aider à déterminer la meilleure solution pour votre entreprise. Rares sont les administrateurs système disposant de l'expertise nécessaire pour planifier l'acquisition et le déploiement de tels systèmes générateurs d'électricité.



Astuce

Il est possible de louer des générateurs portables de toute taille, permettant ainsi de bénéficier des avantages liés à la production d'électricité par un générateur sans devoir pour cela dépenser les fonds nécessaires à l'achat d'un tel dispositif. Gardez toutefois en mémoire que lors de pannes touchant les alentours de votre région, les générateurs de location seront très demandés et par conséquent très coûteux.

8.1.3.2.4. Planification en vue de pannes de courant prolongées

Alors qu'une coupure de courant de cinq minutes ne représente qu'un désagrément mineur pour le personnel devant travaillé dans des bureaux sans lumière, qu'en est-il d'une coupure d'une heure ? De cinq heures ? D'un jour ? D'une semaine ?

Ceci étant, même si le centre de données fonctionne normalement, une coupure de courant prolongée touchera tôt ou tard votre entreprise. Considérez donc les éléments suivants :

- Que se passera-t-il s'il n'y a pas de courant pour maintenir le contrôle de l'environnement du centre de données ?
- Que se passera-t-il s'il n'y a pas de courant pour maintenir le contrôle de l'environnement dans tout le bâtiment ?
- Que se passera-t-il s'il n'y a pas de courant pour faire fonctionner les postes de travail personnels, le système téléphonique, les lumières ?

À ce stade, il est important pour votre organisation de déterminer le niveau au-delà duquel une coupure de courant prolongée devra malheureusement être tolérée. Ou, dans le cas où cette situation ne serait pas une option, votre entreprise devra reconsidérer sa capacité à fonctionner de manière entièrement autonome par rapport à l'alimentation électrique du bâtiment ; ceci implique la nécessité de très gros générateurs pour alimenter tout le bâtiment.

Évidemment, même ce niveau de planification ne peut pas avoir lieu dans le vide. Il est vraisemblable que, quelle que soit la cause de la panne de courant prolongée, son impact se fera sentir sur le monde extérieur à votre entreprise et que ce dernier, à son tour, aura une influence sur la capacité de votre entreprise à poursuivre son activité, même si elle dispose de moyens illimités pour générer de l'électricité.

8.1.3.3. Chauffage, ventilation et climatisation

Les systèmes de chauffage, ventilation et climatisation (ou HVAC de l'anglais Heating, Ventilation, Air Conditioning) utilisés dans les bureaux modernes sont extrêmement sophistiqués. Souvent contrôlés pour des ordinateurs, le système HVAC est vital pour le confort adéquat d'un bon environnement de travail.

Les centres de données disposent généralement d'équipement supplémentaire pour la ventilation, essentiellement afin de contrebalancer l'impact sur la température de la chaleur produite par les nombreux ordinateurs et les équipements connexes. Des pannes au niveau du système HVAC peuvent avoir des conséquences dévastatrices sur le fonctionnement continu d'un centre de données. De plus, en raison de leur complexité et de leur nature électromécanique, les possibilités de pannes sont nombreuses et variées. Ci-dessous figurent un certain nombre d'exemples :

- Les éléments du dispositif de ventilation (principalement de grands ventilateurs propulsés par de gros moteurs électriques) peuvent être défaillants en cas de surtension, de problème de roulements, de panne de courroie/poulie, etc.
- Les éléments du dispositif de refroidissement (souvent appelés *refroidisseurs*) peuvent perdre du réfrigérant suite à des fuites ou leurs compresseurs et/ou moteurs peuvent se gripper

Les réparations et la maintenance du système HVAC font partie d'un domaine spécialisé— un domaine que l'administrateur système moyen devrait laisser aux experts. La seule chose qu'un administrateur système devrait faire est de s'assurer d'une part que l'équipement HVAC utilisé pour les besoins du centre de données est soumis à des vérifications quotidiennes de bon fonctionnement (voire même plus fréquemment) et d'autre part, qu'il est maintenu conformément aux instructions du fabricant.

8.1.3.4. Conditions climatiques et environnement extérieur

Certaines conditions climatiques, comme celles mentionnées ci-dessous, peuvent constituer une source de problèmes pour un administrateur système :

- De fortes tombées de neige ou la glace peuvent empêcher le personnel de se rendre au centre de données et peuvent même boucher les condensateurs de la climatisation, entraînant une hausse des températures dans le centre de données au moment même où personne ne peut se rendre sur place pour prendre les mesures adéquates.
- Des vents forts peuvent interrompre l'alimentation électrique et les communications alors que des vents très élevés peuvent en fait endommager le bâtiment lui-même.

D'autres conditions climatiques peuvent également être source de problèmes, même si elles ne sont pas aussi connues. Par exemple, des températures excessivement élevées peuvent entraîner une surcharge des systèmes de refroidissement avec des baisses de tension ou coupures de courant dues à une demande d'alimentation trop importante pour le réseau local.

Bien que peu de mesures puissent être prises quant aux aléas climatiques, une connaissance de la manière dont ces derniers peuvent affecter le fonctionnement de votre centre de données peut vous aider à maintenir votre activité, même si les conditions climatiques tournent au mauvais temps.

8.1.4. Erreurs d'origine humaine

On entend souvent dire que les ordinateurs *sont* parfaits. Le raisonnement derrière cette déclaration est que si on analyse méticuleusement le problème, on découvre que le catalyseur de chaque problème informatique est en fait une erreur d'origine humaine. Cette section examinera les types d'erreur humaines les plus courants et leurs conséquences.

8.1.4.1. Erreurs de la part de l'utilisateur final

Les utilisateurs d'un ordinateur peuvent commettre des erreurs pouvant avoir de graves conséquences. Toutefois, étant donné que leur environnement d'exécution est généralement dépourvu de tout privilège, les erreurs des utilisateurs ont tendance à avoir une nature locale. Vu que la plupart des utilisateurs interagissent avec un ordinateur exclusivement au moyen d'une ou plusieurs applications, c'est au sein de ces applications que se produisent la plupart des erreurs commises par l'utilisateur.

8.1.4.1.1. Mauvaise utilisation d'applications

La mauvaise utilisation d'applications peut causer les problèmes suivants :

- Écrasement de fichiers par erreur
- Utilisation de mauvaises données comme entrée d'une application
- Fichiers nommés et organisés de manière obscure
- Suppression accidentelle de fichiers

Cette liste pourrait certes être plus longue, mais les exemples fournis suffiront pour illustrer ce point. Étant donné que les utilisateurs n'ont pas les privilèges du super-utilisateur, les erreurs qu'ils sont à même de commettre ne se limitent qu'à leurs propres fichiers. Dans de telles circonstances, la meilleure approche consiste à agir sur les deux fronts suivants :

- D'une part, éduquer les utilisateurs quant à la bonne utilisation de leurs applications et quant aux bonnes techniques de gestion de fichiers

- D'autre part, s'assurer que des copies de sauvegarde des fichiers des utilisateurs sont effectuées régulièrement et que le processus de restauration est aussi sobre et rapide que possible.

Outre ces mesures, il n'y a pas grand chose à faire pour limiter les erreurs des utilisateurs à un niveau minimal.

8.1.4.2. Erreurs commises par le personnel d'opérations

La relation des opérateurs avec les ordinateurs d'une entreprise est plus engagée que celle des utilisateurs. Alors que ces derniers ont tendance à utiliser essentiellement les applications et que leurs erreurs par conséquent se produisent surtout à ce niveau, les opérateurs eux ont tendance à effectuer un éventail de tâches plus vaste. Bien que la nature de ces tâches ait été dictée par d'autres, certaines d'entre elles peuvent inclure l'utilisation d'utilitaires au niveau du système, des situations dans lesquelles la possibilité de causer des dégâts étendus suite à des erreurs, est beaucoup plus élevée. Par conséquent, les différents types d'erreurs qu'un opérateur est à même de commettre sont centrés sur la capacité de ce dernier à suivre les procédures établies à son intention.

8.1.4.2.1. Non-respect des procédures

Les opérateurs devraient disposer d'ensembles de procédures documentées et disponibles pour presque toutes les actions qu'ils effectuent³. Il se peut qu'un opérateur ne suive pas les procédures telles qu'elles sont définies. Cette situation peut être due aux raisons suivantes :

- À un moment donné dans le passé, l'environnement a été changé et les procédures n'ont jamais été mises à jour. Maintenant, l'environnement change à nouveau, invalidant par là-même les procédures mémorisées par l'opérateur. À ce stade, même si les procédures venaient à être mises à jour (un cas peu vraisemblable étant donné qu'elles ne l'ont pas été dans le passé), l'opérateur n'en aurait pas conscience.
- L'environnement a été modifié et il n'existe aucune procédure. Le cas présent n'est autre qu'une variation encore plus incontrôlable de la situation précédente.
- Les procédures existantes sont correctes, mais l'opérateur ne les suivra pas (ou ne peut pas les suivre).

Selon l'organigramme de votre entreprise, vous ne pourrez peut-être rien faire de plus que de partager vos inquiétudes avec le responsable approprié. Dans tous les cas, la meilleure approche consiste à être disponible afin de pouvoir prendre toute mesure appropriée pour résoudre le problème.

8.1.4.2.2. Erreurs commises lors des procédures

Même si l'opérateur suit les procédures et que ces dernières sont correctes, il est toujours possible que des erreurs soient commises. Si tel est le cas, il se peut que l'opérateur soit négligent (auquel cas le supérieur de l'opérateur en question devrait être consulté).

La situation pourrait être due à une simple erreur. Dans de tels cas, les meilleurs opérateurs se rendront compte qu'il y a un problème et demanderont de l'aide. Encouragez toujours les opérateurs avec lesquels vous travaillez à s'adresser immédiatement aux personnes appropriées s'il ont l'impression qu'il y a un problème. Bien que de nombreux opérateurs soient hautement qualifiés et donc capables de résoudre bien des problèmes eux-mêmes, le fait est que ce n'est pas leur travail. En outre, un problème

3. Si les opérateurs de votre entreprise ne disposent pas d'un ensemble de procédures de fonctionnement, collaborez avec eux, avec la direction de votre entreprise et avec vos utilisateurs afin de les créer. Sans procédures, votre centre de données sera incontrôlable et rencontrera vraisemblablement de graves problèmes au cours du déroulement de son activité quotidienne.

qui est aggravé par un opérateur bien intentionné a des conséquences néfastes non seulement sur la carrière de cette personne mais également sur votre capacité à résoudre rapidement une situation qui au départ, n'était qu'un petit problème.

8.1.4.3. Erreurs de la part des administrateurs système

Contrairement aux opérateurs, les administrateurs systèmes effectuent un vaste éventail de tâches en utilisant les ordinateurs de l'entreprise. De même, contrairement aux opérateurs, les tâches que les administrateurs système effectuent ne sont souvent pas basées sur des procédures documentées.

Par conséquent, des administrateurs système effectuent quelquefois des tâches qui ne sont pas nécessaires lorsqu'ils ne sont pas prudents dans leur travail. Dans le cadre des responsabilités quotidiennes qui leur incombent, les administrateurs système ont un accès aux systèmes informatiques qui est plus étendu que ce dont ils ont vraiment besoin (sans parler de leurs privilèges de super-utilisateur) d'où la possibilité de rendre, par erreur, le système indisponible.

Les administrateurs système peuvent commettre des erreurs soit au niveau d'une mauvaise configuration, soit lors de la maintenance.

8.1.4.3.1. Erreurs dues à une mauvaise configuration

Les administrateurs système doivent souvent configurer différents aspects d'un système informatique. Il est possible que cette configuration inclue les aspects suivants :

- Email
- Comptes utilisateur
- Réseau
- Applications

La liste pourrait bien sûr être un peu plus longue. La tâche de configuration proprement dite peut prendre des formes très variées ; certaines tâches demandent qu'un fichier texte soit édité (à l'aide d'une des centaines de syntaxes différentes utilisées pour les fichiers de configuration), alors que d'autres nécessitent l'exécution d'un utilitaire de configuration.

Le fait que ces tâches soient toutes traitées de manière différente ne représente rien d'autre qu'un défi supplémentaire au fait que chaque tâche de configuration elle-même, nécessite des connaissances différentes. Par exemple, les connaissances nécessaires pour configurer l'agent de transport de courrier sont fondamentalement différentes de celles nécessaires à la configuration d'une nouvelle connexion réseau.

Suite à ce bref exposé de la situation générale, il est surprenant de voir qu'en fait si *peu* d'erreurs se produisent. Dans tous les cas, la configuration est, et demeurera, un défi pour les administrateurs système. Existe-t-il un moyen de rendre le processus moins vulnérable aux erreurs ?

