Manuel FreeBSD

Résumé

Bienvenue à FreeBSD! Ce manuel décrit l'installation et l'utilisation quotidienne de *FreeBSD 13.1-RELEASE*, et *FreeBSD 12.3-RELEASE*. Ce document est le résultat du travail toujours en cours de nombreuses personnes. Certaines sections peuvent ne pas être à jour. Les personnes qui sont intéressées pour aider à mettre à jour et à compléter ce document devraient envoyer un courrier électronique à la liste de diffusion du groupe de documentation de FreeBSD.

La dernière version anglaise de ce document est disponible sur le site Web de FreeBSD. Les versions antérieures peuvent être obtenues auprès de http://docs.FreeBSD.org/doc/). Il peut être aussi téléchargé dans divers formats et options de compression depuis le serveur de téléchargement FreeBSD ou l'un des nombreux sites miroirs. Des recherches dans le Manuel et les autres documents peuvent être effectuées à partir de la page de recherches.

N.d.T.: Contactez Marc Fonvieille <blackend@FreeBSD.org> si vous voulez collaborer à la traduction.

Table des matières

Préface . . . 11
Public visé . . . 11
Modifications depuis la Seconde Edition . . . 11
Modifications depuis la Première Edition . . . 12
Organisation de cet ouvrage . . . 13
Conventions utilisées dans ce livre . . . 16
Remerciements . . . 17
I: Pour commencer . . . 18
1. Introduction . . . 19
1.1. Synopsis . . . 19
1.2. Bienvenue à FreeBSD! . . . 19
1.3. A propos du Projet FreeBSD . . . 22
2. Installing FreeBSD . . . 28
2.1. Synopsis . . . 28
2.2. Configuration matérielle minimale . . . 29
2.3. Tâches de pré-installation . . . 30
2.4. Lancer l'installation . . . 34
2.5. Utilisation de bsdinstall . . . 38
2.6. Allouer l'espace disque . . . 44
2.7. Récupération des fichiers de distribution . . . 67
2.8. Comptes utilisateurs, fuseau horaire, services et renforcement de la sécurité . . . 70
2.9. Interfaces réseau . . . 88
2.10. Dépannage . . . 99
2.11. Utilisation du CD Live . . . 100
3. Quelques bases d'UNIX . . . 101
3.1. Synopsis . . . 101
3.2. Consoles virtuelles terminaux . . . 101
3.3. Permissions . . . 105
3.4. Organisation de l'arborescence des répertoires . . . 108
3.5. Organisation des disques . . . 111
3.6. Monter et démonter des systèmes de fichiers . . . 117
3.7. Processus . . . 120
3.8. Daemons, signaux, et comment tuer un processus . . . 122
3.9. Interpréteurs de commandes - "Shells" . . . 124
3.10. Editeurs de texte . . . 127
3.11. Périphériques et fichiers spéciaux de périphérique . . . 127
3.12. Le format des fichiers binaires . . . 128
3.13. Pour plus d'information . . . 130

4. Installer des applications: les logiciels pré-compilés et les logiciels portés . . . 133
4.1. Synopsis . . . 133
4.2. Généralités sur l'installation de logiciels . . . 133
4.3. Trouver votre application . . . 135
4.4. Utiliser le système des logiciels pré-compilés . . . 137
4.5. Utiliser le catalogue des logiciels portés . . . 140
4.6. Activités de post-installation . . . 151
4.7. Que faire avec les logiciels portés ne fonctionnant pas? . . . 152
5. Le système X Window . . . 154
5.1. Synopsis . . . 154
5.2. Terminologie . . . 154
5.3. Installer X11 . . . 156
5.4. Configuration d'Xorg . . . 156
5.5. Utilisation des polices de caractères sous Xorg . . . 166
5.6. Le gestionnaire de connexion graphique XDM . . . 170
5.7. Environnements de bureau . . . 172
5.8. Installation de Compiz Fusion . . . 176
II: Tâches courantes . . . 180
6. Bureautique . . . 181
6.1. Synopsis . . . 181
6.2. Navigateurs . . . 181
6.3. Productivité . . . 185
6.4. Lecteurs de document . . . 188
6.5. Finance . . . 190
6.6. Résumé . . . 192
7. Multimédia . . . 194
7.1. Synopsis . . . 194
7.2. Configurer une carte son . . . 195
7.3. Fichiers MP3 . . . 199
7.4. Lecture des Vidéos . . . 202
7.5. Configuration des cartes TV . . . 211
7.6. Scanners . . . 213
8. Configurer le noyau de FreeBSD . . . 218
8.1. Synopsis . . . 218
8.2. Pourquoi compiler un noyau sur mesure? . . . 218
8.3. Compiler et installer un noyau sur mesure . . . 219
8.4. Le fichier de configuration . . . 222
8.5. Si quelque chose se passe mal . . . 238
9. Imprimer . . . 240
9.1. Synopsis . . . 240
9.2. Introduction . . . 240

9.3. Configuration de base . . . 242
9.4. Configuration avancée de l'imprimante . . . 257
9.5. Using Printers **Traduction en Cours** . . . 289
9.6. Alternatives to the Standard Spooler **Traduction en Cours** . . . 290
9.7. Troubleshooting **Traduction en Cours** . . . 290
10. Compatibilité binaire avec Linux . . . 291
10.1. Synopsis . . . 291
10.2. Configurer la compatibilité binaire avec Linux . . . 291
10.3. Système de base CentOS à partir des paquets binaires FreeBSD . . . 292
10.4. Système de base Debian / Ubuntu avec debootstrap(8) . . . 292
10.5. Sujets avancés . . . 293
11. WINE . . . 298
11.1. Synopsis . . . 298
11.2. WINE généralités et concepts . . . 299
11.3. Installer WINE sur FreeBSD . . . 301
11.4. Lancer un premier programme WINE sous FreeBSD . . . 303
11.5. Configurer WINE après installation . . . 305
11.6. Interfaces graphiques de gestion de WINE . . . 313
11.7. WINE sur un système FreeBSD avec plusieurs utilisateurs . . . 328
11.8. WINE sur FreeBSD Foire Aux Questions . . . 330
III: Administration Système . . . 334
12. Configuration et optimisation . . . 335
12.1. Synopsis . . . 335
12.2. Configuration principale . . . 335
12.3. Configuration des applications . . . 336
12.4. Démarrer des services . . . 337
12.5. Configuration de l'utilitaire `cron` . . . 338
12.6. Utilisation du système rc(8) sous FreeBSD . . . 340
12.7. Configuration des cartes réseaux . . . 342
12.8. Hôtes virtuels . . . 349
12.9. Fichiers de configuration . . . 350
12.10. Optimisation avec sysctl(8) . . . 354
12.11. Optimiser les disques . . . 355
12.12. Optimisation des limitations du noyau . . . 360
12.13. Ajouter de l'espace de pagination . . . 363
12.14. Gestion de l'énergie et des ressources . . . 365
12.15. Utiliser et déboguer l'ACPI sous FreeBSD . . . 367
13. Processus de démarrage de FreeBSD . . . 375
13.1. Synopsis . . . 375
13.2. Le problème du démarrage . . . 375
13.3. Le gestionnaire de démarrage et les étapes de démarrage . . . 376

13.4. Interaction avec le noyau au démarrage . . . 381
13.5. "Device Hints"-Paramétrage des périphériques . . . 381
13.6. Init: Initialisation de la gestion des processus . . . 382
13.7. Séquence d'arrêt du système . . . 383
14. Gestion des comptes et des utilisateurs . . . 385
14.1. Synopsis . . . 385
14.2. Introduction . . . 385
14.3. Le compte super-utilisateur . . . 387
14.4. Comptes système . . . 387
14.5. Comptes utilisateur . . . 387
14.6. Modifier des comptes . . . 388
14.7. Mettre en place des restrictions pour les utilisateurs . . . 392
14.8. Groupes . . . 395
15. Sécurité . . . 397
15.1. Synopsis . . . 397
15.2. Introduction . . . 397
15.3. Securing FreeBSD **Traduction en Cours** . . . 399
15.4. DES, MD5, et chiffrement . . . 399
15.5. Mots de passe non réutilisables . . . 400
15.6. L'encapsuleur TCP ("TCP Wrappers") . . . 407
15.7. Kerberos . . . 410
15.8. Kerberos5 **Traduction en Cours** . . . 418
15.9. OpenSSL . . . 418
15.10. IPsec . . . 421
15.11. OpenSSH . . . 427
15.12. Listes de contrôle d'accès au système de fichiers . . . 432
15.13. Surveillance des problèmes de sécurité relatifs aux programmes tierce-partie . . . 434
15.14. Avis de sécurité de FreeBSD . . . 436
15.15. Comptabilité des processus . . . 438
16. Jails . . . 440
16.1. Synopsis . . . 440
16.2. Termes relatifs aux environnements jail . . . 440
16.3. Introduction . . . 441
16.4. Création et contrôle de l'environnement jail . . . 442
16.5. Optimisation et administration . . . 444
17. Mandatory Access Control **Traduction en Cours** . . . 447
17.1. Synopsis . . . 447
17.2. Key Terms in this Chapter . . . 447
17.3. Explanation of MAC . . . 447
17.4. Understanding MAC Labels . . . 447
17.5. Module Configuration . . . 447

17.6. The MAC bsdextended Module . . . 447
17.7. The MAC ifoff Module . . . 447
17.8. The MAC portacl Module . . . 447
17.9. MAC Policies with Labeling Features . . . 447
17.10. The MAC partition Module . . . 447
17.11. The MAC Multi-Level Security Module . . . 447
17.12. The MAC Biba Module . . . 447
17.13. The MAC LOMAC Module . . . 447
17.14. Implementing a Secure Environment with MAC . . . 447
17.15. Another Example: Using MAC to Constrain a Web Server . . . 447
17.16. Troubleshooting the MAC Framework . . . 447
18. Audit des événements relatifs à la sécurité du système . . . 448
18.1. Synopsis . . . 448
18.2. Mots-clés . . . 449
18.3. Configuration de l'audit . . . 449
18.4. Travailler avec les traces d'audit . . . 454
19. Stockage des données . . . 458
19.1. Synopsis . . . 458
19.2. Noms des périphériques . . . 458
19.3. Ajouter des disques . . . 459
19.4. RAID . . . 462
19.5. Périphériques de stockage USB . . . 467
19.6. Création et utilisation de supports optiques (CDs) . . . 469
19.7. Création et utilisation de supports optiques (DVDs) . . . 477
19.8. Création et utilisation de disquettes . . . 482
19.9. Créer et utiliser les bandes magnétiques . . . 484
19.10. Sauvegardes sur disquettes . . . 487
19.11. Stratégies de sauvegarde . . . 488
19.12. Sauvegardes . . . 489
19.13. Systèmes de fichiers réseaux, en mémoire et sauvegardés sur fichier . . . 497
19.14. Instantané ("Snapshot") d'un système de fichiers . . . 500
19.15. Quotas d'utilisation des disques . . . 501
19.16. Chiffrer les partitions d'un disque . . . 505
19.17. Chiffrage de l'espace de pagination . . . 513
20. GEOM: architecture modulaire de gestion des disques . . . 515
20.1. Synopsis . . . 515
20.2. Introduction à GEOM . . . 515
20.3. RAID0 - "Striping" . . . 515
20.4. RAID1 - "mirroring" . . . 517
20.5. Périphériques réseau "GEOM Gate" . . . 520
20.6. Ajouter un label à un disque . . . 521

21. The Z File System (ZFS) **Traduction en Cours** . . . 523
21.1. What Makes ZFS Different . . . 523
21.2. Quick Start Guide . . . 523
21.3. `zpool` Administration . . . 523
21.4. `zfs` Administration . . . 523
21.5. Delegated Administration . . . 523
21.6. Additional Resources . . . 523
21.7. ZFS Features and Terminology . . . 523
22. Autres systèmes de fichiers . . . 524
22.1. Synopsis . . . 524
22.2. Systèmes de fichiers Linux® . . . 524
23. Le gestionnaire de volume Vinum . . . 526
23.1. Synopsis . . . 526
23.2. Les disques sont trop petits . . . 526
23.3. Les goulots d'étranglement d'accès aux données . . . 526
23.4. Intégrité des données . . . 528
23.5. Objets Vinum . . . 529
23.6. Quelques exemples . . . 531
23.7. Appellation des objets . . . 538
23.8. Configuration de Vinum . . . 541
24. Virtualisation . . . 544
24.1. Synopsis . . . 544
24.2. FreeBSD comme système d'exploitation invité . . . 544
24.3. FreeBSD comme système d'exploitation hôte . . . 568
25. Localisation - Utilisation et configuration de l'I18N/L10N . . . 569
25.1. Synopsis . . . 569
25.2. Les bases . . . 569
25.3. Utiliser la localisation . . . 570
25.4. Compiler des programmes I18N . . . 577
25.5. Localiser FreeBSD pour des langues spécifiques . . . 577
26. Mise à jour de FreeBSD . . . 581
26.1. Synopsis . . . 581
26.2. Mise à jour de FreeBSD . . . 581
26.3. Portsnap: un outil de mise à jour du catalogue des logiciels portés . . . 589
26.4. Updating the Documentation Set **Traduction en Cours** . . . 590
26.5. Suivre une branche de développement . . . 591
26.6. Synchroniser vos sources . . . 595
26.7. Recompiler le système . . . 596
26.8. Suivre les mises à jour pour plusieurs machines . . . 611
27. DTrace . . . 613
27.1. Synopsis . . . 613

27.2. Des différences de mise en oeuvre . . . 613
27.3. Activer la prise en charge de DTrace . . . 614
27.4. Utiliser DTrace . . . 615
27.5. Le langage D . . . 618
IV: Réseau . . . 619
28. Serial Communications **Traduction en Cours** . . . 620
28.1. Synopsis . . . 620
28.2. Introduction . . . 620
28.3. Terminals . . . 620
28.4. Dial-in Service . . . 620
28.5. Dial-out Service . . . 620
28.6. Setting Up the Serial Console . . . 620
29. PPP et SLIP . . . 621
29.1. Synopsis . . . 621
29.2. Using User PPP **Traduction en Cours** . . . 621
29.3. Utiliser PPP intégré au noyau . . . 621
29.4. Utiliser PPP sur Ethernet (PPPoE) . . . 629
29.5. Utiliser PPP sur ATM (PPPoA) . . . 632
29.6. Utiliser SLIP . . . 635
30. Courrier électronique . . . 647
30.1. Synopsis . . . 647
30.2. Utilisation du courrier électronique . . . 647
30.3. Configuration de sendmail . . . 650
30.4. Changer votre agent de transfert de courrier . . . 653
30.5. Dépannage . . . 656
30.6. Sujets avancés . . . 659
30.7. SMTP avec UUCP . . . 662
30.8. Configuration pour l'envoi seul . . . 664
30.9. Utiliser le courrier électronique avec une connexion temporaire . . . 665
30.10. Authentification SMTP . . . 667
30.11. Clients de messagerie . . . 668
30.12. Utiliser fetchmail . . . 676
30.13. Utiliser procmail . . . 677
31. Serveurs réseau . . . 680
31.1. Synopsis . . . 680
31.2. Le "super-serveur" inetd . . . 680
31.3. Système de fichiers réseau (NFS) . . . 685
31.4. Services d'information réseau (NIS/YP) . . . 692
31.5. Configuration réseau automatique (DHCP) . . . 710
31.6. Serveurs de noms (DNS) . . . 715
31.7. Serveur HTTP Apache . . . 726

31.8. Protocole de transfert de fichiers (FTP) . . . 731
31.9. Serveur de fichiers et d'impression pour clients Microsoft® Windows® (Samba) . . . 732
31.10. Synchronisation de l'horloge avec NTP . . . 735
32. Firewalls **Traduction en Cours** . . . 739
32.1. Introduction . . . 739
32.2. Firewall Concepts . . . 739
32.3. Firewall Packages . . . 739
32.4. The OpenBSD Packet Filter (PF) and ALTQ . . . 739
32.5. The IPFILTER (IPF) Firewall . . . 739
32.6. IPFW . . . 739
33. Administration réseau avancée . . . 740
33.1. Synopsis . . . 740
33.2. Passerelles et routes . . . 740
33.3. Réseau sans fil . . . 747
33.4. Bluetooth . . . 755
33.5. Bridging . . . 765
33.6. Système sans disque dur . . . 768
33.7. ISDN . . . 777
33.8. Translation d'adresses . . . 781
33.9. IP sur liaison parallèle (PLIP) . . . 785
33.10. IPv6 . . . 787
33.11. ATM ("Asynchronous Transfer Mode") . . . 793
V: Annexes . . . 796
Annexe A: Se procurer FreeBSD . . . 797
A.1. Editeurs de CD-ROMs et DVDs . . . 797
A.2. Sites FTP . . . 799
A.3. CVS anonyme . . . 806
A.4. Utiliser CTM . . . 809
A.5. Utiliser CVSup . . . 813
A.6. Utiliser Portsnap . . . 827
A.7. Etiquettes CVS . . . 830
A.8. Sites AFS . . . 835
A.9. Sites rsync . . . 835
Annexe B: Bibliographie . . . 837
B.1. Livres magazines consacrés à FreeBSD . . . 837
B.2. Manuels d'utilisation . . . 838
B.3. Manuels d'administration . . . 839
B.4. Manuels de programmation . . . 839
B.5. "Internes" du système d'exploitation . . . 840
B.6. Ouvrages de référence en matière de sécurité . . . 840
B.7. Ouvrages de référence sur le matériel . . . 841

B.8. Histoire d’UNIX® . . . 841
B.9. Revues et journaux . . . 842
Annexe C: Ressources sur Internet . . . 843
C.1. Listes de diffusion . . . 843
C.2. Forums de discussion . . . 858
C.3. Serveurs World Wide Web . . . 859
C.4. Adresses électroniques . . . 859
C.5. Comptes . . . 860
Annexe D: Clés OpenPGP . . . 861
D.1. Officers . . . 861

Préface

Public visé

Le nouveau venu à FreeBSD constatera que la première section de ce livre guide l'utilisateur à travers le processus d'installation de FreeBSD, et présente progressivement les concepts et les conventions qui sont les fondements d'UNIX®. Travailler avec cette section demande un peu plus que le simple désire d'explorer, et la capacité d'assimiler de nouveaux concepts quand ils sont présentés.

Une fois que vous en êtes arrivé là, la seconde, bien plus grande, section du Manuel est une référence complète de tous les sujets qui intéressent les administrateurs systèmes de FreeBSD. Certains de ces chapitres peuvent vous recommander d'effectuer des lectures préliminaires, cela est noté dans le synopsis au début de chaque chapitre.

Pour une liste de sources d'informations complémentaires, veuillez consulter Bibliographie.

Modifications depuis la Seconde Edition

Cette seconde édition est le point culminant de plus de deux ans de travail pour les membres du Groupe de Documentation de FreeBSD. Ce qui suit présente les changements principaux de cette nouvelle édition:

- Configuration et optimisation, le chapitre "Configuration et optimisation", a été augmenté avec des informations nouvelles sur la gestion ACPI des ressources et de l'énergie, sur l'utilitaire système `cron`, et sur d'autres d'options supplémentaires d'optimisation du noyau.
- Sécurité, le chapitre "Sécurité", a été augmenté avec de nouvelles informations sur les réseaux privés virtuels (VPNs), les listes de contrôle d'accès au système de fichiers (ACLs), et sur les avis de sécurité.
- Mandatory Access Control, "Le contrôle d'accès obligatoire" (MAC) est un nouveau chapitre ajouté avec cette édition. Il explique ce qu'est le MAC et comment ce mécanisme peut être utilisé pour sécuriser un système FreeBSD.
- Stockage des données, le chapitre "Stockage des données", a bénéficié de l'ajout de nouvelles sections concernant les périphériques de stockage USB, les instantanés de systèmes de fichiers, les quotas d'utilisation des disques, les systèmes de fichiers réseaux et sauvegardés sur fichier, et le chiffrage de partitions.
- Le gestionnaire de volume Vinum, "Vinum", est un nouveau chapitre apparaissant avec cette édition. Il décrit l'utilisation de Vinum, un gestionnaire de volume qui permet la création de disques logiques indépendants du périphérique, et l'utilisation de systèmes RAID-0, RAID-1 et RAID-5 logiciels.
- Une section dépannage a été ajoutée au chapitre PPP et SLIP, PPP et SLIP.
- Courrier électronique, le chapitre "Courrier électronique", bénéficie de nouvelles sections sur l'utilisation d'agents de transfert de courrier alternatifs, sur l'authentification SMTP, l'UUCP, fetchmail, procmail, et d'autres sujets avancés.

- Serveurs réseau le chapitre "Serveurs réseau", apparaît avec cette édition. Ce chapitre traite de la configuration du serveur HTTP Apache, de ftpd, et celle d'un serveur pour clients Microsoft® Windows® à l'aide de Samba. Certaines sections du chapitre Administration réseau avancée, "Administration réseau avancée" ont été déplacées vers ce nouveau chapitre.
- Administration réseau avancée, le chapitre "Administration réseau avancée" a été complété avec des informations sur l'utilisation des périphériques Bluetooth® sous FreeBSD, la configuration de réseaux sans fil, et sur le mode de transfert réseau asynchrone (ATM).
- Un glossaire a été ajouté pour centraliser les définitions des termes techniques employés tout au long de cet ouvrage.
- La présentation des tableaux et des figures a été améliorée.

Modifications depuis la Première Edition

La seconde édition est le point culminant de deux ans de travail pour les membres du Groupe de Documentation de FreeBSD. Ce qui suit présente les changements principaux de cette nouvelle édition:

- Un sommaire complet a été ajouté.
- Toutes les figures ASCII ont été remplacées par des graphiques.
- Un synopsis standard a été ajouté à chaque chapitre pour donner un rapide résumé des informations contenues par ce dernier et ce qu'est sensé connaître le lecteur.
- Le contenu a été réorganisé de façon logique en trois parties: "Pour commencer", "L'Administration Système", et "Annexes".
- Le Installer FreeBSD ("Installer FreeBSD") fut complètement réécrit avec de nombreuses photos d'écrans pour rendre le texte plus facile à comprendre pour les nouveaux utilisateurs.
- Le Quelques bases d'UNIX ("Quelques bases d'UNIX®") a été augmenté pour contenir des informations additionnelles sur les processus, daemons et signaux.
- Le Installer des applications. les logiciels pré-compilés et les logiciels portés ("Installer des applications") a été augmenté pour contenir des informations complémentaires sur la gestion des applications pré-compilées.
- Le Le système X Window ("Le système X Window") a complètement été réécrit en insistant sur l'utilisation de technologies modernes d'environnement de travail comme KDE et GNOME sous XFree86™ 4.X.
- Le Processus de démarrage de FreeBSD ("Le processus de démarrage de FreeBSD") a été augmenté.
- Le Stockage des données ("Stockage des données") fut réécrit à partir de ce qui était à l'origine deux chapitres séparés "Disques" et "Sauvegardes". Nous pensons que le sujet est plus facile à appréhender quand il est présenté en un seul chapitre. Une section sur RAID (matériel et logiciel) fut également ajoutée.
- Le Serial Communications ("Communications série") a été complètement réorganisé et mis à jour pour FreeBSD 4.X/5.X.
- Le PPP et SLIP ("PPP et SLIP") a été sensiblement mis à jour.

- Plusieurs nouvelles sections ont été ajouté au Administration réseau avancée ("Administration réseau avancée").
- Le Courrier électronique ("Courrier électronique") fut augmenté pour inclure plus d'informations au sujet de la configuration de sendmail.
- Le Compatibilité binaire avec Linux® ("Compatibilité Linux®") a été augmenté pour inclure des informations sur l'installation d'Oracle® et SAP® R/3®.
- Les nouveaux sujets suivants sont abordés dans cette seconde édition:
  - Configuration et optimisation (Configuration et optimisation).
  - Multimédia (Multimédia)

Organisation de cet ouvrage

Ce livre est divisé en cinq parties logiquement distinctes. Le première section, *Pour commencer*, couvre l'installation et les bases de l'utilisation de FreeBSD. On s'attend à ce que le lecteur suive ces chapitres dans l'ordre, sautant éventuellement les chapitres traitant de sujets familiers. La seconde section *Tâches courantes*, couvre les fonctionnalités de FreeBSD fréquemment utilisées. Cette section, ainsi que toutes les sections suivantes, peuvent être lues dans n'importe quel ordre. Chaque chapitre débute avec un synopsis succinct qui décrit ce dont parle le chapitre et ce qu'on s'attend à ce que le lecteur sache déjà. Cela en vue de permettre au lecteur occasionnel de se rendre directement aux chapitres qui l'intéresse. La troisième section, *Administration système*, traite des sujets concernant l'administration. La quatrième section, *Réseaux*, couvre le domaine des réseaux et des serveurs. La cinquième section contient des annexes d'information de référence.

Introduction

Présente FreeBSD à un nouvel utilisateur. Il décrit l'histoire du projet FreeBSD, ses objectifs, son mode de développement.

Installer FreeBSD

Guide un utilisateur à travers le processus d'installation. Quelques sujets d'installation avancée, comme l'installation avec une console série, sont aussi couverts.

Quelques bases d'UNIX

Couvre les commandes et fonctionnalités de base du système d'exploitation FreeBSD. Si vous êtes familier avec Linux® ou un autre type d'UNIX® alors vous pouvez probablement passer ce chapitre.

Installer des applications. les logiciels pré-compilés et les logiciels portés

Couvre l'installation de logiciels tiers avec l'innovant "Catalogue de logiciels portés" de FreeBSD et les logiciels pré-compilés.

Le système X Window

Décrit le système X Window en général et l'utilisation d'X11 sur FreeBSD en particulier. Décrit également les environnements de travail comme KDE et GNOME.

Bureautique

Liste les applications de bureautique courantes, comme les navigateurs Web et les suites de

bureautique, et décrit comment les installer sous FreeBSD.

Multimédia

Montre comment installer le support du son et de la vidéo pour votre système. Décrit également quelques applications audio et vidéo.

Configurer le noyau de FreeBSD

Explique pour quelles raisons vous devriez configurer un nouveau noyau et fournit des instructions détaillées pour la configuration, la compilation et l'installation d'un noyau sur mesures.

Imprimer

Décrit la gestion des imprimantes sous FreeBSD, y compris les informations sur les pages d'en-tête, la comptabilisation de l'usage et la configuration de base.

Compatibilité binaire avec Linux®

Décrit les caractéristiques de la compatibilité Linux® sous FreeBSD. Fournit également les instructions détaillées de l'installation de plusieurs applications Linux® populaires comme Oracle®, SAP® R/3® et Mathematica®.

Configuration et optimisation

Décrit les paramètres disponibles pour les administrateurs systèmes afin d' optimiser les performances d'un système FreeBSD. Décrit également les différents fichiers de configuration utilisés dans FreeBSD et où les trouver.

Processus de démarrage de FreeBSD

Décrit le processus de démarrage de FreeBSD et explique comment contrôler ce processus avec des options de configuration.

Gestion des comptes et des utilisateurs

Décrit la création et la manipulation des comptes utilisateur. Traite également des limitations de ressources qui peuvent être appliquées aux utilisateurs et des autres tâches de gestion des comptes.

Sécurité

Décrit différents outils disponibles pour vous aider à sécuriser votre système FreeBSD, dont Kerberos, IPsec et OpenSSH.

Environnements jails

Décrit l'organisation des environnements jail, et les améliorations apportées par ces environnements par rapport au support chroot traditionnel de FreeBSD.

Mandatory Access Control

Explique ce qu'est le contrôle d'accès mandataire (MAC) et comment ce mécanisme peut être utilisé pour sécuriser un système FreeBSD.

Audit des événements relatifs à la sécurité du système

Décrit ce qu'est l'audit d'événements sous FreeBSD, comment cette fonctionnalité peut être

installée, configurée et comment les audits peuvent être examinés et surveillés.

Stockage des données

Décrit comment gérer les supports de stockage et les systèmes de fichiers avec FreeBSD. Cela inclut les disques physiques, les systèmes RAID, les supports optiques et bandes, les disques mémoires, et les systèmes de fichiers réseau.

GEOM. architecture modulaire de gestion des disques

Décrit ce qu'est le système GEOM sous FreeBSD et comment configurer les différents niveaux de RAID supportés.

Le gestionnaire de volume Vinum

Décrit comment utiliser Vinum, un gestionnaire de volume logique qui permet d'avoir des disques logiques indépendants du périphérique, et le RAID-0, RAID-1 et RAID-5 logiciel.

Virtualisation

Décrit ce que les systèmes de virtualisation apportent, et comment ils peuvent être utilisés avec FreeBSD.

Localisation - Utilisation et configuration de l'I18N/L10N

Décrit comment utiliser FreeBSD avec des langues autres que l'anglais. Couvre la localisation du système et des applications.

Mise à jour de FreeBSD

Explique les différences entre FreeBSD-STABLE, FreeBSD-CURRENT et les versions de publication;. Décrit quel type d'utilisateurs pourrait tirer profit de suivre un système de développement et présente le processus.

Communications série

Explique comment connecter terminaux et modems à votre système FreeBSD aussi bien pour les connexions entrantes que sortantes.

PPP et SLIP

Décrit comment utiliser PPP, SLIP ou PPP sur Ethernet pour se connecter à des systèmes distants à l'aide de FreeBSD.

Courrier électronique

Explique les différents composants d'un serveur de courrier et plonge dans la configuration de base du serveur de courrier le plus populaire: sendmail.

Serveurs réseau

Fournit des instructions détaillées et des exemples de fichiers de configuration pour configurer votre machine FreeBSD comme serveur de fichiers, serveur de noms de domaine, serveur d'information réseau, ou comme serveur de synchronisation d'horloge.

Firewalls

Explique la philosophie des coupe-feux logiciels et fournit des informations détaillées sur la configuration des différents coupe-feux disponibles pour FreeBSD.

Administration réseau avancée

Décrit de nombreux sujets sur l'utilisation réseau, dont le partage d'une connexion Internet avec d'autres ordinateurs sur votre réseau local, routage, réseaux sans-fils, Bluetooth®, ATM, IPv6, et bien plus.

Se procurer FreeBSD

Enumère les différentes sources pour obtenir FreeBSD sur CDROM ou DVD, ainsi que les différents sites Internet qui vous permettent de télécharger et d'installer FreeBSD.

Bibliographie

Cet ouvrage aborde de nombreux sujets cela peut vous laisser sur votre faim et à la recherche de plus de détails. La bibliographie énumère d'excellents ouvrages qui sont référencés dans le texte.

Ressources sur Internet

Décrit les nombreux forums disponibles pour les utilisateurs de FreeBSD pour poster des questions et engager des conversations techniques au sujet de FreeBSD.

Clés OpenPGP

Liste les clés PGP de nombreux développeurs FreeBSD.

Conventions utilisées dans ce livre

Pour fournir un texte logique et facile à lire, plusieurs conventions sont respectées tout au long du livre.

Conventions typographiques

Italique

Une police de caractères *italique* est utilisée pour les noms de fichiers, les URLs, le texte à mettre en valeur et la première utilisation de termes techniques.

`Police de caractères à chasse fixe`

Une police de caractères à `chasse fixe` est utilisée pour les messages d'erreurs, les commandes, les variables d'environnement, les noms des logiciels portés, les noms d'hôtes, les noms d'utilisateurs, les noms de groupes, les noms de périphériques, les variables et les morceaux de code source.

Caractères gras

Des caractères gras sont utilisés pour les applications, les commandes et les touches.

Utilisation du clavier

Les touches sont représentées en **gras** pour ressortir du texte. Les combinaisons de touches qui sont sensées être tapées simultanément sont représentées avec `+` entre chaque touche, comme par exemple:

`Ctrl` + `Alt` + `Del`

Indiquant que l'utilisateur devra appuyer simultanément sur les touches `Ctrl`, `Alt`, et `Del`.

Les touches qui sont sensées être tapées en séquence seront séparées par une virgule, par exemple:

`Ctrl` + `X`, `Ctrl` + `S`

Signifiera que l'on on attend à ce que l'utilisateur tape les touches `Ctrl` et `X` simultanément et ensuite tape `Ctrl` et `S` simultanément.

Exemples

Les exemples commençant par E:\ indiquent une commande MS-DOS®. Sauf indication contraire, on peut exécuter ces commandes depuis une fenêtre "d'invite de commande" dans un environnement Microsoft® Windows® moderne.

```
E:\ tools\fdimage floppies\kern.flp A:
```

Les exemples commençant par # indiquent que la commande doit être lancée en tant que super-utilisateur sous FreeBSD. Vous pouvez ouvrir une session en tant que `root` pour taper cette commande, ou ouvrir une session sous votre compte normal et utiliser su(1) pour obtenir les privilèges de super-utilisateur.

```
# dd if=kern.flp of=/dev/fd0
```

Les exemples commençant par % indiquent une commande qui devrait être lancée par un utilisateur normal. Sauf indication contraire, la syntaxe de l'interpréteur de commandes C-shell est utilisée pour configurer les variables d'environnement et autres commandes de l'interpréteur.

```
% top
```

Remerciements

L'ouvrage que vous avez en main représente les efforts de plusieurs centaines de personnes dans le monde. Qu'ils aient envoyé des corrections de fautes de frappe, ou soumis des chapitres entiers, toutes les contributions ont été utiles.

Plusieurs entreprises ont supporté le développement de ce document en payant des auteurs à travailler à plein temps dessus, en payant pour la publication etc... En particulier, BSDi (rachetée plus tard par Wind River Systems) a payé à temps plein des membres du Groupe de Documentation de FreeBSD à l'amélioration de ce livre menant ainsi à la publication de la première version imprimée en Mars 2000 (ISBN 1-57176-241-8). Wind River Systems a ensuite payé plusieurs auteurs supplémentaires pour apporter un certain nombre d'améliorations à l'infrastructure de publication et à l'ajout de chapitres. Ce travail a abouti à la publication de la deuxième édition imprimée en Novembre 2001 (ISBN 1-57176-303-1). En 2003-2004, FreeBSD Mall, Inc, a payé plusieurs auteurs pour travailler sur l'amélioration de ce manuel en vue de la publication de la troisième édition papier.

Partie I: Pour commencer

Cette partie du Manuel FreeBSD est destinée aux nouveaux venus à FreeBSD, utilisateurs et administrateurs. Ces chapitres:

- Présenteront FreeBSD.
- Guideront les lecteurs à travers le processus d'installation.
- Enseigneront quelques bases et fondements d'UNIX®.
- Montreront comment installer la profusion d'applications tierces disponibles pour FreeBSD.
- Présenteront X, le système de fenêtrage d'UNIX®, et détailleront comment configurer un environnement de travail qui rendra les utilisateurs plus productifs.

Le nombre de références dans le texte a été limité au minimum afin que cette section du Manuel puisse être lue du début jusqu'à la fin avec le moins de changements de pages possibles.

Chapitre 1. Introduction

1.1. Synopsis

Merci de votre intérêt pour FreeBSD! Le chapitre suivant traite de divers aspects concernant le projet FreeBSD, comme son histoire, ses objectifs, son mode de développement, et d'autres.

Après la lecture de ce chapitre, vous connaîtrez:

- Comment FreeBSD est lié aux autres systèmes d'exploitation.
- L'histoire du Projet FreeBSD.
- Les objectifs du Projet FreeBSD.
- Les bases du mode de développement open-source de FreeBSD.
- Et bien sûr: l'origine du nom "FreeBSD".

1.2. Bienvenue à FreeBSD!

FreeBSD est une système d'exploitation basé sur 4.4BSD-Lite2 pour les ordinateurs à base d'architecture Intel (x86 et Itanium®), AMD64, les ordinateurs DEC Alpha™, et Sun UltraSPARC®. Le portage pour d'autres architectures est également en cours. Pour connaître l'histoire du projet, lisez Un court historique de FreeBSD. Pour avoir une description de la version la plus récente, allez à la section A propos de cette version. Si vous voulez contribuer d'une façon ou d'une autre au projet FreeBSD (code, matériel, dons), voyez s'il vous plaît à la section Contribuer à FreeBSD.

1.2.1. Que peut faire FreeBSD?

FreeBSD dispose de nombreuses caractéristiques remarquables. Parmi lesquelles:

- *Multi-tâche préemptif* avec ajustement dynamique des priorités pour garantir un partage équilibré et fluide de l'ordinateur entre les applications et les utilisateurs et cela même sous les charges les plus importantes.
- *Accès multi-utilisateurs* qui permet à de nombreuses personnes d'utiliser en même temps un système FreeBSD à des fins très différentes. Cela signifie, par exemple, que des périphériques tels que les imprimantes ou les lecteurs de bandes peuvent être partagés entre tous les utilisateurs sur le système ou sur le réseau et que des limitations d'utilisation des ressources peuvent être appliquées à des utilisateurs ou groupes d'utilisateurs, protégeant ainsi les ressources systèmes critiques d'une sur-utilisation.
- *Réseau TCP/IP* complet dont le support de standards industriels comme SCTP, DHCP, NFS, NIS, PPP, SLIP, IPsec, et IPv6. Cela signifie que votre machine FreeBSD peut coopérer facilement avec d'autres systèmes ou être utilisée comme serveur d'entreprise, fournissant des fonctions essentielles comme NFS (accès aux fichiers en réseau) et le service de courrier électronique, ou encore l'accès de votre entreprise à l'Internet grâce aux services WWW, FTP, et aux fonctionnalités de routage et de coupe-feu (sécurité).
- *La protection de la mémoire* garantit que les applications (ou les utilisateurs) ne peuvent

interférer entre eux. Une application qui plante n'affectera en rien les autres.

- FreeBSD est un système d'exploitation *32-bits* (*64-bits* sur l'architecture Alpha, Itanium®, AMD64, et UltraSPARC®) et a été conçu comme tel dès le début.
- Le *Système X Window* (X11R7), standard industriel, fournit une interface graphique à l'utilisateur (Graphical User Interface - GUI), moyennant l'achat d'une carte VGA ordinaire et d'un moniteur, et est livré avec l'intégralité de son code source.
- *Compatibilité binaire* avec de nombreux programmes compilés pour Linux, SCO, SVR4, BSDI et NetBSD.
- Des milliers d'applications *prêtes à l'emploi* sont disponibles grâce au catalogue des logiciels portés (ports) et au catalogue des logiciels *pré-compilés* (packages). Pourquoi chercher sur l'Internet alors que tout est là?.
- Des milliers d'applications *faciles à porter* sont disponibles sur l'Internet. FreeBSD est compatible au niveau du code source avec les systèmes UNIX® commerciaux les plus répandus et donc la plupart des applications exigent peu, sinon aucune modification, pour les compiler.
- *Mémoire virtuelle* à la demande et "cache unifié pour les disques et la mémoire virtuelle" cela permet de répondre aux besoins des applications gourmandes en mémoire tout en garantissant le temps de réponse aux autres utilisateurs.
- Support du *traitement symétrique multiprocesseurs* (SMP).
- Des outils complets de développement *C*, *C++*, et *Fortran*. De nombreux autres langages pour la recherche de pointe et le développement sont aussi disponibles dans les catalogues des logiciels portés et pré-compilés.
- La disponibilité *Code source* de l'intégralité du système vous donne un contrôle total sur votre environnement. Pourquoi être prisonnier d'une solution propriétaire et dépendant de votre fournisseur alors que vous pouvez avoir un véritable système ouvert?
- Une *documentation en ligne* très complète.
- *Et beaucoup d'autres choses encore!*

FreeBSD est basé sur la version 4.4BSD-Lite2 du "Computer Systems Research Group" (CSRG) de l'Université de Californie à Berkeley et continue la tradition de développement renommée des systèmes BSD. En plus de l'excellent travail fourni par le CSRG, le Projet FreeBSD a investi des milliers d'heures de travail pour optimiser le système pour arriver aux meilleures performances et au maximum de fiabilité sous la charge d'un environnement de production. Alors que la plupart des géants dans le domaine des systèmes d'exploitation pour PC s'acharnent encore à obtenir de telles possibilités, performances et fiabilité, FreeBSD peut les offrir *dès maintenant*!

La seule limite aux domaines d'application auxquels FreeBSD peut satisfaire est votre propre imagination. Du développement de logiciels à la production robotisée, de la gestion de stocks à la correction d'azimut pour les antennes satellites; si un UNIX® commercial peut le faire, il y a de très fortes chances que FreeBSD le puisse aussi! FreeBSD bénéficie aussi de centaines d'applications de haute qualité développées par les centres de recherche et les universités du monde entier, souvent disponibles gratuitement ou presque. Il existe aussi des applications commerciales et leur nombre croît de jour en jour.

Comme le code source de FreeBSD lui-même est globalement disponible, le système peut aussi être

adapté sur mesure à un point pratiquement jamais atteint pour des applications ou des projets particuliers, d'une façon qui serait habituellement impossible avec les systèmes d'exploitation commerciaux de la plupart des principaux fournisseurs. Voici juste quelques exemples d'applications pour lesquelles FreeBSD est utilisé:

- *Services Internet:* les fonctionnalités réseau TCP/IP robustes qu'inclut FreeBSD en font la plate-forme idéale pour un éventail de services Internet, tels que:
  - Serveurs FTP
  - Serveurs World Wide Web (standard ou sécurisé [SSL])
  - Routage IPv4 et IPv6
  - Coupe-feux et passerelles de traduction d'adresses ("IP masquerading")
  - Serveurs de courrier électronique
  - Serveurs de News USENET (forums de discussion) ou Bulletin Board Systems (BBS)
  - Et plus...

    Avec FreeBSD, vous pouvez facilement commencer petit avec un PC 386 à bas prix et évoluer jusqu'à un quadri-processeurs Xeon avec stockage RAID au fur et à mesure que votre entreprise s'agrandit.
- *Education:* Etes-vous étudiant en informatique ou dans un domaine d'ingénierie apparenté? Il n'y a pas de meilleur moyen pour étudier les systèmes d'exploitation, l'architecture des ordinateurs et les réseaux que l'expérience directe et de "derrière la coulisse" que FreeBSD peut vous apporter. Il y a aussi un grand nombre d'outils mathématiques, graphiques et de Conception Assistée par Ordinateur qui en font un outil très utile pour ceux qui s'intéressent aux ordinateurs essentiellement pour faire un *autre* travail!
- *Recherche:* Avec le code source de la totalité du système disponible, FreeBSD est un excellent outil de recherche sur les systèmes d'exploitation tout autant que pour d'autres branches de l'informatique. Le fait que FreeBSD soit librement disponible rend aussi possible l'échange d'idées et le développement partagé entre groupes éloignés sans avoir à se préoccuper de problèmes de licence particulières ou de restrictions à ce qui pourrait être discuté sur des forums ouverts.
- *Réseau:* Il vous faut un nouveau routeur? Un serveur de domaine (DNS)? Un coupe-feu pour tenir les gens à l'écart de votre réseau interne? FreeBSD peut facilement faire de votre vieux 386 ou 486 inutilisé qui traîne dans un coin un routeur évolué avec des fonctionnalités sophistiquées de filtrage de paquets.
- *Station de travail X Window:* FreeBSD est un excellent choix pour faire un terminal X peu coûteux, en utilisant le serveur X11 librement disponible. Au contraire d'un terminal X, FreeBSD permet d'exécuter localement, si désiré, un grand nombre d'applications, déchargeant ainsi le serveur central. FreeBSD peut même démarrer "sans disque", ce qui permet de concevoir des postes de travail individuels moins chers et plus faciles à administrer.
- *Développement de logiciel:* Le système FreeBSD de base inclut un environnement de développement complet dont les compilateur et débogueur GNU C/C++ réputés.

FreeBSD est disponible sous forme de code source ou binaire sur CDROM, DVD ou par ftp anonyme,

Voyez Se procurer FreeBSD pour plus de détails.

1.2.2. Qui utilise FreeBSD?

FreeBSD est utilisé par certains des plus importants sites sur l'Internet, parmi lesquels:

- Yahoo!
- Apache
- Blue Mountain Arts
- Pair Networks
- Sony Japan
- Netcraft
- Weathernews
- Supervalu
- TELEHOUSE America
- Sophos Anti-Virus
- JMA Wired

et de nombreux autres.

1.3. A propos du Projet FreeBSD

La section suivante fournit des informations générales sur le projet, dont un court historique, les objectifs du projet, et le mode de développement du projet.

1.3.1. Un court historique de FreeBSD

Le projet FreeBSD a vu le jour au début de 1993, en partie comme extension du "Kit de mise à jour non officiel de 386BSD" des trois derniers coordinateurs du kit de mise à jour : Nate Williams, Rod Grimes et moi-même.

Notre objectif de départ était de fournir une distribution intermédiaire de 386BSD pour corriger un certain nombre de problèmes que le mécanisme du kit de mise à jour ne permettait pas de résoudre. Certains d'entre vous se rappellent peut-être que l'intitulé de travail d'origine du projet était "386 BSD 0.5" ou "386BSD Interim" en référence à ce problème.

386BSD était le système d'exploitation de Bill Jolitz, qui souffrait assez sévèrement à ce moment-là d'avoir été négligé pendant presque un an. Comme le kit de mise à jour enflait de plus en plus inconfortablement au fil des jours, nous avons décidé à l'unanimité qu'il fallait faire quelque chose et aider Bill en fournissant cette distribution provisoire de "remise à plat". Ces projets se sont brutalement interrompus lorsque Bill a décidé de retirer son aval au projet sans dire clairement ce qui serait fait à la place.

Il ne nous a pas fallu longtemps pour décider que l'objectif restait valable, même sans l'adhésion de Bill, et nous avons donc adopté le nom "FreeBSD", une proposition de David Greenman. Nos

objectifs de départ ont été définis après avoir consulté les utilisateurs du moment du système et, dès qu'il est devenu clair que le projet était parti pour devenir un jour éventuellement réalité, nous avons contacté Walnut Creek CDROM dans l'optique d'améliorer la distribution de FreeBSD pour le grand nombre de ceux qui n'avaient pas la chance de pouvoir accéder facilement à l'Internet. Non seulement Walnut Creek CDROM a adopté l'idée de distribuer FreeBSD sur CDROM, mais a été jusqu'à fournir au projet une machine pour travailler et une connexion rapide à l'Internet. Sans le degré pratiquement sans précédent de confiance de Walnut Creek CDROM en ce qui n'était alors qu'un projet totalement inconnu, il y a peu de chance que FreeBSD ait été aussi loin, aussi vite, que là où il en est aujourd'hui.

La première version sur CDROM (et sur l'ensemble du Net) fut FreeBSD 1.0, parue en Décembre 1993. Elle reposait sur la bande 4.3BSD-Lite ("Net/2") de l'Université de Californie à Berkeley, avec de nombreux composants venant aussi de 386BSD et de la "Free Software Foundation". Ce fut un succès honnête pour une version initiale, qui fut suivi par le franc succès de la version 1.1 de FreeBSD, publiée en Mai 1994.

A peu près à cette époque, des nuages menaçants et inattendus apparurent lorsque commença la bataille juridique entre Novell et l'U.C. Berkeley autour du statut légal de la bande Net/2 de Berkeley. Dans les termes de l'accord, l'U.C. Berkeley concédait qu'une grande partie de Net/2 était du code "protégé" et propriété de Novell, qui l'avait à son tour racheté à AT&T quelque temps auparavant. Berkeley obtint en retour la "bénédiction" de Novell que 4.4BSD-Lite soit, lorsqu'il vit finalement le jour, déclaré non protégé et que tous les utilisateurs de Net/2 soit fortement incités à migrer. Cela incluait FreeBSD, et l'on donna au projet jusqu'à Juillet 1994 pour mettre un terme à son propre produit basé sur Net/2. Selon les termes de cet accord, une dernière livraison était autorisée avant le délai final; ce fut FreeBSD 1.1.5.1.

FreeBSD s'attela alors à la tâche difficile de littéralement se réinventer à partir de fragments totalement nouveaux et assez incomplets de 4.4BSD-Lite. Les versions "Lite" étaient légères ("light") en partie parce que le CSRG avait retiré de gros morceaux du code nécessaires pour que l'on puisse effectivement en faire un système qui démarre (pour différentes raisons légales) et parce que le portage pour Intel de la version 4.4 était très partiel. Il fallu au projet jusqu'à Novembre 1994 pour terminer cette étape de transition et que FreeBSD 2.0 paraisse sur l'Internet et sur CDROM (fin Décembre). Bien qu'elle fut encore assez rugueuse aux angles, cette livraison obtint un succès significatif et fut suivie par la version 2.0.5 de FreeBSD, plus fiable et facile à installer, en Juin 1995.

Nous avons publié FreeBSD 2.1.5 en Août 1996, et il s'avéra suffisamment populaire chez les fournisseurs d'accès et les utilisateurs professionnels pour qu'une nouvelle version sur la branche 2.1-STABLE soit justifiée. Ce fut la version FreeBSD 2.1.7.1, parue en Février 1997 et qui marque la fin de 2.1-STABLE comme branche principale de développement. Dès lors, il n'y aurait plus que des améliorations quant à la sécurité et autres corrections de bogues critiques sur cette branche, (RELENG_2_1_0), passée en phase de maintenance.

La branche FreeBSD 2.2 fut créée à partir de la branche principale de développement ("-CURRENT") en Novembre 1996 en tant que branche RELENG_2_2, et la première version complète (2.2.1) parut en Avril 1997. Il y eut d'autres versions sur la branche 2.2 à l'été et à l'automne 97, la dernière (2.2.8) parut en Novembre 1998. La première version officielle 3.0 sortira en Octobre 1998 et annoncera le début de la fin pour la branche 2.2.

Il y eut la création de nouvelles branches le 20 Janvier 1999, donnant une branche 4.0-CURRENT et

une branche 3.X-STABLE. De cette dernière il y eut la version 3.1 livrée le 15 Février 1999, la version 3.2 livrée le 15 Mai 1999, la 3.3 le 16 Septembre 1999, la 3.4 le 20 Décembre 1999 et la 3.5 le 24 Juin 2000, qui fut suivit quelques jours plus tard par une mise à jour mineure 3.5.1 pour rajouter quelques correctifs de sécurité de dernière minute sur Kerberos. Cela sera la dernière version de la la branche 3.X à paraître.

Le 13 Mars 2000 a vu l'apparition d'une nouvelle branche: la branche 4.X-STABLE. Il y a eu plusieurs versions jusqu'ici: la 4.0-RELEASE est sortie en Mars 2000, et la dernière version, la 4.11-RELEASE est sortie en Janvier 2005.

La tant attendue 5.0-RELEASE a été annoncée le 19 Janvier 2003. Etant le point culminant de près de trois ans de travail, cette version a engagé FreeBSD sur la voie d'un support avancé des systèmes multiprocesseurs et des "threads", et a introduit le support des plateformes UltraSPARC® et `ia64`. Cette version fut suivie de la 5.1 en Juin 2003. La dernier version 5.X issue de la branche -CURRENT fut la 5.2.1-RELEASE présentée en Février 2004.

La branche RELENG_5 créée en Août 2004, suivie par la 5.3-RELEASE, marque le début de la branche 5-STABLE. La version la plus récente, la 11.2-RELEASE, est sortie en June 28, 2018. Il n'est pas prévu de publier d'autres versions de la branche RELENG_5.

La branche RELENG_6 a été créée en Juillet 2005. La version 6.0-RELEASE, la première version issue de la branche 6.X a été rendue publique en Novembre 2005. La version la plus récente, la 12.0-RELEASE, est sortie en December 11, 2018. De nouvelles versions sont prévues pour la branche RELENG_6.

Pour le moment, les projets de développement à long terme continuent à se faire dans la branche (tronc) 7.X-CURRENT, et des "instantanées" de la 7.X sur CDROM (et, bien sûr, sur le net) sont continuellement mises à disposition sur le serveur d'instantané pendant l'avancement des travaux.

1.3.2. Les objectifs du projet FreeBSD

L'objectif du projet FreeBSD est de fournir du logiciel qui puisse être utilisé à n'importe quelle fin et sans aucune restriction. Nombre d'entre nous sont impliqués de façon significative dans le code (et dans le projet) et ne refuseraient certainement pas une petite compensation financière de temps à autre, mais ce n'est certainement pas dans nos intentions d'insister là dessus. Nous croyons que notre première et principale "mission" est de fournir du code à tout le monde, pour n'importe quel projet, de façon à ce qu'il soit utilisé le plus possible et avec le maximum d'avantages. C'est, nous le pensons, l'un des objectifs les plus fondamentaux du Logiciel Libre et l'un de ceux que nous soutenons avec enthousiasme.

Le code de l'arborescence des sources, qui est régi par la Licence Publique GNU ("GNU Public License" - GPL) ou la Licence Publique GNU pour les Bibliothèques ("GNU Library Public License" - GLPL) impose légèrement plus de contraintes, bien que plutôt liées à une disponibilité plus grande qu'au contraire, comme c'est généralement le cas. En raison des complications supplémentaires qui peuvent résulter de l'utilisation commerciale de logiciels GPL, nous essayons, cependant de remplacer ces derniers par des logiciels soumis à la licence BSD qui est plus souple, chaque fois que c'est possible.

1.3.3. Le mode de développement de FreeBSD

Le développement de FreeBSD est un processus très ouvert et très souple, c'est littéralement le résultat de contributions de centaines de personnes dans le monde entier, ce que reflète notre liste des participants. L'infrastructure de développement de FreeBSD permet à ces centaines de développeurs de collaborer via l'Internet. Nous sommes toujours à l'affût de nouveaux développeurs et de nouvelles idées, et ceux que s'impliquer de plus près intéresse n'ont besoin que de contacter la liste de diffusion pour les discussions techniques sur FreeBSD. La liste de diffusion pour les annonces relatives à FreeBSD est aussi disponible pour ceux qui veulent faire connaître aux autres utilisateurs de FreeBSD les principaux domaines de développement en cours.

Quelques points utiles à connaître à propos du projet FreeBSD et de son processus de développement, que vous travailliez indépendamment ou en collaboration étroite:

Les archives CVS

L'arborescence centrale des sources de FreeBSD est gérée sous CVS (Concurrent Version System), un système librement disponible de gestion de version des sources qui est livré avec FreeBSD. Les archives CVS principales sont sur une machine à Santa Clara CA, USA, d'où elles sont répliquées sur de nombreuses machines miroir à travers le monde. L'arborescence CVS qui contient les branches -CURRENT et -STABLE peut facilement être dupliquée sur votre propre machine. Reportez-vous à la section Synchroniser votre arborescence des sources pour plus d'informations sur la façon de procéder.

La liste des personnes autorisées, les "committers"

Les personnes autorisées (*committers*) sont celles qui ont les droits en *écriture* sur l'arborescence CVS, et sont autorisées à faire des modifications dans les sources de FreeBSD (le terme "committer" vient de la commande cvs(1) `commit`, que l'on utilise pour reporter des modifications dans les archives CVS). La meilleure façon de proposer des modifications pour qu'elles soient validées par les "committers" est d'utiliser la commande send-pr(1). S'il semble y avoir un problème dans ce système, vous pouvez aussi les joindre en envoyant un courrier électronique à liste de diffusion pour les committers de FreeBSD.

L'équipe de base de FreeBSD

L'équipe de base de FreeBSD serait l'équivalent du comité de direction si le Projet FreeBSD était une entreprise. La responsabilité principale de l'équipe de base est de s'assurer que le projet, dans son ensemble, fonctionne correctement et va dans la bonne direction. Proposer à des développeurs impliqués et responsables de rejoindre notre groupe de personnes autorisées est une des fonctions de l'équipe de base, ainsi que le recrutement de nouveaux membres de l'équipe de base quand d'autres s'en vont. L'actuelle équipe de base a été élu à partir d'un ensemble de "committers" candidats en Juillet 2006. Des élections ont lieu tous les 2 ans.

Certains membres de l'équipe de base ont aussi leur propre domaine de responsabilité, ce qui signifie qu'il leur est dévolu de veiller à ce qu'une partie significative du système satisfasse aux fonctionnalités annoncées. Pour une liste complète des développeurs FreeBSD et de leurs domaines de responsabilité, veuillez consulter la liste des participants au projet.

La plupart des membres de l'équipe de base sont volontaires en ce qui concerne le développement de FreeBSD et ne retirent aucun profit financier du projet,

> donc "implication" ne doit pas être compris "support garanti". La comparaison précédente avec un comité directeur n'est pas tout à fait exacte, et il serait plus juste de dire que ce sont des gens qui ont sacrifié leur vie à FreeBSD contre toute raison!

Contributions extérieures

Enfin, mais certainement pas des moindres, le groupe le plus important de développeurs est constitué par les utilisateurs eux-mêmes qui nous fournissent de façon quasi régulière leur retour d'expérience et leurs corrections de bogues. Le principal moyen d'entrer en contact avec le développement plus décentralisé de FreeBSD est de s'inscrire sur la liste de diffusion pour les discussions techniques sur FreeBSD où ces questions sont abordées. Voyez Ressources sur Internet pour plus d'informations concernant les diverses listes de discussion FreeBSD.

La liste de ceux qui ont contribué au projet est longue et en augmentation, pourquoi donc ne pas vous y joindre et contribuer à quelque chose en retour dès aujourd'hui?

Fournir du code n'est pas la seule manière de contribuer au projet; pour avoir une liste plus complète de ce qu'il y a à faire, voyez s'il vous plaît le site du projet FreeBSD.

En résumé, notre modèle de développement est organisé comme un ensemble relâché de cercles concentriques. Ce modèle centralisé est en place pour la commodité des *utilisateurs* de FreeBSD, qui disposent ainsi d'un moyen facile de suivre l'évolution d'une base de code centrale, et non pour tenir à l'écart d'éventuels participants! Nous souhaitons fournir un système d'exploitation stable avec un nombre conséquent de programmes d'application cohérents que les utilisateurs puissent facilement installer et employer - c'est un modèle qui fonctionne très bien pour cela.

Tout ce que nous attendons de ceux qui se joindraient à nous pour développer FreeBSD est un peu de la même implication que les développeurs actuels ont vis-à-vis de sa réussite continue!

1.3.4. A propos de cette version

FreeBSD est une version librement disponible et incluant tout le code source basé sur 4.4BSD-Lite2 pour les ordinateurs à architectures Intel i386™, i486™, Pentium®, Pentium® Pro, Celeron®, Pentium® II, Pentium® III, Pentium® 4 (ou compatible), Xeon™, DEC Alpha™ et systèmes basés sur UltraSPARC® de Sun. Il est basé essentiellement sur du logiciel du groupe CSRG de l'Université de Californie à Berkeley, avec des additions venant de NetBSD, OpenBSD, 386BSD, et de la "Free Software Foundation".

Depuis la publication de FreeBSD 2.0 fin 1994, les performances, fonctionnalités et la stabilité de FreeBSD ont été améliorées de façon spectaculaire. La plus grosse modification est un gestionnaire de mémoire virtuelle totalement revu qui comprend un cache commun au disque et à la mémoire virtuelle, qui n'améliore pas seulement les performances, mais diminue aussi l'occupation de la mémoire, de telle sorte qu'une configuration avec 5 MO devienne un minimum acceptable. D'autres ajouts concernent le support intégral des clients et serveurs NIS, le support des transactions TCP, les connexions PPP à la demande, le support intégré DHCP, un sous-système SCSI amélioré, support ISDN, support pour l'ATM, FDDI, les cartes "Fast et Gigabit Ethernet" (1000 Mbit), un meilleur support des derniers contrôleurs Adaptec et des milliers de corrections de bogues.

En plus du système lui-même, FreeBSD offre un nouveau catalogue de logiciels portés ("ports") qui

inclut des milliers de programmes habituellement demandés. A l'heure où sont écrites ces lignes il y avait plus de 36000 logiciels portés! La liste va des serveurs HTTP (WWW) aux jeux, langages, éditeurs et presque tout ce qui existe entre. Le catalogue complet des logiciels demande près de 3 GB d'espace disque, les portages se présentant sous forme de "delta" avec les sources d'origine. Cela rend leur mise à jour bien plus facile, et diminue de façon sensible l'espace nécessaire par rapport à l'ancien catalogue 1.0. Pour compiler un logiciel porté, il vous suffit d'aller dans le répertoire du programme que vous désirez installer, de taper `make install`, et de laisser le système faire le reste. La distribution originale complète de chaque logiciel est chargée dynamiquement depuis le CDROM ou un site FTP proche, il vous suffit de disposer de suffisamment d'espace disque pour compiler le logiciel que vous voulez. Presque tous les logiciels sont aussi fournis sous forme pré-compilée ("package"-paquetage) qui peut être installé avec une seule commande (`pkg_add`), si vous ne voulez pas les compiler à partir des sources. Plus d'information sur les paquetages et les logiciels portés peut être trouvée dans le Installer des applications. les logiciels pré-compilés et les logiciels portés..

Il y a un certain nombre d'autres documents qui vous serons peut-être très utiles à l'installation et à l'utilisation de FreeBSD, que vous pouvez maintenant trouver dans le répertoire /usr/shared/doc de n'importe quelle machine sous une version récente de FreeBSD. Vous pouvez consulter les manuels localement disponibles avec n'importe quel navigateur HTML aux URLs suivantes:

Le Manuel FreeBSD

/usr/shared/doc/handbook/index.html

La FAQ de FreeBSD

/usr/shared/doc/faq/index.html

Vous pouvez aussi consulter les exemplaires originaux (et les plus souvent mis à jour) sur http://www.FreeBSD.org.

Chapitre 2. Installing FreeBSD

2.1. Synopsis

En fonction de l'environnement utilisé, il existe plusieurs manières différentes pour obtenir un FreeBSD en mesure de fonctionner. Il existe des:

- Images de machines virtuelles, à télécharger et à importer dans l'environnement virtuel de votre choix. Elles peuvent être récupérées à partir de la page Download FreeBSD. Il existe des images pour KVM ("qcow2"), VMWare ("vmdk"), Hyper-V ("vhd"), ainsi que des images disque brutes ("raw") qui sont universellement supportées. Ce ne sont pas des images d'installation, mais plutôt des instances préconfigurées ("déjà installées"), prêtes à fonctionner et à effectuer les tâches de post-installation.
- Images de machines virtuelles disponibles sur les plateformes Amazon AWS Marketplace, Microsoft Azure Marketplace, et Google Cloud Platform, à exécuter sur leurs services d'hébergement respectifs. Pour plus d'information sur le déploiement de FreeBSD sur Azure, veuillez consulter le chapitre correspondant de la Documentayion Azure.
- Images disque de cartes SD, pour les systèmes embarqués comme le Raspberry Pi ou le BeagleBone Black. Elles peuvent être téléchargées à partir de la page Download FreeBSD. Ces fichiers doivent être décompressés et écrits sur une carte SD, comme un fichier d'image disque brut, à partir de laquelle la carte embarquée pourra démarrer.
- Images disque d'installation, pour installer FreeBSD sur un disque dur pour les ordinateurs de bureau, ordinateurs portables ou les systèmes serveurs.

Le reste de ce chapitre décrit les quatre cas, en expliquant comment installer FreeBSD en utilisant un programme d'installation en mode texte appelé bsdinstall.

Par défaut, les instructions d'installation de ce chapitre sont écrites pour les architectures i386™ et AMD64. Où elles seront applicables, des instructions spécifiques à d'autres architectures seront indiquées. Il peut y avoir des différences mineures entre le programme d'installation et ce qui est montré ici, aussi il faut utiliser ce chapitre comme un guide général plutôt qu'une suite d'instructions à suivre à la ligne près.

Les utilisateurs préférant installer FreeBSD à l'aide d'un programme d'installation graphique peuvent être intéressés par GhostBSD, MidnightBSD ou NomadBSD.

Après la lecture de ce chapitre, vous connaîtrez:

- La configuration matérielle minimale nécessaire et les architectures matérielles supportées par FreeBSD.
- Comment créer le support d'installation de FreeBSD.
- Comment lancer bsdinstall.
- Les questions que bsdinstall posera, ce qu'elles signifient, et comment y répondre.
- Comment dépanner une installation qui a échoué.

- Comment accéder à la version "live" de FreeBSD avant d'effectuer une installation.

Avant de lire ce chapitre, vous devrez:

- Lire la liste du matériel supporté fournie avec la version de FreeBSD qui va être installée, et vérifier que le matériel du système est supporté.

2.2. Configuration matérielle minimale

La configuration minimale pour installer FreeBSD varie avec l'architecture matérielle concernée. Les architectures matérielles et les périphériques supportés par une version de FreeBSD sont listés sur la page d'Information sur les versions de FreeBSD. La page de Téléchargement de FreeBSD donne également des recommandations pour le choix de l'image correcte pour les différentes architectures/

Une installation de FreeBSD nécessite un minimum de 96 Mo de RAM et 1.5 Go d'espace libre sur le disque dur. Néanmoins, des quantités aussi faibles de mémoire et d'espace disque ne sont réellement utilisables que pour des applications particulières comme les applications embarquées. Un ordinateur d'usage général aura besoin de plus de ressources. 2-4 Go de RAM et au moins 8 Go d'espace disque sont un bon point de départ.

Voici les contraintes sur les processeurs pour chaque architecture:

amd64

C'est le type de processeur pour ordinateur de bureau et portable le plus courant, utilisé dans les systèmes modernes. Intel® l'appelle Intel64. D'autres fabricants l'appelle parfois x86-64.

Des exemples de processeurs compatibles amd64 comprennent: les AMD Athlon™64, AMD Opteron™, Intel® Xeon™ multi-coeurs, Intel® Core™ 2 et processeurs suivants.

i386

Les ordinateurs de bureau et portables plus anciens utilisent souvent cette architecture x86 32bits.

Presque tous les processeurs compatibles i386 avec une unité de calcul en virgule flottante sont supportés. Tous les processeurs Intel® 486 ou supérieurs sont supportés. Néanmoins, les binaires publiés par le projet sont compilés pour le processeur 686, une version spécifiquement compilée sera nécessaire pour les systèmes 486 et 586.

FreeBSD utilisera le support de l'extension d'adresse physique ("Physical Address Extensions" ou PAE) sur les CPUs avec cette fonctionnalité. Un noyau avec la fonctionnalité PAE activée détectera la mémoire au-dessus de 4 Go et permettra son utilisation par le système. Néanmoins, utiliser PAE ajoutera des contraintes aux pilotes de périphériques et à d'autres fonctionnalités de FreeBSD.

arm64

La plupart des cartes embarquées sont des systèmes à base d'ARM 64bits. De nombreux serveurs arm64 sont supportés.

arm

Les anciennes cartes armv7 sont supportées.

powerpc

Tous les systèmes Apple® Mac® utilisant une ROM"New World" avec l'USB intégré sont supportés. Le fonctionnement SMP (multi-processeurs) est supporté sur les machines dotées de plusieurs CPUs.

Un noyau 32bits ne peut utiliser que les 2 premiers Go de RAM.

2.3. Tâches de pré-installation

Une fois déterminé que le système répond bien aux exigences minimales en termes de matériel pour installer FreeBSD, le fichier d'installation devrait être téléchargé et le support d'installation préparé. Avant de faire cela, vérifier que le système est prêt pour une installation en vérifiant les différents éléments de la liste de contrôle suivante:

1. Sauvegarder les données importantes

   Avant d'installer tout système d'exploitation, il faut *toujours* en premier sauvegarder toutes les données importantes. Ne pas stocker la sauvegarde sur le système sur lequel aura lieu l'installation. A la place, sauvegarder les données sur un disque amovible comme un disque USB, sur un autre système sur le réseau, ou sur un système de sauvegarde en ligne. Tester la sauvegarde avant de lancer l'installation afin de s'assurer qu'elle contient tous les fichiers nécessaires. Quand le programme d'installation formate le disque du système, toutes les données stockées sur ce disque seront perdues.

2. Où installer FreeBSD?

   Si FreeBSD sera le seul système d'exploitation installé, cette étape peut être passée. Mais si FreeBSD partagera le disque avec un autre système d'exploitation, choisir quel disque ou partition sera utilisée pour FreeBSD.

   Dans les architectures i386 et amd64, les disques durs peuvent être divisés en plusieurs partitions en utilisant une des deux méthodes de partitionnement. Le *Master Boot Record* (MBR) traditionnel contient une table de partitions définissant jusqu'à quatre *partitions primaires*. Pour des raisons historiques, FreeBSD appelle ces partitions primaires *slices* (*tranches*). Une de ces partitions primaire peut devenir une *partition étendue* contenant plusieurs *partitions logiques*. La *table de partitionnement GUID* (*GUID Partition Table* ou GPT) est une méthode nouvelle et plus simple pour partitionner un disque. Les implémentations classiques de GPT autorisent jusqu'à 128 partitions par disque, supprimant ainsi le recours à des partitions logiques.

   Le chargeur d'amorçage de FreeBSD a besoin soit d'une partition primaire soit d'une partition GPT. Si toutes les partitions primaires ou GPT sont déjà utilisées, l'une d'entre elles devra être libérée pour FreeBSD. Pour créer une partition sans effacer les données existantes, utiliser un outil de redimensionnement de partition pour réduire une partition existante et créer une nouvelle partition en utilisant l'espace libéré.

De nombreux outils de partionnement gratuits et commerciaux sont listés sur http://en.wikipedia.org/wiki/List_of_disk_partitioning_software. GParted Live (http://gparted.sourceforge.net/livecd.php) est un CD Live gratuit qui comprend l'éditeur de partition GParted. GParted est également disponible sur d'autres CDs Live Linux.

Utilisés correctement, les outils de redimensionnement des disques peuvent créer, sans risque, l'espace nécessaire pour la création d'une nouvelle partition. Etant donnée que la possibilité de sélectionner la mauvaise partition existe, effectuer toujours une sauvegarde des données importantes et vérifier son intégrité avant de modifier les partitions du disque.

Disposer de différentes partitions contenant chacune un système d'exploitation différent rend possible l'installation de plusieurs systèmes d'exploitation sur un ordinateur. Une autre méthode est d'utiliser la virtualisation (Virtualisation) qui permet l'exécution simultanée de plusieurs systèmes d'exploitation sans avoir à modifier les partitions du disque dur.

3. Récupérer les informations relatives au réseau

   Certaines méthodes d'installation de FreeBSD requièrent une connexion réseau pour télécharger les fichiers d'installation. Après toute installation, le programme d'installation proposera de configurer les interfaces réseau du système.

   Si le réseau dispose d'un serveur DHCP, il peut être utilisé pour fournir une configuration réseau automatique. Si la configuration par DHCP n'est pas possible, les informations réseau suivantes pour le système doivent être obtenues auprès de l'administrateur réseau ou du fournisseur d'accès:

   a. Adresse IP
   b. Masque de sous-réseau
   c. Adresse IP de la passerelle par défaut
   d. Nom de domaine du réseau
   e. Adresse(s) IP du serveur DNS du réseau

4. Vérifier l'Errata FreeBSD

   Bien que le projet FreeBSD s'efforce de s'assurer que chaque version de FreeBSD soit aussi stable que possible, des bogues peuvent parfois exister. Il est très rare que ces bogues affectent le processus d'installation. Dès que ces problèmes sont découverts et corrigés, ils sont notés dans l'Errata de FreeBSD (https://www.freebsd.org/releases/12.1r/errata/) présent sur le site Web de FreeBSD. Vérifier l'errata avant l'installation afin d'être sûr qu'il n'y a pas de problème pouvant affecter l'installation.

   Les informations sur chaque version, y compris les errata, peuvent être trouvés sur le site web de FreeBSD dans la section d'information sur les différentes versions (https://www.freebsd.org/releases/).

2.3.1. Préparer le support d'installation

Le programme d'installation FreeBSD n'est pas une application qui peut être exécutée à partir d'un autre système d'exploitation. Au lieu de cela, télécharger un fichier d'installation de FreeBSD, copiez-le sur le support correspondant à sa taille (CD, DVD, ou clé USB) et démarrer le système pour installer à partir du support inséré ou branché sur l'ordinateur.

Les fichiers d'installation de FreeBSD sont disponibles sur www.freebsd.org/where/#download. Chaque nom de fichier d'installation contient le numéro de la version de FreeBSD, l'architecture et le type de fichier. Par exemple pour installer FreeBSD 12.1 sur un système amd64 à partir d'un DVD, téléchargez FreeBSD-12.1-RELEASE-amd64-dvd1.iso, gravez ce fichier sur un DVD, et démarrer le système avec le DVD inséré.

Les fichiers d'installation sont disponibles dans différents formats. Les formats varient en fonction de l'architecture matérielle et du type de support.

Des fichiers d'installation supplémentaires sont prévus pour les ordinateurs qui sont amorcés par UEFI (Unified Extensible Firmware Interface pour "Interface micrologicielle extensible unifiée"). Le nom de ces fichiers comprend la chaîne de caractères uefi.

Types de fichiers:

- `-bootonly.iso`: C'est le plus petit fichier d'installation car il ne contient que le programme d'installation. Une connexion à Internet fonctionnelle est requise lors de l'installation puisque le programme d'installation téléchargera les fichiers nécessaires pour effectuer l'installation de FreeBSD. Ce fichier doit être gravé sur un CD en utilisant une application de gravure de CDs.
- `-disc1.iso`: Ce fichier contient tous les fichiers nécessaires pour installer FreeBSD, ses sources, et le catalogue des logiciels portés. Il doit être gravé sur un CD en utilisant une application de gravure de CDs.
- `-dvd1.iso`: Ce fichier contient tous les fichiers nécessaires pour installer FreeBSD, ses sources, et le catalogue des logiciels portés. Il contient également un ensemble de paquetages binaires populaires pour installer un gestionnaire de fenêtres et des applications de manière à ce qu'un système complet puisse être installé sans nécessiter une connexion à Internet. Ce fichier être gravé sur un DVD en utilisant une application de gravure de DVDs.
- `-memstick.img`: Ce fichier contient tous les fichiers nécessaires pour installer FreeBSD, ses sources, et le catalogue des logiciels portés. Il doit être copié sur une clé USB en suivant les instructions données plus bas.
- `-mini-memstick.img`: Comme `-bootonly.iso`, ne contient pas les fichiers d'installation, mais les téléchargera au fur et à mesure des besoins. Une connexion à Internet fonctionnelle est requise lors de l'installation. Copier ce fichier sur une clé USB comme décrit dans Ecrire un fichier image sur un disque USB.

Après avoir téléchargé le fichier image du support d'installation, téléchargez également le fichier CHECKSUM.SHA256 à partir du même répertoire. Calculez une *somme de contrôle* ou *checksum* du fichier image. FreeBSD fournit sha256(1) à cet effet, à utiliser comme `sha256 fichierimage`. Les autres systèmes d'exploitation proposent des outils similaires.

Comparez la somme de contrôle calculée avec celle donnée dans le fichier CHECKSUM.SHA256. Les

sommes de contrôle doivent être identiques. Si une des sommes ne correspond pas, le fichier est corrompu et devra être téléchargé à nouveau.

2.3.1.1. Ecrire un fichier image sur un disque USB

Le fichier *.img est une *image* de l'intégralité du contenu d'une clé USB. Il *ne peut pas* être copié directement vers le périphérique de destination comme un simple fichier. Plusieurs applications existent pour écrire le fichier *.img sur une clé USB. Cette section décrit deux de ces utilitaires.

Avant de continuer, sauvegardez toutes les données importantes présentes sur la clé USB. Cette procédure effacera toutes les données sur la clé.

Procedure: Utiliser `dd` pour écrire une image

Cet exemple prend /dev/da0 comme périphérique cible sur lequel l'image sera écrite. Vérifiez que le périphérique utilisé comme cible est bien le bon, car cette commande détruira les données existantes.

1. L'utilitaire en ligne de commande dd(1) est disponible sur les systèmes BSD, Linux®, et Mac OS®. Pour écrire une image en utilisant `dd`, brancher la clé USB et déterminez son nom de périphérique. Indiquer, alors, le nom du fichier d'installation téléchargé et le nom du périphérique pour la clé USB. Cet exemple écrit le fichier image d'installation amd64 sur le premier périphérique USB sur un système FreeBSD existant.

   ```
   # dd if=FreeBSD-12.1-RELEASE-amd64-memstick.img of=/dev/da0 bs=1M conv=sync
   ```

   Si cette commande échoue, vérifier que la clé USB n'est pas montée et que le nom de périphérique est bien celui d'un disque et non d'une partition. Certains systèmes d'exploitation pourront nécessiter l'exécution de cette commande avec sudo(8). La syntaxe dd(1) varie légèrement en fonction des plate-formes; par exemple, Mac OS® a besoin d'un `bs=1m` en minuscules. Des systèmes comme Linux® pourront mettre en tampon les écritures. Pour forcer toutes les écritures en attente à s'effectuer, utiliser sync(8).

Procedure: Utiliser Windows® pour écrire l'image

Assurez-vous de préciser le bon disque comme cible, car les données existantes sur ce disque seront écrasées et détruites.

1. Récupérer Image Writer for Windows®

   Image Writer for Windows® est une application gratuite pour écrire une image sur une clé USB. Téléchargez-la depuis https://sourceforge.net/projects/win32diskimager/ et décompressez-la dans un répertoire.

2. Ecrire l'image avec Image Writer

Double-cliquez sur l'icone Win32DiskImager pour lancer le programme. Vérifiez que le lecteur affiché sous `Device` est celui de la clé USB. Cliquer sur l'icone répertoire et sélectionner l'image à écrire sur la clé. Cliquer sur **[Save]** pour accepter le nom du fichier image. Vérifiez que tout est correct, et qu'il n'y a pas de répertoires présents sur la clé USB ouverts dans d'autres fenêtres. Puis quand tout est prêt, cliquer sur **[Write]** pour écrire le fichier image sur la clé USB.

Vous êtes maintenant prêt à commencer l'installation de FreeBSD.

2.4. Lancer l'installation

Par défaut, le processus d'installation ne modifiera rien sur le(s) disque(s) dur(s) jusqu'au message suivant:

```
Your changes will now be written to disk. If you
have chosen to overwrite existing data, it will
be PERMANENTLY ERASED. Are you sure you want to
commit your changes?
```

L'installation peut être quittée à tout moment avant cet avertissement. Si quelque chose a mal été configurée, arrêtez juste l'ordinateur avant ce point, et aucun changement ne sera effectué sur le disque dur.

Cette section décrit comment démarrer le système à partir du support d'installation qui a été préparé à l'aide des instructions de Préparer le support d'installation. Pour démarrer avec une clé USB démarrable, brancher la clé USB avant d'allumer l'ordinateur. Pour démarrer avec un CD ou un DVD, allumer l'ordinateur et insérer le disque à la première occasion. Comment configurer le système pour démarrer à partir du support utilisé dépend de l'architure matérielle.

2.4.1. Démarrage pour les architectures i386™ et amd64

Ces architectures disposent d'un menu du BIOS pour sélectionner le périphérique de démarrage. En fonction du support de démarrage choisi, sélectionner le lecteur CD/DVD ou l'USB comme premier périphérique de démarrage. La plupart des systèmes proposent également la sélection du périphérique d'amorçage au démarrage à l'aide d'une touche sans avoir à entrer dans le BIOS. Généralement, la touche est soit `F10`, soit `F11`, soit `F12`, ou encore `Escape`.

Si l'ordinateur charge le système d'exploitation existant, alors soit:

1. Le support d'installation n'a pas été inséré suffisamment tôt lors du processus de démarrage. Laisser le support inséré, et essayer de redémarrer l'ordinateur.
2. Soit les modifications du BIOS étaient incorrectes ou non-sauvegardées. Vérifier à nouveau que le bon périphérique a été choisi comme premier périphérique de démarrage.
3. Ce système est trop ancien pour supporter l'amorçage à partir du support choisi. Dans ce cas, le gestionnaire de démarrage Plop (http://www.plop.at/en/bootmanager.html) peut être utilisé pour démarrer à partir du support sélectionné.

2.4.2. Démarrage pour l'architecture PowerPC®

Sur la plupart des machines, maintenir la touche `C` enfoncée lors du démarrage provoquera l'amorçage du CD. Sinon appuyez sur `Command` + `Option` + `O` + `F`, ou `Windows` + `Alt` + `O` + `F` dans le cas des claviers non-Apple®. A l'invite `0`, entrez:

```
boot cd:,\ppc\loader cd:0
```

2.4.3. Menu d'amorçage FreeBSD

Une fois le système démarré à partir du support d'installation, un menu similaire au suivant sera affiché:

Figure 1. Menu du chargeur FreeBSD

Par défaut, le menu attendra dix secondes une saisie de l'utilisateur avant de démarrer dans le programme d'installation de FreeBSD ou, si FreeBSD est déjà installé, avant de démarrer sous FreeBSD. Pour mettre en pause ce décompte afin d'examiner les options offertes, appuyer sur `Espace`. Pour sélectionner une option, appuyer sur le chiffre, le caractère ou la touche en surbrillance. Les options disponibles sont les suivantes.

- `Boot Multi User` (Démarrage en mode multi-utilisateur): Cette option provoquera la poursuite du processus de démarrage de FreeBSD. Si le décompte du démarrage a été mis en pause, appuyer sur `1`, `B` majuscule ou minuscule, ou encore `Entrée`.

- `Boot Single User` (Démarrage en mode mono-utilisateur): Ce mode peut être employé pour réparer une installation de FreeBSD existante comme décrit dans la Mode mono-utilisateur. Appuyer sur `2` ou `B` majuscule ou minuscule pour entrer dans ce mode.
- `Escape to loader prompt` (Quitter vers l'interpréteur de commandes du chargeur): Cela démarrera le système dans l'interpréteur de commandes du chargeur qui offre un nombre limité de commandes bas-niveau. Cette invite de commandes est abordée dans la Etape trois. Appuyer sur `3` ou `Echap` pour démarrer dans ce mode.
- `Reboot`: Redémarre le système.
- `Kernel`: Charge un noyau différent.
- `Configure Boot Options`: Ouvre le menu montré et décrit sur la Menu des options du chargeur FreeBSD.

Figure 2. Menu des options du chargeur FreeBSD

Le menu des options du chargeur est divisé en deux parties. La première partie peut être utilisée pour soit retourner au menu de démarrage principal soit pour réinitialiser les options à leur valeur par défaut.

La partie suivante est utilisée pour positionner les options disponibles sur `On` ou `Off` en appuyant sur le chiffre ou le caractère en surbrillance pour chaque option. Le système démarre toujours en utilisant le paramétrage choisi pour ces options jusqu'à ce qu'il soit modifié. Plusieurs options peuvent être modifées en utilisant ce menu:

- `ACPI Support`: Si le système se fige au démarrage, essayer de positionner cette option à `Off`.
- `Safe Mode`: Si le système se fige toujours durant le démarrage même avec l'option `ACPI Support` à `Off`, essayer de positionner cette option à `On`.
- `Single User` (Mono-utilisateur): Positionner cette option sur `On` pour réparer une installation existante de FreeBSD comme décrit dans la Mode mono-utilisateur. Une fois le problème réglé, repositionner l'option à `Off`.
- `Verbose` (Verbeux): Positionner cette option sur `On` pour voir des messages plus détaillés lors du processus de démarrage. Cela peut être utile pour dépanner un matériel.

Après avoir effectué les sélections nécessaires, appuyer sur `1` ou `Retour arrière` pour retourner au menu de démarrage principal, puis appuyer sur `Entrée` pour démarrer sous FreeBSD. Une série de messages de démarrage apparaîtra au fur et à mesure que FreeBSD détectera le matériel et chargera le programme d'installation. Une fois le démarrage achevé, le menu d'accueil de la Menu d'accueil sera affiché.

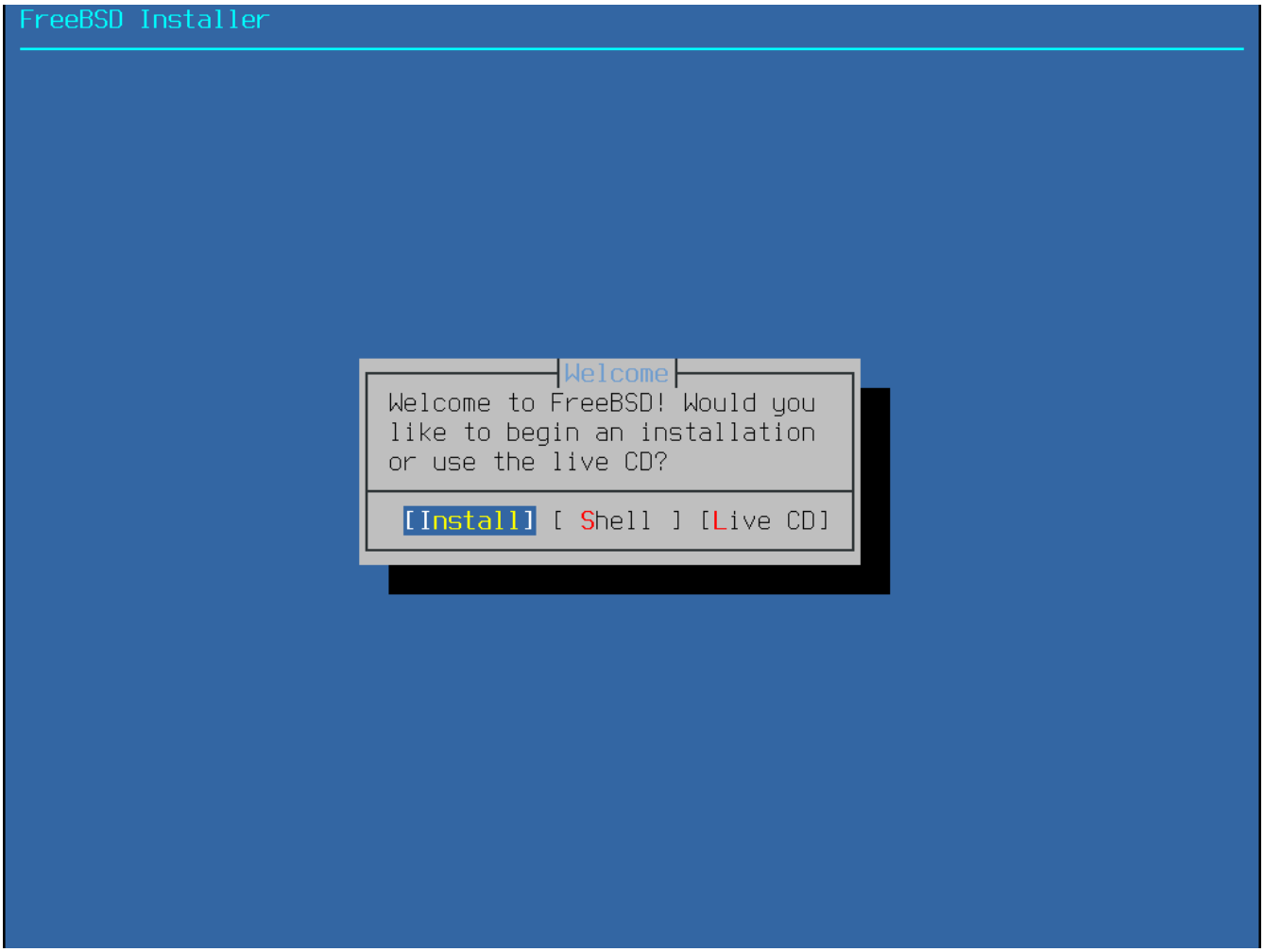


Figure 3. Menu d'accueil

Appuyer sur `Enter` pour sélectionner **[Install]** pour entrer dans le programme d'installation. Le reste de ce chapitre décrit comment utiliser ce programme d'installation. Sinon, utiliser la flèche droite ou gauche ou les lettres colorées pour sélectionner l'élément désiré. **[Shell]** peut être sélectionné pour accéder à un interpréteur de commandes FreeBSD afin d'utiliser des utilitaires en ligne de commande pour préparer les disques avant l'installation. L'option **[Live CD]** peut être employée pour tester FreeBSD avant de l'installer. Cette option est décrite dans la Utilisation du CD

Live.

Pour relire les messages de démarrage, dont la détection du matériel, appuyer sur la touche `S` majuscule ou minuscule, puis sur `Entrée` pour accéder à un interpréteur de commandes. A l'invite, taper `more /var/run/dmesg.boot` et utiliser la barre d'espace pour faire défiler les messages. Une fois terminé, taper `exit` pour revenir au menu d'accueil.

2.5. Utilisation de bsdinstall

Cette section présente dans l'ordre les menus de bsdinstall et le type d'information qui sera demandé avant l'installation du système. Utiliser les touches fléchées pour sélectionner un menu, et ensuite la touche `Espace` pour sélectionner ou déselectionner cet élément du menu. Une fois terminé, utiliser `Enter` pour sauvegarder la sélection et passer à l'écran suivant.

2.5.1. Sélectionner le menu des tables de clavier

Avant de démarrer le processus d'installation, bsdinstall chargera les fichiers de tables de clavier comme indiqué dans Chargement de la table de clavier.

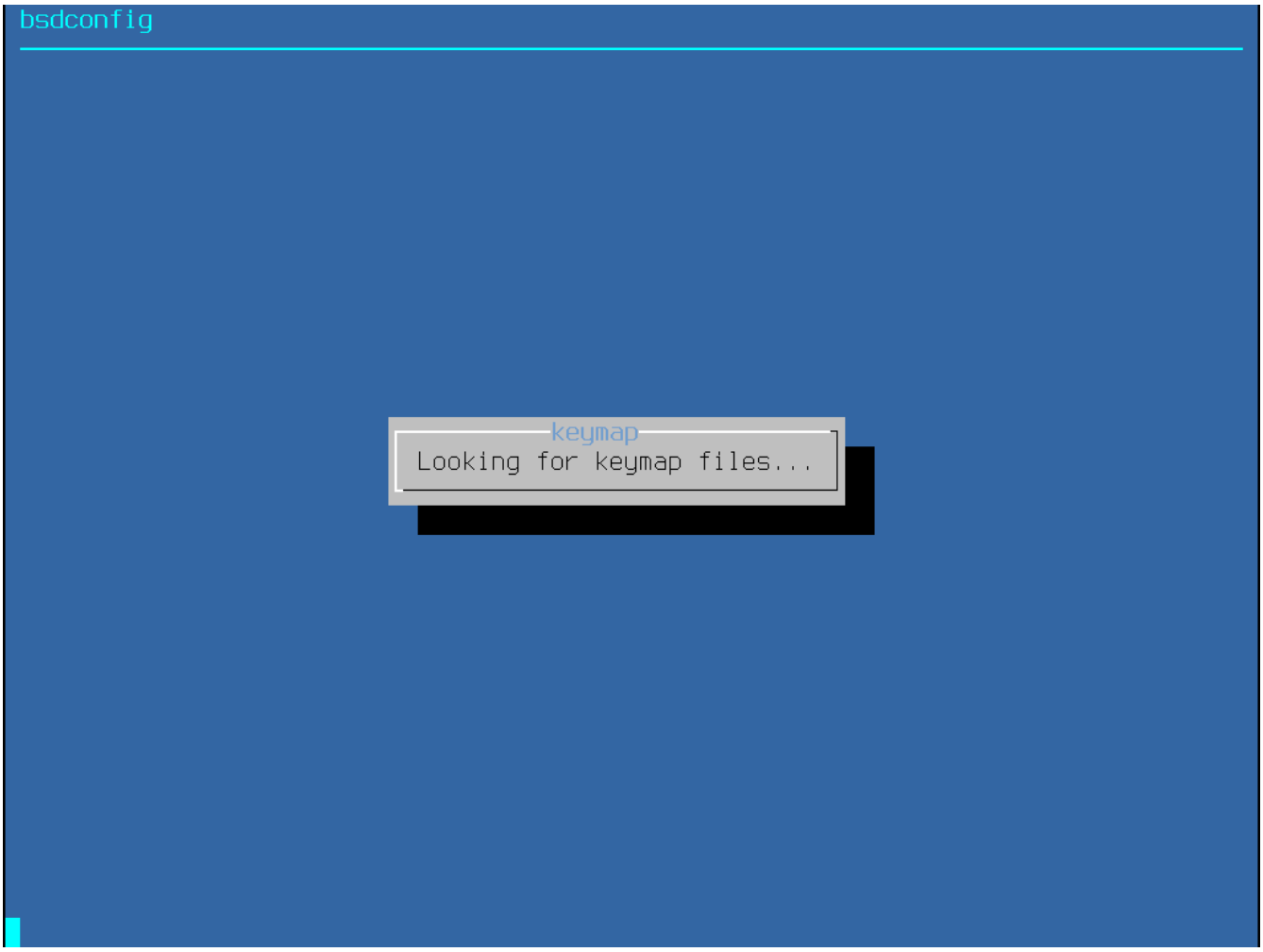


Figure 4. Chargement de la table de clavier

Après le chargement des tables de clavier, bsdinstall affiche le menu montré sur Menu de sélection de la table de clavier. Utilisez les flèches haut et bas pour choisir la table de clavier la plus proche

de celle du clavier relié au système. Appuyer sur `Enter` pour sauvegarder la sélection.

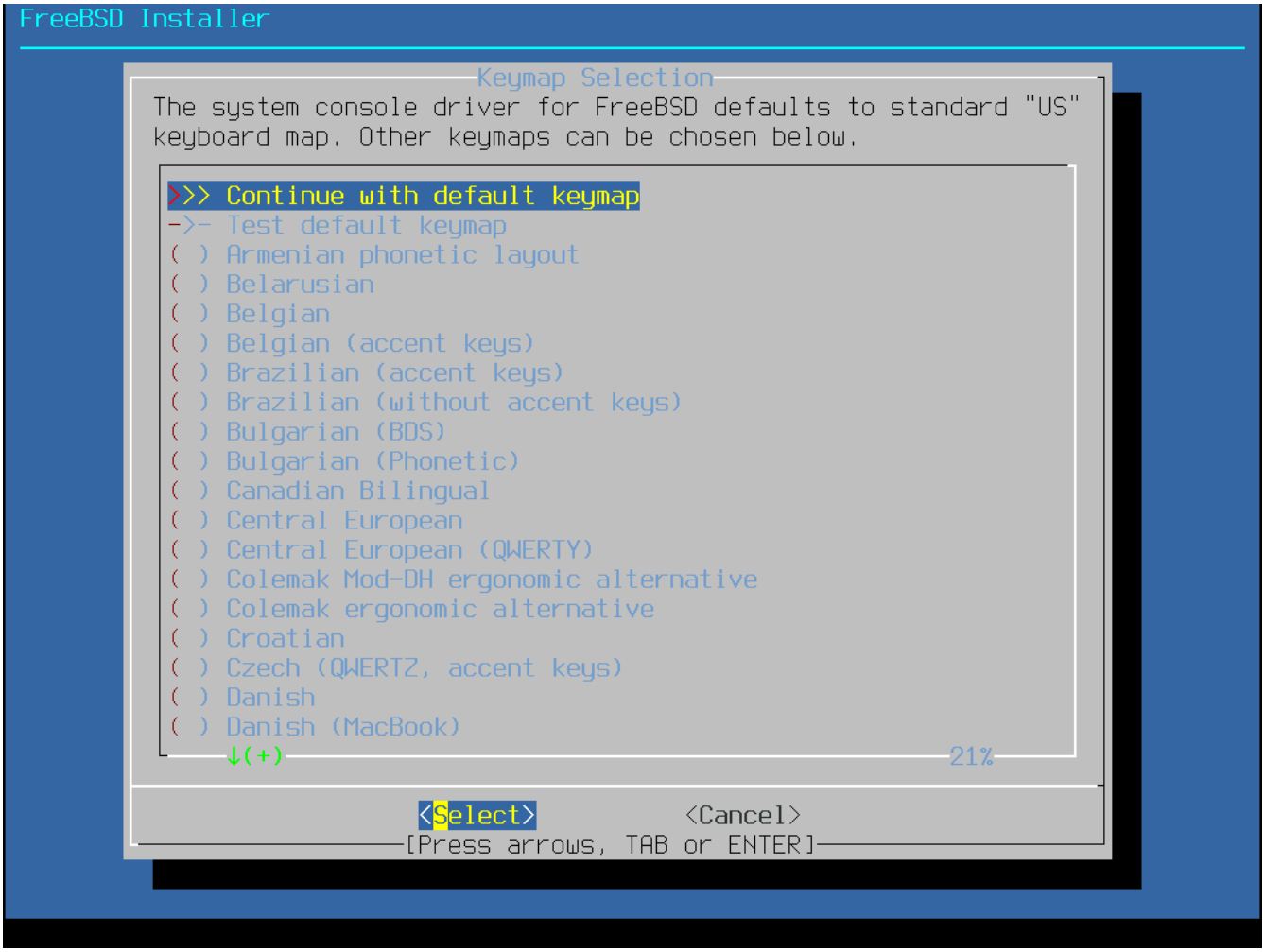


Figure 5. Menu de sélection de la table de clavier

Un appui sur `Echap` provoquera la sortie de ce menu et l'utilisation de la table par défaut. Si le choix ne semble pas évident, choisir United States of America ISO-8859-1 est conseillé.

De plus, lors de la sélection d'une table de clavier différente, l'utilisateur peut tester la table et s'assurer qu'elle est correcte avant de prendre en compte le changement comme montré sur Menu de test de la table de clavier.