8.1.4.3.1.1. Contrôle des changements

Le point commun à toute modification de la configuration est qu'un certain changement a été apporté. Ce dernier peut être d'une grande ou d'une petite envergure. Il s'agit néanmoins d'un changement et à ce titre devrait être traité d'une manière particulière.

De nombreuses entreprises implémentent un certain type de processus de contrôle. L'intention de ce dernier est d'aider les administrateurs système (et toutes les parties affectées par ces changements) à gérer le processus de changement et de réduire l'exposition de l'entreprise aux erreurs qui pourraient se produire.

Lors du processus de contrôle des changements, chaque changement suit normalement un certain nombre d'étapes différentes. Ci-dessous figure un exemple des étapes pouvant faire partie du processus :

Recherches préliminaires

Les recherches préliminaires tentent de clairement définir :

- La nature du changement devant avoir lieu
- Son impact, dans le cas où le changement serait effectué avec succès
- Une position de repli, dans le cas où le changement échouerait
- Une évaluation des différents types de défaillances possibles

Les recherches préliminaires incluront peut-être un test du changement proposé qui sera effectué pendant un moment d'indisponibilité prévu ; ou cette étape pourra même aller jusqu'à l'implémentation du changement dans un premier temps, dans un environnement test, sur du matériel test prévu à cet effet.

Panification

Le changement est examiné avec une attention toute particulière aux mécanismes mêmes de son implémentation. La planification nécessaire du changement inclut un aperçu des différentes étapes et du cadre temporel de ce changement (ainsi que la série des différentes étapes et le cadre temporel à respecter pour sortir du changement engendré, au cas où un problème surgirait) et une estimation adéquate du temps alloué à l'implémentation du changement, en s'assurant bien que l'opération n'entrera pas en conflit avec tout autre activité effectuée au niveau du système.

Le résultat de ce processus se présente souvent sous la forme d'une liste d'étapes que l'administrateur système utilisera lors de l'implémentation du changement. Chacune de ces étapes expose les instructions à suivre afin de sortir du changement amorcé, dans le cas où l'étape échouerait. Une estimation des durées de chaque étape est souvent donnée, permettant ainsi à l'administrateur système de déterminer facilement si l'opération se déroule comme prévue ou non.

Exécution

À ce stade, l'exécution même des étapes nécessaires à l'implémentation du changement devrait être claire et simple. Soit le changement est implémenté, soit il est annulé pour revenir à la situation précédente (dans le cas où un problème surgirait).

Contrôle

Que le changement soit implémenté ou non, l'environnement est contrôlé afin de s'assurer que tout fonctionne bien comme prévu.

Documentation

Si le changement a été implémenté, toute documentation existante est mise à jour afin de refléter la nouvelle configuration.

Il est évident que tous les changements de configuration ne nécessitent pas ce niveau de détail. La création d'un nouveau compte utilisateur ne devrait nécessiter aucune recherche préliminaire et la planification de cette tâche ne consistera probablement qu'à déterminer si l'administrateur système dispose de temps libre pour créer le compte. L'étape d'exécution sera tout aussi rapide, l'activité de contrôle consistera peut-être à s'assurer que le compte est bien utilisable et la tâche de documentation elle, prendra vraisemblablement la forme d'un email envoyé au gestionnaire du nouvel utilisateur.

Mais, au fur et à mesure que la complexité des changements de configuration augmente, un processus de contrôle des changements plus formel s'impose.

8.1.4.3.2. Erreurs commises lors de la maintenance

Ce type d'erreur peut être insidieux car la panification et le suivi effectués lors des opérations de maintenance quotidiennes sont généralement réduits au minimum.

Tous les jours les administrateurs système sont les témoins des conséquences de ce type d'erreur, venant particulièrement de la part de nombreux utilisateurs affirmant catégoriquement qu'ils n'ont rien changé — l'ordinateur est tout simplement tombé en panne. L'utilisateur ayant cette conviction ne se rappelle généralement pas ce qu'il a fait, et quant vous serez dans cette même situation, vous ne vous rappellerez certainement pas non plus ce que vous avez fait.

L'élément essentiel à garder à l'esprit est que vous devez être à même de vous rappeler les changements que vous avez apportés lors de la maintenance, si vous voulez être en mesure de résoudre les problèmes rapidement. Il n'est pas réaliste d'envisager un processus minutieux de contrôle des changements portant sur des centaines de petites modifications apportées pendant la journée. Que faire pour effectuer un suivi des centaines de petites choses qu'un administrateur système fait au cours d'une journée ?

La réponse est simple — il faut prendre des notes. Qu'elles se présentent sous une forme quelconque, dans un carnet, dans un assistant personnel ou comme commentaires dans le fichier concerné, prenez des notes. En documentant ce que vous avez fait, vous avez une meilleure chance d'identifier une défaillance liée à un changement que vous avez apporté récemment.

8.1.4.4. Erreurs de la part des techniciens d'assistance

Dans certains cas, les personnes mêmes qui sont supposées vous aider à garantir le bon fonctionnement de vos systèmes en fait, les endommagent. Une telle situation n'est pas due à une conspiration, seulement, toute personne travaillant sur une technologie quelle qu'elle soit, risque pour une raison ou une autre de mettre cette technologie hors service. Il en va de même lorsque les programmeurs en essayant de corriger un bogue, finissent par en créer un autre.

8.1.4.4.1. Matériel mal réparé

Dans ce cas, le technicien a soit échoué dans son diagnostic du problème et a par conséquent effectué une réparation qui n'était pas nécessaire (ou inutile) ou le diagnostic était bon mais la réparation n'a pas été effectuée comme elle aurait dû l'être. Il se peut aussi que la pièce de rechange elle-même ait été défectueuse ou que la procédure adéquate n'ait pas été suivie lors de la réparation.

C'est la raison pour laquelle il est très important de savoir ce que le technicien fait à tout moment. Ce faisant, vous serez plus attentif aux défaillances qui semblent être liées d'une manière ou d'une autre, au problème d'origine. Cette approche permet de mettre le technicien sur la bonne voie, dans le cas où un problème surviendrait ; autrement, il y a une forte chance que le technicien considère cette erreur comme étant nouvelle et complètement indépendante de celle qui devait être corrigée au départ. De cette manière, les techniciens ne perdent pas de temps à essayer de résoudre un faux problème.

8.1.4.4.2. Correction d'une erreur et création d'une autre

Parfois, bien que le problème ait été diagnostiqué et résolu avec succès, un autre problème surgit à sa place. Le module CPU a été remplacé, mais le sac anti-statique dans lequel il se trouvait a été oublié dans le placard et a bloqué le ventilateur entraînant un arrêt dû à une température trop élevée. Ou le disque dur défaillant de la matrice RAID a bien été remplacé mais une personne a butté contre le connecteur d'un autre disque et l'a accidentellement déconnecté si bien que la matrice est toujours hors service.

De tels incidents peuvent être dûs à des négligences chroniques ou à une simple erreur. Dans tous les cas, vous devriez toujours passer en revue les modifications apportées par le technicien et vous assurer que le système fonctionne bien correctement avant que le technicien ne parte.

8.2. Sauvegardes

Les sauvegardes ont deux buts principaux :

- Permettre la restauration de fichiers individuels
- Permettre la restauration en bloc de systèmes de fichiers entiers

Le premier but représente la base d'une requête de restauration de fichiers typique : un utilisateur supprime un fichier par accident et demande à ce qu'il soit restauré à partir de la dernière sauvegarde. Il se peut que les circonstances exactes changent quelque peu, mais d'une manière générale, ce type de restauration représente l'utilisation quotidienne la plus courante des sauvegardes.

La deuxième situation illustre le pire cauchemar d'un administrateur système : pour une raison ou une autre, l'administrateur système regarde fixement le matériel qui à un moment donné représentait la partie productive du centre de données. Maintenant, il n'est rien d'autre qu'un vieux morceau d'acier et de silicone. Tous les logiciels et toutes les données que vous et vos utilisateurs avez rassemblés au fil des années ont disparu. Tous ces logiciels et toutes ces données sont supposés avoir fait l'objet de sauvegardes. Mais est-ce bien le cas ?

Et si c'est le cas, serez-vous à même de restaurer le contenu de ces sauvegardes ?

8.2.1. À données de types différents, besoins de sauvegarde différents

Si vous examinez les différents types de données⁴ traités et stockés par un système informatique standard, vous remarquerez que certaines données ne changent jamais, alors que d'autres changent constamment.

Le rythme auquel les données changent est crucial dans la conception d'une procédure de sauvegarde, et ce, pour deux raisons :

- Une sauvegarde n'est rien d'autre qu'une image statique des données sauvegardées. Elle représente une copie de ces données à un moment précis.
- Des données ne changeant occasionnellement peuvent être sauvegardées épisodiquement, alors que des données qui changent souvent doivent elles être sauvegardées plus fréquemment.

Les administrateurs système ayant une bonne connaissance de leurs systèmes, de leurs utilisateurs et de leurs applications devraient être en mesure de regrouper rapidement en différentes catégories les données relatives à leurs systèmes. À cet égard, les exemples de catégories suivants peuvent constituer un bon point de départ :

Système d'exploitation

D'une manière générale, ces données ne changent que lors de mises à niveau, lors de l'installation de correctifs de bogues et lorsque des modifications quelconques sont nécessaires pour répondre aux besoins d'un site spécifique.



Astuce

Est-il vraiment nécessaire que vous vous préoccupiez de sauvegarder votre système d'exploitation ? Au fil des années, cette question a fait l'objet de nombreuses réflexions parmi les administrateurs système. Si le processus d'installation est relativement simple, que l'application des correctifs de bogues et l'environnement personnalisé sont non seulement bien

4. Le terme *données* utilisé dans cette section fait référence à tout ce qui est traité par le biais des logiciels de sauvegarde. Parmi ces derniers figurent les logiciels du système d'exploitation, les logiciels d'applications ainsi que les données réelles. Ainsi, quoi que ce soit, tout ce qui a trait aux logiciels de sauvegarde est considéré comme faisant partie des données.

documentés mais peuvent également être facilement reproduits, la réinstallation du système d'exploitation est une option tout à fait possible.

Si, en revanche, il existe un doute quant à la possibilité de pouvoir recréer l'environnement système d'origine au moyen d'une nouvelle installation, la sauvegarde du système d'exploitation est la meilleure option, même si ce type de sauvegarde est effectué moins fréquemment que la sauvegarde des données de production. Des sauvegardes épisodiques du système d'exploitation sont également très utiles lorsque seuls quelques petits fichiers doivent être restaurés (par exemple, en cas de suppression accidentelle d'un fichier).

Logiciels d'applications

Ces données changent lors de toute installation, mise à niveau ou suppression d'applications.

Données d'applications

Ces données changent dès lors que les applications qui les utilisent sont exécutées. Selon l'application elle-même et selon l'entreprise, il se peut que les changements aient lieu toutes les secondes ou au contraire à la fin de chaque exercice fiscal.

Données utilisateur

Ces données changent en fonction des modes d'utilisation de la communauté des utilisateurs. Dans la plupart des entreprises, ce type de données change en permanence.

Sur la base de ces catégories (et de toutes autres catégories supplémentaires s'appliquant à votre entreprise spécifique) vous devriez désormais avoir une idée relativement claire de la nature des sauvegardes nécessaires pour protéger vos données.



Remarque

Vous devriez garder à l'esprit que la plupart des logiciels de sauvegarde traitent les données au niveau des fichiers et des répertoires du système. En d'autres termes, la structure des répertoires de votre système joue un rôle important dans la manière selon laquelle les sauvegardes seront effectuées. Ce point essentiel représente d'ailleurs une autre raison pour laquelle il est toujours recommandé, lors de la configuration d'un nouveau système, de bien réfléchir à la meilleure structure de répertoires possible et de regrouper avec précautions les fichiers et répertoires en fonction de leur utilisation prévue.

8.2.2. Logiciels de sauvegarde : acheter ou construire ?

Afin de pouvoir effectuer des sauvegardes, il est évidemment nécessaire de disposer des bons logiciels. Ces derniers ne doivent pas seulement être capables d'effectuer la tâche élémentaire de copie de bits sur des supports de sauvegarde, ils doivent aussi interfacer parfaitement avec les besoins commerciaux et les besoins du personnel de votre entreprise. Lors de la revue des logiciels de sauvegarde possibles, il est important de prendre en considération les fonctionnalités suivantes :

- Programmation des sauvegardes pour une exécution au moment voulu
- Gestion de l'emplacement, de la rotation et de l'utilisation des supports de sauvegarde
- Collaboration avec les opérateurs (et/ou les changeurs robotisés de supports) pour obtenir l'assurance que le bon support est disponible
- Localisation aisée par les opérateurs du support contenant une sauvegarde spécifique d'un fichier donné

Comme vous pouvez le constater, une solution de sauvegarde vraiment adaptée à la réalité de l'environnement de votre entreprise ne consiste pas seulement en un simple enregistrement de bits sur un support de sauvegarde.