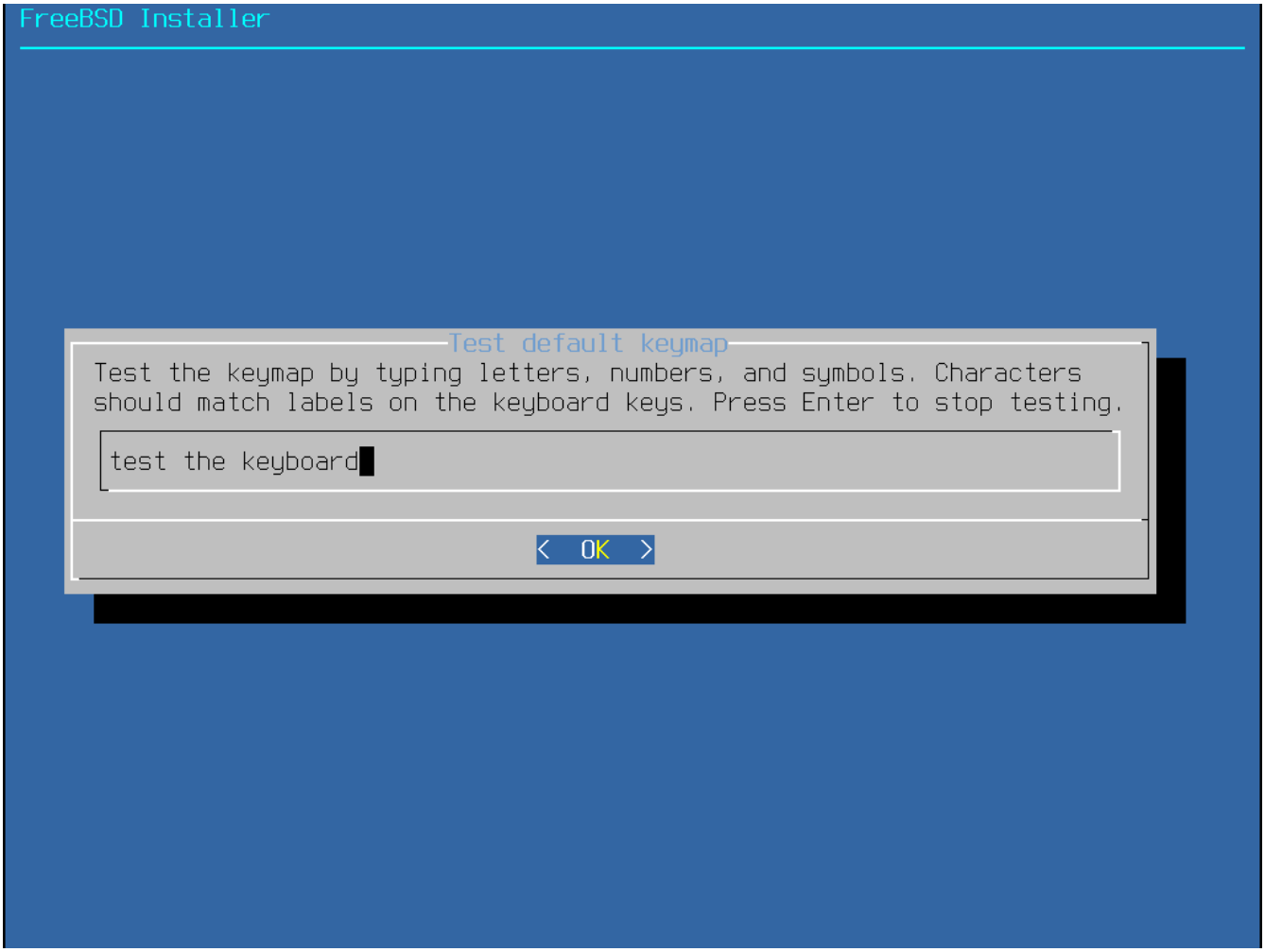


Figure 6. Menu de test de la table de clavier

2.5.2. Configurer le nom de la machine

Le menu bsdinstall suivant est utilisé pour configurer le nom de machine à donner au système nouvellement installé.

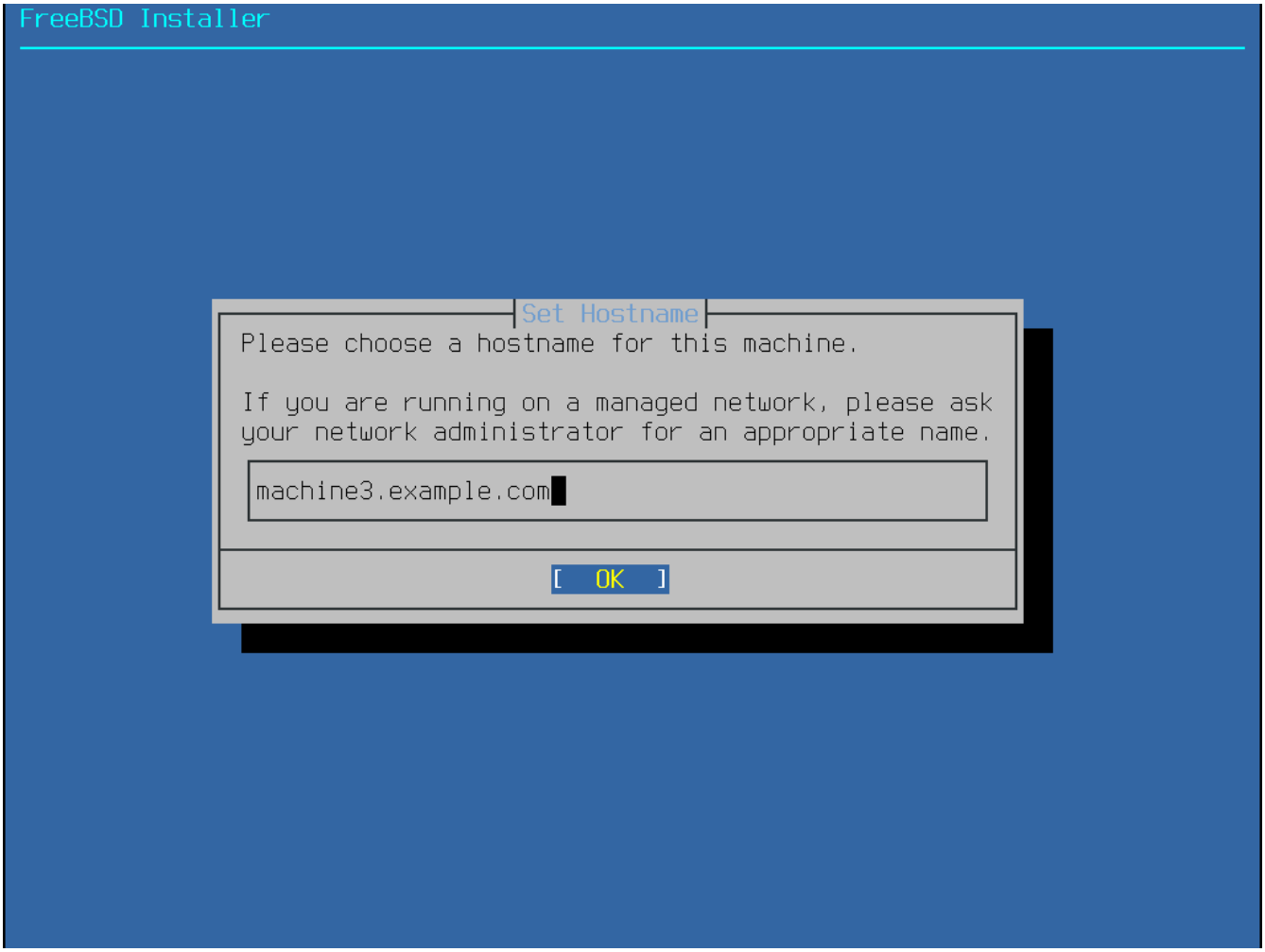


Figure 7. Configuration du nom de machine

Saisir un nom de machine qui est unique sur le réseau. Cela doit être un nom de machine complet comme `machine3.example.com`

2.5.3. Choisir les composants à installer

Ensuite, bsdinstall demandera de choisir les composants optionnels à installer.

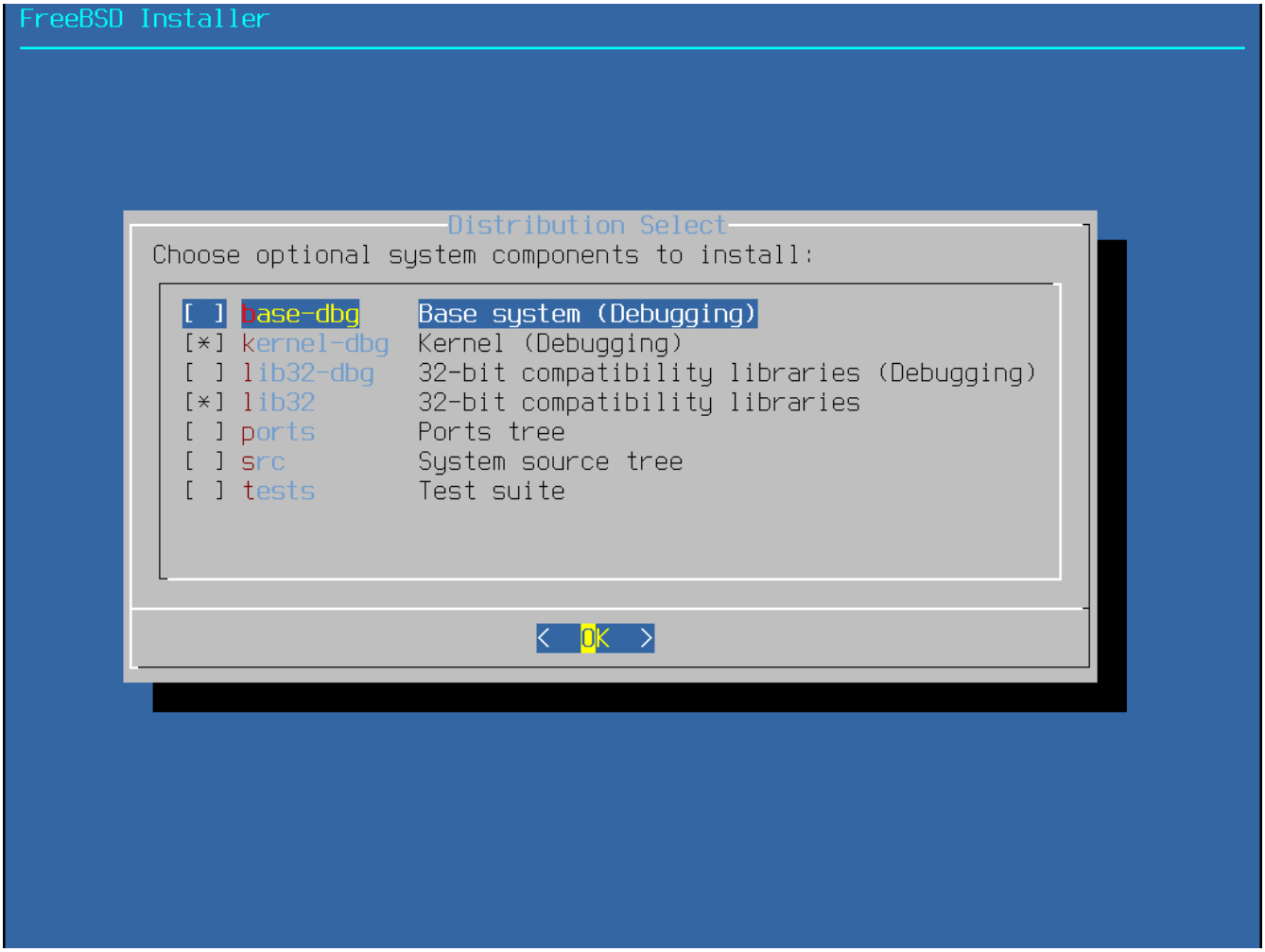


Figure 8. Sélection des composants à installer

Décider quels composants installer dépendra principalement de l'utilisation prévue du système et de l'espace disque disponible. Le noyau FreeBSD et les utilitaires de base, formant ensemble ce que l'on nomme le *système de base*, sont toujours installés. Selon l'architecture, certains de ces composants peuvent ne pas apparaître:

- `base-dbg` - Outils de base comme cat, ls parmi tant d'autres avec les symboles de débogage activés.
- `kernel-dbg` - Noyau et modules avec les symboles de débogage activés.
- `lib32-dbg` - Bibliothèques de compatibilité pour l'exécution d'applications 32bits sur une version 64bits de FreeBSD avec les symboles de débogage activés.
- `lib32` - Bibliothèques de compatibilité pour l'exécution d'applications 32bits sur une version 64bits de FreeBSD.
- `ports` - Le catalogue des logiciels portés pour FreeBSD.

  Le catalogue des logiciels portés est un ensemble de fichiers qui automatise le téléchargement, la compilation et l'installation de logiciels tierce-partie. Le Installer des applications. les logiciels pré-compilés et les logiciels portés discute de l'utilisation du catalogue des logiciels portés.

Le programme d'installation ne vérifie pas la présence de l'espace requis. Sélectionner cette option uniquement si l'espace disque suffisant est disponible. Le catalogue des logiciels portés occupe environ 3 GB d'espace

disque.

- `src` - Code source complet du noyau et du système de base. Bien que n'étant pas requis pour la majorité des applications, il peut être nécessaire pour compiler des pilotes de périphériques, des modules du noyau, ou des applications du catalogue des logiciels portés. Il est également utilisé pour le développement de FreeBSD. L'arborescence complète des sources demande 1 Go d'espace disque, et la recompilation du système FreeBSD complet nécessite 5 Go d'espace supplémentaire.
- `tests` - Suite d'outils de test pour FreeBSD.

2.5.4. Installation à partir du réseau

Le menu affiché dans Installation à partir du réseau n'apparaît que lors de l'installation à partir d'une image -bootonly.iso ou -mini-memstick.img étant donné que ces supports d'installation ne contiennent pas de copie des fichiers d'installation. Comme les fichiers d'installation doivent être récupérés par l'intermédiaire d'une connexion réseau, ce menu indique qu'une interface réseau doit être configurée en premier lieu. Si ce menu est affiché à un moment donné de l'installation, pensez à suivre les instructions données dans Configuration des interfaces réseau.

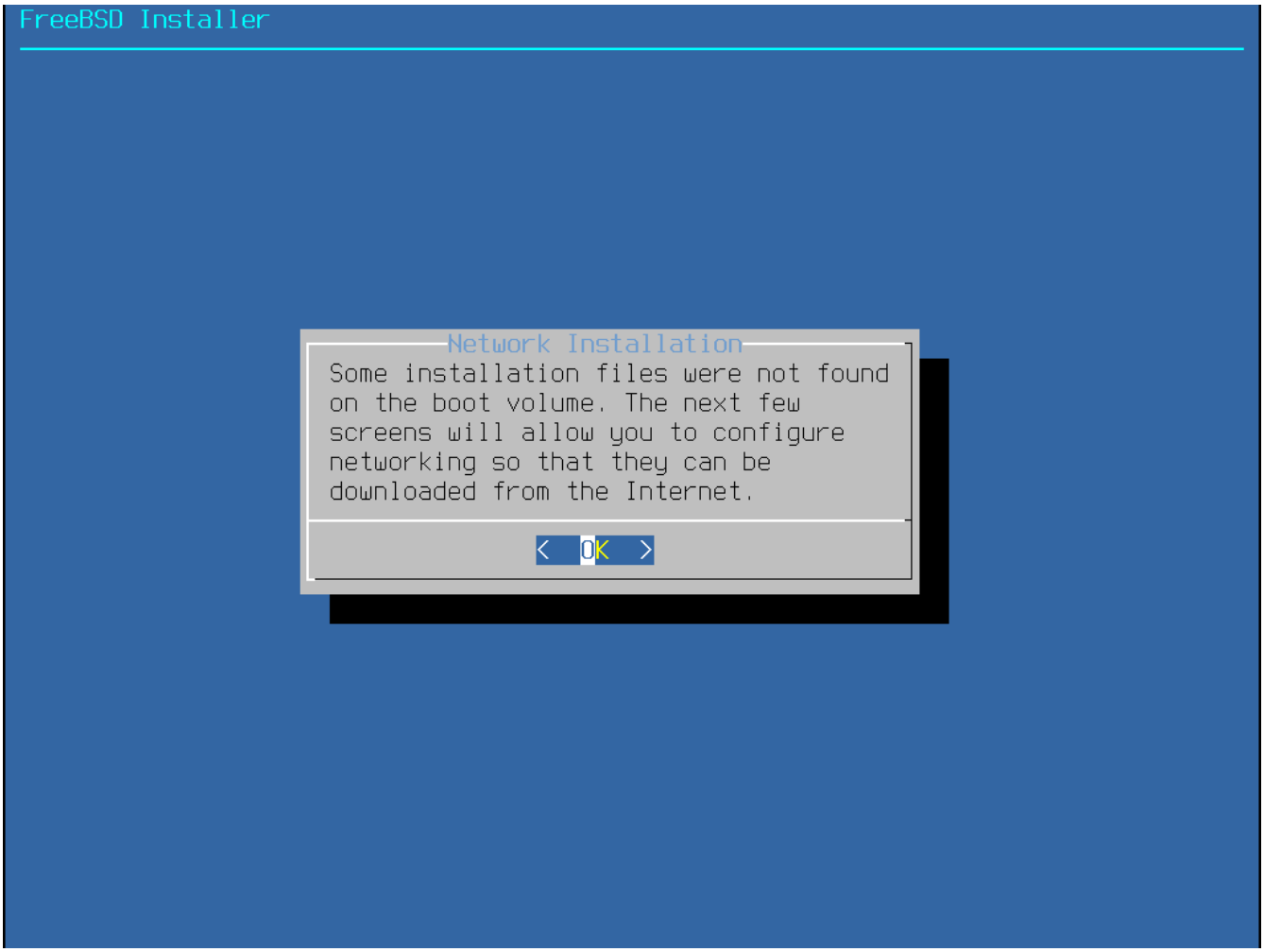


Figure 9. Installation à partir du réseau

2.6. Allouer l’espace disque

Le menu suivant est utilisé pour déterminer la méthode pour allouer l’espace disque.

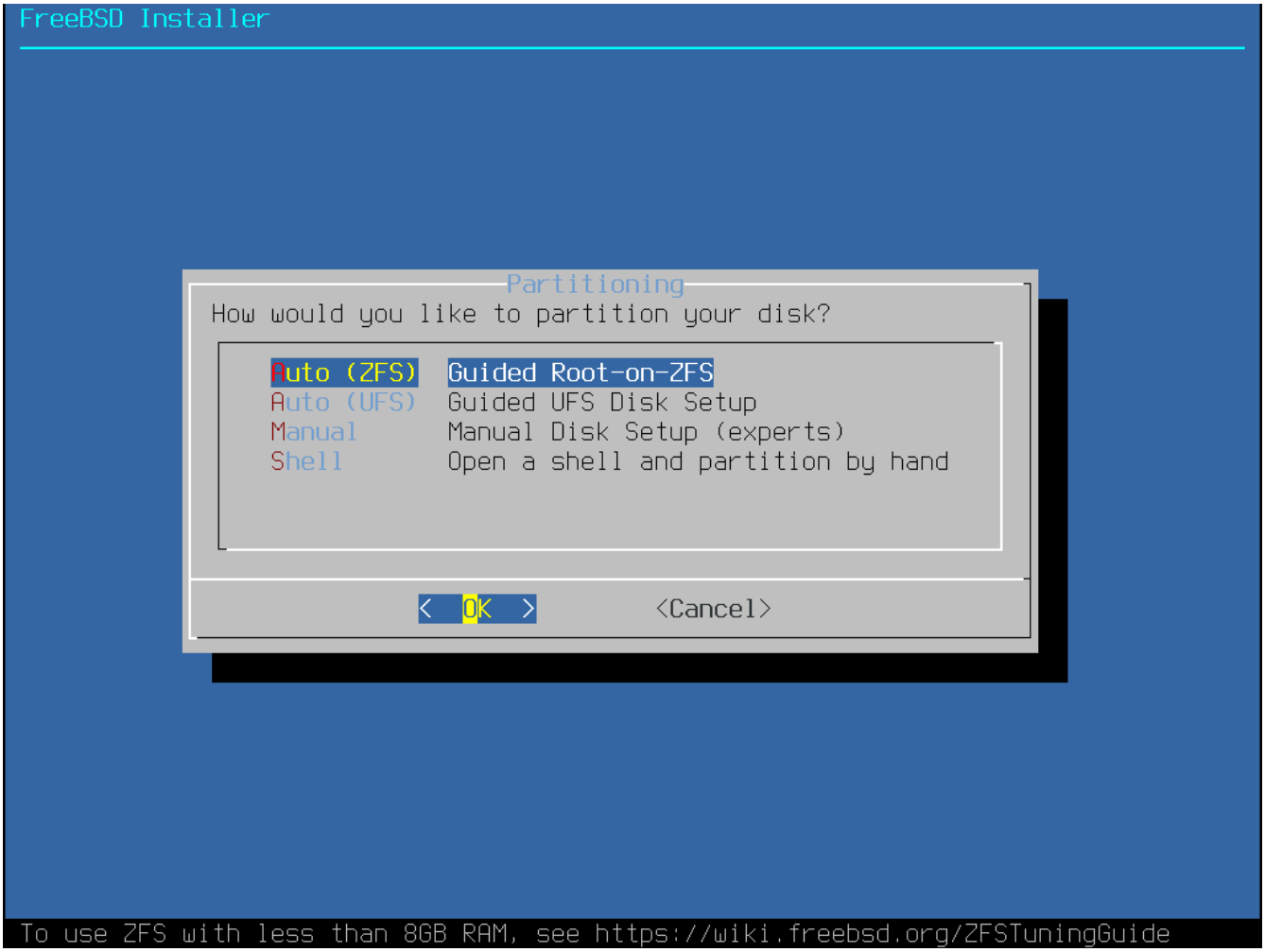


Figure 10. Choix du partitionnement

bsdinstall propose à l’utilisateur quatre méthodes pour allouer l’espace disque:

- le partitionnement `Auto (UFS)` fixe automatiquement les partitions disque et utilise le système de fichiers `UFS`.
- le partitionnement `Manual` ("Manuel") permet aux utilisateurs avancés de créer des partitions sur mesures à partir des options du menu.
- `Shell` ouvre une invite d’interpréteur de commandes dans laquelle les utilisateurs avancés peuvent créer des partitions sur mesures en utilisant des utilitaires en ligne de commande comme gpart(8), fdisk(8), et bsdlabel(8).
- le partitionnement `Auto (ZFS)` créé un système de fichiers racine sur ZFS avec le support optionnel du chiffrement GELI pour les *environnements de démarrage*.

Cette section décrit ce qui doit être pris en compte lors du partitionnement du disque. Elle montre ensuite comment utiliser les différentes méthodes de partionnement.

2.6.1. Choix du partitionnement

Lors du partitionnement, il faut garder à l'esprit que les disques durs transfèrent les données plus rapidement depuis les pistes extérieures que depuis les pistes intérieures. Aussi, les systèmes de fichiers plus petits et très sollicités devraient être positionnés vers l'extérieur du disque, alors que les partitions plus grandes comme /usr devraient être placées vers l'intérieur du disque. C'est une bonne idée de créer les partitions dans l'ordre suivant: /, espace de pagination, /var, et /usr.

La taille de la partition /var reflète l'utilisation prévue de la machine. Cette partition est utilisée pour contenir les boîtes aux lettres de messagerie, les fichiers journaux, et les queues d'impression. Les boîtes aux lettres et les fichiers journaux peuvent croître jusqu'à atteindre des tailles inattendues en fonction du nombre d'utilisateurs et combien de temps sont conservés les fichiers journaux. En moyenne, la plupart des utilisateurs n'auront rarement besoin de plus d'un gigaoctet d'espace disque pour /var.

Parfois, beaucoup d'espace disque est nécessaire pour /var/tmp. Quand de nouveaux logiciels sont installés, les outils de paquetage extraient une copie temporaire des paquetages dans /var/tmp. Les logiciels importants comme Firefox, ou LibreOffice peuvent être délicats à installer si l'espace disque dans /var/tmp n'est pas suffisant.

La partition /usr contient beaucoup de fichiers nécessaires au système, dont le catalogue des logiciels portés de FreeBSD et le code source du système. Au moins 2 gigaoctets d'espace sont recommandés pour cette partition.

Lors du choix de la taille des partitions, gardez à l'esprit les besoins en espace. Manquer d'espace sur une partition alors qu'une autre est à peine utilisée peut être très frustrant.

Par principe, votre espace de pagination devrait typiquement avoir une taille double de la quantité de mémoire physique (RAM). Les systèmes avec peu de mémoire RAM pourront avoir de meilleures performances avec beaucoup plus d'espace de pagination. Configurer trop peu d'espace de pagination peut conduire à une certaine inefficacité du code de pagination de la mémoire virtuelle (VM) et peut être à l'origine de problèmes ultérieurement si vous ajoutez plus de mémoire à votre système.

Sur des systèmes importants avec de multiples disques SCSI ou de multiples disques IDE fonctionnant sur différents contrôleurs, il est vivement recommandé que vous configuriez un espace de pagination sur chaque disque, jusqu'à quatre disques. Les partitions de pagination sur les différents disques devront avoir approximativement la même taille. Le noyau peut gérer des tailles arbitraires mais les structures de données internes sont dimensionnées pour 4 fois la taille de la plus grande partition de pagination. Garder la taille des partitions de pagination proche permettra au noyau de répartir de manière optimale l'espace de pagination entre les disques. Des espaces de pagination importants ne sont pas problématiques, même s'ils sont peu utilisés. Il peut être plus simple de récupérer la main face un programme incontrôlable avant d'être forcé à redémarrer la machine.

En partitionnant correctement votre système, la fragmentation introduite sur les partitions plus petites et plus chargées en écriture ne s'étendra pas sur les partitions principalement utilisées en lecture. De plus, avoir les partitions principalement utilisées en écriture proche du bord du disque

augmentera les performances d'E/S sur les partitions qui le demandent le plus. Bien qu'il soit nécessaire d'avoir de bonnes performances d'E/S sur les grandes partitions, les déplacer plus vers l'extérieur du disque ne donnera pas lieu à une augmentation significative des performances alors que le déplacement de performances alors que le déplacement de /var vers le bord peut avoir un sérieux impact.

2.6.2. Partitionnement guidé avec utilisation d'UFS

Quand cette méthode est sélectionnée, un menu affichera le(s) disque(s) disponible(s). Si plusieurs disques sont connectés, choisissez celui sur lequel FreeBSD doit être installé.

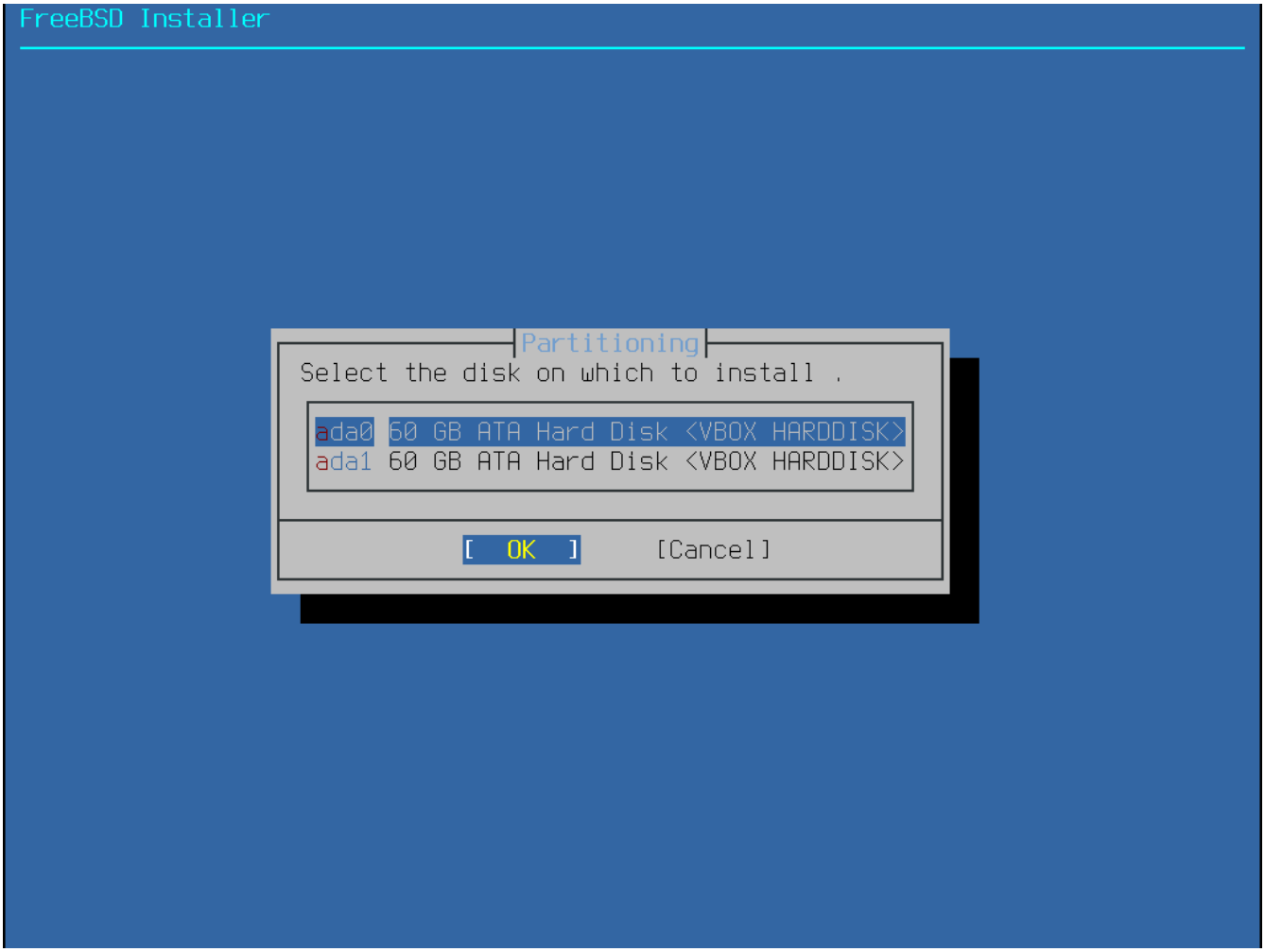


Figure 11. Sélection parmi plusieurs disques

Une fois le disque sélectionné, le menu suivant demande si l'installation se fait soit sur l'intégralité du disque soit sur une partition à créer à partir de l'espace libre. Si **[Entire Disk]** est sélectionné, une partition recouvrant la totalité du disque est automatiquement créée. Sélectionner **[Partition]** créé une partition dans l'espace inutilisé du disque.

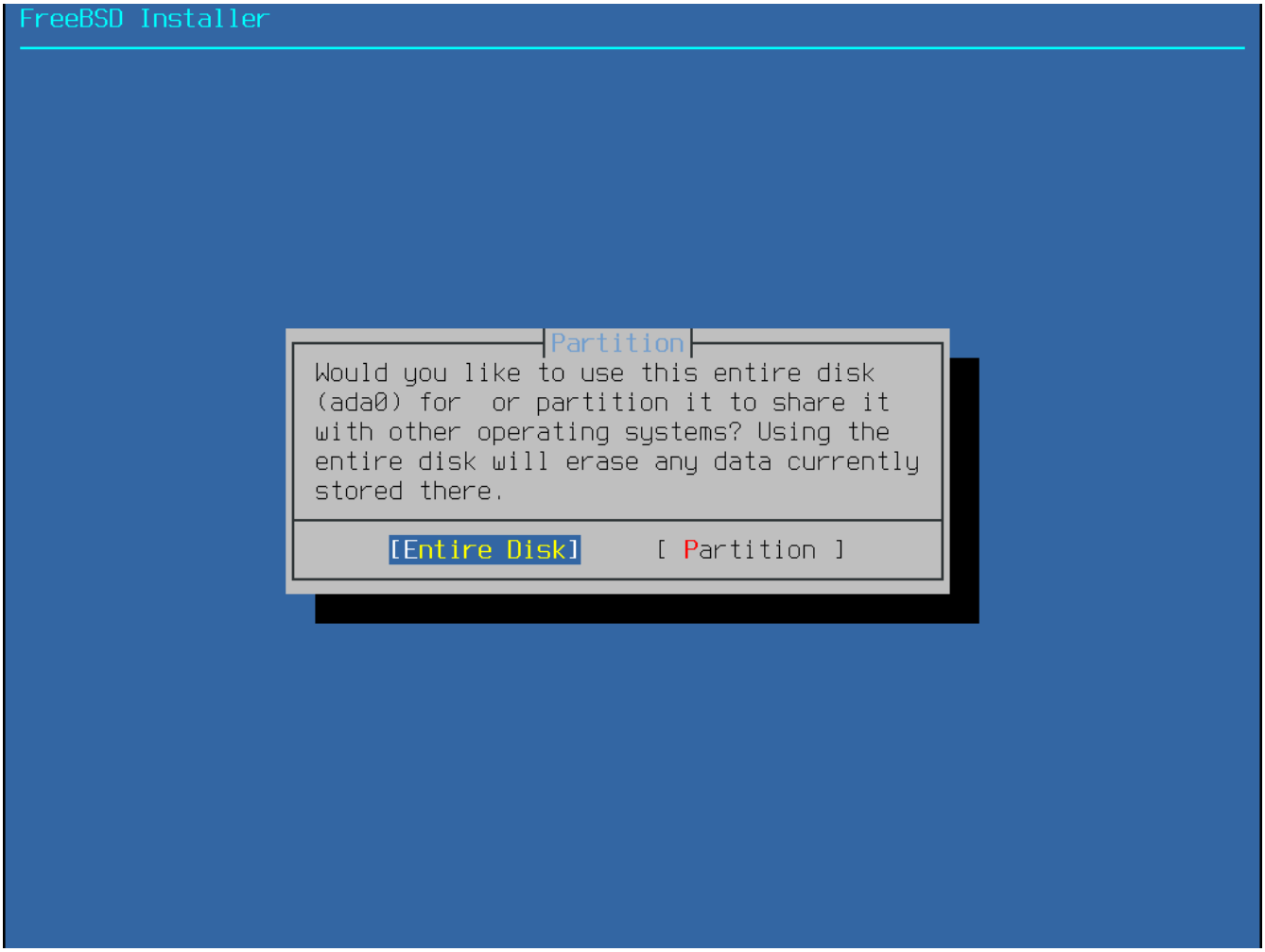


Figure 12. Sélection de l'intégralité du disque ou d'une partition

Après la sélection de **[Entire Disk]**, bsdinstall affiche une boîte de dialogue indiquant que le disque va être effacé.

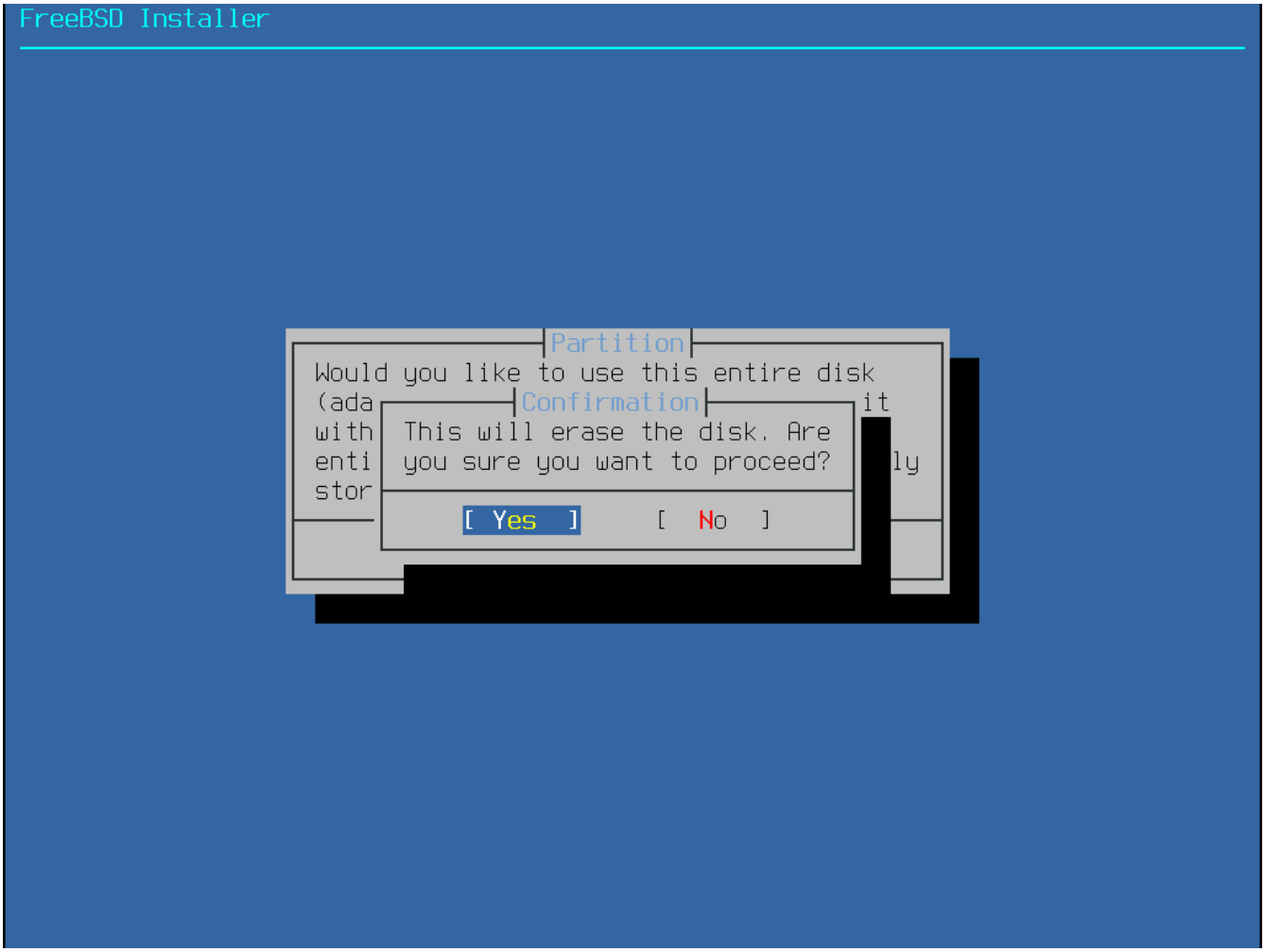


Figure 13. Confirmation

Le menu suivant montre une liste avec les différents types d'organisation des partitions. GPT est généralement le choix le plus adapté pour les ordinateurs de type amd64. Les ordinateurs plus anciens qui ne sont pas compatibles avec GPT devraient utiliser un partionnement de type MBR. Les autres types de partionnement sont généralement utilisés pour les ordinateurs peu courants ou anciens. Plus d'informations sont disponibles dans la Tables de partitionnement.

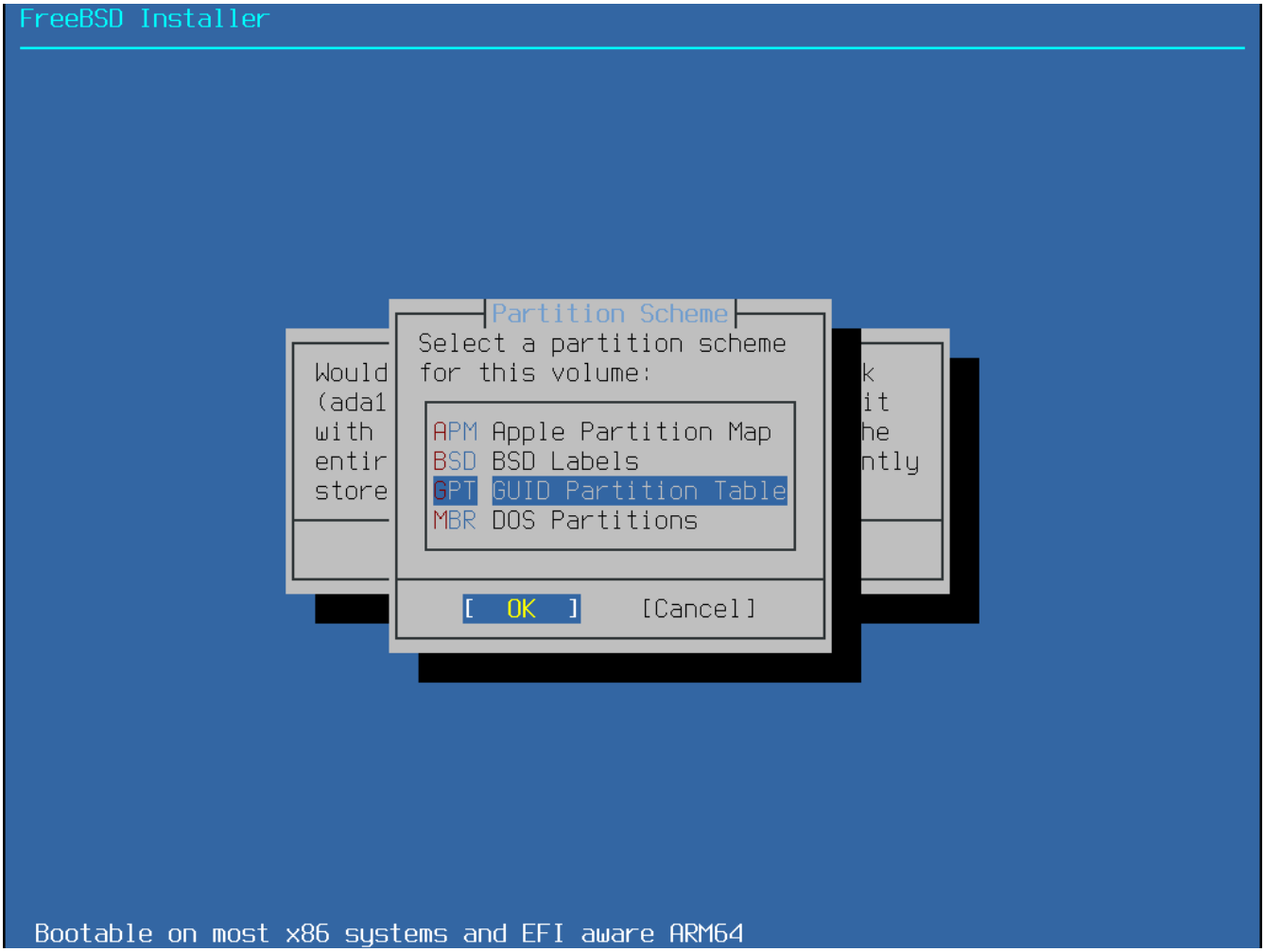


Figure 14. Sélection du système de partionnement

Une fois l'organisation des partitions créée, vérifiez-la afin de s'assurer qu'elle correspond bien aux besoins de l'installation. La sélection de **[Revert]** permettra de revenir au partitionnement de départ, et l'appui sur **[Auto]** créera les partitions FreeBSD automatiquement. Les partitions peuvent être créées, modifiées, ou supprimées manuellement. Quand le partitionnement est correct, sélectionner **[Finish]** pour poursuivre l'installation.

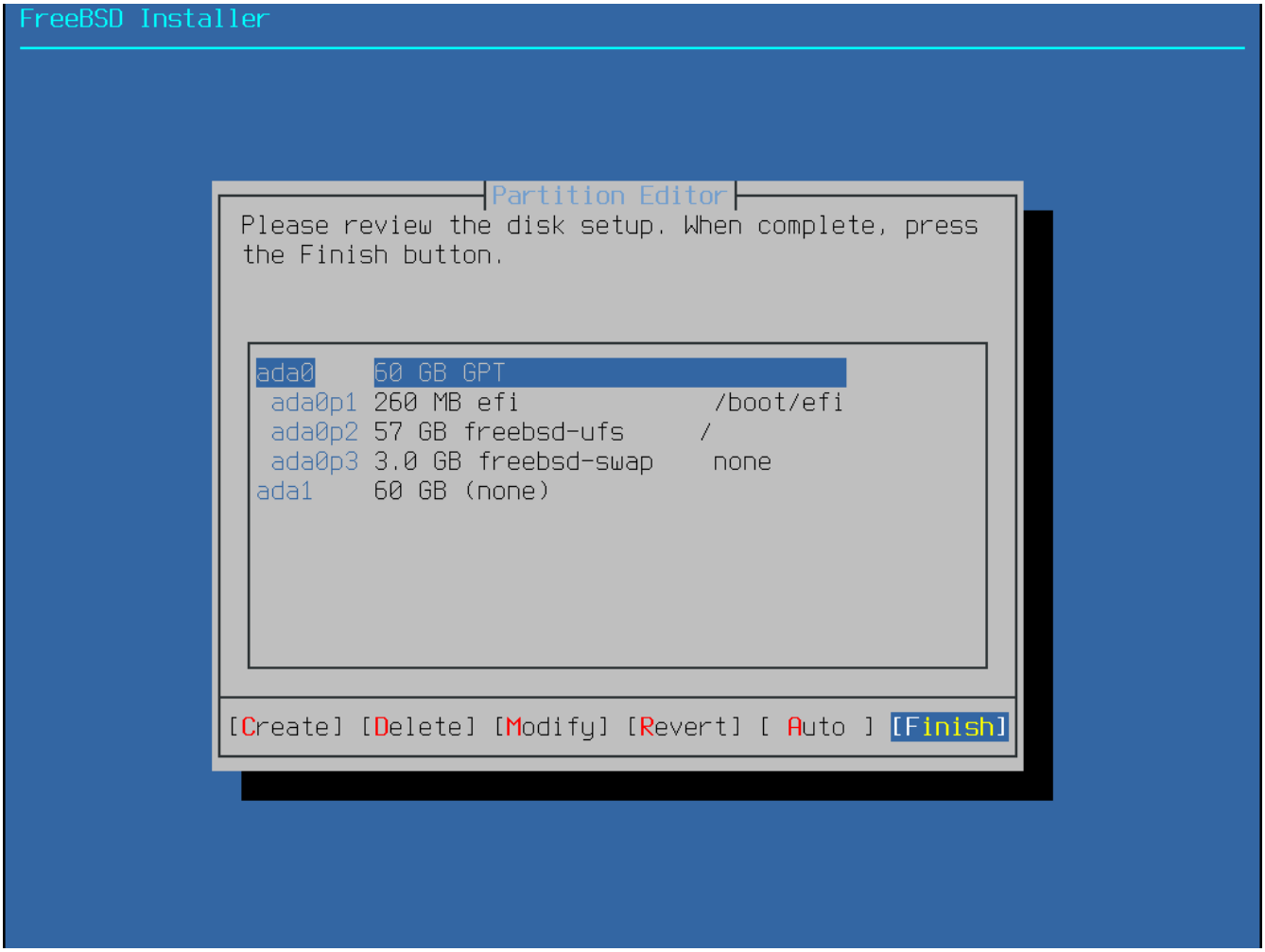


Figure 15. Vérification des partitions créées

Une fois les disques configurés, le menu suivant offre une dernière chance pour effectuer des modifications avant que les disques sélectionnés ne soient formatés. Si des changements doivent être faits, choisir **[Back]** pour retourner dans le menu principal de partionnement. **[Revert Exit]** fera quitter le programme d'installation sans qu'aucun changement n'ait été appliqué au disque dur. Sélectionner **[Commit]** pour lancer le processus d'installation.

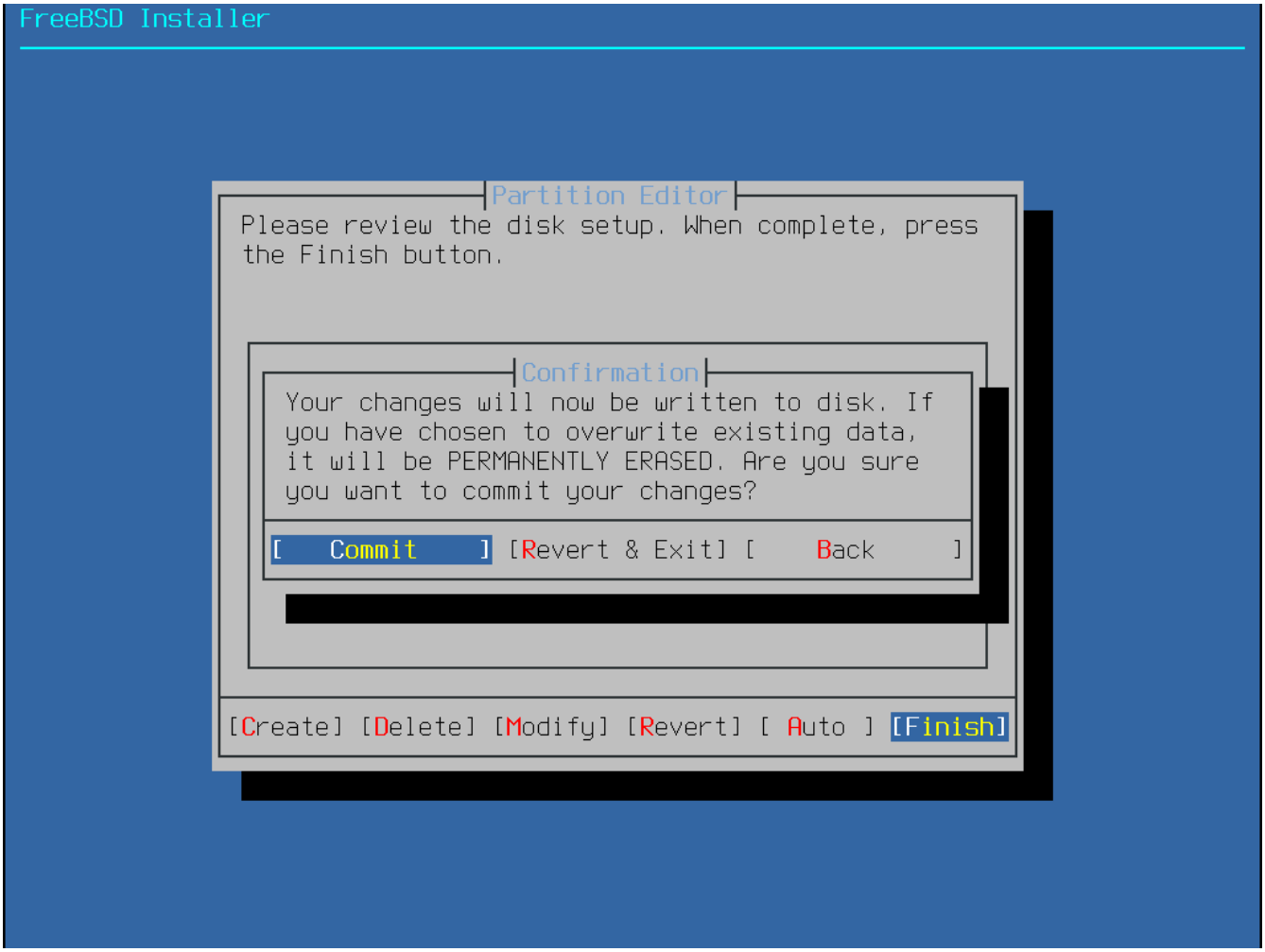


Figure 16. Confirmation finale

Pour poursuivre le processus d'installation, aller à la Récupération des fichiers de distribution.

2.6.3. Partitionnement manuel

La sélection de cette méthode ouvre l'éditeur de partitions.

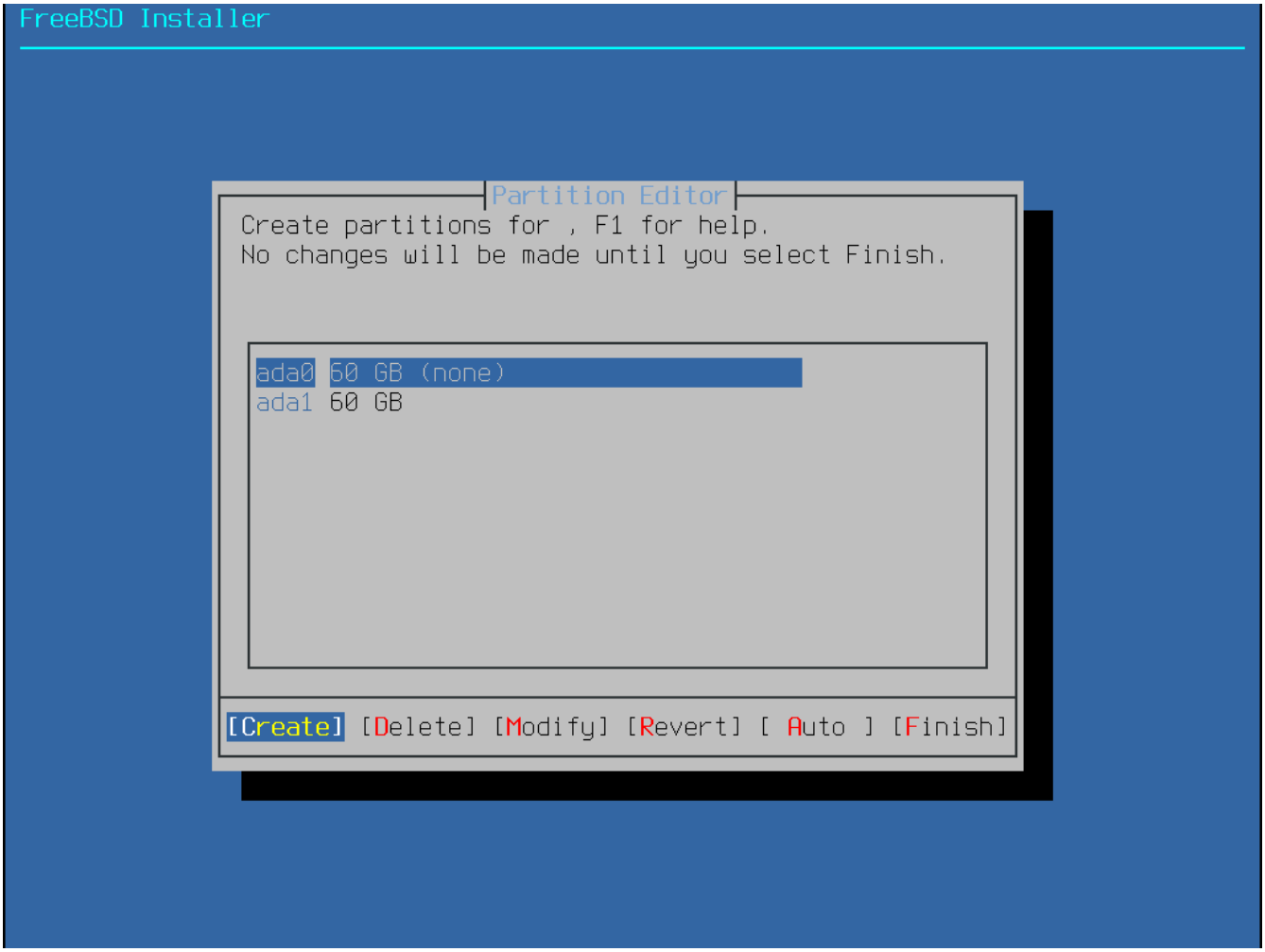


Figure 17. Créer manuellement les partitions

Sélectionner le disque d'installation(ada0 dans cet exemple) et **[Create]** pour afficher un menu sur le choix du type de table de partitionnement.

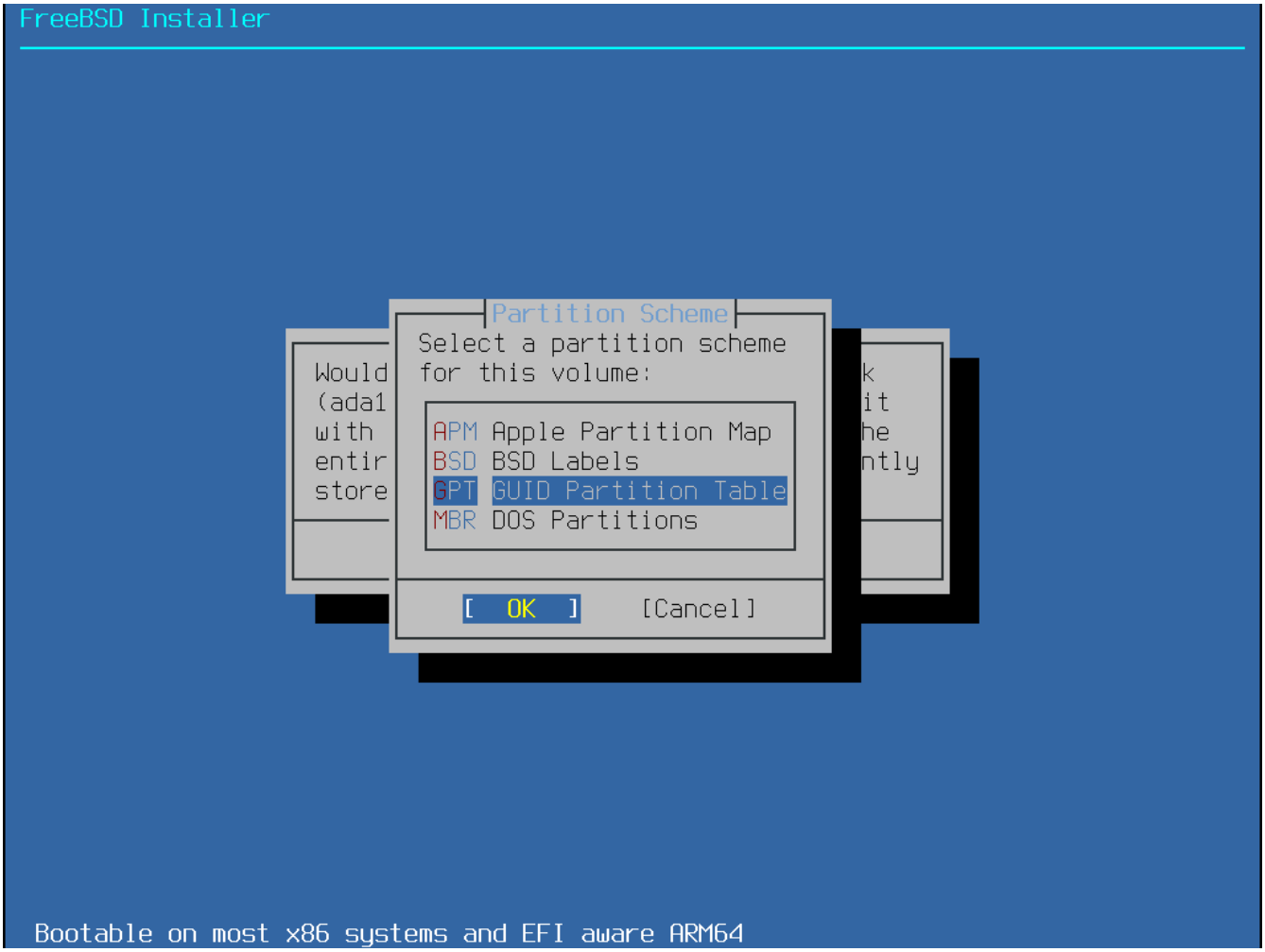


Figure 18. Créer manuellement les partitions

Le partitionnement GPT est généralement le choix le plus approprié pour les ordinateurs de type amd64 Les ordinateurs anciens qui ne sont pas compatibles avec GPT doivent utiliser à la place un partitionnement de type MBR. Les autres systèmes de partitionnement sont en général utilisés pour les ordinateurs plus anciens ou particuliers.

Tableau 1. Tables de partitionnement

Abbréviation	Description
APM	Table de partition Apple, utilisée par l'architecture PowerPC®.
BSD	Partition BSD (*BSD Labels*) sans MBR, parfois appelée *dangerously dedicated mode* ou "mode dédié" car les utilitaires disques non-BSD peuvent ne pas la reconnaître.
GPT	Table de partition GUID (http://en.wikipedia.org/wiki/GUID_Partition_Table").
MBR	Master Boot Record (http://en.wikipedia.org/wiki/Master_boot_record").

Après avoir choisi et créé le partitionnement, sélectionner à nouveau **[Create]** créera les nouvelles partitions. La touche `Tab` est utilisée pour déplacer le curseur entre les différents champs.

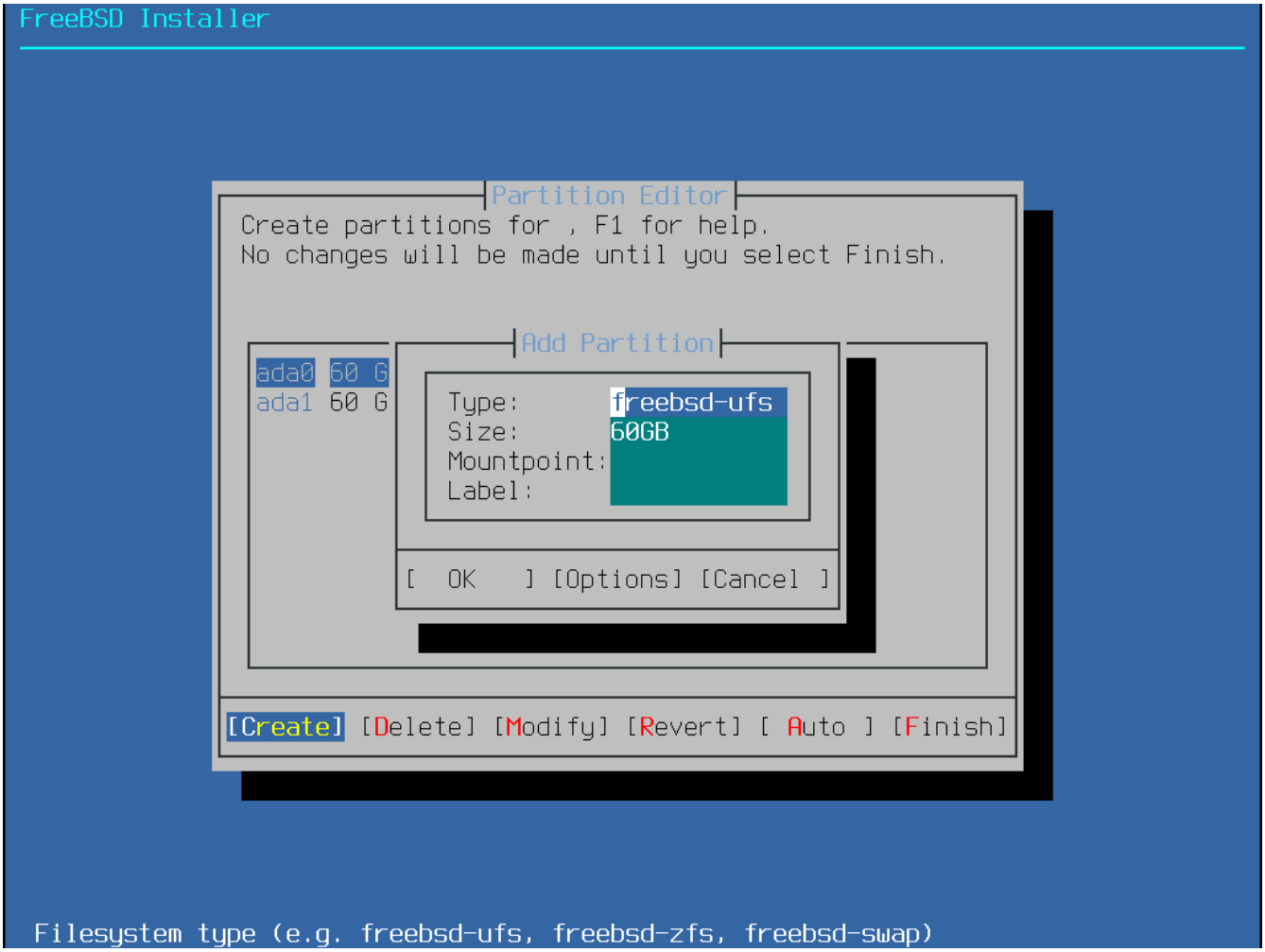


Figure 19. Créer manuellement les partitions

Une installation standard de FreeBSD avec GPT utilise au moins trois partitions:

- `freebsd-boot` - Contient le code de démarrage FreeBSD.
- `freebsd-ufs` - Un système de fichiers UFS FreeBSD.
- `freebsd-zfs` - Un système de fichiers ZFS FreeBSD. Plus d'informations au sujet de ZFS est disponible dans le The Z File System (ZFS) **Traduction en Cours** .
- `freebsd-swap` - Espace de pagination pour FreeBSD.

Consulter la page de manuel gpart(8) pour la description d'autres types de partitions disponibles pour GPT.

Des partitions avec plusieurs systèmes de fichiers peuvent être créées et certaines personnes préfèrent une organisation plus traditionnelle avec des partitions séparées pour les systèmes de fichiers /, /var, /tmp, et /usr. Consulter Création d'un système traditionnel de partitions pour systèmes de fichiers séparés, pour un exemple.

Les tailles peuvent être entrées avec les abréviations courantes: *K* for kilooctet, *M* pour mégaoctets, ou *G* pour gigaoctets.

Un alignement correct des secteurs sur le disque permet de meilleures performances, et créer des partitions de tailles multiples de 4Koctets permet de s'assurer de l'alignement sur les disques à secteur de 512 octets ou 4Koctets. Généralement, employer des tailles de partition qui sont des multiples d'1M ou 1G est le moyen le plus simple de garantir que chaque partition débute sur un multiple de 4K. Il existe une exception: la partition *freebsd-boot* ne devrait pas dépasser 512K en raison de limitations du code de démarrage.

Un point de montage est nécessaire si cette partition contiendra un système de fichiers. Si une seule partition UFS unique sera créée, le point de montage devra être /.

Un `Label` (ou étiquette) est le nom avec lequel la partition sera connue. Les noms ou numéros de disques peuvent varier si le disque est connecté à un contrôleur ou port différent, mais le label de partition ne changera pas. Se référer aux labels plutôt qu'aux noms de disques et numéros de partitions dans les fichiers comme /etc/fstab rend le système plus tolérant aux changements de matériel. Les labels GPT apparaissent dans le répertoire /dev/gpt/ lorsqu'un disque est attaché au système. Les autres systèmes de partitionnement présentent d'autres possibilités au niveau des labels et leurs labels apparaissent sous différentes répertoires dans /dev/.

Employez un label unique pour chaque partition pour éviter les conflits avec les labels identiques. Quelques lettres du nom du l'ordinateur, de son rôle, ou de son emplacement peuvent être ajoutées au label. Par exemple, `labroot` ou `rootfslab` pour la partition UFS racine de l'ordinateur appelé `lab`.

Exemple 1. Création d'un système traditionnel de partitions pour systèmes de fichiers séparés

Pour une organisation traditionnelle de partitions dans laquelle les répertoires /, /var, /tmp, et /usr sont des systèmes de fichiers séparés ayant chacun leur propre partition, créer une table de partition GPT, puis créer les partitions comme montré ci-après. Les tailles de partitions indiquées sont celles typiques pour un disque de 20G. Si plus d'espace est disponible sur le disque cible, une partition de pagination ou une partition /var plus importantes peuvent être utiles. Les labels utilisés ici sont préfixés par `ex` pour "exemple", mais le lecteur peut utiliser un autre label unique comme décrit plus haut.

Par défaut, le programme gptboot de FreeBSD s'attend à ce que la première partition UFS trouvée soit la partition /.

Type de partition	Taille	Point de montage	Label
`freebsd-boot`	`512K`		
`freebsd-ufs`	`2G`	/	`exrootfs`
`freebsd-swap`	`4G`		`exswap`
`freebsd-ufs`	`2G`	/var	`exvarfs`
`freebsd-ufs`	`1G`	/tmp	`extmpfs`
`freebsd-ufs`	valeur proposée par défaut (le reste du disque)	/usr	`exusrfs`

Après la création des partitions, sélectionnez **[Finish]** pour poursuivre l'installation et rendez-vous à la Récupération des fichiers de distribution.

2.6.4. Partitionnement guidé avec la racine du système de fichiers sur ZFS

Ce mode de partitionnement ne fonctionne qu'avec des disques entiers et effacera le contenu du disque entier. Le menu principal de configuration ZFS présente plusieurs options pour contrôler la création du pool (ensemble de stockage constitué d'un ou plusieurs disques).

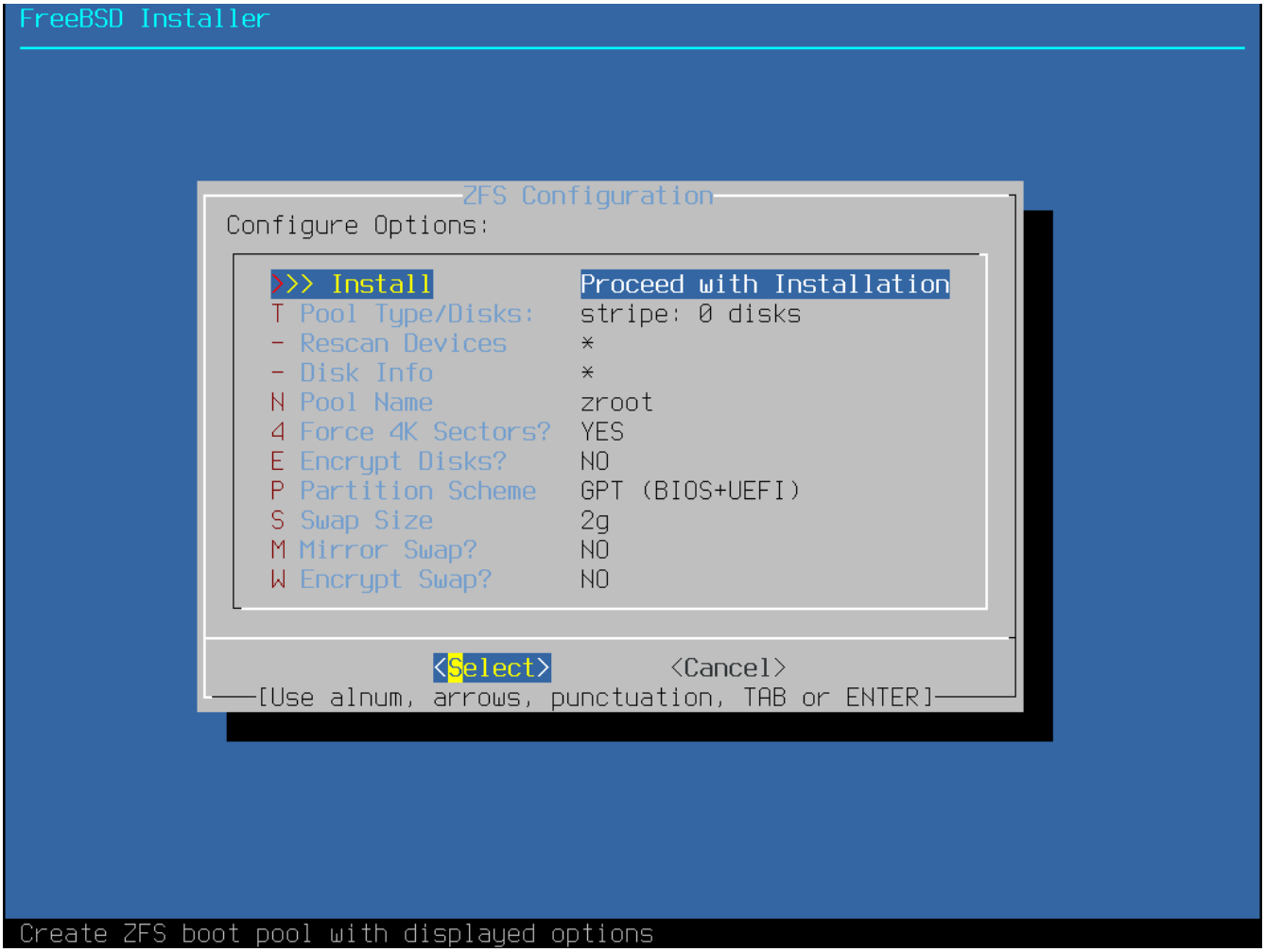


Figure 20. Menu de partionnement ZFS

Voici un résumé des options pouvant être utilisées dans ce menu:

- `Install` - Procède à l'installation avec les options sélectionnées.
- `Pool Type/Disks` - Permet la configuration du `Pool Type` et des disques qui formeront le pool. Le programme d'installation ZFS automatique ne supporte, actuellement qu'un seul périphérique virtuel ("top level vdev") de niveau supérieur en dehors du mode stripe (un seul disque ou concaténation de plusieurs disques). Pour créer des pools plus complexes, utilisez les instructions de la Partitionnement à partir de l'interpréteur de commandes pour créer le pool.
- `Rescan Devices` - Met à jour la liste des disques disponibles.
- `Disk Info` - Ce menu peut être utilisé pour inspecter chaque disque, y compris sa table des partitions et différentes autres informations comme la référence du modèle et son numéro de série s'ils sont disponibles.

- `Pool Name` - Fixe le nom du pool. Le nom par défaut est *zroot*.
- `Force 4K Sectors?` - Force l'utilisation de secteurs d'une taille de 4Ko. Par défaut, le programme d'installation créera automatiquement des partitions qui seront alignées sur des emplacements multiples de 4Ko et force ZFS à utiliser des secteurs de 4Ko. C'est sans risque même pour les disques avec des secteurs de 512 octets, et présente l'avantage de s'assurer que les pools créés sur des disques à secteurs de 512 octets pourront se voir ajouter, dans le futur, des disques avec secteurs de 4Ko comme espace de stockage supplémentaire ou en remplacement de disques défectueux. Appuyez sur la touche `Enter` pour choisir d'activer ou non cette option.
- `Encrypt Disks?` - Le chiffrement des disques permet à l'utilisateur de chiffer les disques avec GELI. Plus d'information au sujet du chiffrement des disques est disponible dans la Chiffrage des disques avec geli. Appuyez sur la touche `Enter` pour choisir d'activer ou non cette option.
- `Partition Scheme` - Permet de choisir le système de partionnement. GPT est l'option recommandée dans la plupart des cas. Appuyez sur la touche `Enter` pour choisir parmi les differentes options.
- `Swap Size` - Fixe la quantité d'espace de pagination.
- `Mirror Swap?` - Permet à l'utilisateur de créer un miroir de l'espace de pagination sur chaque disque. Faites attention, activer l'espace de pagination en mode miroir rend les crashs dumps inutilisables. Appuyez sur la touche `Enter` pour choisir d'activer ou non cette option.
- `Encrypt Swap?` - Permet à l'utilisateur de chiffrer l'espace de pagination. Le système chiffre l'espace de pagination avec une clé temporaire à chaque démarrage du système et en change à chaque redémarrage. Appuyez sur la touche `Enter` pour choisir d'activer ou non cette option. Plus d'information au sujet du chiffrement de l'espace de pagination dans la Chiffrage de l'espace de pagination.

Sélectionner `T` pour configurer le `Pool Type` et le ou les disques qui constitueront le pool.

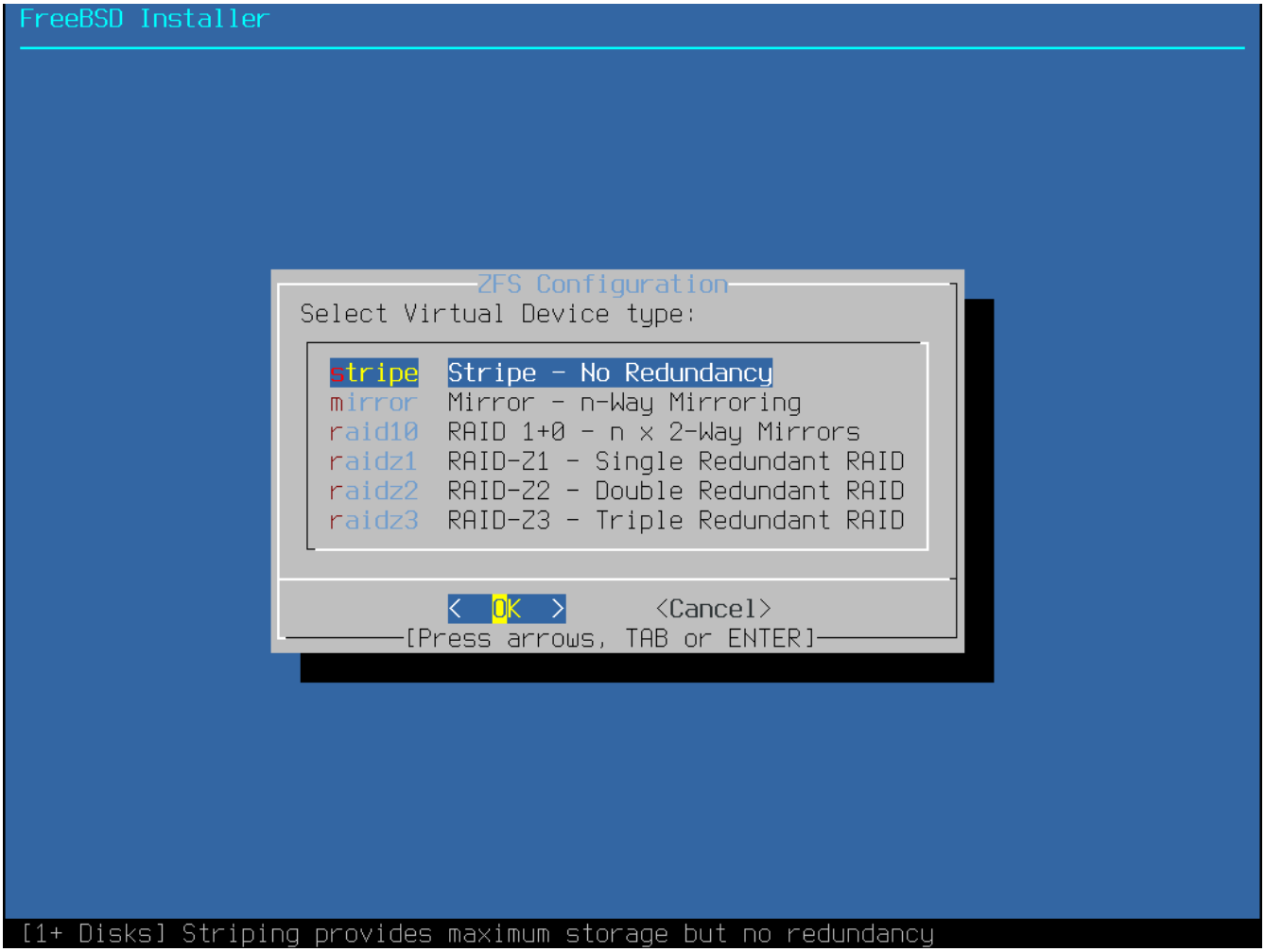


Figure 21. Type de pool ZFS

Voici un résumé des `Pool Type` pouvant être sélectionnés dans ce menu:

- `stripe` - Le mode striping ou entrelacé offre le maximum d'espace de stockage à partir de l'ensemble des périphériques connectés, mais pas de redondance. Si un seul disque tombe en panne, les données du pool seront perdues de manière définitive.
- `mirror` - Le mode miroir stocke une copie complète des données sur chaque disque. Le mode miroir offre de bonnes performances en lecture parce que les données sont lues à partir de tous les disques en parallèles. Les performances en écriture sont plus lentes étant donné que les données doivent être écrites sur tous les disques du pool. Ce mode permet à tous les disques sauf un de tomber en panne. Cette option nécessite aux moins deux disques.
- `raid10` - Miroirs entrelacés. Offre les meilleures performances mais le moins d'espace de stockage. Cette option nécessite un nombre pair de disques et au minimum quatre disques.
- `raidz1` - RAID à simple redondance. Permet la panne d'un seul disque. Cette option nécessite au moins trois disques.
- `raidz2` - RAID à double redondance. Permet la panne simultanée de deux disques. Cette option nécessite au moins quatre disques.
- `raidz3` - RAID à triple redondance. Permet la panne simultanée de trois disques. Cette option nécessite au moins cinq disques.

Une fois que le `Pool Type` a été sélectionné, la liste des disques disponibles est affichée, et

l'utilisateur est invité à choisir un ou plusieurs disques pour former le pool. La configuration doit être alors validée pour s'assurer que suffisamment de disques ont été sélectionnés. Si ce n'est pas le cas, sélectionner **[Change Selection]** pour retourner à la liste des disques, ou **[Back]** pour changer de `Pool Type`.

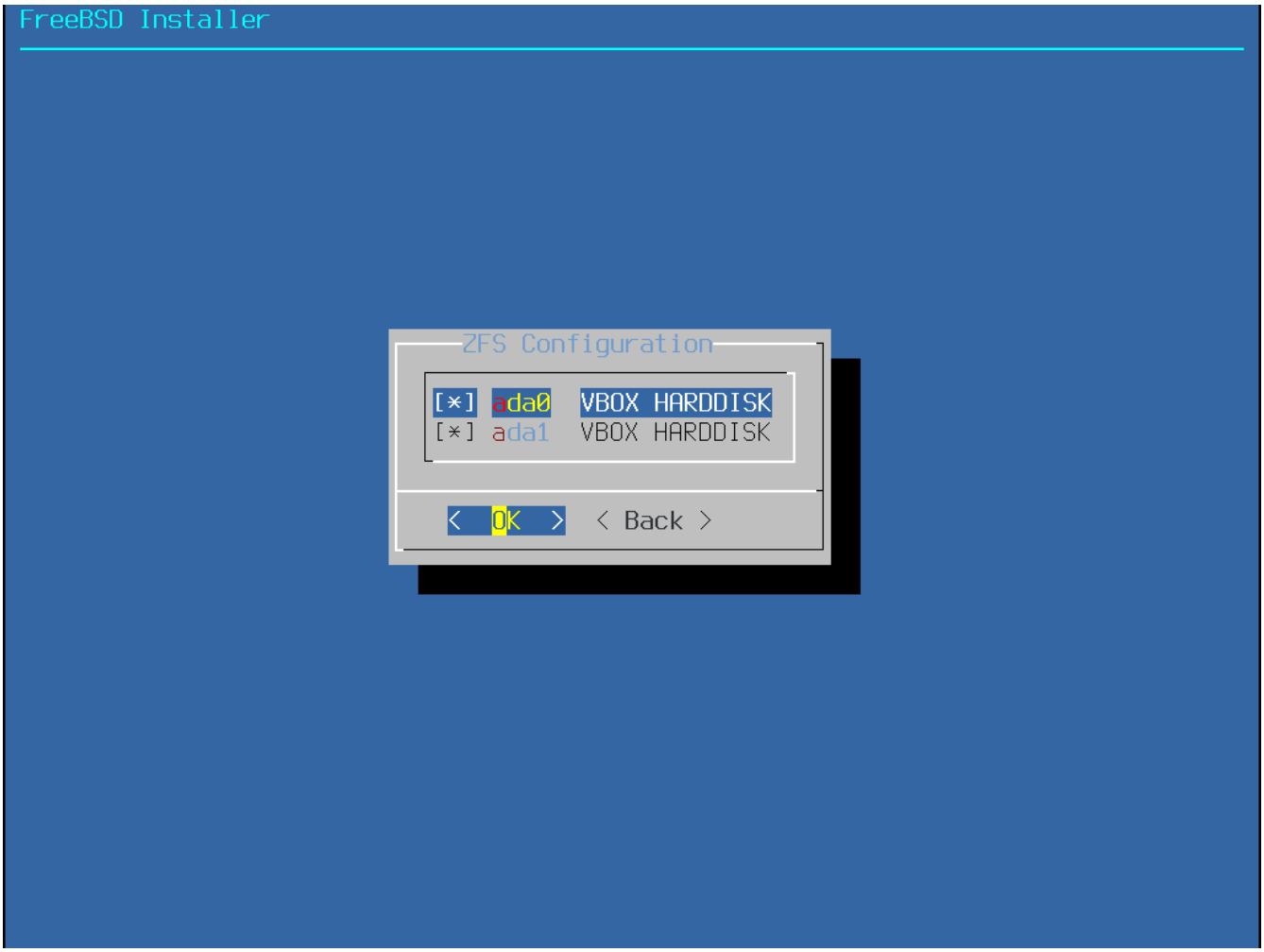


Figure 22. Sélection de disques

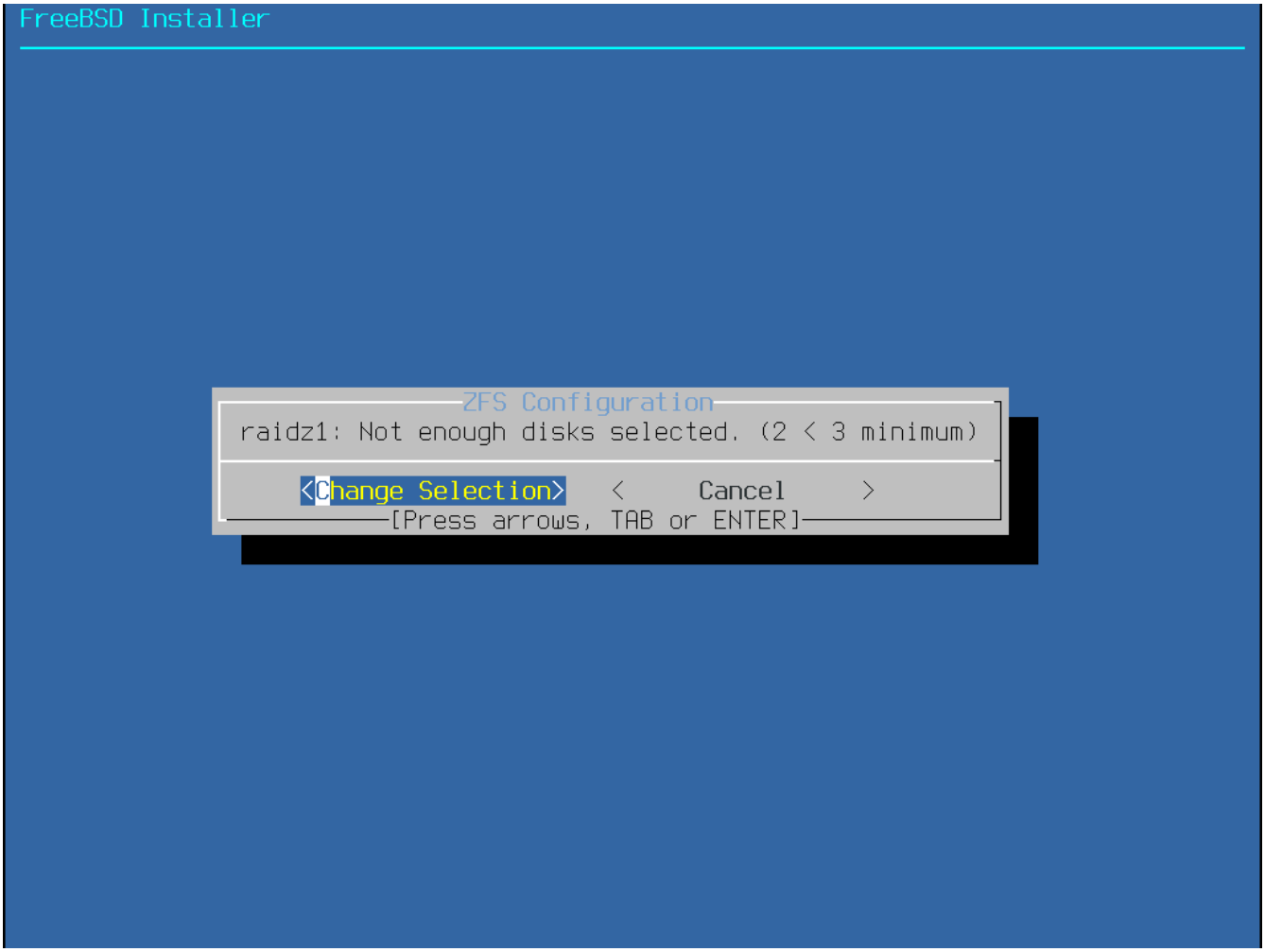


Figure 23. Sélection non-valide

Si un ou plusieurs disques manquent sur la liste, ou si des disques ont été ajoutés après le lancement du programme d'installation, sélectionner **[- Rescan Devices]** pour mettre à jour la liste des disques disponibles.

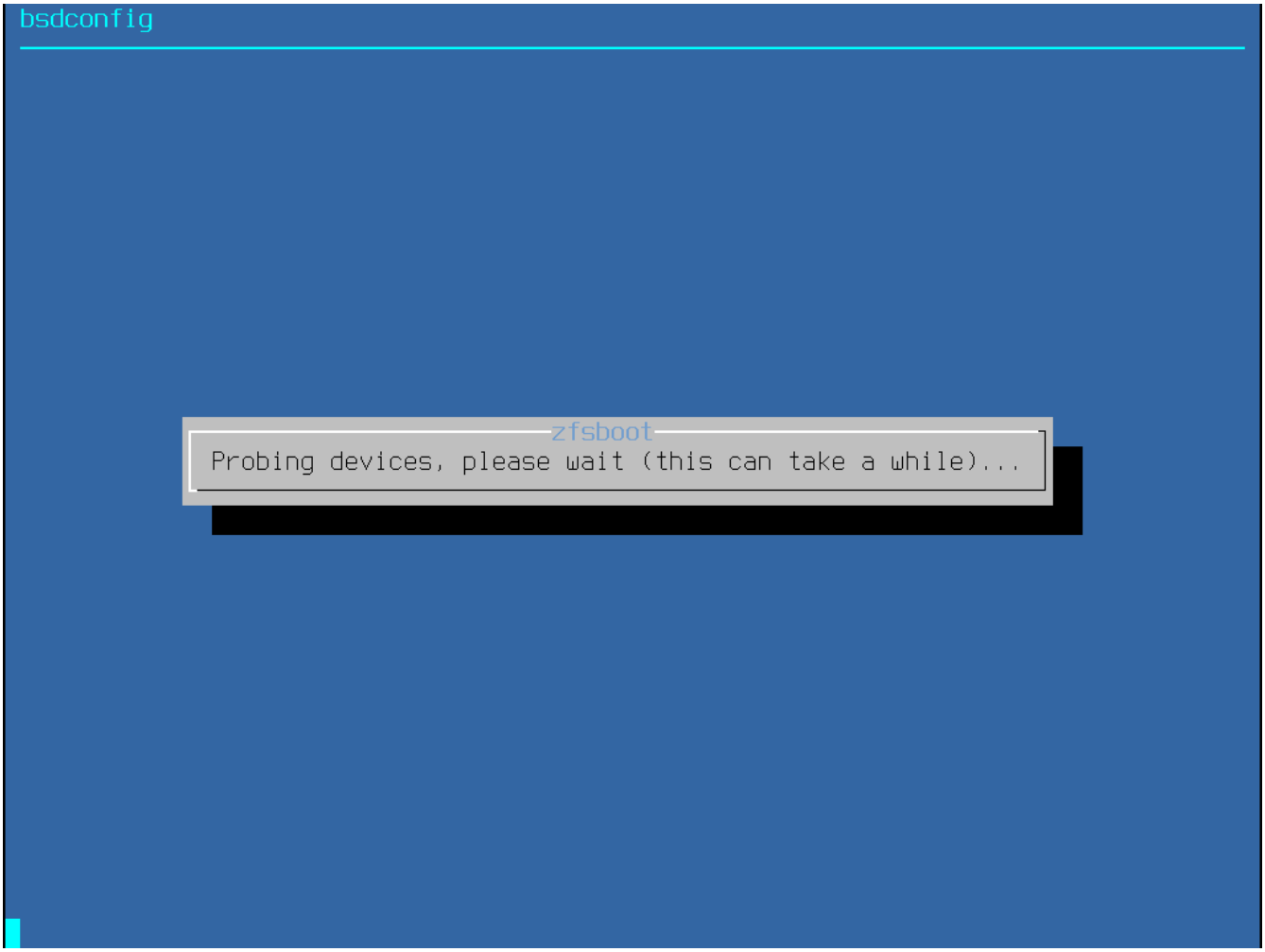


Figure 24. Recherche des périphériques

Pour éviter d'effacer par accident les mauvais disques, le menu **[- Disk Info]** peut être utilisé pour inspecter chaque disque, y compris sa table des partitions et plusieurs autres informations comme le modèle de disque et son numéro de série si disponibles.

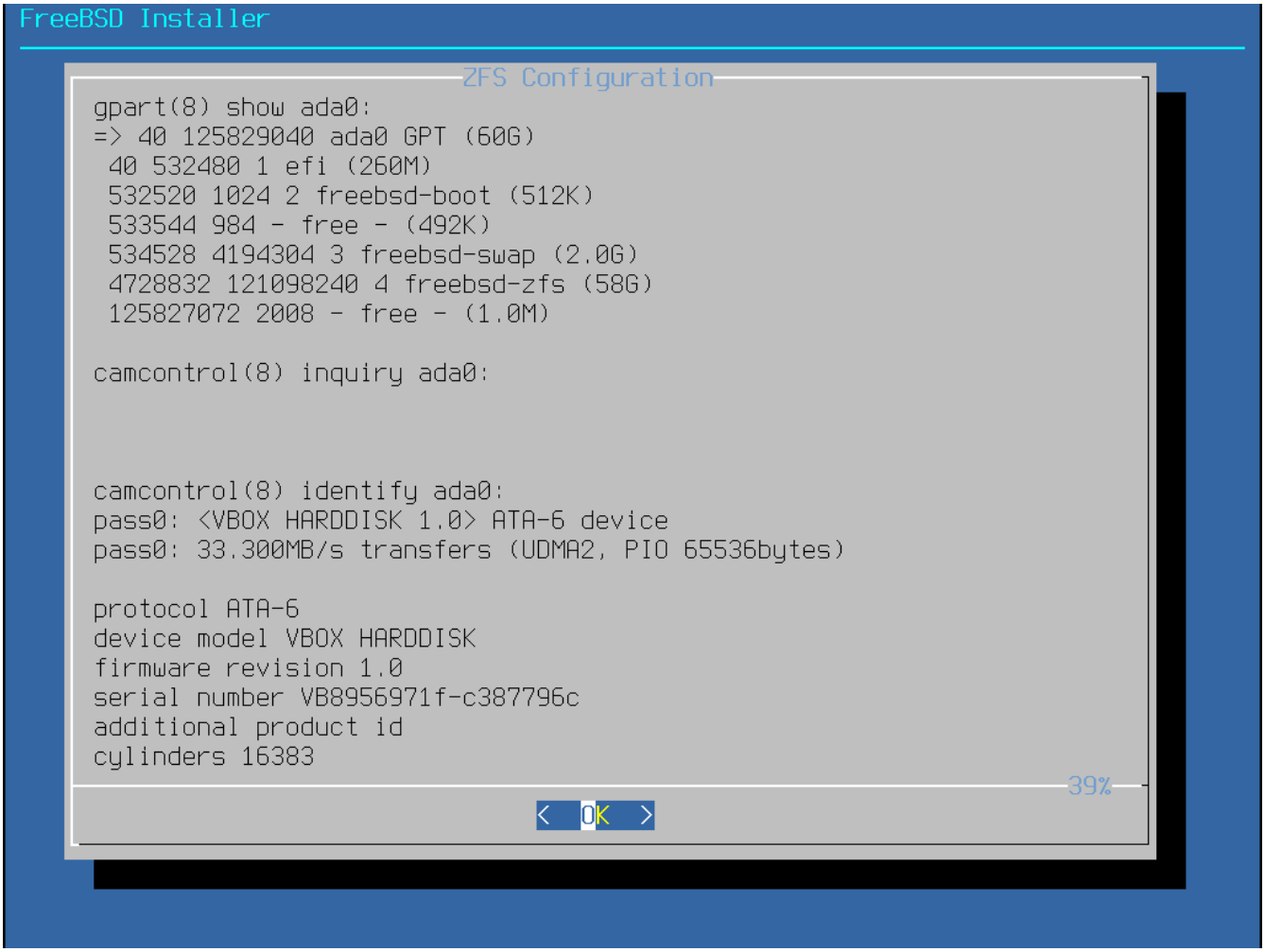


Figure 25. Analyse d'un disque

Sélectionnez `N` pour configurer le `Pool Name`. Entrez le nom souhaité puis sélectionnez **[OK]** pour le prendre en compte ou **[Cancel]** pour retourner au menu principal et conserver le nom par défaut.

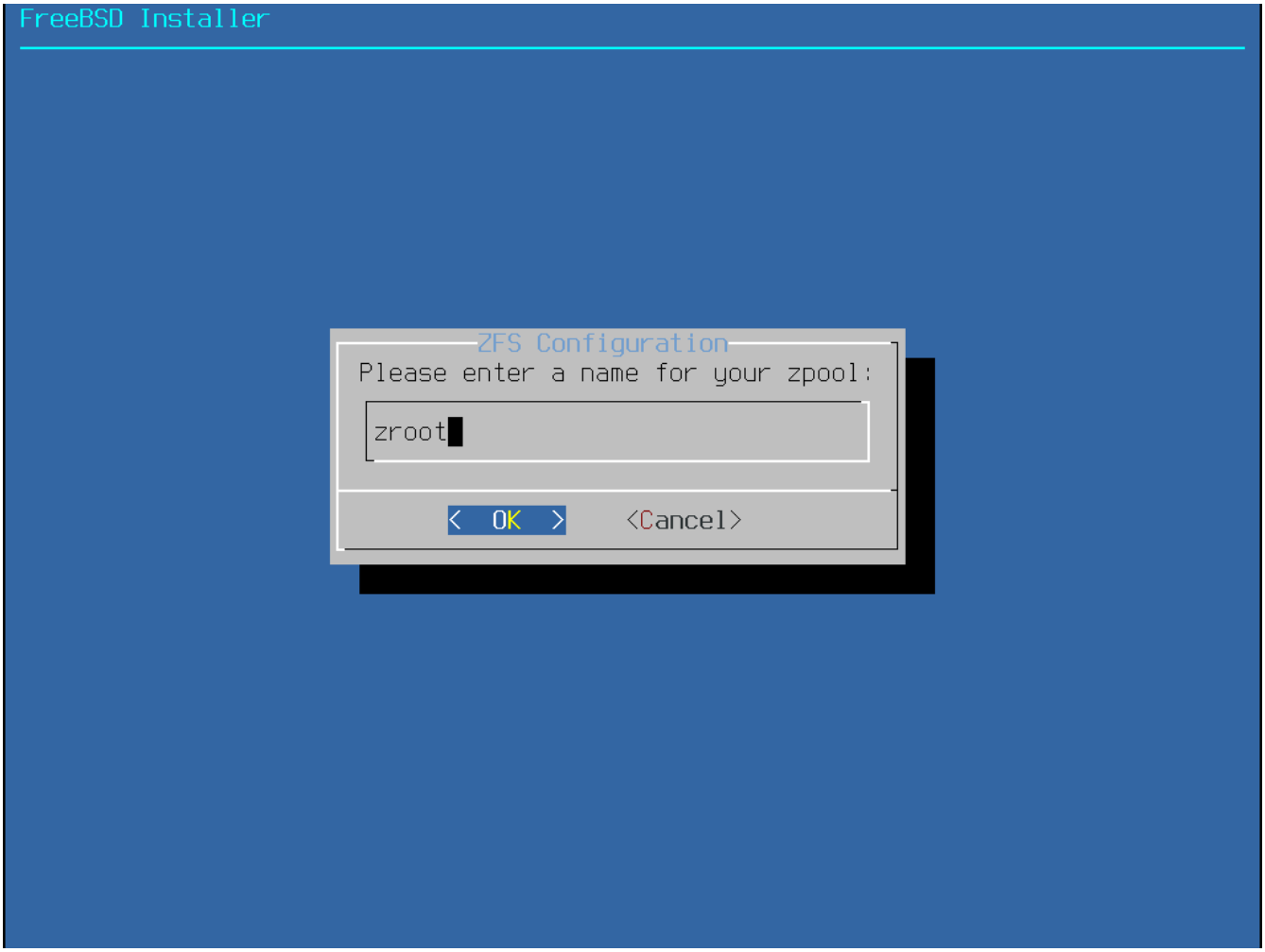


Figure 26. Nom du Pool

Sélectionnez S pour fixer la quantité d'espace de pagination. Entrez la quantité souhaitée puis sélectionnez **[OK]** pour la prendre en compte ou **[Cancel]** pour retourner au menu principal et conserver la quantité par défaut.

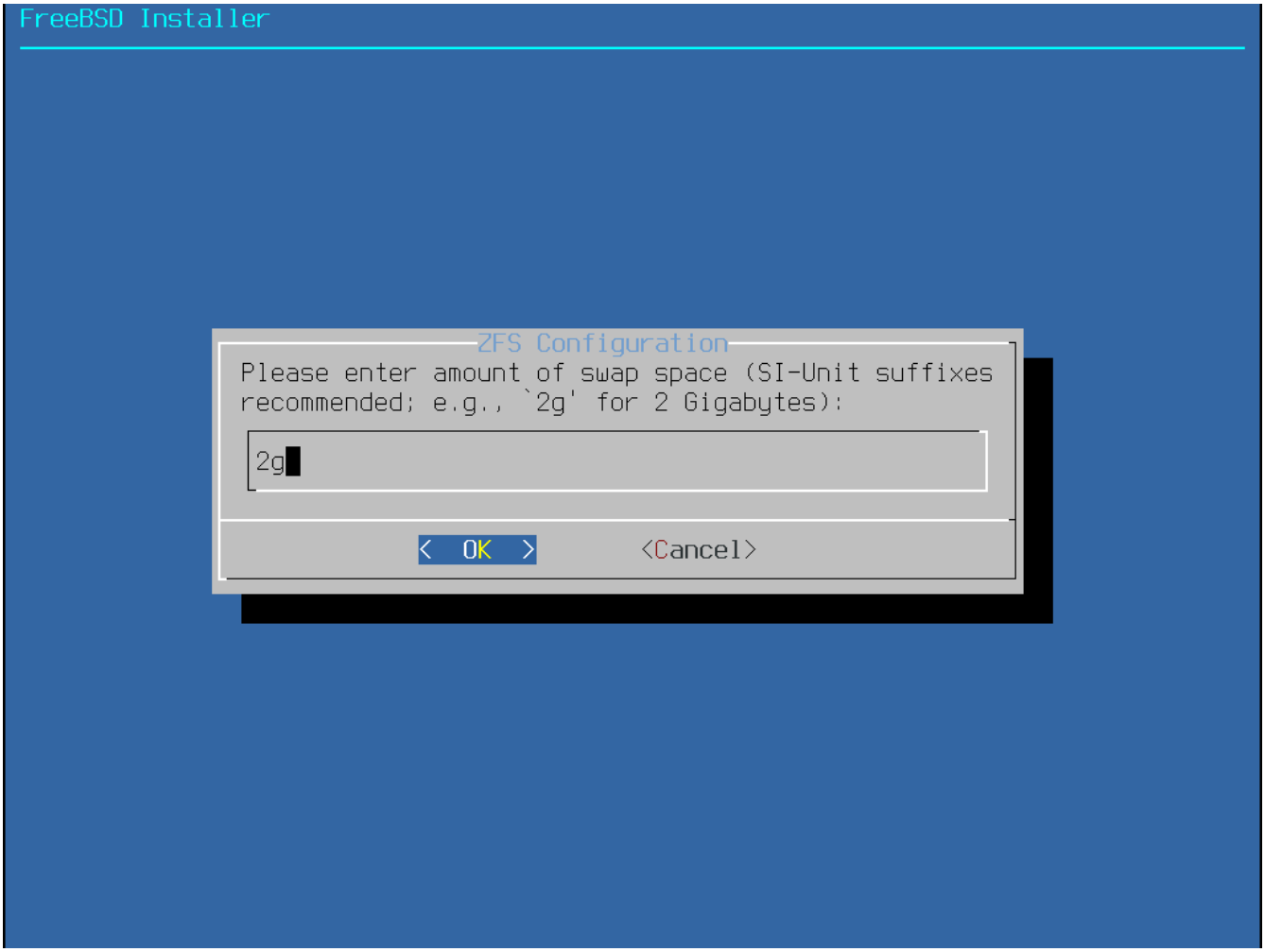


Figure 27. Quantité d'espace de pagination

Une fois que toutes les options ont été configurées aux valeurs souhaitées, sélectionnez l'option **[Install]** en haut du menu. Le programme d'installation offre alors une dernière chance de tout annuler avant que le contenu des disques sélectionnés ne soit détruit pour créer le pool ZFS.

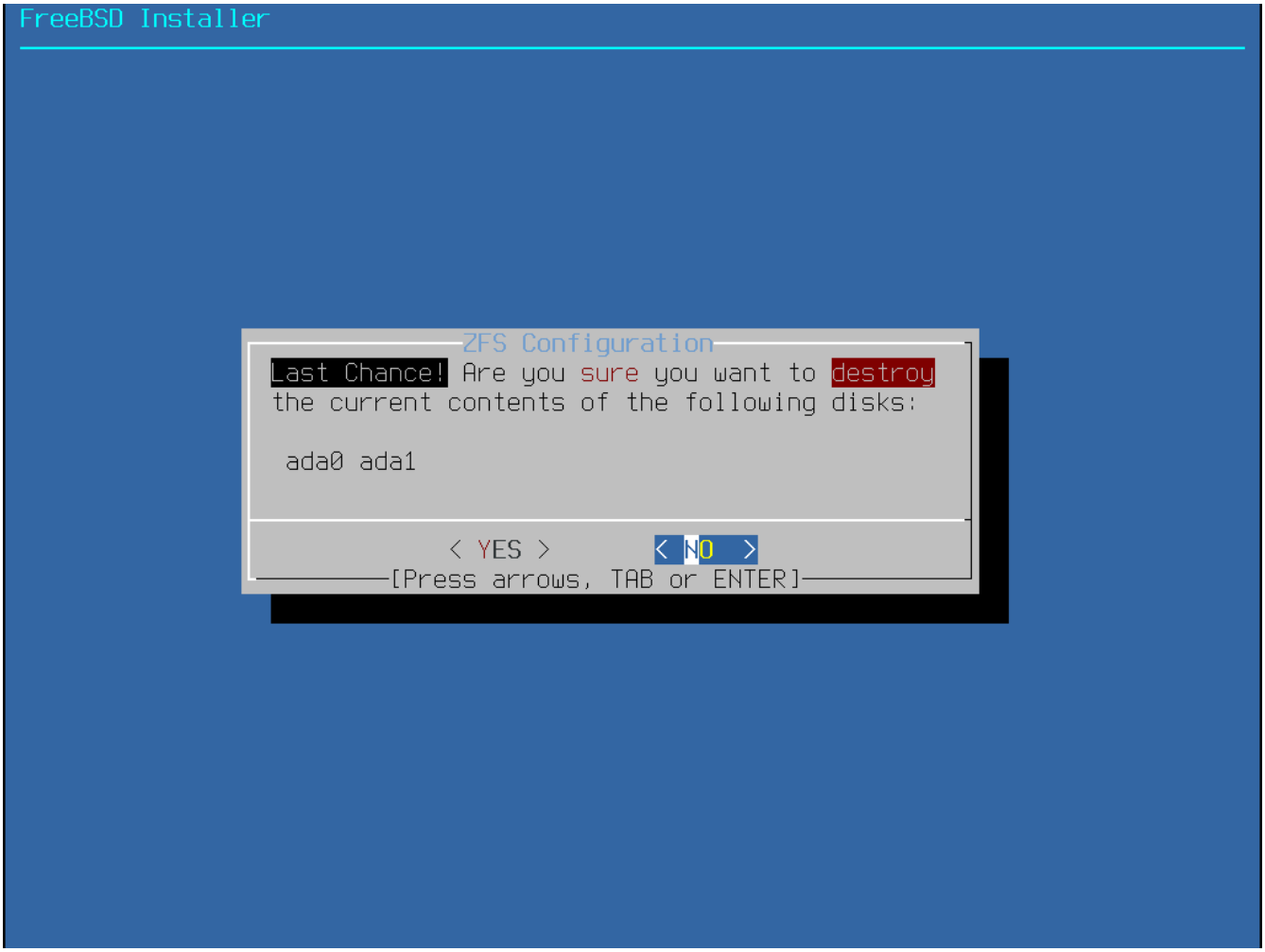


Figure 28. Dernière chance

Si le chiffrement GELI du disque a été activé, le programme d'installation demandera deux fois le mot de passe à utiliser pour chiffrer les disques. Ensuite, après cela, l'initialisation du chiffrement commence.

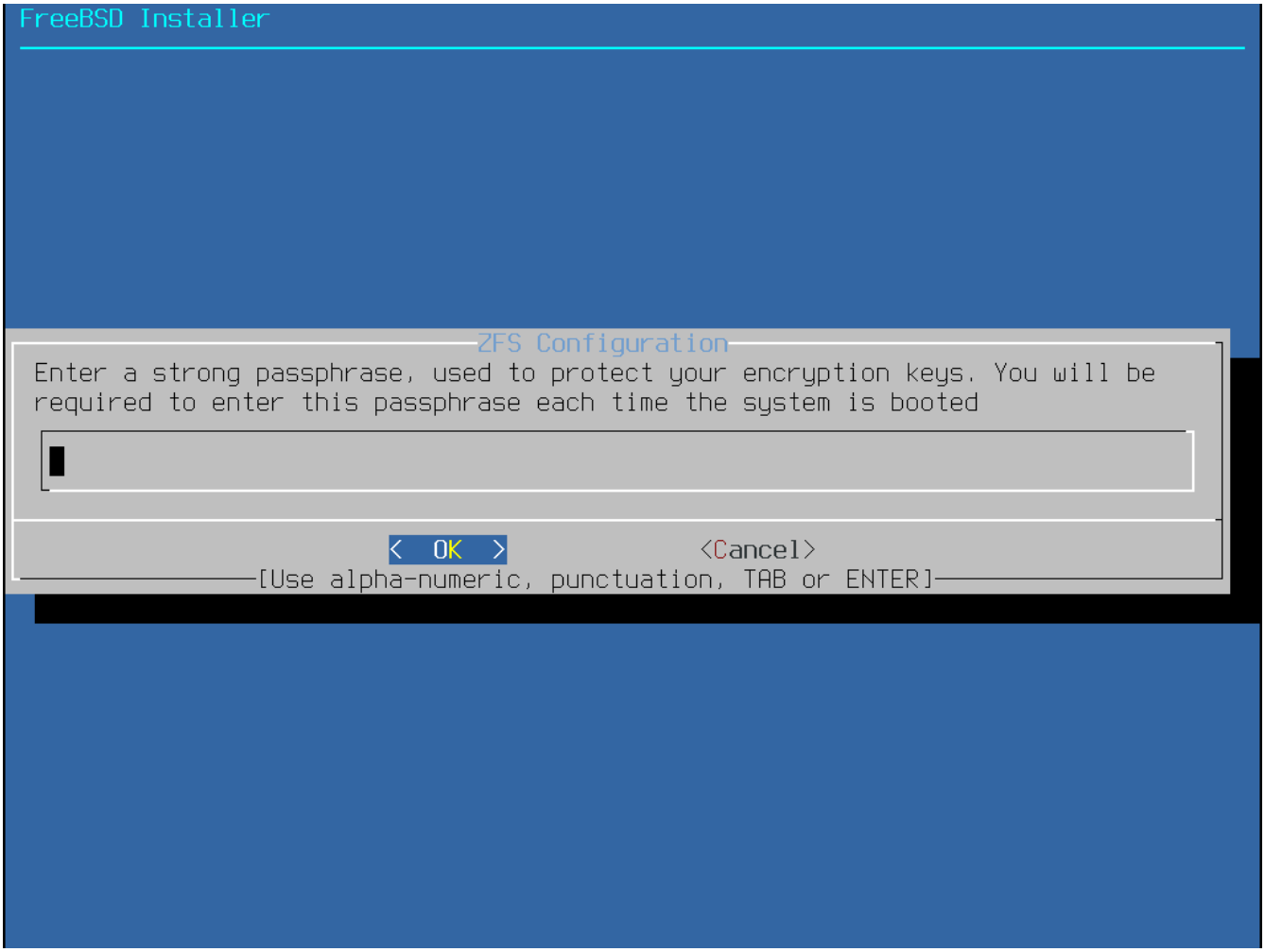


Figure 29. Mot de passe de chiffrement des disques

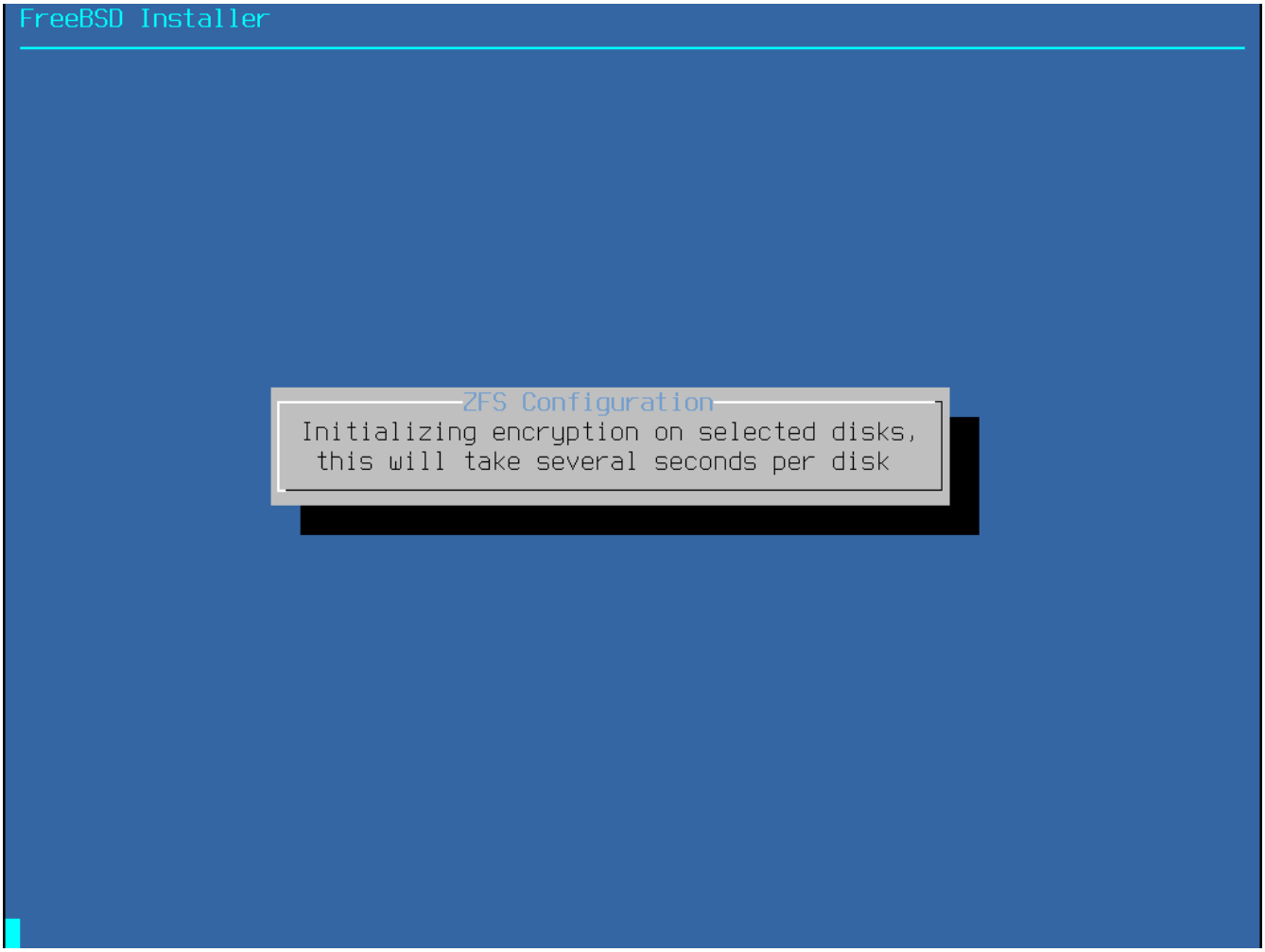


Figure 30. Initialisation du chiffrement

L'installation se poursuit alors normalement. Pour continuer l'installation, aller à Récupération des fichiers de distribution.

2.6.5. Partitionnement à partir de l'interpréteur de commandes

Dans le cas d'installations complexes, les menus de partitionnement de bsdinstall peuvent ne pas proposer le niveau de flexibilité recherché. Les utilisateurs expérimentés peuvent sélectionner l'option **[Shell]** à partir du menu de partitionnement afin de partitionner manuellement les disques, de créer le ou les systèmes de fichiers, d'éditer /tmp/bsdinstall_etc/fstab, et de monter les systèmes de fichiers sous /mnt. Une fois cela fait, taper `exit` pour retourner dans bsdinstall et poursuivre l'installation.

2.7. Récupération des fichiers de distribution

La durée de l'installation variera en fonction de la distribution choisie, du support d'installation, et de la vitesse de l'ordinateur. Une série de messages indiquera la progression de l'installation.

En premier lieu, le programme d'installation formatera le(s) disque(s) sélectionné(s) et initialisera les partitions. Ensuite, dans le cas d'une installation à partir d'un support `bootonly media` ou `mini memstick`, il téléchargera les composants sélectionnés:

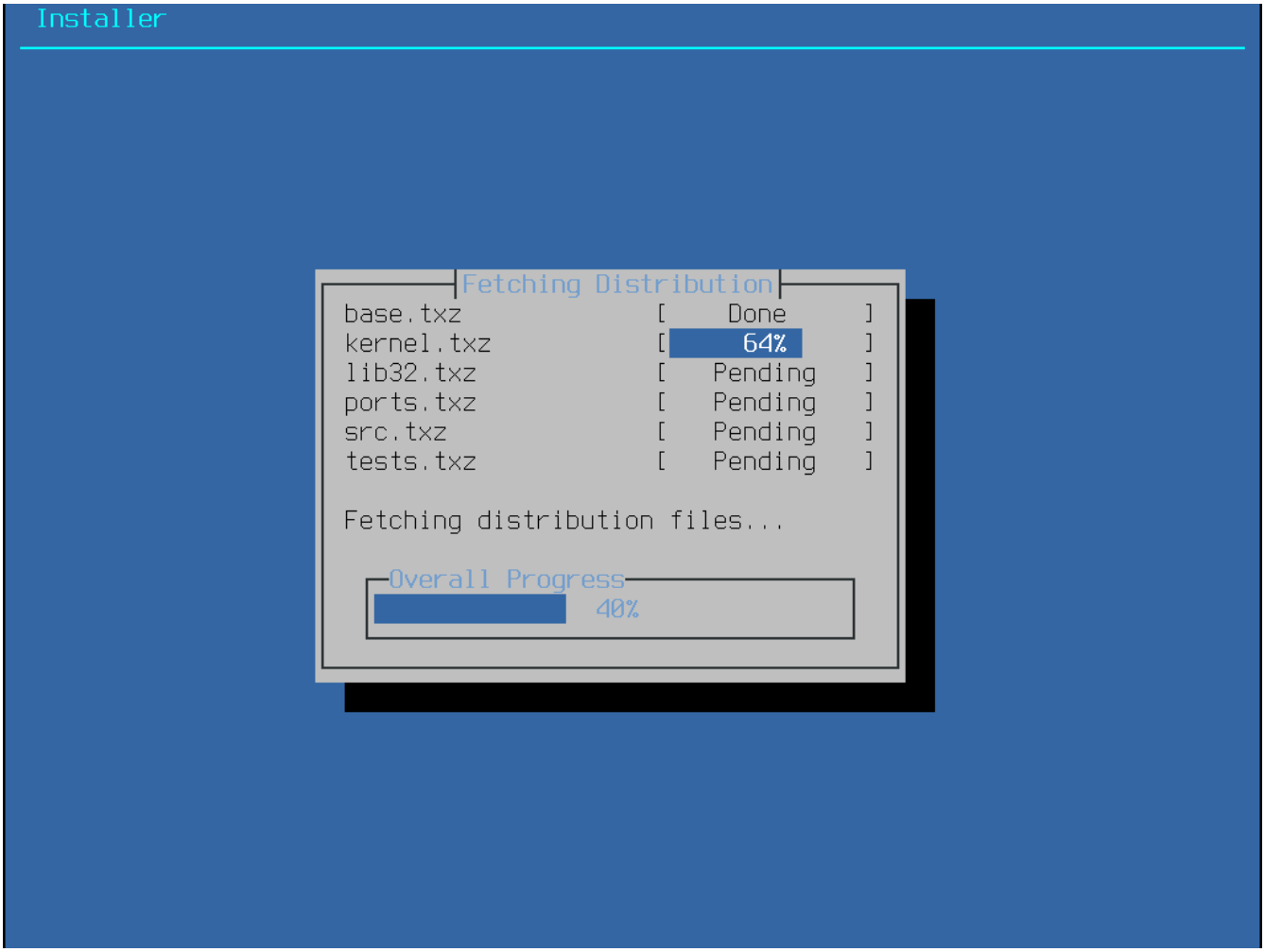


Figure 31. Récupération des fichiers de distribution

Ensuite, l'intégrité des fichiers de distribution est vérifiée pour s'assurer qu'ils n'ont pas été corrompus durant le téléchargement ou leur lecture à partir du support d'installation.

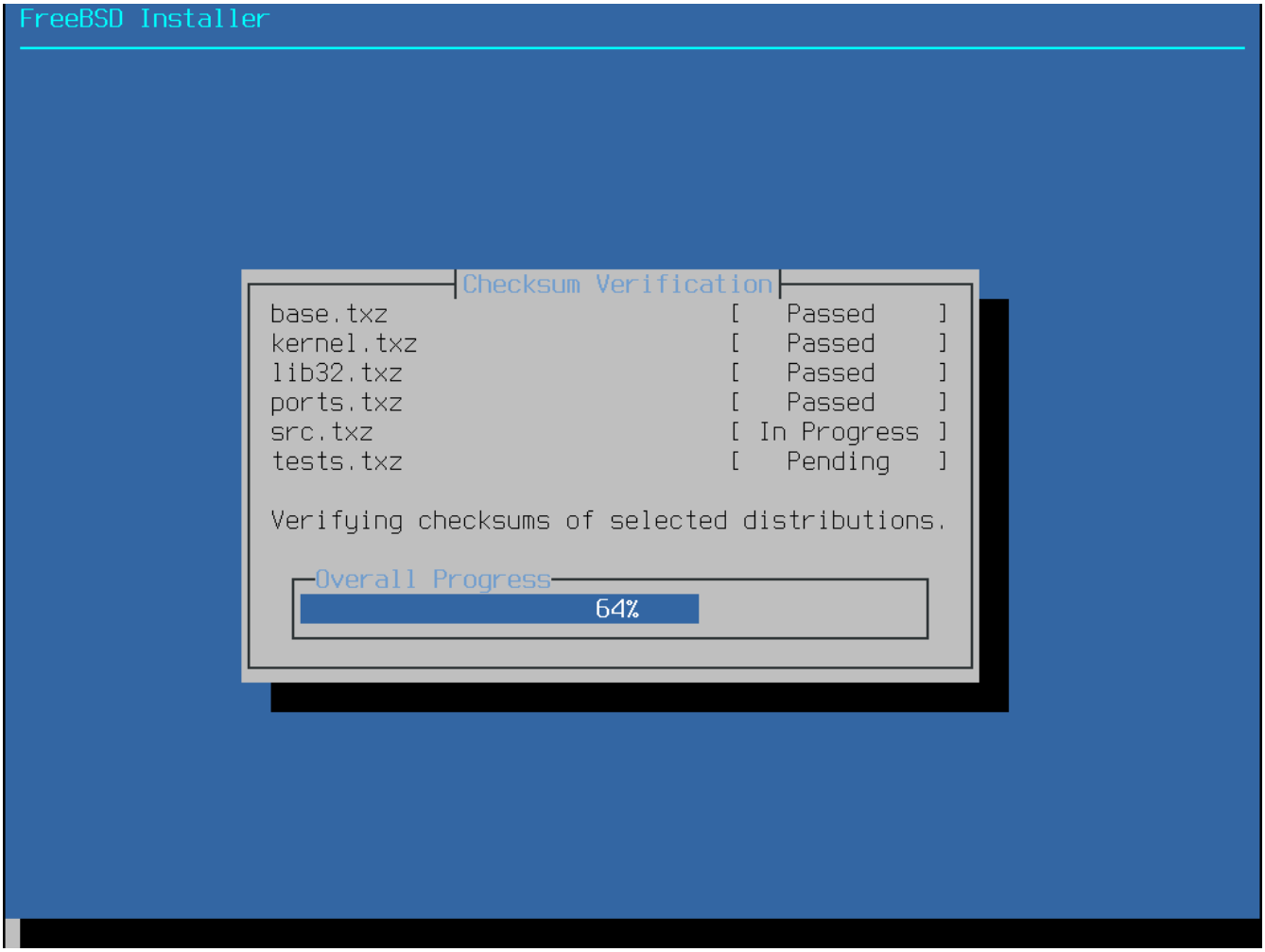


Figure 32. Vérification des fichiers de distribution

Enfin, les fichiers contrôlés sont décompressés sur le disque:

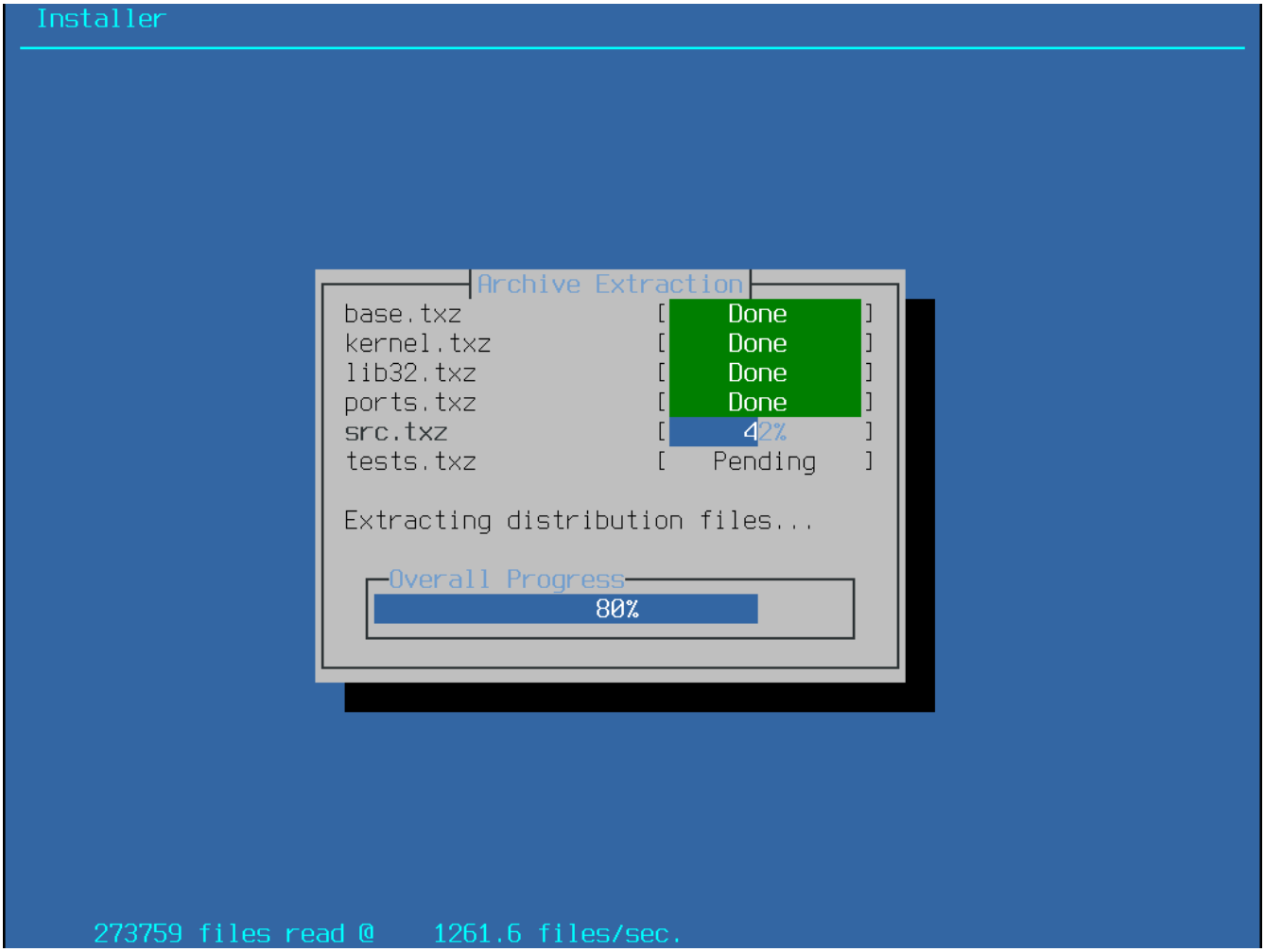


Figure 33. Décompression des fichiers de distribution

Une fois que tous les fichiers de distribution requis ont été décompressés, bsdinstall affichera le premier menu de post-installation. Cette série de menu est décrite dans la section suivante.

2.8. Comptes utilisateurs, fuseau horaire, services et renforcement de la sécurité

2.8.1. Définir le mot de passe de `root`

Tout d'abord, le mot de passe de l'utilisateur `root` doit être défini. Notez que lors de la saisie du mot de passe, les caractères tapés ne sont pas affichés sur l'écran. Après sa saisie, le mot de passe devra être entré une deuxième fois. Cela permet d'éviter les erreurs de frappe.

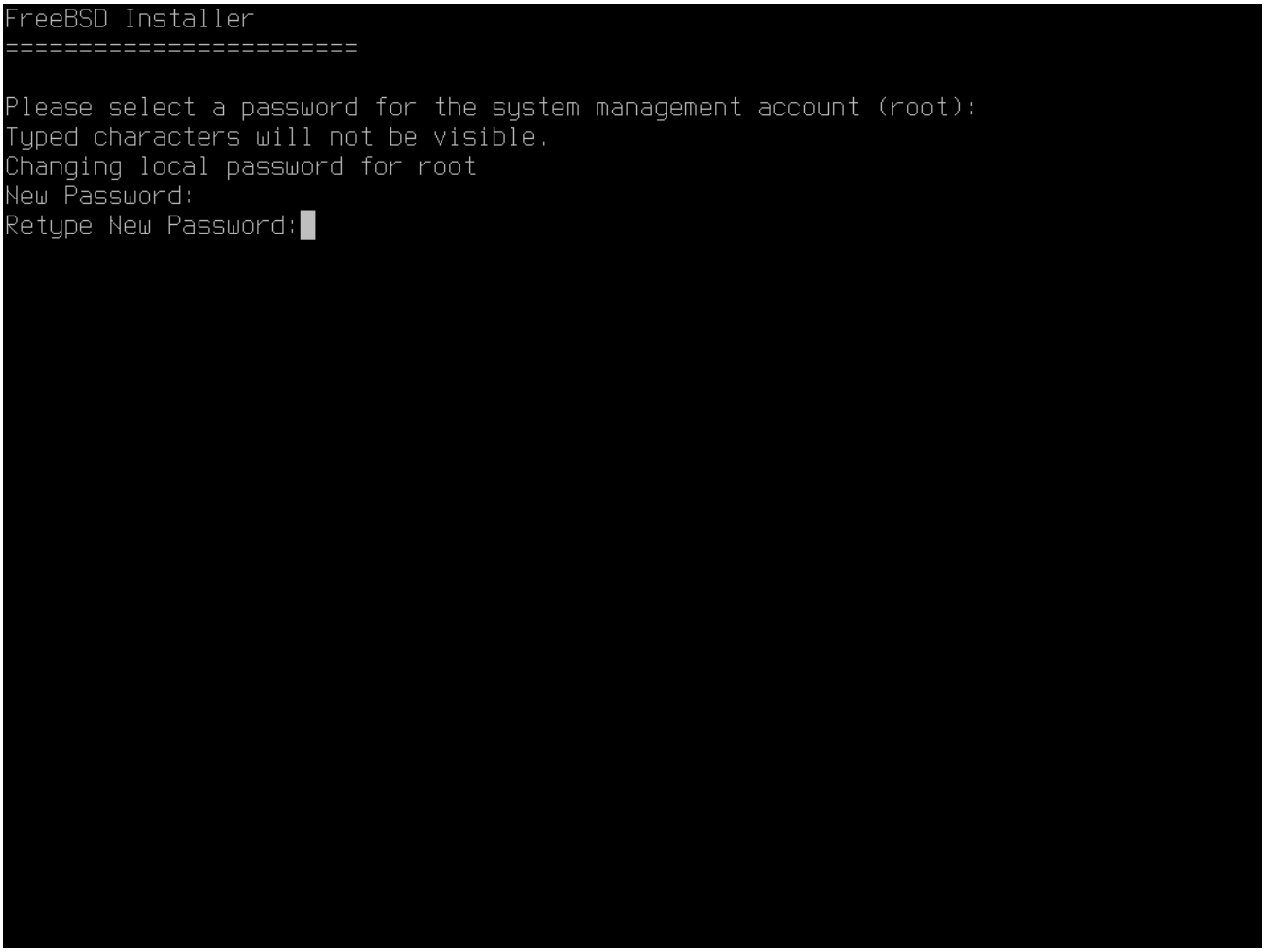


Figure 34. Saisie du mot de passe `root`

2.8.2. Réglage du fuseau horaire

La série de menus suivante permet de déterminer l'heure locale correcte en choisissant la région du monde, le pays et le fuseau horaire. Régler le fuseau horaire permet au système de corriger automatiquement l'heure lors des modifications régionales comme l'heure d'été ou d'hiver, et d'effectuer correctement toute autre modification relative au fuseau horaire.

L'exemple présenté ici concerne une machine située dans le fuseau horaire du centre de l'Espagne en Europe. Les choix pourront varier en fonction de la zone géographique.

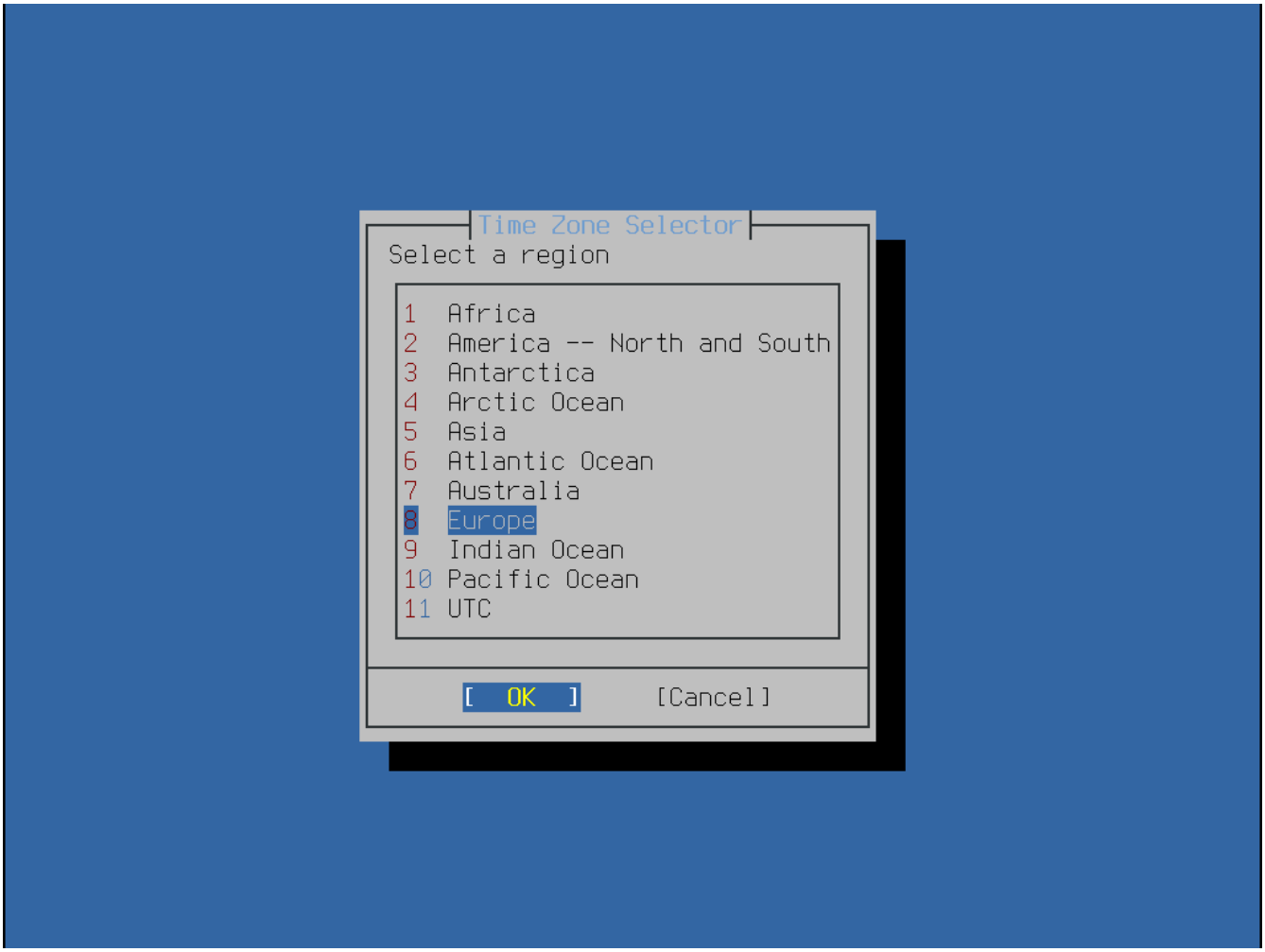


Figure 35. Sélectionner une région

La région appropriée est choisie en utilisant les touches flèches puis en appuyant sur `Entrée`.

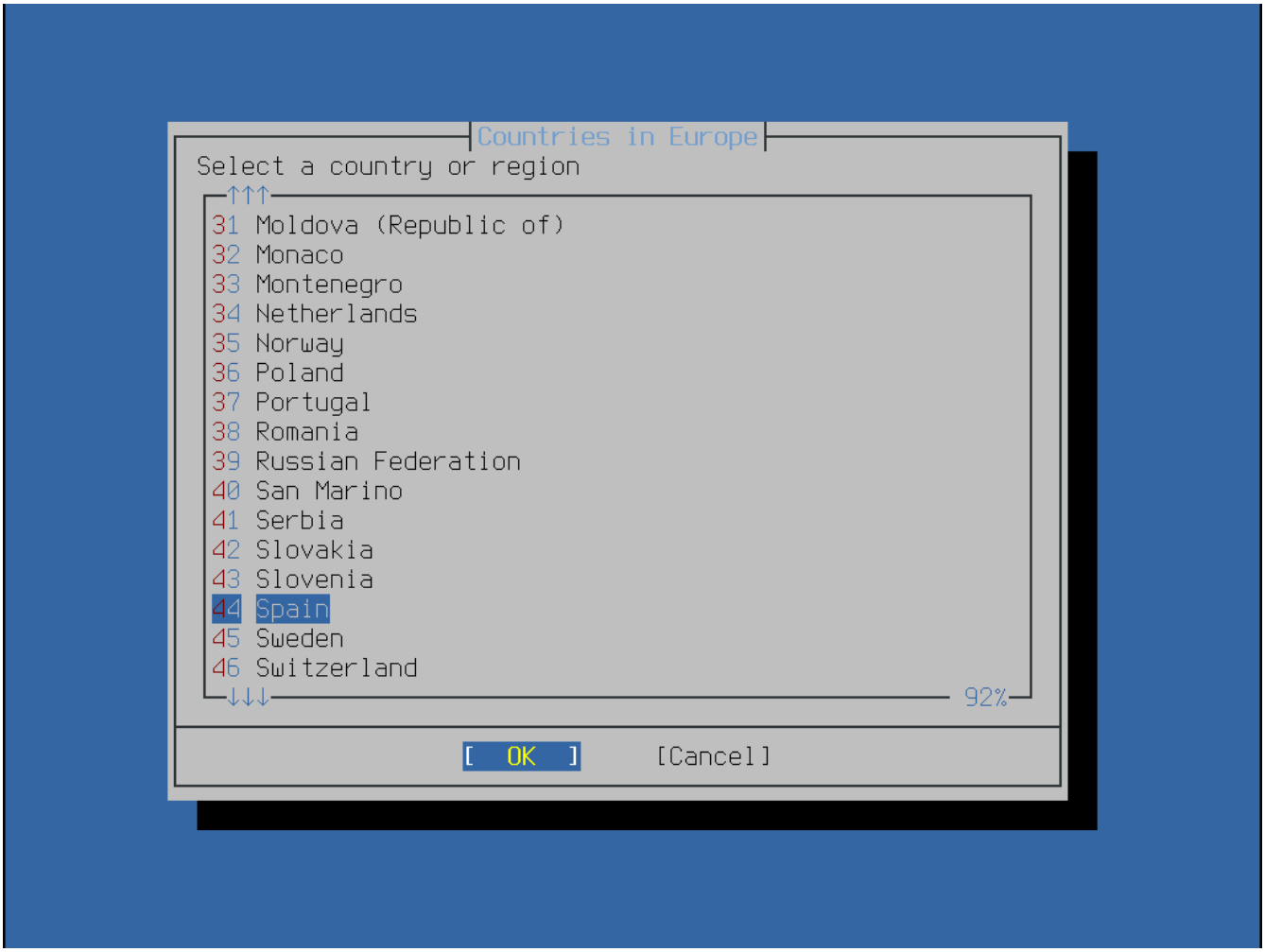


Figure 36. Sélection d'un pays

Sélectionner le pays approprié en utilisant les touches flèches et appuyer sur `Entrée`.

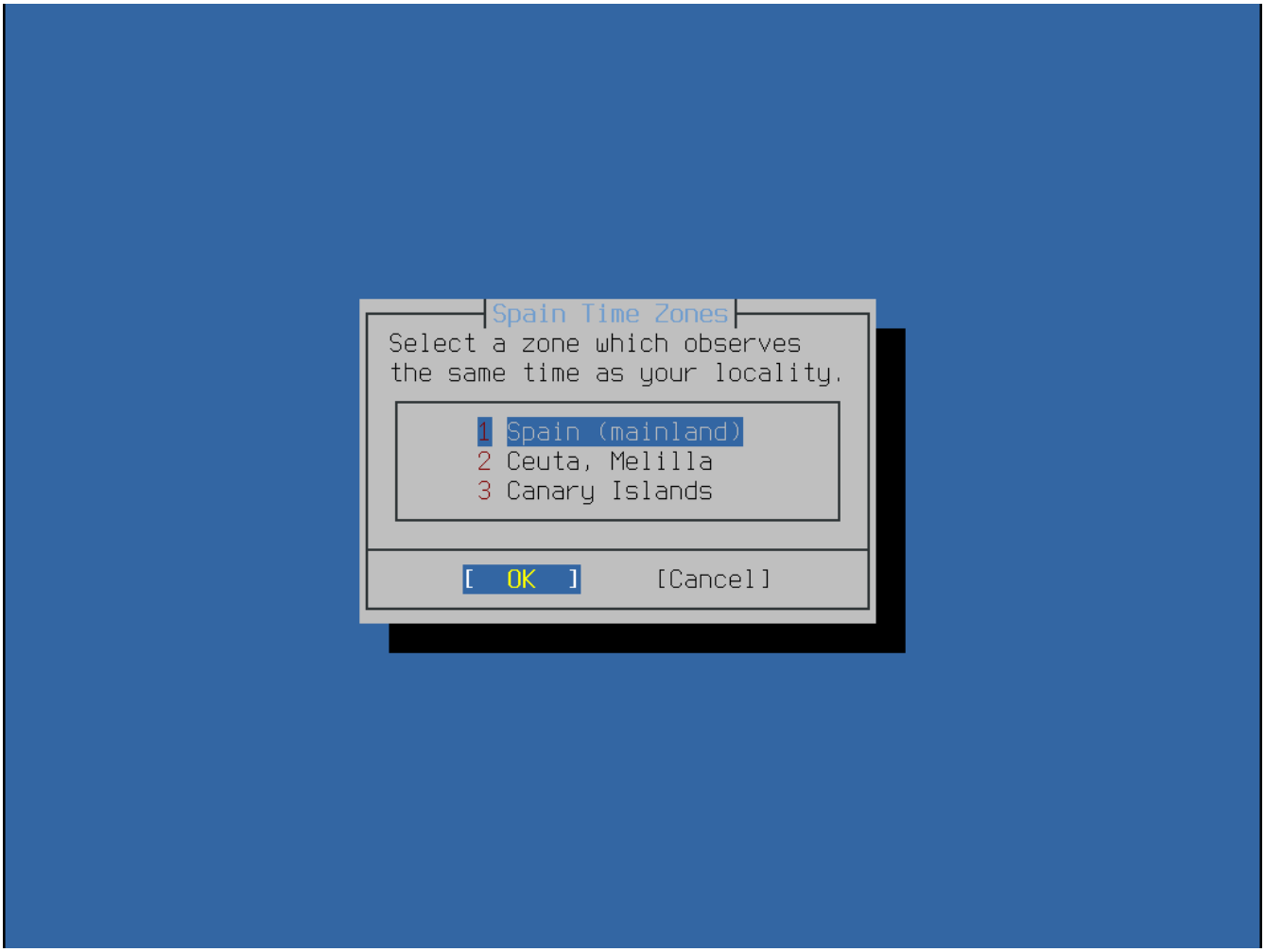


Figure 37. Sélection d'un fuseau horaire

Le fuseau horaire approprié est choisi en utilisant les touches flèches, puis en appuyant sur `Entrée`.

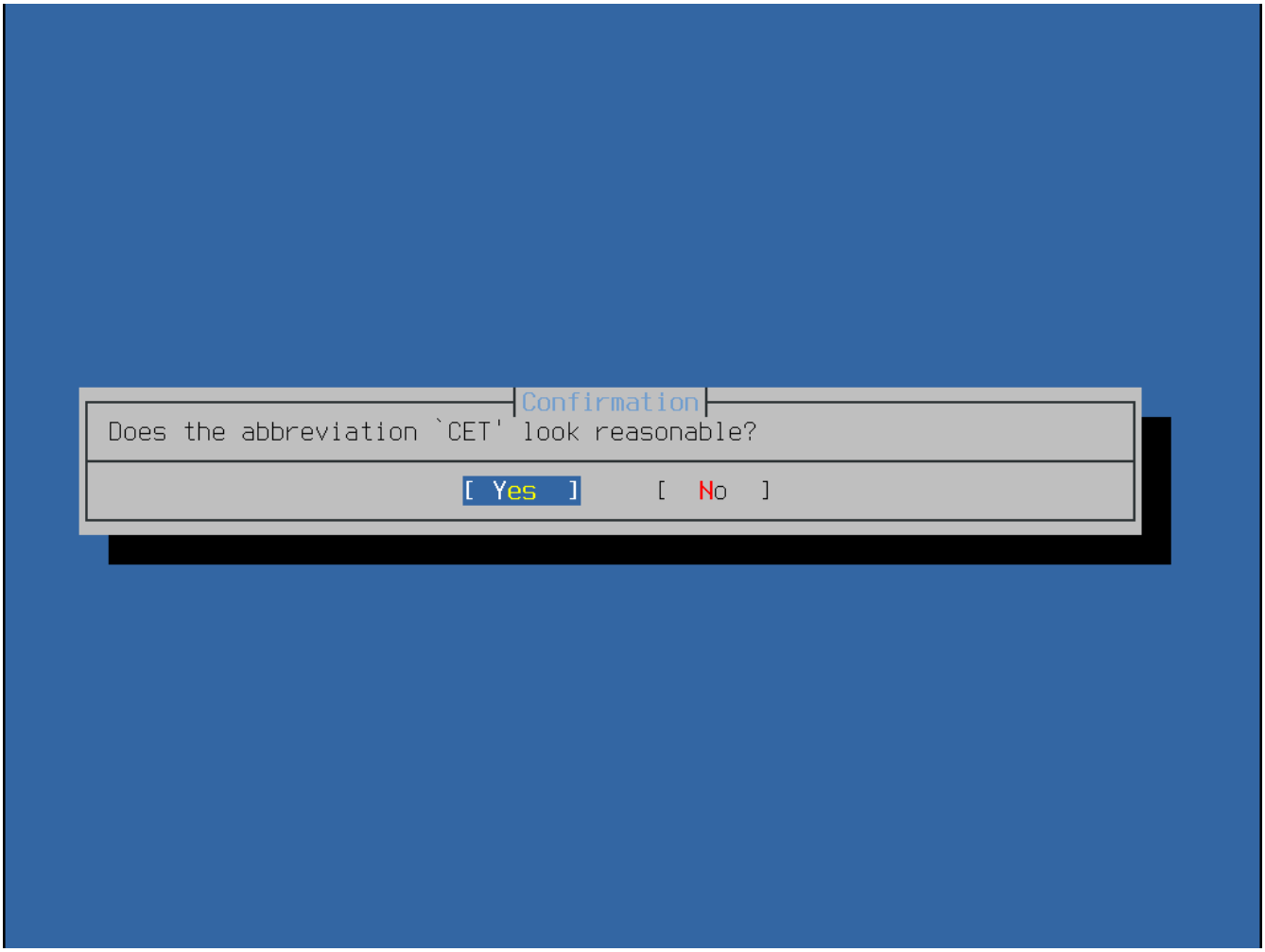


Figure 38. Confirmation du fuseau horaire

Confirmez que l'abréviation pour le fuseau horaire est correcte.

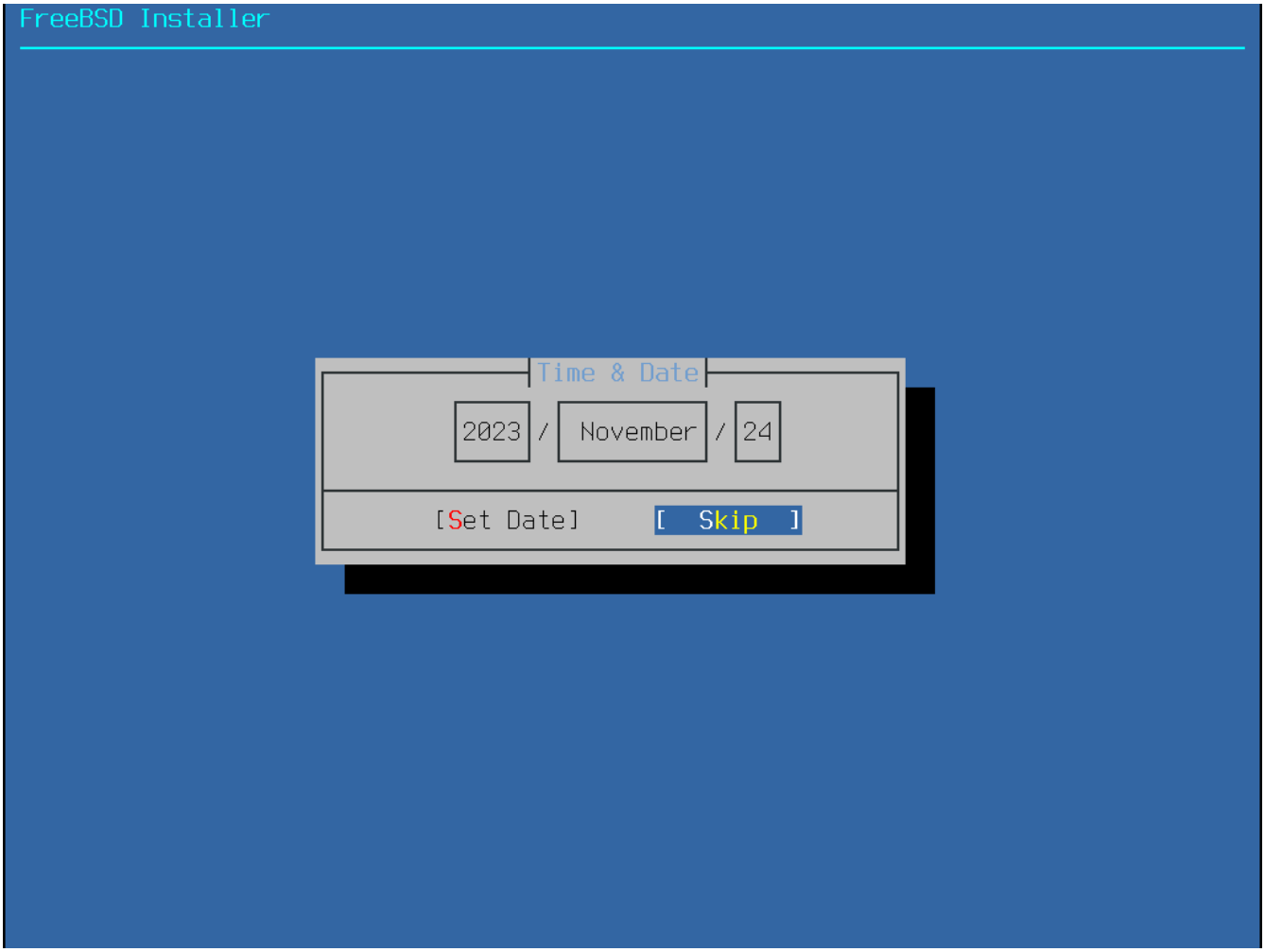


Figure 39. Sélection de la date

La date correcte est sélectionnée en utilisant les touches flèches puis en appuyant sur **[Set Date]**. Sinon, la sélection de la date peut être passée en appuyant sur **[Skip]**.

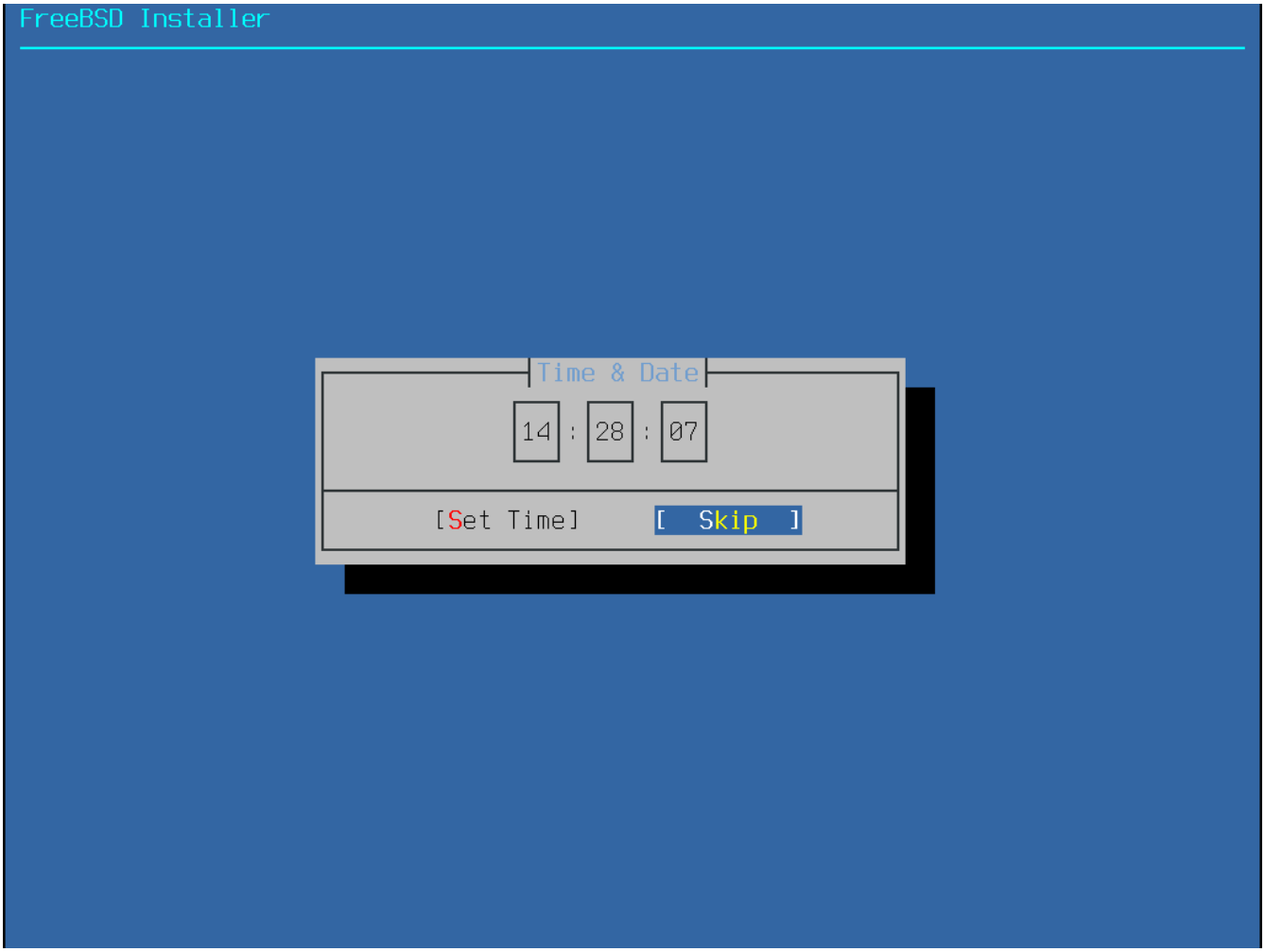


Figure 40. Configuration de l'heure

L'heure correcte est sélectionnée en utilisant les touches flèches puis en appuyant sur **[Set Time]**. Sinon, cette configuration peut être passée en appuyant sur **[Skip]**.

2.8.3. Activation des services

Le menu suivant est destiné à choisir quels services système seront lancés au démarrage. Tous ces services sont optionnels. Ne lancez que les services nécessaires au fonctionnement du système.

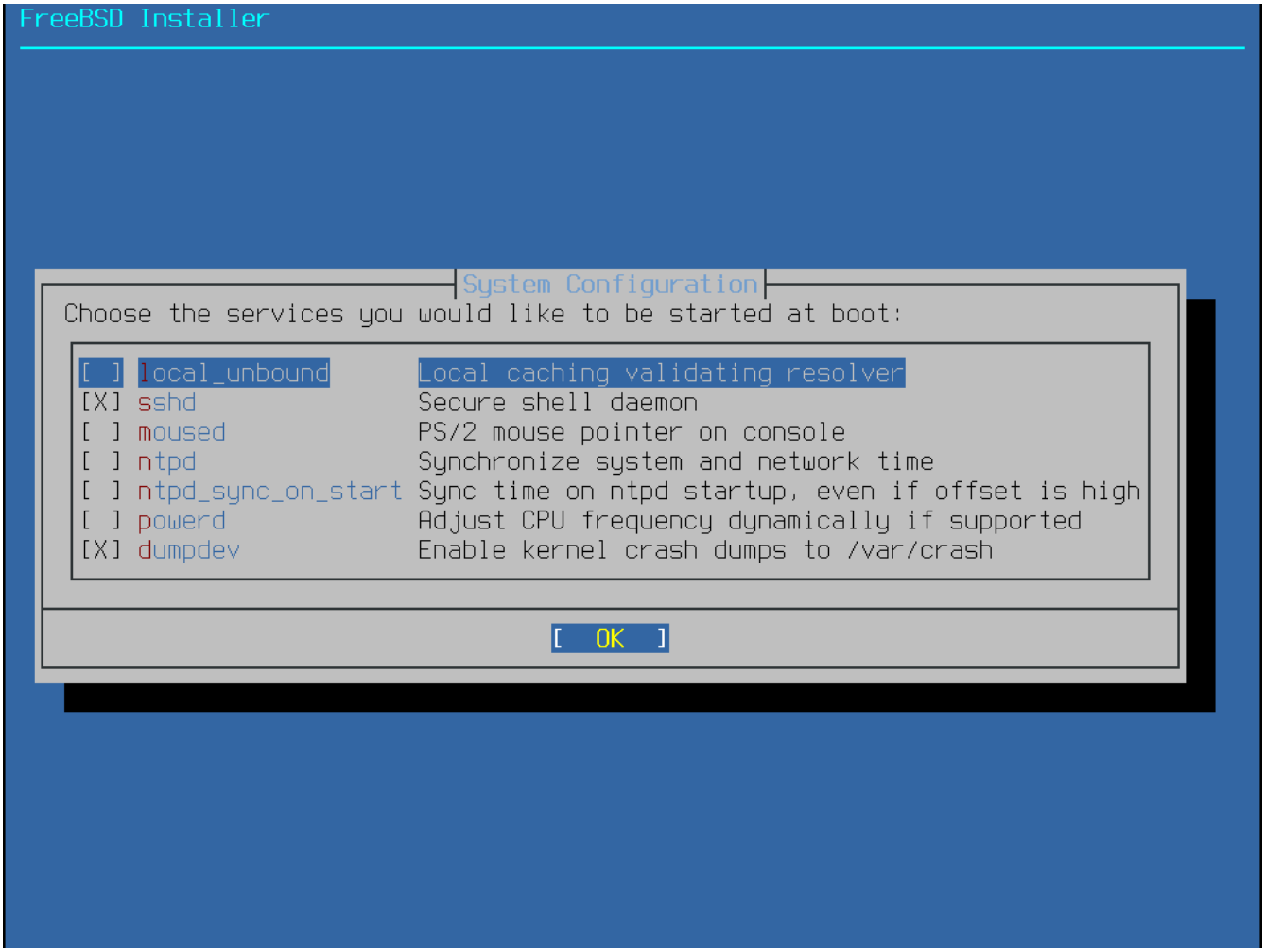


Figure 41. Sélection de services supplémentaires à activer

Voici un résumé des services pouvant être activés dans ce menu:

- `local_unbound` - Active le résolveur DNS local. Il est important de garder à l'esprit que c'est le résolveur du système de base qui n'est destiné à être utilisé uniquement qu'en tant que résolveur cache local. Si l'objectif est de mettre en place un résolveur pour tout le réseau, installer dns/unbound.
- `sshd` - Le daemon *Secure Shell* (SSH) est utilisé pour l'accès à un système à distance via une connexion chiffrée. Activez ce service que si le système doit être accessible pour l'ouverture de session à distance.
- `moused` - Activez ce service si la souris sera utilisée à partir de la console système en ligne de commande.
- `ntpdate` - Active la mise à l'heure automatique de l'horloge au démarrage. La fonction de ce programme est désormais disponible dans le daemon ntpd(8). Après une certaine période d'adaptation, l'utilitaire ntpdate(8) sera supprimé.
- `ntpd` - Le daemon du protocole de temps réseau (*Network Time Protocol*) (NTP) pour la synchronisation automatique de l'horloge. Activez ce service s'il y a un serveur Windows®, Kerberos, ou LDAP sur le réseau.
- `powerd` - Utilitaire de contrôle de la gestion de l'énergie du système pour le contrôle de la consommation en énergie.
- `dumpdev` - Activer les crash dumps peut s'avérer très utile pour déboguer les problèmes du

système, aussi les utilisateurs sont encouragés à activer les crashs dumps.

2.8.4. Activer les options de renforcement de la sécurité

Le menu suivant est utilisé pour sélectionner quelles options de sécurité seront activées. Toutes ces options sont facultatives. Mais leur utilisation est encouragée.

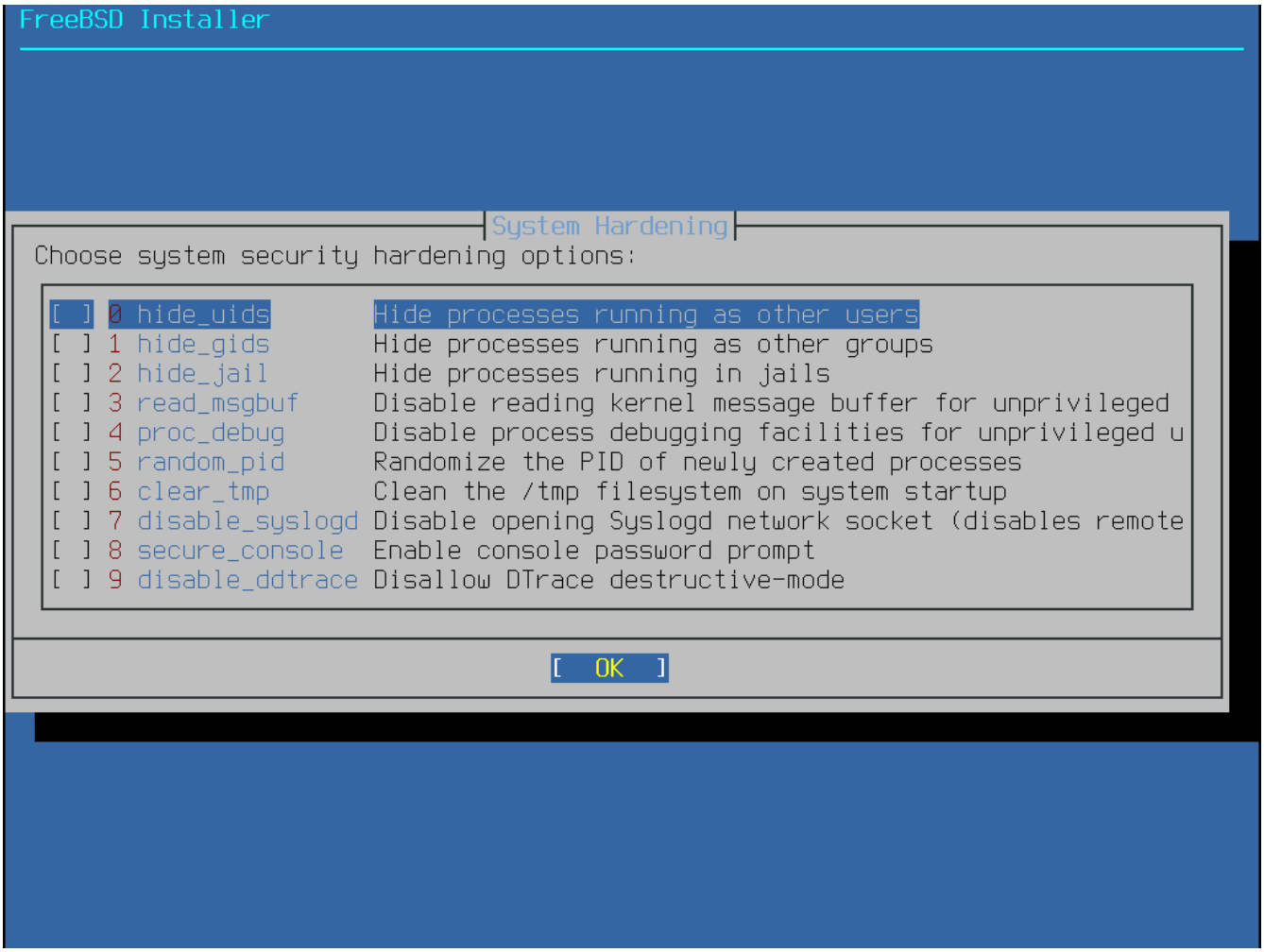


Figure 42. Sélection des options de renforcement de la sécurité

Voici un résumé des options qui peuvent être activées dans ce menu:

- `hide_uids` - Cache les processus en cours d'exécution sous des utilisateurs différents pour éviter que des utilisateurs non autorisés puissent voir les processus en cours d'exécution exécutés par d'autres utilisateurs (UID) évitant ainsi la fuite d'information.
- `hide_gids` - Cache les processus en cours d'exécution sous des groupes différents pour éviter que des utilisateurs non autorisés puissent voir les processus en cours d'exécution exécutés par d'autres groupes (GID) évitant ainsi la fuite d'information.
- `hide_jail` - Cache les processus en cours d'exécution dans des jails pour éviter que des utilisateurs non autorisés puissent voir les processus en cours d'exécution dans les jails.
- `read_msgbuf` - Désactive la lecture du tampon des messages du noyau pour les utilisateurs non autorisés en empêchant l'utilisation de dmesg(8) pour lire les messages du tampon de trace du noyau.
- `proc_debug` - La désactivation des fonctionnalités de débogage des processus pour les utilisateurs

non autorisés désactive une variété de services de débogage inter-processus non-privilégiés, cela comprend certaines fonctionnalités procfs, ptrace(), et and ktrace(). Veuillez noter que cela empêche également le fonctionnement d'outils de débogage pour les utilisateurs non autorisés comme lldb(1), truss(1), procstat(1), ainsi que certaines fonctionnalités de débogage intégrées dans certains langages comme PHP, etc.

- `random_pid` - Rend aléatoire le choix de la valeur du PID de chaque nouveau processus.
- `clear_tmp` - Nettoie le répertoire /tmp au démarrage du système.
- `disable_syslogd` - Désactive l'ouverture d'un socket réseau syslogd. Par défaut, FreeBSD exécute syslogd de manière sécurisée avec le paramètre `-s`. Cela évite que le daemon écoute sur le port 514 les requêtes UDP entrantes. Avec cette option activée syslogd sera exécuté avec les paramètres `-ss` ce qui empêche l'ouverture de ports par syslogd. Pour des informations supplémentaires, consultez la page de manuel syslogd(8).
- `disable_sendmail` - Désactive l'agent de transfert de courrier Sendmail.
- `secure_console` - Quand cette option est activée, l'invite réclame le mot de passe `root` lors de l'entrée en mode utilisateur unique.
- `disable_ddtrace` - DTrace peut fonctionner dans un mode qui affectera le noyau en exécution. Des actions destructives ne pourront pas être utilisées sauf si elles ont été explicitement autorisées. Pour activer cette option lors de l'utilisation de DTrace utilisez le paramètre `-w`. Pour des informations supplémentaires, consultez la page de manuel dtrace(1).

2.8.5. Ajouter des utilisateurs

Le menu suivant demande de créer au moins un compte utilisateur. Il est recommandé d'utiliser un compte utilisateur pour l'ouverture de session sur le système plutôt que d'employer le compte `root`. Quand on utilise une session `root`, il n'existe aucune limite ou protection quant à ce qui peut être fait. Ouvrir une session en tant qu'utilisateur normal est plus sûr et plus sécurisé.

Sélectionner **[Yes]** pour ajouter de nouveaux utilisateurs.

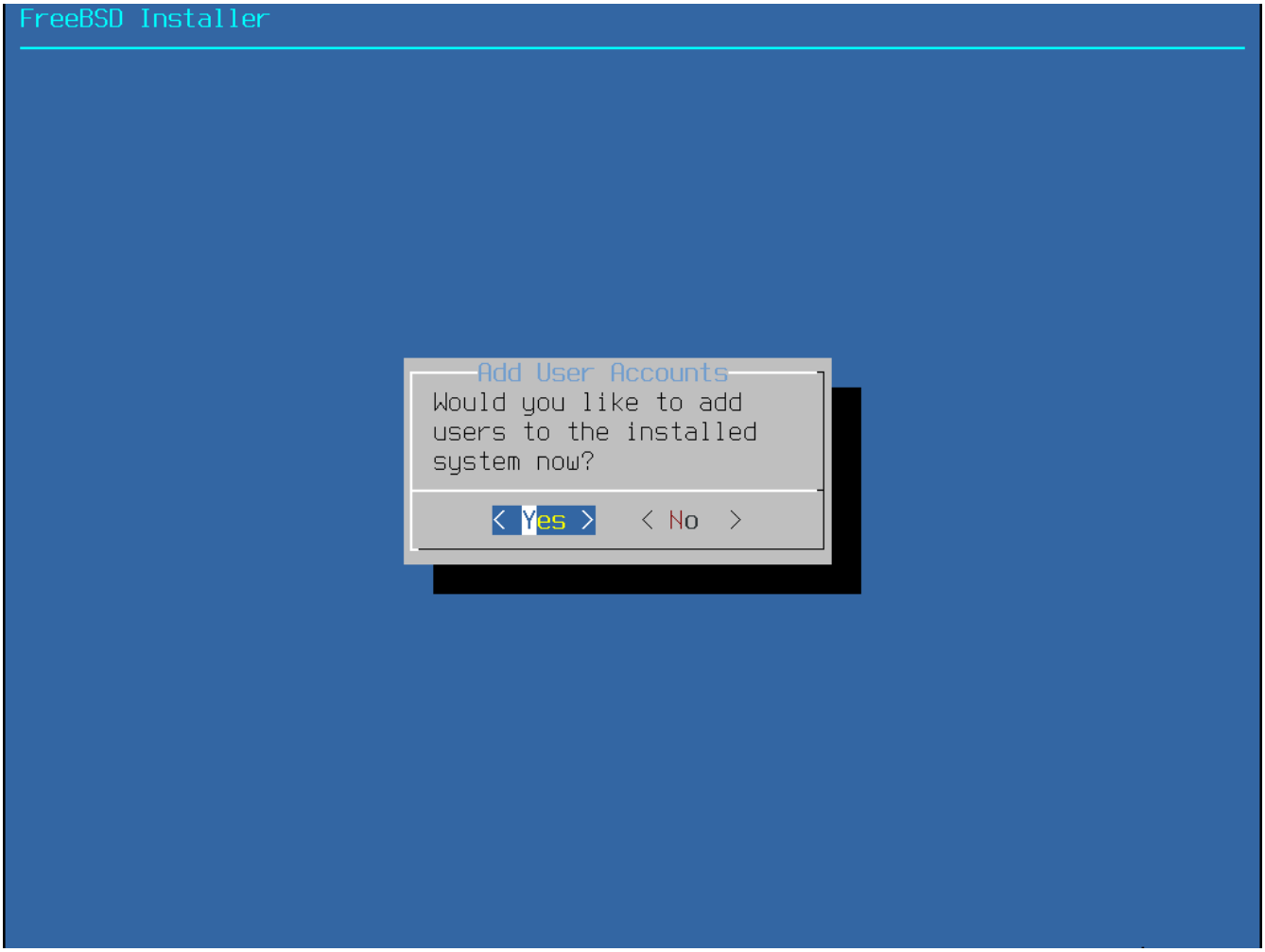


Figure 43. Ajout de comptes utilisateur

Suivez les instructions et saisissez les informations demandées pour le compte utilisateur à ajouter. L'exemple donné dans Entrée des informations utilisateur créé le compte utilisateur `asample`.

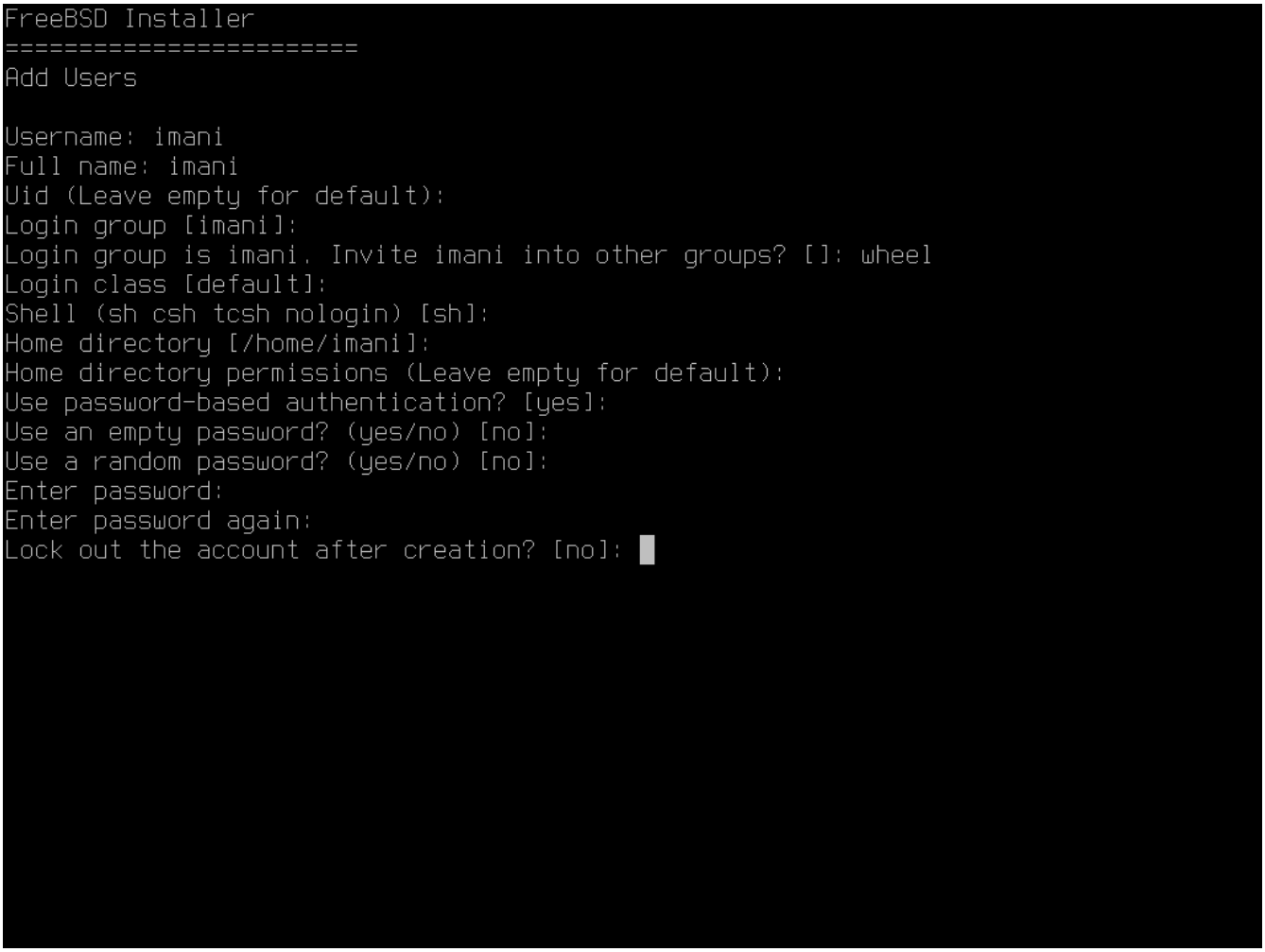


Figure 44. Entrée des informations utilisateur

Voici un résumé des informations à saisir:

- `Username` - Le nom d'utilisateur ou identifiant que l'utilisateur entrera pour ouvrir une session. Une convention courante est d'utiliser la première lettre du prénom associé au nom, tant que chaque nom d'utilisateur reste unique sur le système. Le nom d'utilisateur est sensible à la casse et ne devrait pas contenir d'espace.
- `Full name` - Le nom complet de l'utilisateur. Il peut contenir des espaces et est utilisé comme description du compte utilisateur.
- `Uid` - L'identifiant numérique pour cet utilisateur. En général, ce champ est laissé vide de façon à ce que le système assigne par lui-même une valeur.
- `Login group` - Le groupe de l'utilisateur. Généralement il est laissé vide pour accepter le choix par défaut.
- `Invite user into other groups?` - Groupes supplémentaires pour lesquels l'utilisateur sera également ajouté comme membre. Si l'utilisateur a besoin d'un accès administrateur, tapez `wheel` ici.
- `Login class` - Généralement laissé vide pour accepter la valeur par défaut.
- `Shell` - Tapez un des noms listés pour choisir l'interpréteur de commande de l'utilisateur. Consulter Interpréteurs de commandes - "Shells" pour plus d'information sur les interpréteurs de commande.

- `Home directory` - Le répertoire de l'utilisateur. La valeur par défaut est, en général, correcte.
- `Home directory permissions` - Les permissions sur le répertoire utilisateur. La valeur par défaut est, en général, correcte.
- `Use password-based authentication?` - En général `yes` de manière à ce que l'utilisateur soit invité à entrer son mot de passe à l'ouverture de session.
- `Use an empty password?` - En général `no` car c'est un problème de sécurité d'avoir un mot de passe vide.
- `Use a random password?` - En général `no` de manière à ce que l'utilisateur puisse entrer son propre mot de passe à l'invite suivante.
- `Enter password` - Le mot de passe pour cet utilisateur. Les caractères tapés n'apparaîtront pas sur l'écran.
- `Enter password again` - Le mot de passe doit à nouveau être saisi pour vérification.
- `Lock out the account after creation?` - En général `no` de manière à ce que l'utilisateur puisse ouvrir une session.

Après avoir tout saisi, un résumé est affiché pour vérification. Si une erreur a été faite, entrez `no` et recommencez. Si tout est correct, entrez `yes` pour créer ce nouvel utilisateur.

```
FreeBSD Installer
=======================
Add Users

Username: imani
Full name: imani
Uid (Leave empty for default):
Login group [imani]:
Login group is imani. Invite imani into other groups? []: wheel
Login class [default]:
Shell (sh csh tcsh nologin) [sh]:
Home directory [/home/imani]:
Home directory permissions (Leave empty for default):
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]:
Use a random password? (yes/no) [no]:
Enter password:
Enter password again:
Lock out the account after creation? [no]:
Username   : imani
Password   : *****
Full Name  : imani
Uid        : 1001
Class      :
Groups     : imani wheel
Home       : /home/imani
Home Mode  :
Shell      : /bin/sh
Locked     : no
OK? (yes/no) [yes]:
adduser: INFO: Successfully added (imani) to the user database.
Add another user? (yes/no) [no]:
```

Figure 45. Quitter la gestion des utilisateurs et des groupes

S'il y a d'autres utilisateurs à ajouter, répondez `yes` à la question `Add another user?`. Entrez `no` pour terminer l'ajout d'utilisateurs et continuer l'installation.

Pour plus d'information sur l'ajout d'utilisateurs et leur gestion, consultez Synopsis.

2.8.6. Configuration finale

Après avoir tout installé et configuré, une dernière chance de modifier les réglages est proposée.

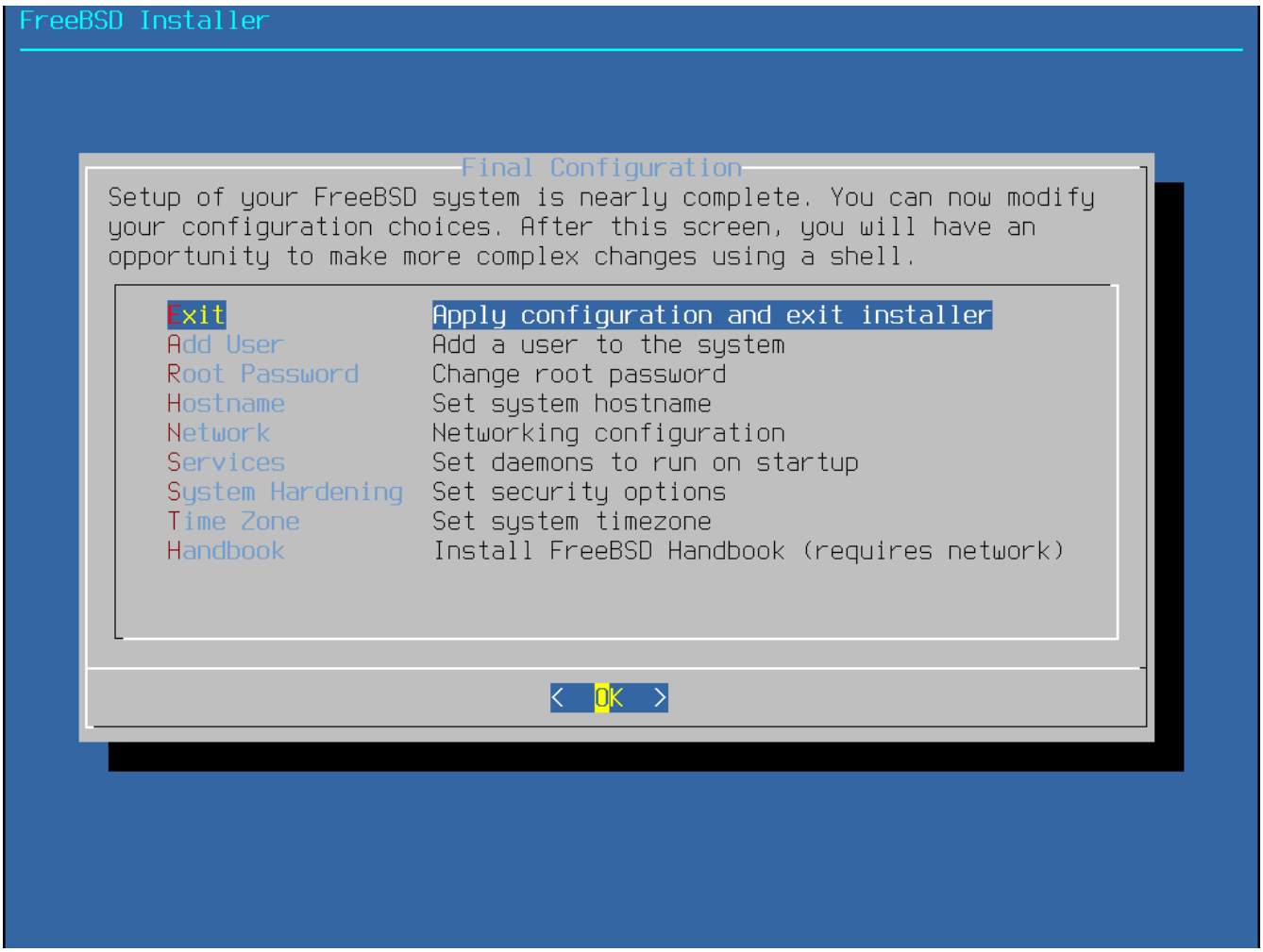


Figure 46. Configuration finale

Utilisez ce menu pour effectuer des changements ou toute configuration supplémentaire avant de terminer l'installation.

- `Add User` - Décrit dans la Ajouter des utilisateurs.
- `Root Password` - Décrit dans la Définir le mot de passe de `root`.
- `Hostname` - Décrit dans la Configurer le nom de la machine.
- `Network` - Décrit dans la Configuration des interfaces réseau.
- `Services` - Décrit dans la Activation des services.
- `System Hardening` - Décrit dans la Activer les options de renforcement de la sécurité.
- `Time Zone` - Décrit dans la Réglage du fuseau horaire.
- `Handbook` - Télécharge et installe le Manuel FreeBSD.

Une fois la configuration finale achevée, sélectionnez **[Exit]**.

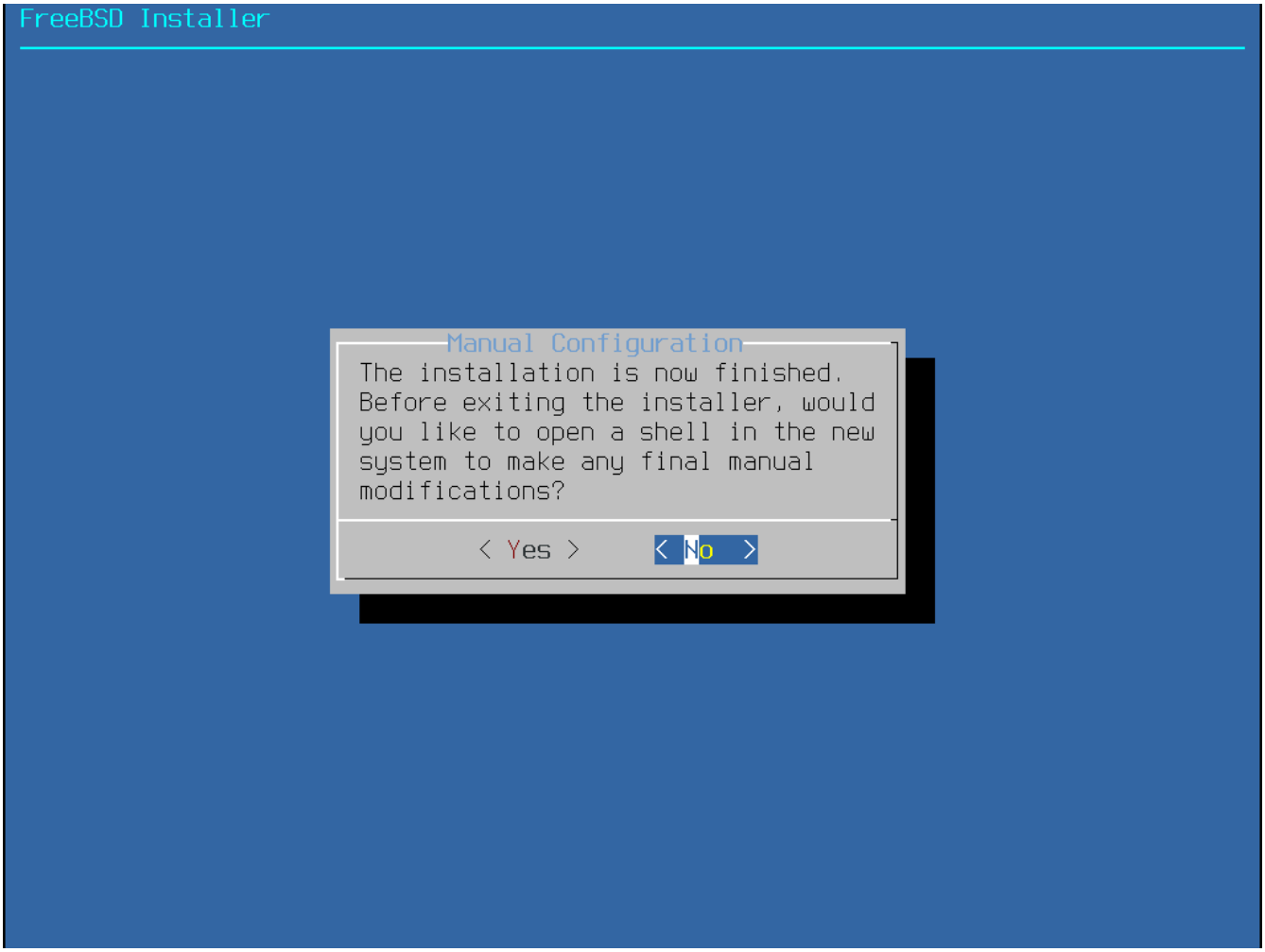


Figure 47. Configuration manuelle

bsdinstall demandera s'il y a des éléments supplémentaires à configurer avant le redémarrage sur le nouveau système. Sélectionner **[Yes]** pour quitter vers un interpréteur de commande, ou **[No]** pour passer à la dernière étape d'installation.

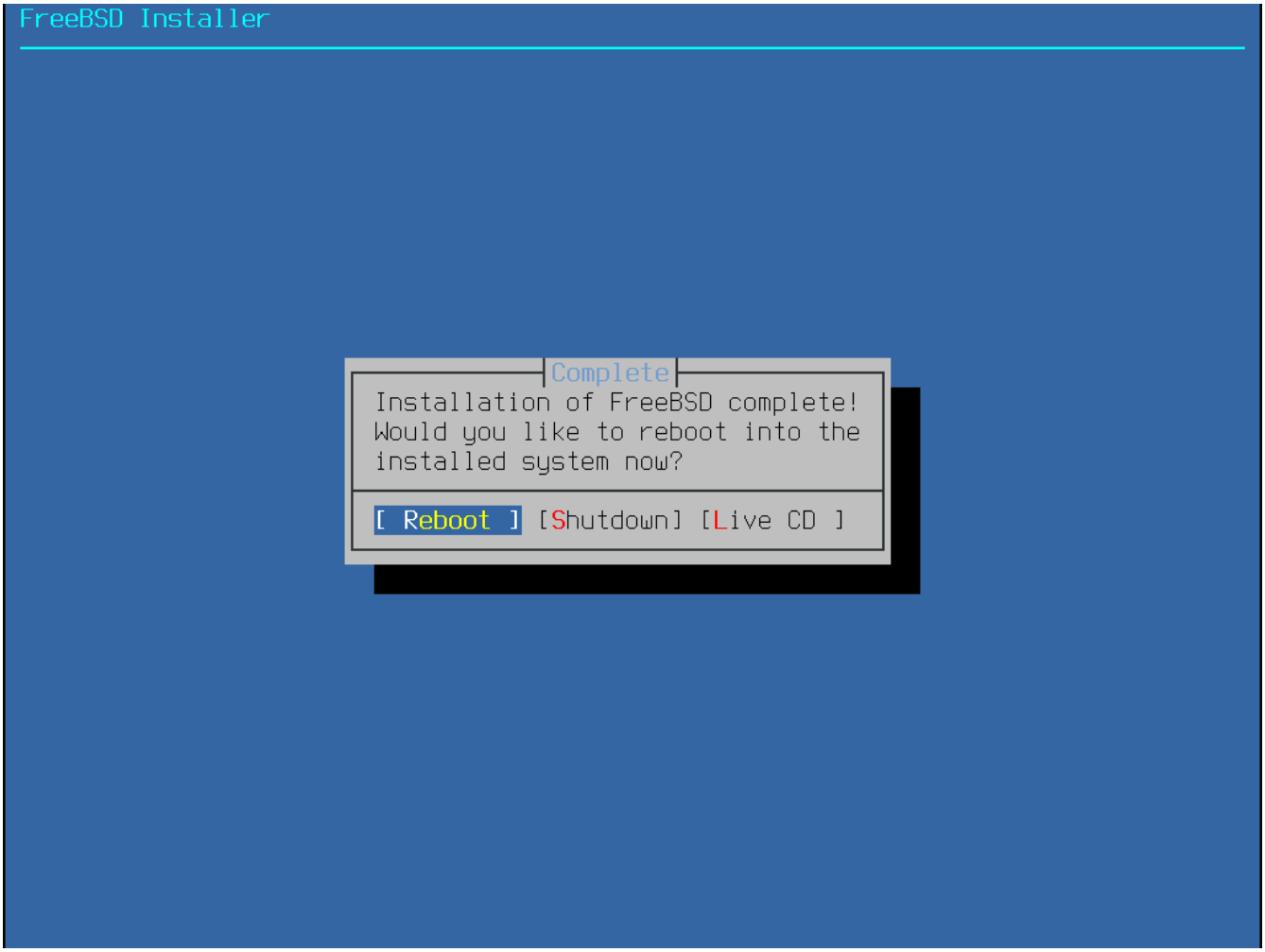


Figure 48. Achever l'installation

Si d'autre configuration ou une configuration spécifique est nécessaire, choisissez **[Live CD]** pour démarrer dans le mode du CD Live.

Si l'installation est achevée, sélectionnez **[Reboot]** pour redémarrer l'ordinateur et démarrer le nouveau système FreeBSD. N'oubliez pas de retirer le support d'installation de FreeBSD ou l'ordinateur risque de redémarrer dessus à nouveau.