À ce stade, la plupart des administrateurs système considèrent une des deux solutions suivantes :

- Achat d'une solution développée commercialement
- Création d'un système de sauvegarde développé entièrement au sein de l'entreprise (en y intégrant peut-être une ou plusieurs technologies Open Source)

Chaque approche a des avantages et des inconvénients. Étant donnée la complexité de la tâche, une solution développée au sein même de l'entreprise ne pourra vraisemblablement pas bien traiter certains aspects (tels que la gestion des supports ou la possibilité d'obtenir une assistance complète au niveau technique ou au niveau de la documentation). Toutefois, pour certaines entreprises, cet aspect ne sera peut-être pas considéré comme un inconvénient.

Une solution développée commercialement sera vraisemblablement très fonctionnelle mais sera peut-être beaucoup trop complexe pour les besoins actuels de l'entreprise. Ceci étant, cette complexité permettra peut-être à l'entreprise de conserver cette solution au fur et à mesure que son activité se développera.

Comme vous pouvez le constater, il n'y a pas vraiment de méthode infaillible quant il s'agit de choisir un système de sauvegarde. En la matière on ne peut que recommander de prendre en considération les points suivants :

- Il est très difficile de changer de logiciel de sauvegarde ; une fois implémenté, le logiciel de sauvegarde est utilisé pour une longue durée. En effet, vous devrez disposer de sauvegardes d'archives à long terme que vous devrez être en mesure de lire plus tard. Le changement de logiciel de sauvegarde implique que vous conserviez le logiciel original (pour pouvoir avoir accès aux sauvegardes des archives) ou que vous convertissiez les sauvegardes de vos archives afin qu'elles soient compatibles avec le nouveau logiciel.

Selon le logiciel de sauvegarde, la tâche de conversion des sauvegardes d'archives consistera peut-être simplement (mais avec une durée relativement longue de traitement) à ouvrir la sauvegarde au moyen d'un programme de conversion déjà existant ou il sera peut-être nécessaire d'utiliser l'ingénierie inverse sur le format des sauvegardes et donc d'écrire un logiciel personnalisé pour effectuer cette tâche.

- Le logiciel doit être fiable à 100% — il doit non seulement effectuer la sauvegarde des informations qu'il est supposé sauvegarder mais il doit aussi le faire au moment voulu.
- Quand c'est le moment de restaurer toute information — qu'il s'agisse d'un seul fichier ou d'un système de fichiers entier — le logiciel de sauvegarde doit être fiable à 100%.

8.2.3. Types de sauvegardes

Dans l'esprit des personnes qui ne s'y connaissent pas beaucoup en matière de sauvegardes informatiques, une sauvegarde n'est rien d'autre qu'une copie identique de *toutes* les données stockées sur l'ordinateur. En d'autres termes, si une sauvegarde était créée mardi soir et qu'aucun changement ne se produisait toute la journée de mercredi, la sauvegarde créée mercredi soir serait identique à celle créée mardi.

Bien qu'il soit tout à fait possible de configurer les sauvegardes de la sorte, il est probable que vous ne le ferez pas. Afin de mieux comprendre cette situation, il est nécessaire tout d'abord de disposer de bonnes connaissances sur les différents types de sauvegardes pouvant être créés. Parmi ces derniers figurent :

- Les sauvegardes complètes

- Les sauvegardes incrémentielles
- Les sauvegardes différentielles

8.2.3.1. Les sauvegardes complètes

Le type de sauvegarde abordé au début de cette section est connu sous le terme de *sauvegarde complète*. Une sauvegarde complète est une sauvegarde au cours de laquelle tous les fichiers individuels sont enregistrés sur un support de sauvegarde. Comme mentionné ci-dessus, si les données devant être sauvegardées ne changent jamais, chaque sauvegarde complète étant créée sera identique à la précédente.

Cette similarité est due au fait qu'une sauvegarde complète ne vérifie pas si le fichier a changé depuis la création de la dernière sauvegarde ; l'opération consiste à enregistrer aveuglément toutes les informations sur un support de sauvegarde, qu'elles aient changé ou non.

Telle est la raison pour laquelle des sauvegardes complètes ne sont pas effectuées tout le temps — en effet, chaque fichier est enregistré sur le support de sauvegarde. Dans ces situations, de nombreux supports de sauvegarde sont utilisés même si aucune donnée n'a changé. Une approche consistant à sauvegarder 100 giga-octets de données tous les soirs quand seulement 10 méga-octets ont changé n'est pas vraiment idéale, d'où la création des *sauvegardes incrémentielles*.

8.2.3.2. Sauvegardes incrémentielles

Contrairement aux sauvegardes complètes, les sauvegardes incrémentielles vérifient si le moment où le fichier a été modifié est postérieur au moment où ce dernier a été sauvegardé pour la dernière fois. Si ce n'est pas le cas, le fichier n'a pas été modifié depuis la dernière sauvegarde et ne sera donc pas pris en compte lors de la sauvegarde actuelle. En revanche, si la date de modification *est* postérieure à la date à laquelle la sauvegarde a été effectuée, le fichier a été modifié et devra donc être sauvegardé.

Les sauvegardes incrémentielles sont utilisées de concert avec une sauvegarde complète se déroulant régulièrement (par exemple, une sauvegarde hebdomadaire, avec des incréments quotidiens).

L'avantage essentiel de l'utilisation de sauvegardes incrémentielles est que l'opération est plus rapide que la création de sauvegardes complètes. Toutefois, l'inconvénient majeur des sauvegardes incrémentielles est que la restauration de tout fichier donné nécessitera peut-être des recherches dans une ou plusieurs sauvegarde(s) incrémentielle(s) jusqu'à ce que le fichier en question puisse être localisé. Lors de la restauration d'un système de fichiers complet, il est nécessaire de restaurer la dernière sauvegarde complète et toute sauvegarde incrémentielle postérieure.

Afin de contourner le besoin de parcourir chaque sauvegarde incrémentielle, une approche légèrement différente a été implémentée. On fait référence à cette dernière sous le terme de *sauvegarde différentielle*.

8.2.3.3. Sauvegardes différentielles

Les sauvegardes différentielles sont semblables aux sauvegardes incrémentielles dans le sens où dans les deux cas, seuls les fichiers ayant été modifiés sont sauvegardés. Toutefois, les sauvegardes différentielles sont *cumulatives* — en d'autres termes, avec une sauvegarde différentielle, dès l'instant où un fichier a été modifié, il sera toujours inclus dans toutes les versions suivantes des sauvegardes différentielles (jusqu'à la prochaine sauvegarde complète bien sûr).

Ainsi, chaque sauvegarde différentielle contient tous les fichiers modifiés depuis la dernière sauvegarde complète, permettant par là-même une restauration complète en n'utilisant que la dernière sauvegarde complète et la dernière sauvegarde différentielle.

Tous comme la stratégie de sauvegarde utilisée pour les sauvegardes incrémentielles, les sauvegardes différentielles suivent généralement la même approche, à savoir, une seule sauvegarde complète est effectuée périodiquement de concert avec des sauvegardes différentielles fréquentes.

Une des conséquences découlant de l'utilisation de sauvegardes différentielles est qu'au fil des années, les sauvegardes différentielles ont tendance à augmenter au niveau de la taille (à condition que des fichiers différents soient modifiés entre les sauvegardes complètes). Ainsi, les sauvegardes différentielles se placent entre les sauvegardes incrémentielles et les sauvegardes complètes en termes d'utilisation de support de sauvegarde et de vitesse de sauvegarde, mais elles permettent en plus des restaurations de fichiers individuels et des restaurations complètes souvent plus rapides (car moins de sauvegardes doivent être examinées/restaurées).

Au vue de ces caractéristiques, les sauvegardes différentielles valent bien la peine d'être prises en considération.

8.2.4. Support de sauvegarde

Tout au long des sections précédentes, nous avons utilisé le terme "support de sauvegarde" avec précaution, et ce, pour une raison bien précise. Lorsque la plupart des administrateurs système expérimentés pensent aux sauvegardes, ils pensent généralement à ces dernières en termes de lecture et écriture de bandes ; de nos jours toutefois, il existe d'autres options.

Dans le passé, les dispositifs à bandes représentaient les seuls supports amovibles pouvant vraiment être utilisés à des fins de sauvegarde. Les choses ont toutefois évoluées. Dans la section suivante, nous examinerons les supports de sauvegarde les plus populaires et passerons en revue leurs avantages et leurs inconvénients.

8.2.4.1. Bande

Dans le passé, la bande était le support amovible de stockage de données préféré et le plus largement utilisé. Cette dernière a l'avantage d'être un support bon marché, avec une capacité de stockage relativement bonne. Toutefois, l'utilisation de bandes a ses inconvénients — non seulement elles s'utilisent, mais l'accès aux données stockées sur un tel support se fait de manière séquentielle.

Dans de telles circonstances il est essentiel d'effectuer un suivi de l'utilisation des bandes (et de les changer lorsqu'elles approchent la fin de leur cycle d'utilisation et lorsque la recherche d'un fichier particulier sur une bande devient une opération très longue).

Ceci étant, les bandes figurent non seulement parmi les supports de stockage en masse les moins coûteux qui existent, mais elles ont également une bonne réputation en matière de fiabilité. Ainsi, la constitution d'une bibliothèque d'une taille raisonnable ne devra pas forcément utiliser une grande partie de votre budget et vous pourrez également compter sur une utilisation aussi bien présente que future.

8.2.4.2. Disque

Dans le passé, les disques durs n'auraient jamais été utilisés en tant que support de sauvegarde. Toutefois, les prix du stockage ont baissé à tel point que dans certains cas, l'utilisation de disques durs pour le stockage de sauvegardes représente en fait une option tout à fait viable.

La raison essentielle justifiant l'utilisation de disques durs en tant que supports de sauvegarde est la rapidité. En effet, il n'existe aucun support de stockage en masse plus rapide que les disques durs. La rapidité peut être un facteur critique lorsque le temps disponible pour la sauvegarde dans votre centre de données est limité et que la quantité de données à sauvegarder est élevée.

Ceci étant, le stockage sur disque dur ne constitue pas le meilleur support de sauvegarde pour les raisons suivantes :

- Les disques durs ne sont généralement pas amovibles. En matière de stratégie de sauvegarde, il est particulièrement important de pouvoir sortir les sauvegardes de votre centre de données afin de les

déposer dans un site en dehors du centre lui-même. Une sauvegarde de votre base de données de production stockée sur un disque dur placé à côté de la base de données elle-même ne constitue pas vraiment une sauvegarde, mais plutôt une copie. En outre, ces copies ne sont pas très utiles si le centre de données et son contenu (y compris vos copies) sont endommagés, voire détruits par de malencontreuses circonstances.

- Les disques durs sont coûteux (du moins en comparaison avec d'autres supports de sauvegarde). Peut-être que dans certains cas le côté financier n'est pas un problème, mais dans toute autre circonstance, les coûts associés à l'utilisation de disques durs à des fins de sauvegarde signifient que le nombre de copies de sauvegarde doit être limité afin de réduire le coût général des sauvegardes. Un nombre plus restreint de copies se traduit en une redondance plus limitée dans le cas où une sauvegarde ne pourrait être lue pour une raison ou pour une autre.
- Les disques durs sont fragiles. Même si vous dépensez des fonds supplémentaires pour obtenir des disques durs amovibles, leur fragilité peut être un problème. Il suffit que vous laissiez tomber le disque dur pour que votre sauvegarde soit perdue. Il est possible d'acheter des boîtes afin de réduire (sans toutefois éliminer entièrement) ce risque, mais ce faisant, cette option déjà coûteuse devient encore plus onéreuse.
- Les disques durs ne sont pas des supports d'archives. Même en supposant que vous soyez en mesure de surmonter tous les autres problèmes associés à la création de sauvegardes sur disques durs, vous devriez prendre en considération les éléments suivants. La plupart des entreprises sont soumises à certaines contraintes juridiques en matière d'archives de comptabilité devant être disponibles pendant certaines périodes de temps. La possibilité de pouvoir extraire des données utilisables depuis une bande vieille de 20 ans est bien supérieure à celle de pouvoir obtenir des données utilisables à partir d'un disque dur âgé de 20 ans. Disposerez-vous encore du matériel nécessaire pour le connecter à votre système ? Un autre élément à prendre en considération est qu'un disque dur est beaucoup plus complexe qu'une cartouche de bande. Lorsqu'un moteur de 20 ans fait tourner le plateau d'un disque de 20 ans, déplaçant des têtes de lecture/écriture de 20 ans au-dessus de la surface du plateau, quelle est la probabilité que tous ces composants fonctionneront sans problème après avoir été à l'arrêt pendant 20 ans ?