Lors du démarrage de FreeBSD, des messages d'information sont affichés. Une fois que le système a achevé son démarrage, une invite de session est affichée. A l'invite `login:`, saisissez le nom d'utilisateur ajouté lors de l'installation. Evitez d'ouvrir des sessions en tant que `root`. Consultez Le compte super-utilisateur pour des instructions sur comment devenir super-utilisateur quand un accès administrateur est nécessaire.

Les messages qui ont défilé lors du démarrage peuvent être à nouveau visualisés en appuyant sur `Scroll-Lock` (ou `Arrêtdéfil`) pour activer le *défilement arrière du tampon des messages*. Les touches `PgUp`, `PgDn`, et les touches fléchées pourront être utilisées pour remonter dans les messages. Une fois terminé, appuyez à nouveau sur `Scroll-Lock` pour déverrouiller l'écran et fera revenir à l'affichage normal de la console. Pour revoir ces messages quand le système en fonctionnement depuis un certain temps, tapez `less /var/run/dmesg.boot` à partir de l'invite. Appuyez sur `q` pour retourner à l'invite de commande après la visualisation.

Si sshd a été activé dans Sélection de services supplémentaires à activer, le premier démarage pourra être un peu plus lent en raison de la génération des clés RSA et DSA. Les démarrages

suivants seront plus rapides. Les empreintes des clés seront affichées, comme montré dans cet exemple:

```
Generating public/private rsa1 key pair.
Your identification has been saved in /etc/ssh/ssh_host_key.
Your public key has been saved in /etc/ssh/ssh_host_key.pub.
The key fingerprint is:
10:a0:f5:af:93:ae:a3:1a:b2:bb:3c:35:d9:5a:b3:f3 root@machine3.example.com
The key's randomart image is:
+--[RSA1 1024]----+
|    o..          |
|   o . .         |
|  .   o          |
|       o         |
|    o   S        |
|   + + o         |
|o . + *          |
|o+ ..+ .         |
|==o..o+E         |
+-----------------+
Generating public/private dsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
7e:1c:ce:dc:8a:3a:18:13:5b:34:b5:cf:d9:d1:47:b2 root@machine3.example.com
The key's randomart image is:
+--[ DSA 1024]----+
|       ..     . .|
|      o  .   . + |
|     . ..   . E .|
|    . .  o o . . |
|     +  S = .    |
|    +  . = o     |
|     +  . * .    |
|    . .  o .     |
|      .o. .      |
+-----------------+
Starting sshd.
```

Consulter OpenSSH pour plus d'information au sujet des empreintes et de SSH.

FreeBSD n'installe pas d'environnement graphique par défaut, mais de nombreux sont disponibles. Consultez Le système X Window pour plus d'information au sujet de l'installation et la configuration d'un gestionnaire de fenêtres graphique.

Arrêter proprement un ordinateur sous FreeBSD aide à protéger les données et même le matériel de tout dommage. *Ne coupez pas l'alimentation tant que le système n'est pas correctement arrêté!* Si l'utilisateur est membre du groupe `wheel`, passez en super-utilisateur en tapant `su` sur la ligne de commande et en entrant le mot de passe de `root`. Ensuite, utilisez la commande `shutdown -p now` et

le système se fermera proprement, et si le matériel le support, s'éteindra lui-même.

2.9. Interfaces réseau

2.9.1. Configuration des interfaces réseau

Ensuite, est affichée une liste des interfaces réseaux trouvées sur l'ordinateur. Sélectionner l'interface à configurer.

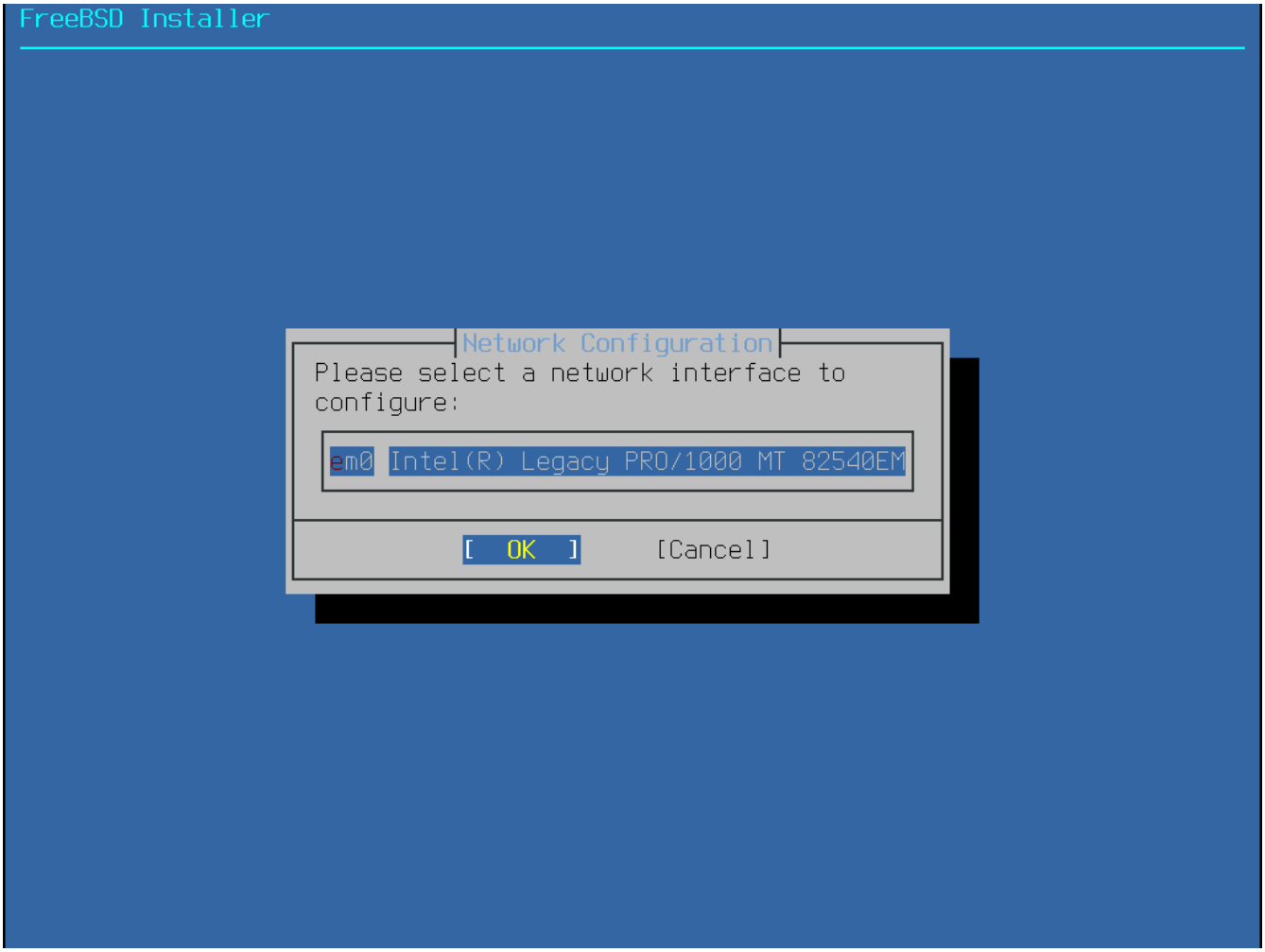


Figure 49. Choix d'une interface réseau

Si une interface réseau Ethernet est choisie, le programme d'installation passera au menu montré dans la Sélection d'un fonctionnement réseau en IPv4. Si une interface réseau sans-fil est choisie, le système recherchera les points d'accès sans-fil:

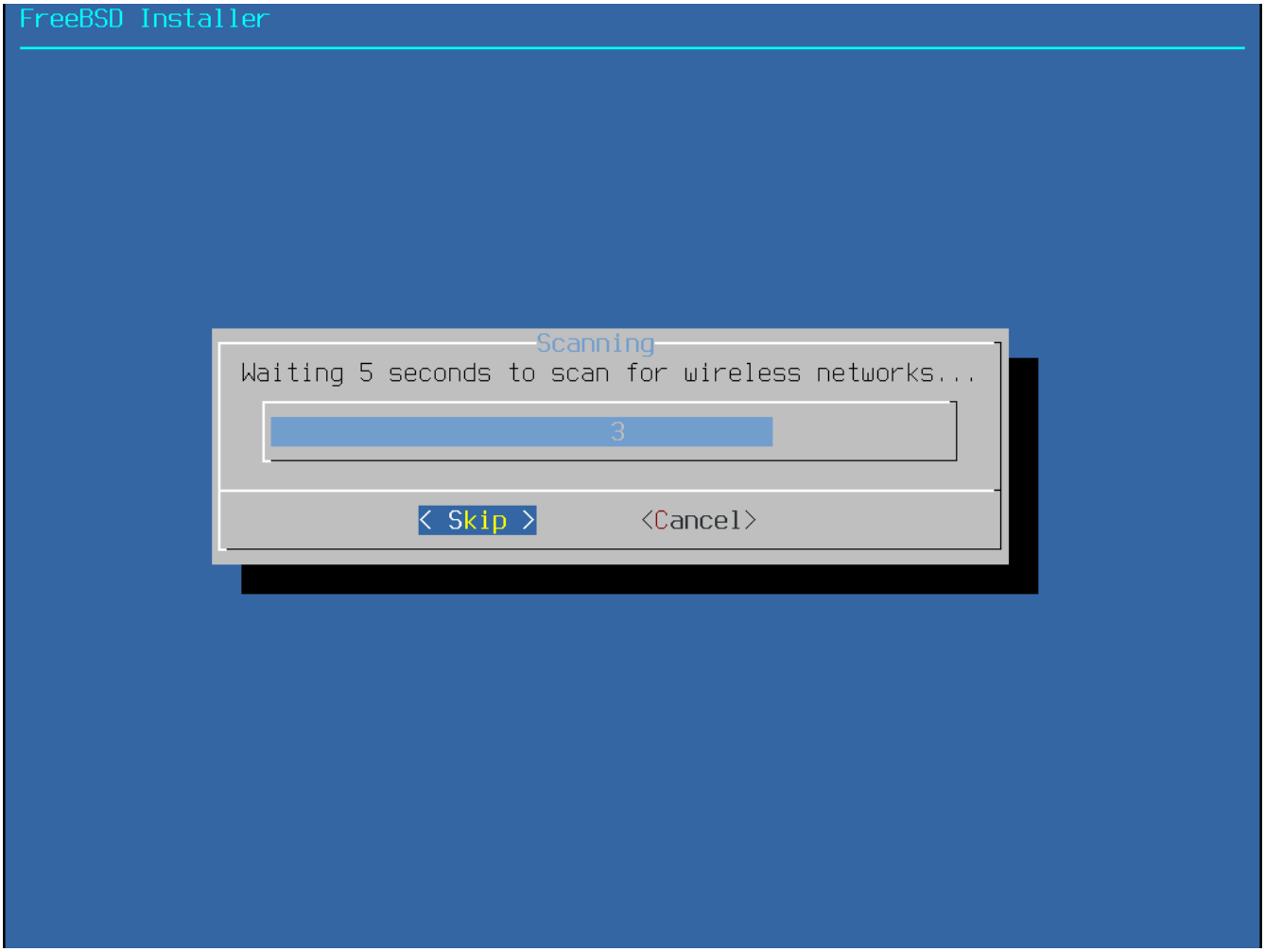


Figure 50. Recherche des points d'accès sans-fil

Les réseaux sans-fil sont identifiés par un *Service Set Identifier* (SSID), qui est un nom, court, unique donné à chaque réseau. Les SSIDs trouvés durant la recherche sont affichés, suivis par une description des types de chiffrement disponibles pour chaque réseau. Si le SSID désiré n'apparaît pas dans la liste, sélectionner **[Rescan]** pour rechercher à nouveau. Si le réseau désiré n'apparaît toujours pas, vérifiez qu'il n'y a pas de problèmes d'antenne ou essayez de rapprocher l'ordinateur du point d'accès. Rescannez après chaque modification.

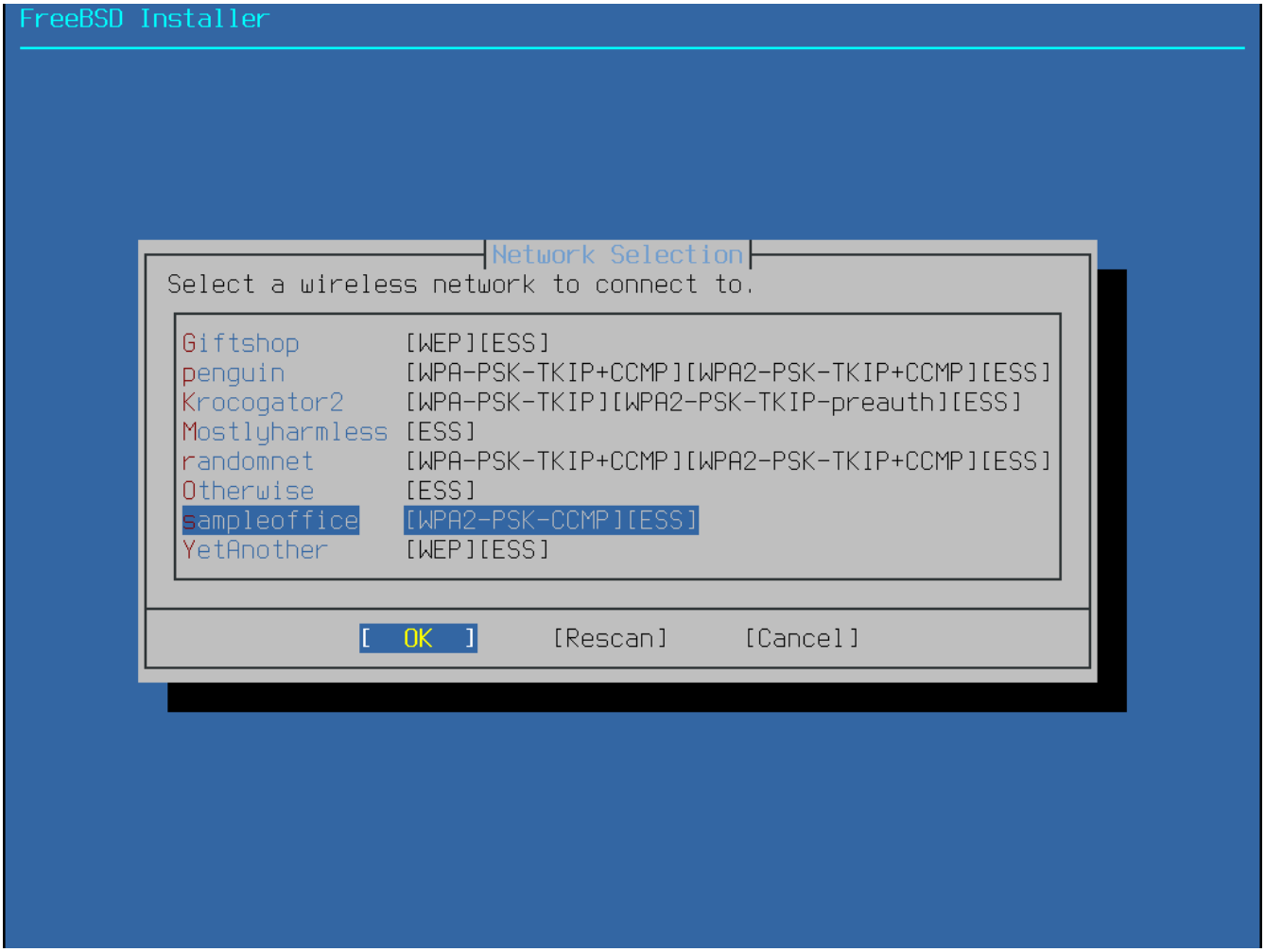


Figure 51. Sélection d'un réseau sans-fil

Ensuite, entrer les informations de chiffrement pour se connecter au réseau sans-fil sélectionné. Le chiffrement WPA2 est fortement recommandé sachant que les chiffrements plus anciens, comme WEP, offrent peu de sécurité. Si le réseau utilise WPA2, entrez le mot de passe également connu sous le nom de *Pre-Shared Key* (PSK). Pour des raisons de sécurité, les caractères tapés dans la boîte de saisie apparaissent sous la forme d'astérisques.

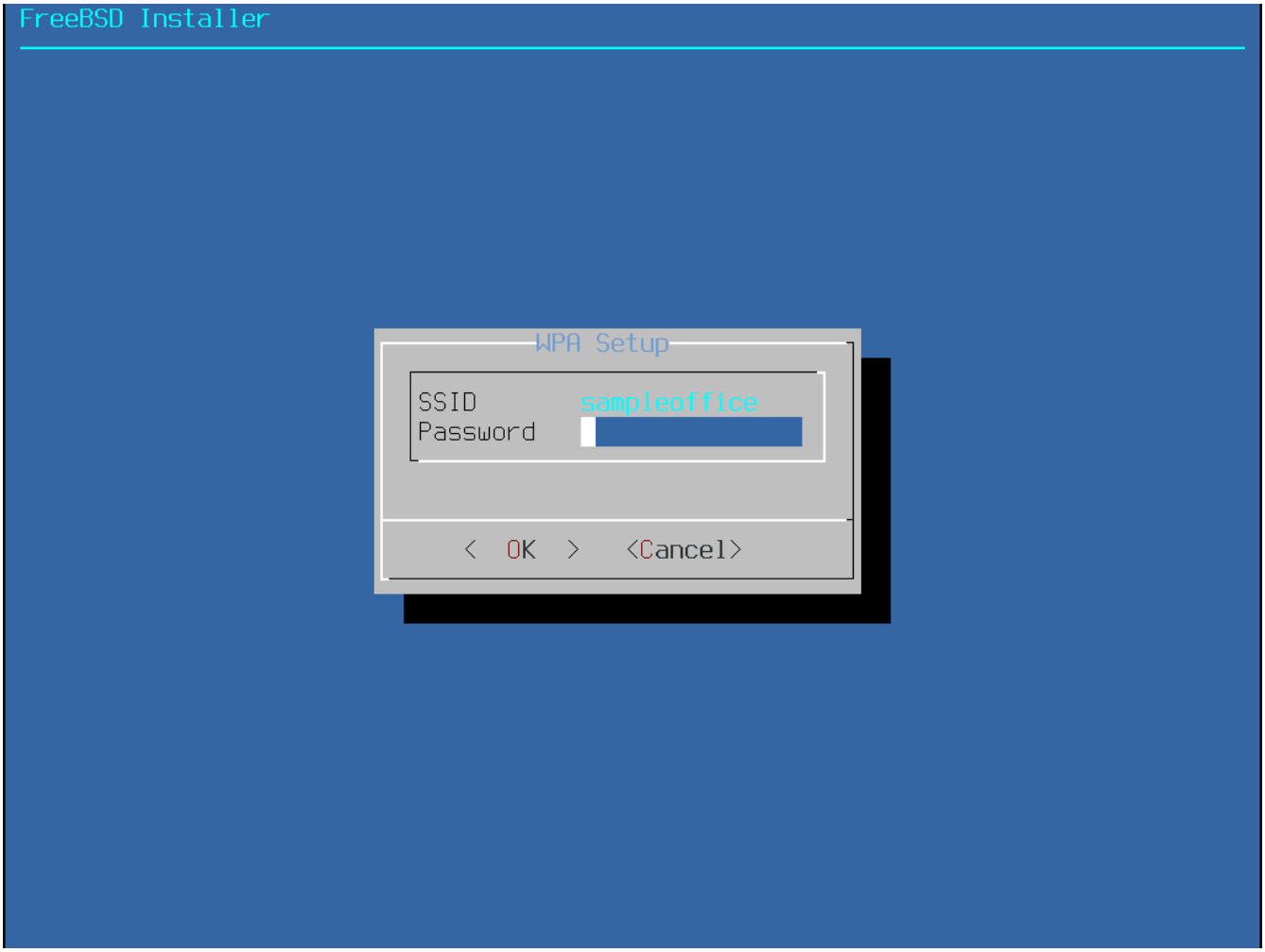


Figure 52. Configuration WPA2

Ensuite, indiquez si une adresse réseau en IPv4 doit être configurée ou non sur l'interface Ethernet ou sans-fil:

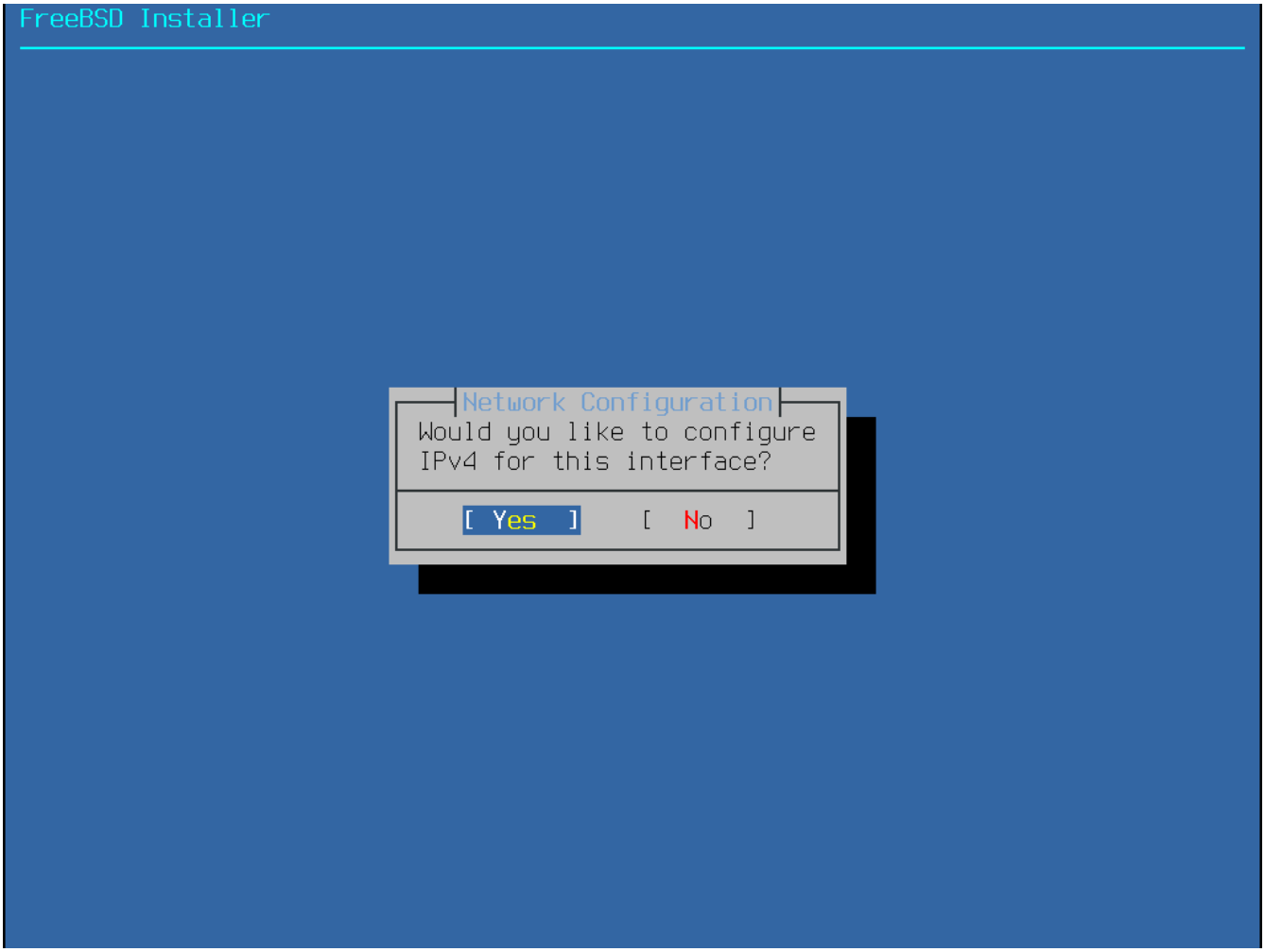


Figure 53. Sélection d'un fonctionnement réseau en IPv4

Il existe deux méthodes de configuration IPv4. En DHCP, l'interface réseau sera configurée automatiquement, c'est la méthode à privilégier si le réseau dispose d'un serveur DHCP. Sinon, les informations de configuration du réseau devront être saisies manuellement sous la forme d'une configuration statique.

N'entrez pas de paramètres réseau au hasard, cela ne fonctionnera pas. Si un serveur DHCP n'est pas disponible, récupérez les paramètres listés dans Informations réseau nécessaires auprès de l'administrateur réseau ou du fournisseur d'accès à Internet.

Si un serveur DHCP est disponible, sélectionner **[Yes]** dans le menu suivant pour configurer automatiquement l'interface réseau. Le programme d'installation s'arrêtera pendant environ une minute pour trouver le serveur DHCP et récupérer l'information de configuration du réseau pour le système.

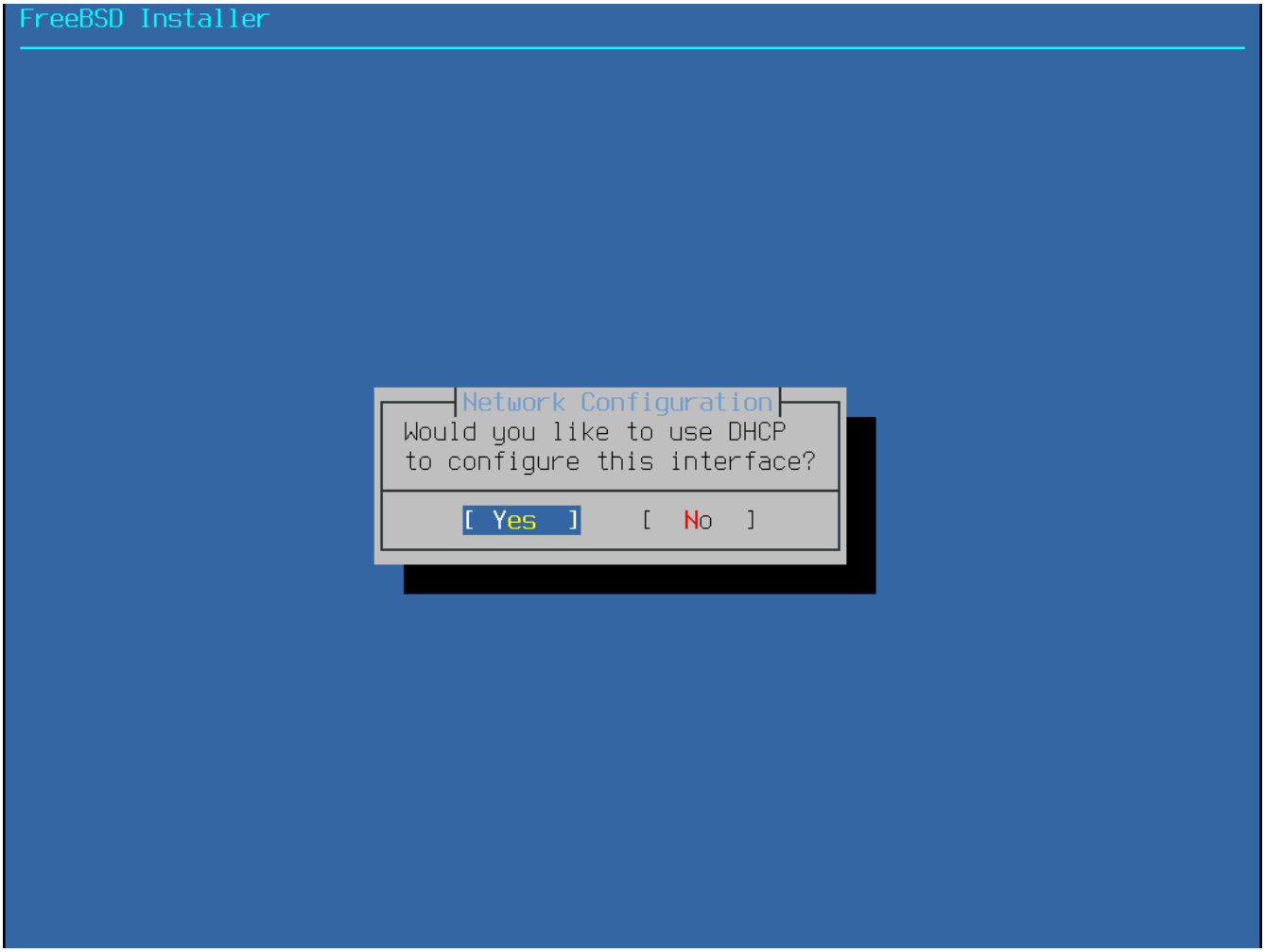


Figure 54. Sélection de la configuration IPv4 avec DHCP

S'il n'y a pas de serveur DHCP, sélectionner **[No]** et tapez les paramètres d'adressage suivants dans le menu qui suit:

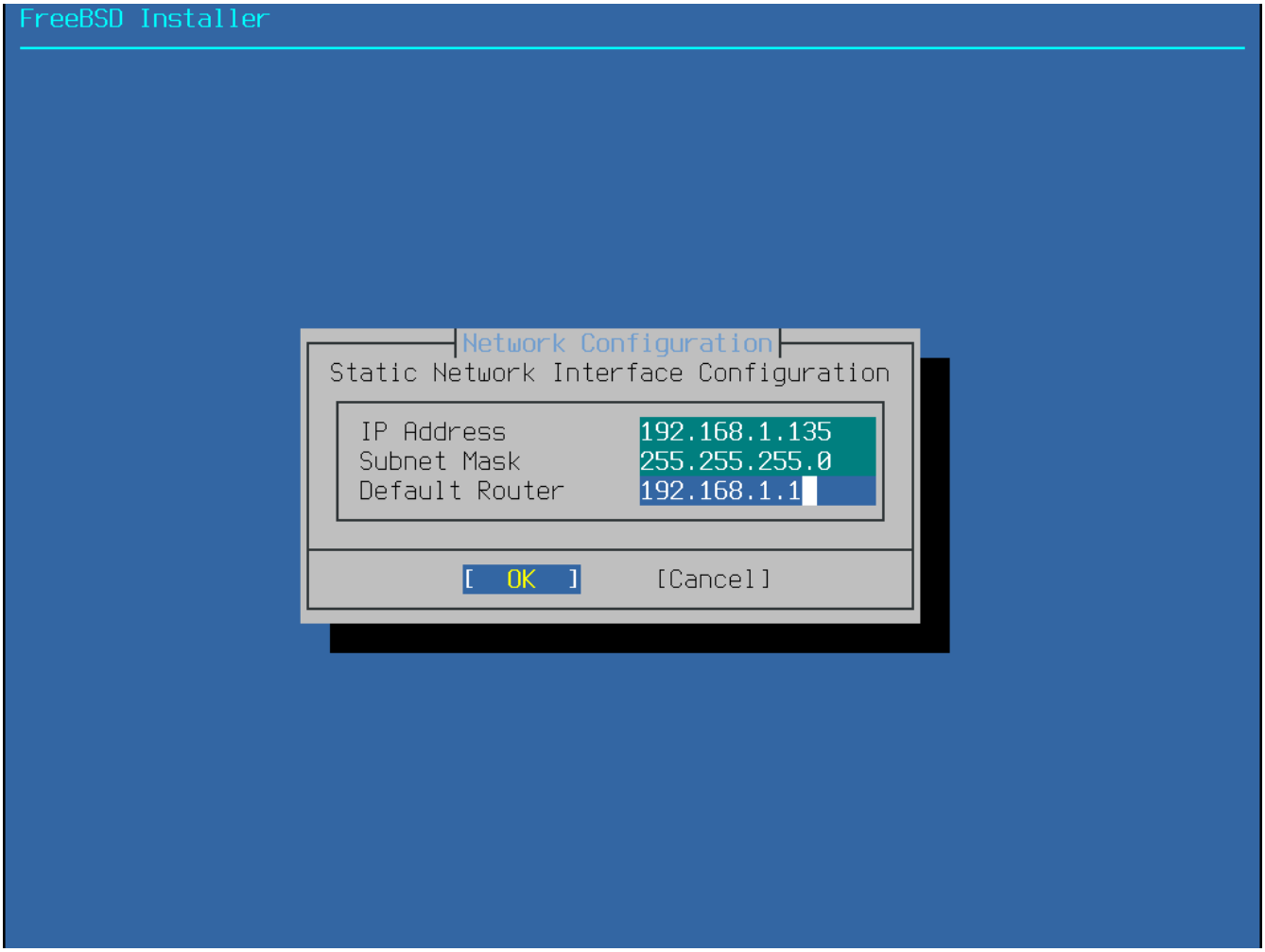


Figure 55. Configuration IPv4 en statique

- `IP Address` - L'adresse IPv4 assignée à cet ordinateur. Cette adresse doit être unique et ne pas être déjà utilisée par un autre équipement sur le réseau local.
- `Subnet Mask` - Le masque de sous-réseau utilisé par le réseau.
- `Default Router` - L'adresse IP de la passerelle par défaut du réseau.

L'écran suivant demandera si l'interface doit être configurée pour l'IPv6. Si l'IPv6 est disponible et désiré, choisir **[Yes]** pour le sélectionner.

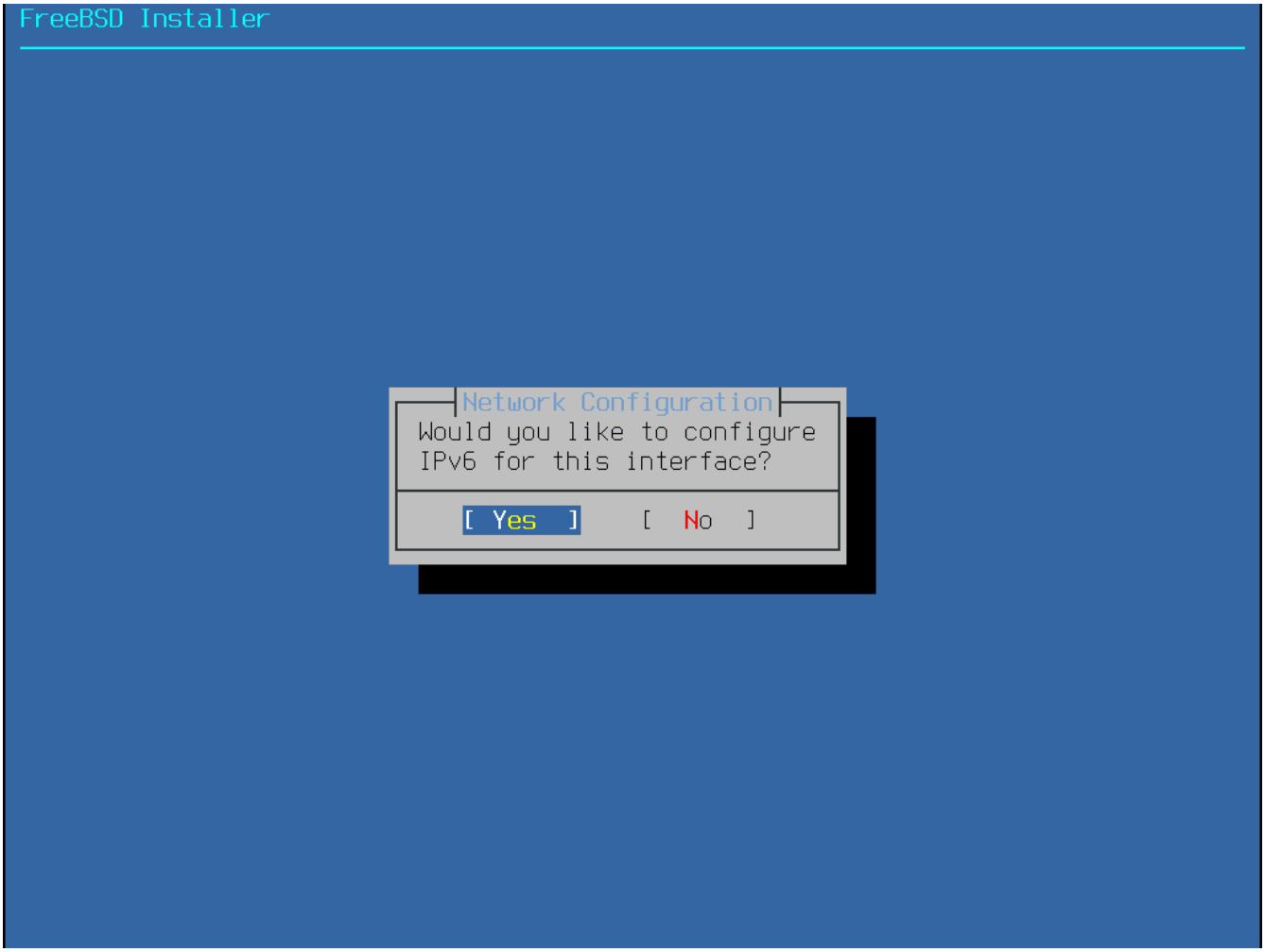


Figure 56. Sélection d'un réseau IPv6

Un réseau IPv6 peut être configuré suivant deux méthodes. Le système d'*autoconfiguration sans état* ou *StateLess Address AutoConfiguration* (SLAAC) demandera automatiquement les informations de configuration correctes à un routeur local. Consulter http://tools.ietf.org pour plus d'information. La configuration statique, quant à elle, demande la saisie manuelle des informations réseau.

Si un routeur IPv6 est disponible, sélectionner **[Yes]** dans le menu suivant pour configurer automatiquement l'interface réseau. Le programme d'installation s'arrêtera pendant environ une minute pour trouver le routeur et obtenir les informations de configuration réseau pour le système.

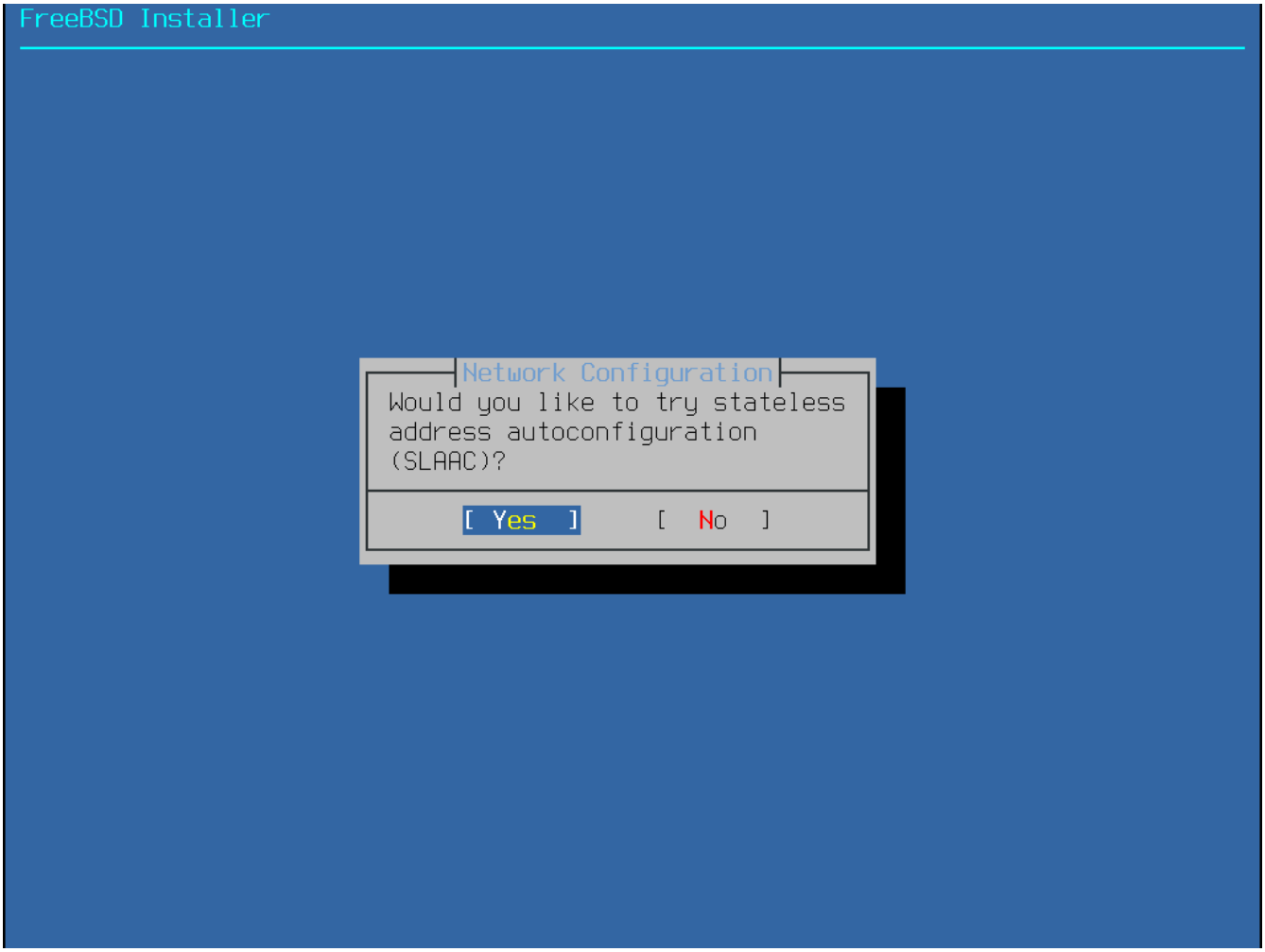


Figure 57. Sélection de la configuration IPv6 SLAAC

S'il n'y a pas de routeur IPv6, sélectionnez **[No]** et tapez les paramètres d'adressage suivants dans le menu qui suit:

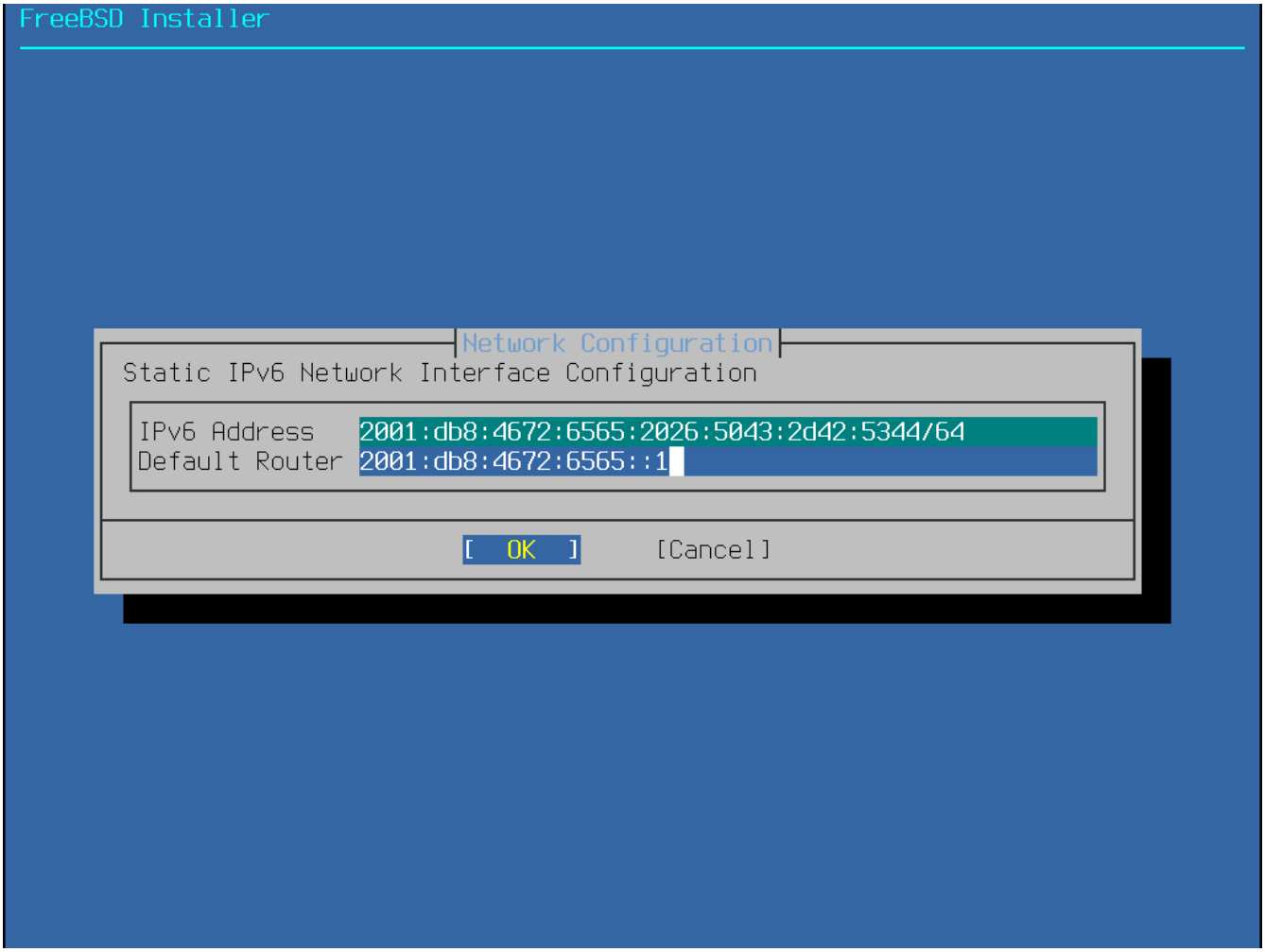


Figure 58. Configuration IPv6 en statique

- `IPv6 Address` - L'adresse IP assignée à cet ordinateur. Cette adresse doit être unique et ne pas être déjà utilisée par un autre équipement sur le réseau local.
- `Default Router` - L'adresse IPv6 de la passerelle par défaut du réseau.

Le dernier menu de configuration est utilisé pour configurer le système de résolution *Domain Name System* (ou DNS) qui convertit les noms de machine en adresses réseau et inversement. Si la méthode du DHCP ou du SLAAC a été utilisée pour configurer automatiquement la carte réseau, les valeurs de configuration du système de résolution de noms (`Resolver Configuration`) pourront déjà être complétées. Dans le cas contraire, entrer le nom de domaine du réseau local dans le champ `Search`. `DNS #1` et `DNS #2` sont les adresses IPv4 et/ou IPv6 des serveurs DNS locaux. Au moins un serveur DNS est nécessaire.

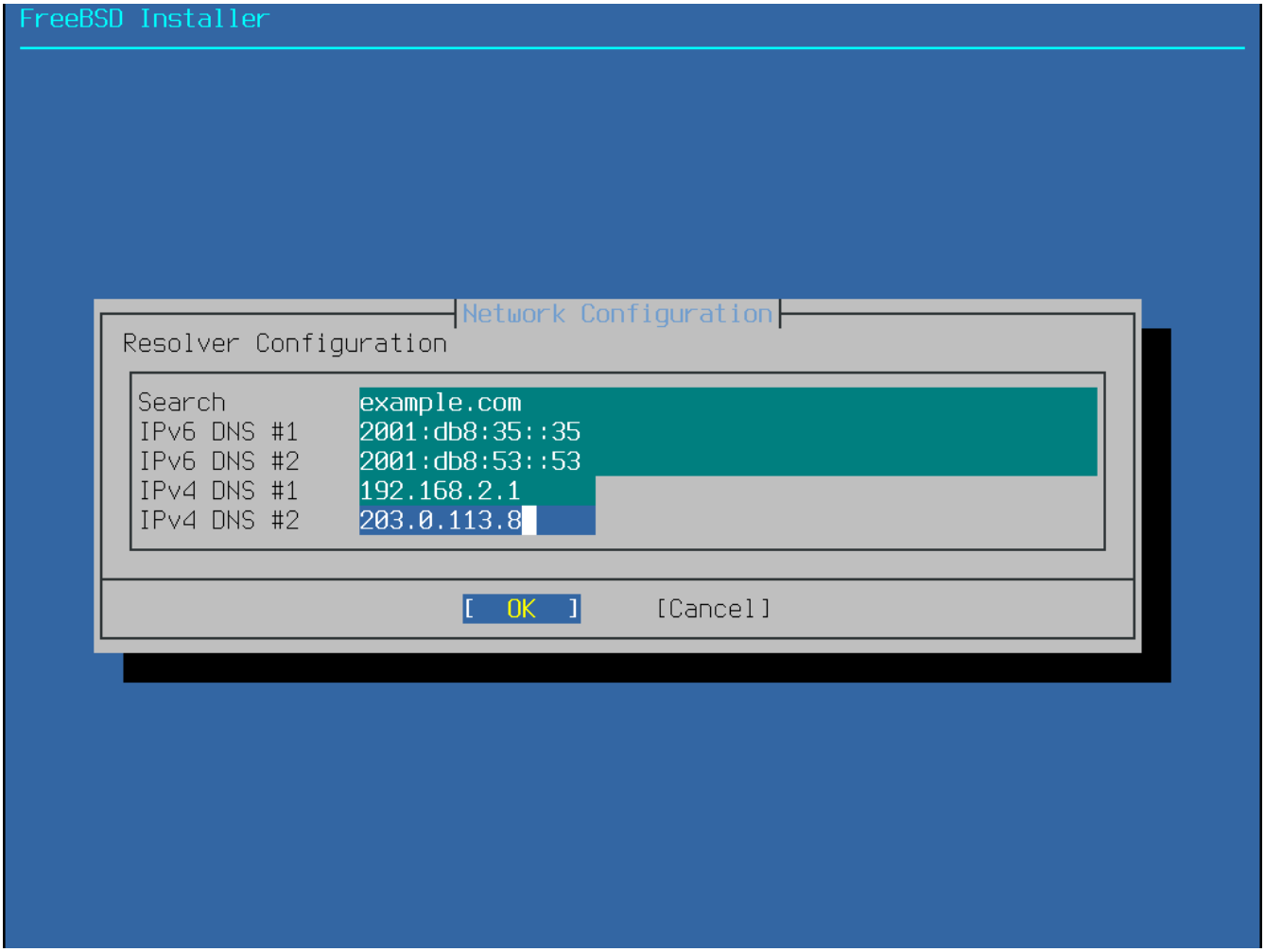


Figure 59. Configuration du DNS

Une fois l'interface réseau configurée, sélectionnez un site miroir qui est situé dans la même région du monde que l'ordinateur sur lequel FreeBSD doit être installé. Les fichiers peuvent être récupérés plus rapidement quand le miroir est proche de l'ordinateur cible, réduisant ainsi le temps d'installation.

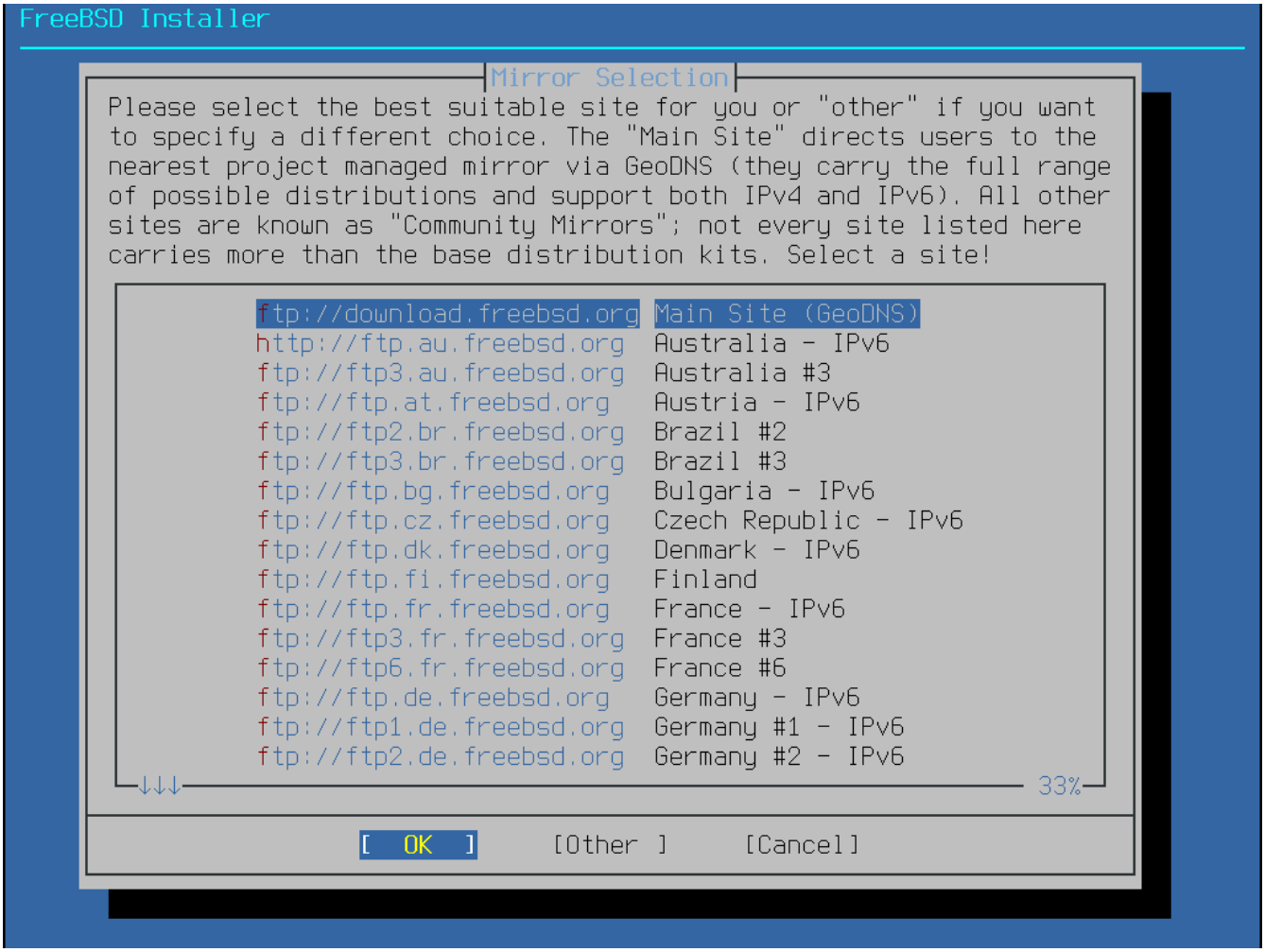


Figure 60. Sélection d'un site miroir

2.10. Dépannage

Cette section couvre le dépannage basique de l'installation, comme les problèmes courants rencontrés.

Vérifier la liste du matériel supporté (https://www.freebsd.org/releases/) de la version de FreeBSD pour être sûr que le matériel est supporté. Si le matériel est supporté et que des blocages ou autres problèmes surviennent, compiler un noyau personnalisé en utilisant les instructions de Configurer le noyau de FreeBSD pour ajouter le support pour les périphériques qui ne sont pas présents dans le noyau GENERIC. Le noyau est configuré de telle façon qu'il supposera que la plupart des périphériques seront dans leur configuration d'usine en termes d'IRQs, d'adresses d'E/S, et canaux de DMA. Si le matériel a été reconfiguré, un fichier de configuration du noyau personnalisé peut indiquer à FreeBSD où trouver les choses.

Quelques problèmes d'installation peuvent être évités ou allégés en mettant à jour le firmware de divers composants matériels, en particulier la carte mère. Le firmware de la carte mère peut également être désigné par le terme BIOS. La plupart des constructeurs de cartes mères ou d'ordinateur disposent d'un site web où peuvent être trouvées les mises à jour et les informations de mises à jour.

Les fabricants déconseillent fortement de mettre à jour le BIOS de la carte mère à moins d'avoir une bonne raison de le faire, comme une mise à jour critique. Le

> processus de mise à jour *peut* mal se passer, laissant un BIOS incomplet et l'ordinateur inutilisable.

Si le système se bloque au démarrage pendant la détection du matériel, ou se comporte de manière étrange lors de l'installation, l'ACPI peut être le coupable. FreeBSD utilise de manière intensive le système ACPI sur les plateformes i386 et amd64, s'il est détecté au démarrage, pour aider à la configuration du matériel. Malheureusement, des bogues persistent dans le pilote ACPI, et sur les cartes mères et leur BIOS. L'ACPI peut être désactivé en positionnant le paramètre `hint.acpi.0.disabled` pour le chargeur de démarrage:

```
set hint.acpi.0.disabled="1"
```

Ce paramètre est réinitialisé à chaque démarrage du système, il est donc nécessaire d'ajouter `hint.acpi.0.disabled="1"` au fichier /boot/loader.conf. Plus d'information au sujet du chargeur peut être trouvée dans la Menu d'accueil.

2.11. Utilisation du CD Live

Le menu d'accueil de bsdinstall, montré dans Menu d'accueil, propose une option **[Live CD]**. C'est utile pour ceux qui se demandent si FreeBSD est le bon choix et désirent tester certaines fonctionnalités avant l'installation.

Les points suivants devront être pris en compte avant l'utilisation du :**[Live CD]**

- Pour utiliser le système, une authentification est nécessaire. Le nom d'utilisateur est `root`, sans mot de passe.
- Etant donné que le système s'exécute directement à partir du support d'installation, le système sera bien plus lent que s'il était installé sur un disque dur.
- Cette option ne propose qu'une invite de commande et pas d'interface graphique.

Chapitre 3. Quelques bases d'UNIX

3.1. Synopsis

Le chapitre suivant couvrira les commandes et fonctionnalités de base du système d'exploitation FreeBSD. La plupart de ces informations sera valable pour n'importe quel système d'exploitation UNIX®. Soyez libre de passer ce chapitre si vous êtes familier avec ces informations. Si vous êtes nouveau à FreeBSD, alors vous voudrez certainement lire attentivement ce chapitre.

Après la lecture de ce chapitre, vous saurez:

- Comment utiliser les "consoles virtuelles" de FreeBSD.
- Comment les permissions des fichiers d'UNIX® fonctionnent ainsi que l'utilisation des indicateurs de fichiers sous FreeBSD.
- L'architecture par défaut du système de fichiers sous FreeBSD.
- L'organisation des disques sous FreeBSD.
- Comment monter et démonter des systèmes de fichier.
- Ce que sont les processus, daemons et signaux.
- Ce qu'est un interpréteur de commande, et comment changer votre environnement de session par défaut.
- Comment utiliser les éditeurs de texte de base.
- Ce que sont les périphériques et les fichiers spéciaux de périphérique.
- Quel est le format des binaires utilisé sous FreeBSD.
- Comment lire les pages de manuel pour plus d'information.

3.2. Consoles virtuelles terminaux

FreeBSD peut être utilisé de diverses façons. L'une d'elles est en tapant des commandes sur un terminal texte. Une bonne partie de la flexibilité et de la puissance d'un système d'exploitation UNIX® est directement disponible sous vos mains en utilisant FreeBSD de cette manière. Cette section décrit ce que sont les "terminaux" et les "consoles", et comment les utiliser sous FreeBSD.

3.2.1. La console

Si vous n'avez pas configuré FreeBSD pour lancer automatiquement un environnement graphique au démarrage, le système vous présentera une invite d'ouverture de session après son démarrage, juste après la fin des procédures de démarrage. Vous verrez quelque chose de similaire à:

```
Additional ABI support:.
Local package initialization:.
Additional TCP options:.

Fri Sep 20 13:01:06 EEST 2002
```

```
FreeBSD/i386 (pc3.example.org) (ttyv0)

login:
```

Les messages pourront être différents sur votre système, mais cela devrait y ressembler. Les deux dernières lignes sont celles qui nous intéressent actuellement. La seconde de ces lignes nous donne:

```
FreeBSD/i386 (pc3.example.org) (ttyv0)
```

Cette ligne contient quelques éléments d'information sur le système que vous venez de démarrer. Vous êtes en train de lire une console "FreeBSD", tournant sur un processeur Intel ou compatible de la famille x86. Le nom de cette machine (chaque machine UNIX® a un nom) est `pc3.example.org`, et vous regardez actuellement sa console système-le terminal ttyv0.

Et enfin, la dernière ligne est toujours:

```
login:
```

C'est le moment où vous êtes supposé taper votre "nom d'utilisateur" pour vous attacher au système FreeBSD. La section suivante décrit comment procéder.

3.2.2. Ouvrir une session sur un système FreeBSD

FreeBSD est un système multi-utilisateur, multi-processeur. C'est la description formelle qui est habituellement donnée pour un système qui peut être utilisé par différentes personnes, qui exécutent simultanément de nombreux programmes sur une machine individuelle.

Chaque système multi-utilisateur a besoin d'un moyen pour distinguer un "utilisateur" du reste. Sous FreeBSD (et sous tous les systèmes de type UNIX®), cela est effectué en demandant à chaque utilisateur de "s'attacher" au système avant d'être en mesure d'exécuter des programmes. Chaque utilisateur possède un nom unique (le nom d'utilisateur) et une clé secrète personnelle (le mot de passe). FreeBSD demandera ces deux éléments avant d'autoriser un utilisateur à lancer un programme.

Juste après que FreeBSD ait démarré et en ait terminé avec l'exécution des procédures de démarrage, il présentera une invite et demandera un nom d'utilisateur valide:

```
login:
```

Pour cet exemple, supposons que votre nom d'utilisateur est `john`. Tapez `john` à cette invite puis appuyez sur `Entrée`. Alors vous devrez être invité à entrer un "mot de passe":

```
login: john
Password:
```

Tapez maintenant le mot de passe de `john`, et appuyez sur `Entrée`. Le mot de passe *n'est pas affiché!* Vous n'avez pas à vous préoccuper de cela maintenant. Il suffit de penser que cela est fait pour des raisons de sécurité.

Si vous avez tapé correctement votre mot de passe, vous devriez être maintenant attaché au système et prêt à essayer toutes les commandes disponibles.

Vous devriez voir apparaître le MOTD ou message du jour suivi de l'invite de commande (un caractère `#`, `$`, ou `%`). Cela indique que vous avez ouvert avec succès une session sous FreeBSD.

3.2.3. Consoles multiples

Exécuter des commandes UNIX® dans une console est bien beau, mais FreeBSD peut exécuter plusieurs programmes à la fois. Avoir une seule console sur laquelle les commandes peuvent être tapées serait un peu du gaspillage quand un système d'exploitation comme FreeBSD peut exécuter des dizaines de programmes en même temps. C'est ici que des "consoles virtuelles" peuvent être vraiment utiles.

FreeBSD peut être configuré pour présenter de nombreuses consoles virtuelles. Vous pouvez basculer d'une console virtuelle à une autre en utilisant une combinaison de touches sur votre clavier. Chaque console a son propre canal de sortie, et FreeBSD prend soin de rediriger correctement les entrées au clavier et la sortie vers écran quand vous basculez d'une console virtuelle à la suivante.

Des combinaisons de touches spécifiques ont été réservées par FreeBSD pour le basculement entre consoles. Vous pouvez utiliser `Alt` + `F1`, `Alt` + `F2`, jusqu'à `Alt` + `F8` pour basculer vers une console virtuelle différente sous FreeBSD.

Quand vous basculez d'une console à une autre, FreeBSD prend soin de sauvegarder et restaurer la sortie d'écran. Il en résulte l'"illusion" d'avoir plusieurs écrans et claviers "virtuels" que vous pouvez utiliser pour taper des commandes pour FreeBSD. Les programmes que vous lancez sur une console virtuelle ne cessent pas de tourner quand cette console n'est plus visible. Ils continuent de s'exécuter quand vous avez basculé vers une console virtuelle différente.

3.2.4. Le fichier /etc/ttys

La configuration par défaut de FreeBSD démarre avec huit consoles virtuelles. Cependant ce n'est pas un paramétrage fixe, et vous pouvez aisément personnaliser votre installation pour démarrer avec plus ou moins de consoles virtuelles. Le nombre et les paramétrages des consoles virtuelles sont configurés dans le fichier /etc/ttys.

Vous pouvez utiliser le fichier /etc/ttys pour configurer les consoles virtuelles de FreeBSD. Chaque ligne non-commentée dans ce fichier (les lignes qui ne débutent pas par le caractère `#`) contient le paramétrage d'un terminal ou d'une console virtuelle. La version par défaut de ce fichier livrée avec FreeBSD configure neuf consoles virtuelles, et en active huit. Ce sont les lignes commençant avec le terme `ttyv`:

```
# name  getty                           type    status          comments
#
```

```
ttyv0   "/usr/libexec/getty Pc"         cons25  on  secure
# Virtual terminals
ttyv1   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv2   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv3   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv4   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv5   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv6   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv7   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv8   "/usr/X11R6/bin/xdm -nodaemon"  xterm   off secure
```

Pour une description détaillée de chaque colonne de ce fichier et toutes les options que vous pouvez utiliser pour configurer les consoles virtuelles, consultez la page de manuel ttys(5).

3.2.5. Console en mode mono-utilisateur

Une description détaillée de ce qu'est "le mode mono-utilisateur" peut être trouvée dans Mode mono-utilisateur. Il est important de noter qu'il n'y a qu'une console de disponible quand vous exécutez FreeBSD en mode mono-utilisateur. Il n'y a aucune console virtuelle de disponible. Le paramétrage de la console en mode mono-utilisateur peut être également trouvé dans le fichier /etc/ttys. Recherchez la ligne qui commence avec le mot `console`:

```
# name  getty                           type    status          comments
#
# If console is marked "insecure", then init will ask for the root password
# when going to single-user mode.
console none                            unknown off secure
```

Comme l'indiquent les commentaires au-dessus de la ligne `console`, vous pouvez éditer cette ligne et changer `secure` pour `insecure`. Si vous faites cela, quand FreeBSD démarrera en mode mono-utilisateur, il demandera le mot de passe de `root`.

Cependant faites attention quand vous modifiez cela pour `insecure`. Si vous oubliez le mot de passe de `root`, le démarrage en mode mono-utilisateur sera condamné. Il est encore possible, mais cela pourra être relativement compliqué pour quelqu'un qui n'est pas à l'aise avec le processus de démarrage de FreeBSD et les programmes entrant en jeu.

3.2.6. Modifier la résolution de la console

La résolution (ou encore le mode vidéo) de la console FreeBSD peut être réglée à 1024x768, 1280x1024, ou tout autre résolution supportée par le circuit graphique et le moniteur. Pour utiliser une résolution vidéo différente vous devez en premier lieu recompiler votre noyau en ajoutant deux options supplémentaires:

```
options VESA
```

```
options SC_PIXEL_MODE
```

Une fois votre noyau recompilé avec ces deux options, vous pouvez déterminer quels sont les modes vidéo supportés par votre matériel en utilisant l'outil vidcontrol(1). Pour obtenir une liste des modes supportés, tapez la ligne suivante:

```
# vidcontrol -i mode
```

La sortie de cette commande est une liste des modes vidéo que supporte votre matériel. Vous pouvez ensuite décider d'utiliser un nouveau mode en le passant à la commande vidcontrol(1) tout en ayant les droits de `root`:

```
# vidcontrol MODE_279
```

Si le nouveau mode vidéo est satisfaisant, il peut être activé au démarrage de manière permanente en le configurant dans le fichier /etc/rc.conf:

```
allscreens_flags="MODE_279"
```

3.3. Permissions

FreeBSD, étant un descendant direct de l'UNIX® BSD, est basé sur plusieurs concepts clés d'UNIX®. Le premier, et le plus prononcé, est le fait que FreeBSD est un système d'exploitation multi-utilisateurs. Le système peut gérer plusieurs utilisateurs travaillant tous simultanément sur des tâches complètement indépendantes. Le système est responsable du partage correct et de la gestion des requêtes pour les périphériques matériels, la mémoire, et le temps CPU de façon équitable entre chaque utilisateur.

Puisque le système est capable de supporter des utilisateurs multiples, tout ce que le système gère possède un ensemble de permissions définissant qui peut écrire, lire, et exécuter la ressource. Ces permissions sont stockées sous forme de trois octets divisés en trois parties, une pour le propriétaire du fichier, une pour le groupe auquel appartient le fichier, et une autre pour le reste du monde. Cette représentation numérique fonctionne comme ceci:

Valeur	Permission	Contenu du répertoire
0	Pas d'accès en lecture, pas d'accès en écriture, pas d'accès en exécution	`---`
1	Pas d'accès en lecture, pas d'accès en écriture, exécution	`--x`
2	Pas d'accès en lecture, écriture, pas d'accès en exécution	`-w-`

Valeur	Permission	Contenu du répertoire
3	Pas d'accès en lecture, écriture, exécution	`-wx`
4	Lecture, pas d'accès en écriture, pas d'accès en exécution	`r--`
5	Lecture, pas d'accès en écriture, exécution	`r-x`
6	Lecture, écriture, pas d'accès en exécution	`rw-`
7	Lecture, écriture, exécution	`rwx`

Vous pouvez utiliser l'option `-l` avec la commande ls(1) pour afficher le contenu du répertoire sous forme une longue et détaillée qui inclut une colonne avec des informations sur les permissions d'accès des fichiers pour le propriétaire, le groupe, et le reste du monde. Par exemple un `ls -l` dans un répertoire quelconque devrait donner:

```
% ls -l
total 530
-rw-r--r--  1 root  wheel     512 Sep  5 12:31 myfile
-rw-r--r--  1 root  wheel     512 Sep  5 12:31 otherfile
-rw-r--r--  1 root  wheel    7680 Sep  5 12:31 email.txt
...
```

Voici comment est divisée la première colonne de l'affichage généré par `ls -l`:

```
-rw-r--r--
```

Le premier caractère (le plus à gauche) indique si c'est un fichier normal, un répertoire, ou un périphérique mode caractère, une socket, ou tout autre pseudo-périphérique. Dans ce cas, `-` indique un fichier normal. Les trois caractères suivants, `rw-` dans cet exemple, donnent les permissions pour le propriétaire du fichier. Les trois caractères qui suivent, `r--`, donnent les permissions pour le groupe auquel appartient le fichier. Les trois derniers caractères, `r--`, donnent les permissions pour le reste du monde. Un tiret signifie que la permission est désactivée. Dans le cas de ce fichier, les permissions sont telles que le propriétaire peut lire et écrire le fichier, le groupe peut lire le fichier, et le reste du monde peut seulement lire le fichier. D'après la table ci-dessus, les permissions pour ce fichier seraient `644`, où chaque chiffre représente les trois parties des permissions du fichier.

Tout cela est bien beau, mais comment le système contrôle les permissions sur les périphériques? En fait FreeBSD traite la plupart des périphériques sous la forme d'un fichier que les programmes peuvent ouvrir, lire, et écrire des données dessus comme tout autre fichier. Ces périphériques spéciaux sont stockés dans le répertoire /dev.

Les répertoires sont aussi traités comme des fichiers. Ils ont des droits en lecture, écriture et exécution. Le bit d'exécution pour un répertoire a une signification légèrement différente que pour les fichiers. Quand un répertoire est marqué exécutable, cela signifie qu'il peut être traversé, i.e. il

est possible d'utiliser "cd" (changement de répertoire). Ceci signifie également qu'à l'intérieur du répertoire il est possible d'accéder aux fichiers dont les noms sont connus (en fonction, bien sûr, des permissions sur les fichiers eux-mêmes).

En particulier, afin d'obtenir la liste du contenu d'un répertoire, la permission de lecture doit être positionnée sur le répertoire, tandis que pour effacer un fichier dont on connaît le nom, il est nécessaire d'avoir les droits d'écriture *et* d'exécution sur le répertoire contenant le fichier.

Il y a d'autres types de permissions, mais elles sont principalement employées dans des circonstances spéciales comme les binaires "setuid" et les répertoires "sticky". Si vous désirez plus d'information sur les permissions de fichier et comment les positionner, soyez sûr de consulter la page de manuel chmod(1).

3.3.1. Permissions symboliques

Les permissions symboliques, parfois désignées sous le nom d'expressions symboliques, utilisent des caractères à la place de valeur en octal pour assigner les permissions aux fichiers et répertoires. Les expressions symboliques emploient la syntaxe: (qui) (action) (permissions), avec les valeurs possibles suivantes:

Option	Lettre	Représente
(qui)	u	Utilisateur
(qui)	g	Groupe
(qui)	o	Autre
(qui)	a	Tous ("le monde entier")
(action)	+	Ajouter des permissions
(action)	-	Retirer des permissions
(action)	=	Fixe les permissions de façon explicite
(permissions)	r	Lecture
(permissions)	w	Ecriture
(permissions)	x	Exécution
(permissions)	t	bit collant (sticky)
(permissions)	s	Exécuter avec l'ID utilisateur (UID) ou groupe (GID)

Ces valeurs sont utilisées avec la commande chmod(1) comme précédemment mais avec des lettres. Par exemple, vous pourriez utiliser la commande suivante pour refuser l'accès au fichier *FICHIER* à d'autres utilisateurs:

```
% chmod go= FICHIER
```

Une liste séparé par des virgules peut être fournie quand plus d'un changement doit être effectué

sur un fichier. Par exemple la commande suivante retirera les permissions d'écriture au groupe et au "reste du monde" sur le fichier *FICHIER*, puis ajoutera la permission d'exécution pour tout le monde:

```
% chmod go-w,a+x FICHIER
```

3.3.2. Indicateurs des fichiers sous FreeBSD

En addition des permissions sur les fichiers précédemment présentées, FreeBSD supporte l'utilisation d'"indicateurs de fichiers". Ces indicateurs rajoutent un niveau de contrôle et de sécurité sur les fichiers, mais ne concernent pas les répertoires.

Ces indicateurs ajoutent donc un niveau de contrôle supplémentaire des fichiers, permettant d'assurer que dans certains cas même le super-utilisateur `root` ne pourra effacer ou modifier des fichiers.

Les indicateurs de fichiers peuvent être modifiés avec l'utilitaire chflags(1), ce dernier présentant une interface simple. Par exemple, pour activer l'indicateur système de suppression impossible sur le fichier file1, tapez la commande suivante:

```
# chflags sunlink file1
```

Et pour désactiver l'indicateur de suppression impossible, utilisez la commande précédente avec le préfixe "no" devant l'option `sunlink`:

```
# chflags nosunlink file1
```

Pour afficher les indicateurs propres à ce fichier, utilisez la commande ls(1) avec l'option `-lo`:

```
# ls -lo file1
```

La sortie de la commande devrait ressembler à:

```
-rw-r--r--  1 trhodes  trhodes  sunlnk 0 Mar  1 05:54 file1
```

Plusieurs indicateurs ne peuvent être positionnés ou retirés que par le super-utilisateur `root`. Dans les autres cas, le propriétaire du fichier peut activer ces indicateurs. Pour plus d'information, la lecture des pages de manuel chflags(1) et chflags(2) est recommandée à tout administrateur.

3.4. Organisation de l'arborescence des répertoires

L'organisation de l'arborescence des répertoires de FreeBSD est essentielle pour obtenir une compréhension globale du système. Le concept le plus important à saisir est celui du répertoire

racine, "/". Ce répertoire est le premier a être monté au démarrage et il contient le système de base nécessaire pour préparer le système d'exploitation au fonctionnement multi-utilisateurs. Le répertoire racine contient également les points de montage pour les autres systèmes de fichiers qui sont montés lors du passage en mode multi-utilisateurs.

Un point de montage est un répertoire où peuvent être greffés des systèmes de fichiers supplémentaires au système de fichiers parent (en général le système de fichiers racine). Cela est décrit plus en détails dans la Organisation des disques. Les points de montage standards incluent /usr, /var, /tmp, /mnt, et /cdrom. Ces répertoires sont en général référencés par des entrées dans le fichier /etc/fstab. /etc/fstab est une table des divers systèmes de fichiers et de leur point de montage utilisé comme référence par le système. La plupart des systèmes de fichiers présents dans /etc/fstab sont montés automatiquement au moment du démarrage par la procédure rc(8) à moins que l'option `noauto` soit présente. Plus de détails peuvent être trouvés dans la Le fichier fstab.

Une description complète de l'arborescence du système de fichiers est disponible dans la page de manuel hier(7). Pour l'instant, une brève vue d'ensemble des répertoires les plus courants suffira.

Répertoire	Description
/	Répertoire racine du système de fichiers.
/bin/	Programmes utilisateur fondamentaux aux deux modes de fonctionnement mono et multi-utilisateurs.
/boot/	Programmes et fichiers de configuration utilisés durant le processus de démarrage du système.
/boot/defaults/	Fichiers de configuration par défaut du processus de démarrage; voir la page de manuel loader.conf(5).
/dev/	Fichiers spéciaux de périphérique; voir la page de manuel intro(4).
/etc/	Procédures et fichiers de configuration du système.
/etc/defaults/	Fichiers de configuration du système par défaut; voir la page de manuel rc(8).
/etc/mail/	Fichiers de configuration pour les agents de transport du courrier électronique comme sendmail(8).
/etc/namedb/	Fichiers de configuration de `named`; voir la page de manuel named(8).
/etc/periodic/	Procédures qui sont exécutées de façon quotidienne, hebdomadaire et mensuelle par l'intermédiaire de cron(8); voir la page de manuel periodic(8).
/etc/ppp/	Fichiers de configuration de `ppp`; voir la page de manuel ppp(8).
/mnt/	Répertoire vide habituellement utilisé par les administrateurs système comme un point de montage temporaire.
/proc/	Le système de fichiers pour les processus; voir les pages de manuel procfs(5), mount_procfs(8).
/rescue/	Programmes liés en statique pour les réparations d'urgence; consultez la page de manuel rescue(8).
/root/	Répertoire personnel du compte `root`.

Répertoire	Description
/sbin/	Programmes systèmes et utilitaires systèmes fondamentaux aux environnements mono et multi-utilisateurs.
/tmp/	Fichiers temporaires. Le contenu de /tmp n'est en général PAS préservé par un redémarrage du système. Un système de fichiers en mémoire est souvent monté sur /tmp. Cela peut être automatisé en utilisant les variables rc.conf(5) relatives au système "tmpmfs" (ou à l'aide d'une entrée dans le fichier /etc/fstab; consultez la page de manuel mdmfs(8)).
/usr/	La majorité des utilitaires et applications utilisateur.
/usr/bin/	Utilitaires généraux, outils de programmation, et applications.
/usr/include/	Fichiers d'en-tête C standard.
/usr/lib/	Ensemble des bibliothèques.
/usr/libdata/	Divers fichiers de données de service.
/usr/libexec/	Utilitaires et daemons système (exécutés par d'autres programmes).
/usr/local/	Exécutables, bibliothèques, etc... Egalement utilisé comme destination de défaut pour les logiciels portés pour FreeBSD. Dans /usr/local, l'organisation générale décrite par la page de manuel hier(7) pour /usr devrait être utilisée. Exceptions faites du répertoire man qui est directement sous /usr/local plutôt que sous /usr/local/share, et la documentation des logiciels portés est dans share/doc/port.
/usr/obj/	Arborescence cible spécifique à une architecture produite par la compilation de l'arborescence /usr/src.
/usr/ports	Le catalogue des logiciels portés (optionnel).
/usr/sbin/	Utilitaires et daemons système (exécutés par les utilisateurs).
/usr/shared/	Fichiers indépendants de l'architecture.
/usr/src/	Fichiers source FreeBSD et/ou locaux.
/usr/X11R6/	Exécutables, bibliothèques etc... de la distribution d'X11R6 (optionnel).
/var/	Fichiers de traces, fichiers temporaires, et fichiers tampons. Un système de fichiers en mémoire est parfois monté sur /var. Cela peut être automatisé en utilisant les variables rc.conf(5) relatives au système "varmfs" (ou à l'aide d'une entrée dans le fichier /etc/fstab; consultez la page de manuel mdmfs(8)).
/var/log/	Divers fichiers de trace du système.
/var/mail/	Boîtes aux lettres des utilisateurs.
/var/spool/	Divers répertoires tampons des systèmes de courrier électronique et d'impression.
/var/tmp/	Fichiers temporaires. Ces fichiers sont généralement conservés lors d'un redémarrage du système, à moins que /var ne soit un système de fichiers en mémoire.
/var/yp	Tables NIS.

3.5. Organisation des disques

Le plus petit élément qu'utilise FreeBSD pour retrouver des fichiers est le nom de fichier. Les noms de fichiers sont sensibles à la casse des caractères, ce qui signifie que readme.txt et README.TXT sont deux fichiers séparés. FreeBSD n'utilise pas l'extension (.txt) d'un fichier pour déterminer si ce fichier est un programme, un document ou une autre forme de donnée.

Les fichiers sont stockés dans des répertoires. Un répertoire peut ne contenir aucun fichier, ou en contenir plusieurs centaines. Un répertoire peut également contenir d'autre répertoires, vous permettant de construire une hiérarchie de répertoires à l'intérieur d'un autre. Cela rend plus simple l'organisation de vos données.

Les fichiers et les répertoires sont référencés en donnant le nom du fichier ou du répertoire, suivi par un slash, `/`, suivi par tout nom de répertoire nécessaire. Si vous avez un répertoire foo, qui contient le répertoire bar, qui contient le fichier readme.txt, alors le nom complet, ou *chemin* ("path") vers le fichier est foo/bar/readme.txt.

Les répertoires et les fichiers sont stockés sur un système de fichiers. Chaque système de fichiers contient à son niveau le plus haut un répertoire appelé *répertoire racine* pour ce système de fichiers. Ce répertoire racine peut alors contenir les autres répertoires.

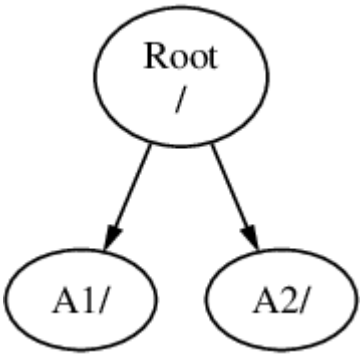
Jusqu'ici cela est probablement semblable à n'importe quel autre système d'exploitation que vous avez pu avoir utilisé. Il y a quelques différences: par exemple, MS-DOS® utilise `\` pour séparer les noms de fichier et de répertoire, alors que MacOS utilise `:`.

FreeBSD n'utilise pas de lettre pour les lecteurs, ou d'autres noms de disque dans le chemin. Vous n'écrirez pas c:/foo/bar/readme.txt sous FreeBSD.

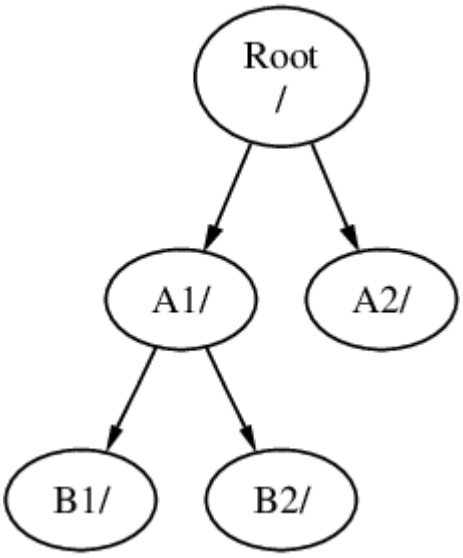
Au lieu de cela, un système de fichiers est désigné comme *système de fichiers racine*. La racine du système de fichiers racine est représentée par un `/`. Tous les autres systèmes de fichiers sont alors *montés* sous le système de fichiers racine. Peu importe le nombre de disques que vous avez sur votre système FreeBSD, chaque répertoire apparaît comme faisant partie du même disque.

Supposez que vous avez trois systèmes de fichiers, appelés `A`, `B`, et `C`. Chaque système de fichiers possède un répertoire racine, qui contient deux autres répertoires, nommés `A1`, `A2` (et respectivement `B1`, `B2` et `C1`, `C2`).

Appelons `A` le système de fichiers racine. Si vous utilisiez la commande `ls` pour visualiser le contenu de ce répertoire, vous verriez deux sous-répertoires, `A1` et `A2`. L'arborescence des répertoires ressemblera à ceci:

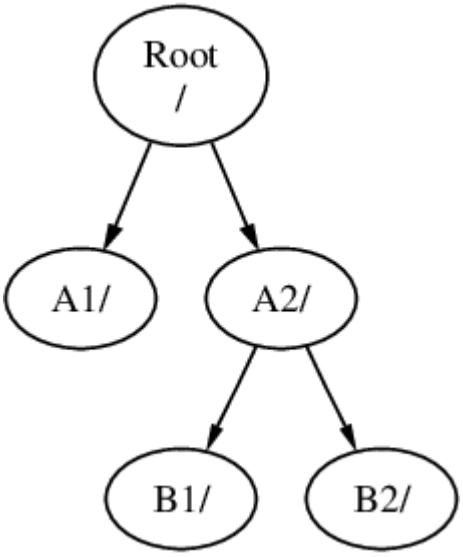


Un système de fichiers doit être monté dans un répertoire d'un autre système de fichiers. Supposez maintenant que vous montez le système de fichiers `B` sur le répertoire `A1`. Le répertoire racine de `B` remplace `A1`, et les répertoires de `B` par conséquent apparaissent:



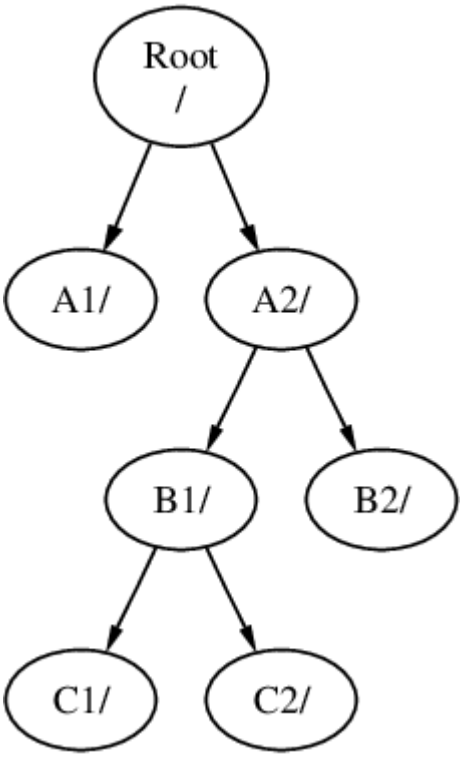
Tout fichier de `B1` ou `B2` peut être atteint avec le chemin /A1/B1 ou /A1/B2 si nécessaire. Tous les fichiers qui étaient dans A1 ont été temporairement cachés. Ils réapparaîtront si `B` est *démonté* de A.

Si `B` a été monté sur `A2` alors le diagramme sera semblable à celui-ci:

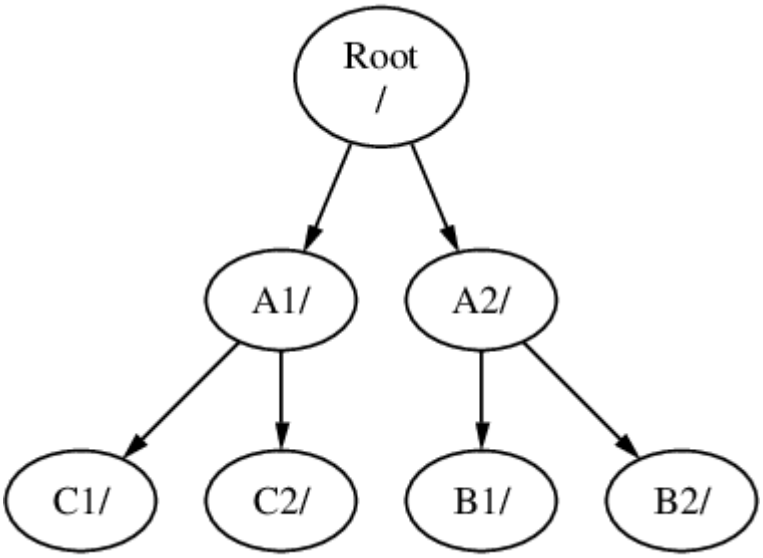


et les chemins seront /A2/B1 et respectivement /A2/B2.

Les systèmes de fichiers peuvent être montés au sommet d'un autre. En continuant l'exemple précédent, le système de fichiers `C` pourrait être monté au sommet du répertoire `B1` dans le système de fichiers `B`, menant à cet arrangement:



Où `C` pourrait être monté directement sur le système de fichiers `A`, sous le répertoire `A1`:



Si vous êtes familier de MS-DOS®, ceci est semblable, bien que pas identique, à la commande `join`.

Ce n'est normalement pas quelque chose qui doit vous préoccuper. Généralement vous créez des systèmes de fichiers à l'installation de FreeBSD et décidez où les monter, et ensuite ne les modifiez jamais à moins que vous ajoutiez un nouveau disque.

Il est tout à fait possible de n'avoir qu'un seul grand système de fichiers racine, et de ne pas en créer d'autres. Il y a quelques inconvénients à cette approche, et un avantage.

Avantages des systèmes de fichiers multiples

- Les différents systèmes de fichiers peuvent avoir différentes *options de montage*. Par exemple, avec une planification soigneuse, le système de fichiers racine peut être monté en lecture seule, rendant impossible tout effacement par inadvertance ou édition de fichier critique. La séparation des systèmes de fichiers inscriptibles par l'utilisateur permet leur montage en mode *nosuid*; cette option empêche les bits *suid*/*guid* des exécutables stockés sur ce système de fichiers de prendre effet, améliorant peut-être la sécurité.
- FreeBSD optimise automatiquement la disposition des fichiers sur un système de fichiers, selon la façon dont est utilisé le système de fichiers. Aussi un système de fichiers contenant beaucoup de petits fichiers qui sont écrits fréquemment aura une optimisation différente à celle d'un système contenant moins, ou de plus gros fichiers. En ayant un seul grand système de fichiers cette optimisation est perdue.
- Les systèmes de fichiers de FreeBSD sont très robustes même en cas de coupure secteur. Cependant une coupure secteur à un moment critique pourrait toujours endommager la structure d'un système de fichiers. En répartissant vos données sur des systèmes de fichiers multiples il est plus probable que le système redémarre, vous facilitant la restauration des données à partir de sauvegardes si nécessaire.

Avantage d'un système de fichiers unique

- Les systèmes de fichiers ont une taille fixe. Si vous créez un système de fichiers à l'installation de FreeBSD et que vous lui donnez une taille spécifique, vous pouvez plus tard vous apercevoir que vous avez besoin d'une partition plus grande. Cela n'est pas facilement faisable sans sauvegardes, recréation du système de fichiers, et enfin restauration des données.

FreeBSD dispose d'une commande, growfs(8), qui permettra d'augmenter la taille d'un système de fichiers au vol, supprimant cette limitation.

Les systèmes de fichiers sont contenus dans des partitions. Cela n'a pas la même signification que l'utilisation commune du terme partition (par exemple une partition MS-DOS®), en raison de l'héritage Unix de FreeBSD. Chaque partition est identifiée par une lettre de a à h. Chaque partition ne contient qu'un seul système de fichiers, cela signifie que les systèmes de fichiers sont souvent décrits soit par leur point de montage typique dans la hiérarchie du système de fichiers, soit par la lettre de la partition qui les contient.

FreeBSD utilise aussi de l'espace disque pour *l'espace de pagination* ("swap"). L'espace de pagination fournit à FreeBSD la *mémoire virtuelle*. Cela permet à votre ordinateur de se comporter comme s'il disposait de beaucoup plus de mémoire qu'il n'en a réellement. Quand FreeBSD vient à manquer de mémoire il déplace certaines données qui ne sont pas actuellement utilisées vers l'espace de pagination, et les rapatrie (en déplaçant quelque chose d'autre) quand il en a besoin.

Quelques partitions sont liées à certaines conventions.

Partition	Convention
a	Contient normalement le système de fichiers racine
b	Contient normalement l'espace de pagination
c	Normalement de la même taille que la tranche ("slice") contenant les partitions. Cela permet aux utilitaires devant agir sur l'intégralité de la tranche (par exemple un analyseur de blocs défectueux) de travailler sur la partition c. Vous ne devriez normalement pas créer de système de fichiers sur cette partition.
d	La partition d a eu dans le passé une signification particulière, ce n'est plus le cas aujourd'hui, et d pourra être utilisée comme une partition classique.

Chaque partition contenant un système de fichiers est stockée dans ce que FreeBSD appelle une *tranche* ("slice"). Tranche - "slice" est le terme FreeBSD pour ce qui est communément appelé partition, et encore une fois, cela en raison des fondations Unix de FreeBSD. Les tranches sont numérotées, en partant de 1, jusqu'à 4.

Les numéros de tranche suivent le nom du périphérique, avec le préfixe s, et commencent à 1. Donc "da0*s1*" est la première tranche sur le premier disque SCSI. Il ne peut y avoir que quatre tranches physiques sur un disque, mais vous pouvez avoir des tranches logiques dans des tranches physiques d'un type précis. Ces tranches étendues sont numérotées à partir de 5, donc "ad0*s5*" est la première tranche étendue sur le premier disque IDE. Elles sont utilisées par des systèmes de fichiers qui s'attendent à occuper une tranche entière.

Les tranches, les disques "en mode dédié", et les autres disques contiennent des *partitions*, qui sont représentées par des lettres allant de a à h. Cette lettre est ajoutée au nom de périphérique, aussi "da0*a*" est la partition a sur le premier disque da, qui est en "en mode dédié". "ad1s3*e*" est la cinquième partition de la troisième tranche du second disque IDE.

En conclusion chaque disque présent sur le système est identifié. Le nom d'un disque commence par un code qui indique le type de disque, suivi d'un nombre, indiquant de quel disque il s'agit. Contrairement aux tranches, la numérotation des disques commence à 0. Les codes communs que vous risquez de rencontrer sont énumérés dans le Codes des périphériques disques.

Quand vous faites référence à une partition, FreeBSD exige que vous nommiez également la tranche et le disque contenant la partition, et quand vous faites référence à une tranche vous devrez également faire référence au nom du disque. On fait donc référence à une partition en écrivant le nom du disque, s, le numéro de la tranche, et enfin la lettre de la partition. Des exemples sont donnés dans l'Exemples d'appellation de disques, tranches et partitions.

L'Modèle conceptuel d'un disque montre un exemple de l'organisation d'un disque qui devrait aider à clarifier les choses.

Afin d'installer FreeBSD vous devez tout d'abord configurer les tranches sur votre disque, ensuite créer les partitions dans la tranche que vous utiliserez pour FreeBSD, et alors créer un système de fichiers (ou espace de pagination) dans chaque partition, et décider de l'endroit où seront montés les systèmes de fichiers.

Tableau 2. Codes des périphériques disques

Code	Signification
ad	Disque ATAPI (IDE)
da	Disque SCSI
acd	CDROM ATAPI (IDE)
cd	CDROM SCSI
fd	Lecteur de disquette

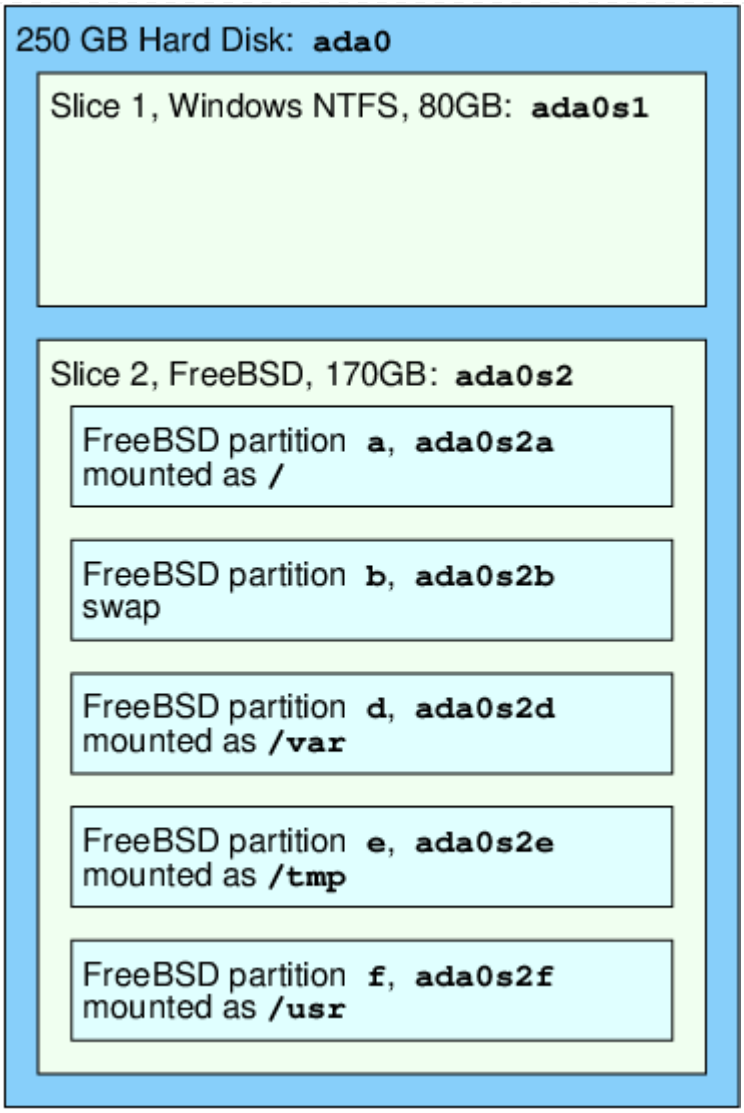
Exemple 2. Exemples d'appellation de disques, tranches et partitions

Nom	Signification
`ad0s1a`	Première partition (`a`) sur la première tranche (`s1`) du premier disque IDE (`ad0`).
`da1s2e`	Cinquième partition (`e`) sur la seconde tranche (`s2`) du deuxième disque SCSI (`da1`).

Exemple 3. Modèle conceptuel d'un disque

Ce diagramme montre comment FreeBSD voit le premier disque IDE attaché au système. Supposons que le disque a une capacité de 4 Go, et contient deux tranches de 2 Go (partitions MS-DOS®). La première tranche contient un disque MS-DOS®, C:, et la seconde tranche contient une installation de FreeBSD. Dans cet exemple l'installation de FreeBSD a trois partitions de données, et une partition de pagination.

Les trois partitions accueilleront chacune un système de fichiers. La partition `a` sera utilisée en tant que système de fichiers racine, la partition `e` pour le contenu du répertoire /var, et `f` pour l'arborescence du répertoire /usr.



3.6. Monter et démonter des systèmes de fichiers

Le système de fichiers peut être vu comme un arbre enraciné sur le répertoire /. /dev, /usr, et les autres répertoires dans le répertoire racine sont des branches, qui peuvent avoir leurs propres branches, comme /usr/local, et ainsi de suite.

Il y a diverses raisons pour héberger certains de ces répertoires sur des systèmes de fichiers séparés. /var contient les répertoires log/, spool/, et divers types de fichiers temporaires, et en tant que tels, peuvent voir leur taille augmenter de façon importante. Remplir le système de fichiers racine n'est pas une bonne idée, aussi séparer /var de / est souvent favorable.

Une autre raison courante de placer certains répertoires sur d'autres systèmes de fichiers est s'ils doivent être hébergés sur des disques physiques séparés, ou sur des disques virtuels séparés, comme les systèmes de fichiers réseau, ou les lecteurs de CDROM.

3.6.1. Le fichier fstab

Durant le processus de démarrage, les systèmes de fichiers listés dans /etc/fstab sont automatiquement montés (à moins qu'il ne soient listés avec l'option `noauto`).

Le fichier /etc/fstab contient une liste de lignes au format suivant:

```
device       /mount-point fstype     options      dumpfreq     passno
```

`device`
: Un nom de périphérique (qui devrait exister), comme expliqué dans la Noms des périphériques.

`mount-point`
: Un répertoire (qui devrait exister), sur lequel sera monté le système de fichier.

`fstype`
: Le type de système de fichiers à indiquer à mount(8). Le système de fichiers par défaut de FreeBSD est l'`ufs`.

`options`
: Soit `rw` pour des systèmes de fichiers à lecture-écriture, soit `ro` pour des systèmes de fichiers à lecture seule, suivi par toute option qui peut s'avérer nécessaire. Une option courante est `noauto` pour les systèmes de fichiers qui ne sont normalement pas montés durant la séquence de démarrage. D'autres options sont présentées dans la page de manuel mount(8).

`dumpfreq`
: C'est utilisé par dump(8) pour déterminer quels systèmes de fichiers nécessitent une sauvegarde. Si ce champ est absent, une valeur de zéro est supposée.

`passno`
: Ceci détermine l'ordre dans lequel les systèmes de fichiers devront être vérifiés. Les systèmes de fichiers qui doivent être ignorés devraient avoir leur `passno` positionné à zéro. Le système de fichiers racine (qui doit être vérifié avant tout le reste) devrait avoir son `passno` positionné à un, et les options `passno` des autres systèmes fichiers devraient être positionnées à des valeurs supérieures à un. Si plus d'un système de fichiers ont le même `passno` alors fsck(8) essaiera de vérifier les systèmes de fichiers en parallèle si c'est possible.

Consultez la page de manuel de fstab(5) pour plus d'information sur le format du fichier /etc/fstab et des options qu'il contient.

3.6.2. La commande `mount`

La commande mount(8) est ce qui est finalement utilisé pour monter des systèmes de fichiers.

Dans sa forme la plus simple, vous utilisez:

```
# mount device mountpoint
```

Il y beaucoup d'options, comme mentionné dans la page de manuel mount(8), mais les plus courantes sont:

Options de montage

`-a`

Monte tous les systèmes de fichiers listés dans /etc/fstab. Exception faite de ceux marqués comme "noauto", ou exclus par le drapeau `-t`, ou encore ceux qui sont déjà montés.

`-d`

Tout effectuer à l'exception de l'appel système de montage réel. Cette option est utile conjointement avec le drapeau `-v` pour déterminer ce que mount(8) est en train d'essayer de faire.

`-f`

Force le montage d'un système de fichiers non propre (dangereux), ou force la révocation de l'accès en écriture quand on modifie l'état de montage d'un système de fichiers de l'accès lecture-écriture à l'accès lecture seule.

`-r`

Monte le système de fichiers en lecture seule. C'est identique à l'utilisation de l'argument `ro` (`rdonly` pour les versions de FreeBSD antérieures à la 5.2) avec l'option `-o`.

`-t` ***fstype***

Monte le système de fichiers comme étant du type de système donné, ou monte seulement les systèmes de fichiers du type donné, si l'option `-a` est précisée.

"ufs" est le type de système de fichiers par défaut.

`-u`

Mets à jour les options de montage sur le système de fichiers.

`-v`

Rends la commande prolixe.

`-w`

Monte le système de fichiers en lecture-écriture.

L'option `-o` accepte une liste d'options séparées par des virgules, dont les suivantes:

noexec

Ne pas autoriser l'exécution de binaires sur ce système de fichiers. C'est également une option de sécurité utile.

nosuid

Ne pas prendre en compte les indicateurs setuid ou setgid sur le système de fichiers. C'est également une option de sécurité utile.

3.6.3. La commande `umount`

La commande umount(8) prend, comme paramètre, un des points de montage, un nom de périphérique, ou l'option `-a` ou `-A`.

Toutes les formes acceptent `-f` pour forcer de démontage, et `-v` pour le mode prolixe. Soyez averti

que l'utilisation de `-f` n'est généralement pas une bonne idée. Démonter de force des systèmes de fichiers pourrait faire planter l'ordinateur ou endommager les données sur le système de fichiers.

Les options `-a` et `-A` sont utilisées pour démonter tous les systèmes de fichiers actuellement montés, éventuellement modifié par les types de systèmes de fichiers listés après l'option `-t`. Cependant l'option `-A`, n'essaye pas de démonter le système de fichiers racine.

3.7. Processus

FreeBSD est un système d'exploitation multi-tâches. Cela veut dire qu'il semble qu'il y ait plus d'un programme fonctionnant à la fois. Tout programme fonctionnant à un moment donné est appelé un *processus*. Chaque commande que vous utiliserez lancera au moins un nouveau processus, et il y a de nombreux processus système qui tournent constamment, maintenant ainsi les fonctionnalités du système.

Chaque processus est identifié de façon unique par un nombre appelé *process ID* (identifiant de processus), ou *PID*, et, comme pour les fichiers, chaque processus possède également un propriétaire et un groupe. Les informations sur le propriétaire et le groupe sont utilisées pour déterminer quels fichiers et périphériques sont accessibles au processus, en utilisant le principe de permissions de fichiers abordé plus tôt. La plupart des processus ont également un processus parent. Le processus parent est le processus qui les a lancés. Par exemple, si vous tapez des commandes sous un interpréteur de commandes, alors l'interpréteur de commandes est un processus, et toute commande que vous lancez est aussi un processus. Chaque processus que vous lancez de cette manière aura votre interpréteur de commandes comme processus parent. Une exception à cela est le processus spécial appelé init(8). `init` est toujours le premier processus, donc son PID est toujours 1. `init` est lancé automatiquement par le noyau au démarrage de FreeBSD.

Deux commandes sont particulièrement utiles pour voir les processus sur le système, ps(1) et top(1). La commande `ps` est utilisée pour afficher une liste statique des processus tournant actuellement, et peut donner leur PID, la quantité de mémoire qu'ils utilisent, la ligne de commande par l'intermédiaire de laquelle ils ont été lancés, et ainsi de suite. La commande top(1) affiche tous les processus, et actualise l'affichage régulièrement, de sorte que vous puissiez voir de façon intéractive ce que fait l'ordinateur.

Par défaut, ps(1) n'affiche que les commandes que vous faites tourner et dont vous êtes le propriétaire. Par exemple:

```
% ps
  PID  TT  STAT      TIME COMMAND
  298  p0  Ss     0:01.10 tcsh
 7078  p0  S      2:40.88 xemacs mdoc.xsl (xemacs-21.1.14)
37393  p0  I      0:03.11 xemacs freebsd.dsl (xemacs-21.1.14)
48630  p0  S      2:50.89 /usr/local/lib/netscape-linux/navigator-linux-4.77.bi
48730  p0  IW     0:00.00 (dns helper) (navigator-linux-)
72210  p0  R+     0:00.00 ps
  390  p1  Is     0:01.14 tcsh
 7059  p2  Is+    1:36.18 /usr/local/bin/mutt -y
 6688  p3  IWs    0:00.00 tcsh
10735  p4  IWs    0:00.00 tcsh
```

```
20256  p5  IWs    0:00.00 tcsh
  262  v0  IWs    0:00.00 -tcsh (tcsh)
  270  v0  IW+    0:00.00 /bin/sh /usr/X11R6/bin/startx -- -bpp 16
  280  v0  IW+    0:00.00 xinit /home/nik/.xinitrc -- -bpp 16
  284  v0  IW     0:00.00 /bin/sh /home/nik/.xinitrc
  285  v0  S      0:38.45 /usr/X11R6/bin/sawfish
```

Comme vous pouvez le voir dans cet exemple, la sortie de ps(1) est organisée en un certain nombre de colonnes. PID est l'identifiant de processus discuté plus tôt. Les PIDs sont assignés à partir de 1, et vont jusqu'à 99999, et puis repassent à 1 quand le maximum est atteint (un PID n'est pas réassigné s'il est déjà utilisé). La colonne TT donne le terminal sur lequel tourne le programme, et peut être pour le moment ignoré sans risque. STAT affiche l'état du programme, peut être également ignoré. TIME est la durée d'utilisation du CPU-ce n'est généralement pas le temps écoulé depuis que vous avez lancé le programme, comme la plupart des programmes passent beaucoup de temps à attendre que certaines choses se produisent avant qu'ils n'aient besoin de dépenser du temps CPU. Et enfin, COMMAND est la ligne de commande qui a été utilisée lors du lancement du programme.

ps(1) supporte un certain nombre d'options différentes pour modifier les informations affichées. Un des ensembles d'options les plus utiles est auxww. a affiche l'information au sujet de tous les processus tournant, et pas seulement les vôtres. u donne le nom de l'utilisateur du propriétaire du processus, ainsi que l'utilisation de la mémoire. x affiche des informations sur les processus "daemon", et ww oblige ps(1) à afficher la ligne de commande complète pour chaque processus, plutôt que de la tronquer quand elle est trop longue pour tenir à l'écran.

La sortie de top(1) est semblable. Un extrait de session ressemble à ceci:

```
% top
last pid: 72257;  load averages:  0.13,  0.09,  0.03    up 0+13:38:33  22:39:10
47 processes:  1 running, 46 sleeping
CPU states: 12.6% user,  0.0% nice,  7.8% system,  0.0% interrupt, 79.7% idle
Mem: 36M Active, 5256K Inact, 13M Wired, 6312K Cache, 15M Buf, 408K Free
Swap: 256M Total, 38M Used, 217M Free, 15% Inuse

  PID USERNAME PRI NICE  SIZE    RES STATE    TIME   WCPU    CPU COMMAND
72257 nik       28   0  1960K  1044K RUN      0:00 14.86%  1.42% top
 7078 nik        2   0 15280K 10960K select   2:54  0.88%  0.88% xemacs-21.1.14
  281 nik        2   0 18636K  7112K select   5:36  0.73%  0.73% XF86_SVGA
  296 nik        2   0  3240K  1644K select   0:12  0.05%  0.05% xterm
48630 nik        2   0 29816K  9148K select   3:18  0.00%  0.00% navigator-linu
  175 root       2   0   924K   252K select   1:41  0.00%  0.00% syslogd
 7059 nik        2   0  7260K  4644K poll     1:38  0.00%  0.00% mutt
...
```

La sortie est divisée en deux sections. L'entête (les cinq premières lignes) donne le PID du dernier processus lancé, la charge système moyenne (qui est une mesure de l'occupation du système), la durée de fonctionnement du système (le temps écoulé depuis le dernier redémarrage), et l'heure actuelle. Les autres éléments de l'entête concernent le nombre de processus en fonctionnement (47 dans notre cas), combien d'espace mémoire et d'espace de pagination sont occupés, et combien de

temps le système passe dans les différents états du CPU.

En dessous il y a une série de colonnes contenant des informations semblables à celles données par ps(1). Comme précédemment vous pouvez lire le PID, le nom d'utilisateur, la quantité de temps CPU consommée, et la commande qui a été lancée. top(1) vous affiche par défaut la quantité d'espace mémoire utilisée par chaque processus. Cela est divisé en deux colonnes, une pour la quantité totale, et une autre pour la quantité résidente-la quantité totale représente l'espace mémoire dont a eu besoin l'application, et la quantité résidente représente l'espace qui est en fait utilisé actuellement. Dans cet exemple vous pouvez voir que getenv(3) a exigé presque 30 Mo de RAM, mais utilise actuellement seulement 9Mo.

top(1) actualise l'affichage toutes les deux secondes; cela peut être modifié avec l'option `s`.

3.8. Daemons, signaux, et comment tuer un processus

Quand vous utilisez un éditeur il est facile de le contrôler, de lui dire de charger des fichiers, et ainsi de suite. Vous pouvez faire cela parce que l'éditeur fournit les possibilités de le faire, et parce qu'un éditeur est attaché à un *terminal*. Certains programmes ne sont pas conçus pour fonctionner avec un dialogue constant avec l'utilisateur, et donc ils se déconnectent du terminal à la première occasion. Par exemple, un serveur web passe son temps à répondre aux requêtes web, il n'attend normalement pas d'entrée de votre part. Les programmes qui transportent le courrier électronique de site en site sont un autre exemple de cette classe d'application.

Nous appelons ces programmes des *daemons* (démons). Les "daemons" étaient des personnages de la mythologie Grecque: ni bon ni mauvais, c'étaient de petits esprits serviteurs qui, généralement, ont été à l'origine de choses utiles à l'humanité, un peu comme les serveurs web ou de messagerie d'aujourd'hui nous sont utiles. C'est pourquoi la mascotte BSD a été, pendant longtemps, un démon à l'apparence joyeuse portant des chaussures de tennis et une fourche.

Il existe une convention pour nommer les programmes qui fonctionnent normalement en tant que daemons qui est d'utiliser une terminaison en "d". BIND est le "Berkeley Internet Name Domain", mais le programme réel qui est exécuté s'appelle `named`); le programme correspondant au serveur web Apache est appelé `httpd`; le daemon de gestion de la file d'attente de l'imprimante est `lpd`, et ainsi de suite. C'est une convention, mais pas une obligation pure et simple; par exemple le daemon principal de gestion du courrier électronique pour l'application Sendmail est appelé `sendmail`, et non pas `maild`, comme vous pourriez l'imaginer.

Parfois vous devrez communiquer avec un processus daemon. Une manière de procéder est de lui (ou à tout processus en cours d'exécution) envoyer ce que l'on appelle un *signal*. Il existe un certain nombre de signaux différents que vous pouvez envoyer-certains d'entre eux ont une signification précise, d'autres sont interprétés par l'application, et la documentation de l'application vous indiquera comment l'application interprète ces signaux. Vous ne pouvez envoyer de signaux qu'aux processus dont vous êtes le propriétaire. Si vous envoyez un signal à un processus appartenant à quelqu'un d'autre avec kill(1) ou kill(2), vous obtiendrez un refus de permission. Il existe une exception à cela: l'utilisateur `root`, qui peut envoyer des signaux aux processus de chacun.

Dans certain cas FreeBSD enverra également aux applications des signaux. Si une application est mal écrite, et tente d'accéder à une partie de mémoire à laquelle elle n'est pas supposée avoir accès, FreeBSD envoie au processus le signal de *violation de segmentation* (`SIGSEGV`). Si une application a

utilisé l'appel système alarm(3) pour être avertie dès qu'une période de temps précise est écoulée alors lui sera envoyé le signal d'alarme (SIGALRM), et ainsi de suite.

Deux signaux peuvent être utilisés pour arrêter un processus, SIGTERM et SIGKILL. SIGTERM est la manière polie de tuer un processus; le processus peut *attraper* le signal, réaliser que vous désirez qu'il se termine, fermer les fichiers de trace qu'il a peut-être ouvert, et généralement finir ce qu'il était en train de faire juste avant la demande d'arrêt. Dans certains cas un processus peut ignorer un SIGTERM s'il est au milieu d'une tâche qui ne peut être interrompue.

SIGKILL ne peut être ignoré par un processus. C'est le signal "Je me fiche de ce que vous faites, arrêtez immédiatement". Si vous envoyez un SIGKILL à un processus alors FreeBSD stoppera le processus.

Les autres signaux que vous pourriez avoir envie d'utiliser sont SIGHUP, SIGUSR1, et SIGUSR2. Ce sont des signaux d'usage général, et différentes applications se comporteront différemment quand ils sont envoyés.

Supposez que vous avez modifié le fichier de configuration de votre serveur web-vous voudriez dire à votre serveur web de relire son fichier de configuration. Vous pourriez arrêter et relancer httpd, mais il en résulterait une brève période d'indisponibilité de votre serveur web, ce qui peut être indésirable. La plupart des daemons sont écrits pour répondre au signal SIGHUP en relisant leur fichier de configuration. Donc au lieu de tuer et relancer httpd vous lui enverriez le signal SIGHUP. Parce qu'il n'y a pas de manière standard de répondre à ces signaux, différents daemons auront différents comportements, soyez sûr de ce que vous faites et lisez la documentation du daemon en question.

Les signaux sont envoyés en utilisant la commande kill(1), comme cet exemple le montre:

Procedure: Envoyer un signal à un processus

Cet exemple montre comment envoyer un signal à inetd(8). Le fichier de configuration d'inetd est /etc/inetd.conf, et inetd relira ce fichier de configuration quand un signal SIGHUP est envoyé.

1. Trouvez l'identifiant du processus (PID) auquel vous voulez envoyer le signal. Faites-le en employant ps(1) et grep(1). La commande grep(1) est utilisée pour rechercher dans le résultat la chaîne de caractères que vous spécifiez. Cette commande est lancée en tant qu'utilisateur normal, et inetd(8) est lancé en tant que root, donc les options ax doivent être passées à ps(1).

   ```
   % ps -ax | grep inetd
     198  ??  IWs    0:00.00 inetd -wW
   ```

   Donc le PID d'inetd(8) est 198. Dans certains cas la commande grep inetd pourrait aussi apparaître dans le résultat. C'est à cause de la façon dont ps(1) recherche la liste des processus en fonctionnement.

2. Utilisez kill(1) pour envoyer le signal. Etant donné qu'inetd(8) tourne sous les droits de l'utilisateur root vous devez utilisez su(1) pour devenir, en premier lieu, root.

```
% su
Password:
# /bin/kill -s HUP 198
```

Comme la plupart des commandes UNIX®, kill(1) n'affichera rien si la commande est couronnée de succès. Si vous envoyez un signal à un processus dont vous n'êtes pas le propriétaire alors vous verrez `kill: PID: Operation not permitted`. Si vous avez fait une erreur dans le PID, vous enverrez le signal soit à un mauvais processus, ce qui peut être mauvais, soit, si vous êtes chanceux, vous enverrez le signal à un PID qui n'est pas actuellement utilisé, et vous verrez `kill: PID: No such process`.

Pourquoi utiliser `/bin/kill`?

De nombreux interpréteurs de commandes fournissent la commande `kill` comme commande interne; c'est à dire, que l'interpréteur de commandes enverra directement le signal, plutôt que de lancer /bin/kill. Cela peut être utile, cependant les différents interpréteurs ont une syntaxe différente pour spécifier le nom du signal à envoyer. Plutôt que de tenter de les apprendre toutes, il peut être plus simple de juste employer directement la commande `/bin/kill …`.

Envoyer d'autres signaux est très semblable, substituez juste `TERM` ou `KILL` dans la ligne de commande si nécessaire.

Tuer au hasard des processus sur le système peut être une mauvaise idée. En particulier, init(8), processus à l'identifiant 1, qui est très particulier. Lancer la commande `/bin/kill -s KILL 1` est une manière rapide d'arrêter votre système. Vérifiez *toujours* à deux fois les arguments que vous utilisez avec kill(1) *avant* d'appuyer sur `Entrée`.

3.9. Interpréteurs de commandes - "Shells"

Sous FreeBSD, beaucoup du travail quotidien est effectué sous une interface en ligne de commande appelée interpréteur de commandes ou "shell". Le rôle principal d'un interpréteur de commandes est de prendre les commandes sur le canal d'entrée et de les exécuter. Beaucoup d'interpréteurs de commandes ont également des fonctions intégrées pour aider dans les tâches quotidiennes comme la gestion de fichiers, le mécanisme de remplacement et d'expansion des jokers ("file globbing"), l'édition de la ligne de commande, les macros commandes, et les variables d'environnement. FreeBSD est fournit avec un ensemble d'interpréteurs de commandes, comme `sh`, l'interpréteur de commandes Bourne, et `tcsh`, l'interpréteur de commandes C-shell amélioré. Beaucoup d'autres interpréteurs de commandes sont disponibles dans le catalogue des logiciels portés, comme `zsh` et `bash`.

Quel interpréteur de commandes utilisez-vous? C'est vraiment une question de goût. Si vous programmez en C vous pourriez vous sentir plus à l'aise avec un interpréteur de commandes proche du C comme `tcsh`. Si vous venez du monde Linux ou que vous êtes nouveau à l'interface en

ligne de commande d'UNIX® vous pourriez essayer `bash`. L'idée principale est que chaque interpréteur de commandes à des caractéristiques uniques qui peuvent ou ne peuvent pas fonctionner avec votre environnement de travail préféré, et que vous avez vraiment le choix de l'interpréteur de commandes à utiliser.

Une des caractéristiques communes des interpréteurs de commandes est de pouvoir compléter les noms de fichiers ("filename completion"). En tapant les premières lettres d'une commande ou d'un fichier, vous pouvez habituellement faire compléter automatiquement par l'interpréteur de commandes le reste de la commande ou du nom du fichier en appuyant sur la touche `Tab` du clavier. Voici un exemple. Supposez que vous avez deux fichiers appelés respectivement foobar et foo.bar. Vous voulez effacer foo.bar. Donc ce que vous devriez taper sur le clavier est: `rm fo[Tab].[Tab]`.

L'interpréteur de commandes devrait afficher `rm foo[BEEP].bar`.

Le [BEEP] est la sonnerie de la console, c'est l'interpréteur de commande indiquant qu'il n'est pas en mesure de compléter totalement le nom du fichier parce qu'il y a plus d'une possibilité. foobar et foo.bar commencent tous les deux par `fo`, mais il fut capable de compléter jusqu'à `foo`. Si vous tapez `.`, puis appuyez à nouveau sur `Tab`, l'interpréteur de commandes devrait pouvoir compléter le reste du nom du fichier pour vous.

Une autre caractéristique de l'interpréteur de commandes est l'utilisation de variables d'environnement. Les variables d'environnement sont une paire variable/valeur stockées dans l'espace mémoire d'environnement de l'interpréteur de commandes. Cet espace peut être lu par n'importe quel programme invoqué par l'interpréteur de commandes, et contient ainsi beaucoup d'éléments de configuration des programmes. Voici une liste des variables d'environnement habituelles et ce qu'elles signifient:

Variable	Description
`USER`	Le nom d'utilisateur de la personne actuellement attachée au système.
`PATH`	La liste des répertoires, séparés par deux points, pour la recherche des programmes.
`DISPLAY`	Le nom réseau de l'affichage X11 auquel on peut se connecter, si disponible.
`SHELL`	Le nom de l'interpréteur de commandes actuellement utilisé.
`TERM`	Le nom du type de terminal de l'utilisateur. Utilisé pour déterminer les capacités du terminal.
`TERMCAP`	L'entrée de la base de données des codes d'échappement pour permettre l'exécution de diverses fonctions du terminal.
`OSTYPE`	Type du système d'exploitation, e.g. FreeBSD.

Variable	Description
MACHTYPE	L'architecture du CPU sur lequel tourne actuellement le système.
EDITOR	L'éditeur de texte préferé de l'utilisateur.
PAGER	Le visualisateur de page de texte préferré de l'utilisateur.
MANPATH	La liste des répertoires, séparés par deux points, pour la recherche des pages de manuel.

Fixer une variable d'environnement diffère légèrement d'un interpréteur de commandes à l'autre. Par exemple, dans le style de l'interpréteur de commandes de type C-shell comme `tcsh` et `csh`, vous utiliseriez `setenv` pour fixer le contenu d'une variable d'environnement. Sous les interpréteurs de commandes Bourne comme `sh` et `bash`, vous utiliseriez `export` pour configurer vos variables d'environnement. Par exemple, pour fixer ou modifier la variable d'environnement `EDITOR`, sous `csh` ou `tcsh` une commande comme la suivante fixera `EDITOR` à /usr/local/bin/emacs:

```
% setenv EDITOR /usr/local/bin/emacs
```

Sous les interpréteurs de commandes Bourne:

```
% export EDITOR="/usr/local/bin/emacs"
```

Vous pouvez faire afficher à la plupart des interpréteurs de commandes la variable d'environnement en plaçant un caractère `$` juste devant son nom sur la ligne de commande. Par exemple, `echo $TERM` affichera le contenu de `$TERM`, car l'interpréteur de commande complète `$TERM` et passe la main à `echo`.

Les interpréteurs de commandes traitent beaucoup de caractères spéciaux, appelés métacaractères, en tant que représentation particulière des données. Le plus commun est le caractère `*`, qui représente zéro ou plusieurs caractères dans le nom du fichier. Ces métacaractères spéciaux peuvent être utilisés pour compléter automatiquement le nom des fichiers. Par exemple, taper `echo *` est presque la même chose que taper `ls` parce que l'interpréteur de commandes prendra tous les fichiers qui correspondent à `*` et les passera à `echo` pour les afficher.

Pour éviter que l'interpréteur de commande n'interprète les caractères spéciaux, ils peuvent être neutralisés en ajoutant un caractère antislash (`\`) devant. `echo $TERM` affichera votre type de terminal. `echo \$TERM` affichera `$TERM` tel quel.

3.9.1. Changer d'interpréteur de commandes

La méthode la plus simple pour changer votre interpréteur de commandes est d'utiliser la commande `chsh`. En lançant `chsh` vous arriverez dans l'éditeur correspondant à votre variable d'environnement `EDITOR`; si elle n'est pas fixée, cela sera `vi`. Modifiez la ligne "Shell:" en conséquence.

Vous pouvez également passer le paramètre `-s` à `chsh`; cela modifiera votre interpréteur de commandes sans avoir à utiliser un éditeur. Par exemple, si vous vouliez changer votre interpréteur de commandes pour `bash`, ce qui suit devrait faire l'affaire:

```
% chsh -s /usr/local/bin/bash
```

L'interpréteur de commandes que vous désirez utiliser *doit* être présent dans le fichier /etc/shells. Si vous avez installé l'interpréteur de commandes à partir du catalogue des logiciels portés, alors cela a dû déjà être fait pour vous. Si vous avez installé à la main l'interpréteur de commandes, vous devez alors le faire.

Par exemple, si vous avez installé `bash` à la main et l'avez placé dans /usr/local/bin, vous devrez faire:

```
# echo /usr/local/bin/bash  /etc/shells
```

Puis relancer `chsh`.

3.10. Editeurs de texte

Beaucoup de configurations sous FreeBSD sont faites en éditant des fichiers textes. Aussi ce serait une bonne idée de se familiariser avec un éditeur de texte. FreeBSD est fourni avec quelques-uns en tant qu'éléments du système de base, et beaucoup d'autres sont disponibles dans le catalogue des logiciels portés.

L'éditeur de plus facile et le plus simple à apprendre est un éditeur appelé ee, qui signifie l'éditeur facile (easy editor). Pour lancer ee, on taperait sur la ligne de commande `ee fichier` où *fichier* est le nom du fichier qui doit être édité. Par exemple, pour éditer /etc/rc.conf, tapez `ee /etc/rc.conf`. Une fois sous `ee`, toutes les commandes pour utiliser les fonctions de l'éditeur sont affichées en haut de l'écran. Le caractère `^` représente la touche `Ctrl` sur le clavier, donc `^e` représente la combinaison de touches `Ctrl` + `e`. Pour quitter ee, appuyez sur la touche `Echap`, ensuite choisissez "leave editor". L'éditeur vous demandera s'il doit sauver les changements si le fichier a été modifié.

FreeBSD est également fourni avec des éditeurs de texte plus puissants comme vi en tant qu'élément du système de base, alors que d'autres éditeurs, comme Emacs et vim, en tant qu'élément du catalogue des logiciels portés de FreeBSD (editors/emacs et editors/vim). Ces éditeurs offrent beaucoup plus de fonctionnalités et de puissance aux dépens d'être un peu plus compliqués à apprendre. Cependant si vous projetez de faire beaucoup d'édition de texte, l'étude d'un éditeur plus puissant comme vim ou Emacs vous permettra d'économiser beaucoup plus de temps à la longue.

3.11. Périphériques et fichiers spéciaux de périphérique

Un périphérique est un terme utilisé la plupart du temps pour les activités en rapport avec le

matériel présent sur le système, incluant les disques, les imprimantes, les cartes graphiques, et les claviers. Quand FreeBSD démarre, la majorité de ce qu'affiche FreeBSD est la détection des périphériques. Vous pouvez à nouveau consulter les messages de démarrage en visualisant le fichier /var/run/dmesg.boot.

Par exemple, acd0 est le premier lecteur de CDROM IDE, tandis que kbd0 représente le clavier.

La plupart de ces périphériques sous un système d'exploitation UNIX® peuvent être accédés par l'intermédiaire de fichiers appelés fichiers spéciaux de périphérique ("device node"), qui sont situés dans le répertoire /dev.

3.11.1. Créer des fichiers spéciaux de périphérique

Quand vous ajoutez un nouveau périphérique à votre système, ou compilez le support pour des périphériques supplémentaires, de nouveaux fichiers spéciaux de périphérique doivent être créés.

3.11.1.1. DEVFS ("DEVice File System" - Système de fichiers de périphérique)

Le système de fichiers de périphérique, ou DEVFS, fournit un accès à l'espace nom des périphériques du noyau dans l'espace nom du système de fichiers global. Au lieu d'avoir à créer et modifier les fichiers spéciaux de périphérique, DEVFS maintient ce système de fichiers particulier pour vous.

Voir la page de manuel de devfs(5) pour plus d'information.

3.12. Le format des fichiers binaires

Afin de comprendre pourquoi FreeBSD utilise le format elf(5), vous devez d'abord connaître quelques détails concernant les trois formats "dominants" d'exécutables actuellement en vigueur sous UNIX®:

- a.out(5)

  Le plus vieux et le format objet "classique" d'UNIX®. Il utilise une entête courte et compacte avec un nombre magique au début qui est souvent utilisé pour caractériser le format (voir la page de manuel a.out(5) pour plus de détails). Il contient trois segments chargés: .text, .data, et .bss plus une table de symboles et une table de chaînes de caractères.

- COFF

  Le format objet SVR3. L'entête comprend une table de section, de telle sorte que vous avez plus de sections qu'uniquement .text, .data et .bss.

- elf(5)

  Le successeur de COFF, qui permet des sections multiples et des valeurs possibles de 32 bits et 64 bits. Un inconvénient majeur: ELF a aussi été conçu en supposant qu'il y aurait qu'un seul ABI par architecture système. Cette hypothèse est en fait assez incorrecte, et même dans le monde SYSV (qui a au moins trois ABIs: SVR4, Solaris, SCO) cela ne se vérifie pas.

  FreeBSD essaye de contourner ce problème en fournissant un utilitaire pour *marquer* un

exécutable connu ELF avec des informations sur l'ABI qui va avec. Consultez la page de manuel de brandelf(1) pour plus d'informations.

FreeBSD vient du camp "classique" et a utilisé le format a.out(5), une technologie employée et éprouvée à travers des générations de BSDs, jusqu'aux débuts de la branche 3.X. Bien qu'il fut possible de compiler et d'exécuter des binaires natifs ELF (et noyaux) sous FreeBSD avant cela, FreeBSD a initialement résisté à la "pression" de passer à ELF comme format par défaut. Pourquoi? Bien, quand le camp Linux ont fait leur pénible transition vers ELF, ce n'est pas tant fuir le format a.out qui rendait difficile la construction de bibliothèques partagée pour les développeurs mais le mécanisme de bibliothèques partagées basé sur des tables de sauts inflexible. Puisque les outils ELF disponibles offraient une solution au problème des bibliothèques partagées et étaient perçus comme "le chemin à suivre" de toute façon, le coût de la migration a été accepté comme nécessaire, et la transition a été réalisée. Le mécanisme FreeBSD de bibliothèques partagées se rapproche plus du style de mécanisme de bibliothèques partagées de SunOS™ de Sun, et est très simple à utiliser.

Pourquoi existe-t-il tant de formats différents?

Dans un obscure et lointain passé, il y avait du matériel simple. Ce matériel simple supportait un simple petit système. a.out était complètement adapté pour représenter les binaires sur ce système simple (un PDP-11). Au fur et à mesure que des personnes portaient UNIX® à partir de ce système simple, ils ont maintenus le format a.out parce qu'il était suffisant pour les premiers portages d'UNIX® sur des architectures comme le Motorola 68k, les VAX, etc.

Alors un certain ingénieur matériel brillant a décidé qu'il pourrait forcer le matériel à faire des choses bizarre, l'autorisant ainsi à réduire le nombre de portes logiques et permettant au coeur du CPU de fonctionner plus rapidement. Bien qu'on l'a fait fonctionner avec ce nouveau type de matériel (connu de nos jour sous le nom de RISC), a.out n'était pas adapté à ce matériel, aussi beaucoup de formats ont été développés pour obtenir de meilleures performances de ce matériel que ce que pouvait offrir le simple et limité format qu'était a.out. Des choses comme COFF, ECOFF, et quelques autres obscures formats ont été inventé et leur limites explorées avant que les choses ne se fixent sur ELF.

En outre, les tailles des programmes devenaient énormes alors que les disques (et la mémoire physique) étaient toujours relativement petits, aussi le concept de bibliothèque partagée est né. Le système de VM (mémoire virtuelle) est également devenu plus sophistiqué. Tandis que chacune de ces avancées était faites en utilisant le format a.out, son utilité a été élargie de plus en plus avec chaque nouvelle fonction. De plus les gens ont voulu charger dynamiquement des choses à l'exécution, ou se débarrasser de partie de leur programme après l'initialisation pour économiser de l'espace mémoire et de pagination. Les langages sont devenus plus sophistiqués et les gens ont voulu du code appelé automatiquement avant la partie principale du programme. Beaucoup de modifications ont été apportées au format a.out pour rendre possible toutes ces choses, et cela a fonctionné pendant un certain temps. Avec le temps, a.out n'était plus capable de gérer tous ces problèmes sans une augmentation toujours croissante du code et de sa complexité. Tandis ELF résolvait plusieurs de ces problèmes, il aurait été pénible de quitter un système qui a fonctionné. Ainsi ELF a dû attendre jusqu'au moment où il était plus pénible de rester avec a.out que d'émigrer vers ELF.

Cependant, avec le temps, les outils de compilation desquels ceux de FreeBSD sont dérivés (l'assembleur et le chargeur tout spécialement) ont évolué en parallèle. Les développeurs FreeBSD

ajoutèrent les bibliothèques partagées et corrigèrent quelques bogues. Les gens de chez GNU qui ont à l'origine écrit ces programmes, les récrivirent et ajoutèrent un support plus simple pour la compilation multi-plateformes, avec différents formats à volonté, et ainsi de suite. Lorsque beaucoup de personnes ont voulu élaborer des compilateurs multi-plateformes pour FreeBSD, elles n'eurent pas beaucoup de chance puisque les anciennes sources que FreeBSD avait pour as et ld n'étaient pas adaptées à cette tâche. Le nouvel ensemble d'outils de GNU (binutils) supporte la compilation multi-plateformes, ELF, les bibliothèques partagées, les extensions C++, etc. De plus, de nombreux vendeurs de logiciels fournissent des binaires ELF, et c'est une bonne chose pour permettre leur exécution sous FreeBSD.

ELF est plus expressif qu'a.out et permet plus d'extensibilité dans le système de base. Les outils ELF sont mieux maintenus, et offrent un support pour la compilation multi-plateformes, ce qui est important pour de nombreuses personnes. ELF peut être légèrement plus lent qu'a.out, mais tenter de mesurer cette différence n'est pas aisé. Il y a également de nombreux détails qui diffèrent entre les deux dans la façon dont ils mappent les pages mémoire, gère le code d'initialisation, etc. Dans le futur, le support a.out sera retiré du noyau GENERIC, et par la suite retiré des sources du noyau une fois que le besoin d'exécuter d'anciens programmes a.out aura disparu.

3.13. Pour plus d'information

3.13.1. Les pages de manuel

La documentation la plus complète sur FreeBSD est sous la forme de pages de manuel. Presque chaque programme sur le système est fournit avec un court manuel de référence expliquant l'utilisation de base et les diverses options. Ces manuels peuvent être visualisés avec la commande `man`. L'utilisation de la commande `man` est simple:

```
% man command
```

`command` est le nom de la commande à propos de laquelle vous désirez en savoir plus. Par exemple, pour en savoir plus au sujet de la commande `ls` tapez:

```
% man ls
```

Les manuels en ligne sont divisés en sections numérotées:

1. Commandes utilisateur.
2. Appels système et numéros d'erreur.
3. Fonctions des bibliothèques C.
4. Pilotes de périphérique.
5. Formats de fichier.
6. Jeux et autres divertissements.
7. Information diverse.

8. Commandes de maintenance et d'utilisation du système.
9. Information de développement du noyau.

Dans certains cas, le même sujet peut apparaître dans plus d'une section du manuel en ligne. Par exemple, il existe une commande utilisateur `chmod` et un appel système `chmod()`. Dans ce cas, vous pouvez préciser à la commande `man` laquelle vous désirez en spécifiant la section:

```
% man 1 chmod
```

Cela affichera la page de manuel de la commande utilisateur `chmod`. Les références à une section particulière du manuel en ligne sont traditionnellement placées entre parenthèses, ainsi chmod(1) se rapporte à la commande utilisateur `chmod` et chmod(2) se rapporte à l'appel système.

C'est parfait si vous connaissez le nom de la commande et vous souhaitez simplement savoir comment l'utiliser, mais qu'en est-il si vous ne pouvez pas vous rappelez du nom de la commande? Vous pouvez utiliser `man` pour rechercher des mots-clés dans les descriptions de commandes en employant l'option `-k`:

```
% man -k mail
```

Avec cette commande on vous affichera la liste des commandes qui ont le mot-clé "mail" dans leurs descriptions. C'est en fait équivalent à l'utilisation de la commande `apropos`.

Ainsi, vous regardez toutes ces commandes fantaisistes contenues dans /usr/bin mais vous n'avez pas la moindre idée de ce quelles font vraiment? Faites simplement:

```
% cd /usr/bin
% man -f *
```

ou

```
% cd /usr/bin
% whatis *
```

ce qui fait la même chose.

3.13.2. Fichiers GNU Info

FreeBSD inclut beaucoup d'applications et d'utilitaires produit par la Fondation pour le Logiciel Libre (Free Software Foundation). En plus des pages de manuel, ces programmes sont fournis avec des documents hypertexte appelés fichiers `info` qui peuvent être lus avec la commande `info` ou, si vous avez installé emacs, dans le mode info d'emacs.

Pour utiliser la commande info(1), tapez simplement:

```
% info
```

Pour une brève introduction, tapez h. Pour une référence rapide sur la commande, tapez ?.

Chapitre 4. Installer des applications: les logiciels pré-compilés et les logiciels portés

4.1. Synopsis

FreeBSD est livré avec une riche collection d'outils en tant que partie du système de base. Beaucoup de choses peuvent être faites avant d'avoir besoin de recourir à l'installation d'une application tiers pour effectuer un travail précis. FreeBSD fournit deux technologies complémentaires pour installer des logiciels tiers sur votre système: le Catalogue des logiciels portés de FreeBSD (pour une installation à partir des sources), et les logiciels pré-compilés ou "paquetages" (pour installer des binaires pré-compilés). N'importe laquelle de ces deux méthodes peut être utilisée pour installer les nouvelles versions de vos applications favorites à partir d'un support local ou directement depuis le réseau.

Après la lecture de ce chapitre, vous saurez:

- Comment installer des logiciels tiers pré-compilés.
- Comment compiler des logiciels tiers à partir des sources en utilisant le catalogue de logiciels portés.
- Comment effacer les logiciels pré-compilés ou portés précédemment installés.
- Comment modifier les paramètres par défaut utilisés par le catalogue des logiciels portés.
- Comment trouver l'application recherchée.
- Comment mettre à jour vos applications.

4.2. Généralités sur l'installation de logiciels

Si vous avez utilisé auparavant un système UNIX® vous saurez que la procédure typique pour installer les logiciels tiers ressemble à ceci:

1. Télécharger le logiciel, qui peut être distribué sous forme de code source, ou sous forme d'un binaire.
2. Extraire le logiciel de son format de distribution (généralement une archive tar compressée soit avec compress(1), soit avec gzip(1), ou encore bzip2(1)).
3. Recherchez la documentation (peut être un fichier INSTALL ou README, ou des fichiers dans un sous répertoire doc/) et lisez les informations sur comment installer le logiciel.
4. Si le logiciel était distribué sous forme de sources, compilez-le. Cela peut impliquer l'édition d'un Makefile, ou l'exécution d'une procédure `configure`, et d'autres activités.
5. Tester et installer le logiciel.

Et cela si seulement tout se passe bien. Si vous installez un logiciel qui n'a pas été spécialement porté pour FreeBSD, il se peut que vous deviez éditer le code source pour le faire fonctionner

correctement.

Si vous le voulez, vous pouvez continuer d'installer des logiciels suivant la méthode "traditionnelle" sous FreeBSD. Cependant, FreeBSD fournit deux technologies avec lesquelles vous pouvez vous économiser beaucoup d'efforts: les logiciels pré-compilés et le catalogue des logiciels portés. A l'heure de l'écriture de ces lignes, plus de 36000 applications tierces sont ainsi mises à disposition.

Pour n'importe quelle application donnée, le logiciel pré-compilé FreeBSD pour cette application est un unique fichier à télécharger. Il contient les copies pré-compilées de toutes les commandes de l'application, ainsi que tous fichiers de configuration et documentation. Un logiciel pré-compilé téléchargé peut être manipulé avec les commandes FreeBSD de gestion des logiciels pré-compilés, comme pkg_add(1), pkg_delete(1), pkg_info(1), et ainsi de suite. L'installation d'une nouvelle application peut être effectuée grâce à une unique commande.

Un logiciel porté pour FreeBSD est un ensemble de fichiers conçus pour automatiser le processus de compilation d'une application à partir du code source.

Rappelez-vous qu'il y a un certain nombre d'étapes que vous effectueriez si vous compiliez un programme vous-même (téléchargement, extraction, application de correctifs, compilation, installation). Les fichiers qui composent un logiciel porté contiennent toute l'information nécessaire pour permettre au système de faire cela pour vous. Vous lancez une poignée de commandes simples et le code source de l'application est automatiquement téléchargé, extrait, corrigé, compilé, et installé pour vous.

En fait, le catalogue des logiciels portés peut être utilisé pour générer ce qui pourra plus tard être manipulé avec `pkg_add` et d'autres commandes de gestion des logiciels pré-compilés qui seront présentés sous peu.

Les logiciels pré-compilés et le catalogue des logiciels portés comprennent la notion de *dépendances*. Supposez que vous voulez installer une application qui dépend de l'installation d'une bibliothèque particulière. L'application et la bibliothèque ont été toutes deux rendues disponibles sous forme de logiciel porté pour FreeBSD ou de logiciel pré-compilé. Si vous utilisez la commande `pkg_add` ou le catalogue des logiciels portés pour ajouter l'application, tous les deux remarqueront que la bibliothèque n'a pas été installée, et installeront automatiquement en premier la bibliothèque.

Etant donné que les deux technologies sont presque semblables, vous pourriez vous demander pourquoi FreeBSD s'ennuie avec les deux. Les logiciels pré-compilés et le catalogue de logiciels portés ont chacun leurs propres forces, et celle que vous emploierez dépendra de votre préférence.

Avantages des logiciels pré-compilés

- L'archive compressée d'un logiciel pré-compilé est généralement plus petite que l'archive compressée contenant le code source de l'application.
- Les logiciels pré-compilés ne nécessitent pas de compilation supplémentaire. Pour les grosses applications, comme Mozilla, KDE, ou GNOME cela peut s'avérer important, particulièrement si vous êtes sur un système lent.
- Les logiciels pré-compilés ne demandent pas une compréhension du processus impliqué dans la compilation de logiciels sous FreeBSD.

Avantages du catalogue des logiciels portés

- Les logiciels pré-compilés sont normalement compilés avec des options conservatrices, parce qu'ils doivent pouvoir tourner sur le plus grand nombre de systèmes. En installant à partir du catalogue des logiciels portés, vous pouvez ajuster les options de compilation pour (par exemple) générer du code spécifique au Pentium 4 ou à l'Athlon.
- Certaines applications ont des options de compilation concernant ce qu'elles peuvent faire et ne pas faire. Par exemple, Apache peut être configuré avec une très large variété d'options intégrées différentes. En compilant à partir du catalogue des logiciels portés vous n'avez pas à accepter les options par défaut, et vous pouvez les configurez vous-même.

  Dans certains cas, de multiples logiciels pré-compilés existeront pour la même application pour spécifier certaines configurations. Par exemple, Ghostscript est disponible comme logiciel pré-compilé ghostscript et ghostscript-nox11 , en fonction de si vous avez installé ou non un serveur X11. Ce type d'arrangement est possible avec les logiciels pré-compilés, mais devient rapidement impossible si une application a plus d'une ou deux options de compilation.

- Les licences de certains logiciels interdisent les distributions binaires. Ils doivent être distribués sous forme de code source.
- Certaines personnes ne font pas confiance aux distributions binaires. Au moins avec le code source, vous pouvez (en théorie) le parcourir et chercher les problèmes potentiels par vous-même.
- Si vous avez des correctifs locaux, vous aurez besoin du code source afin de les appliquer.
- Certaines personnes aiment avoir le code source à portée de main, ainsi elles peuvent le lire si elles s'ennuient, le modifier, y faire des emprunts (si la licence le permet bien sûr), etc...

Pour suivre les mises à jour du catalogue des logiciels portés, inscrivez-vous à la liste de diffusion à propos du catalogue des logiciels portés de FreeBSD et la liste de diffusion à propos des rapports de bogue concernant le catalogue des logiciels portés de FreeBSD.

Avant d'installer une application, vous devriez consulter http://vuxml.freebsd.org/ à la recherche de problème de sécurité concernant votre application.

Vous pouvez également installer ports-mgmt/portaudit qui contrôlera automatiquement toutes les applications installées à la recherche de vulnérabilités connues, un contrôle sera également effectué avant toute compilation de logiciel porté. De même, vous pouvez utiliser la commande `portaudit -F -a` après avoir installé des logiciels pré-compilés.

Le reste de ce chapitre expliquera comment utiliser les logiciels pré-compilés et le catalogue des logiciels portés et la gestion des logiciels tiers sous FreeBSD.

4.3. Trouver votre application

Avant que vous puissiez installer des applications vous devez savoir ce que vous voulez, et comment se nomment les applications.

La liste des applications disponibles pour FreeBSD augmente de jours en jours. Heureusement, il y a

plusieurs façons de trouver ce que vous désirez:

- Le site web de FreeBSD maintient à jour une liste, dans laquelle on peut effectuer des recherches, de toutes les applications disponibles à l'adresse http://www.FreeBSD.org/ports/. Le catalogue des logiciels portés est divisé en catégories, et vous pouvez soit chercher une application par son nom (si vous le connaissez), soit lister toutes les applications disponibles dans une catégorie.
- Dan Langille maintient FreshPorts, à l'adresse http://www.FreshPorts.org/. FreshPorts suit les modifications des applications dans le catalogue des logiciels portés, vous permet de "surveiller" un ou plusieurs logiciels portés, et peut vous envoyer un courrier électronique quand ils sont mis à jour.
- Si vous ne connaissez pas le nom de l'application que vous voulez, essayez d'utiliser un site comme FreshMeat (http://www.freshmeat.net/) pour trouver une application, ensuite vérifiez sur le site de FreeBSD si l'application a déjà été portée.
- Si vous connaissez le nom exact du logiciel, vous devez juste déterminer dans quelle catégorie il se trouve, vous pouvez utiliser la commande whereis(1) pour cela. Tapez simplement `whereis file` où *file* est le programme que vous voulez installer. S'il est trouvé sur le système, on vous indiquera où il se trouve, de la manière suivante:

  ```
  # whereis lsof
  lsof: /usr/ports/sysutils/lsof
  ```

  Cela nous indique que `lsof` (un utilitaire système) peut être trouvé dans le répertoire /usr/ports/sysutils/lsof.

- Vous pouvez également utiliser une simple commande echo(1) pour déterminer où se trouve un logiciel porté dans le catalogue de logiciels portés. Par exemple:

  ```
  # echo /usr/ports/*/*lsof*
  /usr/ports/sysutils/lsof
  ```

  Notez que cette commande retournera tout fichier téléchargé du répertoire /usr/ports/distfiles correspondant à ce motif de recherche.

- Encore une autre façon de trouver un logiciel porté particulier est d'utiliser le mécanisme de recherche interne du catalogue des logiciels portés. Pour utiliser la fonction de recherche, vous devrez vous trouver dans le répertoire /usr/ports. Une fois dans ce répertoire, lancez `make search name=program-name` où *program-name* représente le nom du programme que vous voulez localiser. Par exemple, si vous recherchiez `lsof`:

  ```
  # cd /usr/ports
  # make search name=lsof
  Port:   lsof-4.56.4
  Path:   /usr/ports/sysutils/lsof
  Info:   Lists information about open files (similar to fstat(1))
  Maint:  obrien@FreeBSD.org
  ```

```
Index:  sysutils
B-deps:
R-deps:
```

La partie du message de sortie à laquelle vous devez prêter attention est la ligne "Path:", car cela vous indique où trouver le logiciel porté. Les autres informations ne sont pas nécessaires afin d'installer le logiciel porté, aussi on en parlera pas ici.

Pour une recherche plus en profondeur vous pouvez également utiliser `make search key=string` où *string* est le texte à rechercher. Cela recherche les noms de logiciels portés, les commentaires, les descriptions et les dépendances et peut être utilisé pour trouver des logiciels portés se rapportant à un sujet particulier si vous ne connaissez pas le nom du programme que vous cherchez.

Dans les deux cas, la chaîne de caractère de recherche n'est pas sensible à la casse des caractères. Rechercher "LSOF" mènera aux même résultats que la recherche de "lsof".

4.4. Utiliser le système des logiciels pré-compilés

Il existe plusieurs outils utilisés pour la gestion des logiciels pré-compilés sur FreeBSD

- Les outils de gestion en ligne de commande des logiciels pré-compilés, qui sont le sujet de la suite de cette section.

4.4.1. Installation d'un logiciel pré-compilé

Vous pouvez utiliser l'utilitaire pkg_add(1) pour installer un logiciel pré-compilé FreeBSD à partir d'un fichier local ou d'un serveur sur le réseau.

Exemple 4. Télécharger un logiciel pré-compilé à la main puis l'installer localement

```
# ftp -a ftp2.FreeBSD.org
Connected to ftp2.FreeBSD.org.
220 ftp2.FreeBSD.org FTP server (Version 6.00LS) ready.
331 Guest login ok, send your email address as password.
230-
230-     This machine is in Vienna, VA, USA, hosted by Verio.
230-         Questions? E-mail freebsd@vienna.verio.net.
230-
230-
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /pub/FreeBSD/ports/packages/sysutils/
250 CWD command successful.
ftp> get lsof-4.56.4.tgz
local: lsof-4.56.4.tgz remote: lsof-4.56.4.tgz
200 PORT command successful.
150 Opening BINARY mode data connection for 'lsof-4.56.4.tgz' (92375 bytes).
```

```
100% |***********************************************| 92375       00:00 ETA
226 Transfer complete.
92375 bytes received in 5.60 seconds (16.11 KB/s)
ftp> exit
# pkg_add lsof-4.56.4.tgz
```

Si vous ne disposez pas d'une source locale de logiciels pré-compilés (comme l'ensemble de CDROM de FreeBSD) alors il sera probablement plus facile d'utiliser l'option `-r` de pkg_add(1). Cela fera déterminer automatiquement à l'utilitaire le format objet et la version corrects et ensuite récupérer et installer le logiciel pré-compilé à partir d'un site FTP.

```
# pkg_add -r lsof
```

L'exemple ci-dessus téléchargera le logiciel pré-compilé correct sans plus d'intervention de l'utilisateur. Si vous désirez indiquer un autre miroir FreeBSD pour les logiciels pré-compilés à la place du site de distribution principal, vous devez positionner en conséquence la variable d'environnement `PACKAGESITE`, pour remplacer les paramètres par défaut. pkg_add(1) utilise fetch(3) pour télécharger les fichiers, qui respecte diverses variables d'environnement, dont `FTP_PASSIVE_MODE`, `FTP_PROXY`, et `FTP_PASSWORD`. Il se peut que vous ayez besoin de configurer une ou plusieurs de ces dernières si vous êtes derrière un coupe-feu, ou devez utiliser un proxy FTP/HTTP. Consultez la page de manuel fetch(3) pour la liste complète des variables. Vous pouvez également remarquer que dans l'exemple ci-dessus `lsof` est utilisé au lieu de `lsof-4.56.4`. Quand la fonction de récupération à distance est utilisée, le numéro de version doit être retiré. pkg_add(1) téléchargera automatiquement la toute dernière version de l'application.

pkg_add(1) téléchargera la dernière version de votre application si vous êtes sous FreeBSD-CURRENT ou FreeBSD-STABLE. Si vous utilisez une version -RELEASE, il récupérera la version compilée avec votre version lors de sa publication. Il est possible de modifier ce comportement en surchargeant la variable d'environnement `PACKAGESITE`. Par exemple, si vous utilisez un système FreeBSD 8.1-RELEASE, par défaut pkg_add(1) tentera de récupérer les applications pré-compilées à partir de `ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-8.1-release/Latest/`. Si vous désirez forcer pkg_add(1) à télécharger les versions des logiciels pré-compilés pour FreeBSD 8-STABLE, positionnez la variable `PACKAGESITE` à `ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-8-stable/Latest/`.

Les logiciels pré-compilés sont distribués dans les formats .tgz et .tbz. Vous pouvez les trouver sur ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/packages/, ou sur le CDROM de distribution de FreeBSD. Chaque CD de l'ensemble de 4-CD de FreeBSD (et le PowerPak, etc...) contient des logiciels pré-compilés dans le répertoire /packages. L'organisation des logiciels pré-compilés est semblable à celle de l'arborescence /usr/ports. Chaque catégorie possède son propre répertoire, et chaque logiciel pré-compilé peut être trouvé dans le répertoire All.

La structure de répertoires du système de logiciels pré-compilés correspond à celle du catalogue des logiciels portés; ils travaillent ensemble pour former l'intégralité du système de logiciels pré-compilés/portés.

4.4.2. Gestion des logiciels pré-compilés

pkg_info(1) est un utilitaire qui liste et décrit les divers logiciels pré-compilés installés.

```
# pkg_info
cvsup-16.1          A general network file distribution system optimized for CV
docbook-1.2         Meta-port for the different versions of the DocBook DTD
...
```

pkg_version(1) est un utilitaire qui récapitule les versions de tous les logiciels pré-compilés installés. Il compare la version du logiciel pré-compilé avec la version actuelle trouvée dans le catalogue des logiciels portés.

```
# pkg_version
cvsup                       =
docbook                     =
...
```

Les symboles dans la seconde colonne indiquent l'âge relatif de la version installée et de la version disponible dans le catalogue des logiciels portés local.

Symbole	Signification
=	La version du logiciel pré-compilé installée est équivalente à celle de celui trouvé dans le catalogue des logiciels portés local.
	La version installée est plus ancienne que celle disponible dans le catalogue des logiciels portés.
	La version installée est plus récente que celle trouvée dans le catalogue local des logiciels portés. (le catalogue local des logiciels portés est probablement ancien)
?	Le logiciel pré-compilé ne peut être trouvé dans l'index du catalogue des logiciels portés. (Cela peut se produire quand, par exemple, un logiciel installé est supprimé du catalogue des logiciels portés ou renommé.)
*	Il y a de multiples versions de ce logiciel pré-compilé.
!	Le logiciel installé existe dans l'index mais pour une raison inconnue, `pkg_version` a été incapable de comparer le numéro de version du paquetage installé avec l'entrée correspondante dans l'index.

4.4.3. Effacer un logiciel pré-compilé

Pour désinstaller un logiciel pré-compilé précédemment installé, utilisez l'utilitaire pkg_delete(1).

```
# pkg_delete xchat-1.7.1
```

Notez que pkg_delete(1) a besoin du nom complet du paquetage et du numéro de version; la commande précédente n'aurait pas fonctionné avec *xchat* à la place de *xchat-1.7.1*. It est cependant facile de retrouver la version du paquetage installé à l'aide de la commande pkg_version(1). Vous pouvez à la place simplement utiliser un joker:

```
# pkg_delete xchat\*
```

dans ce cas, tous les logiciels dont le nom commence par `xchat` seront supprimés.

4.4.4. Divers

Toute l'information sur les logiciels pré-compilés est stockée dans le répertoire /var/db/pkg. La liste des fichiers installés pour chaque logiciel pré-compilé peut être trouvée dans des fichiers de ce répertoire.

4.5. Utiliser le catalogue des logiciels portés

Les sections suivantes fournissent des instructions de base sur l'utilisation du catalogue des logiciels portés pour installer et désinstaller des programmes sur votre système. Une description détaillée des cibles `make` et de variables d'environnement est disponible dans la page de manuel ports(7).

4.5.1. Obtenir le catalogue des logiciels portés

Avant que vous puissiez installer des logiciels portés, vous devez d'abord récupérer le catalogue des logiciels portés- qui est essentiellement un ensemble de Makefiles, de correctifs, et de fichiers de description habituellement placés dans /usr/ports.

Quand vous avez installé votre système FreeBSD, sysinstall vous a demandé si vous aimeriez installer le catalogue des logiciels portés. Si vous avez choisi non, vous pouvez suivre ces instructions pour obtenir le catalogue des logiciels portés:

Procedure: La méthode CVSup

C'est une méthode rapide pour récupérer le catalogue des logiciels portés en utilisant le protocole CVSup. Si vous voulez en apprendre plus au sujet de CVSup, lisez la section Utiliser CVSup.

L'implémentation du protocole CVSup présente dans le système de base de FreeBSD se nomme csup.

Assurez-vous que le répertoire /usr/ports est vide avant d'utiliser csup pour la première fois. Si vous avez déjà un catalogue des logiciels portés, obtenu à partir d'une autre source, csup n'effacera pas les correctifs qui ont été supprimés.

1. Exécuter la commande `csup`:

```
# csup -L 2 -h cvsup.FreeBSD.org /usr/shared/examples/cvsup/ports-supfile
```

Remplacez *cvsup.FreeBSD.org* avec un serveur CVSup proche de vous. Voir Sites CVSup (Sites CVSup) pour une liste complète des sites miroirs.

Certains peuvent vouloir utiliser leur propre ports-supfile, par exemple pour éviter d'avoir à passer le serveur CVSup sur la ligne de commande.

a. Dans ce cas, en tant que `root`, copier /usr/shared/examples/cvsup/ports-supfile à un nouvel emplacement, comme /root ou votre répertoire d'utilisateur.

b. Editez ports-supfile.

c. Remplacez *CHANGE_THIS.FreeBSD.org* avec un serveur CVSup proche de vous. Voir Sites CVSup (Sites CVSup) pour une liste complète des sites miroirs.

d. Maintenant pour lancer `csup`, utilisez ce qui suit:

```
# csup -L 2 /root/ports-supfile
```

2. L'exécution ultérieure de csup(1) téléchargera et appliquera tous les changements récents à votre catalogue des logiciels portés sans pour autant recompiler vos logiciels.

Procedure: La méthode Portsnap

Portsnap est un système alternatif de distribution du catalogue des logiciels portés. Veuillez vous reporter à la section Utiliser Portsnap pour une description détaillée de toutes les caractéristiques de Portsnap.

1. Téléchargez un instantané compressé du catalogue des logiciels portés dans le répertoire /var/db/portsnap. Vous pouvez vous déconnecter de l'Internet, si vous le désirez, après cette opération:

```
# portsnap fetch
```

2. Si vous exécutez Portsnap pour la première fois, il faut extraire l'instantané dans le répertoire /usr/ports:

```
# portsnap extract
```

Si votre répertoire /usr/ports contient déjà une version du catalogue des logiciels portés et que vous désirez juste mettre à jour, utilisez plutôt la commande:

```
# portsnap update
```

Procedure: La méthode Sysinstal

Cette méthode implique l'utilisation de sysinstall pour installer le catalogue des logiciels portés à partir du disque d'installation. Il faut noter que la version du catalogue qui sera installée est la version datant de la publication de votre disque d'installation. Si vous disposez d'un accès à l'Internet, vous devriez toujours utiliser une des méthodes précédemment exposées.

1. En tant que `root`, lancez `sysinstall` comme montré ci-dessous:

```
# sysinstall
```

2. Faites défiler l'écran vers le bas et sélectionnez Configure, appuyez sur `Entrée`.
3. Faites défiler l'écran vers le bas et sélectionnez Distributions, appuyez sur `Entrée`.
4. Faites défiler l'écran vers le bas jusqu'à ports, appuyez sur `Espace`.
5. Remontez jusqu'à Exit, appuyez sur `Entrée`.
6. Choisissez le support d'installation désiré, comme un CDROM, par FTP, etc.
7. Remontez jusqu'à Exit et appuyez sur `Enter`.
8. Appuyez sur la touche `X` pour quitter sysinstall.

4.5.2. Installation de logiciels portés

La première chose qui devrait être expliquée quand on aborde le catalogue des logiciels portés est ce que l'on entend par "squelette". En bref, un squelette est un ensemble minimal de fichiers qui indique à votre système FreeBSD comment compiler et installer proprement un programme. Chaque squelette contient:

- Un fichier Makefile. Le fichier Makefile contient les diverses déclarations qui indiquent comment l'application devrait être compilée et où elle devrait être installée sur votre système.
- Un fichier distinfo. Ce fichier contient l'information à propos des fichiers qui doivent être téléchargés pour compiler le logiciel, et leurs sommes de contrôle (en utilisant sha256(1)), pour s'assurer que ces fichiers n'ont pas été corrompus durant le téléchargement.
- Un répertoire files. Ce répertoire contient les correctifs pour permettre la compilation et l'installation du programme sur votre système FreeBSD. Les correctifs sont à la base de petits

fichiers qui indiquent des modifications sur des fichiers particuliers. Ils sont sous forme de fichiers texte, qui disent "Effacer la ligne 10" ou "Modifier la ligne 26 par...". Les correctifs sont également connus sous le nom de "diffs" car ils sont générés par le programme diff(1).

Ce répertoire peut également contenir d'autres fichiers utilisés pour la compilation du logiciel porté.

- Un fichier pkg-descr. C'est une description plus détaillée du programme, souvent en plusieurs lignes.
- Un fichier pkg-plist. C'est une liste de tous les fichiers qui seront installés par le logiciel porté. Il indique également au système des logiciels portés quels fichiers sont à effacer lors d'une désinstallation.

Certains logiciels portés utilisent d'autres fichiers, comme pkg-message. Le catalogue des logiciels portés utilise ces fichiers pour faire face à certaines situations spéciales. Si vous désirez plus de détails au sujet de ces fichiers, et sur les logiciels portés en général, consultez le Manuel du développeur de logiciels portés.

Le logiciel porté contient les instructions pour compiler le code source, mais ne contient pas le code source. Vous pouvez obtenir le code source à partie d'un CDROM ou de l'Internet. Le code source est distribué de la façon dont l'auteur le désire. Fréquemment c'est une archive tar compressée avec gzip, mais elle pourra être compressée avec un autre outil ou même non compressée. Le code source d'un programme, peu importe la forme sous laquelle il est distribué, est appelé un fichier "distfile". Les deux méthodes pour l'installation d'un logiciel porté pour FreeBSD sont décrites ci-dessous.

Vous devez avoir ouvert une session sous l'utilisateur `root` pour installer des logiciels portés.

Avant d'installer un logiciel porté, vous devez vous assurer d'avoir un catalogue des logiciels portés à jour et vous devez consulter http://vuxml.freebsd.org/ pour les problèmes de sécurité relatifs à votre logiciel.

Un contrôle des problèmes de sécurité peut être effectué automatiquement par portaudit avant toute nouvelle installation d'application. Cet outil peut être trouvé dans le catalogue des logiciels porté (security/portaudit). Vous pouvez lancer `portaudit -F` avant l'installation d'un nouveau logiciel porté, pour télécharger la base de données actualisée des vulnérabilités. Un audit de sécurité et une mise à jour de la base de données sera effectuée lors du contrôle quotidien de sécurité de la machine. Pour plus d'informations, lisez les pages de manuel portaudit(1) et periodic(8).

Le catalogue des logiciels portés suppose que vous disposez d'une connection active à l'Internet. Si ce n'est pas le cas, vous devez placer manuellement une copie du distfile dans le répertoire /usr/ports/distfiles.

Pour commencer, rendez-vous dans le répertoire du logiciel porté que vous voulez installer:

```
# cd /usr/ports/sysutils/lsof
```

Une fois à l'intérieur du répertoire lsof vous verrez le squelette du logiciel porté. L'étape suivante est de compiler (également appelé la "construction") le logiciel porté. Cela est fait en tapant simplement `make` à l'invite. Une fois que c'est fait, vous devriez voir quelque chose comme ceci:

```
# make
>> lsof_4.57D.freebsd.tar.gz doesn't seem to exist in /usr/ports/distfiles/.
>> Attempting to fetch from ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/.
===>  Extracting for lsof-4.57
...
[extraction output snipped]
...
>> Checksum OK for lsof_4.57D.freebsd.tar.gz.
===>  Patching for lsof-4.57
===>  Applying FreeBSD patches for lsof-4.57
===>  Configuring for lsof-4.57
...
[configure output snipped]
...
===>  Building for lsof-4.57
...
[compilation output snipped]
...
#
```

Notez qu'une fois la compilation terminée, vous vous retrouvez face à l'invite. L'étape suivante est d'installer le logiciel porté. Afin de l'installer, vous devez juste ajouter un mot à la commande `make`, et ce mot est `install`:

```
# make install
===>  Installing for lsof-4.57
...
[installation output snipped]
...
===>   Generating temporary packing list
===>   Compressing manual pages for lsof-4.57
===>   Registering installation for lsof-4.57
===>  SECURITY NOTE:
      This port has installed the following binaries which execute with
      increased privileges.
#
```

Une fois de retour à l'invite, vous devriez être en mesure d'exécuter l'application que vous venez juste d'installer. Comme `lsof` est un programme qui tourne avec des privilèges accrus, un avertissement sur la sécurité est affiché. Durant la compilation et l'installation de logiciels portés, vous devriez faire attention à tout avertissement qui pourrait apparaître.

Il est conseillé de supprimer le sous-répertoire de travail, qui contient tous les fichiers temporaires utilisés lors de la compilation. Non seulement cela consomme de l'espace disque, mais cela posera problème plus tard lors de la mise à jour vers une nouvelle version du logiciel porté.

```
# make clean
===>  Cleaning for lsof-4.57
#
```

Vous pouvez vous économiser deux étapes supplémentaires en lançant juste `make install clean` à la place de `make`, `make install` et `make clean` sous la forme de trois étapes séparées.

Certains interpréteurs de commandes maintiennent un cache des commandes qui sont disponibles dans les répertoires listés dans la variable d'environnement `PATH`, pour accélérer les opérations de recherche des fichiers exécutables de ces commandes. Si vous utilisez un de ces interpréteurs de commandes, vous pourrez avoir à utiliser la commande `rehash` après l'installation d'un logiciel porté, avant que la commande fraîchement installée ne puisse être utilisée. Cette commande fonctionnera pour les interpréteurs de commandes comme `tcsh`. Utilisez la commande `hash -r` pour les interpréteurs tels que `sh`. Consultez la documentation de votre interpréteur de commandes pour plus d'information.

Certains DVD-ROMs comme le FreeBSD Toolkit de FreeBSD Mall contiennent des distfiles. Ils peuvent être utilisés avec le catalogue des logiciels portés. Montez le DVD-ROM sous /cdrom. Si vous utilisez un point de montage différent, positionnez la variable make(1) `CD_MOUNTPTS`. Les distfiles nécessaires seront automatiquement utilisés s'ils sont présent sur le disque.

Soyez conscient que les licences de quelques logiciels portés n'autorisent pas leur présence sur le CD-ROM. Cela peut être dû à la nécessité de remplir un formulaire d'enregistrement avant le téléchargement, ou que la redistribution n'est pas permise, ou toute autre raison. Si vous désirez installer un logiciel porté qui n'est pas disponible sur le CD-ROM, vous devrez vous connecter afin de récupérer les fichiers nécessaires.

Le catalogue des logiciels portés utilise fetch(1) pour télécharger les fichiers, qui respecte diverses variables d'environnement, dont `FTP_PASSIVE_MODE`, `FTP_PROXY`, et `FTP_PASSWORD`. Il se peut que vous ayez besoin de configurer une ou plusieurs de ces dernières si vous êtes derrière un coupe-feu, ou devez utiliser un proxy FTP/HTTP. Consultez la page de manuel fetch(3) pour la liste complète des variables.

Pour les utilisateurs qui ne peuvent rester connectés à l'Internet indéfiniment, il existe la commande `make fetch`. Exécutez cette commande à la base du catalogue des logiciels portés (/usr/ports) et les fichiers nécessaires seront téléchargés. Cette commande fonctionnera également dans les sous-répertoires du catalogue, par exemple: /usr/ports/net. Notez que si un logiciel porté dépend de bibliothèques particulières ou d'autres logiciels portés, cette commande de récupérera *pas* les sources de ces logiciels. Remplacez `fetch` par `fetch-recursive` si vous voulez récupérer également les sources des logiciels dont dépend un logiciel porté.

Vous pouvez compiler tous les logiciels d'une catégorie ou de l'ensemble du catalogue en exécutant la commande `make` dans un répertoire de base, juste comme la commande `make fetch` précédente. C'est, cependant, une idée dangereuse étant donné que certains logiciels portés ne peuvent coexister. Dans d'autres cas, certains logiciels portés peuvent installer des fichiers différents ayant le même nom.

Dans de rares cas les utilisateurs peuvent vouloir récupérer les archives à partir d'un site différent du `MASTER_SITES` par défaut (l'emplacement par défaut à partir duquel les fichiers sont téléchargés). Vous pouvez surcharger l'option `MASTER_SITES` avec la commande suivante:

```
# cd /usr/ports/répertoire
# make MASTER_SITE_OVERRIDE= \
ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/distfiles/ fetch
```

Dans cet exemple nous modifions la valeur par défaut de l'option `MASTER_SITES` pour `ftp.FreeBSD.org/pub/FreeBSD/ports/distfiles/`.

Certains logiciels portés autorisent (ou même nécessitent) des options de compilation qui permettent l'activation/désactivation de parties de l'application qui ne sont pas nécessaires, de certaines options de sécurité, et autres personnalisations. Quelques noms de logiciels viennent immédiatement à l'esprit: www/mozilla, security/gpgme, et mail/sylpheed-claws. Un message sera affiché quand de telles options sont disponibles.

4.5.2.1. Modifier les répertoires par défaut des logiciels portés

Il est parfois utile (ou obligatoire) d'utiliser des répertoires de travail ou cible différents. Les variables `WRKDIRPREFIX` et `PREFIX` permettent de modifier les répertoires par défaut. Par exemple:

```
# make WRKDIRPREFIX=/usr/home/example/ports install
```

compilera le logiciel dans le répertoire /usr/home/example/ports et installera tout dans /usr/local.

```
# make PREFIX=/usr/home/example/local install
```

le compilera dans /usr/ports et l'installera dans /usr/home/example/local.

Et bien sûr

```
# make WRKDIRPREFIX=../ports PREFIX=../local install
```

combinera les deux (c'est trop long pour tenir sur cette page, mais cela devrait vous donner une idée générale).

Alternativement, ces variables peuvent également être configurées dans votre environnement. Consultez la page de manuel de votre interpréteur de commandes pour des instructions sur la procédure à suivre.

4.5.2.2. Travailler avec `imake`

Certains logiciels portés qui utilisent `imake` (une partie du système X Window) ne fonctionnent pas correctement avec la variable `PREFIX`, et insisteront pour s'installer sous /usr/X11R6. De façon similaire, certains logiciels Perl ignorent `PREFIX` et s'installent dans l'arborescence Perl. Faire en sorte que ces logiciels portés respectent `PREFIX` est une tâche difficile voire impossible.

4.5.2.3. Reconfigurer les logiciels portés

Lors de la compilation de certains logiciels portés, un menu ncurses(3) pourra s'afficher et à partir de celui-ci vous pourrez sélectionner certaines options de compilation. Il n'est pas inhabituel pour les utilisateurs de vouloir revoir ce menu pour ajouter, supprimer, ou modifier ces options après la compilation d'un logiciel. Il y a plusieurs manières pour y parvenir. Une possibilité est de se rendre dans le répertoire contenant le logiciel porté et de taper `make config`, qui affichera à nouveau le menu avec les mêmes options sélectionnées. Une autre possibilité est d'utiliser `make showconfig` qui vous affichera toutes les options de configuration pour le logiciel porté. Enfin, une autre possibilité est d'exécuter `make rmconfig` qui supprimera toutes les options sélectionnées et permettra donc de repartir à zéro. Toutes ces options, et bien d'autres, sont détaillées dans la page de manuel ports(7).

4.5.3. Supprimer des logiciels portés installés

Maintenant que vous savez comment installer des logiciels portés, vous vous demandez probablement comment les effacer, juste au cas où vous en installez un et plus tard vous vous apercevez que vous n'avez pas installé le bon logiciel porté. Nous désinstallerons notre exemple précédent (qui était `lsof` pour ceux d'entre vous qui n'ont pas suivi). Les logiciels portés sont supprimés de la même manière que pour les logiciels pré-compilés (comme décrit dans la section Utiliser le système des logiciels pré-compilés) en utilisant la commande pkg_delete(1):

```
# pkg_delete lsof-4.57
```

4.5.4. Mise à jour des logiciels portés

Tout d'abord, listez les logiciels portés périmés dont une nouvelle version est disponible dans le catalogue des logiciels portés à l'aide de la commande pkg_version(1):

```
# pkg_version -v
```

4.5.4.1. /usr/ports/UPDATING

Une fois que vous avez mis à jour le catalogue des logiciels portés, avant de tenter la mise à jour d'un logiciel porté, vous devrez consulter le fichier /usr/ports/UPDATING. Ce fichier décrit les divers problèmes et les étapes supplémentaires que les utilisateurs pourront rencontrer ou devront effectuer lors de la mise à jour un logiciel porté, comme la modification de format de fichiers, le

changement des emplacements des fichiers de configuration, ou des incompatibilités avec les versions antérieures.

Si le contenu du fichier UPDATING prime même s'il est en est en contradiction avec des informations présentées ici.

4.5.4.2. Mise à jour des logiciels portés à l'aide de portupgrade

Le logiciel portupgrade a été conçu pour une mise à jour aisée des logiciels portés installés. Il est disponible via le logiciel porté ports-mgmt/portupgrade. Installez-le de la même manière que pour n'importe quel autre logiciel en employant la commande `make install clean`:

```
# cd /usr/ports/ports-mgmt/portupgrade
# make install clean
```

Ensuite, parcourez la liste des logiciels installés avec la commande `pkgdb -F` et corrigez toutes les inconsistances qu'il signale. C'est une bonne idée d'effectuer ce contrôle régulièrement avant chaque mise à jour.

En lançant `portupgrade -a`, portupgrade mettra à jour tous les logiciels portés périmés installés sur votre système. Ajoutez l'indicateur `-i` si vous voulez être consulté pour confirmer chaque mise à jour individuelle.

```
# portupgrade -ai
```

Si vous désirez mettre à jour qu'une seule application bien particulière et non pas l'intégralité des applications, utilisez la commande: `portupgrade nom_du_logiciel_porté`. Ajoutez l'option `-R` si portupgrade doit mettre à jour en premier lieu tous les logiciels portés nécessaires à l'application.

```
# portupgrade -R firefox
```

Pour utiliser les versions pré-compilées plutôt que les logiciels portés pour l'installation, utilisez l'option `-P`. Avec cette option portupgrade cherche les répertoires locaux listé dans la variable `PKG_PATH`, ou récupère les paquetages à partir d'un site distant s'ils ne sont pas trouvés localement. Si les paquetages ne peuvent pas être trouvés localement ou récupérés à distance, portupgrade utilisera les logiciels portés. Pour éviter l'usage des logiciels portés, spécifiez l'option `-PP`.

```
# portupgrade -PP gnome2
```

Pour juste récupérer les sources (ou les paquetages, si l'option `-P` est utilisée) sans compiler ni installer quelque chose, utilisez `-F`. Pour plus d'informations consultez la page de manuel portupgrade(1).

4.5.4.3. Mise à jour des logiciels portés à l'aide de Portmanager

Portmanager est un autre utilitaire de mise à jour aisée des logiciels portés installés. Il est disponible via le logiciel portés ports-mgmt/portmanager:

```
# cd /usr/ports/ports-mgmt/portmanager
# make install clean
```

Tous les logiciels portés installés peuvent être mis à jour en utilisant cette simple commande:

```
# portmanager -u
```

Vous pouvez ajouter l'option `-ui` pour être sollicité pour une confirmation à chaque opération qu'effectuera Portmanager. Portmanager peut également être employé pour installer de nouveaux logiciels portés sur le système. Contrairement à la commande `make install clean` habituelle, il mettra à jour toutes les dépendances avant de compiler et d'installer le logiciel sélectionné.

```
# portmanager x11/gnome2
```

Si des problèmes concernant les dépendances du logiciel porté sélectionné apparaissent, vous pouvez utiliser Portmanager pour toutes les recompiler dans le bon ordre. Cette recompilation achevée, le logiciel porté en question peut alors être à son tour recompilé.

```
# portmanager graphics/gimp -f
```

Pour plus d'information, consultez la page de manuel de Portmanager.

4.5.4.4. Mise à jour des logiciels portés à l'aide de Portmaster

Portmaster est un autre utilitaire destiné à la mise à jour des logiciels installés. Portmaster a été conçu pour utiliser les outils présents dans le système de "base" (il ne dépend pas d'un autre logiciel porté) et utilise les informations contenues dans le répertoire /var/db/pkg/ pour déterminer quel logiciel doit être mis à jour. Il est disponible à partir du logiciel porté ports-mgmt/portmaster:

```
# cd /usr/ports/ports-mgmt/portmaster
# make install clean
```

Portmaster répartit les logiciels portés en quatre catégories:

- logiciels dits "Root" (pas de dépendance, aucun logiciel n'en dépend);
- logiciels dits "Trunk" (pas de dépendance, d'autres logiciels en dépendent);
- logiciels dits "Branch" (ont des dépendances, d'autres logiciels en dépendent);
- logiciels dits "Leaf" (ont des dépendances, aucun logiciel n'en dépend).

Vous pouvez lister tous les logiciels installés et rechercher les mises à jour en utilisant l'option `-L`:

```
# portmaster -L
===>>> Root ports (No dependencies, not depended on)
===>>> ispell-3.2.06_18
===>>> screen-4.0.3
        ===>>> New version available: screen-4.0.3_1
===>>> tcpflow-0.21_1
===>>> 7 root ports
...
===>>> Branch ports (Have dependencies, are depended on)
===>>> apache-2.2.3
        ===>>> New version available: apache-2.2.8
...
===>>> Leaf ports (Have dependencies, not depended on)
===>>> automake-1.9.6_2
===>>> bash-3.1.17
        ===>>> New version available: bash-3.2.33
...
===>>> 32 leaf ports

===>>> 137 total installed ports
        ===>>> 83 have new versions available
```

L'ensemble des logiciels portés installés peut être mis à jour en utilisant cette simple commande:

```
# portmaster -a
```

Par défaut Portmaster fera une sauvegarde avant la suppression d'un logiciel porté. Si l'installation de la nouvelle version se passe correctement, Portmaster supprimera la sauvegarde. L'option `-b` demandera à Portmaster de ne pas supprimer automatiquement la sauvegarde. L'ajout de l'option `-i` lancera Portmaster en mode interactif, vous serez alors sollicité avant la mise à jour de chaque logiciel.

Si vous rencontrez des erreurs lors du processus de mise à jour, vous pouvez utiliser l'option `-f` pour mettre à jour ou recompiler tous les logiciels installés:

```
# portmaster -af
```

Vous pouvez également employer Portmaster pour installer de nouveaux logiciels portés en mettant à jour toutes les dépendances avant la compilation et l'installation du nouveau logiciel:

```
# portmaster shells/bash
```

Pour plus d'information veuillez consulter la page de manuel portmaster(8).

4.5.5. Logiciels portés et espace disque

A la longue, l'utilisation du catalogue des logiciels portés consommera rapidement votre espace disque. Après la compilation et l'installation de logiciels à partir du catalogue des logiciels portés, vous devriez toujours penser à supprimer les répertoires de travail temporaires, work, en utilisant la commande `make clean`. Vous pouvez balayer l'intégralité du catalogue des logiciels portés pour supprimer tous les répertoires temporaires oubliés précédement, employez alors la commande suivante:

```
# portsclean -C
```

Avec le temps, vous accumulerez beaucoup de fichiers sources obsolètes dans le répertoire distfiles. Vous pouvez les supprimer manuellement, ou vous pouvez utiliser la commande suivante pour effacer toutes les sources qui ne correspondent plus à des logiciels portés d'actualité:

```
# portsclean -D
```

Ou pour supprimer les fichiers sources ne correspondant à aucun logiciel installé sur votre systèmes.

L'utilitaire `portsclean` fait partie de la suite portupgrade.

Pensez à supprimer les logiciels portés installés que vous n'utilisez plus. Un outil qui permet d'automatiser cette tâche est disponible via le logiciel porté ports-mgmt/pkg_cutleaves.

4.6. Activités de post-installation

Après l'installation d'une nouvelle application vous voudrez normalement lire la documentation qui a pu être également installée, éditer les fichiers de configuration nécessaires, vérifier que l'application est lancée au démarrage (si c'est un daemon), et ainsi de suite.

Les étapes que vous devez suivre pour configurer chaque application seront bien évidemment différentes. Cependant, si vous venez juste d'installer une nouvelle application et que vous vous demandez "Et maintenant?" les astuces suivantes pourront vous aider:

- Utilisez pkg_info(1) pour déterminer quels fichiers ont été installés et à quel endroit. Par exemple, si vous venez juste d'installer FooPackage version 1.0.0, alors la commande

  ```
  # pkg_info -L foopackage-1.0.0 | less
  ```

  affichera tous les fichiers installés par le logiciel pré-compilé. Portez une attention toute particulière aux fichiers dans les répertoires man/, qui seront des pages de manuel, dans les répertoires etc/ , qui seront des fichiers de configuration, et dans doc/ qui seront de la

documentation plus complète.

Si vous n'êtes pas sûr de la version de l'application qui vient juste d'être installée, une commande comme

```
# pkg_info | grep -i foopackage
```

déterminera tous les logiciels pré-compilés installés qui ont *foopackage* dans leur nom. Remplacez *foopackage* dans votre ligne de commande par ce qui convient.

- Une fois que vous avez identifié où les pages de manuel de l'application ont été installées, consultez-les en utilisant la commande man(1). De même, jetez un coup d'oeil aux exemples de fichiers de configuration, et toute autre documentation additionnelle qui peut avoir été fournie.
- Si l'application a un site web, consultez-le pour de la documentation supplémentaire, des listes de questions fréquemment posées, etc. Si vous n'êtes pas sûr de l'adresse du site web, elle peut être affichée dans le résultat de la commande:

```
# pkg_info foopackage-1.0.0
```

La ligne `WWW:`, si elle est présente, devrait donner l'URL du site web de l'application.

- Les logiciels qui doivent être lancés au démarrage (comme les serveurs Internet) installent généralement un exemple de procédure de lancement dans le répertoire /usr/local/etc/rc.d. Vous devriez contrôler si ce fichier est correct et l'éditer ou le renommer si nécessaire. Consultez la section Démarrer des services pour plus d'informations.

4.7. Que faire avec les logiciels portés ne fonctionnant pas?

Si vous rencontrez un portage qui ne fonctionne pas, il y a certaines choses que vous pouvez faire:

1. Vérifiez s'il n'y a pas de correctif en attente pour le logiciel porté dans la base des rapports de bogue. Si c'est le cas, il se peut que vous puissiez utiliser le correctif proposé.
2. Demandez l'aide du responsable du logiciel porté. Tapez la commande `make maintainer` ou lisez le fichier Makefile pour trouver l'adresse électronique du responsable. Pensez à préciser le nom et la version du logiciel porté (envoyer la ligne `$FreeBSD:` du fichier Makefile) et les messages d'erreurs quand vous écrivez au responsable.

Certains logiciels portés ne sont pas maintenus par une personne mais par une liste de diffusion. Plusieurs, si ce n'est toutes, les adresses de ces listes ressemblent à freebsd-listname@FreeBSD.org. Veuillez prendre cela en compte en rédigeant vos questions.

En particulier, les logiciels portés apparaissant comme maintenus par ports@FreeBSD.org ne sont en fait maintenus par personne. Correctifs et aide,

> s'ils y en a, provient de la communauté qui est abonnée à cette liste de diffusion. Des volontaires supplémentaires sont toujours les bienvenus!

Si vous n'obtenez pas de réponse, vous pouvez utiliser send-pr(1) pour soumettre un rapport de bogue (consultez Ecrire des rapports de bogue pour FreeBSD).

3. Corrigez le problème! Le Manuel du développeur de logiciels portés inclut des informations détaillées sur l'infrastructure des logiciels portés vous permettant de corriger le portage éventuellement défectueux ou même soumettre le votre!
4. Récupérez la version pré-compilée sur un serveur FTP proche de vous. Le catalogue de "référence" des logiciels pré-compilés se trouve sur `ftp.FreeBSD.org` dans le répertoire packages, mais vérifiez *d'abord* votre miroir local! Il y a globalement plus de chances que cela marche, que d'essayez de compiler à partir des sources, et cela va également beaucoup plus vite. Utilisez le programme pkg_add(1) pour installer le logiciel pré-compilé sur votre système.

Chapitre 5. Le système X Window

5.1. Synopsis

Une installation de FreeBSD à l'aide de bsdinstall n'installe pas automatiquement d'interface graphique. Ce chapitre décrit comment installer et configurer Xorg, qui implémente une version libre du système X Window qui est utilisé pour fournir un environnement graphique. Il décrit ensuite comme trouver et installer un environnement de bureau ou un gestionnaire de fenêtres.

Les utilisateurs préférant une méthode d'installation qui configure automatiquement Xorg devraient à GhostBSD, MidnightBSD or NomadBSD.

Pour plus d'informations sur le matériel vidéo supporté par Xorg, consultez le site Web x.org.

Après la lecture de ce chapitre, vous connaîtrez:

- Les divers composants du système X Window et comment ils fonctionnent ensemble.
- Comment installer et configurer Xorg.
- Comment installer et configurer différents gestionnaires de fenêtres et environnements de bureau.
- Comment utiliser les polices de caractères TrueType® sous Xorg.
- Comment configurer votre système pour l'utilisation de procédures de connexions graphiques (XDM).

Avant de lire ce chapitre, vous devrez:

- Savoir comment installer des logiciels tiers comme décrit dans le Installer des applications. les logiciels pré-compilés et les logiciels portés.

5.2. Terminologie

Alors qu'il n'est pas nécessaire de comprendre tout le détail des divers composants du système X Window, ni comment ils interagissent entre eux, une certaine connaissance de base de ces composants peut être utile.

Le serveur X

X a été conçu dès le départ centré autour du réseau, et adopte un modèle "client-serveur". Dans ce modèle, le "serveur X" tourne sur l'ordinateur sur lequel sont branchés le clavier, le moniteur et la souris. Le serveur est responsable de tâches telles que la gestion de l'affichage, des entrées en provenance du clavier et de la souris, et les entrées ou sorties d'autres périphériques comme une tablette ou un vidéo-projecteur. Cela jette le trouble chez certaines personnes, parce que la terminologie X est exactement le contraire de ce à quoi ils s'attendent. Ils s'attendent à ce que le "serveur X" soit la grosse machine puissante au fond du couloir, et que le "client X" soit a machine sur leur bureau.

Le client X

Chaque application X, comme XTerm ou Firefox est un "client". Un client envoie des messages au serveur comme "Dessine une fenêtre aux coordonnées suivantes", et le serveur renvoie au client des messages du type "L'utilisateur vient de cliquer sur le bouton OK".

A la maison ou dans un petit bureau, le serveur X et les clients X tourneront en général sur le même ordinateur. Il est également possible de faire tourner le serveur X sur un ordinateur moins puissant et d'exécuter les applications X sur un système plus puissant. Dans ce scénario, la communication entre le client X et le serveur se fera par l'intermédiaire du réseau.

Le gestionnaire de fenêtres

X n'essaye pas de dicter quel aspect doivent avoir les fenêtres à l'écran, comment les déplacer avec la souris, quelles combinaisons de touches devraient être utilisées pour passer de l'une à l'autre, comment devraient être les barres de titres de chaque fenêtre, etc. Au lieu de cela, X délègue cette responsabilité à une application séparée, le gestionnaire de fenêtres ("window manager"). Il existe des douzaines de gestionnaires de fenêtres disponibles. Chaque gestionnaire de fenêtres propose une apparence et une prise en mains différentes: certains supportent les bureaux virtuels, d'autres permettent de personnaliser les combinaisons de touches pour la gestion du bureau, certains ont un bouton "Démarrer", et certains permettent d'utiliser des thèmes, pour un changement complet d'apparence et de prise en main du bureau. Les gestionnaires de fenêtres sont disponibles dans la catégorie x11-wm du catalogue des logiciels portés.

Chaque gestionnaire de fenêtre utilise un mécanisme de configuration propre. Certains demandent un fichier de configuration écrit à la main, alors que d'autres disposent d'outils graphiques pour la plupart des tâches de configuration.

Environnement de bureau

KDE et GNOME sont considérés comme des environnements de bureau car ils intègrent une suite complète d'applications pour effectuer les tâches classiques d'un bureau informatique. Ils peuvent disposer de suites bureautiques, de navigateurs Web, ou encore de jeux.

Politique de focus

Le gestionnaire de fenêtres est responsable de la politique ou stratégie de focus de la souris. Cette politique offre plusieurs méthodes pour choisir quelle fenêtre doit recevoir les frappes au clavier et comment indiquer visuellement la fenêtre actuellement active.

Une des politiques de focus est appelée "click-to-focus" ("cliquer pour obtenir le focus"). Dans ce mode, une fenêtre devient active quand elle reçoit un clic de la souris. Dans le mode "focus-follows-mouse" ("le focus suit la souris"), la fenêtre qui est sous le pointeur de la souris est la fenêtre qui a le focus et le focus est modifié en pointant sur une autre fenêtre. Si la souris est sur la fenêtre racine (ou fond d'écran), alors cette fenêtre a le focus. Dans le mode "sloppy-focus" ("focus relâché"), si la souris est déplacée sur la fenêtre racine, la dernière fenêtre à avoir eu le focus le conserve. Avec le mode focus relâché, le focus n'est modifié que si le pointeur passe sur une nouvelle fenêtre, et non pas quand il quitte la fenêtre actuelle. Dans la politique "click-to-focus", la fenêtre active est sélectionnée par un clic de la souris. La fenêtre peut être remontée au premier plan au-dessus des autres fenêtres. Toutes les frappes au clavier seront désormais dirigées vers cette fenêtre, même si le curseur est déplacé vers une autre fenêtre.

Les différents gestionnaires de fenêtres supportent différents modes pour le focus. Tous supportent le clic pour obtenir le focus, et une grande majorité supporte également d'autres politiques. Consultez la documentation du gestionnaire de fenêtres pour déterminer quels modes sont disponibles.

widgets - Eléments graphiques

Widget est un terme pour désigner tous les éléments de l'interface utilisateur qui peuvent être cliqués ou manipulés d'une façon ou d'une autre. Cela comprend les boutons, les boîtes à cocher, les boutons radio, les icônes et les listes. Une boîte à outils de widgets est un ensemble d'éléments graphiques utilisés afin de créer des applications graphiques. Il existe de nombreuses boîtes à outils d'éléments graphiques populaires comme Qt, utilisée par KDE, et GTK+, utilisée par GNOME. Cela aura pour conséquence pour les applications de présenter une apparence et une prise en main différente en fonction de la famille d'éléments graphiques utilisée pour créer ces applications.

5.3. Installer X11

Sous FreeBSD, Xorg peut être installé à l'aide soit d'un paquet précompilé soit d'un logiciel porté.

Le paquet pré-compilé peut être installé rapidement mais avec moins d'options de personnalisation:

```
# pkg install xorg
```

Pour compiler et installer à partir du catalogue des logiciels portés:

```
# cd /usr/ports/x11/xorg
# make install clean
```

Chacune de ces deux méthodes d'installation installera une version complète d'Xorg. La version en paquets pré-compilés reste la meilleure option pour la plupart des utilisateurs.

Une plus petite version du système X adaptée aux utilisateurs expérimentés est disponible dans le paquet x11/xorg-minimal. La plupart des documentations, des bibliothèques, et des applications ne sera pas installée. Certaines applications ont besoin de ces composants additionnels pour fonctionner.

5.4. Configuration d'Xorg

5.4.1. Démarrage rapide

Xorg supporte les cartes graphiques, les claviers et les périphériques de pointage les plus courants.

Les cartes graphiques, moniteurs et périphériques d'entrée sont détectés automatiquement. Ne créez pas de fichier xorg.conf ou n'utilisez pas l'option

> `-configure` en dehors d'un échec de la configuration automatique.

1. Si Xorg a déjà été utilisé sur cet ordinateur avant, déplacez ou supprimez les fichiers existants:

```
# mv /etc/X11/xorg.conf ~/xorg.conf.etc
# mv /usr/local/etc/X11/xorg.conf ~/xorg.conf.localetc
```

2. Ajouter au groupe `video` ou `wheel` l'utilisateur qui exécutera Xorg pour activer l'accélération 3D quand elle est disponible. Pour ajouter l'utilisateur *jru* aux groupes disponibles:

```
# pw groupmod video -m jru || pw groupmod wheel -m jru
```

3. Le gestionnaire de fenêtres twm est inclu par défaut. Il est lancé quand Xorg démarre:

```
% startx
```

4. Sur certaines anciennes versions de FreeBSD, la console système doit être configurée en vt(4) avant que le retour à la console texte puisse correctement fonctionner. Consultez Kernel Mode Setting (KMS).

5.4.2. Groupe utilisateur pour l'accélération graphique

L'accès à /dev/dri est nécessaire pour autoriser l'accélération 3D sur les cartes graphiques. Il est en général plus simple d'ajouter l'utilisateur qui exécutera X soit au groupe `video` soit au groupe `wheel`. Ici, pw(8) est utilisé pour ajouter l'utilisateur *slurms* au groupe `video`, ou au groupe `wheel` s'il n'y a pas de groupe `video`:

```
# pw groupmod video -m slurms || pw groupmod wheel -m slurms
```

5.4.3. Kernel Mode Setting (KMS)

Quand l'ordinateur bascule de l'affichage sur la console vers une définition d'écran plus haute pour X, il doit fixer le *mode* de sortie graphique. Les versions récentes de Xorg utilisent un système présent dans le noyau pour effectuer ces changements de manière la plus efficace. Les anciennes versions de FreeBSD utilisent sc(4) qui n'a pas connaissance du système KMS. La conséquence est qu'après avoir fermé X, l'affichage de la console système sera vide même si elle reste fonctionnelle. La nouvelle console vt(4) évite ce problème.

Ajoutez la ligne suivante au fichier /boot/loader.conf pour activer vt(4):

```
kern.vty=vt
```

5.4.4. Fichiers de configuration

Une configuration manuelle n'est généralement pas nécessaire. Ne créez pas de fichiers de configuration à la main à moins que la configuration automatique ne fonctionne pas.