Remarque

Certains centres de données sauvegardent sur disques durs et ensuite, une fois les sauvegardes effectuées, les enregistrent sur bande pour l'archivage. Cette approche permet la sauvegarde la plus rapide possible pendant le temps imparti pour cette opération. L'enregistrement sur bande peut alors avoir lieu plus tard dans la journée ; dès l'instant où "l'enregistrement sur bande" est terminé avant la sauvegarde du jour suivant, le facteur temps n'est pas important.

Ceci étant, il existe certaines situations dans lesquelles la sauvegarde sur disques durs peut être appropriée. Dans la section suivante, nous examinerons comment il est possible de les utiliser de concert avec un réseau, pour former une solution de sauvegarde viable (même si elle demeure onéreuse).

8.2.4.3. Réseau

De lui-même, un réseau ne peut servir de support de sauvegarde. Mais associé à des technologies de stockage en masse, il peut représenter une bonne solution. Par exemple, en associant un lien réseau rapide à un centre de données distant qui contient des quantités importantes de stockage sur disques, les inconvénients de la sauvegarde sur disques mentionnés précédemment ne sont plus vraiment des inconvénients.

En sauvegardant sur un réseau, les disques durs se trouvent déjà en dehors de l'entreprise ; ainsi, le transport des disques durs fragiles n'est pas nécessaire. Avec une largeur de bande suffisante pour le réseau, vous pouvez conserver l'avantage de rapidité que vous obtenez en sauvegardant sur disques durs.

Toutefois, cette approche ne résout pas le problème du stockage d'archives (bien que l'approche consistant à "transférer dans un deuxième temps la sauvegarde sur une bande" — une solution mentionnée précédemment — puisse ici aussi être utilisée). De plus, les coûts associés à l'équipement d'un centre de données distant avec un lien rapide au centre de données principal, rendent cette solution très onéreuse. Mais pour les entreprises ayant effectivement besoin des fonctionnalités offertes par cette solution, les coûts nécessaires seront supportés sans hésitation.

8.2.5. Stockage des sauvegardes

Une fois les sauvegardes terminées, que se passe-t-il ? La réponse la plus évidente est que ces dernières doivent être stockées quelquepart. Toutefois, le contenu qui devrait être stocké — et l'emplacement du stockage — sont des aspects moins évidents.

Afin de répondre à ces questions, il est nécessaire d'examiner les circonstances dans lesquelles ces sauvegardes seront utilisées. Il existe trois situations principales, à savoir :

1. Des demandes de petites restaurations envoyées de temps à autres par les utilisateurs
2. Des restaurations énormes afin de récupérer les informations perdues suite à un sinistre
3. Le stockage d'archives qui ne seront probablement jamais utilisées

Malheureusement, il existe des différences irréconciliables entre la première et la deuxième situation. Lorsqu'un utilisateur supprime accidentellement un fichier, il veut obtenir la copie de sauvegarde immédiatement. Dans ce cas, le support de sauvegarde doit se trouver à proximité étroite du système sur lequel les données doivent être restaurées.

Dans le cas d'un sinistre nécessitant une restauration complète d'un ou plusieurs ordinateurs dans votre centre de données, si le sinistre était d'une nature physique, quelque soit l'élément ayant entraîné la destruction de votre ordinateur, ce même élément aura détruit les sauvegardes stockées à quelques mètres des ordinateurs. Cette situation résulterait en un véritable désastre.

Le stockage des archives est lui, moins controversé ; étant donné que les possibilités d'utiliser ces archives ne sont que très faibles, si le support de sauvegarde se trouvait à des kilomètres du centre de données, la distance ne poserait aucun problème.

Les approches selon lesquelles ces différences sont résolues varient en fonction des besoins de l'entreprise elle-même. Une approche possible consiste à stocker les sauvegardes de plusieurs jours sur place et de les transporter vers un endroit plus sûr en dehors de l'entreprise, lorsque de nouvelles sauvegardes sont créées.

Une autre approche consisterait à maintenir deux ensembles différents de supports :

- Une réserve du centre de données, utilisée exclusivement pour des demandes de restaurations imprévues
- Une réserve hors du site, utilisée pour un stockage en dehors du centre de données et pour des opérations de récupération suite à un sinistre

Bien sûr, le fait d'avoir deux ensembles de supports suppose la création de doubles sauvegardes ou la copie des sauvegardes. Bien que cette approche soit tout à fait possible, des sauvegardes doubles peuvent prendre trop de temps et l'opération de copie des sauvegardes nécessite également la disponibilité de disques de sauvegarde multiples, afin de traiter les copies (et probablement un système dédié pour créer la copie).

Le défi d'un administrateur système consiste à trouver l'équilibre à même de répondre aux besoins de tous les utilisateurs, tout en s'assurant que les sauvegardes sont disponibles pour faire face aux pires situations.

8.2.6. Problèmes de restauration

Alors que les sauvegardes se produisent de manière quotidienne, les restaurations sont généralement des événements moins fréquents. Toutefois, les restaurations sont inévitables ; dans de telles conditions, il vaut mieux être préparé.

Il est donc important d'examiner en détail les différents scénarios de restauration abordés dans cette section et de déterminer les moyens de tester votre capacité à effectivement les réaliser. Et rappelez-vous que le scénario le plus difficile à tester et aussi celui ayant une importance absolument vitale.

8.2.6.1. Restauration "bare metal"

L'expression "restauration bare metal" est celle utilisée par les administrateurs système lorsqu'ils décrivent le processus de restauration d'une sauvegarde de tout un système sur un ordinateur dépourvu de toute donnée — aucun système d'exploitation, aucune application, rien du tout.

D'une manière générale, il existe deux façons de procéder en matière de restauration bare metal :

Réinstallation, suivie d'une restauration

Dans cette situation, le système d'exploitation de base est installé, comme si un nouvel ordinateur venait d'être configuré pour la première fois. Une fois le système d'exploitation mis en place et configuré selon les besoins, les disques durs restants peuvent être partitionnés et formatés avant que les sauvegardes ne soient restaurées à partir des supports de sauvegarde.

Disques de récupération de système

Un disque de récupération de système est un support amorçable d'un type ou d'un autre (souvent un CD-ROM) qui contient un environnement système minimal, capable d'effectuer les tâches d'administration système les plus élémentaires. L'environnement de récupération contient les utilitaires nécessaires pour partitionner et formater les disques durs, les lecteurs de périphériques nécessaires pour accéder au périphérique de sauvegarde et les logiciels nécessaires pour la restauration des données à partir du support de sauvegarde.



Remarque

Certains ordinateurs ont la capacité de créer des bandes de sauvegarde amorçables à partir desquelles ils peuvent démarrer et engendrer les processus de restauration. Toutefois, cette fonctionnalité n'est pas disponible sur tous les ordinateurs. En fait, les ordinateurs basés sur des architectures de PC ne se prêtent pas à ce genre d'approche.

8.2.6.2. Test des sauvegardes

Tout type de sauvegarde devrait être testé de temps à autre, afin de garantir l'extraction effective des données. En effet, pour une raison ou pour une autre, il se peut que dans certains cas les sauvegardes créées ne soient pas lisibles. Regrettablement, la plupart du temps, ce n'est que lorsque ces données ont été perdues et qu'elles doivent être restaurées depuis la sauvegarde, que l'on se rend compte de la situation.

Les causes de tels problèmes vont du changement de l'alignement des têtes de lecture du lecteur de bandes, à la mauvaise configuration des logiciels de sauvegarde en passant par une erreur commise par l'opérateur. Quelle que soit la raison du problème, sans effectuer de tests, vous ne pouvez pas garantir que les sauvegardes créées pourront permettre une restauration ultérieure des données.

8.3. Récupération suite à un sinistre

À titre d'expérience, la prochaine fois que vous vous trouvez dans votre centre de données, regardez autour de vous et imaginez qu'il n'existe plus. Pas seulement parce que tous les ordinateurs ont été détruits. Imaginez que tout le bâtiment hébergeant votre centre de données a été détruit. Ensuite, imaginez que votre tâche consiste à assurer la plupart du travail qui était effectué auparavant dans le centre de données mais en étant installé d'une manière ou d'une autre, dans un autre endroit, et ce, aussi rapidement que possible. Que feriez-vous ?

En imaginant ce scénario, vous avez abordé la première étape du processus de récupération suite à un sinistre. La récupération suite à un sinistre représente la capacité de reprise suite à un événement affectant le centre de données de votre entreprise, et ce, aussi rapidement et complètement que possible. Il se peut que la nature du sinistre prenne des formes différentes, mais le but final demeure toujours le même.

Les étapes faisant partie du processus de récupération après un sinistre sont nombreuses et de grande envergure. Ci-après figure un aperçu de ce processus et les points essentiels à garder à l'esprit.

8.3.1. Élaboration, test et mise en oeuvre d'un plan de récupération après sinistre

Un centre de secours est certes essentiel, mais il est inutile sans un plan de récupération après sinistre. Ce dernier stipule chaque phase du plan de récupération après sinistre qui inclut entre autres :

- Les événements qui constituent un sinistre possible
- Les personnes au sein de l'entreprise qui disposent de l'autorité suffisante pour déclarer un sinistre et sont par conséquent habilitées à mettre le plan en oeuvre
- La série d'événements nécessaires pour préparer le centre de secours une fois qu'un sinistre a été déclaré
- Les rôles et responsabilités de tous les membres du personnel impliqués dans la mise en oeuvre du plan
- Un inventaire du matériel nécessaire et des logiciels requis pour restaurer la production
- Un programme détaillant le personnel qui travaillera sur le centre de secours, y compris un programme de rotation du personnel afin de permettre des opérations continues, sans épuiser complètement les membres de l'équipe de sinistre
- La suite des événements nécessaires pour déplacer les opérations du centre de secours au centre de données restauré/au nouveau centre de données

Les plans de récupération après sinistre remplissent souvent de nombreux classeurs. Ce degré de détail est essentiel car, en cas d'urgence, il se peut que le plan soit le seul élément sauvé de votre ancien centre de données (mis à part les dernières sauvegardes stockées en dehors de l'entreprise, cela va de soi) vous aidant à reconstruite et restaurer votre activité.



Astuce

Bien que des plans de récupération après sinistre soient supposés être facilement disponibles dans votre entreprise, des copies de ces documents devraient également se trouver en dehors de l'entreprise. De cette manière, un sinistre ravageant votre entreprise ne détruirait pas toutes les copies du plan de récupération après sinistre. L'emplacement du centre où les sauvegardes sont stockées est un bon endroit où conserver une copie du plan de récupération après sinistre. Dans la mesure où les politiques de votre entreprise ne sont pas enfreintes, il est également possible de conserver des copies du document chez les membres du personnel clé, afin qu'elles soient prêtes à l'emploi à tout moment.

Un tel document se doit d'être examiné avec sérieux (et même avec l'aide de professionnels pour sa rédaction).

Une fois que ce document très important est rédigé, son contenu doit être testé périodiquement. Le test d'un plan de récupération après sinistre consiste à mettre en oeuvre les différentes étapes du plan : il convient donc de se rendre au centre de secours et de mettre en place le centre de données temporaire, d'exécuter les opérations à distance et de reprendre une activité normale une fois le "sinistre" surmonté. La plupart des tests n'essaient pas d'effectuer à 100% les tâches du plan ; à la place, un système et une application qui représentent bien la situation sont transportés au centre de secours où ils sont mis en production pour une certaine durée, avant d'être restitués au centre de données pour des opérations normales à la fin du processus de test.



Remarque

Bien que cette expression soit galvaudée, un plan de récupération après sinistre doit être un document vivant ; au fur et à mesure que le centre de données évolue, le plan doit être mis à jour afin de refléter ces changements. De bien des manières, un plan de récupération après sinistre qui ne correspond pas à la situation actuelle de l'entreprise peut aggraver la situation encore plus que s'il n'existait pas de plan du tout ; dans de telles conditions, assurez-vous de bien passer votre plan en revue à intervalles réguliers (tous les trimestres par exemple) et de bien l'actualiser.

8.3.2. Centres de secours : froids, doux et chauds

Un des aspects les plus importants de la récupération après sinistre est la disponibilité d'un endroit à partir duquel la reprise de l'activité peut avoir lieu. On fait référence à cet endroit sous le terme *centre de secours*. En cas de sinistre, un centre de secours représente l'endroit même où votre centre de données peut être recréé et à partir duquel vous pourrez fonctionner pour la durée du sinistre.