5.4.4.1. Répertoire

Xorg recherche ses fichiers de configuration dans plusieurs répertoires. /usr/local/etc/X11/ est le répertoire recommandé pour ces fichiers sous FreeBSD. L'utilisation de ce répertoire permet de conserver une séparation entre les fichiers des applications et ceux du système d'exploitation.

Stocker les fichiers de configuration dans le répertoire /etc/X11/ originel fonctionne toujours. Cependant, cela a pour conséquence de mélanger des fichiers concernant des applications avec ceux du système de base FreeBSD et n'est pas recommandé.

5.4.4.2. Un seul ou plusieurs fichiers

Il est plus simple d'utiliser plusieurs fichiers qui chacun individuellement s'occupe de la configuration d'un paramètre précis plutôt qu'un seul fichier xorg.conf traditionnel. Ces fichiers sont stockés dans le sous-répertoire xorg.conf.d/ du répertoire principal de configuration. Son chemin d'accès complet est en général /usr/local/etc/X11/xorg.conf.d/.

Des exemples de ces fichiers sont présentés plus bas dans cette section.

Le fichier unique traditionnel xorg.conf fonctionne toujours mais n'est ni clair ni aussi flexible que plusieurs fichiers dans le sous-répertoire xorg.conf.d/.

5.4.5. Cartes graphiques

En raison de changements effectués dans les versions récentes de FreeBSD, il est désormais possible d'utiliser les pilotes de périphériques graphiques proposés dans le catalogue des logiciels portés ou sous forme pré-compilé. Par conséquent, les utilisateurs peuvent utiliser un des pilotes disponibles à partir du logiciel graphics/drm-kmod.

Intel KMS driver

L'accélération 2D et 3D sont supportées par la plupart des cartes graphiques Intel KMS driver en provenance d'Intel.

Nom du pilote: `i915kms`

L'accélération 2D et 3D sont supportées par la plupart des anciennes cartes graphiques Radeon KMS driver en provenance d'AMD.

Nom du pilote: `radeonkms`

L'accélération 2D et 3D sont supportées par la plupart des nouvelles cartes graphiques AMD KMS driver en provenance d'AMD.

Nom du pilote: `amdgpu`

Pour information, veuillez consulter https://en.wikipedia.org/wiki/

List_of_Intel_graphics_processing_units ou https://en.wikipedia.org/wiki/List_of_AMD_graphics_processing_units pour une liste des GPUs supportés.

Intel®

L'accélération 3D est supportée sur la plupart des cartes graphiques Intel® jusqu'au Ivy Bridge (HD Graphics 2500, 4000, et P4000), y compris Iron Lake (HD Graphics) et Sandy Bridge (HD Graphics 2000).

Nom du pilote: `intel`

Pour information, consultez https://en.wikipedia.org/wiki/List_of_Intel_graphics_processing_units.

AMD® Radeon

L'accélération 2D et 3D sont supportées par les cartes Radeon jusqu'à la série HD6000 comprise.

Nom du pilote: `radeon`

Pour information, consultez https://en.wikipedia.org/wiki/List_of_AMD_graphics_processing_units.

NVIDIA

Plusieurs pilotes NVIDIA sont disponibles dans la catégorie x11 du catalogue des logiciels portés. Installez le pilote correspondant à la carte graphique.

Pour information, consultez https://en.wikipedia.org/wiki/List_of_Nvidia_graphics_processing_units.

Configuration graphique hybride

Certains ordinateurs portables ont un processeur graphique supplémentaire en plus de celui intégré dans le chipset ou le microprocesseur. Le système *Optimus* combine du matériel Intel® et NVIDIA. Les *systèmes graphiques sélectionnables* ou *systèmes graphiques hybrides* sont la combinaison d'un processeur Intel® ou AMD® et d'un GPU AMD® Radeon.

L'implémentation de ces systèmes graphiques hybrides varie, et Xorg sous FreeBSD n'est pas en mesure de faire fonctionner toutes les versions.

Certains ordinateurs fournissent une option du BIOS pour désactiver une de ces cartes graphiques ou pour sélectionner un mode *discret* qui peut être utilisé avec un des pilotes graphiques standard. Par exemple, il est parfois possible de désactiver le GPU NVIDIA dans un système Optimus. La partie graphique Intel® peut alors être utilisée avec un pilote Intel®.

Les paramètres du BIOS dépendent du modèle d'ordinateur. Dans certaines situations, les deux GPU peuvent être laissés actifs, mais la création d'un fichier de configuration utilisant seulement le GPU principal dans la partie `Device` est suffisant pour qu'un tel système fonctionne.

Autres cartes graphiques

Les pilotes pour les cartes graphiques moins courantes peuvent être trouvés dans la catégorie x11-drivers du catalogue des logiciels portés.

Les cartes qui ne sont pas supportées par un pilote précis pourront toujours être utilisables avec le pilote x11-drivers/xf86-video-vesa. Ce pilote est installé par x11/xorg. Il peut également être installé manuellement en tant que x11-drivers/xf86-video-vesa. Xorg tente d'utiliser ce pilote quand un pilote spécifique à la carte graphique n'est pas trouvé.

x11-drivers/xf86-video-scfb est un pilote graphique non-spécifique qui fonctionne sur de nombreux ordinateurs UEFI et ARM®.

Configuration du pilote graphique dans un fichier

Pour configurer le pilote Intel® dans un fichier de configuration:

Exemple 5. Sélection du pilote graphique Intel® à l'aide d'un fichier

/usr/local/etc/X11/xorg.conf.d/driver-intel.conf

```
Section "Device"
    Identifier "Card0"
    Driver     "intel"
    # BusID    "PCI:1:0:0"
EndSection
```

Si plus d'une carte graphique est présente, l'identifiant `BusID` peut être décommenté et paramétré pour sélectionné la carte désirée. Une liste des IDs des cartes graphiques peut être obtenu avec `pciconf -lv | grep -B3 display`.

Pour configurer le pilote Radeon dans un fichier de configuration:

Exemple 6. Sélection du pilote graphique Radeon à l'aide d'un fichier

/usr/local/etc/X11/xorg.conf.d/driver-radeon.conf

```
Section "Device"
    Identifier "Card0"
    Driver     "radeon"
EndSection
```

Pour configurer le pilote VESA dans un fichier de configuration:

Exemple 7. Sélection du pilote graphique VESA à l'aide d'un fichier

/usr/local/etc/X11/xorg.conf.d/driver-vesa.conf

```
Section "Device"
    Identifier "Card0"
    Driver     "vesa"
```

```
EndSection
```

Pour configurer le pilote `scfb` pour une utilisation avec un ordinateur UEFI ou ARM®:

Exemple 8. Sélection du pilote graphique `scfb` à l'aide d'un fichier

/usr/local/etc/X11/xorg.conf.d/driver-scfb.conf

```
Section "Device"
    Identifier "Card0"
    Driver     "scfb"
EndSection
```

5.4.6. Moniteurs

Presque tous les moniteurs supportent la norme *Extended Display Identification Data* (EDID). Xorg utilise EDID pour communiquer avec le moniteur et détecter les définitions et les taux de rafraichissement supportés. Ensuite, il sélectionne la combinaison de paramètres la plus adaptée pour le moniteur.

Les autres définitions supportées par le moniteur peuvent être sélectionnées en indiquant celle désirée dans les fichiers de configuration, ou à l'aide de xrandr(1) après avoir lancé le serveur X.

Utilisation de xrandr(1)

Exécutez xrandr(1) sans aucun paramètre pour voir la liste des sorties vidéos et des modes détectés du moniteur:

```
% xrandr
Screen 0: minimum 320 x 200, current 3000 x 1920, maximum 8192 x 8192
DVI-0 connected primary 1920x1200+1080+0 (normal left inverted right x axis y axis)
495mm x 310mm
   1920x1200     59.95*+
   1600x1200     60.00
   1280x1024     85.02    75.02    60.02
   1280x960      60.00
   1152x864      75.00
   1024x768      85.00    75.08    70.07    60.00
   832x624       74.55
   800x600       75.00    60.32
   640x480       75.00    60.00
   720x400       70.08
DisplayPort-0 disconnected (normal left inverted right x axis y axis)
HDMI-0 disconnected (normal left inverted right x axis y axis)
```

Ceci montre que la sortie `DVI-0` est utilisée actuellement pour afficher une définition d'écran de 1920x1200 pixels à une fréquence de rafraichissement d'environ 60 Hz. Il n'y a pas de moniteur

branché aux connecteurs DisplayPort-0 et HDMI-0.

N'importe quel autre mode d'affichage peut être choisi avec xrandr(1). Par exemple, pour basculer sur 1280x1024 à 60 Hz:

```
% xrandr --mode 1280x1024 --rate 60
```

Une opération courante est d'utiliser une sortie vidéo externe sur un ordinateur portable pour un vidéo-projecteur.

Le type et le nombre de connecteurs de sortie varient en fonction des systèmes, et le nom donné à chaque sortie varie d'un pilote graphique à l'autre. Ce qu'un pilote appelle HDMI-1, un autre l'appellera HDMI1. Aussi la première chose à faire est de lancer xrandr(1) pour lister toutes les sorties disponibles.

```
% xrandr
Screen 0: minimum 320 x 200, current 1366 x 768, maximum 8192 x 8192
LVDS1 connected 1366x768+0+0 (normal left inverted right x axis y axis) 344mm x
193mm
   1366x768      60.04*+
   1024x768      60.00
   800x600       60.32    56.25
   640x480       59.94
VGA1 connected (normal left inverted right x axis y axis)
   1280x1024     60.02 +  75.02
   1280x960      60.00
   1152x864      75.00
   1024x768      75.08    70.07    60.00
   832x624       74.55
   800x600       72.19    75.00    60.32    56.25
   640x480       75.00    72.81    66.67    60.00
   720x400       70.08
HDMI1 disconnected (normal left inverted right x axis y axis)
DP1 disconnected (normal left inverted right x axis y axis)
```

Quatre sorties ont été trouvées: l'écran intégré LVDS1, et les connecteurs externes VGA1, HDMI1, et DP1.

Le projecteur a été connecté à la sortie VGA1. xrandr(1) est maintenant utilisé pour régler cette sortie sur la définition native de ce vidéo-projecteur et pour ajouter l'espace d'affichage supplémentaire à droite du bureau:

```
% xrandr --output VGA1 --auto --right-of LVDS1
```

Le paramètre --auto sélectionne la définition et le taux de rafraichissement détecté par EDID. Si la définition n'est pas correctement détectée, une valeur définie peut être donnée avec le paramètre --mode à la place de --auto. Par exemple, la plupart des vidéo-projecteurs acceptent

une définition de 1024x768 qui est réglée avec `--mode 1024x768`.

xrandr(1) est souvent exécuté à partir de .xinitrc pour régler le mode adapté quand X est lancé.

Configuration de la définition du moniteur dans un fichier

Pour configurer la définition de l'écran à 1024x768 dans un fichier de configuration:

Exemple 9. Sélection de la définition d'écran à l'aide d'un fichier

/usr/local/etc/X11/xorg.conf.d/screen-resolution.conf

```
Section "Screen"
    Identifier "Screen0"
    Device     "Card0"
    SubSection "Display"
    Modes      "1024x768"
    EndSubSection
EndSection
```

Les quelques moniteurs ne supportant pas l'EDID peuvent être configurés en paramétrant `HorizSync` et `VertRefresh` avec les plages de fréquences supportées par le moniteur.

Exemple 10. Configuration manuelle des fréquences du moniteur

/usr/local/etc/X11/xorg.conf.d/monitor0-freq.conf

```
Section "Monitor"
    Identifier   "Monitor0"
    HorizSync    30-83   # kHz
    VertRefresh  50-76   # Hz
EndSection
```

5.4.7. Périphériques d'entrée

5.4.7.1. Claviers

Disposition des touches de clavier

L'emplacement normalisé des touches d'un clavier est appelé *disposition* (*layout*). Les dispositions et d'autres paramètres réglables sont listés dans la page de manuel xkeyboard-config(7).

Une disposition des touches américaine est celle utilisée par défaut. Pour sélectionner une disposition différente, configurez les options `XkbLayout` et `XkbVariant` dans une section `InputClass`. Cette configuration sera appliquée à tous les périphériques d'entrée qui correspondent à cette classe.

Cet exemple sélectionne une disposition de touches française.

Exemple 11. Configuration d'une disposition des touches de clavier

/usr/local/etc/X11/xorg.conf.d/keyboard-fr.conf

```
Section "InputClass"
    Identifier  "KeyboardDefaults"
    MatchIsKeyboard "on"
    Option      "XkbLayout" "fr"
EndSection
```

Exemple 12. Configuration de plusieurs dispositions des touches

Configuration des dispositions américaine, espagnole et ukrainienne. Le passage de l'une à l'autre de ces dispositions se fait en appuyant sur kbd[Alt+Shift]. x11/xxkb ou x11/sbxkb peuvent être utilisés pour un contrôle de la sélection de la disposition des touches amélioré et pour avoir des indicateurs de la disposition en cours d'utilisation.

/usr/local/etc/X11/xorg.conf.d/kbd-layout-multi.conf

```
Section "InputClass"
    Identifier  "All Keyboards"
    MatchIsKeyboard "yes"
    Option      "XkbLayout" "us, es, ua"
EndSection
```

Quitter Xorg à partir du clavier

X peut être fermé à partir d'une combinaison de touches. Par défaut, cette combinaison n'est pas définie car elle entre en conflit avec les commandes passées au clavier pour certaines applications. L'activation de cette option nécessite d'effectuer des modifications à la section `InputDevice` du clavier:

Exemple 13. Activation de la sortie d'X à l'aide du clavier

/usr/local/etc/X11/xorg.conf.d/keyboard-zap.conf

```
Section "InputClass"
    Identifier  "KeyboardDefaults"
    MatchIsKeyboard "on"
    Option      "XkbOptions" "terminate:ctrl_alt_bksp"
EndSection
```

5.4.7.2. Souris et périphériques de pointage

Si vous utilisez xorg-server 1.20.8 ou les versions suivantes sous FreeBSD 12.1 et que vous n'utilisez pas moused(8), ajoutez la ligne `kern.evdev.rcpt_mask=12` au fichier /etc/sysctl.conf.

Plusieurs paramètres de la souris peuvent être réglés avec les options de configuration. Consultez la page de manuel mousedrv(4) pour une liste complète.

Butons de la souris

Le nombre de boutons d'une souris peut être configuré dans la section `InputDevice` du fichier xorg.conf. Pour fixer le nombre de boutons à 7:

Exemple 14. Réglage du nombre de boutons de la souris

/usr/local/etc/X11/xorg.conf.d/mouse0-buttons.conf

```
Section "InputDevice"
    Identifier  "Mouse0"
    Option      "Buttons" "7"
EndSection
```

5.4.8. Configuration manuelle

Dans certains cas, la configuration automatique d'Xorg ne fonctionne pas avec un matériel spécifique, ou une configuration différente est recherchée. Pour ces cas, un fichier de configuration personnalisé peut être créé.

Ne créez pas de fichiers de configuration à la main à moins que cela ne soit nécessaire. Une configuration inadaptée peut empêcher un fonctionnement correct.

Un fichier de configuration basé sur le matériel détecté peut être généré par Xorg. Ce fichier est un point de départ utile pour une configuration personnalisée.

Génération d'un fichier xorg.conf:

```
# Xorg -configure
```

Le fichier de configuration est enregistré sous /root/xorg.conf.new. Effectuez les modifications désirées, puis tester ce fichier (avec l'option `-retro` de manière à avoir un fond d'écran visible) avec:

```
# Xorg -retro -config /root/xorg.conf.new
```

Une fois que la nouvelle configuration a été ajustée et testée, elle peut être divisée en plus petits fichiers dans les emplacements habituels, /usr/local/etc/X11/xorg.conf.d/.

5.5. Utilisation des polices de caractères sous Xorg

5.5.1. Polices de caractères Type1

Les polices de caractères livrées par défaut avec Xorg sont loin d'être idéales pour des applications de type publication. Les grandes polices utilisées pour les présentations présentent un aspect en escalier et peu professionnel, et les petites polices sont presque complètement illisibles. Cependant, il existe de nombreuses polices Type1 (PostScript®) gratuites, de hautes qualités qui peuvent être aisément utilisées avec Xorg.. Par exemple, la collection de polices de caractères URW (x11-fonts/urwfonts) comprend une version haute qualité des polices de caractères standards type1 (Times Roman™, Helvetica™, Palatino™ et autres). La collection Freefonts (x11-fonts/freefonts) comprend beaucoup plus de polices de caractères, mais la plupart d'entre elles sont destinées à être utilisées avec des logiciels graphiques comme Gimp, et ne sont pas suffisamment complètes pour servir de polices de caractères d'affichage. De plus Xorg peut être configuré pour utiliser les polices de caractères TrueType® avec un minimum d'effort. Pour plus de détails à ce sujet, consultez la page de manuel X(7) ou la section Polices de caractères TrueType®.

Pour installer les collections de polices de caractères Type1 précédentes à partir des paquets binaires, lancez les commandes suivantes:

```
# pkg install urwfonts
```

Pour les compiler à partir du catalogue des logiciels portés, lancez les commandes suivantes:

```
# cd /usr/ports/x11-fonts/urwfonts
# make install clean
```

Et de même pour la collection Freefont ou d'autres. Pour que le serveur X détecte ces polices, ajoutez une ligne appropriée au fichier de configuration du serveur X (/etc/X11/xorg.conf), du type:

```
FontPath "/usr/local/share/fonts/URW/"
```

Autre possibilité, en ligne de commande dans une session X lancez:

```
% xset fp+ /usr/local/share/fonts/urwfonts
% xset fp rehash
```

Cela fonctionnera mais la configuration sera perdue quand la session X sera fermée, à moins de l'ajouter dans le fichier de démarrage (~/.xinitrc pour une session `startx` classique, ou dans ~/.xsession quand on s'attache au système par l'intermédiaire d'un gestionnaire de session graphique comme XDM). Une troisième méthode est d'utiliser le nouveau fichier

/usr/local/etc/fonts/local.conf: comme montré dans la section Polices de caractères anticrénelage.

5.5.2. Polices de caractères TrueType®

Xorg dispose d'un support intégré pour le rendu des polices TrueType®. Il y a deux différents modules qui peuvent activer cette fonctionnalité. Le module freetype est utilisé dans cet exemple parce qu'il est plus compatible avec les autres moteurs de rendu des polices de caractères. Pour activer le module freetype ajoutez juste la ligne suivante dans la section `"Module"` du fichier /etc/X11/xorg.conf.

```
Load  "freetype"
```

Maintenant créez un répertoire pour les polices TrueType® (par exemple /usr/local/share/fonts/TrueType) et copiez toutes les polices TrueType® dans ce répertoire. Gardez à l'esprit que les polices TrueType® ne peuvent être directement prises d'un Apple® Mac®; elles doivent être dans un format UNIX®/MS-DOS®/Windows® pour être utilisées sous Xorg. Une fois les fichiers copiés dans ce répertoire, utilisez mkfontscale pour créer un fichier fonts.dir, de façon à ce que le moteur d'affichage des polices d'X sache que de nouveaux fichiers ont été installés. mkfontscale peut être installé à partir d'un paquet binaire:

```
# pkg install mkfontscale
```

Puis créez un index des polices de caractères pour X dans le répertoire:

```
# cd /usr/local/share/fonts/TrueType
# mkfontscale
```

Maintenant ajoutez le répertoire des polices TrueType® au chemin des polices de caractères. Cela est identique à ce qui est décrit dans la section Polices de caractères Type1:

```
% xset fp+ /usr/local/share/fonts/TrueType
% xset fp rehash
```

ou ajouter une ligne `FontPath` au fichier xorg.conf.

Désormais Gimp, LibreOffice, et toutes les autres applications X devraient maintenant reconnaître les polices de caractères TrueType® installées. Les polices très petites (comme le texte de page web visualisé sur un écran haute résolution) et les très grandes polices (dans LibreOffice) auront un rendu bien meilleur maintenant.

5.5.3. Polices de caractères anticrénelage

Toutes les polices de caractères sous Xorg se trouvant dans les répertoires /usr/local/share/fonts/ et ~/.fonts/ sont automatiquement disponibles pour l'anticrénelage avec les applications compatibles Xft. La plupart des application sont compatibles Xft, comme KDE, GNOME, et Firefox.

Afin de contrôler quelles polices de caractères sont anticrénelées, ou pour configurer les propriétés de l'anticrénelage, créez (ou éditez, s'il existe déjà) le fichier /usr/local/etc/fonts/local.conf. Plusieurs caractéristiques avancées du système de fontes Xft peuvent être ajustées par l'intermédiaire de ce fichier; cette section ne décrit que des possibilités simples. Pour plus de détails, consultez la page de manuel fonts-conf(5).

Ce fichier doit être dans le format XML. Faites attention à la casse des caractères, et assurez-vous que toutes les balises sont correctement fermées. Le fichier débute avec l'entête XML classique suivie par une définition DOCTYPE, puis de la balise `fontconfig`:

```
    ?xml version="1.0"?
    !DOCTYPE fontconfig SYSTEM "fonts.dtd"
    fontconfig
```

Comme précisé précédemment, l'ensemble des polices de caractères du répertoire /usr/local/share/fonts/ comme du répertoire ~/.fonts/ sont disponibles pour les applications compatibles Xft. Si vous désirez ajouter un autre répertoire en dehors des ces deux là, ajoutez une ligne similaire à la suivante au fichier /usr/local/etc/fonts/local.conf:

```
dir/chemin/vers/mes/fontes/dir
```

Après l'ajout de nouvelles polices, et tout particulièrement de nouveaux répertoires de polices, vous devrez exécuter la commande suivante pour reconstituer le cache des polices de caractères:

```
# fc-cache -f
```

L'anticrénelage rend les bords légèrement flous, ce qui rend le texte très petit plus lisible et enlève l'effet "d'escalier" des grands textes, mais peut provoquer une fatigue visuelle si c'est appliqué au texte de taille normale. Pour exclure les tailles de polices inférieures à 14 points de l'anticrénelage, ajoutez ces lignes:

```
     match target="font"
      test name="size" compare="less"
        double14/double
      /test
      edit name="antialias" mode="assign"
        boolfalse/bool
      /edit
    /match
    match target="font"
      test name="pixelsize" compare="less" qual="any"
        double14/double
      /test
      edit mode="assign" name="antialias"
        boolfalse/bool
      /edit
```

```
    /match
```

L'espacement pour certaines polices de caractères à chasse fixe peut également être inapproprié avec l'anticrénelage. Cela semble être un problème avec KDE, en particulier. Une solution possible pour cela est de forcer l'espacement pour de telles polices de caractères à 100. Ajoutez les lignes suivantes:

```
     match target="pattern" name="family"
      test qual="any" name="family"
        stringfixed/string
      /test
      edit name="family" mode="assign"
        stringmono/string
      /edit
    /match
    match target="pattern" name="family"
      test qual="any" name="family"
        stringconsole/string
      /test
      edit name="family" mode="assign"
        stringmono/string
      /edit
    /match
```

(ceci ajoute un alias "mono" pour les autres noms communs des polices de caractères fixes), puis ajoutez:

```
     match target="pattern" name="family"
      test qual="any" name="family"
        stringmono/string
      /test
      edit name="spacing" mode="assign"
        int100/int
      /edit
    /match
```

Certaines polices de caractères, comme Helvetica, peuvent présenter des problèmes lors de l'anticrénelage. Généralement cela se manifeste par l'impression que la fonte semble coupée en deux verticalement. Au pire cela peut provoquer des crashs avec certaines applications. Pour éviter cela, pensez à ajouter ce qui suit au fichier local.conf:

```
     match target="pattern" name="family"
      test qual="any" name="family"
        stringHelvetica/string
      /test
      edit name="family" mode="assign"
        stringsans-serif/string
```

```
    /edit
  /match
```

Une fois l'édition de local.conf achevée, assurez-vous que le fichier se termine par la balise `/fontconfig`. Si ce n'est pas le cas, tous vos changements seront ignorés.

Les utilisateurs peuvent ajouter leurs propres paramètres par l'intermédiaire de leur propre fichier ~/.config/fontconfig/fonts.conf. Ce fichier doit utiliser le même format XML décrit précédemment.

Un dernier point: avec un écran LCD, un échantillonnage "sub-pixel" peut être désiré. Fondamentalement, ceci traite les composantes rouge, verte et bleu séparément (horizontalement séparées) pour améliorer la résolution horizontale; les résultats peuvent être dramatiques. Pour activer cela, ajoutez quelque part dans le fichier local.conf les lignes:

```
  match target="font"
   test qual="all" name="rgba"
     constunknown/const
   /test
   edit name="rgba" mode="assign"
     constrgb/const
   /edit
 /match
```

En fonction de type d'écran, le terme `rgb` pourra devoir être changé pour `bgr`, `vrgb` ou `vbgr`: expérimentez pour déterminer lequel fonctionne le mieux.

5.6. Le gestionnaire de connexion graphique XDM

Xorg propose un gestionnaire de connexion graphique, XDM, qui peut être utilisé pour la gestion des procédures de connexion graphique. XDM fournit une interface graphique pour sélectionner à quel serveur d'affichage se connecter et entrer des informations d'autorisation d'accès comme l'ensemble identifiant et mot de passe.

Cette section montre comment configurer le gestionnaire de connexion graphique X sous FreeBSD. Certains environnements de bureau fournissent leur propre gestionnaire de connexion graphique. Se référer à la GNOME pour des instructions sur comment configurer le gestionnaire de connexion graphique GNOME et à la KDE pour des instructions concernant la configuration du gestionnaire de connexion graphique KDE.

5.6.1. Configurer XDM

Pour installer XDM, utilisez le logiciel porté ou la version pré-compilée x11/xdm. Une fois installé, XDM peut être configuré pour être lancé au démarrage de la machine en modifiant la ligne suivante dans /etc/ttys:

```
ttyv8   "/usr/local/bin/xdm -nodaemon"  xterm   off secure
```

Modifiez le `off` pour `on` et sauvegardez la modification. Le champ `ttyv8` sur cette ligne indique que XDM démarrera sur le neuvième terminal virtuel.

Le répertoire de configuration d'XDM est situé dans /usr/local/etc/X11/xdm. Ce répertoire contient plusieurs fichiers utilisés pour modifier le comportement et l'apparence d'XDM, ainsi que quelques procédures et programmes utilisés pour configurer le bureau quand XDM est exécuté. Fichiers de configuration d'XDM résume la fonction de chacun de ces fichiers. La syntaxe exacte et l'utilisation de ces fichiers sont décrites dans xdm(1).

Tableau 3. Fichiers de configuration d'XDM

Fichier	Description
Xaccess	Le protocole utilisé pour se connecter à XDM est appelé le "X Display Manager Connection Protocol" (XDMCP). Ce fichier est un ensemble de règles d'autorisation client pour contrôler les connexions XDMCP à partir de machines distantes. Par défaut, ce fichier n'autorise pas la connexion de clients distants.
Xresources	Ce fichier contrôle l'apparence et la prise en main du programme de sélection et d'ouverture de session XDM. La configuration par défaut est une simple fenêtre d'ouverture de session rectangulaire avec le nom de la machine hôte affiché en haut dans une grande police de caractères et avec les invites "Login:" et "Password:" en dessous. Le format de ce fichier est identique au fichier de paramètres par défaut décrit dans la documentation Xorg
Xservers	Liste des affichages distants et locaux que le système doit proposer à l'ouverture de session.
Xsession	Procédure d'ouverture de session par défaut qui est exécutée par XDM quand un utilisateur se connecte. Elle pointe vers une procedure personnalisée de session dans le répertoire ~/.xsession.
Xsetup_*	Procédures utilisées pour lancer automatiquement des applications avant d'afficher les interfaces de sélection et d'ouverture de session. Il existe une procedure pour chaque écran utilisé, nommée Xsetup_*, où * est le numéro local de l'écran. En général, ces procédures exécutent un ou deux programmes en tâche de fond comme `xconsole`.
xdm-config	Configuration globale pour tous les écrans tournant sur cette machine.

Fichier	Description
xdm-errors	Contient les erreurs générées par le programme serveur. Si une connexion qu'XDM tente d'ouvrir se bloque, examinez ce fichier pour trouver des messages d'erreur. Ces messages sont également écrits dans le fichier ~/.xsession-errors de l'utilisateur à chaque session.
xdm-pid	L'identifiant, ID, du processus exécutant XDM.

5.6.2. Configurer l'accès à distance

Par défaut, seuls les utilisateurs sur le même système peuvent ouvrir une session en utilisant XDM. Pour permettre aux utilisateurs d'autres système de se connecter au gestionnaire d'affichage, éditez les règles de contrôle d'accès et activez l'écoute des demandes de connexion.

Pour configurer XDM pour l'écoute des demandes de connexions distantes, commentez la ligne `DisplayManager.requestPort` dans le fichier /usr/local/etc/X11/xdm/xdm-config en ajoutant un `!` devant:

```
! SECURITY: do not listen for XDMCP or Chooser requests
! Comment out this line if you want to manage X terminals with xdm
DisplayManager.requestPort:     0
```

Sauvegardez et relancez XDM. Pour restreindre l'accès à distance, consultez les exemples dans /usr/local/etc/X11/xdm/Xaccess ainsi que la page de manuel xdm(1) pour plus d'informations

5.7. Environnements de bureau

Cette section décrit comment installer sur un système FreeBSD un des trois environnements de bureau populaires. Un environnement de bureau peut aller du simple gestionnaire de fenêtres jusqu'à la suite complète d'applications de bureau. Plus d'une centaine d'environnements est disponible dans la catégorie x11-wm du catalogue des logiciels portés.

5.7.1. GNOME

GNOME est un environnement de bureau convivial. Il comprend un panneau ("panel") pour lancer des applications et afficher des états, un bureau, un ensemble d'outils et d'applications, et un ensemble de conventions qui rendent aisée la coopération et la cohérence entre applications. Plus d'informations concernant GNOME sous FreeBSD peuvent être trouvées sur https://www.FreeBSD.org/gnome. Le site contient de la documentation supplémentaire sur l'installation, la configuration, et l'administration de GNOME sous FreeBSD.

Cet environnement de bureau peut être installé à partir d'un paquet pré-compilé:

```
# pkg install gnome3
```

Pour plutôt compiler GNOME à partir du catalogue des logiciels portés, utilisez la commande qui suit. GNOME est une application importante en taille et qui demandera un temps notable pour être compilée, et cela, même sur un ordinateur rapide.

```
# cd /usr/ports/x11/gnome3
# make install clean
```

GNOME a besoin que /proc soit monté. Ajoutez la ligne suivante au fichier /etc/fstab pour monter ce système de fichiers automatiquement au démarrage:

```
proc           /proc       procfs  rw  0   0
```

GNOME utilise D-Bus et HAL comme bus des messages et couche d'abstraction matérielle. Ces applications sont automatiquement installées comme dépendances à GNOME. Activez-les dans /etc/rc.conf pour qu'elles soient lancées au démarrage du système:

```
dbus_enable="YES"
hald_enable="YES"
```

Après l'installation, il faut configurer Xorg pour lancer GNOME. La manière la plus simple de faire cela est d'activer le gestionnaire d'affichage de GNOME, GDM, qui est installé par défaut comme élément du paquet pré-compilé ou du logiciel porté GNOME. Il peut être activé en ajoutant la ligne suivante au fichier /etc/rc.conf:

```
gdm_enable="YES"
```

Il est souvent intéressant de lancer également tous les services GNOME. Pour accomplir cela, ajoutez une seconde ligne à /etc/rc.conf:

```
gnome_enable="YES"
```

GDM sera lancé automatiquement au démarrage du système.

Une deuxième méthode de lancement de GNOME est de taper `startx` à partir de la ligne de commande après avoir configuré le fichier ~/.xinitrc. Si ce fichier existe déjà, remplacez la ligne qui lance le gestionnaire de fenêtres actuel par une qui exécute /usr/local/bin/gnome-session. Si ce fichier n'existe pas, créez-le avec la commande:

```
% echo "exec /usr/local/bin/gnome-session" > ~/.xinitrc
```

Une troisième méthode est d'utiliser XDM comme gestionnaire d'affichage. Dans ce cas, créez un exécutable ~/.xsession:

```
% echo "exec /usr/local/bin/gnome-session" > ~/.xsession
```

5.7.2. KDE

KDE est un autre environnement de bureau simple d'utilisation. Ce bureau propose une suite d'applications avec une apparence et une prise en main commune, des menus et des barres d'outils, des raccourcis clavier, des couleurs et une régionalisation standardisés, ainsi qu'un système de configuration de l'environnement centralisé. Plus d'informations sur KDE peuvent être trouvées sur http://www.kde.org/. Pour des informations spécifiques à FreeBSD, consultez http://freebsd.kde.org.

Pour installer la version pré-compilée de KDE, tapez:

```
# pkg install x11/kde5
```

Pour plutôt compiler KDE à partir du catalogue des logiciels portés, utilisez la commande qui suit. L'installation du logiciel porté proposera un menu pour sélectionner quel composant à installer. KDE est une application importante en taille et qui demandera un temps notable pour être compilée, et cela, même sur un ordinateur rapide.

```
# cd /usr/ports/x11/kde5
# make install clean
```

KDE a besoin que /proc soit monté. Ajoutez la ligne suivante au fichier /etc/fstab pour monter ce système de fichiers automatiquement au démarrage:

```
proc           /proc       procfs  rw  0   0
```

KDE utilise D-Bus et HAL comme bus des messages et couche d'abstraction matérielle. Ces applications sont automatiquement installées comme dépendances à KDE. Activez-les dans /etc/rc.conf pour qu'elles soient lancées au démarrage du système:

```
dbus_enable="YES"
hald_enable="YES"
```

Depuis KDE Plasma 5, le gestionnaire d'affichage KDE, KDM, n'est plus développé. Un remplacement possible est SDDM. Pour l'installer, tapez:

```
# pkg install x11/sddm
```

Ajoutez cette ligne à /etc/rc.conf:

```
sddm_enable="YES"
```

Une deuxième méthode de lancement de KDE Plasma est de taper `startx` à partir de la ligne de commande. Pour que cela fonctionne, la ligne suivante est requise dans ~/.xinitrc:

```
exec ck-launch-session startplasma-x11
```

Une troisième méthode de lancement de KDE Plasma utilise XDM. Dans ce cas, créez un exécutable ~/.xsession comme indiqué:

```
% echo "exec ck-launch-session startplasma-x11" > ~/.xsession
```

Une fois KDE Plasma lancée, consultez son système d'aide intégrée pour plus d'informations sur comment utiliser ses différents menus et applications.

5.7.3. XFce

XFce est un environnement de bureau basé sur le "toolkit" GTK+ utilisé par GNOME. Cependant, il est plus léger et offre un bureau simple, efficace et simple d'utilisation. Il est complètement configurable, dispose d'une barre principale avec des menus, des petites applications et des lanceurs d'applications, il fournit un gestionnaire de fichiers et un gestionnaire du son, et il est personnalisable avec des thèmes. Puisqu'il est rapide, léger et efficace, il est idéal pour les machines anciennes ou lentes avec des limitations en mémoire. Plus d'informations sur XFce peuvent être trouvées sur le site http://www.xfce.org.

Pour installer le paquet pré-compilé de Xfce:

```
# pkg install xfce
```

Alternativement, pour compiler le logiciel porté:

```
# cd /usr/ports/x11-wm/xfce4
# make install clean
```

Xfce utilise D-Bus comme bus des messages. Cette application est automatiquement installée comme dépendance à Xfce. Activez-la dans /etc/rc.conf pour qu'elle soit lancée au démarrage du système:

```
dbus_enable="YES"
```

Contrairement à GNOME ou KDE, Xfce ne fournit pas son propre gestionnaire de session. Afin de lancer Xfce à partir de la ligne de commande en tapant `startx`, créez d'abord le fichier ~/.xinitrc à l'aide de la ligne:

```
% echo ". /usr/local/etc/xdg/xfce4/xinitrc" > ~/.xinitrc
```

Une méthode alternative est d'utiliser XDM. Pour configurer cette méthode, créez un exécutable ~/.xsession:

```
% echo ". /usr/local/etc/xdg/xfce4/xinitrc" > ~/.xsession
```

5.8. Installation de Compiz Fusion

Une méthode pour rendre l'utilisation d'un ordinateur plus plaisante est l'ajout de jolis effets en 3D.

L'installation du paquet binaire Compiz Fusion est simple, mais sa configuration demande quelques étapes qui ne sont pas décrites dans la documentation du logiciel porté.

5.8.1. Configuration du pilote nVidia FreeBSD

Les effets visuels dans l'environnement de bureau peuvent être à l'origine d'une charge non-négligeable pour la carte graphique. Pour les cartes graphiques nVidia, le pilote de périphérique propriétaire est nécessaire pour obtenir de bonnes performances. Les utilisateurs d'autres cartes graphiques peuvent sauter cette section et poursuivre avec la partie sur la configuration d'xorg.conf.

Pour déterminer quel pilote nVidia est requis, consultez la FAQ à ce sujet.

Après avoir déterminé le pilote correct à utiliser pour votre carte, l'installation est aussi simple que d'installer n'importe quel autre paquet binaire.

Par exemple, pour installer la dernière version du pilote:

```
# pkg install x11/nvidia-driver
```

Le pilote créera un module noyau, qui doit être chargé au démarrage du système. Ajoutez la ligne suivante au fichier /boot/loader.conf:

```
nvidia_load="YES"
```

Pour charger immédiatement le module noyau dans le noyau en cours d'utilisation, utilisez une commande du type `kldload nvidia`. Cependant, il a été remarqué que certaines versions d'Xorg ne fonctionnaient pas correctement si le pilote n'était pas chargé lors du démarrage du système. Après l'édition du fichier /boot/loader.conf, un redémarrage est donc recommandé.

Avec le module noyau chargé, seul la modification d'une ligne dans xorg.conf est nécessaire pour activer le pilote propriétaire:

Trouvez la ligne suivante dans /etc/X11/xorg.conf:

```
Driver      "nv"
```

et modifiez-la pour:

```
Driver      "nvidia"
```

Lancez l'interface graphique comme vous en avez l'habitude, et vous devriez être accueilli par le logo nVidia. Tout devrait fonctionner comme à l'accoutumée.

5.8.2. Configuration d'xorg.conf pour les effets visuels

Pour activer Compiz Fusion, /etc/X11/xorg.conf doit être modifié:

Ajoutez la section suivante pour activer les effets du compositeur:

```
Section "Extensions"
    Option         "Composite" "Enable"
EndSection
```

Recherchez la section "Screen" qui devrait être semblable à celle ci-dessous:

```
Section "Screen"
    Identifier     "Screen0"
    Device         "Card0"
    Monitor        "Monitor0"
    ...
```

et ajouter les deux lignes suivantes (après la ligne "Monitor"):

```
DefaultDepth    24
Option         "AddARGBGLXVisuals" "True"
```

Recherchez la partie "Subsection" faisant référence à la définition de l'écran que vous voulez utiliser. Par exemple, si vous voulez utiliser une définition de 1280x1024, recherchez la partie comme ci-dessous. Si la définition voulue n'apparaît nulle part, vous devrez ajouter l'entrée correspondante à la main:

```
SubSection     "Display"
    Viewport    0 0
    Modes      "1280x1024"
EndSubSection
```

Une profondeur de couleurs de 24 bits est requise pour un bureau utilisant la composition, modifiez la section précédente pour:

```
SubSection     "Display"
    Viewport    0 0
    Depth       24
    Modes      "1280x1024"
EndSubSection
```

Et enfin, vérifiez que les modules "glx" et "extmod" sont chargés dans la section "Module":

```
Section "Module"
    Load           "extmod"
    Load           "glx"
    ...
```

Ce qui précède peut être effectué automatiquement avec x11/nvidia-xconfig en exécutant (en tant que `root`):

```
# nvidia-xconfig --add-argb-glx-visuals
# nvidia-xconfig --composite
# nvidia-xconfig --depth=24
```

5.8.3. Installation et configuration de Compiz Fusion

L'installation de Compiz Fusion est aussi simple que celle de n'importe quel paquet binaire:

```
# pkg install x11-wm/compiz-fusion
```

Quand l'installation est achevée, lancez votre environnement de bureau et, à un terminal, entrez les commandes suivantes (sous l'utilisateur normal):

```
% compiz --replace --sm-disable --ignore-desktop-hints ccp
% emerald --replace
```

Votre écran devrait clignoter quelques secondes, étant donné que votre gestionnaire de fenêtres (par exemple Metacity si vous utilisez GNOME) est remplacé par Compiz Fusion. Emerald s'occupera de la décoration des fenêtres (c'est à dire, les boutons de fermeture, de réduction, d'agrandissement, les barres de titres etc.).

Vous avez la possibilité de convertir tout cela en une procédure à exécuter automatiquement au démarrage (par exemple en l'ajoutant à "Sessions" dans le cas d'un bureau GNOME):

```
#! /bin/sh
```

```
compiz --replace --sm-disable --ignore-desktop-hints ccp
emerald --replace
```

Sauvegardez ce fichier dans votre répertoire personnel sous le nom, par exemple, start-compiz et rendez-le exécutable:

```
% chmod +x ~/start-compiz
```

Utilisez ensuite l'interface graphique pour l'ajouter au menu Startup Programs (situé dans System, Preferences, Sessions dans le cas d'un environnement de bureau GNOME).

Pour sélectionner tous les effets visuels désirés et leurs paramètres, exécutez (toujours en tant qu'utilisateur normal) le programme Compiz Config Settings Manager:

```
% ccsm
```

Sous GNOME, il peut être trouvé dans le menu System, puis Preferences.

Si vous avez sélectionné "gconf support" lors de la compilation, vous pourrez également voir ces paramètres en utilisant `gconf-editor` sous `apps/compiz`.

5.8.4. Dépannage de Compiz Fusion

5.8.4.1. J'ai installé Compiz Fusion, et après avoir lancé les commandes que vous

mentionnez, mes fenêtres n'ont plus de barre de titre et de boutons. Qu'est-ce qui ne va pas?

Il vous manque probablement une configuration dans /etc/X11/xorg.conf. Relisez avec attention ce fichier et contrôlez tout particulièrement les directives `DefaultDepth` et `AddARGBGLXVisuals`.

5.8.4.2. Quand j'exécute la commande pour lancer Compiz Fusion, le serveur X

plante et je retourne à la console. Qu'est-ce qui ne va pas?

Si vous contrôlez le contenu du fichier /var/log/Xorg.0.log, vous trouverez surement des messages d'erreur lors du démarrage de X. Les plus courants seront:

```
(EE) NVIDIA(0):     Failed to initialize the GLX module; please check in your X
(EE) NVIDIA(0):     log file that the GLX module has been loaded in your X
(EE) NVIDIA(0):     server, and that the module is the NVIDIA GLX module.  If
(EE) NVIDIA(0):     you continue to encounter problems, Please try
(EE) NVIDIA(0):     reinstalling the NVIDIA driver.
```

C'est généralement le cas quand vous mettez à jour Xorg. Vous devrez réinstaller le paquet x11/nvidia-driver afin que le module glx soit compilé à nouveau.

Partie II: Tâches courantes

Maintenant que les bases sont maîtrisées, cette partie du Manuel va traiter de certaines fonctionnalités de FreeBSD fréquemment utilisées. Ces chapitres:

- Présentent des applications de bureautique populaires et utiles: des navigateurs, des outils de productivité, des lecteurs de documents, etc.
- Présentent plusieurs outils multimédia disponibles pour FreeBSD.
- Expliquent le processus de compilation d'un noyau FreeBSD personnalisé, pour permettre l'ajout de fonctionnalités supplémentaires.
- Décrivent le système d'impression en détail, pour les configurations d'imprimante locale et en réseau.
- Montrent comment exécuter des applications Linux sur le système FreeBSD.

Certains de ces chapitres conseillent des lectures préalables, ceci est noté dans le synopsis au début de chaque chapitre.

Chapitre 6. Bureautique

6.1. Synopsis

FreeBSD peut faire fonctionner une large variété d'applications de bureautique, comme des navigateurs et des traitements de textes. La plupart de ces derniers sont disponibles sous forme pré-compilée ou peuvent être compilé automatiquement à partir du catalogue des logiciels portés. De nombreux utilisateurs s'attendent à trouver ces types d'applications dans leur environnement de travail. Ce chapitre vous montrera comment installer quelques unes des applications de bureautique les plus populaires sans trop d'effort, soit à partir de versions pré-compilées soit à partir du catalogue des logiciels portés.

Notez que lorsque l'on installe des programmes à partir du catalogue des logiciels portés, ils sont compilés à partir des sources. Cela peut prendre un temps relativement long, en fonction de ce que vous compilez et de la puissance de votre machine. Si la compilation à partir des sources requiert un temps prohibitif, vous pouvez installer la plupart des programmes de l'arbre des ports à partir de version pré-compilées.

Comme FreeBSD dispose d'un système de compatibilité avec les binaires Linux, de nombreuses applications développées à l'origine pour Linux sont disponibles pour votre environnement de travail. Il est vivement recommandé que vous lisiez le Compatibilité binaire avec Linux® avant d'installer des applications Linux. De nombreux logiciels portés utilisant la compatibilité binaire Linux débutent avec le terme "linux-". Souvenez-vous de cela quand vous recherchez un logiciel porté bien particulier, par exemple à l'aide de whereis(1). Dans le reste de ce chapitre on suppose que vous avez activé la compatibilité Linux avant d'installer des applications Linux.

Voici les catégories d'applications couvertes par ce chapitre:

- Navigateurs (comme Mozilla, Opera, Firefox, Konqueror)
- Productivité (comme KOffice, AbiWord, The GIMP, OpenOffice.org)
- Lecteurs de document (comme Acrobat Reader®, gv, Xpdf, GQview)
- Finance (comme GnuCash, Gnumeric, Abacus)

Avant de lire ce chapitre, vous devrez:

- Savoir comment installer des logiciels tiers (Installer des applications. les logiciels pré-compilés et les logiciels portés).
- Savoir comment installer des logiciels pour Linux (Compatibilité binaire avec Linux®).

Pour des informations sur comment mettre en place un environnement multimédia, lisez le Multimédia. Si vous désirez configurer et utiliser le courrier électronique, veuillez vous référer au Courrier électronique.

6.2. Navigateurs

FreeBSD n'est pas livré avec un navigateur particulier installé. Au lieu de cela, le répertoire www

du catalogue des logiciels portés contient de nombreux navigateurs prêts à être installés. Si vous n'avez pas le temps de tout compiler (cela peut prendre un temps relativement long dans certains cas) nombres d'entre eux sont disponibles sous forme pré-compilée.

KDE et GNOME fournissent déjà un navigateur HTML. Veuillez vous référer au Environnements de bureau pour plus d'information sur comment configurer ces environnements de travail.

Si vous êtes à la recherche de navigateurs légers, vous devriez consulter le catalogue des logiciels portés pour www/dillo, www/links, ou www/w3m.

Cette section couvre les applications suivantes:

Nom de l'application	Ressources nécessaires	Installation à partir du catalogue des logiciels portés	Dépendances principales
Mozilla	importantes	lourde	Gtk+
Opera	faibles	légère	Version native FreeBSD et Linux disponibles. La version Linux dépend de la compatibilité binaire Linux et de linux-openmotif.
Firefox	moyennes	lourde	Gtk+
Konqueror	moyennes	lourde	Bibliothèques KDE

6.2.1. Mozilla

Mozilla est un navigateur moderne et stable, dont le portage FreeBSD est complet: il présente un moteur d'affichage HTML qui respecte vraiment les normes; il intègre un lecteur de courrier électronique et de forums de discussion. Il possède même un éditeur HTML si vous projetez d'écrire vous-même quelques pages Web. Les utilisateurs de getenv(3) trouveront des similitudes avec la suite Communicator, étant donné que les deux navigateurs partagent certains développements passés.

Sur les machines lentes, avec une vitesse de processeur de moins de 233MHz ou avec moins de 64MO de RAM, Mozilla peut être trop consommateur en ressources pour être vraiment utilisable. Vous pourrez vouloir essayer à la place le navigateur Opera décrit plus tard dans ce chapitre.

Si vous ne pouvez ou ne voulez compiler Mozilla, pour une quelconque raison, l'équipe GNOME de FreeBSD l'a déjà fait pour vous. Installez juste la version pré-compilée à partir du réseau avec:

```
# pkg_add -r mozilla
```

Si la version pré-compilée n'est pas disponible, et que vous avez suffisamment de temps et d'espace disque, vous pouvez obtenir les sources pour Mozilla, le compiler et l'installer sur votre système. Cela s'effectue en faisant:

```
# cd /usr/ports/www/mozilla
# make install clean
```

Le logiciel porté Mozilla s'assure d'une initialisation correcte en exécutant la configuration de la base de registre chrome avec les privilèges de `root` privilèges. Cependant si vous désirez récupérer des modules additionnels comme "mouse gestures", vous devez exécuter Mozilla en tant que `root` pour obtenir une installation correcte de ces modules.

Une fois que vous avez achevé l'installation de Mozilla, vous n'avez plus besoin d'être sous `root`. Vous pouvez lancer Mozilla en tant que navigateur en tapant:

```
% mozilla
```

Vous pouvez lancer directement les lecteurs de courrier électronique et de forums comme montré ci-dessous:

```
% mozilla -mail
```

6.2.2. Firefox

Firefox est la génération suivante de navigateurs basés sur le code de Mozilla. Mozilla est une suite complète d'applications, comme un navigateur, un client de messagerie, un client de discussion et bien plus. Firefox est juste un navigateur, ce qui le rend plus petit et plus rapide.

Installez la version pré-compilée du logiciel en tapant:

```
# pkg_add -r firefox
```

Vous pouvez également utiliser le catalogue des logiciels portés si vous désirez effectuer la compilation à partir des sources:

```
# cd /usr/ports/www/firefox
# make install clean
```

6.2.3. Firefox, Mozilla et le greffon Java™

Dans cette section et la suivante, nous supposerons que vous avez déjà installé Firefox ou Mozilla.

La fondation FreeBSD a acquis auprès de Sun Microsystems une licence de distribution des binaires FreeBSD pour le Java Runtime Environment (JRE™) et le Java Development Kit (JDK™). Les paquetages binaires pour FreeBSD sont disponibles sur le site de la fondation FreeBSD.

Pour ajouter le support Java™ à Firefox ou Mozilla, vous devez installer tout d'abord le logiciel porté java/javavmwrapper. Ensuite, téléchargez le paquetage Diablo JRE™ à l'adresse http://www.freebsdfoundation.org/downloads/java.shtml, et installez-le à l'aide de pkg_add(1).

Lancez votre navigateur et tapez `about:plugins` dans la barre d'adresse et appuyez sur `Entrée`. Une page listant les greffons installés s'affichera; le greffon Java™ devrait désormais apparaître dans la liste. Si ce n'est pas le cas, en tant que `root`, exécutez la commande suivante:

```
# ln -s /usr/local/diablo-jre1.5.0/plugin/i386/ns7/libjavaplugin_oji.so \
  /usr/local/lib/browser_plugins/
```

puis relancez votre navigateur.

6.2.4. Firefox, Mozilla et le greffon Macromedia® Flash™

Le greffon Macromedia® Flash™ n'est pas disponible pour FreeBSD. Cependant il existe une couche logicielle ("wrapper") pour utiliser la version Linux du greffon. Ce "wrapper" supporte également les greffons Adobe® Acrobat®, RealPlayer® et plus.

Installez le logiciel porté www/nspluginwrapper. Ce logiciel nécessite emulators/linux_base qui occupe un espace relativement important.

L'étape suivante est l'installation du logiciel porté www/linux-flashplugin7. Une fois le logiciel installé, le greffon doit être installé par chaque utilisateur à l'aide de la commande `nspluginwrapper`:

```
% nspluginwrapper -v -a -i
```

Lancez ensuite votre navigateur, tapez `about:plugins` dans la barre d'adresse et appuyez sur `Entrée`. Une liste des greffons actuellement disponibles devrait apparaître.

6.2.5. Opera

Opera est un navigateur complet respectant les standards. Il intègre un lecteur de courrier électronique et de forums de discussion, un client IRC, un lecteur de flux RSS/Atom et beaucoup plus. Malgré cela, Opera reste relativement léger et très rapide. Il est disponible en deux versions: une version "native" pour FreeBSD et une version utilisant l'émulation Linux.

Pour naviguer sur le Web avec la version FreeBSD d'Opera, installez la version pré-compilée:

```
# pkg_add -r opera
```

Certains sites FTP n'ont pas toutes les versions pré-compilées, mais Opera peut également être obtenu avec le catalogue des logiciels portés en tapant:

```
# cd /usr/port/www/opera
```

```
# make install clean
```

Pour installer la version Linux d'Opera, utilisez `linux-opera` à la place d'`opera` dans les exemples précédents. La version Linux est utile dans les situations demandant l'utilisation de greffons qui sont uniquement disponibles pour Linux, comme Acrobat Reader®. Dans tous les autres aspects, les versions FreeBSD et Linux devraient être identiques.

6.2.6. Konqueror

Konqueror fait partie de KDE mais peut être également utilisé en dehors de KDE en installant x11/kdebase3. Konqueror est plus qu'un navigateur, c'est également un gestionnaire de fichiers et une visionneuse multimedia

Il existe également un ensemble de greffons pour Konqueror disponible dans misc/konq-plugins.

Konqueror supporte également Flash™; un tutorial pour avoir le support de Flash™ sous Konqueror est disponible à l'adresse http://freebsd.kde.org/howto.php.

6.3. Productivité

Quand on parle de productivité, les nouveaux utilisateurs recherchent souvent une bonne suite bureautique ou un traitement de texte convivial. Bien que certains environnements de travail comme KDE fournissent déjà une suite de bureautique, il n'y a pas de logiciels de productivité par défaut. FreeBSD fournit tout ce qui est nécessaire, indépendamment de votre environnement de travail.

Cette section couvre les applications suivantes:

Nom de l'application	Ressources nécessaires	Installation à partir du catalogue des logiciels portés	Dépendances principales
KOffice	légères	lourde	KDE
AbiWord	légères	lourde	Gtk+ ou GNOME
The Gimp	légères	lourde	Gtk+
OpenOffice.org	importantes	très lourde	JDK™ 1.4, Mozilla

6.3.1. KOffice

La communauté KDE propose son environnement de travail avec une suite de bureautique qui peut être utilisée en dehors de KDE. Elle comprend quatre composants standard que l'on peut trouver dans d'autres suites. KWord est le traitement de texte, KSpread est le tableur, KPresenter est le programme pour gérer des présentations, et Kontour vous permet de créer des documents graphiques.

Avant d'installer la dernière version de KOffice, soyez sûr d'avoir une version à jour de KDE.

Pour installer KOffice à partir de la version pré-compilée, utilisez la commande suivante:

```
# pkg_add -r koffice
```

Si la version pré-compilée n'est pas disponible, vous pouvez utiliser le catalogue des logiciels portés. Par exemple, pour installer KOffice pour KDE3, faites:

```
# cd /usr/ports/editors/koffice-kde3
# make install clean
```

6.3.2. AbiWord

AbiWord est un traitement de texte gratuit similaire au niveau de l'apparence et de la prise en main à Microsoft® Word. Il convient pour taper des lettres, des rapports, des mémos, et ainsi de suite. Il est très rapide, dispose de nombreuses fonctions, et très convivial.

AbiWord peut importer et exporter dans de nombreux formats de fichiers, dont certains formats propriétaires comme le .doc de Microsoft®.

AbiWord est disponible sous forme pré-compilée. Vous pouvez l'installer avec:

```
# pkg_add -r abiword
```

Si la version pré-compilée n'est pas disponible, il peut être compilé à partir du catalogue des logiciels portés. Le catalogue devra être plus à jour. Cela peut être fait de cette façon:

```
# cd /usr/ports/editors/abiword
# make install clean
```

6.3.3. The GIMP

Pour la création et la retouche d'image The GIMP est un programme de manipulation d'image très sophistiqué. Il peut être utilisé comme un simple programme de dessin ou comme une suite de retouche d'image de qualité photo. Il supporte un grand nombre de modules additionnels et présente une interface de création de procédures. The GIMP peut lire et écrire dans un très grand nombre de formats de fichiers. Il supporte l'interfaçage avec des scanners et des tablettes graphiques.

Vous pouvez installer la version pré-compilée en utilisant cette commande:

```
# pkg_add -r gimp
```

Si votre site FTP ne dispose pas de la version pré-compilée, vous pouvez utiliser le catalogue des logiciels portés. Le répertoire graphics du catalogue contient également le Manuel de The Gimp. Voici comment les installer:

```
# cd /usr/ports/graphics/gimp
# make install clean
# cd /usr/ports/graphics/gimp-manual-pdf
# make install clean
```

Le répertoire graphics du catalogue des logiciels portés contient la version de développement de The GIMP dans graphics/gimp-devel. Une version HTML du Manuel de The Gimp est disponible à partir de graphics/gimp-manual-html.

6.3.4. OpenOffice.org

OpenOffice.org comprend toutes les applications indispensables d'une suite de bureautique complète: un traitement de texte, un tableur, un programme de gestion de présentation, et un logiciel de dessin. Son interface utilisateur est très proche de celle d'autres suites de bureautique, et elle peut importer et exporter dans divers formats de fichiers populaires. Elle est disponible dans de nombreuses langues - l'interface, les correcteurs orthographiques, et les dictionnaires ont été internationalisés.

Le traitement de texte d'OpenOffice.org utilise un format de fichier natif en XML pour augmenter la portabilité et la flexibilité. Le tableur dispose d'un langage de macro et il peut être interfacé avec des bases de données extérieures. OpenOffice.org est déjà stable et fonctionne en natif sous Windows®, Solaris™, Linux, FreeBSD, et Mac OS® X. Plus d'information à propos d'OpenOffice.org peut être trouvé sur le site Web d'OpenOffice.org. Pour une information spécifique à FreeBSD, et pour télécharger directement les versions précompilées, utilisez le site Web de l'Equipe FreeBSD de portage d'OpenOffice.org.

Pour installer OpenOffice.org, faites:

```
# pkg_add -r openoffice.org
```

Cette commande devrait fonctionner si vous utilisez une version -RELEASE de FreeBSD. Si ce n'est pas le cas, vous devriez consulter le site de l'équipe de portage d'OpenOffice.org pour télécharger puis installer le paquetage adéquat en utilisant pkg_add(1). Les versions actuelles et de développement sont disponibles.

Une fois l'installation effective, vous avez juste à taper la commande suivante pour exécuter OpenOffice.org:

```
% openoffice.org
```

Lors de la première exécution, quelques questions vous seront posées et un répertoire .openoffice.org2 sera créé dans votre répertoire utilisateur.

Si les version pré-compilées d'OpenOffice.org ne sont pas disponibles, vous avez toujours la possibilité de compiler le logiciel porté. Cependant, vous devez garder à l'esprit que cela demande

beaucoup d'espace disque et un temps de compilation relativement long.

```
# cd /usr/ports/editors/openoffice.org-2
# make install clean
```

Si vous désirez compiler une version localisée, remplacez la dernière ligne de commande avec la suivante:

```
# make LOCALIZED_LANG=votre_langage install clean
```

Vous devez remplacer *votre_langage* avec le code ISO de langage approprié. Une liste des codes de langage supportés est disponible dans le fichier files/Makefile.localized situé dans le répertoire du logiciel porté.

Une fois cela effectué, OpenOffice.org peut être lancé avec la commande:

```
% openoffice.org
```

6.4. Lecteurs de document

Certains nouveaux formats de documentation ont gagné en popularité depuis l'avènement d'UNIX®; les lecteurs standard qu'ils nécessitent peuvent ne pas être disponibles dans le système de base. Nous verrons, dans cette section, comment installer ces lecteurs de document.

Cette section couvre les applications suivantes:

Nom de l'application	Ressources nécessaires	Installation à partir du catalogue des logiciels portés	Dépendances principales
Acrobat Reader®	faibles	légère	Compatibilité binaire Linux
gv	faibles	légère	Xaw3d
Xpdf	faibles	légère	FreeType
GQview	faibles	légère	Gtk+ ou GNOME

6.4.1. Acrobat Reader®

De nombreux documents sont désormais distribués sous forme de fichiers PDF, qui signifie "Format Portable de Document" - Portable Document Format. Un des lecteurs recommandé est Acrobat Reader®, sorti par Adobe pour Linux. Comme FreeBSD peut exécuter les binaires Linux, il est également disponible pour FreeBSD.

Pour installer Acrobat Reader® 7, à partir du catalogue de logiciels portés, faire:

```
# cd /usr/ports/print/acroread7
# make install clean
```

Il n'existe pas de paquetage pour des raisons de licence.

6.4.2. gv

gv un lecteur de fichier PostScript® et PDF. Il est a l'origine basé sur ghostview mais présente un plus bel aspect grâce à la bibliothèque Xaw3d. Il est rapide et son interface est simple. gv possède de nombreuses fonctionnalités comme l'orientation, le format du papier, l'échelle, l'anticrénelage. Presque toutes les opérations peuvent être effectuées soit à partir du clavier soit à la souris.

Pour installer gv à partir de la version pré-compilée, faites:

```
# pkg_add -r gv
```

Si vous ne pouvez obtenir la version pré-compilée, vous pouvez utiliser le catalogue des logiciels portés:

```
# cd /usr/ports/print/gv
# make install clean
```

6.4.3. Xpdf

Si vous désirez un petit lecteur de fichiers PDF, Xpdf est léger et efficace. Il demande très peu de ressources et est très stable. Il utilise les polices de caractères standards de X et ne requiert pas Motif® ou tout autre ensemble d'éléments graphiques pour X.

Pour installer la version pré-compilée d'Xpdf utilisez la commande suivante:

```
# pkg_add -r xpdf
```

Si la version pré-compilée n'est pas disponible ou que vous préfériez utiliser le catalogue des logiciels portés, faites:

```
# cd /usr/ports/graphics/xpdf
# make install clean
```

Une fois l'installation achevée, vous pouvez lancer Xpdf et utiliser le bouton droit de la souris pour activer le menu.

6.4.4. GQview

GQview est un gestionnaire d'image. Vous pouvez visualiser un fichier avec un simple clic, lancer

un éditeur externe, obtenir une pré-visualisation par vignettes, et bien plus. Il propose également un mode présentation et quelques possibilités d'opérations sur fichiers de base. Vous pouvez gérer des collections d'images et trouver facilement les doublons. GQview supporte l'affichage plein écran et l'internationalisation de l'interface.

Si vous désirez installer la version pré-compilée de GQview, faites:

```
# pkg_add -r gqview
```

Si la version pré-compilée n'est pas disponible ou que vous préférez utiliser le catalogue des logiciels portés, faites:

```
# cd /usr/ports/graphics/gqview
# make install clean
```

6.5. Finance

Si, pour diverses raisons, vous voudriez gérer vos finances personnelles sous FreeBSD, il existe quelques applications puissantes et simples d'emploi prêtes à être installées. Certaines d'entre elles sont compatibles avec des formats de fichiers très répandus comme ceux utilisés par Quicken ou Excel pour stocker des documents.

Cette section couvre les programmes suivants:

Nom de l'application	Ressources nécessaires	Installation à partir du catalogue des logiciels portés	Dépendances principales
GnuCash	faibles	lourde	GNOME
Gnumeric	faibles	lourde	GNOME
Abacus	faibles	légère	Tcl/Tk
KMyMoney	faibles	lourde	KDE

6.5.1. GnuCash

GnuCash fait partie de l'effort GNOME en vue de fournir des applications puissantes et conviviales pour l'utilisateur final. Avec GnuCash, vous pouvez suivre vos crédits et débits, vos comptes bancaires, et vos actions. Il présente une interface intuitive tout en restant très professionnel.

GnuCash fournit un registre intelligent, un système hiérarchique pour les comptes, de nombreux raccourcis clavier et des systèmes d'autocomplémentation de la frappe au clavier. Il peut diviser une simple transaction en plusieurs étapes plus détaillées. GnuCash peut importer et fusionner des fichiers QIF de Quicken. Il supporte également la plupart des formats internationaux de date et de monnaies.

Pour installer GnuCash sur votre système, faites:

```
# pkg_add -r gnucash
```

Si la version pré-compilée n'est pas disponible, vous pouvez utiliser le catalogue des logiciels portés:

```
# cd /usr/ports/finance/gnucash
# make install clean
```

6.5.2. Gnumeric

Gnumeric est un tableur, faisant partie de l'environnement de travail GNOME. Il dispose d'un système automatique "devinant" le type d'entrée de l'utilisateur en fonction du format de la cellule avec un système de remplissage automatique pour de nombreuses séquences d'utilisation. Il peut importer des fichiers de nombreux formats populaires comme ceux d'Excel, Lotus 1-2-3, ou Quattro Pro. Gnumeric supporte l'affichage de graphiques grâce au programme de tracé math/guppi. Il dispose d'un grand nombre de fonctions intégrées et permet tous les formats de cellule habituels comme le format numérique, monétaire, date, temps, et bien plus.

Pour installer Gnumeric sous forme pré-compilée, tapez:

```
# pkg_add -r gnumeric
```

Si la version pré-compilée n'est pas disponible, vous pouvez utiliser le catalogue des logiciels portés en faisant:

```
# cd /usr/ports/math/gnumeric
# make install clean
```

6.5.3. Abacus

Abacus est un tableur léger et facile d'emploi. Il incorpore de nombreuses fonctions utiles dans plusieurs domaines comme les statistiques, la finance, et les mathématiques. Il peut importer et exporter en format Excel. Abacus peut produire des sorties en PostScript®.

Pour installer Abacus à partir de la version pré-compilée, faites:

```
# pkg_add -r abacus
```

Si la version pré-compilée n'est pas disponible, vous pouvez utiliser le catalogue des logiciels portés en faisant:

```
# cd /usr/ports/deskutils/abacus
```

```
# make install clean
```

6.5.4. KMyMoney

KMyMoney est un programme de comptabilité personnelle pour KDE. KMyMoney a pour objectif de fournir et d'incorporer toutes les fonctionnalités importantes que l'on retrouve dans les applications de comptabilité personnelle commerciales. Il met également l'accent sur la facilité d'utilisation et la mise en place d'une comptabilité en partie double. KMyMoney peut importer les fichiers au format Quicken (QIF), suivre des placements, gérer plusieurs monnaies et fournir une quantité de compte-rendus. La possibilité d'importer des fichiers au format OFX est également disponible à l'aide d'un greffon séparé.

Pour installer KMyMoney sous forme d'un paquetage:

```
# pkg_add -r kmymoney2
```

Si le paquetage n'est pas disponible, vous pouvez utiliser le catalogue des logiciels portés:

```
# cd /usr/ports/finance/kmymoney2
# make install clean
```

6.6. Résumé

Alors que FreeBSD est populaire parmi les fournisseurs d'accès à Internet pour ses performances et sa stabilité, il est quasiment prêt pour une utilisation quotidienne en tant que station de travail. Avec plusieurs milliers d'applications disponibles sous forme pré-compilées ou dans le catalogue des logiciels portés, vous pouvez vous construire l'environnement de travail qui vous conviendra le mieux.

Voici un bref rappel de toutes les applications abordées dans ce chapitre:

Nom de l'application	Nom du logiciel pré-compilé	Nom du logiciel porté
Mozilla	`mozilla`	www/mozilla
Opera	`opera`	www/opera
Firefox	`firefox`	www/firefox
KOffice	`koffice-kde3`	editors/koffice-kde3
AbiWord	`abiword`	editors/abiword
The GIMP	`gimp`	graphics/gimp
OpenOffice.org	`openoffice`	editors/openoffice-1.1
Acrobat Reader®	`acroread`	print/acroread7
gv	`gv`	print/gv

Nom de l'application	Nom du logiciel pré-compilé	Nom du logiciel porté
Xpdf	`xpdf`	graphics/xpdf
GQview	`gqview`	graphics/gqview
GnuCash	`gnucash`	finance/gnucash
Gnumeric	`gnumeric`	math/gnumeric
Abacus	`abacus`	deskutils/abacus

Chapitre 7. Multimédia

7.1. Synopsis

FreeBSD supporte une grande variété de cartes son, vous permettant d'obtenir un son haute fidélité à partir de votre ordinateur. Ceci inclut la possibilité d'enregistrer et de jouer les formats "MPEG Audio Layer 3" (MP3), WAV et Ogg Vorbis aussi bien que de nombreux autres formats. Le catalogue de logiciels portés de FreeBSD contient également des applications vous permettant d'éditer vos enregistrements, rajouter des effets sonores, et contrôler des périphériques MIDI.

Avec un peu d'expérimentation, FreeBSD pourra lire des fichiers vidéo et des DVDs. Le nombre d'applications pour encoder, convertir, et lire divers supports vidéo est plus limité que le nombre d'applications équivalentes dans le domaine du son. Par exemple au moment de l'écriture de ces lignes, il n'existe pas de bonne application d'encodage dans le catalogue des logiciels portés de FreeBSD, qui pourra être utilisée pour convertir d'un format à un autre, comme peut le faire pour le son le programme audio/sox. Cependant, le paysage logiciel dans ce domaine évolue rapidement.

Ce chapitre décrira les étapes nécessaires pour configurer votre carte son. La configuration et l'installation d'X11 (Le système X Window) ont déjà pris soin des problèmes matériel de votre carte vidéo, bien qu'il puisse y avoir quelques réglages à ajuster pour obtenir une meilleure lecture des vidéos.

Après la lecture de ce chapitre, vous connaîtrez:

- Comment configurer votre système afin que votre carte son soit reconnue.
- Les méthodes pour tester le fonctionnement de votre carte.
- Comment faire face aux problèmes de configuration de votre carte son.
- Comment jouer et encoder des MP3s.
- Comment la vidéo est supportée par X11.
- Quelques logiciels portés qui donnent de bon résultats pour lire/encoder de la vidéo.
- Comment lire des DVDs, des fichiers .mpg et .avi.
- Comment extraire l'information présente sur des CDs et des DVDs.
- Comment configurer une carte TV.
- Comment configurer un scanner.

Avant de lire ce chapitre, vous devrez:

- Savoir comment configurer et installer un nouveau noyau (Configurer le noyau de FreeBSD).

Essayer de monter des CDs audio avec la commande mount(8) aura pour résultat une erreur, au moins, et une *panique du noyau*, au pire. Ces supports ont des codages spécifiques qui diffèrent du système de fichiers ISO classique.

7.2. Configurer une carte son

7.2.1. Configuration du système

Avant que vous commenciez, vous devriez connaître le modèle de carte son que vous avez, la puce qu'elle utilise, et si c'est une carte PCI ou ISA. FreeBSD supporte une grande variété de cartes PCI et ISA. Consultez la liste des périphériques audio supportés des notes de compatibilité matériel pour voir si votre carte est supportée. Ces notes indiqueront également quel pilote supporte votre carte.

Pour utiliser votre carte son, vous devrez charger le pilote de périphérique approprié. Cela peut être fait de deux façons. La plus simple est de charger le module pour votre carte son avec kldload(8), ce qui peut être soit fait à partir de la ligne de commande:

```
# kldload snd_emu10k1
```

soit en ajoutant la ligne appropriée dans le fichier /boot/loader.conf comme cela:

```
snd_emu10k1_load="YES"
```

Ces exemples concernent la carte Creative SoundBlaster® Live!. Les autres modules son chargeables sont listés dans /boot/defaults/loader.conf. Si vous n'êtes pas sûr du pilote à utiliser, vous pouvez tenter de charger le pilote snd_driver:

```
# kldload snd_driver
```

C'est un méta-pilote chargeant directement les pilotes les plus courants. Cela accélère la recherche du pilote adapté. Il est également possible de charger l'intégralité des pilotes de cartes son en utilisant le système /boot/loader.conf.

Si vous voulez connaître le pilote sélectionné lors du chargement du méta-pilote snd_driver, vous pouvez consulter le fichier /dev/sndstat à cet effet, et cela à l'aide de la commande `cat /dev/sndstat`.

Une seconde méthode est de compiler le support pour votre carte son en statique dans votre noyau. La section ci-dessous fournit les informations nécessaires pour ajouter le support de votre matériel de cette manière. Pour plus d'informations au sujet de la recompilation de votre noyau, veuillez consulter le Configurer le noyau de FreeBSD.

7.2.1.1. Configurer un noyau sur mesure avec support du son

La première chose à effectuer est d'ajouter au noyau le pilote de périphérique audio générique sound(4); pour cela vous devrez ajouter la ligne suivante au fichier de configuration du noyau:

```
device sound
```

Ensuite, vous devez ajouter le support pour votre carte son. Par conséquent, vous devez savoir quel

pilote supporte la carte. Consultez la liste des périphériques audio supportés des notes de compatibilité matériel pour déterminer le pilote correct pour votre carte son. Par exemple, une carte son Creative SoundBlaster® Live! est supportée par le pilote snd_emu10k1(4). Pour ajouter le support pour cette carte, utilisez ce qui suit:

```
device snd_emu10k1
```

Assurez-vous de lire la page de manuel du pilote pour la syntaxe à utiliser. La syntaxe de la configuration du noyau pour chaque pilote de carte son supportée peut être également trouvée dans le fichier /usr/src/sys/conf/NOTES.

Les cartes son ISA non-PnP pourront nécessiter de fournir au noyau des informations sur le paramétrage de la carte (IRQ, port d'E/S, etc.), comme c'est en général le cas pour toutes les cartes ISA non-PnP. Cela s'effectue par l'intermédiaire du fichier /boot/device.hints. Au démarrage du système, le chargeur (loader(8)) lira ce fichier et passera les paramètres au noyau. Par exemple, une vieille carte ISA non-PnP Creative SoundBlaster® 16 utilisera le pilote snd_sbc(4) de paire avec `snd_sb16`, on ajoutera alors la ligne suivante au fichier de configuration du noyau:

```
device snd_sbc
device snd_sb16
```

avec également ceci dans le fichier /boot/device.hints:

```
hint.sbc.0.at="isa"
hint.sbc.0.port="0x220"
hint.sbc.0.irq="5"
hint.sbc.0.drq="1"
hint.sbc.0.flags="0x15"
```

Dans ce cas, la carte utilise le port d'E/S `0x220` et l'IRQ `5`.

La syntaxe utilisée dans le fichier /boot/device.hints est abordée dans la page de manuel du pilote sound(4) ainsi que celle du pilote spécifique à la carte son.

Les paramètres donnés ci-dessus sont ceux par défaut. Dans certains cas, vous pouvez avoir besoin de modifier l'IRQ ou tout autre paramètre en fonction de votre carte son. Consultez la page de manuel snd_sbc(4) pour plus d'informations au sujet de cette carte.

7.2.2. Tester la carte son

Après avoir redémarré avec le noyau modifié, ou après avoir chargé le module nécessaire, la carte son devrait apparaître dans le tampon des messages du système (dmesg(8)) d'un manière proche de la suivante:

```
pcm0: <Intel ICH3 (82801CA)> port 0xdc80-0xdcbf,0xd800-0xd8ff irq 5 at device 31.5 on
pci0
```

```
pcm0: [GIANT-LOCKED]
pcm0: <Cirrus Logic CS4205 AC97 Codec>
```

L'état de la carte son peut être contrôlée par l'intermédiaire du fichier /dev/sndstat:

```
# cat /dev/sndstat
FreeBSD Audio Driver (newpcm)
Installed devices:
pcm0: <Intel ICH3 (82801CA)> at io 0xd800, 0xdc80 irq 5 bufsz 16384
kld snd_ich (1p/2r/0v channels duplex default)
```

Le résultat pourra être différent sur votre système. Si aucun périphérique pcm n'apparaît, retournez en arrière et revoyez ce qui a été fait précédemment. Contrôlez à nouveau votre fichier de configuration du noyau et vérifiez que vous avez choisi le périphérique correct. Les problèmes courants sont listés dans la Problèmes courants.

Si tout va bien, vous devriez avoir maintenant une carte son qui fonctionne. Si la sortie audio de votre lecteur de CD-ROM ou de DVD-ROM est correctement reliée à votre carte son, vous pouvez introduire un CD dans le lecteur et le jouer avec cdcontrol(1):

```
% cdcontrol -f /dev/acd0 play 1
```

Diverses applications, comme audio/workman offrent une meilleure interface. Vous pouvez vouloir installer une application comme audio/mpg123 pour écouter des fichiers audio MP3.

Une autre méthode rapide pour tester la carte est d'envoyer des données au /dev/dsp, de la manière suivante:

```
% cat filename  /dev/dsp
```

où *filename* peut être n'importe quel fichier. Cette ligne de commande devrait produire des sons, confirmant le bon fonctionnement de la carte son.

Les niveaux du mixer de la carte son peuvent être modifiés par la commande mixer(8). Plus de détails peuvent être trouvés dans la page de manuel mixer(8).

7.2.2.1. Problèmes courants

Erreur	Solution
`sb_dspwr(XX) timed out`	Le port d'E/S n'est pas configuré correctement.
`bad irq XX`	L'IRQ sélectionnée est incorrecte. Vérifiez que l'IRQ choisie et l'IRQ de la carte son sont les mêmes.

Erreur	Solution
`xxx: gus pcm not attached, out of memory`	Il n'y a pas suffisamment de mémoire disponible pour utiliser ce périphérique.
`xxx: can't open /dev/dsp!`	Vérifiez avec la commande `fstat | grep dsp` si une autre application maintient le périphérique ouvert. Souvent à l'origine de ce type de problème on trouve esound et le support son de KDE.

7.2.3. Utiliser des sources sonores multiples

Il est souvent intéressant de pouvoir jouer simultanément du son à partir de multiples sources, comme lorsque esound ou artsd ne supportent pas le partage du périphérique son avec certaines applications.

FreeBSD vous permet de le faire par l'intermédiaire de *Canaux Sonores Virtuels*, qui peuvent être activés avec la fonction sysctl(8). Les canaux virtuels vous permettent de multiplexer la sortie de votre carte son en mixant le son au niveau du noyau.

Pour configurer le nombre de canaux virtuels, il existe deux paramètres de sysctl qui, si vous avez les privilèges de l'utilisateur `root`, peuvent être configurés comme ceci:

```
# sysctl hw.snd.pcm0.vchans=4
# sysctl hw.snd.maxautovchans=4
```

L'exemple ci-dessus alloue quatre canaux virtuels, ce qui est un nombre suffisant pour une utilisation classique. `hw.snd.pcm0.vchans` est le nombre de canaux virtuels que possède pcm0, et est configurable une fois que le périphérique a été attaché au système. `hw.snd.maxautovchans` est le nombre de canaux virtuels alloués à un nouveau périphérique audio quand il est attaché à l'aide de kldload(8). Comme le module pcm peut être chargé indépendamment des pilotes de périphériques, `hw.snd.maxautovchans` peut stocker combien de canaux virtuels seront alloués à chaque périphérique attaché par la suite.

Vous ne pouvez pas modifier le nombre de canaux virtuels pour un périphérique en cours d'utilisation. Quittez avant tout autre chose les programmes utilisant le périphérique en question, comme les lecteurs de fichiers sonores ou les "daemons" audios.

Si vous n'utilisez pas devfs(5), vous devrez faire pointer vos applications sur /dev/dsp0.*x*, où *x* est 0 à 3 si `hw.snd.pcm.0.vchans` est fixé à 4. Sur un système utilisant devfs(5), ce qui précède sera automatiquement effectué de façon transparente pour le programme qui réclame le périphérique /dev/dsp0.

7.2.4. Définir les valeurs par défaut du mixeur des différents canaux

Les valeurs par défaut du mixeur des différents canaux sont fixées en dur dans le code source du

pilote pcm(4). Il existe plusieurs applications et "daemons" qui vous permettent de fixer les valeurs du mixeur qui seront mémorisées entre chaque invocation, mais ce n'est pas une solution idéale. Il est possible régler les valeurs par défaut au niveau du pilote - ceci se fait en définissant les valeurs adéquates dans le fichier /boot/device.hints. Par exemple:

```
hint.pcm.0.vol="50"
```

Cela fixera le volume du canal à une valeur par défaut de 50; dès que le module pcm(4) est chargé.

7.3. Fichiers MP3

Les fichiers MP3 (MPEG Layer 3 Audio) donnent un son proche de la qualité d'un CD audio, il n'y a aucune raison pour que votre station de travail FreeBSD ne puisse pas en profiter.

7.3.1. Lecteurs de MP3s

De loin, le plus populaire des lecteurs MP3 pour X11 est XMMS (X Multimedia System). Les thèmes (skins) de Winamp peuvent être utilisés avec XMMS dès lors que l'interface est quasiment identique à celle du Winamp de Nullsoft. XMMS dispose aussi d'un support natif pour modules externes (plug-in).

XMMS peut être installé à partir du catalogue de logiciels portés multimedia/xmms ou de la version pré-compilée.

L'interface d'XMMS est intuitive, avec une liste de lecture, un égaliseur graphique, et plus. Ceux qui sont familiers avec Winamp trouveront XMMS simple d'utilisation.

Le logiciel porté audio/mpg123 est une alternative, un lecteur de MP3 en ligne de commande.

mpg123 peut être utilisé en spécifiant le périphérique sonore et le fichier MP3 sur la ligne de commande, comme montré ci-dessous:

```
# mpg123 -a /dev/dsp1.0 Foobar-GreatestHits.mp3
High Performance MPEG 1.0/2.0/2.5 Audio Player for Layer 1, 2 and 3.
Version 0.59r (1999/Jun/15). Written and copyrights by Michael Hipp.
Uses code from various people. See 'README' for more!
THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTY! USE AT YOUR OWN RISK!

Playing MPEG stream from Foobar-GreastestHits.mp3 ...
MPEG 1.0 layer III, 128 kbit/s, 44100 Hz joint-stereo
```

`/dev/dsp1.0` devrait être remplacé par le périphérique dsp correspondant sur votre système.

7.3.2. Extraire les pistes de CDs Audio

Avant d'encoder la totalité d'un CD ou une piste en MP3, les données audio doivent être extraites et transférées sur le disque dur. Cela se fait en copiant les données brutes CDDA (CD Digital Audio) en

fichiers WAV.

L'utilitaire `cdda2wav`, qui fait partie de la suite sysutils/cdrtools, est utilisé pour extraire les données audio de CDs et les informations rattachées.

Avec le CD audio dans le lecteur, la commande suivante peut être utilisée (en tant que `root`) pour convertir l'intégralité d'un CD en fichiers WAV (un par piste):

```
# cdda2wav -D 0,1,0 -B
```

cdda2wav supportera également les lecteurs de CDROM ATAPI (IDE). Pour faire l'extraction à partir d'un lecteur IDE, précisez le nom du périphérique à la place de l'unité SCSI. Par exemple, pour extraite la piste 7 à partir d'un lecteur IDE:

```
# cdda2wav -D /dev/acd0 -t 7
```

Le `-D 0,1,0` spécifie le périphérique SCSI 0,1,0, qui correspond à ce qui est donné par la commande `cdrecord -scanbus`.

Pour extraire des pistes individuelles, utilisez l'option `-t` comme ceci:

```
# cdda2wav -D 0,1,0 -t 7
```

Cet exemple extrait la septième piste du CD audio. Pour extraire un ensemble de pistes, par exemple, de la piste 1 à 7, précisez un intervalle:

```
# cdda2wav -D 0,1,0 -t 1+7
```

L'utilitaire dd(1) peut également être utilisé pour extraire des pistes audios à partir de lecteurs ATAPI, consultez la Dupliquer des CDs Audio pour plus d'informations sur cette possibilité.

7.3.3. Encoder des MP3s

De nos jours, l'encodeur mp3 à utiliser est lame. Lame peut être trouvé dans le catalogue de logiciels portés: audio/lame.

En utilisant les fichiers WAV extraits, la commande suivante convertira le fichier audio01.wav en audio01.mp3:

```
# lame -h -b 128 \
--tt "La chanson XY" \
--ta "Artiste XY" \
--tl "Album XY" \
--ty "2001" \
--tc "Extrait et encodé par XY" \
```

```
--tg "Genre" \
audio01.wav audio01.mp3
```

128 kbits semble être le taux standard actuel du débit audio utilisé pour les MP3s. Nombreux sont ceux qui préfèrent des taux de haute qualité: 160 ou 192. Plus le débit audio est élevé plus l'espace disque utilisé par le fichier MP3 sera grand mais la qualité sera meilleure. L'option `-h` active le mode "haute qualité, mais un peu plus lent". Les options commençant par `--t` indiquent des balises ID3, qui généralement contiennent les informations sur le morceau, devant être intégrées au fichier MP3. D'autres informations sur l'encodage peuvent être trouvées en consultant la page de manuel de Lame.

7.3.4. Décoder des MP3s

Afin de pouvoir graver un CD audio à partir de fichiers MP3, ces derniers doivent être convertis dans le format WAV non compressé. XMMS et mpg123 supportent tous les deux la sortie de fichiers MP3 en format de fichier non compressé.

Ecriture sur le disque avec XMMS:

1. Lancez XMMS.
2. Clic-droit sur la fenêtre pour faire apparaître le menu d'XMMS.
3. Sélectionner `Preference` sous `Options`.
4. Changez l'option "Output Plugin" pour "Disk Writer Plugin".
5. Appuyez sur `Configure`.
6. Entrez (ou choisissez browse) un répertoire où va être écrit le fichier décompressé.
7. Chargez le fichier MP3 dans XMMS comme à l'accoutumé, avec le volume à 100% et l'égaliseur (EQ settings) désactivé.
8. Appuyez sur `Play` - XMMS devrait se comporter comme s'il jouait le MP3, mais aucun son ne sera audible. Il est en fait en train de "jouer" le MP3 dans un fichier.
9. Vérifiez que vous avez rétabli l'option "Output Plugin" à sa valeur de départ afin de pouvoir écouter à nouveau des MP3s.

Ecriture sur le disque avec mpg123:

1. Lancez `mpg123 -s audio01.mp3 audio01.pcm`

XMMS crée un fichier au format WAV, tandis que mpg123 convertit le fichier MP3 en données audio PCM brutes. Ces deux formats peuvent être utilisés avec cdrecord pour créer des CDs audio. Vous devez utiliser des fichiers PCM bruts avec burncd(8). Si vous utilisez des fichiers WAV, vous noterez un petit parasite au début de chaque piste, ce son est l'entête du fichier WAV. Vous pouvez simplement retirer l'entête d'un fichier WAV avec l'utilitaire SoX (il peut être installé à partir du logiciel porté audio/sox ou de la version pré-compilée):

```
% sox -t wav -r 44100 -s -w -c 2 track.wav track.raw
```

Lisez la Création et utilisation de supports optiques (CDs) pour plus d'informations sur l'utilisation d'un graveur de CD sous FreeBSD.

7.4. Lecture des Vidéos

Les applications pour lire des vidéos sont assez récentes et se développent très rapidement. Soyez patient. Tout ne va pas fonctionner aussi bien que cela pu être le cas avec le son.

Avant que vous ne commenciez, vous devrez connaître le modèle de carte vidéo dont vous disposez ainsi que le circuit intégré qu'elle utilise. Alors qu'Xorg et XFree86™ supportent une large variété de cartes vidéo, seul un petit nombre d'entre elles donne de bonnes performances en lecture de vidéos. Pour obtenir la liste des extensions supportées par le serveur X utilisant votre carte employez la commande xdpyinfo(1) durant le fonctionnement d'X11.

C'est une bonne idée d'avoir un court fichier MPEG qui pourra être utilisé comme fichier test pour évaluer divers lecteurs et leurs options. Comme certains programmes de lecture de DVD chercheront un support DVD sur /dev/dvd par défaut, ou ont ce périphérique fixé définitivement dans leur code, vous pourrez trouver utile de créer des liens symboliques vers les périphériques corrects:

```
# ln -sf /dev/acd0 /dev/dvd
# ln -sf /dev/acd0 /dev/rdvd
```

Notez qu'en raison de la nature du système devfs(5), les liens créés à la main comme les précédents ne seront pas conservés si vous redémarrez le système. Afin de créer automatiquement les liens symboliques dès que vous redémarrez votre système, ajoutez les lignes suivantes au fichier /etc/devfs.conf:

```
link acd0 dvd
link acd0 rdvd
```

De plus, le décodage de DVD, qui nécessite de faire appel à des fonctions spéciales du lecteur de DVD, demande d'avoir la permission d'écrire sur les périphériques DVD.

Pour augmenter la mémoire partagée pour l'interface X11, il est recommandé que les valeurs de certaines variables sysctl(8) soient augmentées:

```
kern.ipc.shmmax=67108864
kern.ipc.shmall=32768
```

7.4.1. Déterminer les capacités vidéo

Il y a plusieurs manières possibles pour afficher de la vidéo sous X11. Ce qui fonctionnera vraiment est énormément dépendant du matériel. Chaque méthode décrite ci-dessous donnera différents résultats en fonction du matériel. De plus, le rendu de la vidéo sous X11 est un sujet recevant beaucoup d'attention dernièrement, et avec chaque nouvelle version d'Xorg, ou d'XFree86™, il pourra y avoir des améliorations significatives.

Une liste des interfaces vidéo communes:

1. X11: sortie X11 classique utilisant de la mémoire partagée.
2. XVideo: une extension de l'interface X11 qui supporte la vidéo sur n'importe quelle partie de l'écran contrôlé par X11.
3. SDL: "Simple Directmedia Layer" - couche simple d'accès directe au média.
4. DGA: "Direct Graphics Access" - accès direct au graphique.
5. SVGAlib: couche graphique bas niveau pour la console.

7.4.1.1. XVideo

Xorg et XFree86™ 4.X disposent d'une extension appelée *XVideo* (également connue sous les termes Xvideo, Xv, ou xv) qui permet d'afficher directement de la vidéo à travers une accélération spécifique. Cette extension fournit une très bonne qualité de rendu même sur les machines bas de gamme.

Pour vérifier si l'extension fonctionne utilisez `xvinfo`:

```
% xvinfo
```

XVideo est supporté pour votre carte si le résultat de la commande ressemble à:

```
X-Video Extension version 2.2
screen #0
  Adaptor #0: "Savage Streams Engine"
    number of ports: 1
    port base: 43
    operations supported: PutImage
    supported visuals:
      depth 16, visualID 0x22
      depth 16, visualID 0x23
    number of attributes: 5
      "XV_COLORKEY" (range 0 to 16777215)
              client settable attribute
              client gettable attribute (current value is 2110)
      "XV_BRIGHTNESS" (range -128 to 127)
              client settable attribute
              client gettable attribute (current value is 0)
      "XV_CONTRAST" (range 0 to 255)
```

```
            client settable attribute
            client gettable attribute (current value is 128)
    "XV_SATURATION" (range 0 to 255)
            client settable attribute
            client gettable attribute (current value is 128)
    "XV_HUE" (range -180 to 180)
            client settable attribute
            client gettable attribute (current value is 0)
  maximum XvImage size: 1024 x 1024
  Number of image formats: 7
    id: 0x32595559 (YUY2)
      guid: 59555932-0000-0010-8000-00aa00389b71
      bits per pixel: 16
      number of planes: 1
      type: YUV (packed)
    id: 0x32315659 (YV12)
      guid: 59563132-0000-0010-8000-00aa00389b71
      bits per pixel: 12
      number of planes: 3
      type: YUV (planar)
    id: 0x30323449 (I420)
      guid: 49343230-0000-0010-8000-00aa00389b71
      bits per pixel: 12
      number of planes: 3
      type: YUV (planar)
    id: 0x36315652 (RV16)
      guid: 52563135-0000-0000-0000-000000000000
      bits per pixel: 16
      number of planes: 1
      type: RGB (packed)
      depth: 0
      red, green, blue masks: 0x1f, 0x3e0, 0x7c00
    id: 0x35315652 (RV15)
      guid: 52563136-0000-0000-0000-000000000000
      bits per pixel: 16
      number of planes: 1
      type: RGB (packed)
      depth: 0
      red, green, blue masks: 0x1f, 0x7e0, 0xf800
    id: 0x31313259 (Y211)
      guid: 59323131-0000-0010-8000-00aa00389b71
      bits per pixel: 6
      number of planes: 3
      type: YUV (packed)
    id: 0x0
      guid: 00000000-0000-0000-0000-000000000000
      bits per pixel: 0
      number of planes: 0
      type: RGB (packed)
      depth: 1
```

```
        red, green, blue masks: 0x0, 0x0, 0x0
```

Notez également que les formats listés (YUV2, YUV12, etc...) ne sont pas présents dans chaque implémentation d'XVideo et leur absence pourra gêner certains programmes.

Si le résultat ressemble à:

```
X-Video Extension version 2.2
screen #0
no adaptors present
```

Alors XVideo n'est probablement pas supporté pour votre carte.

Si XVideo n'est pas supporté pour votre carte, cela signifie seulement qu'il sera plus difficile pour votre système d'affichage de répondre aux demandes du rendu vidéo en termes de puissance de calcul. En fonction de votre carte vidéo et de votre processeur, vous pourriez encore obtenir de bons résultats. Vous devriez probablement vous documenter sur les méthodes pour améliorer les performances en lisant la Lectures supplémentaires.

7.4.1.2. "Simple Directmedia Layer" - couche simple d'accès directe au média

La couche simple d'accès directe au média, SDL, a été prévue pour être une couche de portage entre Microsoft® Windows®, BeOS, et UNIX®, permettant à des applications "cross-platform" qui font un usage efficace du son et du graphique d'être développées. La couche SDL fournit une abstraction de bas niveau vers le matériel qui peut parfois être plus efficace que l'interface X11.

La bibliothèque SDL peut être trouvée dans devel/sdl12.

7.4.1.3. "Direct Graphics Access" - accès direct au graphique

L'accès direct au graphique est une extension X11 qui permet à un programme de bypasser le serveur X et d'accéder directement au matériel. Comme il repose sur une copie bas niveau de la mémoire, les programmes l'utilisant doivent être exécutés avec les privilèges de l'utilisateur `root`.

L'extension DGA et ses performances peuvent être testées avec dga(1). Quand `dga` est exécuté, il changera les couleurs de l'affichage à chaque appui sur une touche. Pour quitter, utilisez la touche `q`.

7.4.2. Logiciels portés et pré-compilés relatifs à la vidéo

Cette section traite des logiciels disponibles dans le catalogue des logiciels portés de FreeBSD qui peuvent être utilisés pour lire de la vidéo. Les applications vidéos sont un domaine de développement très actif, et les capacités de diverses applications seront sujettes à des divergences avec la description donnée ici.

Premièrement, il est important de savoir que plusieurs des applications vidéos fonctionnant sous FreeBSD ont été développées comme des applications pour Linux. Plusieurs de ces applications sont encore considérées comme étant de qualité bêta. Parmi les problèmes que l'on peut rencontrer

avec les applications vidéos sous FreeBSD, nous trouvons:

1. Une application ne peut pas lire un fichier produit par une autre application.
2. Une application ne peut pas lire un fichier quelle a produit.
3. La même application sur deux machines différentes, recompilée sur chaque machine pour la machine elle-même, jouera le fichier différemment.
4. Un filtre apparemment insignifiant comme un changement d'échelle de l'image donne de très mauvais résultats en raison d'une routine de changement d'échelle boguée.
5. Une application qui plante régulièrement.
6. La documentation n'est pas installée avec le logiciel porté et peut être trouvée sur Internet ou dans le répertoire work du logiciel porté.

Parmin ces applications, nombreuses sont celles qui peuvent présenter des "Linuxismes". Aussi, il y peut y avoir des problèmes résultants de la façon dont certaines bibliothèques standards sont implémentées dans les distributions Linux, ou certaines caractéristiques du noyau Linux qui ont été employées par les auteurs des applications. Ces problèmes ne sont pas toujours remarqués et contournés par les responsables du portage du logiciel ce qui peut mener vers quelques ennuis comme ceux-ci:

1. L'utilisation de /proc/cpuinfo pour détecter les caractéristiques du processeur.
2. Une mauvaise utilisation des "threads" qui provoque le blocage de programme au lieu de se terminer complètement.
3. Des logiciels habituellement utilisés en conjonction avec l'application ne sont pas encore dans le catalogue des logiciels portés.

Jusqu'ici, les développeurs de ces applications ont été coopératifs avec les responsables des logiciels portés pour minimiser les modifications nécessaires au portage.

7.4.2.1. MPlayer

MPlayer est une application pour lire des vidéos récemment et rapidement développée. Les objectifs de l'équipe de MPlayer sont la rapidité et la flexibilité sur Linux et autre UNIX®. Le projet fut démarré quand le fondateur de l'équipe en eu assez des mauvaises performances en lecture des autres lecteurs disponibles. Certains diront que l'interface graphique a été sacrifiée pour une conception rationalisée. Cependant, une fois que vous avez les options en ligne de commande et les combinaisons de touches en main, cela fonctionne très bien.