Il existe trois types différents de centres de secours, à savoir :

- Centres de secours froids (ou Cold)
- Centres de secours doux (ou Warm)
- Centres de secours chauds (ou Hot)

Évidemment, ces termes ne font pas référence à la température du centre de secours. Ils font en fait référence aux efforts nécessaires pour commencer les opérations au centre de secours en cas de sinistre.

Un centre de secours froid (aussi appelé Cold) n'est guère plus qu'un endroit dans un bâtiment, configuré à cet effet. Tout ce qui est nécessaire pour restaurer le service offert à vos utilisateurs doit être fourni et transporté à cet endroit avant que le processus de récupération ne puisse commencer. Comme vous pouvez vous en douter, le délai requis pour que le centre de secours froid devienne opérationnel à part entière peut être relativement long.

Les sites de secours froids sont les sites les moins onéreux.

Un centre de secours doux contient déjà le matériel qui représente une copie assez proche du matériel se trouvant dans votre centre de données. Afin de pouvoir restaurer le service, les dernières sauvegardes stockées dans votre centre de secours situé à l'extérieur à l'entreprise doivent être acheminées vers l'entreprise et une restauration bare metal doit être effectuée avant que l'opération de récupération proprement dite ne puisse commencer.

Les centres de secours chauds représentent une image virtuelle identique de votre centre de données, incluant tous les systèmes configurés ; les seuls éléments manquants sont les dernières sauvegardes de vos données utilisateur stockées dans votre centre de secours situé à l'extérieur de l'entreprise. Comme

vous le comprendrez aisément, un centre de secours chaud peut devenir pleinement opérationnel en moins de quelques heures.

Un centre de secours chaud constitue l'approche la plus coûteuse en matière de récupération après sinistre.

Les centres de secours peuvent avoir trois origines différentes, à savoir :

- Les sociétés spécialisées dans la prestation de services de récupération après sinistre
- D'autres endroits que votre entreprise possède ou utilise
- Un accord mutuel avec une autre entreprise permettant en cas de sinistre, de partager les installations des centres de données respectifs

Chaque approche a bien sûr ses avantages et ses inconvénients. Par exemple, un contrat avec une entreprise de récupération après sinistre vous donne souvent la possibilité de consulter des experts dont la spécialité consiste à aider les entreprises lors de la création, du test et de la mise en oeuvre d'un plan de récupération après sinistre. Comme vous pouvez l'imaginer, ces services sont assez onéreux.

L'utilisation d'espace dans un autre bâtiment que votre entreprise possède ou utilise peut certes apparaître comme une option quasiment gratuite, mais les coûts associés au stockage du centre de secours et à son maintien en vue d'une utilisation imminente font de cette option un choix toujours onéreux.

L'élaboration d'un accord permettant de partager des centres de données avec une autre entreprise peut être une option très bon marché, mais un fonctionnement à long terme dans de telles conditions n'est généralement pas possible dans la mesure où le centre de données hôte doit toujours maintenir son activité normale, résultant dans le meilleur des cas, en une situation quelque peu tendue.

En fin de compte, le choix d'un centre de secours particulier est le résultat d'un compromis entre les coûts occasionnés et les besoins de votre entreprise quant à l'importance de la continuation de sa production.

8.3.3. Disponibilité matérielle et logicielle

Votre plan de récupération après sinistre doit inclure des méthodes permettant d'obtenir le matériel et les logiciels nécessaires pour que l'activité puisse reprendre au centre de secours. Un centre de secours géré par une entreprise spécialisée en la matière disposera peut-être déjà de tout ce dont vous avez besoin (ou vous devrez peut-être vous organiser pour obtenir et faire livrer des éléments matériels spécialisés dont le centre ne dispose pas) ; un centre de secours froid, en revanche, implique l'identification d'une source fiable pour chacun des composants. Souvent, les entreprises essaient d'obtenir un accord avec les fabricants afin de garantir la livraison rapide de matériel et/ou de logiciels en cas de sinistre.

8.3.4. Disponibilité des sauvegardes

Lorsqu'un sinistre est déclaré, il est nécessaire de notifier votre centre de stockage se trouvant à l'extérieur de l'entreprise, pour les deux raisons suivantes :

- Afin que les dernières sauvegardes puissent être acheminées vers le centre de secours
- Afin de pouvoir organiser l'obtention et le dépôt réguliers de sauvegardes au centre de secours (en plus des sauvegardes normales au centre de secours)

**Astuce**

En cas de sinistre, les toutes dernières sauvegardes de votre ancien centre de données sont d'une importance vitale. Songez à faire des copies avant même que tout élément ne soit ajouté et stockez les originaux à l'extérieur de l'entreprise aussi rapidement que possible.

8.3.5. Connectivité réseau au centre de secours

Un centre de données ne sert pas à grand chose s'il est entièrement déconnecté du reste de l'entreprise qu'il alimente en données. Selon le plan de récupération après sinistre et selon la nature même du sinistre, la communauté de vos utilisateurs se trouvera peut-être à des kilomètres du centre de secours. Dans ces cas-là, une bonne connectivité est essentielle pour effectuer la reprise de la productivité.

Un autre type de connectivité à garder à l'esprit est celui de la connectivité téléphonique. Vous devez vous assurer qu'il existe un nombre suffisant de lignes téléphoniques disponibles pour assurer la communication verbale avec vos utilisateurs. Cette communication qui auparavant pouvait s'effectuer tout simplement en parlant à voix haute au-dessus de la cloison d'un box devra peut-être maintenant prendre la forme d'une conversation téléphonique longue distance ; dans de telles circonstances, il est fortement recommandé de prévoir une connectivité téléphonique supérieure à celle jugée nécessaire pour des opérations normales.

8.3.6. Personnel du centre de secours

Le problème de l'affectation de personnel au centre de secours est multidimensionnel. Un aspect du problème est la détermination de l'effectif du personnel nécessaire pour faire fonctionner le centre de secours pendant toute la durée nécessaire. Alors qu'une équipe réduite au strict minimum puisse être à même de faire fonctionner ce centre pendant une courte durée, si le sinistre se prolonge, davantage de personnel devra être déployé afin de maintenir les efforts nécessaires au déroulement de l'activité dans les circonstances exceptionnelles liées au sinistre.

Il est important de s'assurer que les membres du personnel se voient accorder suffisamment de temps libre pour se reposer et peut-être, se rendre à leur domicile. Dans le cas où l'envergure du sinistre serait telle que les maisons et familles des employés ont été touchées, du temps supplémentaire doit leur être accordé afin qu'ils puissent traiter le sinistre à un niveau personnel. Un hébergement temporaire à proximité du centre de secours est nécessaire, ainsi qu'un système de transport pour acheminer les membres du personnel entre le centre de secours et leur hébergement.

Souvent, un plan de récupération après sinistre inclut un représentant du personnel venant de toutes les couches de la communautés des utilisateurs de l'entreprise. Cet aspect dépend de la capacité de votre entreprise à fonctionner avec un centre de données distant. Si des représentants des utilisateurs doivent travailler au centre de secours, un hébergement doit être disponible pour eux aussi.

8.3.7. Retour à la normale

À un moment ou à un autre, cette situation catastrophique se terminera. Tout plan de récupération après sinistre doit aussi inclure cette phase. Le nouveau centre de données doit être équipé avec tous le matériel et les logiciels nécessaires ; bien que cette phase n'ait souvent pas la même importance critique au niveau du temps que la phase de préparation ayant lieu lorsque le sinistre est déclaré, les dépenses engendrées peuvent être considérables. Les coûts liés aux centres de secours étant proportionnels au nombre de jours pendant lesquels ils sont utilisés, il est logique que des préoccupations d'ordre économique exigent un transfert aussi rapide que possible.

Les dernières sauvegardes du centre de secours doivent être créées et transportées au nouveau centre de données. Après leur restauration sur le nouveau matériel, la production peut alors reprendre dans le nouveau centre de données.

À ce stade, le centre de données de secours peut être dé-commissionné et il est important que la dernière partie du plan mentionne ce qui doit advenir du matériel temporaire. Finalement, l'efficacité du plan est passée en revue et toute modification recommandée par le comité de révision est intégrée dans une version mise à jour du plan.

8.4. Informations spécifiques à Red Hat Enterprise Linux

En matière de sinistres et de récupération après sinistre, peu de choses ont une influence directe sur un système d'exploitation particulier. En effet, les ordinateurs d'un centre de données inondé ne pourront pas fonctionner, qu'ils exécutent Red Hat Enterprise Linux ou tout autre système d'exploitation. Toutefois, certains aspects de Red Hat Enterprise Linux ont un lien avec des aspects spécifiques de la récupération après sinistre ; ces dernières sont abordées dans cette section.

8.4.1. Assistance logicielle

En tant que fournisseur de logiciels, Red Hat offre un certain nombre d'options d'assistance pour ses produits, y compris Red Hat Enterprise Linux. En ce moment, en lisant ce manuel, vous utilisez l'outil d'assistance le plus élémentaire : la documentation. De la documentation pour Red Hat Enterprise Linux est disponible sur le CD-ROM de documentation de Red Hat Enterprise Linux (qui peut être installé sur votre système pour un accès rapide), sous forme écrite et sous forme électronique sur le site Web de Red Hat à l'adresse suivante : <http://www.redhat.com/docs/>.

Des options d'assistance autonomes existent également par le biais des nombreuses listes de diffusion hébergées par Red Hat (disponibles à l'adresse suivante : <https://listman.redhat.com/mailman/listinfo/>). Ces listes de diffusion permettent d'être exposé à l'ensemble des connaissances existant dans la communauté des utilisateurs de Red Hat ; de plus, de nombreuses listes sont placées sous le contrôle de membres du personnel de Red Hat qui apportent des contributions en fonction de leur disponibilité. D'autres ressources sont également disponibles sur la page principale d'assistance de Red Hat figurant à l'adresse suivante : <http://www.redhat.com/apps/support/>.

Il existe également des options d'assistance plus complètes au sujet desquelles vous trouverez des informations détaillées sur le site Web de Red Hat.

8.4.2. Technologies de sauvegarde

Red Hat Enterprise Linux est vendu avec de nombreux programmes différents pour la sauvegarde et la restauration de données. Ces programmes utilitaires ne constituent toutefois pas une solution complète de sauvegarde. Ceci étant, ils peuvent tout à fait être utilisés en tant que noyau d'une telle solution.



Remarque

Comme nous le faisons remarqué dans la Section 8.2.6.1, la plupart des ordinateurs basés sur une architecture PC standard ne disposent pas de la fonctionnalité leur permettant de démarrer directement à partir d'une bande de sauvegarde. Par conséquent, Red Hat Enterprise Linux n'est pas en mesure d'effectuer un amorçage par bande lorsqu'il est exécuté sur un tel matériel.

Il est toutefois possible d'utiliser votre CD-ROM Red Hat Enterprise Linux comme un disque de secours ; pour de plus amples informations sur le sujet, reportez-vous au chapitre traitant du mode de secours qui figure dans le *Guide d'administration système de Red Hat Enterprise Linux*.

8.4.2.1. tar

L'utilitaire `tar` est très connu parmi les administrateurs de systèmes UNIX. C'est la méthode d'archivage préférée pour partager entre différents systèmes des bits de code source et des fichiers. L'implémentation de `tar` incluse dans Red Hat Enterprise Linux est GNU `tar`, une des implémentations de `tar` les plus riches en fonctionnalités.

En utilisant `tar`, la sauvegarde du contenu d'un répertoire peut être aussi simple que l'exécution d'une commande semblable à celle figurant ci-dessous :

```
tar cf /mnt/backup/home-backup.tar /home/
```

Cette commande crée un fichier d'archive nommé `home-backup.tar` dans `/mnt/backup/`. L'archive elle-même renferme de contenu du répertoire `/home/`.

La taille du fichier d'archive créé sera presque aussi grande que celle de l'ensemble des données sauvegardées. Selon le type de données sauvegardées, la compression des données peut permettre de réduire considérablement la taille du fichier d'archive. Ce dernier peut être compressé en ajoutant une seule option à la commande précédente, comme le montre la commande ci-dessous :

```
tar czf /mnt/backup/home-backup.tar.gz /home/
```

Le fichier d'archive `home-backup.tar.gz` ainsi créé est désormais compressé avec `gzip`⁵.

La commande `tar` accepte une variété d'options ; afin d'obtenir de plus amples informations sur le sujet, lisez la page de manuel de `tar` (1).