7.4.2.1.1. Compiler MPlayer

MPlayer réside dans multimedia/mplayer. MPlayer effectue un certain nombre de contrôle du matériel durant le processus de compilation, il en résulte un binaire qui ne sera pas portable d'un système à l'autre. Ainsi il est important d'utiliser le logiciel porté et de ne pas utiliser un logiciel pré-compilé. En plus, un certain nombre d'options peuvent être spécifiées dans la ligne de commande `make`, comme décrit dans le fichier Makefile et au départ de la compilation:

```
# cd /usr/ports/multimedia/mplayer
```

```
# make
N - O - T - E

Take a careful look into the Makefile in order
to learn how to tune mplayer towards you personal preferences!
For example,
make WITH_GTK1
builds MPlayer with GTK1-GUI support.
If you want to use the GUI, you can either install
/usr/ports/multimedia/mplayer-skins
or download official skin collections from
http://www.mplayerhq.hu/homepage/dload.html
```

Les options par défaut du logiciel porté devraient être suffisantes pour la plupart des utilisateurs. Cependant si vous avez besoin du codec XviD, vous devez spécifier l'option `WITH_XVID` dans la ligne de commande. Le périphérique DVD par défaut peut également être défini avec l'option `WITH_DVD_DEVICE`, par défaut /dev/acd0 sera utilisé.

Au moment de l'écriture de ces lignes, le logiciel porté de MPlayer compilera sa documentation HTML et deux exécutables, `mplayer` et `mencoder`, qui est un outil pour ré-encoder de la vidéo.

La documentation HTML de MPlayer est très complète. Si le lecteur trouve l'information sur le matériel vidéo et les interfaces manquante dans ce chapitre, la documentation de MPlayer est une alternative très complète. Vous devriez certainement prendre le temps de lire la documentation de MPlayer, si vous êtes à la recherche d'informations sur le support vidéo sous UNIX®.

7.4.2.1.2. Utiliser MPlayer

Chaque utilisateur de MPlayer doit créer un sous-répertoire .mplayer dans son répertoire d'utilisateur. Pour créer ce sous-répertoire nécessaire, vous pouvez taper ce qui suit:

```
% cd /usr/ports/multimedia/mplayer
% make install-user
```

Les options de commande de `mplayer` sont données dans la page de manuel. Pour plus de détails il y a la documentation HTML. Dans cette section, nous décrirons que quelques unes des utilisations les plus courantes.

Pour lire à un fichier, comme testfile.avi en utilisant une des diverses interfaces vidéo utilisez l'option `-vo`:

```
% mplayer -vo xv testfile.avi
```

```
% mplayer -vo sdl testfile.avi
```

```
% mplayer -vo x11 testfile.avi
```

```
# mplayer -vo dga testfile.avi
```

```
# mplayer -vo 'sdl:dga' testfile.avi
```

Cela vaut la peine d'essayer toutes ces options, comme leur performance relative dépend de nombreux facteurs et variera de façon significative avec le matériel.

Pour lire un DVD, remplacez testfile.avi par `dvd://N -dvd-device DEVICE` où *N* est le numéro du titre à jouer et DEVICE est le fichier spécial de périphérique correspondant au lecteur de DVD. Par exemple, pour jouer le titre 3 depuis /dev/dvd:

```
# mplayer -vo xv dvd://3 -dvd-device /dev/dvd
```

Le périphérique DVD par défaut peut être défini lors de la compilation du logiciel porté MPlayer par l'intermédiaire de l'option `WITH_DVD_DEVICE`. Par défaut, ce périphérique est /dev/acd0. Plus de détails peuvent être trouvés dans le Makefile du logiciel porté.

Pour arrêter, avancer, etc..., consultez les combinaisons de touches, qui sont données en exécutant `mplayer -h` ou lisez la page de manuel.

D'autres options importantes pour la lecture sont: `-fs -zoom` qui active le mode plein écran et `-framedrop` qui aide au niveau des performances.

Pour que la ligne de commande à taper ne devienne pas trop longue, l'utilisateur peut créer un fichier .mplayer/config et y fixer les options par défaut:

```
vo=xv
fs=yes
zoom=yes
```

Enfin, `mplayer` peut être utilisé pour extraire une piste du DVD dans un fichier .vob. Pour récupérer la seconde piste vidéo d'un DVD, tapez ceci:

```
# mplayer -dumpstream -dumpfile out.vob dvd://2 -dvd-device /dev/dvd
```

Le fichier de sortie, out.vob, sera du MPEG et peut être manipulé par les autres logiciels décrits dans cette section.

7.4.2.1.3. mencoder

Avant d'utiliser `mencoder` c'est une bonne idée de vous familiariser avec les options données par la documentation HTML. Il existe une page de manuel, mais elle n'est pas très utile sans la documentation en HTML. Il y a d'innombrables façons d'améliorer la qualité, diminuer le débit binaire, et modifier les formats, et certaines de ces options peuvent faire la différence entre de bonnes et mauvaises performances. Voici quelques exemples pour y arriver. Tout d'abord une simple copie:

```
% mencoder input.avi -oac copy -ovc copy -o output.avi
```

De mauvaises combinaisons d'options peuvent conduire à des fichiers illisibles même par `mplayer`. Aussi, si vous voulez juste extraire un fichier, restez sur l'option `-dumpfile` de `mplayer`.

Pour convertir input.avi au format MPEG4 avec un codage audio MPEG3 (audio/lame est nécessaire):

```
% mencoder input.avi -oac mp3lame -lameopts br=192 \
     -ovc lavc -lavcopts vcodec=mpeg4:vhq -o output.avi
```

Ceci a produit un fichier lisible par `mplayer` et `xine`.

input.avi peut être remplacé par `dvd://1 -dvd-device /dev/dvd` et exécuté en tant que `root` pour ré-encoder directement un titre DVD. Puisque vous êtes susceptible de ne pas être satisfait du résultat la première fois, il est recommandé d'extraire le titre vers un fichier et de travailler sur le fichier.

7.4.2.2. Le lecteur xine

Le lecteur xine est un projet de grande envergure visant non seulement à être une solution vidéo tout-en-un, mais également de produire une bibliothèque de base réutilisable et un exécutable modulaire qui peut être étendu grâce à des greffons. Il est fourni sous forme pré-compilée et de logiciel porté, multimedia/xine.

Le lecteur xine est encore un peu brut, mais c'est clairement un bon début. Dans la pratique, xine demande soit un processeur rapide avec une carte vidéo rapide, soit l'extension XVideo. L'interface graphique est utilisable, mais peu pratique.

Au moment de l'écriture de ces lignes, il n'y a pas de module d'entrée fourni avec xine qui lira les DVDs codés en CSS. Il existe des versions tiers qui ont des modules à cet effet intégrés, mais aucune de ces dernières ne se trouve dans le catalogue des logiciels portés de FreeBSD.

Comparé à MPlayer, xine fait plus pour l'utilisateur, mais au même moment, rend inaccessible à l'utilisateur certains contrôles bien précis. Le lecteur xine se comporte le mieux sur les interfaces XVideo.

Par défaut, le lecteur xine lancera une interface graphique. Les menus peuvent alors être utilisés pour ouvrir un fichier précis:

```
% xine
```

Alternativement, le lecteur peut être invoqué pour jouer directement un fichier sans l'interface graphique avec la commande:

```
% xine -g -p mymovie.avi
```

7.4.2.3. Les utilitaires transcode

Le logiciel transcode n'est pas un lecteur, mais une suite d'outils pour ré-encoder les fichiers audio et vidéo. Avec transcode, on a la capacité de fusionner des fichiers vidéos, réparer les fichiers endommagés, en utilisant les outils en ligne de commande avec des interfaces de flots stdin/stdout.

Un grand nombre d'options peut être précisé lors de la compilation du logiciel porté multimedia/transcode, nous recommandons d'utiliser la ligne de commande suivante pour compiler transcode:

```
# make WITH_OPTIMIZED_CFLAGS=yes WITH_LIBA52=yes WITH_LAME=yes WITH_OGG=yes \
WITH_MJPEG=yes -DWITH_XVID=yes
```

Le paramétrage proposé devrait convenir à la plupart des utilisateurs.

Pour illustrer les capacités de `transcode`, voici un exemple montrant comment convertir un fichier DivX en fichier MPEG-1 en standard PAL (VCD PAL):

```
% transcode -i input.avi -V --export_prof vcd-pal -o output_vcd
% mplex -f 1 -o output_vcd.mpg output_vcd.m1v output_vcd.mpa
```

Le fichier MPEG résultant, output_vcd.mpg, peut être directement lu avec MPlayer. Vous pourrez même le graver sur un CD pour créer ainsi un Vidéo CD; dans ce cas vous devrez installer et utiliser les programmes multimedia/vcdimager et sysutils/cdrdao.

Il existe une page de manuel pour `transcode`, mais il est conseillé de consulter également le wiki de transcode pour plus d'information et des exemples.

7.4.3. Lectures supplémentaires

Les différents logiciels vidéo pour FreeBSD se développent rapidement. Il est fort possible que dans un futur proche plusieurs des problèmes abordés ici seront résolus. Entre temps ceux qui veulent tirer partie des possibilités audio/vidéo de FreeBSD devront se débrouiller avec des connaissances extraites de plusieurs FAQs et guides et utiliser différentes applications. Cette section existe pour fournir au lecteur des références sur ces documentations additionnelles.

La documentation de MPlayer est techniquement très instructive. Ces documents devraient probablement être consultés par quiconque désirant obtenir un niveau élevé d'expertise sur la

vidéo et UNIX®. La liste de diffusion de MPlayer est hostile à toute personne qui n'a pas pris la peine de lire la documentation, aussi si vous projetez de leur envoyer des rapports de bogue, lisez la documentation!

Le HOWTO de xine contient un chapitre sur l'amélioration des performances qui est général à tous les lecteurs de vidéo.

Et enfin, il y a quelques autres applications prometteuses que le lecteur devrait essayer:

- Avifile qui est également un logiciel porté multimedia/avifile.
- Ogle qui est également un logiciel porté multimedia/ogle.
- Xtheater
- multimedia/dvdauthor, un logiciel libre pour la création de DVDs.

7.5. Configuration des cartes TV

7.5.1. Introduction

Les cartes TV vous permettent de regarder sur votre ordinateur la télévision par voie hertzienne ou par câble. La plupart d'entre elles acceptent de la vidéo composite par l'intermédiaire de connecteurs RCA ou S-video et certaines de ces cartes disposent d'un tuner radio FM.

FreeBSD founit le support pour les cartes TV PCI utilisant un circuit de capture video Brooktree Bt848/849/878/879 ou Conexant CN-878/Fusion 878a à l'aide du pilote bktr(4). Vous devez également vous assurer que la carte dispose d'un tuner supporté, consultez la page de manuel bktr(4) pour une liste des tuners supportés.

7.5.2. Ajout du pilote de périphérique

Pour utiliser votre carte, vous devrez charger le pilote bktr(4), cela peut être effectué en ajoutant la ligne suivante au fichier /boot/loader.conf:

```
bktr_load="YES"
```

Alternativement, vous pouvez compiler en statique dans le noyau le support pour la carte TV, dans ce cas ajouter les lignes suivantes dans votre fichier de configuration du noyau:

```
device   bktr
device  iicbus
device  iicbb
device  smbus
```

Ces pilotes de périphériques supplémentaires sont nécessaires étant donné que les composants de la carte sont interconnectés via un bus I2C. Compilez et installez, ensuite, un nouveau noyau.

Une fois que le support a été ajouté au système, vous devez redémarrer votre machine. Durant le

processus de démarrage, votre carte TV devrait apparaître de cette manière:

```
bktr0: BrookTree 848A mem 0xd7000000-0xd7000fff irq 10 at device 10.0 on pci0
iicbb0: I2C bit-banging driver on bti2c0
iicbus0: Philips I2C bus on iicbb0 master-only
iicbus1: Philips I2C bus on iicbb0 master-only
smbus0: System Management Bus on bti2c0
bktr0: Pinnacle/Miro TV, Philips SECAM tuner.
```

Bien évidemment ces messages peuvent varier en fonction de votre matériel. Cependant assurez-vous que le tuner est correctement détecté; il est possible de forcer certains des paramètres détecté à l'aide du système sysctl(8) et d'options de configuration du noyau. Par exemple, si vous désirez forcer le tuner pour un tuner Philips SECAM, vous devrez ajouter la ligne suivante au fichier de configuration du noyau:

```
options OVERRIDE_TUNER=6
```

ou vous pouvez directement utiliser sysctl(8):

```
# sysctl hw.bt848.tuner=6
```

Consultez la page de manuel bktr(4) et le fichier /usr/src/sys/conf/NOTES pour plus de détails sur les options disponibles.

7.5.3. Applications utiles

Pour utiliser votre carte TV, vous devrez installer une des applications suivantes:

- multimedia/fxtv qui permet de regarder la télévision et d'enregistrer des images, du son et de la vidéo.
- multimedia/xawtv est également une application pour regarder la télévision avec les mêmes fonctionnalités que fxtv.
- misc/alevt décode et affiche les informations Vidéotexte/Télétexte.
- audio/xmradio, un programme pour utiliser le tuner FM fourni avec certaines cartes TV.
- audio/wmtune, une application intégrable dans votre environnement de travail pour gérer les tuners radio.

Plus d'applications sont disponibles dans le catalogue des logiciels portés de FreeBSD.

7.5.4. En cas de problème

Si vous rencontrez un quelconque problème avec votre carte TV, vous devriez contrôler tout d'abord que le circuit de capture video et le tuner sont vraiment supportés par le pilote bktr(4) et si vous avez utilisé les bonnes options de configuration. Pour plus de support et pour les diverses questions que vous pouvez vous poser à propos de votre carte TV, vous pouvez contacter et utiliser

les archives de la liste de diffusion liste de diffusion pour les discussions concernant le multimédia sous FreeBSD.

7.6. Scanners

7.6.1. Introduction

Sous FreeBSD, l'accès aux scanners est possible grâce à l'APISANE (Scanner Access Now Easy) disponible dans le catalogue des logiciels portés. SANE utilisera également certains pilotes de périphériques FreeBSD pour accéder à la partie matérielle du scanner.

FreeBSD supporte les scanners SCSI et USB. Assurez-vous que votre scanner est supporté par SANE avant d'effectuer une quelconque configuration. SANE dispose d'une liste des périphériques supportés qui peut vous informer sur le support et son statut pour un scanner particulier. La page de manuel uscanner(4) donne également une liste des scanners USB supportés.

7.6.2. Configuration du noyau

Comme mentionné plus haut les interfaces SCSI et USB sont supportées. En fonction de l'interface de votre scanner, différents pilotes de périphérique sont nécessaires.

7.6.2.1. Interface USB

Le noyau GENERIC inclut par défaut les pilotes nécessaires au support des scanners USB. Si vous décidez d'utiliser un noyau personnalisé, assurez-vous que les lignes suivantes sont présentes dans votre fichier de configuration du noyau:

```
device usb
device uhci
device ohci
device uscanner
```

En fonction du contrôleur USB présent sur votre carte mère, vous n'avez besoin que d'une des deux lignes `device uhci` et `device ohci`, cependant avoir ces deux lignes simultanément dans la configuration du noyau est sans risque.

Si vous ne désirez pas recompiler votre noyau et que votre noyau n'est pas le GENERIC, vous pouvez directement charger le module du pilote uscanner(4) à l'aide de la commande kldload(8):

```
# kldload uscanner
```

Pour charger ce module à chaque démarrage du système, ajoutez la ligne suivante au fichier /boot/loader.conf:

```
uscanner_load="YES"
```

Après avoir redémarré avec le bon noyau, ou après avoir chargé le module nécessaire, branchez votre scanner USB. Une ligne montrant la détection de votre scanner devrait apparaître dans le tampon des messages du système (dmesg(8)):

```
uscanner0: EPSON EPSON Scanner, rev 1.10/3.02, addr 2
```

Ceci nous indique que notre scanner utilise le fichier spécial de périphérique /dev/uscanner0.

7.6.2.2. Interface SCSI

Si votre scanner dispose d'une interface SCSI, il est important de connaître quelle carte contrôleur SCSI vous utiliserez. En fonction du contrôleur sur la carte, vous devrez adapter votre configuration du noyau. Le noyau GENERIC supporte les contrôleurs SCSI les plus courants. Assurez-vous d'avoir lu le fichier NOTES et ajoutez la ligne adéquate dans votre fichier de configuration du noyau. En plus du pilote de votre carte SCSI, vous avez besoin des lignes suivantes dans votre fichier de configuration du noyau:

```
device scbus
device pass
```

Une fois que votre noyau a été correctement compilé et installé, vous devriez être en mesure de voir les périphériques au démarrage:

```
pass2 at aic0 bus 0 target 2 lun 0
pass2: <AGFA SNAPSCAN 600 1.10> Fixed Scanner SCSI-2 device
pass2: 3.300MB/s transfers
```

Si votre scanner n'était pas alimenté au démarrage du système, il est encore possible de forcer sa détection, en en sondant le bus SCSI avec la commande camcontrol(8):

```
# camcontrol rescan all
Re-scan of bus 0 was successful
Re-scan of bus 1 was successful
Re-scan of bus 2 was successful
Re-scan of bus 3 was successful
```

Ensuite le scanner apparaîtra dans la liste des périphériques SCSI:

```
# camcontrol devlist
<IBM DDRS-34560 S97B>              at scbus0 target 5 lun 0 (pass0,da0)
<IBM DDRS-34560 S97B>              at scbus0 target 6 lun 0 (pass1,da1)
<AGFA SNAPSCAN 600 1.10>           at scbus1 target 2 lun 0 (pass3)
<PHILIPS CDD3610 CD-R/RW 1.00>     at scbus2 target 0 lun 0 (pass2,cd0)
```

Plus de détails sur les périphériques SCSI sont disponibles dans les pages de manuel scsi(4) et camcontrol(8).

7.6.3. Configuration de SANE

Le système SANE est divisé en deux parties: les "backend"s (graphics/sane-backends) et les "frontend"s (graphics/sane-frontends). Les "backend"s fournissent l'accès au scanner. La liste des périphériques supportés par SANE indique quel "backend" supportera votre scanner. Il est indispensable de déterminer correctement le "backend" relatif à votre scanner si vous voulez être en mesure d'utiliser votre périphérique. La partie "frontend"s fournie l'interface graphique de numérisation (xscanimage).

La première étape est d'installer le logiciel porté graphics/sane-backends ou sa version pré-compilée. Ensuite, utilisez la commande `sane-find-scanner` pour contrôler la détection du scanner par l'ensemble SANE:

```
# sane-find-scanner -q
found SCSI scanner "AGFA SNAPSCAN 600 1.10" at /dev/pass3
```

Le résultat de la commande affichera le type d'interface utilisée par le scanner et le fichier spécial de périphérique utilisé pour attacher le scanner au système. Le fabricant et le modèle peuvent ne pas apparaître, cela n'est pas important.

Certains scanners USB requièrent le chargement préalable d'un "firmware", cela est expliqué dans la page de manuel du "backend" utilisé. Vous devriez également consulter les pages de manuel de sane-find-scanner(1) et linprocfs(7).

Nous devons maintenant vérifier si le scanner sera identifié par un "frontend" de numérisation. Par défaut, les "backend"s SANE sont fournies avec un outil en ligne de commande appelé sane(1). Cette commande vous permet de lister les périphériques et d'effectuer une acquisition d'image à partir de la ligne de commande. L'option `-L` est employée pour afficher les scanners présents sur le système:

```
# scanimage -L
device `snapscan:/dev/pass3' is a AGFA SNAPSCAN 600 flatbed scanner
```

Aucun résultat, ou un message disant qu'aucun scanner n'a été identifié indiquent que sane(1) est incapable d'identifier le scanner. Si cela se produit, vous devrez éditer le fichier de configuration du "backend" du scanner et définir le type de scanner utilisé. Le répertoire /usr/local/etc/sane.d/ contient tous les fichiers de configurations des "backend"s. Ce problème d'identification apparaît essentiellement avec certains scanners USB.

Par exemple, avec le scanner USB utilisé dans la Interface USB, `sane-find-scanner` nous donne l'information suivante:

```
# sane-find-scanner -q
```

```
found USB scanner (UNKNOWN vendor and product) at device /dev/uscanner0
```

Le scanner est correctement détecté, il utilise l'interface USB et est attaché au fichier spécial de périphérique /dev/uscanner0. Nous pouvons maintenant vérifier si le scanner est correctement identifié:

```
# scanimage -L

No scanners were identified. If you were expecting something different,
check that the scanner is plugged in, turned on and detected by the
sane-find-scanner tool (if appropriate). Please read the documentation
which came with this software (README, FAQ, manpages).
```

Comme le scanner n'est pas identifié, nous devons éditer le fichier /usr/local/etc/sane.d/epson.conf. Le scanner utilisé était un EPSON Perfection® 1650, nous en déduisons donc que ce scanner utilisera le "backend" `epson`. Assurez-vous de bien lire les commentaires d'aide présents dans les fichiers de configuration des "backend"s. Les modifications à faire sont relativement simples: commentez toutes les lignes concernant une interface différente de celle utilisée par votre scanner (dans notre cas, nous commenterons toutes les lignes débutant par le mot `scsi` étant donné que notre scanner utilise une interface USB), ajoutez ensuite à la fin du fichier une ligne indiquant l'interface et le fichier spécial de périphérique utilisé. Dans ce cas, nous ajoutons la ligne suivante:

```
usb /dev/uscanner0
```

Veuillez vous assurer de bien lire les commentaires fournis dans les fichiers de configurations des "backend"s ainsi que les pages de manuel correspondantes pour plus de détails concernant la syntaxe correcte à utiliser. Nous pouvons maintenant vérifier si le scanner est identifié:

```
# scanimage -L
device `epson:/dev/uscanner0' is a Epson GT-8200 flatbed scanner
```

Notre scanner a été identifié. Ce n'est pas important si la marque et le modèle ne correspondent pas au scanner. L'important est le champ `epson:/dev/uscanner0'`, qui nous donne le "backend" et le fichier spécial de périphérique corrects.

Une fois que la commande `scanimage -L` est en mesure d'identifier le scanner, la configuration est terminée. Le périphérique est prêt à effectuer sa première numérisation.

Bien que sane(1) permette d'effectuer une numérisation à partir de la ligne de commande, il est préférable d'utiliser une interface graphique. SANE offre une interface graphique simple mais efficace: xscanimage (graphics/sane-frontends).

Xsane (graphics/xsane) est une autre interface graphique de numérisation assez populaire. Ce programme offre des fonctions avancées comme différents mode de numérisation (photocopie, fax, etc.), la correction des couleurs, la numérisation par lots, etc. Ces deux applications sont utilisables comme greffon pour GIMP.

7.6.4. Donner l'accès au scanner aux autres utilisateurs

Toutes les opérations précédentes ont été effectuées avec les privilèges `root`. Vous pourrez, cependant, avoir besoin que d'autres utilisateurs puissent accéder au scanner. L'utilisateur devra avoir les permissions de lecture et d'écriture sur le fichier spécial de périphérique /dev/uscanner0 dont le propriétaire est le groupe `operator`. L'ajout de l'utilisateur `joe` au groupe `operator` lui autorisera l'accès au scanner:

```
# pw groupmod operator -m joe
```

Pour plus de détails, consultez la page de manuel de pw(8). Vous devez également fixer les permissions d'écriture correctes (0660 or 0664) sur le fichier spécial de périphérique /dev/uscanner0, par défaut le groupe `operator` n'a qu'un accès en lecture. Cela se fait en ajoutant les lignes suivantes au fichier /etc/devfs.rules:

```
[system=5]
add path uscanner0 mode 660
```

Ajoutez ensuite ce qui suit au fichier /etc/rc.conf et redémarrez la machine:

```
devfs_system_ruleset="system"
```

Plus d'information concernant ces lignes peut être trouvée dans la page de manuel devfs(8).

Bien sûr, pour des raisons de sécurité, vous devriez réfléchir à deux fois avant d'ajouter un utilisateur à n'importe quel groupe, tout particulièrement au groupe `operator`.

Chapitre 8. Configurer le noyau de FreeBSD

8.1. Synopsis

Le noyau est le coeur du système d'exploitation FreeBSD. Il est responsable de la gestion de la mémoire, de la mise en application des contrôles de sécurité, du réseau, des accès disque, et bien plus. Bien que FreeBSD devienne de plus en plus configurable dynamiquement, il est toujours nécessaire occasionnellement de reconfigurer et recompiler votre noyau.

Après la lecture de ce chapitre, vous saurez:

- Pourquoi vous pourriez avoir besoin de compiler un noyau sur mesure.
- Comment écrire un fichier de configuration du noyau, ou modifier un fichier de configuration existant.
- Comment utiliser le fichier de configuration du noyau pour créer et recompiler un nouveau noyau.
- Comment installer un nouveau noyau.
- Que faire si quelque chose se passe mal.

Toutes les commandes listées dans les exemples de ce chapitre doivent être exécutées en tant que `root` afin de fonctionner.

8.2. Pourquoi compiler un noyau sur mesure?

Traditionnellement, FreeBSD a eu ce qui s'appelle un noyau "monolithique". Cela signifie que le noyau était un gros programme, supportant une liste figée de périphériques, et si vous vouliez modifier le comportement du noyau alors vous deviez compiler un nouveau noyau, et ensuite redémarrer votre ordinateur avec le nouveau noyau.

Aujourd'hui, FreeBSD s'oriente rapidement vers un modèle où une grande partie des fonctions du noyau est contenue dans des modules qui peuvent être dynamiquement chargés et déchargés si nécessaire. Cela permet au noyau de s'adapter au nouveau matériel devenant soudainement disponible (comme les cartes PCMCIA dans un ordinateur portable), ou pour qu'une nouvelle fonctionnalité qui n'était pas nécessaire lors de la compilation du noyau y soit intégrée. On appelle cela un noyau modulaire.

En dépit de cela, il est encore nécessaire d'effectuer certaines configurations de noyau en statique. Dans certains cas c'est parce que la fonctionnalité est si proche du noyau qu'elle ne peut être rendue dynamiquement chargeable. Dans d'autres cas, cela peut tout simplement venir du fait que personne n'a encore pris le temps d'écrire un module dynamiquement chargeable pour cette fonctionnalité.

Compiler un noyau sur mesure est l'un des plus importants rites de passage que doit endurer tout utilisateur BSD. Cette opération, tout en prenant du temps, apportera de nombreuses améliorations à votre système FreeBSD. A la différence du noyau GENERIC, qui doit supporter une large gamme de matériels, un noyau sur mesure ne contient que le support pour *votre* configuration matérielle.

Cela a de nombreux avantages, comme:

- Un temps de démarrage plus court. Comme le noyau ne recherchera que le matériel présent sur votre système, le temps nécessaire au démarrage de votre système peut diminuer de façon importante.
- Une utilisation plus faible de la mémoire. Un noyau sur mesure utilise souvent moins de mémoire que le noyau GENERIC, ce qui est important car le noyau doit toujours résider en mémoire. Pour cette raison, un noyau sur mesure est tout particulièrement utile sur un système dont les ressources mémoire sont limitées.
- Le support de matériels supplémentaires. Un noyau sur mesure vous permet d'intégrer le support pour des périphériques, qui ne sont pas présents dans le noyau GENERIC comme les cartes son.

8.3. Compiler et installer un noyau sur mesure

Commençons par passer rapidement en revue le répertoire de configuration du noyau. Tous les chemins d'accès mentionnés seront relatifs au répertoire principal /usr/src/sys, qui est également accessible via le lien symbolique /sys. Il comporte un certain nombre de sous-répertoires correspondants à différentes parties du noyau, mais les plus importantes, en ce qui nous concerne, sont arch/conf, où vous éditerez votre fichier configuration personnalisé, et compile, qui est l'espace de travail où votre noyau sera compilé. *arch* représente une des architectures suivante: i386, soit alpha, amd64, ia64, powerpc, sparc64, ou encore pc98 (une branche alternative de développement de l'architecture PC, populaire au Japon). Tout ce qui se trouve dans un répertoire particulier à une architecture est propre uniquement à cette architecture; le reste du code est un code indépendant du type de machine et commun à toutes les plates-formes sur lesquelles FreeBSD pourrait être potentiellement porté. Remarquez l'organisation logique de l'arborescence des répertoires, où chaque périphérique, système de fichiers, et option supportés a son propre sous-répertoire.

Les exemples de ce chapitre supposent que vous utilisez l'architecture i386. Si ce n'est pas votre cas, effectuez les ajustements appropriés au niveau des chemins d'accès pour votre architecture.

S'il n'y a *pas* de répertoire /usr/src/sys sur votre système, alors c'est que les sources du noyau n'ont pas été installées. La manière la plus facile de les installer est d'exécuter `sysinstall` en tant que `root`, et sélectionner Configure, puis Distributions, src, puis base et sys. Si vous avez une aversion envers sysinstall et que vous disposez d'un CDROM "officiel" de FreeBSD, alors vous pouvez installer les sources depuis la ligne de commande:

```
# mount /cdrom
# mkdir -p /usr/src/sys
# ln -s /usr/src/sys /sys
# cat /cdrom/src/ssys.[a-d]* | tar -xzvf -
# cat /cdrom/src/sbase.[a-d]* | tar -xzvf -
```

Ensuite allez dans le répertoire arch/conf et copiez le fichier de configuration GENERIC dans un

fichier qui portera le nom que vous voulez donner à votre noyau. Par exemple:

```
# cd /usr/src/sys/i386/conf
# cp GENERIC MONNOYAU
```

Par tradition, c'est un nom en majuscules, et si vous maintenez plusieurs machines FreeBSD avec des configurations matérielles différentes, c'est une bonne idée de lui donner le même nom que la machine. Nous l'appellerons MONNOYAU pour les besoins de cet exemple.

Conserver votre fichier de configuration du noyau directement sous /usr/src peut être une mauvaise idée. Si vous avez des problèmes il peut être tentant de juste effacer /usr/src et recommencer à nouveau. Après avoir fait cela ne prends que quelques secondes pour vous rendre compte que vous venez d'effacer votre fichier de configuration du noyau personnalisé. N'éditez pas, non plus, directement le fichier GENERIC, il peut être écrasé à la prochaine mise à jour de l'arborescence des sources, et vos modifications seraient perdues.

Vous voudrez peut être conserver votre fichier de configuration du noyau ailleurs et alors créer un lien symbolique vers le fichier dans le répertoire i386.

Par exemple:

```
# cd /usr/src/sys/i386/conf
# mkdir /root/noyaux
# cp GENERIC /root/noyaux/MONNOYAU
# ln -s /root/noyaux/MONNOYAU
```

Editez maintenant MONNOYAU avec votre éditeur de texte préféré. Si vous venez tout juste de finir l'installation, le seul éditeur disponible sera probablement vi, qui est trop complexe pour être décrit ici, mais est bien expliqué dans de nombreux ouvrages de la bibliographie. Cependant, FreeBSD offre un éditeur plus simple appelé ee qui, si vous êtes débutant, sera votre éditeur de choix. N'hésitez pas à modifier les commentaires d'entête pour y décrire votre configuration ou les modifications que vous avez apportés par rapport au noyau GENERIC.

Si vous avez déjà compilé un noyau sur SunOS™ ou tout autre système d'exploitation BSD, l'essentiel de fichier vous sera familier. Si vous venez d'un système d'exploitation comme DOS, à l'inverse, le fichier de configuration GENERIC vous paraîtra inintelligible, lisez alors lentement et attentivement la section sur le fichier de configuration.

Si vous synchronisez votre arborescence des sources avec les toutes dernières sources du projet FreeBSD, assurez-vous de toujours lire le fichier /usr/src/UPDATING avant d'effectuer une quelconque opération de mise à jour. Ce fichier décrit les problèmes importants ou les domaines demandant une attention particulière dans le code mis à jour. /usr/src/UPDATING correspond toujours à votre version des sources de FreeBSD, et est donc plus à jour que ce Manuel.

Vous devez maintenant compiler le code source du noyau.

Procedure: Compiler un noya

1. Passez dans le répertoire /usr/src.

```
# cd /usr/src
```

2. Compilez le noyau:

```
# make buildkernel KERNCONF=MONNOYAU
```

3. Installez le nouveau noyau:

```
# make installkernel KERNCONF=MONNOYAU
```

Il est indispensable d'avoir l'intégralité des sources du système FreeBSD pour compiler le noyau.

Par défaut, quand vous compilez un noyau personnalisé, *tous* les modules seront également recompilés. Si vous désirez mettre à jour un noyau plus rapidement ou compiler que certains modules, vous devez éditer le fichier /etc/make.conf avant de compiler le noyau:

```
MODULES_OVERRIDE = linux acpi sound/sound sound/driver/ds1 ntfs
```

Cette variable définit une liste de modules à compiler à la place de l'intégralité des modules.

```
WITHOUT_MODULES = linux acpi sound/sound sound/driver/ds1 ntfs
```

Cette variable définit une liste de modules à exclure du processus de compilation. Pour d'autres variables qui peuvent être intéressantes pour le processus de compilation du noyau, consultez la page de manuel make.conf(5).

Le nouveau noyau sera copié dans le répertoire /boot/kernel avec le nom /boot/kernel/kernel et l'ancien noyau sera renommé en /boot/kernel.old/kernel. Maintenant, arrêtez le système et redémarrez pour utiliser votre nouveau noyau. Si quelque chose se passe mal, il y a quelques instructions de dépannage à la fin de ce chapitre que vous pourrez trouver utiles. Assurez-vous de lire la section qui explique comment revenir en arrière dans le cas où votre nouveau noyau ne démarre pas.

Les autres fichiers concernant le processus de démarrage, comme le chargeur

(loader(8)) et la configuration du démarrage sont conservés dans le répertoire /boot. Les modules tiers et personnalisés peuvent être placés dans /boot/kernel, bien que les utilisateurs doivent être conscients que garder ses modules synchronisés avec le noyau compilé est très important. Les modules qui ne sont pas destinés à fonctionner avec le noyau compilé peuvent être instables et ne pas donner les résultats escomptés.

8.4. Le fichier de configuration

Le format général du fichier de configuration est assez simple. Chaque ligne est composée d'un mot-clé et d'un ou plusieurs arguments. Pour simplifier, la plupart des lignes ne contiennent qu'un seul argument. Tout ce qui suit le caractère # est considéré comme un commentaire et ignoré. Les sections suivantes décrivent chaque mot-clé, dans l'ordre où ils apparaissent dans le fichier GENERIC. Pour une liste exhaustive des options et périphériques dépendants de l'architecture utilisée, consultez le fichier NOTES présent dans le même répertoire que le fichier GENERIC. Pour les options ne dépendant pas de l'architecture, consultez le fichier /usr/src/sys/conf/NOTES.

Pour compiler un fichier contenant toutes les options possibles, en général pour effectuer des tests, exécutez la commande suivante en tant que root:

```
# cd /usr/src/sys/i386/conf  make LINT
```

Ce qui suit est un exemple de fichier de configuration du noyau GENERIC avec divers commentaires aux endroits nécessaires pour un peu plus de clarté. Cet exemple devrait correspondre de façon très proche à votre copie du fichier /usr/src/sys/i386/conf/GENERIC.

```
machine     i386
```

C'est l'architecture de la machine. Elle doit être alpha, amd64, i386, ia64, pc98, powerpc, ou encore sparc64.

```
cpu          I486_CPU
cpu          I586_CPU
cpu          I686_CPU
```

Ce qui précède définit le type de CPU présent dans votre système. Il peut y avoir plusieurs occurrences de la ligne CPU (si, par exemple, vous n'êtes pas sûr de devoir utiliser I586_CPU ou I686_CPU), cependant, pour un noyau personnalisé, il est mieux de spécifier uniquement le CPU que vous avez. Si vous n'êtes pas sûr du type, vous pouvez lister le fichier /var/run/dmesg.boot pour visualiser les messages de démarrage.

```
ident         GENERIC
```

C'est l'identification du noyau. Vous devriez changer cela pour le nom, quel qu'il soit, que vous donnez à votre noyau, par exemple `MONNOYAU` si vous avez suivi les instructions des exemples précédents. La valeur que vous donnez à la chaîne `ident` s'affichera au démarrage du noyau, il est donc utile de donner au nouveau noyau un nom différent si vous voulez le différencier de votre noyau habituel (e.g., vous voulez compiler un noyau expérimental).

```
#To statically compile in device wiring instead of /boot/device.hints
#hints          "GENERIC.hints"         #Default places to look for devices.
```

Le fichier device.hints(5) est utilisé pour configurer les paramètres des pilotes de périphériques. Le loader(8) recherchera le fichier /boot/device.hints au démarrage. En utilisant l'option `hints` vous pouvez compiler ces valeurs en statique dans votre noyau. Il n'est alors pas utile de créer de fichier device.hints dans /boot.

```
makeoptions     DEBUG=-g          #Build kernel with gdb(1) debug symbols
```

Le processus normal de compilation de FreeBSD inclut les informations de débogage lors de la compilation du noyau avec l'option `-g`, qui autorisera les informations de débogage quand le noyau sera passé à gcc(1).

```
options         SCHED_4BSD        # 4BSD scheduler
```

L'ordonnanceur ("scheduler") traditionnel et par défaut de FreeBSD. Conservez cette ligne.

```
options         PREEMPTION        # Enable kernel thread preemption
```

Permet aux processus légers présents dans le noyau d'être devancés par des processus de priorité plus élevée. Cela améliore l'interactivité et permet aux processus d'interruption d'être exécutés le plus tôt possible au lieu d'attendre leur tour.

```
options         INET          #InterNETworking
```

Support réseau. Conservez-le, même si vous n'envisagez pas de vous connecter à un réseau. La plupart des programmes utilisent le réseau "en boucle" (i.e., établissent des connexions réseau avec le PC lui-même), cette option est donc quasiment obligatoire.

```
options         INET6          #IPv6 communications protocols
```

Ceci active les protocoles de communication IPv6.

```
options         FFS          #Berkeley Fast Filesystem
```

C’est le système de fichiers de base sur disque dur. Gardez ces options si vous démarrez depuis le disque dur.

```
options         SOFTUPDATES  #Enable FFS Soft Updates support
```

Cette option rajoutera le support des "Soft Updates" dans le noyau, ce qui aidera l’accélération des accès en écriture sur les disques. Même quand cette fonction est fournit par le noyau, elle doit être activée sur chaque disque. Regardez le résultat de la commande mount(8) pour voir si les "Soft Updates" sont activées sur les disques de votre système. Si vous ne voyez pas apparaître l’option `soft-updates` alors vous devrez l’activer en utilisant les commandes tunefs(8) (pour les systèmes de fichiers existant) ou newfs(8) (pour les nouveaux systèmes de fichiers).

```
options         UFS_ACL      #Support for access control lists
```

Cette option active le support des listes de contrôle d’accès au système de fichiers (ACL). Elles reposent sur l’utilisation d’attributs étendus et d’UFS2, cette fonctionnalité est décrite dans la Listes de contrôle d’accès au système de fichiers. Les ACLs sont activées par défaut, et leur support ne devraient pas être retiré du noyau si elles ont été précédemment utilisées sur un système de fichiers, étant donné que cela supprimera les listes de contrôle d’accès changeant alors la façon dont sont protégés les fichiers d’une manière imprévisible.

```
options         UFS_DIRHASH  #Improve performance on big directories
```

Cette option inclut certaines fonctions pour accélérer les opérations disque sur de gros répertoires, aux dépens d’employer de la mémoire supplémentaire. Vous conserverez normalement cela pour un gros serveur, ou une station de travail très active, et vous l’enlèverez si vous utilisez FreeBSD sur un petit système où la mémoire prime et la vitesse d’accès disque est moins importante, comme pour un coupe-feu.

```
options         MD_ROOT      #MD is a potential root device
```

Cette option active le support pour des disques virtuels en mémoire utilisés comme périphérique racine.

```
options         NFSCLIENT         # Network Filesystem Client
options         NFSSERVER         # Network Filesystem Server
options         NFS_ROOT          # NFS usable as /, requires NFSCLIENT
```

Le système de fichiers réseau. A moins que vous n’envisagiez de monter des partitions d’un serveur de fichiers UNIX® par l’intermédiaire d’un réseau TCP/IP, vous pouvez mettre en commentaire ces options.

```
options         MSDOSFS      #MSDOS Filesystem
```

Le système de fichiers MS-DOS®. A moins que vous n'envisagiez de monter une partition DOS d'un disque dur au démarrage, vous pouvez sans risque commenter cette option. Le module sera automatiquement chargé la première fois que vous monterez une partition DOS, comme décrit plus haut. Par ailleurs, l'excellent logiciel emulators/mtools vous permet d'accéder à des disquettes DOS sans avoir besoin de les monter (et ne requiert pas non plus `MSDOSFS`).

```
options         CD9660       #ISO 9660 Filesystem
```

Le système de fichiers ISO 9660 pour les CDROMs. Commentez ces options si vous n'avez pas de lecteur de CDROM ou que vous ne montez qu'occasionnellement des CDROMs (il sera chargé dynamiquement dès que vous monterez un CDROM). Les CDROMs audios n'ont pas besoin de ce système de fichiers.

```
options         PROCFS           # Process filesystem (requires PSEUDOFS)
```

Le système de fichiers pour les processus. C'est un "pseudo-système" de fichiers monté sur /proc qui permet à des programmes comme ps(1) de vous fournir plus d'informations sur les processus qui tournent sur le système. L'utilisation de `PROCFS` n'est pas nécessaire la plupart du temps, comme la majeur partie des outils de débogage et de monitoring ont été adaptés pour s'exécuter sans `PROCFS`: les nouvelles installations ne monteront pas par défaut ce système de fichiers.

```
options         PSEUDOFS     #Pseudo-filesystem framework
```

Les noyaux 6.X faisant usage du système `PROCFS` doivent également inclure le support pour `PSEUDOFS`.

```
options         GEOM_GPT         # GUID Partition Tables.
```

Cette option apporte la possibilité d'avoir un grand nombre de partitions sur un seul disque.

```
options         COMPAT_43    #Compatible with BSD 4.3 [KEEP THIS!]
```

Compatibilité avec 4.3BSD. Conservez cette option; certains programmes auront un comportement bizarre si vous la commentez.

```
options         COMPAT_FREEBSD4     #Compatible with FreeBSD4
```

Cette option est nécessaires aux systèmes i386™ et Alpha fonctionnant sous FreeBSD 5.X pour supporter les applications compilées sur d'anciennes version de FreeBSD qui utilisent d'anciennes interfaces d'appel système. Il est recommandé d'utiliser cette option sur tous les systèmes i386™ et

Alpha susceptibles d'exécuter d'anciennes applications; les plateformes apparues sous FreeBSD 5.0, comme l'ia64 et sparc64, n'ont pas besoin de cette option.

```
options         COMPAT_FREEBSD5   # Compatible with FreeBSD5
```

Cette option est nécessaire sous FreeBSD 6.X et versions supérieures pour supporter les applications compilées sous FreeBSD 5.X et qui utilisent les interfaces d'appel système FreeBSD 5.X.

```
options         SCSI_DELAY=5000    #Delay (in ms) before probing SCSI
```

Cette option oblige le noyau à attendre 5 secondes avant de rechercher les périphériques SCSI présents sur votre système. Si vous n'avez que des disques IDE, vous pouvez l'ignorer, sinon vous pouvez essayer de diminuer cette valeur, pour accélérer le démarrage du système. Bien sûr, si vous le faites, et que FreeBSD a du mal à reconnaître vos périphériques SCSI, vous devrez l'augmenter à nouveau.

```
options         KTRACE             #ktrace(1) support
```

Ceci permet de tracer le processus du noyau, ce qui est utile pour le débogage.

```
options         SYSVSHM            #SYSV-style shared memory
```

Cette option implémente la mémoire partagée System V. L'usage le plus courant qui en est fait est l'extension XSHM d'X, dont de nombreux logiciels gourmants en graphique tireront automatiquement parti pour fonctionner plus vite. Si vous utilisez X, vous utiliserez absolument cette option.

```
options         SYSVMSG            #SYSV-style message queues
```

Support des messages System V. Cette option n'augmente que de quelques centaines d'octets la taille du noyau.

```
options         SYSVSEM            #SYSV-style semaphores
```

Support des sémaphores System V. D'un usage moins courant, mais n'augmente la taille du noyau que de quelques centaines d'octets.

L'option `-p` de la commande ipcs(1) donnera la liste des processus utilisant chacun de ces mécanismes System V.

```
options         _KPOSIX_PRIORITY_SCHEDULING # POSIX P1003_1B real-time extensions
```

Extensions temps-réel ajoutées dans la norme POSIX® 1993. Certaines applications du catalogue des logiciels portés les utilisent (comme StarOffice™).

```
options         KBD_INSTALL_CDEV  # install a CDEV entry in /dev
```

Cette option concerne le clavier. Elle installe une entrée CDEV dans le répertoire /dev.

```
options         ADAPTIVE_GIANT    # Giant mutex is adaptive.
```

"Giant" est le nom d'un mécanisme d'exclusion mutuelle (un "mutex" dormant) qui protège l'accès à un ensemble important de ressources du noyau. Aujourd'hui c'est un goulot d'étranglement des performances inacceptable que l'on est en train de remplacer activement par des verrous qui protègent les ressources individuelles. L'option `ADAPTIVE_GIANT` permet à Giant d'être inclus dans l'ensemble des mutex lancés de manière adaptative. C'est à dire, quand un thread désire verrouiller le mutex Giant, mais que ce dernier est déjà verrouillé par un thread sur un autre CPU, le premier thread continuera à fonctionner et attendra la libération du verrou. Normalement, le thread retournera à l'état dormant et attendra une nouvelle chance de pouvoir s'exécuter. Si vous n'êtes pas sûr, laissez la configuration en l'état.

```
device          apic              # I/O APIC
```

Le périphérique apic active l'utilisation de l'E/S APIC pour l'acheminement des interruptions. Le périphérique apic peut être utilisé dans les noyaux UP (monoprocesseur) et SMP, mais est requis pour les noyaux SMP. Ajoutez `options SMP` pour inclure le support pour plusieurs processeurs.

Le périphérique apic n'existe que sur l'architecture i386, cette ligne de configuration ne doit pas être utilisée sur d'autres architectures.

```
device          eisa
```

Rajoutez cela si vous avez une carte mère EISA. Cela permet l'auto-détection et la configuration de tous les périphériques présents sur le bus EISA.

```
device          pci
```

Ajoutez cette option si vous avez une carte mère PCI. Cela permet l'auto-détection des cartes PCI et gère l'interface entre les bus PCI et ISA.

```
# Floppy drives
device          fdc
```

C'est le contrôleur de lecteur de disquettes.

```
# ATA and ATAPI devices
device          ata
```

Ce pilote supporte tous les périphériques ATA et ATAPI. Vous n'avez besoin que d'une seule ligne `device ata` pour que le noyau détecte tous les périphériques PCI ATA/ATAPI sur les machines modernes.

```
device          atadisk                 # ATA disk drives
```

Ceci est requis avec `device ata` pour les disques ATA.

```
device          ataraid                 # ATA RAID drives
```

Ceci est nécessaire avec `device ata` pour les disques RAID ATA.

```
device          atapicd                 # ATAPI CDROM drives
```

Ceci est nécessaire avec `device ata` pour le support des lecteurs de CDROM ATAPI.

```
device          atapifd                 # ATAPI floppy drives
```

Ceci est nécessaire avec `device ata` pour le support des lecteurs de disquettes ATAPI.

```
device          atapist                 # ATAPI tape drives
```

Ceci est nécessaire avec `device ata` pour le support des lecteurs de bande ATAPI.

```
options         ATA_STATIC_ID           #Static device numbering
```

Cela rend la numérotation des périphériques statique, sans cela l'allocation des numéros de périphériques sera dynamique.

```
# SCSI Controllers
device          ahb         # EISA AHA1742 family
device          ahc         # AHA2940 and onboard AIC7xxx devices
options         AHC_REG_PRETTY_PRINT    # Print register bitfields in debug
                                        # output.  Adds ~128k to driver.
device          ahd         # AHA39320/29320 and onboard AIC79xx devices
options         AHD_REG_PRETTY_PRINT    # Print register bitfields in debug
                                        # output.  Adds ~215k to driver.
device          amd         # AMD 53C974 (Teckram DC-390(T))
device          isp         # Qlogic family
```

```
#device         ispfw      # Firmware for QLogic HBAs- normally a module
device          mpt        # LSI-Logic MPT-Fusion
#device         ncr        # NCR/Symbios Logic
device          sym        # NCR/Symbios Logic (newer chipsets + those of `ncr')
device          trm        # Tekram DC395U/UW/F DC315U adapters

device          adv        # Advansys SCSI adapters
device          adw        # Advansys wide SCSI adapters
device          aha        # Adaptec 154x SCSI adapters
device          aic        # Adaptec 15[012]x SCSI adapters, AIC-6[23]60.
device          bt         # Buslogic/Mylex MultiMaster SCSI adapters

device          ncv        # NCR 53C500
device          nsp        # Workbit Ninja SCSI-3
device          stg        # TMC 18C30/18C50
```

Contrôleurs SCSI. Mettez en commentaires ceux que vous n'avez pas sur votre système. Si vous n'avez qu'un système IDE, vous pouvez supprimer toutes ces lignes. Les lignes `*_REG_PRETTY_PRINT` sont des options de débogage pour leur pilote respectif.

```
# SCSI peripherals
device          scbus      # SCSI bus (required for SCSI)
device          ch         # SCSI media changers
device          da         # Direct Access (disks)
device          sa         # Sequential Access (tape etc)
device          cd         # CD
device          pass       # Passthrough device (direct SCSI access)
device          ses        # SCSI Environmental Services (and SAF-TE)
```

Périphériques SCSI. A nouveau, mettez en commentaires tous ceux que vous n'avez pas, ou si vous n'avez que du matériel IDE, vous pouvez tous les supprimer.

Le pilote USB umass(4) et quelques autres pilotes utilisent le sous-système SCSI même si ce ne sont pas de véritables périphériques SCSI. Par conséquent assurez-vous de ne pas retirer le support SCSI si un tel pilote fait partie de la configuration du noyau.

```
# RAID controllers interfaced to the SCSI subsystem
device          amr        # AMI MegaRAID
device          arcmsr     # Areca SATA II RAID
device          asr        # DPT SmartRAID V, VI and Adaptec SCSI RAID
device          ciss       # Compaq Smart RAID 5*
device          dpt        # DPT Smartcache III, IV - See NOTES for options
device          hptmv      # Highpoint RocketRAID 182x
device          rr232x     # Highpoint RocketRAID 232x
device          iir        # Intel Integrated RAID
device          ips        # IBM (Adaptec) ServeRAID
device          mly        # Mylex AcceleRAID/eXtremeRAID
```

```
device          twa         # 3ware 9000 series PATA/SATA RAID

# RAID controllers
device          aac         # Adaptec FSA RAID
device          aacp        # SCSI passthrough for aac (requires CAM)
device          ida         # Compaq Smart RAID
device          mfi         # LSI MegaRAID SAS
device          mlx         # Mylex DAC960 family
device          pst         # Promise Supertrak SX6000
device          twe         # 3ware ATA RAID
```

Contrôleurs RAID supportés. Si vous n'avez aucun de ces derniers dans votre système, vous pouvez les mettre en commentaires ou les supprimer.

```
# atkbdc0 controls both the keyboard and the PS/2 mouse
device          atkbdc      # AT keyboard controller
```

Le contrôleur du clavier (atkbdc) permet de gérer les E/S du clavier AT et des périphériques de pointage PS/2. Ce contrôleur est nécessaire au pilote de périphérique du clavier (atkbd) et celui des périphériques de pointage PS/2 (psm).

```
device          atkbd       # AT keyboard
```

Le pilote de périphérique atkbd, associé au contrôleur atkbdc, fournit un accès au clavier AT 84 touches ou au clavier AT étendu qui est connecté au contrôleur de clavier de la machine.

```
device          psm         # PS/2 mouse
```

Utilisez ce périphérique si votre souris se branche sur le port PS/2.

```
device          kbdmux         # keyboard multiplexer
```

Support de base pour le multiplexage de claviers. Si vous n'avez pas l'intention d'utiliser sur le système plus d'un clavier, vous pouvez supprimer cette ligne sans risque.

```
device          vga         # VGA video card driver
```

Pilote de la carte graphique.

```
device          splash      # Splash screen and screen saver support
```

Ecran/bannière de démarrage. Les économiseurs d'écran ont également besoin de ce pseudo-périphérique.

```
# syscons is the default console driver, resembling an SCO console
device          sc
```

`sc` est le pilote par défaut pour la console, qui ressemble à une console SCO. Comme la plupart des programmes en mode plein-écran accèdent à la console par l'intermédiaire d'une base de données de description des terminaux comme termcap, cela n'a guère d'importance que vous choisissiez ce pilote ou `vt`, le pilote compatible `VT220`. Quand vous ouvrez une session, positionnez votre variable d'environnement `TERM` à `scoansi` si vous avez des problèmes pour utiliser des programmes en mode plein-écran avec cette console.

```
# Enable this for the pcvt (VT220 compatible) console driver
#device          vt
#options         XSERVER          # support for X server on a vt console
#options         FAT_CURSOR       # start with block cursor
```

C'est le pilote de console compatible VT220, et, rétrospectivement, compatible VT100/102. Il fonctionne bien sur certains ordinateurs portables qui sont matériellement incompatibles avec le pilote `sc`. Comme précédemment, positionnez la variable d'environnement `TERM` lorsque que vous ouvrez une session, mais cette fois-ci à `vt100` ou `vt220`. Ce pilote peut aussi s'avérer utile quand vous vous connectez à un grand nombre de machines différentes par le réseau sur lesquelles les entrées pour le périphérique `sc` ne sont souvent pas définies dans leurs fichiers termcap ou terminfo - alors que le terminal `vt100` devrait être disponible sur pratiquement toutes les plates-formes.

```
device          agp
```

Ajoutez cette option si vous avez une carte AGP dans votre système. Cela activera le support AGP, et l'AGP GART pour les cartes qui ont cette fonction.

```
# Power management support (see NOTES for more options)
device          apm
```

"Advanced Power Management support" - gestion avancée de l'énergie. Utile pour les ordinateurs portables, ceci est cependant désactivé par défaut dans le noyau GENERIC sous FreeBSD 5.X et versions suivantes

```
# Add suspend/resume support for the i8254.
device          pmtimer
```

Pilote du périphérique de gestion du temps pour les événements de la gestion de l'énergie, comme l'APM ou l'ACPI.

```
# PCCARD (PCMCIA) support
# PCMCIA and cardbus bridge support
```

```
device          cbb             # cardbus (yenta) bridge
device          pccard          # PC Card (16-bit) bus
device          cardbus         # CardBus (32-bit) bus
```

Support PCMCIA. Vous en avez besoin si vous utilisez un ordinateur portable.

```
# Serial (COM) ports
device          sio             # 8250, 16[45]50 based serial ports
```

Cela représente les ports séries, appelés ports COM dans le monde MS-DOS®/Windows®.

Si vous avez un modem interne sur le port COM4 et un port série COM2, vous devrez changer l'IRQ du modem en 2 (pour d'obscures raisons techniques, IRQ 2 = IRQ 9) pour y accéder avec FreeBSD. Si vous avez une carte série multi-ports, consultez la page de manuel de sio(4) pour plus d'informations sur les bonnes valeurs à ajouter à votre fichier /boot/device.hints. Certaines cartes vidéo (notamment celle à base de circuits S3) utilisent des adresses d'E/S sous la forme `0x*2e8`, et comme de nombreuses cartes séries bon marché de décodent pas complètement l'espace d'adresse d'E/S 16 bits, il y a aura des conflits avec ces cartes, rendant le port COM4 pratiquement inutilisable.

Chaque port série doit avoir une IRQ unique (à moins que vous n'utilisiez une carte multi-ports qui autorise le partage d'interruption), donc les IRQs par défaut pour les ports COM3 et COM4 ne peuvent être utilisées.

```
# Parallel port
device          ppc
```

C'est l'interface parallèle du bus ISA.

```
device          ppbus       # Parallel port bus (required)
```

Fournit le support pour le bus du port parallèle.

```
device          lpt         # Printer
```

Support pour les imprimantes parallèles.

Les trois lignes précédentes sont nécessaires pour permettre le support des imprimantes parallèles.

```
device          plip        # TCP/IP over parallel
```

C’est le pilote pour l’interface réseau sur port parallèle.

```
device          ppi         # Parallel port interface device
```

Port d’E/S d’usage général ("geek port") + port d’E/S IEEE1284.

```
#device         vpo         # Requires scbus and da
```

Ceci est pour le lecteur Zip de Iomega. Les options `scbus` et `da` sont également requises. Les meilleures performances sont obtenues avec les ports configurés dans le mode EPP 1.9.

```
#device         puc
```

Décommentez ce périphérique si vous disposez d’une carte PCI série ou parallèle "idiote" qui est supportée par le pilote puc(4).

```
# PCI Ethernet NICs.
device          de          # DEC/Intel DC21x4x (Tulip)
device          em          # Intel PRO/1000 adapter Gigabit Ethernet Card
device          ixgb        # Intel PRO/10GbE Ethernet Card
device          txp         # 3Com 3cR990 (Typhoon)
device          vx          # 3Com 3c590, 3c595 (Vortex)
```

Divers pilotes de cartes réseaux PCI. Mettez en commentaires ou supprimer les lignes de celles qui ne sont pas présentes sur votre système.

```
# PCI Ethernet NICs that use the common MII bus controller code.
# NOTE: Be sure to keep the 'device miibus' line in order to use these NICs!
device          miibus      # MII bus support
```

Le support du bus MII est nécessaire pour certaines cartes Ethernet PCI 10/100, à savoir celles qui utilisent des interfaces compatibles MII ou implémentent une gestion de l’interface opérant comme le bus MII. Ajouter `device miibus` à la configuration du noyau intègre le support pour l’API miibus générique et tous les pilotes d’interfaces PHY, incluant un pilote générique pour les interfaces PHYs qui ne sont pas spécifiquements gérées par un pilote individuel.

```
device          bce         # Broadcom BCM5706/BCM5708 Gigabit Ethernet
device          bfe         # Broadcom BCM440x 10/100 Ethernet
device          bge         # Broadcom BCM570xx Gigabit Ethernet
device          dc          # DEC/Intel 21143 and various workalikes
device          fxp         # Intel EtherExpress PRO/100B (82557, 82558)
device          lge         # Level 1 LXT1001 gigabit ethernet
device          msk         # Marvell/SysKonnect Yukon II Gigabit Ethernet
device          nge         # NatSemi DP83820 gigabit ethernet
```

```
device          nve         # nVidia nForce MCP on-board Ethernet Networking
device          pcn         # AMD Am79C97x PCI 10/100 (precedence over 'lnc')
device          re          # RealTek 8139C+/8169/8169S/8110S
device          rl          # RealTek 8129/8139
device          sf          # Adaptec AIC-6915 (Starfire)
device          sis         # Silicon Integrated Systems SiS 900/SiS 7016
device          sk          # SysKonnect SK-984x  SK-982x gigabit Ethernet
device          ste         # Sundance ST201 (D-Link DFE-550TX)
device          stge        # Sundance/Tamarack TC9021 gigabit Ethernet
device          ti          # Alteon Networks Tigon I/II gigabit Ethernet
device          tl          # Texas Instruments ThunderLAN
device          tx          # SMC EtherPower II (83c170 EPIC)
device          vge         # VIA VT612x gigabit ethernet
device          vr          # VIA Rhine, Rhine II
device          wb          # Winbond W89C840F
device          xl          # 3Com 3c90x (Boomerang, Cyclone)
```

Pilotes qui utilisent le code du contrôleur du bus MII.

```
# ISA Ethernet NICs.  pccard NICs included.
device          cs          # Crystal Semiconductor CS89x0 NIC
# 'device ed' requires 'device miibus'
device          ed          # NE[12]000, SMC Ultra, 3c503, DS8390 cards
device          ex          # Intel EtherExpress Pro/10 and Pro/10+
device          ep          # Etherlink III based cards
device          fe          # Fujitsu MB8696x based cards
device          ie          # EtherExpress 8/16, 3C507, StarLAN 10 etc.
device          lnc         # NE2100, NE32-VL Lance Ethernet cards
device          sn          # SMC's 9000 series of Ethernet chips
device          xe          # Xircom pccard Ethernet

# ISA devices that use the old ISA shims
#device         le
```

Pilotes pour les cartes Ethernet ISA. Consultez le fichier /usr/src/sys/i386/conf/NOTES pour savoir quelles cartes sont supportées et par quel pilote.

```
# Wireless NIC cards
device          wlan            # 802.11 support
```

Support 802.11 générique. Cette ligne est nécessaire pour le réseau sans fil.

```
device          wlan_wep        # 802.11 WEP support
device          wlan_ccmp       # 802.11 CCMP support
device          wlan_tkip       # 802.11 TKIP support
```

Support pour le chiffrage pour les périphériques 802.11. Ces lignes sont nécessaires si vous avez

l'intention d'utiliser le chiffrage et les protocoles de sécurité 802.11i.

```
device          an         # Aironet 4500/4800 802.11 wireless NICs.
device          ath             # Atheros pci/cardbus NIC's
device          ath_hal         # Atheros HAL (Hardware Access Layer)
device          ath_rate_sample # SampleRate tx rate control for ath
device          awi        # BayStack 660 and others
device          ral        # Ralink Technology RT2500 wireless NICs.
device          wi         # WaveLAN/Intersil/Symbol 802.11 wireless NICs.
#device         wl         # Older non 802.11 Wavelan wireless NIC.
```

Support pour diverses cartes réseau sans fil.

```
# Pseudo devices
device   loop          # Network loopback
```

C'est l'interface générique en boucle de TCP/IP. Si vous employez telnet ou FTP sur `localhost` (aussi connu en tant qu'adresse `127.0.0.1`) la réponse vous parviendra via ce pseudo-périphérique. Ceci est *obligatoire*.

```
device   random        # Entropy device
```

Générateur de nombres aléatoire sécurisé pour les applications de chiffrement.

```
device   ether         # Ethernet support
```

`ether` ne sert que si vous avez une carte Ethernet. Cela intègre le code générique pour le protocole Ethernet.

```
device   sl            # Kernel SLIP
```

`sl` est le support pour le protocole SLIP. Il a été presque entièrement supplanté par le protocole PPP, plus facile à mettre en oeuvre, mieux adapté aux connexions par modem, et aussi plus puissant.

```
device   ppp           # Kernel PPP
```

C'est le support intégré au noyau du protocole PPP pour les connexions par modem. Il y a aussi une version de PPP sous forme de programme utilisateur qui utilise `tun` et offre plus de souplesse et de possibilités comme la connexion à la demande.

```
device   tun           # Packet tunnel.
```

Ceci est utilisé par le programme PPP en mode utilisateur. Voyez la section PPP de ce manuel pour plus d'informations.

```
device   pty           # Pseudo-ttys (telnet etc)
```

C'est un "pseudo-terminal" ou un port simulant une session. Il est utilisé par les sessions `telnet` et `rlogin` entrantes, par xterm, et d'autres applications comme Emacs.

```
device   md            # Memory disks
```

Pseudo-périphérique de disque mémoire.

```
device   gif     # IPv6 and IPv4 tunneling
```

Ceci implémente l'encapsulation du protocole IPv6 par dessus l'IPv4, l'IPv4 par dessus l'IPv6, l'encapsulation IPv4 par dessus l'IPv4, et IPv6 par dessus IPv6. Le périphérique `gif`"s'auto-duplique", et créera les fichiers spéciaux de périphérique en fonction des besoins.

```
device   faith   # IPv6-to-IPv4 relaying (translation)
```

Ce pseudo-périphérique capture les paquets qui lui sont envoyés et les détourne vers le "daemon" de translation IPv4/IPv6.

```
# The `bpf' device enables the Berkeley Packet Filter.
# Be aware of the administrative consequences of enabling this!
# Note that 'bpf' is required for DHCP.
device   bpf           # Berkeley packet filter
```

C'est le filtre de paquets de Berkeley. Ce pseudo-périphérique permet de placer les interfaces en mode "promiscuous" (indiscret), pour capturer chaque paquet sur réseau de diffusion (e.g., un réseau Ethernet). Ces paquets peuvent être enregistrés sur le disque et/ou examinés avec le programme tcpdump(1).

Le périphérique bpf(4) est également utilisé par dhclient(8) pour obtenir une adresse IP du routeur par défaut (passerelle) et ainsi de suite. Si vous utilisez DHCP, conservez cette ligne non commentée.

```
# USB support
device          uhci          # UHCI PCI-USB interface
device          ohci          # OHCI PCI-USB interface
device          ehci          # EHCI PCI-USB interface (USB 2.0)
device          usb           # USB Bus (required)
#device         udbp          # USB Double Bulk Pipe devices
```

```
device          ugen          # Generic
device          uhid          # Human Interface Devices
device          ukbd          # Keyboard
device          ulpt          # Printer
device          umass         # Disks/Mass storage - Requires scbus and da
device          ums           # Mouse
device          ural          # Ralink Technology RT2500USB wireless NICs
device          urio          # Diamond Rio 500 MP3 player
device          uscanner      # Scanners
# USB Ethernet, requires mii
device          aue           # ADMtek USB Ethernet
device          axe           # ASIX Electronics USB Ethernet
device          cdce          # Generic USB over Ethernet
device          cue           # CATC USB Ethernet
device          kue           # Kawasaki LSI USB Ethernet
device          rue           # RealTek RTL8150 USB Ethernet
```

Support pour divers périphériques USB.

```
# FireWire support
device          firewire      # FireWire bus code
device          sbp           # SCSI over FireWire (Requires scbus and da)
device          fwe           # Ethernet over FireWire (non-standard!)
```

Support pour divers périphériques Firewire.

Pour plus d'informations et pour avoir la liste de périphériques supplémentaires supportés par FreeBSD, voyez le fichier /usr/src/sys/i386/conf/NOTES.

8.4.1. Configurations mémoire importantes (PAE)

Les machines à configuration mémoire importante ont besoin de pouvoir accéder à plus d'espace mémoire utilisateur et noyau que la limite des 4 gigaoctets de l'espace d'adresse noyau+utilisateur ("Kernel Virtual Address"-KVA). En raison de cette limite, Intel a ajouté le support d'adresses physiques sur 36 bits pour l'espace d'adresses dans les familles de microprocesseurs Pentium® Pro et suivantes.

L'extension de l'adressage physique-,"Physical Address Extension" (PAE) est une caractéristique des microprocesseurs Intel® Pentium® Pro et suivants autorisant les configurations mémoires jusqu'à 64 gigaoctets. FreeBSD fournit un support pour cette caratéristique via l'option de configuration du noyau PAE, disponible sous toutes les versions actuelles de FreeBSD. En raison des limitations de l'architecture mémoire Intel®, aucune distinction n'est faite entre la mémoire au-dessus et en-dessous de 4 gigaoctets. La mémoire allouée au-dessus de 4 gigaoctets est simplement ajoutée à l'ensemble de la mémoire disponible.

Pour activer le support PAE dans le noyau, ajoutez simplement la ligne suivante dans votre fichier de configuration du noyau:

```
options     PAE
```

Le support PAE sous FreeBSD est uniquement disponible pour les processeurs IA-32 d'Intel®. Il doit être noté que le support PAE sous FreeBSD n'a pas été énormément testé, et devrait être considéré comme bêta comparé aux autres fonctionnalités stables de FreeBSD.

Le support PAE sous FreeBSD a quelques limitations:

- Un processus est incapable d'accéder à plus de 4 gigaoctets d'espace mémoire.
- Les modules KLD ne peuvent être chargés dans un noyau avec PAE activé, en raison des différences entre la structure d'un module et du noyau.
- Les pilotes de périphériques qui n'utilisent pas l'interface bus_dma(9) seront à l'origine de corruption de données avec un noyau PAE et ne sont pas recommandés. Pour cette raison, le fichier de configuration du noyau avec support PAE qui est fourni avec FreeBSD exclut tous les pilotes connus pour ne pas fonctionner avec un noyau avec support PAE.
- Certains paramètres modifiables du système déterminent l'utilisation des ressources mémoire par la quantité de la mémoire physique disponible. De tels paramètres peuvent être inutilement sur-alloués en raison de la grande quantité de mémoire d'un système PAE. Un bon exemple est le "sysctl" `kern.maxvnodes`, qui contrôle le nombre maximal de "vnodes" alloués par le noyau. Il est recommandé d'ajuster ce dernier et les autres paramètres du même genre à des valeurs raisonnables.
- Il pourra être nécessaire d'augmenter l'espace d'adressage virtuel du noyau ("kernel virtual address"-KVA) ou de réduire le montant de la ressource spécifique du noyau qui est fortement utilisée (voir plus haut) afin d'éviter l'épuisement de l'espace KVA. L'option du noyau `KVA_PAGES` peut être employée pour augmenter l'espace KVA.

Pour des considérations de performance et de stabilité, il est recommandé de consulter la page de manuel tuning(7). La page de manuel pae(4) contient des informations à jour sur le support PAE sous FreeBSD.

8.5. Si quelque chose se passe mal

Il y a cinq types de problèmes qui peuvent survenir lors de la compilation d'un noyau sur mesure. Ce sont:

La commande `config` échoue

Si la commande config(8) échoue quand vous lui passez en paramètre la description de votre noyau, vous avez probablement fait une simple erreur quelque part. Heureusement config(8) affichera le numéro de la ligne qui lui a posé problème, vous pouvez donc localiser rapidement la ligne contenant l'erreur. Par exemple, si vous avez:

```
config: line 17: syntax error
```

Vérifiez que la ligne est correctement écrite, en le comparant avec le noyau GENERIC ou une autre référence.

La commande `make` échoue

Si la commande `make` échoue, cela signale habituellement une erreur dans la description de votre noyau, mais qui n'est pas suffisamment sérieuse pour que la commande config(8) la détecte. A nouveau, vérifiez votre fichier de configuration, et si vous n'arrivez toujours pas à résoudre le problème, envoyez un courrier électronique à la liste de diffusion pour les questions d'ordre général à propos de FreeBSD en joignant votre fichier de configuration du noyau, le diagnostic devrait être rapide.

Le noyau ne démarre pas:

Si votre nouveau noyau ne démarre pas, ou ne reconnaît pas vos périphériques, ne paniquez pas! Heureusement, FreeBSD dispose d'un excellent mécanisme pour récupérer si le noyau ne fonctionne pas. Sélectionnez simplement le noyau, à partir duquel vous désirez démarrer, à l'invite du chargeur de FreeBSD. Vous pouvez y accéder quand le menu de démarrage apparaît. Sélectionner l'option 6, "Escape to a loader prompt". A l'invite, tapez `unload kernel` et ensuite `boot /boot/kernel.old/kernel`, ou le nom de fichier d'un autre noyau qui pourra démarrer proprement. Quand on reconfigure un noyau, il est toujours bon de conserver à portée de la main un noyau dont on sait qu'il fonctionne.

Après avoir démarré avec un noyau en état de marche, vous pouvez revérifier votre fichier de configuration et essayer de recompiler à nouveau votre noyau. Une ressource utile est le fichier /var/log/messages qui enregistre, entre autres, tous les messages du noyau à chaque démarrage réussi. En outre, la commande dmesg(8) affichera les messages du noyau pour le dernier démarrage.

Si vous avez des difficultés à compiler un noyau, veillez à conserver un noyau GENERIC, ou un autre noyau dont vous savez qu'il fonctionne, sous la main, avec un nom différent de sorte qu'il ne soit pas écrasé à la prochaine compilation. Vous ne pouvez pas faire confiance au noyau kernel.old parce qu'en installant un nouveau noyau, kernel.old est remplacé par le dernier noyau installé dont il n'est pas certain qu'il soit opérationnel. Aussi, dès que possible, déplacez le noyau opérationnel vers le bon emplacement /boot/kernel où des commandes comme ps(1) pourront ne pas fonctionner correctement. Pour cela, renommez le répertoire contenant le bon noyau:

```
# mv /boot/kernel /boot/kernel.bad
# mv /boot/kernel.good /boot/kernel
```

Le noyau est opérationnel, mais la commande `ps` ne fonctionne plus du tout

Si vous avez installé une version du noyau différente de celle avec laquelle ont été compilés les utilitaires système, par exemple, un noyau -CURRENT sur un système -RELEASE, de nombreuses commandes d'affichage de l'état du système comme ps(1) and vmstat(8) ne fonctionneront plus. Vous devrez recompiler et installer un système avec la même version de l'arborescence des sources de celle utilisée pour votre noyau. C'est une des raisons pour lesquelles il n'est pas judicieux d'utiliser des versions différentes du noyau et du reste du système d'exploitation.

Chapitre 9. Imprimer

9.1. Synopsis

FreeBSD peut être utilisé pour imprimer sur une grande variété d'imprimantes, depuis la plus ancienne des imprimantes matricielles jusqu'aux toutes dernières imprimantes laser, en passant par tout ce qui peut exister entre les deux, et vous permet d'obtenir des impressions de haute qualité avec les programmes que vous exécutez.

Il est également possible de configurer FreeBSD pour qu'il fasse office de serveur d'impression sur un réseau; de cette manière FreeBSD peut recevoir des travaux d'impression ("jobs") en provenance de différents ordinateurs, comprenant d'autres machines sous FreeBSD et des machines sous Windows® ou Mac OS®. FreeBSD veillera à ce qu'un seul travail d'impression ne soit imprimé à la fois, et pourra tenir des statistiques sur les utilisateurs et les machines lançant le plus d'impressions, produire des pages d'"en-têtes" pour distinguer les impressions de chacun, et plus encore.

Après la lecture de ce chapitre, vous saurez:

- Comment configurer le gestionnaire d'impression de FreeBSD
- Comment installer des filtres d'impression, pour gérer des travaux d'impression particuliers de manière différente, ce qui inclut la transformation de documents entrants en un format que vos imprimantes comprennent.
- Comment inclure des en-têtes ou des pages bannière dans vos impressions.
- Comment imprimer en utilisant des imprimantes connectées à d'autres ordinateurs.
- Comment imprimer en utilisant des imprimantes connectées directement au réseau.
- Comment gérer des restrictions d'impression, notamment comment limiter la taille des travaux d'impression, et empêcher certains utilisateurs d'imprimer.
- Comment tenir des statistiques d'impression, et rendre compte de l'utilisation de l'imprimante.
- Comment résoudre les problèmes d'impression.

Avant de lire ce chapitre, vous devriez:

- Savoir comment configurer et installer un nouveau noyau (Configurer le noyau de FreeBSD).

9.2. Introduction

Afin d'utiliser des imprimantes avec FreeBSD, vous avez la possibilité de les paramétrer pour qu'elles utilisent le gestionnaire d'impression de Berkeley, également connu sous le nom de gestionnaire d'impression LPD, ou tout simplement LPD. C'est le système contrôle d'imprimante par défaut de FreeBSD. Ce chapitre présente LPD et vous assistera tout au long de sa configuration.

Si vous connaissez déjà LPD ou un autre système de gestion des impressions, vous pouvez directement vous rendre à la section Paramétrage de base.

LPD contrôle tout ce qui relève des imprimantes. Il est responsable de plusieurs tâches:

- Il contrôle l'accès aux imprimantes directement connectées au système ainsi qu'à celles connectées à d'autres machines via le réseau.
- Il permet aux utilisateurs de soumettre des fichiers à imprimer; ces requêtes sont connues sous le nom de *travaux*.
- Il empêche l'accès simultané de plusieurs utilisateurs à une même imprimante, en gérant une *queue* pour chaque imprimante.
- Il peut produire des *pages d'en-tête* (également connues sous le nom de *pages bannières* ou encore *cartouches*) afin que les utilisateurs puissent facilement retrouver dans une pile d'impressions celles correspondant aux travaux qu'ils ont soumis.
- Il s'occupe de paramétrer les communications lorsque les imprimantes sont connectées via un port série.
- Il peut transmettre des travaux par réseau à un gestionnaire d'impression LPD situé sur une autre machine.
- Il peut appliquer des filtres spéciaux afin d'assurer le formatage des travaux en fonction des différents langages et caractéristiques des imprimantes.
- Il peut comptabiliser l'utilisation de l'imprimante.

Vous pouvez, au travers d'un fichier de configuration (/etc/printcap) et en fournissant les programmes de filtres spéciaux, faire exécuter par LPD tout ou partie des tâches mentionnées ci-dessus sur une grande variété de modèles d'imprimantes.

9.2.1. Pourquoi vous devriez utiliser le gestionnaire d'impression

Si vous êtes l'unique utilisateur de votre système, vous vous demandez sans doute pourquoi il vous faudrait vous préoccuper du gestionnaire d'impression, alors que vous n'avez pas besoin de contrôle d'accès, de pages d'en-tête ni de statistiques relatives à l'utilisation de l'imprimante. Quand bien même il est possible de mettre en oeuvre l'accès direct à l'imprimante, vous devriez tout de même utiliser le gestionnaire d'impression, parce que:

- LPD imprime les travaux en tâche de fond: vous n'êtes pas obligé d'attendre que les données soient passées à l'imprimante.
- LPD peut commodément se charger d'appliquer des filtres à un travail pour adjoindre une en-tête contenant la date et l'heure, ou convertir un fichier au format particulier (comme un fichier DVI TeX) en un format que l'imprimante comprenne. Ainsi, vous n'aurez pas à vous charger de ces manipulations à la main.
- Beaucoup d'applications, tant libres que commerciales, fournissant une fonctionnalité d'impression s'attendent généralement à traiter avec le gestionnaire d'impression. En le mettant en oeuvre, vous vous faciliterez le support des autres applications que vous pourriez ajouter plus tard, ou que vous avez déjà installées.

9.3. Configuration de base

Pour utiliser des imprimantes avec le gestionnaire d'impression, il vous faudra configurer à la fois la partie matérielle (c'est à dire les imprimantes) et la partie logicielle (c'est à dire LPD). Ce document présente deux niveaux de configuration:

- La section Configuration simple de l'imprimante vous apprendra à connecter une imprimante, à renseigner LPD sur la façon dont il doit communiquer avec elle, et à imprimer de simples fichiers textes.
- La section Configuration avancée de l'imprimante vous apprendra à imprimer différents formats de fichiers, des pages d'en-tête, par l'intermédiaire d'un réseau, à contrôler l'accès aux imprimantes, et comptabiliser leur utilisation.

9.3.1. Configuration simple de l'imprimante

Cette section vous apprendra à configurer l'imprimante et LPD. Elle présente les bases:

- La section Configuration matérielle donne des indications sur la façon de connecter l'imprimante à l'un des ports de votre ordinateur.
- La section Configuration logicielle montre comment renseigner le fichier de configuration du gestionnaire d'impression LPD (/etc/printcap).

Si vous mettez en oeuvre une imprimante réceptionnant les données à imprimer via un protocole réseau plutôt que par les interfaces locales de l'ordinateur, lisez la section Imprimantes avec des interfaces utilisant des flux réseau.

Bien que cette section soit intitulée "Configuration simple de l'imprimante", elle s'avère en réalité plutôt complexe. La partie la plus difficile consiste à faire fonctionner l'imprimante avec votre ordinateur et LPD. Les options avancées telles les pages d'en-tête ou les statistiques sont relativement faciles à mettre en oeuvre une fois que l'imprimante fonctionne.

9.3.1.1. Configuration matérielle

Cette section détaille les différentes manières de connecter une imprimante à votre PC. Elle discute les types de ports et de câbles, et de la configuration noyau dont vous pourriez avoir besoin afin que FreeBSD puisse communiquer avec l'imprimante.

Si vous avez déjà connecté votre imprimante et réussi à imprimer sous un autre système d'exploitation, vous pouvez probablement passer à la section Configuration logicielle.

9.3.1.1.1. Les ports et les câbles

Les imprimantes pour PC vendues aujourd'hui sont en général pourvues d'une ou plusieurs des trois interfaces suivantes:

- Les interfaces *série*, également connues sous les noms RS-232 ou ports COM, utilisent un port série sur votre ordinateur pour envoyer des données à l'imprimante. Les interfaces série sont courantes, dans l'industrie informatique, et les câbles sont à la fois disponibles et faciles à réaliser. Elles réclament parfois des câbles spéciaux et peuvent nécessiter le paramétrage

d'options de communication assez complexes. La plupart des ports série PC ont une vitesse de transmission maximale de 115200 bps, ce qui rend l'impression de travaux comportant beaucoup de graphismes malaisée.

- Les interfaces *parallèles* utilisent un port parallèle sur votre ordinateur pour envoyer des données à l'imprimante. Les interfaces parallèles sont courantes dans l'industrie informatique et plus rapides que les interfaces série RS-232. Les câbles sont disponibles mais sont moins faciles à fabriquer à la main. En général, il n'y a aucune option de communication à paramétrer avec ces interfaces, ce qui rend leur configuration particulièrement simple.

  Les interfaces parallèles sont parfois appelées "Centronics", nom tiré du type de connecteur de l'imprimante

- Les interfaces USB, tenant leur nom de "Universal Serial Bus", ou "Bus Série Universel", s'avèrent plus véloces encore que les interfaces parallèles ou série RS-232. Les câbles sont simples et peu onéreux. L'USB surpasse les interfaces série RS-232 et parallèles pour l'impression, mais son support par les systèmes UNIX® n'est pas aussi bon. Une façon d'éviter ce problème est d'acheter une imprimante qui dispose à la fois d'une interface USB et d'une interface parallèle, comme beaucoup de modèles.

En règle générale, les interfaces parallèles n'offrent qu'une communication unidirectionnelle (de l'ordinateur vers l'imprimante) alors que les interfaces série et USB permettent un échange bidirectionnel. Les imprimantes et ports parallèles plus récents (EPP et ECP) peuvent communiquer dans les deux sens sous FreeBSD lorsque l'on a recourt à un câble conforme à la norme IEEE-1284.

La communication bidirectionnelle avec l'imprimante en utilisant un port parallèle se fait en général de l'une des deux manières suivantes. La première utilise un pilote d'imprimante compilé pour FreeBSD comprenant le langage propriétaire de l'imprimante. C'est couramment le cas des imprimantes jet d'encre et cela peut être utilisé pour retourner les niveaux d'encre et autres informations d'état. La seconde méthode est employée lorsque l'imprimante supporte PostScript®.

Les travaux PostScript® sont en fait des programmes envoyés à l'imprimante. Ils ne génèrent pas nécessairement de sortie papier et peuvent retourner leurs résultats directement à l'ordinateur. PostScript® utilise aussi la communication bidirectionnelle pour avertir l'ordinateur de problèmes, comme des erreurs dans le programme PostScript® ou des bourrages papier. Vos utilisateurs apprécieraient certainement de telles informations. De surcroît, la meilleure façon de tenir des statistiques sérieusement avec une imprimante PostScript® nécessite la communication bidirectionnelle: on demande à l'imprimante quel est son compteur de pages (combien en a-t-elle imprimées depuis sa fabrication), puis on lui envoie le travail de l'utilisateur, enfin on lui redemande son compteur de pages. La différence entre les deux valeurs donne la consommation de papier que vous pouvez attribuer à cet utilisateur.

9.3.1.1.2. Les ports parallèles

Pour raccorder une imprimante utilisant une interface parallèle, branchez le câble Centronics sur l'imprimante et sur l'ordinateur. Les instructions accompagnant l'imprimante, l'ordinateur, ou les deux, devraient parfaitement vous renseigner.

Souvenez-vous du port parallèle que vous avez utilisé sur l'ordinateur. Pour FreeBSD, le premier se nomme ppc0; le deuxième, ppc1, et ainsi de suite. Le nom du fichier spécial de périphérique de

l'imprimante suit les mêmes règles: /dev/lpt0 pour celle connectée sur le premier port parallèle, etc.

9.3.1.1.3. Les ports série

Pour raccorder une imprimante utilisant une interface série, branchez le câble série adéquat sur l'imprimante et sur l'ordinateur. Les instructions accompagnant l'imprimante, l'ordinateur, ou les deux, devraient parfaitement vous renseigner.

Si vous n'êtes pas sûr de savoir quel est le bon câble, voici ce que vous pouvez essayer:

- Un câble *modem* relie chacune des broches du connecteur depuis l'une des extrémités du câble directement à la broche lui correspondant dans le connecteur de l'autre extrémité. Ce type de câble est également connu sous le nom de câble "DTE-to-DCE".
- Un câble *null-modem* relie certaines des broches directement, en intervertit d'autres (par exemple, "émission de données" et "réception de données"), et en court-circuite d'autres en interne sur chacun des sertissages des connecteurs. Ce type de câble est également connu sous le nom de câble "DTE-to-DTE".
- Un câble *série pour imprimante*, requis par certaines imprimantes peu conventionnelles, ressemble au câble null-modem, à ceci près qu'il envoie certains signaux à l'autre extrémité au lieu de les court-circuiter en interne.

Vous devriez également définir les paramètres de communication pour l'imprimante, d'ordinaire en utilisant les contrôles sur la face avant ou les commutateurs sur l'imprimante. Choisissez la valeur la plus élevée de `bps` (bits par seconde, encore appelés "vitesse de transmission") autorisée conjointement par votre ordinateur et votre imprimante. Choisissez 7 ou 8 bits de données; aucun contrôle de parité ou un bit de parité paire ou impaire; et 1 ou 2 bits d'arrêt. Choisissez également un protocole de contrôle de flux: soit aucun, soit XON/XOFF (également appelé "in-band", ou encore "contrôle logiciel"). Retenez ces paramètres pour la configuration logicielle, dans la section qui suit.

9.3.1.2. Configuration logicielle

Cette section détaille la configuration logicielle nécessaire pour imprimer sous FreeBSD avec le gestionnaire d'impression LPD.

Voici un aperçu des étapes à suivre:

1. Configurez le noyau, si nécessaire, pour utiliser le port sur lequel vous raccorderez votre imprimante; la section Configurer le noyau de FreeBSD vous donnera la marche à suivre.
2. Paramétrez le mode de communication du port parallèle si vous utilisez une imprimante de ce type; la section Paramétrer le mode de communication du port parallèle vous donnera les détails.
3. Configurez LPD pour qu'il communique avec l'imprimante en renseignant le fichier /etc/printcap. Vous apprendrez comment faire un peu plus loin dans ce chapitre.

9.3.1.2.1. Configuration du noyau

Le noyau du système d'exploitation est compilé avec le support d'un certain ensemble de

périphériques. Les interfaces série ou parallèle de votre imprimante en font partie. De ce fait, vous pourriez avoir à ajouter le support d'un port série ou parallèle supplémentaire si votre noyau n'a pas déjà été configuré en ce sens.

Pour savoir si le support d'une interface série est activé dans le noyau que vous êtes en train d'utiliser, entrez:

```
# # grep sioN /var/run/dmesg.boot
```

Où *N* représente le numéro du port série, en commençant à zéro. Si vous obtenez un affichage similaire à:

```
sio2 at port 0x3e8-0x3ef irq 5 on isa sio2: type 16550A
```

alors le port est activé dans le noyau.

Pour savoir si le noyau supporte une interface parallèle, entrez:

```
# grep ppcN /var/run/dmesg.boot
```

Où *N* représente le numéro du port parallèle, en commençant à zéro. Si vous obtenez un affichage similaire à:

```
ppc0: <Parallel port> at port 0x378-0x37f irq 7 on isa0
ppc0: SMC-like chipset (ECP/EPP/PS2/NIBBLE) in COMPATIBLE mode
ppc0: FIFO with 16/16/8 bytes threshold
```

alors le port est activé dans le noyau.

Il se pourrait que vous ayez à reconfigurer le noyau afin que le système détecte et puisse utiliser un port parallèle ou série auquel vous avez connecté votre imprimante.

Pour ajouter le support d'un port série, voyez la section sur la configuration du noyau. Pour ajouter le support du port parallèle, voyez cette même section *et* celle qui suit.

9.3.1.3. Paramétrer le mode de communication du port parallèle

Lorsque vous utilisez l'interface parallèle, vous avez le choix entre deux modes de communication avec l'imprimante: par interruption, ou par polling (interrogation régulière ou scrutation). Le pilote d'imprimante générique (lpt(4)) de FreeBSD utilise le système ppbus(4), qui contrôle le chipset du port via le pilote ppc(4).

- Le mode par *interruption* est le mode par défaut avec un noyau GENERIC. De cette manière, le système d'exploitation utilise une ligne d'interruption (IRQ) pour déterminer si l'imprimante est prête à recevoir des données.

- Le mode *par scrutation* enjoint au système d'exploitation d'interroger à intervalles réguliers l'imprimante pour savoir si elle est prête à recevoir d'autres données. Lorsqu'elle répond par l'affirmative, le noyau lui en envoie plus.

Le mode par interruption est en général nettement plus rapide, mais consomme une précieuse ligne d'interruption (IRQ). On rapporte que certaines imprimantes HP récentes ne fonctionneraient pas correctement en mode par interruption, apparemment à cause d'un problème (pas encore très bien identifié) d'horloge. Ces imprimantes nécessitent le recours au mode par scrutation. Utilisez celui des deux qui fonctionne. Certaines imprimantes fonctionnent dans les deux modes, mais s'avèrent désagréablement lentes en mode par interruption.

Vous pouvez choisir le mode de communication de deux manières différentes: en configurant le noyau ou en utilisant le programme lptcontrol(8).

Pour paramétrer le mode de communication en configurant le noyau:

1. Editez le fichier de configuration de votre noyau. Cherchez une entrée `ppc0`. Si vous voulez configurer le deuxième port parallèle, cherchez plutôt `ppc1`. Ou `ppc2` pour le troisième, et ainsi de suite.
   - Si vous souhaitez activer le mode par interruption, éditez la ligne suivante:

     ```
     hint.ppc.0.irq="N"
     ```

     dans le fichier /boot/device.hints et remplacez *N* par le numéro d'IRQ approprié. Le fichier de configuration du noyau doit également comporter le pilote ppc(4):

     ```
     device ppc
     ```

   - Si vous souhaitez activer le mode par scrutation, ôtez la ligne suivante de votre fichier /boot/device.hints:

     ```
     hint.ppc.0.irq="N"
     ```

     Dans certains cas, positionner le port en mode scrutation sous FreeBSD n'est pas suffisant. La plupart du temps cela vient du pilote acpi(4), ce dernier étant capable de sonder et d'attacher des périphériques, et donc de contrôler le mode d'accès au port de l'imprimante. Vous devrez donc vérifier votre configuration acpi(4) pour résoudre ce problème.
2. Sauvegardez le fichier, puis configurez, compilez, et installez le noyau avant de redémarrer. Consultez la section configuration du noyau pour plus de détails.

Pour paramétrer le mode de communication avec lptcontrol(8):

1. Entrez:

   ```
   # lptcontrol -i -d /dev/lptN
   ```

   pour sélectionner le mode par interruption pour `lptN`.

2. Entrez:

   ```
   # lptcontrol -p -d /dev/lptN
   ```

   pour sélectionner le mode par scrutation pour `lptN`.

Vous pouvez placer ces commandes dans votre fichier /etc/rc.local pour sélectionner le mode à chaque démarrage du système. Consultez lptcontrol(8) pour obtenir plus d'informations.

9.3.1.4. Vérifier la communication avec l'imprimante

Avant de passer à la configuration du gestionnaire d'impression, vous devriez vous assurer que le système d'exploitation fait parvenir avec succès des données à l'imprimante. Il est beaucoup plus facile de déboguer séparément la communication avec l'imprimante et la configuration du gestionnaire d'impression.

Pour tester l'imprimante, nous allons lui envoyer du texte. Pour les imprimantes qui peuvent immédiatement imprimer les caractères qui leur sont envoyés, le programme lptest(1) est parfait: il génère les 96 caractères ASCII imprimables sur 96 lignes.

Pour une imprimante PostScript® (ou basée sur un autre langage), il va nous falloir un test plus sophistiqué. Un petit programme PostScript®, tel que celui qui suit, devrait suffire:

```
%!PS
100 100 moveto 300 300 lineto stroke
310 310 moveto /Helvetica findfont 12 scalefont setfont
(Is this thing working?) show
showpage
```

Le code PostScript® ci-dessus peut être placé dans un fichier et utilisé comme indiqué dans les exemples qui apparaissent dans les sections suivantes.

Lorsque ce document fait référence à un langage d'imprimante, il suppose un langage comme PostScript®, et pas le PCL de Hewlett-Packard. Quoique PCL dispose de fonctionnalités intéressantes, il est possible de mélanger du texte simple avec des séquences d'échappement. PostScript® ne permet pas d'imprimer du texte clair, c'est le type de langage d'imprimante pour lequel nous devons prendre des mesures particulières.

9.3.1.4.1. Tester une imprimante parallèle

Cette section vous apprendra à vérifier si FreeBSD peut communiquer avec une imprimante connectée sur un port parallèle.

Pour tester une imprimante connectée sur un port parallèle:

1. Passez en `root` avec su(1).
2. Envoyez des données à l'imprimante.
   - Si l'imprimante peut sortir du texte simple, alors utilisez lptest(1). Entrez:

     ```
     # lptest  /dev/lptN
     ```

     Où *N* est le numéro du port parallèle, en commençant à zéro.

   - Si l'imprimante comprend le PostScript® ou un autre langage d'imprimante, alors envoyez lui un petit programme. Entrez:

     ```
     # cat  /dev/lptN
     ```

     Tapez ensuite le programme, ligne à ligne et *attentivement*, car vous ne pouvez plus éditer une ligne une fois que vous avez appuyé sur la touche `Retour Chariot` ou `Entrée`. Une fois terminé, faites `CONTROL+D`, ou la combinaison correspondant à votre fin de fichier.

     Une autre manière de procéder est de placer le programme dans un fichier et d'entrer:

     ```
     # cat fichier  /dev/lptN
     ```

     Où *fichier* désigne le nom du fichier que vous désirez envoyer à l'imprimante.

Vous devriez voir quelque chose s'imprimer. Ne vous inquiétez pas si l'apparence du texte n'est pas satisfaisante; nous remédierons à ce genre de soucis plus tard.

9.3.1.4.2. Tester une imprimante série

Dans cette section vous apprendrez à vérifier si FreeBSD parvient à communiquer avec une imprimante connectée à un port série.

Pour tester une imprimante connectée sur un port série:

1. Passez en `root` avec su(1).
2. Editez le fichier /etc/remote. Ajoutez l'entrée suivante:

```
printer:dv=/dev/port:br#bps-rate:pa=parity
```

Où *port* représente le fichier de périphérique du port série (`ttyd0`, `ttyd1`, etc.), *bps-rate* représente la vitesse en bits-par-seconde à laquelle l'imprimante communique, et *parity* représente la parité réclamée par l'imprimante (`even` pour paire, `odd` pour impaire, `none` pour aucune, ou `zero` pour zéro).

Voici un exemple d'entrée pour une imprimante connectée à 19200 bps, sans parité, sur le troisième port série:

```
printer:dv=/dev/ttyd2:br#19200:pa=none
```

3. Connectez-vous à l'imprimante avec tip(1). Entrez:

```
# tip printer
```

Si cette étape ne fonctionne pas, éditez le fichier /etc/remote à nouveau et essayez d'utiliser /dev/cuaaN au lieu de /dev/ttydN.

4. Envoyez des données à l'imprimante.
   - Si l'imprimante peut sortir du texte simple, alors utilisez lptest(1). Entrez:

```
% $lptest
```

   - Si l'imprimante comprend le PostScript® ou tout autre langage d'imprimante, envoyez-lui un petit programme. Entrez-le ligne à ligne et *très attentivement*, dans la mesure où les touches d'édition, comme retour-arrière, peuvent revêtir une signification particulière pour l'imprimante. Vous pourriez également avoir besoin d'un caractère de fin de fichier ("EOF") particulier pour que l'imprimante sache qu'elle a reçu tout le programme. Pour les imprimantes PostScript®, appuyez sur `CONTROL+D`.

     Une autre manière de procéder est de placer le programme dans un fichier et d'entrer:

```
% >fichier
```

     Où *fichier* est le nom du fichier contenant le programme. Après avoir envoyé le fichier avec tip(1), appuyez sur la touche de fin de fichier appropriée.

Vous devriez voir quelque chose s'imprimer. Ne vous inquiétez pas si l'apparence du texte n'est pas satisfaisante; nous remédierons à ce genre de soucis plus tard.

9.3.1.5. Mettre en place le gestionnaire d'impression: le fichier /etc/printcap

A ce stade, votre imprimante doit être branchée, votre noyau configuré pour communiquer avec elle (si cela est nécessaire); et vous avez réussi à faire parvenir des données simples à l'imprimante. Nous sommes maintenant prêts à paramétrer LPD pour qu'il contrôle l'accès à l'imprimante.

LPD se paramètre en éditant le fichier /etc/printcap. Le gestionnaire d'impression LPD le lit à chaque fois que le gestionnaire est solicité, donc les mises à jour du fichier sont immédiatement prises en compte.

Le format du fichier printcap(5) est explicite. Utilisez votre éditeur favori pour modifier /etc/printcap. Le format est identique aux autres fichiers de configuration comme /usr/shared/misc/termcap et /etc/remote. Pour obtenir des informations complètes concernant ce format, consultez cgetent(3).