8.4.2.2. cpio

L'utilitaire `cpio` est un autre programme UNIX traditionnel. C'est un excellent programme pour effectuer des tâches générales comme le transfert de données d'un endroit à un autre et en tant que tel, peut servir également de programme de sauvegarde.

Le comportement de `cpio` et légèrement différent de celui de `tar`. Contrairement à `tar`, `cpio` lit le nom des fichiers qu'il doit traiter par le biais d'entrées standard. Pour dresser une liste de fichiers pour `cpio`, une méthode courante est utilisée ; cette dernière consiste à utiliser des programmes comme `find` et à tuber la sortie vers `cpio`, comme le montre la commande ci-dessous :

```
find /home/ | cpio -o > /mnt/backup/home-backup.cpio
```

Suite à cette commande, un fichier d'archive `cpio` est créé (renfermant tout le contenu de `/home/`) et placé dans le répertoire `/mnt/backup` sous le nom `home-backup.cpio`.



Astuce

Étant donné que la commande `find` dispose d'un vaste ensemble d'options pour la sélection de fichiers, des sauvegardes sophistiquées peuvent facilement être créées. Par exemple, la commande suivante effectue uniquement la sauvegarde des fichiers qui n'ont pas été touchés au cours de l'année écoulée :

5. L'extension `.gz` est typiquement utilisée pour indiquer que le fichier a été compressé à l'aide de `gzip`. Parfois `.tar.gz` est abrégé en `.tgz` afin que le nom des fichiers conserve un longueur acceptable.

```
find /home/ -atime +365 | cpio -o > /mnt/backup/home-backup.cpio
```

De nombreuses options peuvent être utilisées avec `cpio` (et `find`) ; afin d'obtenir de plus amples informations sur le sujet, lisez les pages de manuel de `cpio(1)` et de `find(1)`

8.4.2.3. Il est déconseillé d'utiliser les programmes `dump/restore` pour des systèmes de fichiers montés !

Les programmes `dump` et `restore` sont les équivalents Linux des programmes UNIX portant le même nom. En tant que tels, de nombreux administrateurs système ayant une expérience des systèmes UNIX peuvent estimer que `dump` et `restore` sont des options tout à fait acceptables pour un bon programme de sauvegarde sous Red Hat Enterprise Linux. Toutefois, une façon particulière d'utiliser `dump` est susceptible de créer de nombreux problèmes. Comme l'explique Linus Torvald dans l'email original reproduit ci-dessous, `dump` ne fonctionnera pas de façon suffisamment fiable, même avec 2.4.x : le cache tampon et le cache de page (là où se trouvent en fait toutes les données) ne sont pas homogènes. La situation ne sera que pire avec 2.5.x, lorsque les répertoires sont déplacés dans le cache. Dans de telles conditions, toute personne dépendant de `dump` pour effectuer de bonnes opérations de sauvegarde joue à la roulette russe avec ces dernières. Le résultat escompté n'est absolument pas garanti — il se peut que les données se trouvant dans le cache tampon ne soient pas les plus récentes et malgré tout fassent l'objet de la sauvegarde. Toujours selon lui, à l'heure actuelle (2001), les solutions `cpio/tar/xxx` sont pour sûr les meilleures et fonctionneront sur de multiples systèmes de fichiers (une autre limitation de `dump`). Quels que soient les problèmes soulevés par de telles solutions, ils sont préférables à la corruption garantie des données que la commande `dump` causera.

```
From: Linus Torvalds
To: Neil Conway
Subject: Re: [PATCH] SMP race in ext2 - metadata corruption.
Date: Fri, 27 Apr 2001 09:59:46 -0700 (PDT)
Cc: Kernel Mailing List <linux-kernel At vger Dot kernel Dot org>
```

```
[ linux-kernel added back as a cc ]
```

On Fri, 27 Apr 2001, Neil Conway wrote:

```
> > I'm surprised that dump is deprecated (by you at least ;-)). What to
> use instead for backups on machines that can't umount disks regularly?
```

Note that `dump` simply won't work reliably at all even in 2.4.x: the buffer cache and the page cache (where all the actual data is) are not coherent. This is only going to get even worse in 2.5.x, when the directories are moved into the page cache as well.

So anybody who depends on "dump" getting backups right is already playing Russian roulette with their backups. It's not at all guaranteed to get the right results - you may end up having stale data in the buffer cache that ends up being "backed up".

`Dump` was a stupid program in the first place. Leave it behind.

```
> I've always thought "tar" was a bit undesirable (updates atimes or
> ctimes for example).
```

Right now, the `cpio/tar/xxx` solutions are definitely the best ones, and will work on multiple filesystems (another limitation of "dump"). Whatever problems they have, they are still better than the `_guaranteed_(*)` data corruptions of "dump".

However, it may be that in the long run it would be advantageous to have a

```
"filesystem maintenance interface" for doing things like backups and defragmentation..
```

Linus

```
(* ) Dump may work fine for you a thousand times. But it will fail under the right circumstances. And there is nothing you can do about it.
```

En raison de ce problème, l'utilisation de `dump/restore` sur des systèmes de fichiers montés est fortement déconseillée. Toutefois, `dump` a été conçu à l'origine pour sauvegarder des systèmes de fichiers non montés ; par conséquent, dans des situations où il est possible de déconnecter un système de fichiers à l'aide de la commande `umount`, `dump` demeure une technologie de sauvegarde tout à fait viable.

8.4.2.4. Le logiciel Advanced Maryland Automatic Network Disk Archiver (AMANDA)

AMANDA est une application client/serveur de sauvegarde élaborée par l'Université du Maryland. En ayant une architecture client/serveur, un seul serveur de sauvegarde (généralement un système relativement puissant disposant d'une grande quantité d'espace libre sur les disques rapides et configuré avec le périphérique de sauvegarde souhaité) peut sauvegarder de nombreux systèmes clients, qui n'ont eux besoin que du logiciel client AMANDA.

Cette approche en matière de sauvegardes est tout à fait logique dans la mesure où elle regroupe sur un seul système, toutes les ressources nécessaires pour la création de sauvegardes, au lieu de nécessiter du matériel supplémentaire pour chaque système ayant besoin de services de sauvegarde. La conception d'AMANDA sert également à centraliser l'administration des sauvegardes, simplifiant par là-même considérablement la vie de l'administrateur système.

Le serveur AMANDA gère un ensemble de supports de sauvegarde et effectue une rotation de leur utilisation au sein de cet ensemble, afin d'assurer que toutes les sauvegardes sont conservées pour la durée déterminée par l'administrateur. Tout support est pré-formaté avec des données qui permettent à AMANDA de détecter si le bon support est disponible ou non. De plus, AMANDA peut être interfacé avec des dispositifs robotisés pour le changement de supports, permettant par là-même de complètement automatiser les opérations de sauvegarde.

AMANDA peut utiliser soit `tar` soit `dump` pour effectuer les sauvegardes (bien que sous Red Hat Enterprise Linux, l'utilisation de `tar` soit préférable, en raison des problèmes en relation avec `dump` qui ont été mentionnés dans la Section 8.4.2.3). En tant que tel, les sauvegardes effectuées avec AMANDA n'ont pas besoin d'AMANDA pour la restauration des fichiers — un avantage indéniable.

Au niveau de son utilisation, AMANDA est généralement programmé pour être exécuté une fois par jour pendant la période de temps allouée aux opérations de sauvegarde dans le centre de données. Le serveur AMANDA se connecte aux systèmes clients et guide les clients dans la création des sauvegardes selon l'estimation de leur taille. Une fois ces estimations disponibles, le serveur établit un programme déterminant automatiquement l'ordre selon lequel les systèmes seront sauvegardés.

Une fois que les sauvegardes commencent effectivement, les données sont envoyées par le réseau du client au serveur, où elles sont stockées sur un disque intermédiaire. Une fois qu'une sauvegarde est terminée, le serveur commence à effectuer l'enregistrement du disque intermédiaire sur le support de sauvegarde. En même temps, d'autres clients envoient leurs sauvegardes sur le serveur afin qu'elles soient elles aussi stockées sur le disque intermédiaire. Ce processus crée un flux continu de données disponibles pour l'enregistrement sur le support de sauvegarde. Au fur et à mesure que les sauvegardes sont enregistrées sur le support de sauvegarde, elles sont supprimées du disque intermédiaire du serveur.

Une fois que toutes les sauvegardes sont terminées, un rapport détaillant l'état des sauvegardes est envoyé à l'administrateur système sous forme d'email, rendant par là-même la révision simple et rapide.

Dans le cas où il serait nécessaire de restaurer des données, AMANDA contient un programme utilitaire qui permet à l'opérateur d'identifier le système de fichiers, la date et le(s) nom(s) des fichiers. Une fois cette opération terminée, AMANDA identifie le bon support de sauvegarde et ensuite localise et restaure les données désirées. Comme nous l'avons mentionné précédemment, AMANDA est conçu de telle manière qu'il puisse restaurer des données même sans l'assistance d'AMANDA, mais dans ce cas l'identification du support approprié s'effectue selon un processus manuel d'une certaine lenteur.

Cette section n'a couvert qu'une partie infime des concepts les plus élémentaires d'AMANDA. Si vous souhaitez effectuer des recherches plus approfondies sur AMANDA, nous vous suggérons de commencer par la lecture de la page de manuel d'`amanda(8)`.

8.5. Ressources supplémentaires

Cette section inclut différentes ressources pouvant être utilisées pour étendre vos connaissances sur la récupération après sinistre et sur les thèmes spécifiques à Red Hat Enterprise Linux qui ont été développés dans ce chapitre.

8.5.1. Documentation installée

Les ressources suivantes, installées lors d'une installation normale de Red Hat Enterprise Linux, peuvent vous aider à acquérir des connaissances plus approfondies sur les sujets abordés dans ce chapitre.

- Page de manuel de `tar(1)` — Pour apprendre comment archiver les données.
- Page de manuel de `cpio(1)` — Pour apprendre comment vider le contenu de systèmes de fichiers.
- Page de manuel de `restore(8)` — Pour apprendre comment extraire le contenu de systèmes de fichiers enregistrés par `dump`.
- Page de manuel de `cpio(1)` — Pour apprendre comment copier les fichiers depuis et dans des archives.
- Page de manuel de `find(1)` — Pour apprendre comment rechercher des fichiers
- Page de manuel d'`amanda(8)` — Pour obtenir davantage d'informations sur les commandes faisant partie du système de sauvegarde AMANDA.
- Fichiers contenus dans `/usr/share/doc/amanda-server-<version>/` — Pour obtenir de plus amples informations sur AMANDA en passant en revue les différents documents et fichiers types

8.5.2. Sites Web utiles

- <http://www.redhat.com/apps/support/> — La page d'accueil de l'assistance Red Hat offre un accès facile à de nombreuses ressources traitant de la prise en charge de Red Hat Enterprise Linux.
- <http://www.disasterplan.com/> — Une page intéressante avec des liens vers des nombreux sites traitant de la récupération après sinistre. Vous y trouverez un exemple de plan de récupération après sinistre.
- <http://web.mit.edu/security/www/isorecov.htm> — La page d'accueil intitulée "Information Systems Business Continuity Planning" du Massachusetts Institute of Technology contient de nombreux liens informatiques.

- <http://www.linux-backup.net/> — Un aperçu intéressant sur de nombreux problèmes liés aux sauvegardes.
- http://www.linux-mag.com/1999-07/guru_01.html — Un excellent article tiré de Linux Magazine traitant des aspects plus techniques de la création de sauvegardes sous Linux.
- <http://www.amanda.org/> — La page d'accueil d'AMANDA (ou Advanced Maryland Automatic Network Disk Archiver). Contient des pointeurs vers de nombreuses listes de diffusion associées à AMANDA et d'autres ressources en ligne.

8.5.3. Livres sur le sujet

Les livres suivants qui traitent de différents problèmes en relation avec la récupération après sinistre, constituent de bonnes ressources pour les administrateurs de systèmes Red Hat Enterprise Linux :

- *Guide d'administration système de Red Hat Enterprise Linux*; Red Hat, Inc. — Contient un chapitre sur le mode de secours qui pourrait être utile lors de restaurations bare metal.
- *Unix Backup & Recovery* de W. Curtis Preston ; O'Reilly & Associates — Bien que n'étant pas rédigé pour les systèmes Linux, ce livre sur les sauvegardes et récupérations de systèmes UNIX examine en détail de nombreux problèmes liés aux sauvegardes et inclut même un chapitre sur la récupération après sinistre.

Index

Symboles

/etc/cups/, 161
/etc/printcap, 161
échange (ou swapping), 59

A

activation de votre abonnement, v
administration système
 philosophie de , 1
 automatisation, 1
 communication, 3
 documentation, 2
 entreprise, 7
 ingénierie sociale, dangers de, 8
 planification, 8
 ressources, 6
 situations inattendues, 9
 sécurité, 7
 utilisateurs, 6
automatisation, 9
 aperçu de , 1

C

CD-ROM
 systèmes de fichiers
 (Voir système de fichiers ISO 9660)
chgrp command, 150
chmod command, 150
chown command, 150
commande chage , 148
commande chfn, 148
commande chpasswd, 148
commande df , 112
commande free , 21, 61
commande gpasswd, 148
commande groupadd, 148
commande groupdel, 148
commande groupmod, 148
commande grpck, 148
commande iostat, 25, 43
commande Moniteur système de GNOME, 23
commande mpstat, 25
commande passwd, 148
commande raidhotadd, utilisation, 125
commande sa1, 25
commande sa2, 25
commande sadc, 25
commande sar, 25, 27, 44, 46, 62
 rapports, lecture, 27

commande top, 21, 22, 45
commande useradd, 148
commande userdel, 148
commande usermod , 148
commande vmstat, 21, 23, 43, 46, 61
commande watch, 21
communication
 Informations spécifiques à Red Hat Enterprise Linux, 10
 nécessité de , 3
compte
 (Voir compte utilisateur)
compte utilisateur
 accès aux données partagées, 140
 contrôle d'accès, 137
 fichiers contrôlant, 145
 /etc/group, 147
 /etc/gshadow, 148
 /etc/passwd, 145
 /etc/shadow, 146
 gestion de, 129, 129, 138
 Changement d'emploi, 139
 licenciements, 138
 nouveaux employés, 138
GID, 144
GID système, 144
mot de passe, 132
 aspect court de, 133
 expiration, 137
 faibles, 133
 forts, 136
 jeu de caractères grands pour, 136
 mots utilisés dans, 134
 mémorisable, 136
 petit jeu de caractères utilisé dans, 134
 plus longs, 136
 renseignements personnels utilisés dans, 135
 simples transformations de mots, 135
 utilisés plusieurs fois, 135
 écrits, 135
nom d'utilisateur, 129
 changement de, 131
 collisions dans le nommage, 130
 convention de nommage, 129
outils de gestion , 148
 commande chage , 148
 commande chfn, 148
 commande chpasswd, 148
 commande passwd, 148
 commande useradd, 148
 commande userdel, 148
 commande usermod , 148
permissions en relation avec , 143
 exécution, 143
 lecture, 143
 setgid, 143

- setuid, 143
- sticky bit, 143
- écriture, 143
- ressources, gestion de, 140
- répertoires personnels
 - centralisés, 142
- UID, 144
- UID système, 144
- configuration de l'imprimante, 160
 - application en mode texte, 161
 - CUPS, 160
- contrôle
 - performance du système, 16
 - ressources, 15
- contrôle de la performance du système, 16
- contrôle des changements, 183
- contrôle des ressources, 15
 - capacité du système, 16
 - concepts derrière, 15
 - largeur de bande, 18
 - mémoire, 19
- outils
 - free, 21
 - iostat, 25
 - Moniteur système de Gnome, 23
 - mpstat, 25
 - OProfile, 28
 - sa1, 25
 - sa2, 25
 - sadc, 25
 - sar, 25, 27
 - Sysstat, 25
 - top, 22
 - vmstat, 23
- outils utilisés par, 21
- performance du système, 16
- planification de la capacité, 16
- Puissance de CPU, 17
- que contrôler ?, 17
- stockage, 20
- conventions
 - documentation, ii
- CUPS, 160

D

- devlabel, 107
- disque dur SCSI
 - ajout, 100
- disques durs, 55
- disques durs ATA
 - ajout, 99
- documentation
 - Informations spécifiques à Red Hat Enterprise Linux, 10

- documentation, nécessité de , 2
- données
 - accès partagé aux, 140, 141
 - problèmes de propriété globale, 142
- défauts de pages, 58

E

- enregistrement de votre abonnement, v
- entreprise, connaissance de , 7
- espace d'adressage virtuel, 57
- espace disque
 - (Voir stockage)
- examen du fichier /etc/mtab, 111

F

- fichier /etc/fstab
 - mise à jour, 116
 - montage de systèmes de fichiers avec, 113
- fichier /etc/group
 - compte utilisateur, rôle, 147
 - groupe, rôle, 147
- fichier /etc/gshadow
 - compte utilisateur, rôle, 148
 - groupe, rôle, 148
- fichier /etc/passwd
 - compte utilisateur, rôle, 145
 - groupe, rôle, 145
- fichier /etc/shadow
 - compte utilisateur, rôle, 146
 - groupe, rôle, 146
- fichier /proc/mdstat , 124
- fichier /proc/mounts, 111

G

- gestion
 - imprimantes, 153
- gestionnaire de paquets RPM
 - (Voir RPM)
- gestionnaire de volumes logiques (LVM)
 - (Voir LVM)
- GID, 144
- groupe
 - accès aux données partagées via, 141
 - fichiers contrôlant, 145
 - /etc/group, 147
 - /etc/gshadow, 148
 - /etc/passwd, 145
 - /etc/shadow, 146
 - gestion de, 129
 - GID, 144
 - GID système, 144

outils de gestion , 148
 commande gpasswd, 148
 commande groupadd, 148
 commande groupdel, 148
 commande groupmod, 148
 commande grpck, 148
 permissions en relation avec , 143
 exécution, 143
 lecture, 143
 setgid, 143
 setuid, 143
 sticky bit, 143
 écriture, 143
 structure, établissement, 141
 UID, 144
 UID système, 144

I

ID groupe
 (Voir GID)
 ID utilisateur
 (Voir UID)
 imprimantes
 considérations, 153
 couleur, 156
 CMYK (ou CMJN), 156
 jet d'encre, 156
 laser, 158
 duplex, 153
 gestion, 153
 langages
 (Voir langages de description de pages (ou
 PDL, printer description languages))
 locales, 160
 ressources supplémentaires, 162
 réseau, 160
 types, 153
 cire thermique, 158
 encre solide, 158
 impact, 155
 imprimantes matricielles à aiguilles (ou dot-
 matrix), 155
 jet d'encre, 156
 laser, 157
 laser couleur, 158
 ligne, 155
 marguerite, 155
 sublimation de teinture , 158
 imprimantes couleur laser , 158
 imprimantes laser, 157
 consommables, 158
 couleur, 158
 imprimantes ligne
 (Voir imprimantes à impact)
 imprimantes matricielles à aiguilles
 (Voir imprimantes à impact)
 imprimantes à impact, 155
 consommables, 156
 imprimantes matricielles à aiguilles (ou dot-
 matrix), 155
 ligne, 155
 marguerite, 155
 imprimantes à jet d'encre, 156
 consommables, 157
 imprimantes à marguerite
 (Voir imprimantes à impact)
 inattendu, préparation pour, 9
 informations spécifiques à Red Hat Enterprise Linux
 assistance logicielle, 198
 assistance, logicielle, 198
 automatisation, 9
 communication, 10
 contrôle des ressources
 largeur de bande, 42
 mémoire, 61
 puissance CPU, 42
 documentation, 10
 outils de contrôle des ressources, 21
 free, 21, 61
 iostat, 43
 OProfile, 21
 sar, 44, 46, 62
 Sysstat, 21
 top, 21, 45
 vmstat, 21, 43, 46, 61
 PAM, 11
 perl, 9
 RPM, 11
 récupération suite à un sinistre, 198
 scripts shell, 9
 shell bash , 9
 système de détection des intrusions, 11
 sécurité, 11
 technologies de sauvegarde
 AMANDA, 201
 aperçu de, 198
 cpio, 199
 dump, 200
 tar, 199
 ingénierie sociale, dangers de, 8
 ingénierie, sociale, 8
 interface IDE
 aperçu de, 73
 interface SCSI
 aperçu de, 73

J

jeu de pages de travail, 59

L

langages de description de pages (ou PDL, printer description languages) , 159

Interpress, 159

PCL, 159

PostScript, 159

logiciel

assistance en matière de

aperçu, 172

assistance email, 173

assistance sur place, 174

assistance téléphonique, 174

assistance Web, 173

auto-assistance, 173

documentation, 173

lpd, 162

LVM

aperçu de, 91

groupement du stockage, 91

migration de données, 92

migration, données, 92

par opposition à RAID, 92

redimensionnement de volumes logiques, 91

redimensionnement, volume logique, 91

M

matérielles

compétences nécessaires pour réparer, 166

contracts d'assistance, 167

assistance en atelier , 168

assistance fournie lorsque l'élément posant

problème est amené à l'atelier, 168

assistance fournie lorsque la personne se dé-

place, 168

budget pour, 170

disponibilité des pièces, 170

heures de couverture, 168

matériel couvert, 171

technicien sur place, 170

temps de réponse, 169

matériel de rechange

garder, 165

stock, quantités, 166

stock, sélection du, 166

échange de matériel, 167

pannes, 165

modules d'authentification enfichables (ou PAM de l'anglais Pluggable Authentication Modules)

(Voir PAM)

montage des systèmes de fichiers

(Voir stockage, systèmes de fichiers, montage)

mot de passe, 132

aspect court de, 133

expiration, 137

faibles, 133

forts, 136

jeu de caractères grands pour, 136

mots utilisés dans, 134

mémorisable, 136

petit jeu de caractères utilisé dans, 134

plus longs, 136

renseignements personnels utilisés dans, 135

simples transformations de mots, 135

utilisés plusieurs fois, 135

écrits, 135

mémoire

contrôle de, 19

mémoire virtuelle, 56

aperçu de, 56

défauts de pages, 58

espace d'adressage virtuel, 57

jeu de pages de travail, 59

mémoire auxiliaire, 57

performance de , 59

performance, meilleur cas, 60

performance, pire cas, 60

échange (ou swapping), 59

utilisation des ressources, 51

mémoire cache, 52

mémoire physique

(Voir mémoire)

mémoire virtuelle

(Voir mémoire)

N

NFS, 113

nom d'utilisateur, 129

changement, 131

collisions entre , 130

convention de nommage, 129

noms de fichier

périphérique, 105

O

- OProfile, 21, 28
- Outil de configuration de l'imprimante
(Voir configuration de l'imprimante)
- outils
 - comptes utilisateurs, gestion
(Voir compte utilisateur, outils de gestion)
 - contrôle des ressources, 21
 - free, 21
 - iostat, 25
 - Moniteur système de Gnome, 23
 - mpstat, 25
 - OProfile, 28
 - sa1, 25
 - sa2, 25
 - sadc, 25
 - sar, 25, 27
 - Sysstat, 25
 - top, 22
 - vmstat, 23
 - groupes, gestion
(Voir groupe, outils de gestion)

P

- PAM, 11
- partition, 106
 - aperçu de, 79
 - attributs des, 79
 - champ du type, 80
 - géométrie, 79
 - type, 80
 - création de, 101, 114
 - logiques, 80
 - primaires, 80
 - étendues, 80
- perl, automatisation et , 9
- permission d'exécution, 143
- permission d'écriture, 143
- permission de lecture, 143
- permission des sticky bits, 143
- permission setgid, 11, 143
- permission setuid, 11, 143
- permissions, 143
 - outils de gestion
 - chgrp command, 150
 - chmod command, 150
 - chown command, 150
- philosophie de l'administration système, 1
- planification de la capacité, 16
- planification, importance de , 8
- points de montage
(Voir stockage, système de fichiers, points de montage)
- printconf

- (Voir configuration de l'imprimante)
- printtool
(Voir configuration de l'imprimante)
- préparation à un sinistre, 165
 - alimentation électrique, secours, 177
 - groupe électrogène, 177
 - générateur, 179
 - pannes de courant, prolongées, 180
 - UPS, 178
 - types de sinistres, 165
 - alimentation électrique, sécurité de, 175
 - chauffage, 180
 - climatisation, 180
 - erreurs d'origine humaine, 181
 - erreurs de la part de l'opérateur, 182
 - erreurs de la part de l'utilisateur, 181
 - erreurs de la part des administrateurs système, 183
 - erreurs de la part des techniciens d'assistance, 185
 - erreurs de procédure, 182
 - erreurs dues à une mauvaise configuration, 183
 - erreurs liées à la maintenance, 185
 - erreurs lors des procédures, 182
 - facteurs climatiques, 181
 - HVAC, 180
 - Intégrité du bâtiment, 174
 - mauvaise réparation, 185
 - mauvaise utilisation d'applications, 181
 - pannes des applications, 172
 - pannes du système d'exploitation, 172
 - pannes environnementales, 174
 - pannes logicielles, 171
 - pannes matérielles, 165
 - plantages du système d'exploitation (ou crash), 172
 - situations de systèmes d'exploitation suspendus (hangs), 172
 - ventilation, 180
 - électricité, qualité de, 176
 - éléments électriques, 175
- puissance CPU
(Voir ressources, système, puissance de traitement)
- puissance de traitement, ressources en relation avec
(Voir ressources, système, puissance de traitement)
- périphérique
 - accès au périphérique entier, 106
 - Alternatives aux noms de périphériques, 106
 - convention de nommage, 104
 - devlabel, nommage avec , 107
 - nommage avec devlabel, 107
 - noms de fichier, 105
 - noms de périphériques, alternatives, 106
 - partition, 106
 - type, 105
 - unité, 105

étiquettes de système de fichiers, 107
 étiquettes, système de fichiers, 107

Q

quota, disque
 (Voir quotas de disque)
 quotas de disque
 activation, 120
 aperçu de, 118
 limites douces, 120
 limites dures, 120
 périodes de grâce, 120
 spécifique au groupe, 119
 spécifique au système de fichiers, 119
 spécifique à l'utilisateur même, 119
 suivi de l'utilisation de blocs, 119
 suivi de l'utilisation des inodes, 120
 gestion de, 122
 présentation de, 118

R

RAID

aperçu de, 86
 création de matrices
 (Voir RAID, matrices, création)
 implémentations de, 90
 RAID logiciel, 90
 RAID matériel, 90
 matrices
 commande raidhotadd, utilisation, 125
 gestion de, 124
 reconstruction, 125
 état, vérification, 124
 matrices, création, 122
 après l'installation, 123
 au moment de l'installation, 122
 niveaux de, 86
 RAID 0, 86
 RAID 0, avantages de, 87
 RAID 0, inconvénients de, 87
 RAID 1, 87
 RAID 1, avantages de, 87
 RAID 1, inconvénients de, 87
 RAID 5, 88
 RAID 5, avantages de, 88
 RAID 5, inconvénients de, 89
 RAID combiné, 89
 par opposition au LVM, 92
 présentation de, 85
 RAID combiné, 89
 RAM, 54
 ressources en relation avec la largeur de bande
 (Voir ressources, système, largeur de bande)

ressources système
 (Voir ressources, système)
 ressources, importance des, 6
 ressources, système
 largeur de bande, 35
 aperçu de, 35
 bus, exemples de, 36
 capacité, augmentation, 37
 charge, réduction, 37
 charge, répartition, 37
 chemin aux données, rôle dans, 36
 chemins des données, exemples de, 36
 contrôle de, 18
 problèmes en relation avec, 36
 rôle des bus dans, 35
 solutions aux problèmes avec, 37
 mémoire
 (Voir mémoire)
 puissance de traitement, 35
 aperçu de, 38
 applications, élimination, 41
 capacité, augmentation, 41
 charge, réduction, 40
 consommateurs de, 39
 contrôle de, 17
 CPU, mise à niveau, 41
 faits en relation avec, 38
 insuffisance de, réponse à, 40
 mise à niveau, 41
 SMP, 41
 temps de gestion des activités d'E/S, réduction, 40
 temps de gestion des applications, réduction, 40
 traitement multitâche symétrique, 41
 utilisation du système d'exploitation en matière de, 39
 utilisation par les applications, 39
 stockage
 (Voir stockage)
 RPM, 11
 récupération suite à un sinistre
 aperçu, 194
 centre de secours, 195
 connectivité réseau avec, 197
 personnel du, 197
 disponibilité logicielle, 196
 disponibilité matérielle, 196
 fin de, 197
 plan, élaboration, test, mise en oeuvre, 194
 sauvegardes, disponibilité, 196
 récursion
 (Voir récursion)
 répertoire personnel centralisé, 142
 répertoires personnels
 centralisés, 142

S

- sauvegardes
 - achat des logiciels, 187
 - aperçu , 186
 - construction des logiciels, 187
 - environnement des problèmes en relation avec les données, 186
 - Logiciel de sauvegarde AMANDA, 201
 - plan, modification, 102
 - problèmes de restauration, 193
 - restauration "bare metal", 193
 - test de la restauration, 193
 - stockage , 192
 - technologies utilisées, 198
 - cpio, 199
 - dump, 200
 - tar, 199
 - types de, 188
 - sauvegardes complètes, 189
 - sauvegardes différentielles, 189
 - sauvegardes incrémentielles, 189
 - types de supports, 190
 - bande, 190
 - disque, 190
 - réseau, 191
- scripts shell, 9
- shell bash, automatisation et , 9
- SMB, 113
- SMP, 41
- statistiques de contrôle
 - en relation avec la largeur de bande, 18
 - en relation avec la mémoire, 19
 - en relation avec le CPU, 17
 - en relation avec le stockage, 20
 - sélection de, 17
- stockage
 - accessible en réseau, 84, 112
 - NFS, 113
 - SMB, 113
 - ajout, 98, 114
 - configuration, mise à jour, 102
 - disque dur SCSI, 100
 - disques durs ATA, 99
 - formatage , 102, 116
 - matériel, installation, 98
 - mise à jour, /etc/fstab, 116
 - partitionnement , 101, 114
 - programme de sauvegarde, modification, 102
 - basé sur RAID
 - (Voir RAID)
 - contrôle de, 20
 - déploiement, 79
 - gestion de, 67, 92
 - consommation excessive de, 93
 - contrôle de l'espace libre, 93
 - croissance, normale, 95
 - problèmes liés à l'utilisateur, 93
 - utilisation par une application, 95
 - modes d'accès, 51
 - partition
 - aperçu de, 79
 - attributs des, 79
 - champ du type, 60
 - géométrie de, 79
 - logiques, 80
 - primaires, 80
 - type de, 80
 - étendues, 80
 - problèmes liés aux fichiers, 96
 - accès aux fichiers, 96
 - partage de fichiers, 97
 - périphérique de stockage de masse
 - adressage basé sur la géométrie, 69
 - adressage basé sur les blocs, 71
 - adressage, basé sur la géométrie, 69
 - adressage, en fonction des blocs, 71
 - aperçu de, 67
 - bras d'accès, 68
 - charges des E/S, opérations d'écriture, 77
 - charges des E/S, opérations de lecture, 77
 - charges des E/S, performance, 77
 - concepts d'adressage, 69
 - cylindre, 70
 - emplacement des E/S, 78
 - géométrie, problème avec, 71
 - interface IDE, 73
 - interface SCSI, 73
 - interfaces aux normes de l'industrie, 73
 - interfaces de, 71
 - interfaces, historique, 72
 - interfaces, normes de l'industrie , 73
 - latence rotationnelle, 77
 - latence, rotationnelle, 77
 - lecteurs contre scripteurs, 78
 - lecture des têtes, 77
 - limitations mécaniques de, 76
 - limitations électriques de, 76
 - mouvement du bras d'accès, 77
 - mouvement, bras d'accès, 77
 - performance de, 75
 - plateaux de disque, 67
 - plateaux, disque, 67
 - secteur, 70
 - traitement des commandes, 76
 - traitement, commande, 76
 - tête, 70
 - têtes, 68
 - écriture des têtes, 77
 - quotas de disque, 96
 - (Voir quotas de disque)
 - suppression, 103, 116

- /etc/fstab, suppression dans, 117
- commande umount, utilisation de , 117
- données, suppression, 103
- effacement du contenu, 104, 118
- systèmes de fichiers, 80, 107
 - activation de l'accès au stockage, 84
 - affichage des éléments montés, 110
 - basé sur des fichiers, 81
 - commande df, utilisation, 112
 - comptabilisation de l'espace, 82
 - comptabilisation, espace, 82
 - contrôle d'accès, 82
 - dates d'accès, 82
 - dates de création, 82
 - dates de modification, 82
 - examen du fichier /etc/mntab, 111
 - EXT2, 108
 - EXT3, 108
 - fichier /proc/mounts, 111
 - ISO 9660, 108
 - montage, 109
 - montage avec le fichier /etc/fstab, 113
 - MSDOS, 109
 - points de montage, 110
 - répertoire hiérarchique, 81
 - répertoires, 81
 - structure, répertoire, 83
 - VFAT, 109
- technologies, 51
 - Cache L1, 53
 - Cache L2, 53
 - disque dur, 55
 - disques dur, 55
 - Les registres du CPU, 52
 - mémoire cache, 52
 - mémoire principale, 54
 - RAM, 54
 - stockage de sauvegarde, 55
 - stockage hors ligne, 55
- technologies, avancées, 84
- Sysstat, 21, 25
- system-config-printer
 - (Voir configuration de l'imprimante)
- système de détection des intrusions, 11
- système de fichiers EXT3, 108
- système de fichiers ISO 9660, 108
- système de fichiers MSDOS , 109
- système de fichiers VFAT, 109
- systèmes de fichiers
 - étiquettes, 107
- systèmes de fichiers EXT2, 108
- sécurité
 - importance de , 7
 - Informations spécifiques à Red Hat Enterprise Linux, 11

T

- traitement multitâche symétrique, 41

U

- UID, 144
- utilisateurs
 - importance de , 6
- utilisation abusive des ressources, 142
- utilisation abusive, ressource, 142

Colophon

Les guides sont écrits sous format DocBook SGML v4.1. Les formats HTML et PDF sont produits à l'aide de feuilles de style DSSSL personnalisées et de scripts de wrapper jade personnalisés. Les fichiers DocBook SGML sont écrits avec **Emacs** avec l'aide du mode PSGML.

Garrett LeSage a créé les graphiques d'admonition (remarque, astuce, important, attention et avertissement). Ils peuvent être librement redistribués avec la documentation Red Hat.

L'équipe de documentation de produits Red Hat est composée des personnes suivantes :

Sandra A. Moore — Rédaction/Conception du *Guide d'installation pour les architectures x86, Itanium™, AMD64 et Intel® Extended Memory 64 Technology (Intel® EM64T) Red Hat Enterprise Linux* ; Rédaction/Conception du *Guide d'installation pour les architectures POWER IBM® Red Hat Enterprise Linux* ; Rédaction/Conception du *Guide d'installation pour les architectures S/390® IBM® et zSeries® eServer™ IBM® Red Hat Enterprise Linux*

John Ha — Rédaction/Conception du manuel *Configuration et gestion d'un cluster de Suite de cluster de Red Hat* ; Contribution à la rédaction/conception du *Guide de sécurité de Red Hat Enterprise Linux* ; Conception des feuilles de style et des scripts DocBook personnalisés

Edward C. Bailey — Rédaction/Conception du manuel *Introduction à l'administration système de Red Hat Enterprise Linux* ; Rédaction/Conception des *Notes de mise à jour* ; Contribution à la rédaction du *Guide d'installation pour les architectures x86, Itanium™, AMD64 et Intel® Extended Memory 64 Technology (Intel® EM64T) Red Hat Enterprise Linux*

Karsten Wade — Rédaction/Conception du *Guide de développement d'applications SELinux de Red Hat* ; Rédaction/Conception du *Guide de rédaction de politiques SELinux de Red Hat*

Andrius Benokraitis — Rédaction/Conception du *Guide de référence de Red Hat Enterprise Linux* ; Contribution à la rédaction/conception du *Guide de sécurité de Red Hat Enterprise Linux* ; Contribution à la rédaction du manuel *Guide d'administration système de Red Hat Enterprise Linux*

Paul Kennedy — Rédaction/Conception du *Guide de l'administrateur de GFS de Red Hat* ; Contribution à la rédaction du manuel *Configuration et gestion d'un cluster de Suite de cluster de Red Hat*

Mark Johnson — Rédaction/Conception du *Guide d'administration et de configuration du bureau de Red Hat Enterprise Linux*

Melissa Goldin — Rédaction/Conception du *Guide étape par étape de Red Hat Enterprise Linux*

L'équipe de traduction de Red Hat est composée des personnes suivantes :

Amanpreet Singh Alam — Traductions en punjabi

Jean-Paul Aubry — Traductions françaises

David Barzilay — Traductions portugaises (brésiliennes)

Runa Bhattacharjee — Traductions en bengali

Chester Cheng — Traductions chinoises traditionnelles

Verena Fuehrer — Traductions allemandes

Kiyoto James Hashida — Traductions japonaises

N. Jayaradha — Traductions en tamil

Michelle Jiyeen Kim — Traductions coréennes

Yelitz Louze — Traductions espagnoles

Noriko Mizumoto — Traductions japonaises

Ankitkumar Rameshchandra Patel — Traductions en gujarati

Rajesh Ranjan — Traductions en hindi

Nadine Richter — Traductions allemandes

Audrey Simons — Traductions françaises

Francesco Valente — Traductions italiennes

Sarah Saiying Wang — Traductions chinoises simplifiées

Ben Hung-Pin Wu — Traductions chinoises traditionnelles