Le paramétrage simple du gestionnaire d'impression s'effectue selon les étapes suivantes:

1. Choisissez un nom (et quelques alias appropriés) pour l'imprimante, et placez-les dans /etc/printcap; lisez la section Nommer l'imprimante pour plus d'informations sur le nommage.
2. Désactivez les pages d'en-tête (elles sont activées par défaut) en insérant le paramètre `sh`; lisez la section Supprimer les pages d'en-tête pour plus d'informations.
3. Créez un répertoire de file d'attente, et précisez son chemin d'accès avec le paramètre `sd`; lisez la section Créer le répertoire de fil d'attente pour obtenir plus d'informations.
4. Sélectionnez l'entrée dev à utiliser pour l'imprimante, et notez la dans /etc/printcap avec le paramètre `lp`; lisez la section Identifier le périphérique d'imprimante pour obtenir plus d'informations. De plus, si l'imprimante est reliée par un port série, précisez les paramètres de communication avec le paramètre `ms#`, qui est détaillé dans la section Configurer les paramètres de communication du gestionnaire d'impression.
5. Installez un filtre d'entrée sous forme de fichier texte simple; lisez la section Installer le filtre texte pour obtenir plus de détails.
6. Testez la configuration en imprimant quelque chose avec la commande lpr(1). Vous trouverez plus de détails dans les sections Tester l'impression et Résolution des problèmes.

Les imprimantes basées sur un langage d'impression, telles les imprimantes PostScript®, ne peuvent imprimer du texte simple directement. La configuration simple esquissée ci-dessus et détaillée dans les sections suivantes présuppose que si vous installez ce genre d'imprimante vous n'imprimerez que des fichiers qu'elle peut comprendre.

Les utilisateurs s'attendent souvent à pouvoir imprimer du texte simple sur n'importe laquelle des imprimante installées sur votre système. Les applications qui s'en remettent à LPD pour imprimer s'y attendent en général elles aussi. Si vous installez ce genre d'imprimante et désirez pouvoir imprimer à la fois des travaux dans le langage de l'imprimante *et* des travaux en texte simple, vous êtes instamment prié d'ajouter une étape supplémentaire à la configuration simple esquissée ci-

dessus: installez un programme de conversion automatique texte simple vers PostScript® (ou tout autre langage d'imprimante). La section Prendre en charge des travaux texte sur des imprimantes PostScript® vous apprendra à le faire.

9.3.1.5.1. Nommer l'imprimante

La première étape (facile) est de choisir un nom pour l'imprimante. Que vous choisissiez un nom fonctionnel ou fantaisiste n'a aucune importance puisque vous pouvez également fournir une série d'alias.

Au moins l'une des imprimantes définies dans le fichier /etc/printcap devrait avoir pour alias `lp`. C'est le nom de l'imprimante par défaut. Si les utilisateurs n'ont pas positionné la variable d'environnement `PRINTER` et ne spécifient pas le nom d'une imprimante lorsqu'ils utilisent une ligne de commande relative à LPD, `lp` sera l'imprimante par défaut utilisée.

Par ailleurs, l'usage commun veut que le dernier alias d'une imprimante en soit une description complète, en incluant le fabricant et le modèle.

Une fois le nom et des alias communs choisis, placez-les dans le fichier /etc/printcap. Le nom de l'imprimante devrait commencer dans la colonne la plus à gauche. Séparez chaque alias par une barre verticale et mettez le caractère deux-points après le dernier alias.

Dans l'exemple suivant, nous commençons avec le squelette d'un /etc/printcap qui définit deux imprimantes (une Diablo 630 et une imprimante PostScript® laser Panasonic KX-P4455):

```
#
#  /etc/printcap for host rose
#
rattan|line|diablo|lp|Diablo 630 Line Printer:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:
```

Dans cet exemple, la première imprimante se nomme `rattan` et possède les alias suivants: `line`, `diablo`, `lp` et `Diablo 630 Line Printer`. Puisque l'alias `lp` lui est attribué, elle est également l'imprimante par défaut. La seconde s'appelle `bamboo` et possède les alias suivants: `ps`, `PS`, `S`, `panasonic` et `Panasonic KX-P4455 PostScript v51.4`.

9.3.1.5.2. Supprimer les pages d'en-tête

Par défaut, le gestionnaire d'impression LPD imprime une *page d'en-tête* pour chaque impression. Celle-ci mentionne le nom de l'utilisateur qui a demandé l'impression, la machine qui l'a envoyé, et le nom de l'impression, en grands et jolis caractères. Malheureusement, tout ce texte supplémentaire parasite le débogage d'une configuration simple de l'imprimante, aussi supprimerons-nous ces pages d'en-têtes.

Pour cela, ajoutez le paramètre `sh` à l'entrée de l'imprimante dans /etc/printcap. Voici un exemple de /etc/printcap où `sh` a été ajouté:

```
#
```

```
#  /etc/printcap for host rose - no header pages anywhere
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:
```

Observez la façon dont nous avons respecté le format correct: la première ligne commence dans la colonne la plus à gauche, et les lignes suivantes sont indentées. Toutes les lignes d'une entrée sauf la dernière se terminent par un antislash.

9.3.1.5.3. Créer le répertoire de file d'attente

La prochaine étape dans la configuration simple du gestionnaire d'impression consiste à créer un *répertoire de file d'attente*, c'est à dire un répertoire où les travaux vont demeurer jusqu'à ce qu'ils soient imprimés, et où un certain nombre d'autres fichiers nécessaires au gestionnaire d'impression prennent place.

A cause de la nature variable des répertoires de file d'attente, il est d'usage de les placer dans /var/spool. Il n'est pas non plus nécessaire de sauvegarder leur contenu. Les recréer est aussi simple que de faire un mkdir(1).

Il est également d'usage de créer le répertoire avec un nom identique à celui de l'imprimante, comme dans l'exemple ci-dessous:

```
# mkdir /var/spool/nom-de-l-imprimante
```

Toutefois, si votre réseau comporte beaucoup d'imprimantes, vous pouvez préférer placer les répertoires de file d'attente dans un unique répertoire que vous réserverez à l'impression avec LPD. C'est ce que nous allons faire pour les deux imprimantes de notre exemple, `rattan` et `bamboo`:

```
# mkdir /var/spool/lpd
# mkdir /var/spool/lpd/rattan
# mkdir /var/spool/lpd/bamboo
```

Si la confidentialité des travaux imprimés par les utilisateurs vous importe, vous souhaiterez certainement protéger le répertoire de file d'attente afin qu'il ne soit pas accessible par tout le monde. Les répertoires de file d'attente doivent appartenir, être accessibles en lecture et écriture et pouvoir être parcourus par l'utilisateur `daemon` et le groupe `daemon`, et personne d'autre. C'est ce que nous allons faire pour les deux imprimantes de notre exemple:

```
# chown daemon:daemon /var/spool/lpd/rattan
# chown daemon:daemon /var/spool/lpd/bamboo
# chmod 770 /var/spool/lpd/rattan
```

```
# chmod 770 /var/spool/lpd/bamboo
```

Pour finir, vous devez avertir LPD de l'existence de ces répertoires en utilisant le fichier /etc/printcap. Vous spécifiez le chemin du répertoire file d'attente avec le paramètre `sd`:

```
#
#  /etc/printcap for host rose - added spooling directories
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:
```

Notez que le nom de l'imprimante commence dans la première colonne mais que toutes les autres entrées décrivant l'imprimante doivent être indentées et que chaque fin de ligne doit être protégée par un antislash.

Si vous ne précisez pas de répertoire de file d'attente avec `sd`, le gestionnaire d'impression utilisera /var/spool/lpd par défaut.

9.3.1.5.4. Identifier le périphérique d'imprimante

Dans la section Entrées des périphériques nous avons identifié l'entrée du répertoire /dev que FreeBSD utiliserait pour communiquer avec l'imprimante. Maintenant, nous allons passer cette information à LPD. Quand le gestionnaire d'impression aura une impression à effectuer, il ouvrira le périphérique spécifié au nom du programme de filtre (qui est responsable de la transmission des données à l'imprimante).

Positionnez l'entrée pour le chemin d'accès /dev dans le fichier /etc/printcap en utilisant le paramètre `lp`.

Dans notre exemple, supposons que `rattan` est sur le premier port parallèle, et que `bamboo` est sur un sixième port série; voici les ajouts à apporter à /etc/printcap:

```
#
#  /etc/printcap for host rose - identified what devices to use
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:\
        :lp=/dev/lpt0:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:\
        :lp=/dev/ttyd5:
```

Si dans votre /etc/printcap vous ne précisez pas le paramètre `lp` pour une imprimante, LPD utilisera

/dev/lp par défaut. A l'heure actuelle, il n'existe pas d'entrée /dev/lp sous FreeBSD.

Si l'imprimante que vous êtes en train d'installer est connectée à un port parallèle, vous pouvez directement vous rendre à la section Installer le filtre texte. Sinon, assurez-vous de suivre les instructions de la section qui suit.

9.3.1.5.5. Configurer les paramètres de communication du gestionnaire d'impression

Pour les imprimantes connectées au port série, LPD peut configurer la vitesse en bps, la parité, et d'autres paramètres de communication série, pour le compte du programme de filtre qui envoie les données à l'imprimante. C'est avantageux dans la mesure où:

- Cela vous laisse essayer divers paramètres simplement en éditant le fichier /etc/printcap; vous n'avez pas besoin de recompiler le programme de filtre.
- Cela permet au gestionnaire d'impression d'utiliser le même programme pour de multiples imprimantes qui peuvent avoir des paramètres de communication série différents.

Les paramètres /etc/printcap suivants contrôlent les options de communication série pour le périphérique spécifié dans le paramètre `lp`:

`br#vitesse-bps`
: Positionne la vitesse de transmission du périphérique à *vitesse-bps*, où *vitesse-bps* peut prendre l'une des valeurs suivantes: 50, 75, 110, 134, 150, 200, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, ou 115200 bits par seconde.

`ms#stty-mode`
: Positionne les options du périphérique de terminal après l'avoir ouvert. stty(1) présente les options disponibles.

Quand LPD ouvre le périphérique spécifié par le paramètre `lp`, il positionne les caractéristiques de ce périphérique aux valeurs précisées par le paramètre `ms#`. Les modes suivants, détaillés dans stty(1) sont particulièrement intéressants: `parenb`, `parodd`, `cs5`, `cs6`, `cs7`, `cs8`, `cstopb`, `crtscts`, et `ixon`.

Peaufinons notre exemple pour l'imprimante qui est connectée au sixième port série. Nous allons paramétrer sa vitesse à 38400 bps. Quant au mode, nous allons spécifier aucune parité avec `-parenb`, des caractères 8 bits avec `cs8`, aucun contrôle modem avec `clocal` et un contrôle de flux matériel avec `crtscts`:

```
bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:\
        :lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:
```

9.3.1.5.6. Installer le filtre texte

Nous sommes maintenant en mesure de dire à LPD quel filtre texte utiliser pour envoyer les travaux à l'imprimante. Un *filtre texte*, également connu sous le nom de *filtre d'entrée*, est un programme que LPD lance lorsqu'il a une impression à effectuer. Lorsque LPD exécute le filtre texte pour une imprimante, il redirige l'entrée standard du filtre sur le travail d'impression, et la

sortie standard sur le fichier spécial de périphérique spécifié par le paramètre `lp`. On attend du filtre qu'il lise le travail d'impression sur son entrée standard, effectue les transformations nécessaires pour l'imprimante, et écrive le résultat sur sa sortie standard, qui sera imprimée. Pour plus d'informations sur les filtres texte, lisez la section Filtres.

Pour notre configuration simple de l'imprimante, le filtre texte peut être une petite procédure d'interpréteur de commandes qui ne fera qu'exécuter `/bin/cat` pour envoyer le travail d'impression à l'imprimante. Un autre filtre est livré avec FreeBSD, nommé lpf, qui se charge de faire des suppressions arrière et des soulignements pour les imprimantes qui ne sauraient pas gérer correctement ce genre de flux de caractères. Et bien sûr, vous pouvez utiliser un autre filtre, quel qu'il soit. Le filtre lpf est détaillé dans la section lpf: un filtre texte.

Tout d'abord, composons le filtre /usr/local/libexec/if-simple qui sera un simple filtre texte. Ecrivez ceci avec votre éditeur de texte favori:

```
#!/bin/sh
#
# if-simple - Simple text input filter for lpd
# Installed in /usr/local/libexec/if-simple
#
# Simply copies stdin to stdout.  Ignores all filter arguments.

/bin/cat  exit 0
exit 2
```

Rendez le fichier exécutable:

```
# chmod 555 /usr/local/libexec/if-simple
```

Et avertissez LPD qu'il doit l'utiliser, en renseignant le paramètre `if` dans /etc/printcap. Nous l'ajouterons aux deux imprimantes utilisées jusqu'ici dans notre /etc/printcap d'exemple:

```
#
#  /etc/printcap for host rose - added text filter
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:\ :lp=/dev/lpt0:\
        :if=/usr/local/libexec/if-simple:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:\
        :lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:\
        :if=/usr/local/libexec/if-simple:
```

Vous trouverez une copie du filtre if-simple dans le répertoire /usr/shared/examples/printing.

9.3.1.5.7. Lancer LPD

lpd(8) se lance depuis /etc/rc, avec la variable de contrôle `lpd_enable`. Cette variable a `NO` pour valeur par défaut. Si vous ne l'avez pas déjà fait, ajoutez la ligne:

```
lpd_enable="YES"
```

à votre /etc/rc.conf, puis relancez votre machine, ou lancez simplement lpd(8).

```
# lpd
```

9.3.1.5.8. Tester la configuration

Vous avez achevé la configuration simple de LPD. Malheureusement, les félicitations ne sont pas encore à l'ordre du jour, puisque nous devons encore tester la configuration et résoudre tout problème. Pour tester la configuration, essayez d'imprimer quelque chose. Pour imprimer avec le système LPD, vous devez utiliser la commande lpr(1), qui soumet un travail d'impression.

Vous pouvez combiner lpr(1) au programme lptest(1), que nous avons présenté à la section Vérifier la communication avec l'imprimante, pour produire du texte de test.

Pour tester la configuration simple de LPD

Entrez:

```
# lptest 20 5 | lpr -Pnom-de-l-imprimante
```

Où *nom-de-l-imprimante* représente le nom (ou l'alias) d'une imprimante tel que spécifié dans /etc/printcap. Pour tester l'imprimante par défaut, tapez lpr(1) sans aucun argument `-P`. Encore une fois, si vous faites ce test avec une imprimante qui s'attend à recevoir du PostScript®, envoyez un programme PostScript® au lieu d'employer lptest(1). Vous pouvez le faire en plaçant le programme dans un fichier et en entrant `lpr fichier`.

Pour une imprimante PostScript®, vous devriez obtenir le résultat du programme. Si vous utilisez lptest(1), alors votre sortie devrait ressembler à ça:

```
!"#$%'()*+,-./01234
"#$%'()*+,-./012345
#$%'()*+,-./0123456
$%'()*+,-./01234567
%'()*+,-./012345678
```

Pour tester l'imprimante plus encore, téléchargez des programmes (pour les imprimantes basées sur un langage spécifique) plus longs, ou lancez lptest(1) avec des arguments différents. Par exemple, `lptest 80 60` produira 60 lignes de 80 caractères chacune.

Si l'impression ne fonctionne pas, lisez la section Résolution des problèmes.

9.4. Configuration avancée de l'imprimante

Cette section décrit les filtres à utiliser pour imprimer des fichiers au formatage particulier, des pages d'en-tête, pour imprimer en réseau, et pour restreindre et comptabiliser l'utilisation de l'imprimante.

9.4.1. Les filtres

Bien que LPD gère les protocoles réseaux, les files d'attente, le contrôle d'accès et d'autres aspects de l'impression, la plus grande partie du *véritable* travail intervient dans les *filtres*. Les filtres sont des programmes qui communiquent avec l'imprimante et gèrent ses dépendances matérielles ainsi que ses besoins particuliers. Dans la configuration simple de l'imprimante, nous avons installé un filtre texte simple- un filtre particulièrement basique qui devrait fonctionner avec la plupart des imprimantes (voir la section Installer le filtre texte).

Toutefois, afin de profiter de la conversion de format, de la comptabilisation de l'utilisation de l'imprimante, de particularités matérielles, et ainsi de suite, il vous faut comprendre le fonctionnement des filtres. En dernier ressort, il incombera au filtre de gérer ces aspects. Et la mauvaise nouvelle, c'est que la plupart du temps, c'est *vous* qui devrez produire ces filtres vous-même. La bonne nouvelle, c'est que beaucoup existent déjà et que, sinon, ils sont en général assez faciles à écrire.

Par ailleurs, il en est un livré avec FreeBSD, /usr/libexec/lpr/lpf, qui fonctionne avec beaucoup d'imprimantes capables d'imprimer du texte brut. (Il gère les retours arrière et les tabulations dans le fichier, effectue une comptabilisation, mais c'est à peu près tout). Vous trouverez également d'autres filtres et composants de filtres dans le catalogue des logiciels portés de FreeBSD.

Voici ce que vous trouverez dans cette section:

- La section Fonctionnement des filtres tâche de donner une vue générale du rôle des filtres dans le processus d'impression. Il vous faut lire cette section pour comprendre ce qui se passe "sous le capot" lorsque LPD utilise des filtres. Cette connaissance vous permettra d'anticiper et de résoudre les problèmes que vous pourriez rencontrer quand vous installerez de plus en plus de filtres pour chacune de vos imprimantes.
- LPD s'attend à ce que toutes les imprimantes sachent imprimer du texte brut par défaut. Cela pose un problème pour les imprimantes PostScript® (ou les imprimantes basées sur un autre langage) qui ne peut pas imprimer du texte brut directement. La section Gérer les travaux d'impression de texte brut sur des imprimantes PostScript® vous indique la marche à suivre pour résoudre ce problème. Vous devrez lire cette section si vous avez une imprimante PostScript®.
- PostScript® est un format de sortie courant pour beaucoup d'applications. Certaines personnes écrivent même du code PostScript® directement. Malheureusement, les imprimantes PostScript® sont onéreuses. La section Emuler du PostScript® sur les imprimantes non-PostScript® vous indiquera comment modifier un filtre texte pour qu'une imprimante *non-PostScript*® accepte et imprime du PostScript®. Vous devrez lire cette section si vous ne disposez pas d'une imprimante PostScript®.

- La section Filtres de conversion vous apprendra à automatiser la conversion de formats de fichiers spécifiques, comme des graphiques ou des données de composition, en formats compréhensibles par l'imprimante. Après avoir lu cette section, vous serez en mesure de configurer vos imprimantes de telle sorte que vos utilisateurs pourront entrer la commande `lpr -t` pour imprimer du troff, ou `lpr -d` pour imprimer le format DVI produit par TeX, ou `lpr -v` pour imprimer des images en mode point, etc. Nous recommandons la lecture de cette section.
- La section Filtres de sortie révèle tout d'une fonctionnalité peu utilisée de LPD: les filtres de sortie. A moins que vous n'imprimiez des pages d'en-têtes (voir la section Pages d'en-tête), vous pouvez probablement complètement ignorer cette section.
- La section lpf: un filtre texte détaille `lpf`, un filtre texte destiné aux imprimantes en ligne (et aux imprimantes laser se comportant comme telles) plutôt complet malgré sa simplicité, et livré avec FreeBSD. Si vous avez besoin de mettre rapidement en place la comptabilisation de l'utilisation de l'imprimante pour du texte brut, ou si vous avez une imprimante qui fume lorsqu'elle voit passer des caractères de retour arrière, vous devez vraiment penser à `lpf`.

Une copie des différents scripts présentés ci-dessous se trouve dans le répertoire /usr/shared/examples/printing.

9.4.1.1. Fonctionnement des filtres

Comme expliqué précédemment, un filtre est un programme exécutable lancé par LPD pour gérer la partie de la communication avec l'imprimante qui est dépendante du périphérique.

Lorsque LPD veut imprimer un fichier d'un travail d'impression, il lance un programme de filtre. Il redirige l'entrée standard du filtre sur le fichier à imprimer, sa sortie standard vers l'imprimante, et l'erreur standard vers le fichier journal des erreurs (spécifié dans le paramètre `lf` du fichier /etc/printcap, ou /dev/console par défaut).

Le filtre lancé par LPD ainsi que les paramètres qui lui sont donnés dépendent de ce qui est placé dans le fichier /etc/printcap et des paramètres que l'utilisateur a passé sur la ligne de commande lpr(1) pour ce travail d'impression. Par exemple, si l'utilisateur a entré `lpr -t`, LPD aurait lancé le filtre troff, précisé par la paramètre `tf` pour l'imprimante de destination. Si l'utilisateur veut imprimer du texte brut, il lancerait le filtre `if` (c'est vrai la plupart du temps: lisez la section Filtres de sortie pour plus de détails).

Il existe trois types de filtres que vous pouvez spécifier dans /etc/printcap:

- Le *filtre texte*, confusément appelé *filtre d'entrée* dans la documentation LPD, gère l'impression de texte classique. Considérez-le comme le filtre par défaut. LPD s'attend à ce que toutes les imprimantes sachent imprimer du texte brut par défaut, et c'est au filtre texte de s'assurer que les retours arrière, tabulations et autres caractères spéciaux ne trompent pas l'imprimante. Si vous êtes dans un environnement où il vous faut rendre compte de l'utilisation de l'imprimante, le filtre texte doit également comptabiliser les pages imprimées, généralement en comptant le nombre de lignes imprimées et en le comparant avec le nombre de lignes par page supporté par l'imprimante. Le filtre texte est exécuté avec la liste de paramètres suivante:

  `nom_du_filtre` [-c] -w *largeur* -l *hauteur* -i *indentation* -n *utilisateur* -h *machine* *fichier_comptabilité*

où

`-c`

apparaît si le travail d'impression est lancé par la commande `lpr -l`

largeur

est la valeur du paramètre `pw` ("page width", pour "largeur de page") spécifié dans /etc/printcap, et possédant la valeur par défaut 132.

hauteur

est la valeur du paramètre `pl` ("page length", pour "hauteur de page"), par défaut: 66.

indentation

est le nombre d'indentations inséré par `lpr -i`, par défaut: 0.

utilisateur

est le nom du compte de l'utilisateur imprimant le fichier.

machine

est le nom de la machine depuis laquelle le travail d'impression a été soumis.

fichier_comptabilité

est le nom du fichier de comptabilisation spécifié par le paramètre `af`.

- Un *filtre de conversion* convertit un format de fichier spécifique en un autre que l'imprimante saura imprimer sur papier. Par exemple, des données de composition ditroff ne peuvent être imprimées directement, mais il vous est possible d'installer un filtre de conversion ditroff afin de convertir ces données ditroff en une forme que l'imprimante sait ingérer et imprimer. La section Filtres de conversion vous dira tout sur ce sujet. Les filtres de conversion doivent également tenir des statistiques, si vous avez besoin de comptabiliser les impressions. Les filtres de conversion sont lancés avec les paramètres suivants:

  `nom-du-filtre` -x *largeur-en-pixels* -y *hauteur-en-pixels* -n *login* -h *hôte fichier_comptabilité*

  où *largeur-en-pixels* est la valeur du paramètre `px` (0 par défaut) et *hauteur-en-pixels* est la valeur du paramètre `py` (0 par défaut).

- Le *filtre de sortie* n'est utilisé que s'il n'y a pas de filtre texte, ou si les pages d'en-tête ont été activées. D'après notre expérience, les filtres de sortie sont rarement employés. La section Filtres de sortie les détaillera. Un filtre de sortie ne prend que deux paramètres:

  `nom-du-filtre` -w *largeur* -l *hauteur*

  qui sont identiques aux paramètres `-w` et `-l` des filtres textes.

Les filtres doivent également *retourner* avec le code de retour suivant:

exit 0

Si le filtre a imprimé avec succès le fichier.

exit 1

Si le filtre n'a pu imprimer le fichier, mais désire que LPD essaie de l'imprimer à nouveau. LPD relancera un filtre s'il retourne avec ce code.

exit 2

Si le filtre n'a pu imprimer le fichier et ne veut pas que LPD retente l'impression. LPD rejettera le fichier.

Le filtre texte livré avec FreeBSD, /usr/libexec/lpr/lpf, tire parti des paramètres de largeur et hauteur de page pour savoir quand envoyer une instruction de saut de page et comment comptabiliser l'utilisation de l'imprimante. Il utilise les paramètres nom d'utilisateur, nom de machine, et fichier de comptabilisation pour enregistrer les entrées concernant la consommation.

Si vous recherchez des filtres, prenez garde à ce qu'ils soient compatibles avec LPD. Si c'est le cas, ils doivent se conformer à la liste de paramètres décrite ci-dessus. Si vous songez à écrire des filtres à usage général, alors faites en sorte qu'ils se conforment à ces mêmes listes de paramètres et de codes de retour.

9.4.1.2. Gérer les travaux d'impression de texte brut sur des imprimantes PostScript®

Si vous êtes l'unique utilisateur de votre ordinateur et de votre imprimante PostScript® (ou basée sur un autre langage), et que vous promettez de ne jamais envoyer de texte brut à votre imprimante et de ne jamais utiliser les fonctionnalités des divers programmes qui voudraient lui en envoyer, alors vous pouvez tout à fait passer cette section l'esprit tranquille.

Toutefois, si vous désirez envoyer du PostScript® et du texte brut à l'imprimante, alors vous êtes instamment priés de compléter la configuration de votre imprimante. Pour ce faire, nous chargerons le filtre texte de détecter si le travail d'impression est du texte brut ou du PostScript®. Tous les travaux d'impression PostScript® doivent débuter par `%!` (en ce qui concerne les autres langages, référez-vous à la documentation de l'imprimante). Si ces deux caractères sont les deux premiers du travail d'impression, il s'agit de PostScript® et le reste du travail d'impression peut être passé directement à l'imprimante. Dans le cas contraire, alors le filtre convertit le texte en PostScript® et imprime le résultat.

Comment procéder?

Si vous disposez d'une imprimante série, une bonne façon de faire est d'installer `lprps`. Il s'agit d'un filtre d'impression PostScript® qui assure une communication en duplex avec l'imprimante. Il met à jour le fichier d'état de l'imprimante avec des informations détaillées que cette dernière lui fournit, de sorte que les utilisateurs et les administrateurs puissent connaître précisément l'état de l'imprimante (par exemple `niveau de toner bas` ou `bourrage papier`). Mais plus important encore, il inclut un programme nommé `psif` qui détecte si le travail d'impression qui vient d'arriver est du texte brut et lance `textps` (un autre programme fourni avec `lprps`) pour le convertir en PostScript®. Il utilise alors `lprps` pour envoyer le travail d'impression à l'imprimante.

`lprps` fait partie du catalogue des logiciels portés FreeBSD (lisez la section Le catalogue des logiciels portés). Vous pouvez installer un des deux logiciels portés print/lprps-a4 et print/lprps-letter en fonction du format de papier utilisé. Après avoir installé `lprps`, précisez simplement le chemin vers le programme `psif` qui fait partie de `lprps`. Si vous avez installé `lprps` en recourant au catalogue des

logiciels portés, placez les valeurs suivantes pour l'entrée de l'imprimante série PostScript® dans /etc/printcap:

```
:if=/usr/local/libexec/psif:
```

Vous devrez également renseigner le paramètre `rw` qui indique à LPD de requérir l'imprimante en mode lecture/écriture.

Si vous disposez d'une imprimante PostScript® parallèle (et ne pouvez donc pas utiliser la communication en duplex avec l'imprimante dont a besoin `lprps`), vous pouvez recourir à la procédure suivante en tant que filtre texte:

```
#!/bin/sh
#
#  psif - Imprime du PostScript ou du texte brut sur une imprimante PostScript
#  Version script; CECI N'EST PAS la version fournie avec lprps
#  Fichier /usr/local/libexec/psif
#

IFS="" read -r first_line
first_two_chars=`expr "$first_line" : '\(..\)'`

if [ "$first_two_chars" = "%!" ]; then
    #
    #  Travail PostScript, l'imprimer.
    #
    echo "$first_line"  cat  printf "\004"  exit 0
    exit 2
else
    #
    #  Texte brut, le convertir, puis l'imprimer.
    #
    ( echo "$first_line"; cat ) | /usr/local/bin/textps  printf "\004"  exit 0
    exit 2
fi
```

Dans la procédure ci-dessus, `textps` est un programme que nous avons installé séparément pour convertir du texte en PostScript®. Vous pouvez recourir à n'importe quel programme texte-vers-PostScript®, selon votre désir. Le catalogue des logiciels portés de FreeBSD (voir la section Le catalogue des logiciels portés) comprend un programme de conversion texte-vers-PostScript® complet nommée `a2ps`, qui pourrait vous intéresser.

9.4.1.3. Emuler du PostScript® sur les imprimantes non-PostScript®

PostScript® est le standard *de fait* pour l'impression et la composition de haute qualité. Cependant, PostScript® est un standard *onéreux*. Heureusement, Aladdin Enterprises propose un succédané gratuit de PostScript® nommé Ghostscript qui fonctionne sous FreeBSD. Ghostscript peut lire la majorité des fichiers PostScript® et peut produire leurs pages sur une diversité de périphériques,

incluant beaucoup de marques d'imprimantes non-PostScript®. En installant Ghostscript et en recourant à un filtre texte spécial, vous pouvez obtenir de votre imprimante non-PostScript® qu'elle se comporte comme une véritable imprimante PostScript®.

Ghostscript fait partie du catalogue des logiciels portés, de nombreuses versions sont disponibles, la version la plus couramment utilisée est print/ghostscript-gpl.

Pour émuler du PostScript®, il nous faut faire en sorte que le filtre texte détecte s'il imprime un fichier PostScript®. Si ce n'est pas le cas, alors le filtre doit passer le fichier directement à l'imprimante; sinon il recourra à Ghostscript pour tout d'abord le convertir dans un format que l'imprimante saura interpréter.

Voici un exemple: la procédure suivante est un filtre texte pour les imprimantes Hewlett Packard Deskjet 500. Pour d'autres modèles, changez le paramètre `-sDEVICE` de la commande `gs` (Ghostscript). (Entrez `gs -h` pour obtenir une liste des périphériques reconnus par l'installation actuelle de Ghostscript).

```
#!/bin/sh
#
#  ifhp - Imprime du PostScript émulé par Ghostscript sur une DeskJet 500
#  Fichier /usr/local/libexec/ifhp

#
#  Traite LF comme CR+LF (pour éviter l'"effet d'escalier" sur les
#  imprimantes HP/PCL):
#
printf "\033k2G" || exit 2

#
#  Lit les deux premiers caractères du fichier
#
IFS="" read -r first_line
first_two_chars=`expr "$first_line" : '\(..\)'`

if [ "$first_two_chars" = "%!" ]; then
    #
    #  Si c'est du PostScript; utiliser Ghostscript pour le convertir et l'imprimer
    #
    /usr/local/bin/gs -dSAFER -dNOPAUSE -q -sDEVICE=djet500 \
      -sOutputFile=- -  exit 0
else
    #
    #  Texte brut ou HP/PCL, donc impression directe; effectuer un
    #  saut de page à la fin pour éjecter la dernière page.
    #
    echo "$first_line"  cat  printf "\033l0H"
exit 0
fi
```

```
exit 2
```

Pour finir, vous devez communiquer à LPD le filtre utilisé en positionnant le paramètre `if`:

```
:if=/usr/local/libexec/ifhp:
```

Voilà. Vous pouvez entrer `lpr texte.simple` et lpr peuimporte.ps, et chacune des deux commandes devrait imprimer avec succès.

9.4.1.4. Filtres de conversion

Après avoir mené à bien la configuration basique décrite à la section Configuration simple de l'imprimante, la première chose que vous souhaiterez probablement faire sera d'installer des filtres de conversion pour vos formats de fichiers favoris (le simple texte ASCII mis à part).

9.4.1.4.1. Pourquoi installer des filtres de conversion?

Les filtres de conversion facilitent l'impression de différentes sortes de fichiers. Par exemple, supposons que nous travaillions énormément avec le système de composition TeX, et que nous ayons une imprimante PostScript®. Chaque fois que nous générerons un fichier DVI à partir de TeX, nous ne pouvons l'imprimer directement avant d'avoir converti ce fichier DVI en PostScript®. La séquence de commandes serait la suivante:

```
% dvips seaweed-analysis.dvi
% lpr seaweed-analysis.ps
```

En installant un filtre de conversion pour fichiers DVI, nous pouvons à chaque fois nous passer de l'étape de conversion manuelle en chargeant LPD de le faire à notre place. Maintenant, à chaque fois que nous avons un fichier DVI, nous ne sommes plus qu'à un pas de l'impression:

```
% lpr -d seaweed-analysis.dvi
```

Nous faisons en sorte que LPD se charge de la conversion du fichier DVI à notre place en positionnant l'option `-d`. La section Options de conversion et de formatage donne la liste des options de conversion.

Pour chacune des options de conversion que vous voulez faire accepter par une imprimante, installez un *filtre de conversion* et indiquez son chemin d'accès dans /etc/printcap. Un filtre de conversion ressemble au filtre texte de notre configuration de base (voir la section Installer le filtre texte), à ceci près qu'au lieu d'imprimer du texte brut, le filtre convertit le fichier en un format compréhensible par l'imprimante.

9.4.1.4.2. Quels filtres de conversion dois-je installer?

Vous devez installer les filtres de conversion que vous vous attendez à utiliser. Si vous imprimez beaucoup de données DVI, alors un filtre de conversion DVI est dans la logique des choses. Si vous

devez imprimer beaucoup de troff, alors vous aurez sûrement besoin d'un filtre troff.

Le tableau suivant récapitule les filtres avec lesquels LPD fonctionne, leurs paramètres /etc/printcap, et comment les invoquer avec la `lpr`:

Type de fichier	paramètre /etc/printcap	option lpr
cifplot	`cf`	`-c`
DVI	`df`	`-d`
plot	`gf`	`-g`
ditroff	`nf`	`-n`
code FORTRAN	`rf`	`-f`
troff	`tf`	`-f`
image en mode point	`vf`	`-v`
texte brut	`if`	aucune, `-p`, or `-l`

Dans notre exemple, utiliser `lpr -d` veut dire que l'imprimante a besoin du paramètre `df` dans l'entrée /etc/printcap la concernant.

Aussi fortement que certains puissent s'en émouvoir, des formats comme le code FORTRAN ou le plot sont probablement obsolètes. Sur votre site, vous pouvez attribuer de nouvelles significations à ces options ou à toute autre option de formatage en installant simplement des filtres personnalisés. Par exemple, supposons que vous aimeriez imprimer des fichiers Printerleaf directement (fichiers issus du programme de publication assistée par ordinateur Interleaf), mais jamais de fichiers plot. Vous pourriez alors installer un filtre de conversion Printerleaf sous le paramètre `gf` et ensuite informer vos utilisateurs que `lpr -g` veut dire "imprimer des fichiers Printerleaf".

9.4.1.4.3. Installer des filtres de conversion

Etant donné que les filtres de conversion sont des applications qui ne font pas partie du système FreeBSD de base, vous devriez les installer dans /usr/local. Le répertoire /usr/local/libexec est une destination de choix, car ce sont des programmes spécialisés que seul LPD lancera; les utilisateurs ordinaires ne devraient jamais avoir à les lancer.

Pour activer un filtre de conversion, précisez son chemin d'accès dans le paramètre relatif à l'imprimante de destination dans /etc/printcap.

Dans notre exemple, nous allons ajouter le filtre de conversion DVI pour l'imprimante nommée `bamboo`. Revoici le fichier /etc/printcap d'exemple, avec le nouveau paramètre `df` pour l'imprimante `bamboo`:

```
#
#  /etc/printcap pour la machine rose - ajout du filtre df pour bamboo
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:\
        :lp=/dev/lpt0:\
```

```
        :if=/usr/local/libexec/if-simple:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:\
        :lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:rw:\
        :if=/usr/local/libexec/psif:\
        :df=/usr/local/libexec/psdf:
```

Le filtre DVI est une procédure nommée /usr/local/libexec/psdf. En voici le contenu:

```
#!/bin/sh
#
#  psdf - filtre DVI vers imprimante PostScript
#  Fichier /usr/local/libexec/psdf
#
# Appelé par lpd quand l'utilisateur lance lpr -d
#
exec /usr/local/bin/dvips -f | /usr/local/libexec/lprps "$@"
```

Cette procédure lance `dvips` en mode filtre (cela correspond au paramètre `-f`) sur l'entrée standard, qui est le travail d'impression à exécuter. Ensuite, elle lance le filtre pour imprimante PostScript® `lprps` (voir la section Gérer les travaux d'impression de texte brut sur des imprimantes PostScript®) avec les paramètres que LPD lui a passés. Le programme `lprps` utilisera ces paramètres pour comptabiliser les pages imprimées.

9.4.1.4.4. Exemples de filtre de conversion supplémentaires

Il n'existe pas de procédure figée pour l'installation des filtres de conversion, des exemples fonctionnels sont présentés dans cette section. Inspirez-vous de ces exemples pour créer vos propres filtres. Utilisez les tels quels s'il s'avèrent adéquats.

Cet exemple présente un filtre de conversion d'image en mode point (en fait un fichier GIF) pour une imprimante Hewlett-Packard LaserJet III-Si:

```
#!/bin/sh
#
#  hpvf - Convertit des fichiers GIF en HP/PCL, puis les imprime
#  Fichier /usr/local/libexec/hpvf

PATH=/usr/X11R6/bin:$PATH; export PATH
giftopnm | ppmtopgm | pgmtopbm | pbmtolj -resolution 300 \
     exit 0 \
    || exit 2
```

Son fonctionnement est le suivant: il convertit le fichier GIF en un format portable universel, puis en format portable en niveau de gris, et ensuite en bitmap portable, qu'il convertit enfin en données compatibles LaserJet/PCL.

Voici le /etc/printcap comportant une entrée pour une imprimante recourant au filtre ci-dessus:

```
#
#  /etc/printcap pour la machine orchid
#
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
        :lp=/dev/lpt0:sh:sd=/var/spool/lpd/teak:mx#0:\
        :if=/usr/local/libexec/hpif:\
        :vf=/usr/local/libexec/hpvf:
```

La procédure suivante est un filtre de conversion de données troff du système de composition groff pour l'imprimante PostScript® `bamboo`:

```
#!/bin/sh
#
#  pstf - Convertit des données troff de groff en PS, puis imprime.
#  Fichier /usr/local/libexec/pstf
#
exec grops | /usr/local/libexec/lprps "$@"
```

La procédure ci-dessus emploie de nouveau `lprps` pour gérer la communication avec l'imprimante. S'il s'agissait d'une imprimante sur port parallèle, nous utiliserions plutôt la procédure suivante:

```
#!/bin/sh
#
#  pstf - Convertit des données troff de groff en PS, puis imprime.
#  Fichier /usr/local/libexec/pstf
#
exec grops
```

C'est tout. Voici l'entrée qu'il faut ajouter dans /etc/printcap pour activer le filtre:

```
:tf=/usr/local/libexec/pstf:
```

Voici un exemple qui pourrait faire rougir les vieux briscards de FORTRAN. C'est un filtre de code FORTRAN pour toute imprimante sachant imprimer du texte brut. Nous l'installerons pour l'imprimante `teak`:

```
#!/bin/sh
#
# hprf - filtre texte FORTRAN pour LaserJet 3si:
# Fichier /usr/local/libexec/hprf
#

printf "\033k2G"  fpr  printf "\033l0H"
```

```
 exit 0
exit 2
```

Et nous ajouterons cette ligne dans /etc/printcap pour l'imprimante `teak` afin d'activer le filtre:

```
:rf=/usr/local/libexec/hprf:
```

Voici un dernier exemple, quelque peu complexe. Nous allons ajouter un filtre DVI pour l'imprimante LaserJet `teak` présentée ci-dessus. Tout d'abord, la partie facile: mettre à jour /etc/printcap avec l'emplacement du filtre DVI:

```
:df=/usr/local/libexec/hpdf:
```

Et maintenant, la partie difficile: écrire le filtre. Pour cela, nous avons besoin d'un programme de conversion DVI-vers-LaserJet/PCL. Le catalogue des logiciels portés (voyez la section Le catalogue des logiciels portés) en possède un: print/dvi2xx. Installer ce logiciel porté nous fournira le programme dont nous avons besoin, `dvilj2p`, qui convertit le DVI en code compatible LaserJet IIp, LaserJet III et LaserJet 2000.

L'utilitaire `dvilj2p` rend le filtre `hpdf` assez complexe, parce que `dvilj2p` ne sait pas lire l'entrée standard. Il lui faut un nom de fichier. Pire encore, le nom du fichier doit se terminer par .dvi, ce qui rend l'utilisation de /dev/fd/0 pour l'entrée standard problématique. Nous pouvons contourner cette difficulté en créant un lien symbolique temporaire (se terminant par .dvi) pointant vers /dev/fd/0, obligeant ainsi `dvilj2p` à lire l'entrée standard.

Le seul petit accroc restant est que nous ne pouvons pas utiliser /tmp pour le lien temporaire. Les liens symboliques ont pour propriétaire l'utilisateur et le group `bin`. Le filtre est lancé sous l'utilisateur `daemon`. Et le bit "sticky" est positionné sur le répertoire /tmp. Le filtre peut créer le lien, mais il ne pourra pas nettoyer lorsqu'il aura fini et supprimer ce lien puisqu'il appartient à un utilisateur différent.

Au lieu de ça, le filtre créera le lien dans le répertoire courant, qui est le répertoire de la file d'attente des travaux d'impression (précisé par le paramètre `sd` dans /etc/printcap). C'est l'endroit idéal pour faire travailler les filtres, particulièrement parce qu'il y a (parfois) plus d'espace disque libre dans ce répertoire que sous /tmp.

Voici, enfin, le filtre:

```
#!/bin/sh
#
#  hpdf - Imprime des données DVI sur une imprimante HP/PCL
#  Fichier /usr/local/libexec/hpdf

PATH=/usr/local/bin:$PATH; export PATH

#
#  Définit une fonction de nettoyage de nos fichiers temporaires.  Ils prennent place
```

```
#  dans le répertoire courant, qui sera le répertoire
#  de file d'attente
#  de l'imprimante.
#
cleanup() {
   rm -f hpdf$$.dvi
}

#
#  Définit une fonction de gestion des erreurs fatales: affiche le message
#  d'erreur et retourne 2.  Ce code d'erreur de 2 indique à LPD
#  de ne pas essayer de réimprimer le travail d'impression
#
fatal() {
    echo "$@" 12
    cleanup
    exit 2
}

#
#  Si l'utilisateur enlève le travail d'impression, LPD envoie SIGINT, donc
#  il faut capturer le signal SIGINT
#  (et quelques autres signaux) pour nettoyer après notre passage.
#
trap cleanup 1 2 15

#
#  Assurons-nous qu'il n'y ait pas conflit ce nom avec des fichiers existants.
#
cleanup

#
#  Lien du fichier DVI vers l'entrée standard (fichier à imprimer).
#
ln -s /dev/fd/0 hpdf$$.dvi || fatal "Cannot symlink /dev/fd/0"

#
#  Conversion LF = CR+LF
#
printf "\033k2G" || fatal "Cannot initialize printer"

#
#  Conversion et impression.  Le code de retour de dvilj2p ne semble
#  pas fiable: ignorons-le.
#
dvilj2p -M1 -q -e- dfhp$$.dvi

#
#  Nettoyage et sortie de la procédure
#
cleanup
```

```
exit 0
```

9.4.1.4.5. Conversion automatique: une alternative aux filtres de conversion

Tous ces filtres de conversion apportent beaucoup à votre environnement d'impression, mais nécessitent que l'utilisateur précise (dans la ligne de commande lpr(1)) lequel utiliser. Si vos utilisateurs ne sont pas particulièrement versés en informatique, préciser une option de filtre sera problématique. Mais ce qui s'avère pire encore est qu'une option de filtre mal choisie peut lancer un filtre sur un type de fichier erroné et causer l'impression de centaines de pages.

Plutôt que d'installer quelque filtre de conversion que ce soit, vous préférerez sans doute laisser le filtre texte (puisque c'est le filtre par défaut) déterminer le type de fichier qu'on lui a demandé d'imprimer et lancer automatiquement le filtre de conversion approprié. Des outils comme `file` peuvent s'avérer utiles dans ce cas. Bien entendu, il sera difficile d'établir les différences entre *certains* types de fichiers-et vous pouvez toujours, bien sûr, fournir des filtres de conversion uniquement pour eux.

Le catalogue des logiciels portés FreeBSD contient un filtre texte, nommé `apsfilter` (print/apsfilter), qui sait effectuer la conversion automatique. Il peut reconnaître le texte brut, le PostScript® les fichiers DVI et quasiment n'importe quelle sorte de fichier, effectuer les conversions appropriées et imprimer.

9.4.1.5. Filtres de sortie

Le gestionnaire d'impression LPD reconnaît un autre type de filtre dont nous n'avons pas encore discuté: le filtre de sortie. Un filtre de sortie est destiné à l'impression de texte brut seulement, comme le filtre texte, mais avec de nombreuses simplifications. Si vous utilisez un filtre de sortie mais pas de filtre texte, alors:

- LPD lance un filtre de sortie une seule fois par travail d'impression, au lieu d'une fois pour chacun des fichiers du travail d'impression.
- LPD ne fournit rien pour permettre au filtre de sortie de repérer le début ou la fin des fichiers du travail d'impression.
- LPD ne passe pas le nom de l'utilisateur ou le nom de la machine au filtre, qui n'est donc pas prévu pour effectuer la comptabilisation de l'impression. En fait, il ne reçoit que deux paramètres:

  `nom-du-filtre` -w *largeur* -l *hauteur*

  Où *largeur* provient du paramètre `pw` et *hauteur* du paramètre `pl` de l'entrée /etc/printcap pour l'imprimante en question.

Ne vous laissez pas séduire par la simplicité d'un filtre de sortie. Si vous désirez que chaque fichier d'un travail d'impression commence sur une page différente, un filtre de sortie *ne conviendra pas*. Utilisez un filtre texte (également appelé filtre d'entrée); voir la section Installer le filtre texte. De plus, le filtre de sortie se révèle en fait *plus complexe* en ce sens qu'il doit examiner le flux d'octets qui lui est envoyé pour y rechercher des caractères spéciaux et qu'il doit s'envoyer à lui-même des signaux comme s'ils provenaient de LPD.

Toutefois, un filtre de sortie s'avère *nécessaire* si vous désirez des pages d'en-tête et avez besoin d'envoyer des séquences d'échappement ou d'autres chaînes d'initialisation afin de pouvoir imprimer la page d'en-tête. (Mais il est également *futile* si vous voulez imputer les pages d'en-tête au compte de l'utilisateur, puisque LPD ne livre pas d'information sur l'utilisateur ou la machine au filtre de sortie).

Sur une seule imprimante, LPD permet à la fois un filtre de sortie et des filtres texte ou autres. Dans de tels cas, LPD ne lancera le filtre de sortie que pour imprimer la page d'en-tête (consultez la section Pages d'en-tête). LPD attend alors que le filtre de sortie *s'arrête par lui-même* en envoyant deux octets au filtre: ASCII 031 suivi d'ASCII 001. Lorsqu'un filtre de sortie lit ces deux octets (031,001), il devrait s'arrêter en s'envoyant à lui-même un `SIGSTOP`. Lorsque LPD a fini d'exécuter les autres filtres, il relance le filtre de sortie en lui envoyant un `SIGCONT`.

S'il y a un filtre de sortie mais *aucun* filtre texte et que LPD s'occupe d'un travail d'impression concernant du texte brut, alors LPD utilise le filtre de sortie pour réaliser ce travail d'impression. Comme exposé plus haut, le filtre de sortie imprimera chacun des travaux d'impression séquentiellement sans que des sauts de page ou autres formes d'avancement du papier ne surviennent, et ce n'est vraisemblablement *pas* ce que vous désirez. Dans presque tous les cas, il vous faut un filtre texte.

Le programme `lpf`, que nous avons présenté précédemment comme un filtre texte, peut également fonctionner en tant que filtre de sortie. Si vous avez besoin d'un filtre de sortie vite-fait-bien-fait mais ne voulez pas écrire le code d'examen d'octets et d'envoi de signal, essayez `lpf`. Vous pouvez également inclure `lpf` dans une procédure pour prendre en charge tout code d'initialisation qui pourrait être requis par l'imprimante.

9.4.1.6. `lpf`: un filtre texte

Le programme /usr/libexec/lpr/lpf qui est fourni avec la distribution binaire FreeBSD est un filtre texte (un filtre d'entrée) qui sait indenter la sortie (un travail d'impression soumis avec `lpr -i`), laisse passer les caractères littéraux (travail d'impression soumis avec `lpr -l`), ajuste la position d'impression des retours arrière et des tabulations dans le travail d'impression, et comptabilise les pages imprimées. Il peut également servir de filtre de sortie.

Le filtre `lpf` convient à de nombreux environnements d'impression. Et bien qu'il ne puisse pas envoyer de séquences d'initialisation à une imprimante, il est aisé d'écrire une procédure pour effectuer l'initialisation nécessaire et ensuite exécuter `lpf`.

Afin que `lpf` mène à bien la comptabilisation des pages, il faut que des valeurs correctes soient indiquées pour les paramètres `pw` et `pl` dans le fichier /etc/printcap. Il utilise ces valeurs pour déterminer combien de texte peut être imprimé sur une page et combien de pages ont été imprimées dans le travail d'impression d'un utilisateur. Pour plus d'informations sur la comptabilisation de l'impression, lisez la section Comptabiliser l'utilisation de l'imprimante.

9.4.2. Pages d'en-tête

Si vous avez *beaucoup* d'utilisateurs, et que tous utilisent des imprimantes diverses, alors vous allez certainement envisager les *pages d'en-tête* comme un mal nécessaire.

Les pages d'en-tête, également appelées *bannières* ou *burst page*, identifient à qui appartiennent les travaux d'impression après qu'ils aient été imprimés. Elles sont en général imprimées en caractères de grande taille et en gras, peuvent comporter des bordures décorées, de sorte qu'elles contrastent dans une pile d'impressions avec les véritables documents formant les travaux d'impression des utilisateurs. Elles leur permettent de retrouver facilement leurs travaux d'impression. L'inconvénient majeur d'une page d'en-tête est qu'elle représente une page supplémentaire à imprimer pour chacun des travaux d'impression, son utilité éphémère ne dépasse pas quelques minutes, et elle termine au recyclage du papier ou dans une corbeille. (Notez que une page d'en-tête est liée à chaque travail d'impression et non à chaque fichier dans un travail d'impression: il se pourrait donc que le gâchis de papier ne soit pas si grand.)

Le système LPD peut fournir des pages d'en-tête automatiquement pour vos impressions *si* votre imprimante sait imprimer directement du texte brut. Si vous disposez d'une imprimante PostScript®, il vous faudra un programme externe pour générer la page d'en-tête; lisez la section Les pages d'en-tête sur les imprimantes PostScript®.

9.4.2.1. Activer les pages d'en-tête

Dans la section Configuration simple de l'imprimante, nous avons désactivé les pages d'en-tête en positionnant le paramètre `sh` (ce qui signifie "suppress header", soit "suppression des en-têtes") dans /etc/printcap. Pour activer les pages d'en-tête sur une imprimante, il suffit d'enlever ce paramètre `sh`.

Cela semble trop facile, n'est-ce pas?

C'est vrai. Il se *pourrait* que vous ayez à fournir un filtre de sortie pour envoyer des chaînes d'initialisation à l'imprimante. Voici un exemple de filtre sortie pour les imprimantes Hewlett-Packard compatibles-PCL:

```
#!/bin/sh
#
#  hpof - filtre de sortie pour les imprimantes Hewlett Packard compatibles PCL
#  Fichier /usr/local/libexec/hpof

printf "\033k2G" || exit 2
exec /usr/libexec/lpr/lpf
```

Spécifiez le chemin d'accès au filtre de sortie avec le paramètre `of`. Lisez la section Filtres de sortie pour plus de détails.

Voici un fichier /etc/printcap d'exemple pour l'imprimante `teak` que nous avons présentée plus haut; nous avons activé les pages d'en-tête et ajouté le fichier de sortie ci-dessus:

```
#
#  /etc/printcap pour la machine orchid
#
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
        :lp=/dev/lpt0:sd=/var/spool/lpd/teak:mx#0:\
```

```
        :if=/usr/local/libexec/hpif:\
        :vf=/usr/local/libexec/hpvf:\
        :of=/usr/local/libexec/hpof:
```

Désormais, lorsque les utilisateurs lancent des travaux d'impression avec `teak`, ils obtiennent une page d'en-tête avec chaque travail d'impression. Si vos utilisateurs désirent perdre du temps à rechercher leurs impressions, ils peuvent omettre la page d'en-tête en soumettant le travail d'impression avec la commande `lpr -h`; lisez la section Options des pages d'en-tête pour connaître plus d'options lpr(1).

LPD imprime un caractère de saut de page après une page d'en-tête. Si votre imprimante utilise un autre caractère ou séquence de caractères différente pour éjecter une page, précisez-le avec le paramètre `ff` dans /etc/printcap.

9.4.2.2. Contrôle des pages d'en-tête

Une fois les pages d'en-tête activées, LPD produira un *en-tête long*, c'est à dire une page entière de grands caractères identifiant l'utilisateur, le nom de la machine et le travail d'impression. Voici un exemple (`kelly` a lancé le travail d'impression nommé "outline" depuis la machine `rose`):

```
k                 ll       ll
k                  l        l
k                  l        l
k   k     eeee     l        l     y    y
k  k     e    e    l        l     y    y
k k      eeeeee    l        l     y    y
kk k     e         l        l     y    y
k   k    e    e    l        l     y   yy
k    k    eeee    lll      lll     yyy y
                                       y
                                  y    y
                                   yyyy

                          ll
                  t        l       i
                  t        l
 oooo    u    u   ttttt    l      ii     n nnn     eeee
o    o   u    u     t      l       i     nn   n   e    e
o    o   u    u     t      l       i     n    n   eeeeee
o    o   u    u     t      l       i     n    n   e
o    o   u   uu     t  t    l       i     n    n   e    e
 oooo     uuu u      tt     lll     iii    n    n    eeee

r rrr     oooo     ssss     eeee
rr   r   o    o   s    s   e    e
r        o    o    ss      eeeeee
r        o    o      ss    e
r        o    o   s    s   e    e
r         oooo     ssss     eeee
```

```
                                        Job:  outline
                                        Date: Sun Sep 17 11:04:58 1995
```

LPD ajoute un saut de page à ce texte de sorte que le travail d'impression commence sur une nouvelle page (à moins que `sf` (supprimer les sauts de page) ne soit dans l'entrée correspondant à l'imprimante dans /etc/printcap).

Si vous préférez, LPD peut générer des *en-tête courts*; ajoutez le paramètre `sb` (en-tête court) dans le fichier /etc/printcap. La page d'en-tête ressemblera à ceci:

```
rose:kelly  Job: outline  Date: Sun Sep 17 11:07:51 1995
```

Par défaut également, LPD imprime d'abord la page d'en-tête, puis le travail d'impression. Pour inverser ce comportement, placez le paramètre `hl` (en-tête à la fin) dans /etc/printcap.

9.4.2.3. Comptabiliser les pages d'en-tête

Utiliser les pages d'en-tête fournies par LPD provoque un comportement particulier lorsqu'il s'agit de comptabiliser l'utilisation de l'imprimante: les pages d'en-tête doivent être *gratuites*.

Pourquoi?

Parce que le filtre de sortie est le seul programme externe pouvant tenir les comptes qui aura le contrôle lors de l'impression de la page d'en-tête, et qu'aucune information sur *l'utilisateur ou le nom de la machine* ne lui est donnée ni aucun fichier de comptabilisation, par conséquent il ne sait pas à qui attribuer le coût de l'utilisation de l'imprimante. Il ne suffit pas non plus de simplement "ajouter une page" au filtre texte ou un quelconque filtre de conversion (qui, eux, possèdent des informations sur l'utilisateur et la machine) puisque les utilisateurs peuvent supprimer les pages d'en-tête avec `lpr -h`. Ils pourraient toujours se voir imputer des pages d'en-tête qu'ils n'auraient pas imprimées. En somme, `lpr -h` demeurera l'option favorite des utilisateurs soucieux de l'environnement, mais vous ne pouvez aucunement les inciter à l'utiliser.

Il ne *suffit pas non plus* de laisser chacun des filtres générer ses propres pages d'en-tête (ce qui permettrait de savoir à qui imputer les coûts). Si les utilisateurs désiraient omettre les pages d'en-tête avec `lpr -h`, ils les obtiendraient quand même et le coût leur serait attribué puisque LPD ne donne aucun renseignement sur l'emploi de l'option `-h` à aucun des filtres.

Alors, quelles sont les options à votre disposition?

Vous pouvez:

- Accepter le comportement de LPD et la gratuité des pages d'en-tête.
- Installer une alternative à LPD, comme LPRng. La section Alternatives au gestionnaire d'impression standard en dit plus au sujet des autres gestionnaires d'impression qui peuvent être substitués à LPD.
- Ecrire un filtre de sortie *intelligent*. Normalement, un filtre de sortie n'est pas censé faire plus que d'initialiser une imprimante ou exécuter une conversion simple de caractères. Il convient

aux pages d'en-tête et aux travaux d'impression de texte brut (lorsqu'il n'y a aucun filtre (d'entrée) texte). Mais, s'il existe un filtre texte pour les travaux d'impression de texte, alors LPD ne lancera le filtre de sortie que pour les pages d'en-tête. Le filtre de sortie peut également analyser le texte de la page d'en-tête généré par LPD pour déterminer quels sont l'utilisateur et la machine à qui il faut attribuer le coût de cette page d'en-tête. Le seul autre problème avec cette méthode est que le filtre de sortie ne sait toujours pas quel fichier de comptabilisation utiliser (le nom du fichier spécifié par le paramètre `af` ne lui est pas fourni), mais si vous disposez d'un fichier de comptabilisation bien identifié, vous pouvez le coder en dur dans le filtre de sortie. Afin de faciliter l'étape d'analyse, utilisez le paramètre `sh` (en-tête courte) dans /etc/printcap. D'un autre côté, tout cela pourrait bien représenter beaucoup de dérangement, et les utilisateurs apprécieront certainement davantage l'administrateur généreux qui propose la gratuité des pages d'en-tête.

9.4.2.4. Les pages d'en-tête sur les imprimantes PostScript®

Comme décrit précédemment, LPD est en mesure de générer des pages d'en-tête texte convenant pour de nombreuses d'imprimantes. Bien entendu, PostScript® ne peut pas imprimer du texte directement, donc la fonctionnalité de page d'en-tête offerte par LPD est inutilisable ou presque.

Une solution manifeste est de faire générer la page d'en-tête par tous les filtres de conversion et le filtre texte. Les filtres devraient employer les paramètres utilisateur et nom de machine pour générer une page d'en-tête convenable. L'inconvénient de cette méthode est que les utilisateurs obtiendront toujours une page d'en-tête, même s'ils soumettent leurs travaux d'impression avec `lpr -h`.

Examinons cette méthode. La procédure ci-dessous prend trois paramètres (le nom de l'utilisateur, le nom de la machine et celui du travail d'impression) et réalise une page d'en-tête simple en PostScript®:

```
#!/bin/sh
#
#  make-ps-header - génére une page d'en-tête PostScript sur la sortie standard
#  Fichier /usr/local/libexec/make-ps-header
#

#
#  Ce sont des unités PostScript (72 par pouce).  A modifier pour A4 ou
#  tout autre format papier employé:
#
page_width=612
page_height=792
border=72

#
#  Vérification des paramètres
#
if [ $# -ne 3 ]; then
    echo "Usage: `basename $0` user host job" 12
    exit 1
```

```
fi

#
#  Mémorisation des paramètres, pour la lisibilité du PostScript, plus bas.
#
user=$1
host=$2
job=$3
date=`date`

#
#  Envoi du code PostScript sur stdout.
#
exec cat EOF
%!PS

%
%  Assurons-nous qu'il n'y a pas d'interférence avec le travail
%  utilisateur qui suivra
%
save

%
%  Applique une grosse bordure désagréable autour
%  du bord de la page.
%
$border $border moveto
$page_width $border 2 mul sub 0 rlineto
0 $page_height $border 2 mul sub rlineto
currentscreen 3 -1 roll pop 100 3 1 roll setscreen
$border 2 mul $page_width sub 0 rlineto closepath
0.8 setgray 10 setlinewidth stroke 0 setgray

%
%  Affiche le nom de l'utilisateur, de façon jolie, grande et proéminente
%
/Helvetica-Bold findfont 64 scalefont setfont
$page_width ($user) stringwidth pop sub 2 div $page_height 200 sub moveto
($user) show

%
%  Maintenant, les détails ennuyant:
%
/Helvetica findfont 14 scalefont setfont
/y 200 def
[ (Job:) (Host:) (Date:) ] {
200 y moveto show /y y 18 sub def }
forall

/Helvetica-Bold findfont 14 scalefont setfont
/y 200 def
```

```
[ ($job) ($host) ($date) ] {
        270 y moveto show /y y 18 sub def
} forall

%
% C'est tout
%
restore
showpage
EOF
```

Désormais, chacun des filtres de conversion et le filtre texte peuvent appeler cette procédure pour d'abord générer la page d'en-tête, et ensuite imprimer le travail d'impression de l'utilisateur. Voici le filtre de conversion DVI déjà mentionné plus haut dans ce document, modifié afin de générer une page d'en-tête:

```
#!/bin/sh
#
#  psdf - filtre DVI vers imprimante PostScript
#  Fichier /usr/local/libexec/psdf
#
#  Appelé par lpd quand l'utilisateur lance lpr -d
#

orig_args="$@"

fail() {
    echo "$@" 12
    exit 2
}

while getopts "x:y:n:h:" option; do
    case $option in
        x|y)  ;; # Ignore
        n)    login=$OPTARG ;;
        h)    host=$OPTARG ;;
        *)    echo "LPD started `basename $0` wrong." 12
              exit 2
              ;;
    esac
done

[ "$login" ] || fail "Pas de nom d'utilisateur"
[ "$host" ] || fail "PAs de nom de machine"

( /usr/local/libexec/make-ps-header $login $host "DVI File"
  /usr/local/bin/dvips -f ) | eval /usr/local/libexec/lprps $orig_args
```

Observez que le filtre doit analyser la liste des paramètres pour déterminer le nom de l'utilisateur

et celui de la machine. L'analyse menée par les autres filtres de conversion est identique. Toutefois, le filtre texte réclame un ensemble de paramètres légèrement différent (voyez la section Fonctionnement des filtres).

Comme précédemment exposé, cette solution, quoique relativement simple, invalide l'option de "suppression de page d'en-tête" (l'option `-h`) de `lpr`. Si les utilisateurs désiraient épargner la vie d'un arbre (ou économiser quelques centimes, si vous faites payer les pages d'en-tête), ils ne seraient pas en mesure de le faire, puisque chaque filtre va imprimer une page d'en-tête avec chaque travail d'impression.

Pour permettre aux utilisateurs de désactiver les pages d'en-tête en fonction du travail d'impression, il vous faudra recourir à l'une des astuces de la section Comptabiliser les pages d'en-tête: écrire un filtre de sortie qui analyse la page d'en-tête générée par LPD et produit une version PostScript®. Si l'utilisateur soumet le travail d'impression avec `lpr -h` alors ni LPD ni votre filtre de sortie ne généreront de page d'en-tête. Sinon, votre filtre de sortie lira le texte en provenance de LPD et enverra la page d'en-tête PostScript® appropriée à l'imprimante.

Si vous disposez d'une imprimante PostScript® sur une interface série, vous pouvez utiliser `lprps`, qui est livré avec un filtre de sortie, `psof`, qui réalise ce que nous venons d'exposer ci-dessus. Notez que `psof` n'assume pas la tenue de comptes pour les pages d'en-tête.

9.4.3. Imprimer via un réseau

FreeBSD gère l'impression via un réseau: c'est à dire en envoyant les travaux d'impression à des imprimantes distantes. L'impression via un réseau désigne deux choses différentes:

- Accéder à une imprimante connectée à une machine distante. Vous installez une imprimante disposant d'une interface conventionnelle, série ou parallèle, sur une machine. Puis vous configurez LPD pour permettre l'accès à l'imprimante depuis d'autres machines du réseau. La section Imprimantes installées sur des machines distantes en détaillera la mise en œuvre.
- Accéder à une imprimante directement connectée au réseau. L'imprimante dispose d'une interface réseau en plus (ou à la place) d'interfaces plus conventionnelles, série ou parallèle. Une imprimante de ce genre peut fonctionner ainsi:
  - Elle peut comprendre le protocole LPD et sait même gérer une file d'attente de travaux d'impression provenant de machines distantes. En ce cas, elle se comporte comme une machine normale qui exécuterait LPD. Suivez la même procédure que celle exposée à la section Imprimantes installées sur des machines distantes afin de configurer une imprimante de ce genre.
  - Elle peut savoir gérer un flux de données au travers d'une connexion réseau. Dans ce cas, vous pouvez "attacher" l'imprimante à l'une des machines du réseau en la rendant responsable de la gestion de la file d'impression et de l'envoi des travaux d'impression à l'imprimante. La section Imprimantes avec des interfaces utilisant des flux réseau donne quelque indications sur l'installation d'imprimantes de ce type.

9.4.3.1. Imprimantes installées sur des machines distantes

Le gestionnaire d'impression LPD dispose des fonctions pour gérer l'envoi des travaux d'impression à d'autres machines exécutant également LPD (ou un système qui lui est compatible).

Cette fonctionnalité vous permet d'installer une imprimante sur une machine, puis de la rendre accessible depuis les autres machines. Cela fonctionne également avec les imprimantes disposant d'interfaces réseau comprenant le protocole LPD.

Pour activer ce type d'impression à distance, installez d'abord une imprimante sur une machine, qui sera *la machine d'impression*, en suivant les instructions de configuration basique décrites à la section Configuration simple de l'imprimante. Réalisez toute étape de la configuration avancée de l'imprimante dont vous pourriez avoir besoin. Veillez à tester l'imprimante et vérifiez qu'elle fonctionne avec les paramètres de LPD que vous avez activés. Assurez-vous également que *la machine locale* est autorisée à utiliser le service LPD sur *la machine distante* (lisez la section Restreindre les impressions à distance).

Si vous utilisez une imprimante avec une interface réseau qui est compatible avec LPD, alors *la machine d'impression* dans le texte ci-dessous est l'imprimante elle-même, et le *nom de l'imprimante* est le nom que vous avez paramétré pour l'imprimante. Lisez la documentation livrée avec votre imprimante ou l'interface réseau-imprimante.

Si vous utilisez une Hewlett Packard Laserjet, alors le nom d'imprimante `text` réalisera la conversion LF en CRLF automatiquement, de sorte que vous n'aurez pas besoin de la procédure hpif.

Ensuite, sur les autres machines pour lesquelles vous désirez autoriser l'accès à l'imprimante, créez une ligne dans leur /etc/printcap avec les paramètres suivants:

1. Nommez cette entrée comme vous le voulez. Par souci de simplicité, cependant, vous préférerez certainement employer les mêmes nom et alias que ceux utilisés sur la machine de d'impression.
2. Laissez le paramètre `lp` non-renseigné, de manière explicite (`:lp=:`).
3. Créez un répertoire de file d'impression et indiquez son chemin d'accès dans le paramètre `sd`. C'est là où LPD entreposera les travaux d'impression avant leur envoi vers la machine d'impression.
4. Indiquez le nom de la machine d'impression avec le paramètre `rm`.
5. Placez le nom de l'imprimante sur *la machine d'impression* dans le paramètre `rp`.

C'est tout. Il n'est pas nécessaire de préciser la liste des filtres de conversion, les dimensions de la page, ou quoique ce soit d'autre dans le fichier /etc/printcap.

Voici un exemple. La machine `rose` dispose de deux imprimantes, `bamboo` et `rattan`. Nous allons permettre aux utilisateurs de la machine `orchid` d'imprimer avec ces imprimantes. Voici le fichier /etc/printcap pour `orchid` (apparu dans la section Activer les pages d'en-tête). Il contenait déjà une entrée pour l'imprimante `teak`; nous avons ajouté celles pour les deux imprimantes sur la machine `rose`:

```
#
#  /etc/printcap pour la machine orchid - ajout d'imprimantes (distantes)
#    sur rose
#
```

```
#
#  teak est locale; connectée directement à orchid:
#
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
        :lp=/dev/lpt0:sd=/var/spool/lpd/teak:mx#0:\
        :if=/usr/local/libexec/ifhp:\
        :vf=/usr/local/libexec/vfhp:\
        :of=/usr/local/libexec/ofhp:

#
#  rattan est connectée à rose; envoie les travaux pour rattan
#    à rose:
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :lp=:rm=rose:rp=rattan:sd=/var/spool/lpd/rattan:

#
#  bamboo est également connectée à rose:
#
bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :lp=:rm=rose:rp=bamboo:sd=/var/spool/lpd/bamboo:
```

Ensuite, nous n'avons qu'à créer les répertoires de file d'impression sur `orchid`:

```
# mkdir -p /var/spool/lpd/rattan /var/spool/lpd/bamboo
# chmod 770 /var/spool/lpd/rattan /var/spool/lpd/bamboo
# chown daemon:daemon /var/spool/lpd/rattan /var/spool/lpd/bamboo
```

Maintenant les utilisateurs d'`orchid` peuvent imprimer sur `rattan` et `bamboo`. Par exemple, si un utilisateur sur `orchid` entrait:

```
% lpr -P bamboo -d sushi-review.dvi
```

le système LPD sur `orchid` copierait le travail d'impression dans le répertoire de file d'impression /var/spool/lpd/bamboo et relèverait qu'il s'agit d'un travail d'impression DVI. Dès que la machine `rose` dispose d'assez de place dans son répertoire de file d'impression, les deux LPD transfèrent le fichier à `rose`. Le fichier reste en attente dans la file de `rose` jusqu'à son impression. Il sera converti de DVI en PostScript® (puisque `bamboo` est une imprimante PostScript®) sur `rose`.

9.4.3.2. Imprimantes avec des interfaces utilisant des flux réseau

Bien souvent, lorsque vous achetez une carte d'interface réseau pour une imprimante, vous avez le choix entre deux versions: l'une qui émule un gestionnaire d'impression (la version la plus onéreuse), ou une autre qui ne vous permet que de lui envoyer des données comme s'il s'agissait d'un port série ou parallèle (c'est la version la moins chère). Cette section vous indique comment utiliser cette seconde version moins onéreuse. Pour la plus chère, lisez la section précédente

Imprimantes installées sur des machines distantes.

Le format du fichier /etc/printcap vous permet de préciser quelle interface série ou parallèle vous souhaitez utiliser, et (si vous employez une interface série) à quelle vitesse de transmission, s'il faut employer le contrôle de flux, les temporisations pour les tabulations, la conversion des sauts de lignes, et plus encore. Mais il n'existe aucun moyen de préciser une connexion à une imprimante qui écoute sur un port TCP/IP ou un autre port réseau.

Pour envoyer des données à une imprimante mise en réseau, il vous faut développer un programme de communication qui puisse être appelé par les filtres textes et de conversion. Voici un exemple: la procédure `netprint` récupère toutes les données sur l'entrée standard et les envoie à une imprimante connectée au réseau. Nous précisons le nom de machine de l'imprimante dans le premier paramètre et le numéro de port auquel se connecter dans le deuxième paramètre de `netprint`. Notez qu'il ne gère que la communication unidirectionnelle (dans le sens FreeBSD vers imprimante); de nombreuses imprimantes réseau supporte la communication bidirectionnelle, et vous désirerez certainement en tirer parti (afin de connaître le statut de l'imprimante, de comptabiliser l'utilisation, etc.).

```
#!/usr/bin/perl
#
#  netprint - Filtre texte pour imprimante connectée au réseau
#  Fichier /usr/local/libexec/netprint
#
$#ARGV eq 1 || die "Usage: $0 printer-hostname port-number";

$printer_host = $ARGV[0];
$printer_port = $ARGV[1];

require 'sys/socket.ph';

($ignore, $ignore, $protocol) = getprotobyname('tcp');
($ignore, $ignore, $ignore, $ignore, $address)
    = gethostbyname($printer_host);

$sockaddr = pack('S n a4 x8', AF_INET, $printer_port, $address);

socket(PRINTER, PF_INET, SOCK_STREAM, $protocol)
    || die "Can't create TCP/IP stream socket: $!";
connect(PRINTER, $sockaddr) || die "Can't contact $printer_host: $!";
while (STDIN) { print PRINTER; }
exit 0;
```

Nous pouvons maintenant utiliser cette procédure avec différents filtres. Supposons que nous ayons une imprimante Diablo 750-N connectée au réseau. Elle reçoit les données à imprimer sur le port 5100. Le nom de machine de l'imprimante est `scrivener`. Voici le filtre texte pour cette imprimante:

```
#!/bin/sh
```

```
#
#  diablo-if-net - Filtre texte pour l'imprimante  Diablo `scrivener' écoutant
#  le port 5100.  Fichier /usr/local/libexec/diablo-if-net
#
exec /usr/libexec/lpr/lpf "$@" | /usr/local/libexec/netprint scrivener 5100
```

9.4.4. Restreindre l'utilisation de l'imprimante

Cette section fournit des informations sur la restriction de l'utilisation de l'imprimante. Le système LPD vous permet de contrôler quels utilisateurs peuvent accéder à une imprimante, tant localement qu'à distance, s'il leur est autorisé d'imprimer en plusieurs exemplaires, quelles sont les tailles maximales de leurs travaux d'impression et des files d'impression.

9.4.4.1. Restreindre l'impression en plusieurs exemplaires

Le système LPD facilite l'impression de plusieurs copies d'un même fichier par les utilisateurs. Ils peuvent imprimer leur travail avec `lpr -#5` (par exemple) et obtenir cinq exemplaires de chaque fichier du travail d'impression. Le fait de savoir s'il s'agit là d'une bonne idée vous appartient.

Si vous estimez que les copies multiples provoquent charge et usure inutiles pour vos imprimantes, vous pouvez désactiver l'option `-` de `lpr(1)` en ajoutant le paramètre `sc` au fichier `/etc/printcap`. Lorsque des utilisateurs soumettront un travail d'impression avec l'option `-`, ils obtiendront cet affichage:

```
lpr: multiple copies are not allowed
```

Notez que si vous avez mis en œuvre l'accès à une imprimante distante (voir la section Imprimantes installées sur des machines distantes), il faut que le paramètre `sc` soit positionné sur les /etc/printcap distants également, sinon vos utilisateurs auront toujours la possibilité d'imprimer des copies multiples en passant par une autre machine.

Voici un exemple. C'est le /etc/printcap pour la machine `rose`. L'imprimante `rattan` est plutôt robuste, et autorisera donc les copies multiples, par contre l'imprimante laser `bamboo` est quant à elle plus délicate, nous interdiront donc les impressions multiples en ajoutant le paramètre `sc`:

```
#
#  /etc/printcap pour la machine rose - restreint les impressions en plusieurs
exemplaires sur bamboo
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:\
        :lp=/dev/lpt0:\
        :if=/usr/local/libexec/if-simple:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:sc:\
        :lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:rw:\
        :if=/usr/local/libexec/psif:\
```

```
        :df=/usr/local/libexec/psdf:
```

Maintenant, il nous faut également ajouter le paramètre `sc` dans le fichier /etc/printcap de `orchid` (et tant que nous y sommes, désactivons les copies multiples pour l'imprimante `teak`):

```
#
#  /etc/printcap pour la machine orchid - pas d'impression en
#  plusieurs exemplaires pour
#  l'imprimante locale teak ou l'imprimante distante bamboo
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
        :lp=/dev/lpt0:sd=/var/spool/lpd/teak:mx#0:sc:\
        :if=/usr/local/libexec/ifhp:\
        :vf=/usr/local/libexec/vfhp:\
        :of=/usr/local/libexec/ofhp:

rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :lp=:rm=rose:rp=rattan:sd=/var/spool/lpd/rattan:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :lp=:rm=rose:rp=bamboo:sd=/var/spool/lpd/bamboo:sc:
```

En recourant au paramètre `sc`, nous empêchons l'utilisation de `lpr -#`, mais cela n'empêche toujours pas les utilisateurs de lancer lpr(1) à plusieurs reprises, ou de soumettre le même fichier plusieurs fois en un seul travail, de cette façon:

```
% lpr forsale.sign forsale.sign forsale.sign forsale.sign forsale.sign
```

Il existe plusieurs moyens de prévenir ces abus (y compris les ignorer) que vous êtes libres d'essayer.

9.4.4.2. Restreindre l'accès aux imprimantes

Vous pouvez contrôler qui a le droit d'imprimer sur quelles imprimantes en utilisant le mécanisme des groupes UNIX® et le paramètre `rg` dans /etc/printcap. Placez simplement les utilisateurs à qui vous voulez donner l'accès à une imprimante dans un groupe, et précisez ce groupe avec le paramètre `rg`.

Les utilisateurs n'appartenant pas au groupe (`root` inclus) se verront gratifiés d'un `lpr: Not a member of the restricted group` s'ils essaient d'imprimer avec l'imprimante contrôlée.

De même que pour le paramètre `sc` (supprimer les exemplaires multiples), il vous faut activer `rg` sur les machines distantes qui eux aussi ont accès à vos imprimantes, si vous estimez que c'est approprié (voir la section Imprimantes installées sur des machines distantes).

Dans notre exemple, nous allons permettre l'accès à `rattan` à quiconque, mais seuls les membres du groupe `artists` pourront utiliser `bamboo`. Voici l'habituel /etc/printcap pour la machine `rose`:

```
#
#  /etc/printcap pour la machine rose - restreint au groupe pour bamboo
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:\
        :lp=/dev/lpt0:\
        :if=/usr/local/libexec/if-simple:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:sc:rg=artists:\
        :lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:rw:\
        :if=/usr/local/libexec/psif:\
        :df=/usr/local/libexec/psdf:
```

Ne nous préoccupons pas de l'autre fichier /etc/printcap (pour la machine `orchid`). Bien entendu, n'importe qui sur `orchid` peut imprimer avec `bamboo`. Selon le cas, nous pourrons autoriser que certains utilisateurs sur `orchid`, et leur donner accès à l'imprimante. Ou non.

Il ne peut exister qu'un seul groupe de restriction par imprimante.

9.4.4.3. Contrôler la taille des travaux d'impression

Si beaucoup de vos utilisateurs accèdent aux imprimantes, vous aurez sans doute besoin de fixer une limite supérieure à la taille des fichiers qu'ils peuvent soumettre à l'impression. Après tout, le système de fichiers hébergeant les répertoires de file d'impression ne peut offrir que l'espace libre dont il dispose, et vous devez également vous assurer que de la place existe pour les travaux d'impression des autres utilisateurs.

LPD vous permet de fixer la taille maximale en octets qu'un fichier d'un travail d'impression peut atteindre avec le paramètre `mx`. Les unités sont exprimées en blocs de `BUFSIZ`, valant 1024 octets. Si vous donnez la valeur 0 à ce paramètre, la taille ne sera pas du tout limitée; en revanche, si aucun paramètre `mx` n'est défini, alors une limite par défaut de 1000 blocs sera utilisée.

La limite s'applique aux *fichiers* dans un travail d'impression, et *non pas* à la taille totale du travail d'impression.

LPD ne refusera pas un fichier dont la taille excède la limite que vous fixez pour une imprimante. Au lieu de cela, il placera les octets du fichier dans la file jusqu'à ce que la limite soit atteinte, puis imprimera. Les octets supplémentaires seront ignorés. S'il s'agit là d'un comportement approprié est un choix qui vous appartient.

Ajoutons des limites pour nos imprimantes d'exemple, `rattan` et `bamboo`. Puisque les fichiers PostScript® des utilisateurs du groupe `artists` ont tendance à être volumineux, nous allons les limiter à cinq mégaoctets. Nous ne fixerons aucune limite pour l'imprimante texte:

```
#
#  /etc/printcap pour la machine rose
#
```

```
#
#  Pas de limite sur la taille des travaux:
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:mx#0:sd=/var/spool/lpd/rattan:\
        :lp=/dev/lpt0:\
        :if=/usr/local/libexec/if-simple:

#
#  Limite de cinq mégaoctets:
#
bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:sc:rg=artists:mx#5000:\
        :lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:rw:\
        :if=/usr/local/libexec/psif:\
        :df=/usr/local/libexec/psdf:
```

Là encore, les limites ne s'appliquent qu'aux utilisateurs locaux. Si vous avez mis en place un accès distant à vos imprimantes, les utilisateurs distants ne seront pas contraints par ces limites. Il vous faudra positionner le paramètre `mx` dans les fichiers /etc/printcap distants également. Lisez la section Imprimantes installées sur des machines distantes pour obtenir plus d'informations sur l'impression à distance.

Il existe une autre manière spécifique pour limiter la taille des travaux d'impression sur les imprimantes à distance; lisez la section Restreindre les impressions à distance.

9.4.4.4. Restreindre les impressions à distance

Le gestionnaire d'impression LPD propose plusieurs moyens de restreindre les travaux d'impression soumis depuis des machines distants:

Restrictions en fonction des machines

Vous pouvez contrôler de quelles machines distantes les requêtes seront acceptées par un LPD local avec les fichiers /etc/hosts.equiv et /etc/hosts.lpd. LPD vérifie qu'une requête entrante provient d'une machine listée dans l'un de ces deux fichiers. Si ce n'est pas le cas, LPD refuse la requête.

Le format de ces fichiers est simple: un nom de machine par ligne. Notez que /etc/hosts.equiv est également utilisé par le protocole ruserok(3), et qu'il a un impact sur des programmes comme rsh(1) et rcp(1), aussi soyez prudent.

Par exemple, voici le fichier /etc/hosts.lpd présent sur la machine `rose`:

```
orchid
violet
madrigal.fishbaum.de
```

Cela signifie que `rose` accepte les requêtes provenant des machines `orchid`, `violet` et

madrigal.fishbaum.de. Si une quelconque autre machine tente d'accéder au LPD de rose, le travail d'impression sera refusé.

Restrictions sur la taille

Vous pouvez contrôler combien d'espace doit demeurer libre sur le système de fichiers où se trouve un répertoire de file d'impression. Créez un fichier nommé minfree dans le répertoire de file d'impression pour l'imprimante locale. Placez dans ce fichier un nombre représentant combien de blocs disques (de 512 octets) d'espace libre il doit rester pour qu'un travail d'impression soit accepté.

Cela vous permet de vous assurer que des utilisateurs distants ne rempliront pas votre système de fichiers. Vous pouvez également vous en servir pour accorder une certaine priorité aux utilisateurs locaux: ils pourront placer des travaux d'impression dans la file bien après que l'espace libre soit tombé sous le seuil indiqué dans le fichier minfree.

Par exemple, ajoutons un fichier minfree pour l'imprimante bamboo. Nous examinons /etc/printcap pour trouver le répertoire de file d'impression pour cette imprimante; voici l'entrée concernant bamboo:

```
bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:sc:rg=artists:mx#5000:\
        :lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:rw:mx#5000:\
        :if=/usr/local/libexec/psif:\
        :df=/usr/local/libexec/psdf:
```

Le répertoire de file d'impression est précisé par le paramètre sd. Nous placerons à trois méga-octets (soit 6144 blocs disque) la limite d'espace libre devant exister sur le système de fichiers pour que LPD accepte les travaux d'impression distants:

```
# echo 6144 > /var/spool/lpd/bamboo/minfree
```

Restrictions sur l'utilisateur

Vous pouvez contrôler quels utilisateurs distants ont le droit d'imprimer sur les imprimantes locales en positionnant le paramètre rs dans /etc/printcap. Lorsque rs est présent dans l'entrée d'une imprimante connectée localement, LPD acceptera les travaux d'impressions de machines distantes *si* l'utilisateur soumettant le travail possède également un compte sous le même nom sur la machine locale. Sinon, LPD refusera le travail d'impression.

Ce paramètre se révèle particulièrement utile dans un environnement où (par exemple) existent plusieurs services qui partagent un réseau, et que des utilisateurs débordent les frontières de ces services. En leur donnant des comptes sur vos systèmes, vous leur permettez d'utiliser vos imprimantes depuis les systèmes de leur propre service. Si vous préférez les autoriser à n'utiliser *que* vos imprimantes et pas les autres ressources de l'ordinateur, alors vous pouvez leur attribuer des comptes "bloqués", sans répertoire de connexion et avec un interpréteur de commandes inutilisable comme /usr/bin/false.

9.4.5. Comptabiliser l'utilisation de l'imprimante

Donc vous voulez faire payer vos impressions. Et pourquoi pas? Le papier et l'encre coûtent de l'argent. Et puis, il y a les coûts de maintenance-les imprimantes sont constituées de pièces mobiles et ont tendance à tomber en panne. Vous avez étudié vos imprimantes, vos modes d'utilisation et factures de maintenance, et avez abouti à un coût par page (ou par pied, par mètre, ou par ce que vous voulez). Maintenant, comment commencer à comptabiliser les impressions, dans les faits?

Eh bien, la mauvaise nouvelle est que le gestionnaire d'impression LPD ne vous aide pas beaucoup dans ce domaine. La comptabilisation dépend fortement du type d'imprimante que vous employez, des formats que vous imprimez et de *vos* besoins pour ce qui est de faire payer l'utilisation de l'imprimante.

Pour mettre en œuvre la comptabilisation, il vous faut modifier le filtre texte de l'imprimante (pour faire payer les travaux d'impression de texte brut) et ses filtres de conversion (pour faire payer les autres formats de fichiers), pour compter les pages ou demander à l'imprimante combien elle en a imprimées. Vous ne pouvez pas vous en tirer en utilisant le filtre de sortie simple, puisqu'il ne peut pas gérer la comptabilisation. Voir la section Les filtres.

En général, il existe deux façons de procéder à la comptabilisation:

- La comptabilisation *périodique* est la plus habituelle, probablement parce que la plus facile. Chaque fois que quelqu'un imprime un travail, le filtre enregistre l'utilisateur, la machine et le nombre de pages dans un fichier de comptabilisation. Tous les mois, semestres, années ou toute autre échéance que vous désirez, vous récupérez les fichiers de comptabilisation des diverses imprimantes, établissez les pages imprimées par les utilisateurs, et faites payer l'utilisation. Purgez ensuite tous les fichiers de comptabilisation, pour commencer à zéro la nouvelle période.
- La comptabilisation *à la volée* est moins répandue, peut-être parce qu'elle s'avère plus difficile. Cette méthode laisse les filtres s'occuper de taxer les utilisateurs pour les impressions dès qu'ils utilisent les imprimantes. Tout comme les quotas disques, la comptabilisation est immédiate. Vous pouvez empêcher les utilisateurs d'imprimer quand leur compte est dans le rouge, et pourriez leur fournir un moyen de vérifier et ajuster leurs "quotas d'impression". Cependant, cette méthode nécessite la mise en oeuvre d'une base de données afin de tracer les utilisateurs et leurs quotas.

Le gestionnaire d'impression LPD gère les deux méthodes facilement: puisque vous devez fournir les filtres (enfin, la plupart du temps), vous devez également fournir le code de comptabilisation. Mais il y a un bon côté: vous disposez d'une énorme flexibilité dans vos méthodes de comptabilisation. Par exemple, vous avez le choix entre les comptabilisations périodique et à la volée. Vous avez le choix des informations à tracer: noms d'utilisateurs, noms de machines, types des travaux d'impression, pages imprimées, surface de papier utilisée, durée d'impression du travail, etc. Et vous le faites en modifiant les filtres afin d'enregistrer ces informations.

9.4.5.1. Comptabilisation rapide et simplifiée des impressions

Deux programmes sont livrés avec FreeBSD qui vous permettent de mettre en place une comptabilisation périodique simple immédiatement. Il s'agit du filtre texte `lpf`, détaillé dans la section lpf: un filtre texte, et de pac(8), un programme qui rassemble et fait le total des entrées

contenues dans des fichiers de comptabilisation d'impressions.

Comme indiqué dans la section sur les filtres (Fonctionnement des filtres), LPD lance les filtres texte et de conversion avec le nom du fichier de comptabilisation à employer fourni en argument. Les filtres peuvent utiliser ce paramètre pour savoir où écrire un enregistrement de comptabilisation. Le nom de ce fichier provient du paramètre `af` dans /etc/printcap, et si le chemin donné n'est pas absolu, alors c'est un chemin d'accès relatif au répertoire de file d'impression.

LPD lance `lpf` avec les paramètres de largeur et hauteur de page (qui correspondent aux paramètres `pw` et `pl`). Le filtre `lpf` les utilise pour déterminer combien de papier sera consommé. Après avoir envoyé le fichier à l'imprimante, il enregistre ensuite une entrée dans le fichier de comptabilisation. Les entrées ressemblent à ceci:

```
2.00 rose:andy
3.00 rose:kelly
3.00 orchid:mary
5.00 orchid:mary
2.00 orchid:zhang
```

Vous devriez utiliser un fichier de comptabilisation séparé pour chaque imprimante, `lpf` ne disposant pas de mécanisme de verrouillage des fichiers, deux `lpf` pourraient corrompre leurs entrées respectives s'ils essayaient d'écrire dans le même fichier en même temps. Une manière aisée de s'assurer d'un fichier de comptabilisation séparé pour chaque imprimante est de recourir au paramètre `af=acct` dans /etc/printcap. Dès lors, un fichier de comptabilisation, nommé acct, sera placé dans le répertoire de file d'impression de chaque imprimante.

Lorsque vous serez prêts à faire payer les utilisateurs pour leurs impressions, lancez le programme pac(8). Placez-vous simplement dans le répertoire de file d'impression de l'imprimante pour laquelle vous voulez collecter les informations, et tapez `pac`. Vous obtiendrez un récapitulatif en dollars ressemblant à ceci:

```
 Login               pages/feet   runs    price
orchid:kelly                5.00    1   $  0.10
orchid:mary                31.00    3   $  0.62
orchid:zhang                9.00    1   $  0.18
rose:andy                   2.00    1   $  0.04
rose:kelly                177.00  104   $  3.54
rose:mary                  87.00   32   $  1.74
rose:root                  26.00   12   $  0.52

total                     337.00  154   $  6.74
```

Voici les arguments attendus par pac(8):

`-Pimprimante`

Pour quelle *imprimante* effectuer un récapitulatif. Cette option ne fonctionne que si un chemin d'accès absolu est donné dans le paramètre `af` de /etc/printcap.

`-c`

Trier selon le coût plutôt qu'alphabétiquement par nom d'utilisateur.

`-m`

Ignorer le nom de la machine dans les fichiers de comptabilisation. Avec cette option, l'utilisateur `smith` sur la machine `alpha` est le même que l'utilisateur `smith` sur la machine `gamma`. Sans elle, ils représentent des utilisateurs distincts.

`-pprix`

Calculer le coût en comptant un *prix* en dollars par page ou par pied au lieu du prix indiqué par le paramètre `pc` dans /etc/printcap, ou deux cents (la valeur par défaut). Vous pouvez préciser le *prix* en nombre à virgule flottante.

`-r`

Inverser l'ordre du tri.

`-s`

Créer un fichier de rapport et tronquer le fichier de comptabilisation.

nom ...

N'imprimer des statistiques que pour les utilisateurs dont les *nom*s sont donnés.

Dans le récapitulatif produit par défaut par pac(8), vous pouvez lire le nombre de pages imprimées par chaque utilisateur depuis les différentes machines. Si, sur votre site, la machine n'a pas d'importance (parce que les utilisateurs peuvent utiliser n'importe quelle machine), lancez `pac -m`, afin de produire le récapitulatif ci-dessous:

```
  Login               pages/feet   runs    price
andy                        2.00    1   $  0.04
kelly                     182.00  105   $  3.64
mary                      118.00   35   $  2.36
root                       26.00   12   $  0.52
zhang                       9.00    1   $  0.18

total                     337.00  154   $  6.74
```

Afin de calculer le montant dû en dollars, pac(8) utilise le paramètre `pc` de /etc/printcap (200 par défaut, c'est à dire 2 cents par page). Précisez avec ce paramètre le prix par page ou par pied, exprimé en centièmes de cents, que vous voulez imputer aux impressions. Vous pouvez spécifier cette valeur lorsque vous lancez pac(8) avec l'option `-p`. Cependant, avec cette option, les unités sont exprimées en dollars, et non en centièmes de cents. Par exemple,

```
# pac -p1.50
```

fait en sorte que chaque page coûte un dollar et cinquante cents. Vous pouvez vraiment faire des bénéfices en utilisant cette option.

Enfin, lancer `pac -s` enregistrera les informations du récapitulatif dans un fichier, dont le nom sera le même que le fichier de comptabilisation de l'imprimante mais avec le suffixe `_sum`. Il procède alors à la troncature du fichier de comptabilisation. Lorsque vous exécutez pac(8) à nouveau, il relit le fichier récapitulatif pour établir les totaux de départ, puis ajoute les informations du fichier de comptabilisation normal.

9.4.5.2. Comment compter les pages imprimées?

Afin de réaliser une comptabilisation précise et cela même à distance, vous devez pouvoir déterminer combien un travail d'impression consomme de papier. C'est le problème principal de la comptabilisation des impressions.

Pour du texte brut, ce problème n'est pas compliqué à résoudre: vous comptez combien un travail d'impression comporte de lignes et comparez avec le nombre de lignes par page que gère votre imprimante. N'oubliez pas de tenir compte des retours arrière dans le fichier, qui superposent les lignes, ou des longues lignes qui s'étendent sur une ou plusieurs lignes physiques supplémentaires.

Le filtre texte `lpf` (présenté à la section lpf: un filtre texte) prend ces éléments en considération lorsqu'il effectue la comptabilisation. Si vous écrivez un filtre texte qui doit effectuer une comptabilisation, vous pouvez vous inspirer du code source de `lpf`.

Mais comment gérer les autres formats?

Eh bien, pour la conversion DVI-vers-LaserJet ou DVI-vers-PostScript®, vous pouvez faire analyser les messages de sortie de `dvilj` ou `dvips` par votre filtre et regarder combien de pages ont été converties. Vous devriez pouvoir procéder de manière identique avec d'autres formats de fichiers et programmes de conversion.

Mais ces méthodes connaissent un défaut: il se peut que l'imprimante n'imprime pas toutes ces pages. Par exemple, un bourrage peut se produire, l'imprimante peut arriver à cours d'encre, ou exploser - et l'utilisateur serait tout de même débité.

Alors, que pouvez-vous faire?

Il n'existe qu'une seule méthode *sûre* pour procéder à une comptabilisation *précise*. Prenez une imprimante qui sache dire combien de papier elle utilise, et reliez-la par un câble série ou une connection réseau. Presque toutes les imprimantes PostScript® gèrent cela. D'autres types et modèles également (les imprimantes laser réseau Imagen, par exemple). Modifiez les filtres pour ces imprimantes afin d'obtenir la consommation de pages après chaque travail d'impression et faites en sorte qu'elles enregistrent des informations de comptabilisation basées sur cette *seule* valeur. Nul besoin de compter les lignes ou d'une analyse de fichier susceptible d'être erronée.

Bien entendu, vous pouvez toujours être généreux et rendre toutes les impressions gratuites.

9.5. Using Printers Traduction en Cours

9.5.1. Printing Jobs

9.5.2. Checking Jobs

9.5.3. Removing Jobs

9.5.4. Beyond Plain Text: Printing Options

9.5.4.1. Formatting and Conversion Options

9.5.4.2. Job Handling Options

9.5.4.3. Header Page Options

9.5.5. Administering Printers

9.6. Alternatives to the Standard Spooler Traduction en Cours

9.7. Troubleshooting Traduction en Cours

Chapitre 10. Compatibilité binaire avec Linux

10.1. Synopsis

FreeBSD fournit en option une compatibilité binaire avec Linux®, permettant aux utilisateurs d'installer et d'exécuter desapplications Linux, sans avoir à les modifier, sur un système FreeBSD. Cette option est disponible pour les architectures i386, amd64, et arm64.

Certaines caractéristiques spécifiques au système Linux ne sont pas encore supportées sous FreeBSD; cela concerne principalement des fonctionnalités spécifiques au matériel ou relatives à la gestion du système, comme les cgroups ou les espaces de noms.

Après la lecture de ce chapitre, vous connaîtrez:

- Comment activer la compatibilité binaire avec Linux sur un système FreeBSD.
- Comment installer des bibliothèques partagées Linux supplémentaires.
- Comment installer des applications Linux sur un système FreeBSD.
- Les détails de l'implémentation de la compatibilité Linux sous FreeBSD.

Avant de lire ce chapitre, vous devrez:

- Savoir comment installer des logiciels tiers.

10.2. Configurer la compatibilité binaire avec Linux

Par défaut, la compatibilité binaire avec Linux n'est pas activée. Pour l'activer au démarrage, ajoutez cette ligne au fichier /etc/rc.conf:

```
linux_enable="YES"
```

Une fois activée, elle peut être lancée sans redémarrer en exécutant:

```
# service linux start
```

La procédure /etc/rc.d/linux changera les modules noyau nécessaires et montera sous /compat/linux les systèmes de fichiers attendus par les applications Linux. Ceci est suffisant pour faire fonctionner les binaires Linux statiques. Ils peuvent être lancés de la même manière qu'un binaire natif FreeBSD; ils se comportent exactement de la même manière que des processus natifs et peuvent être suivis et debogués avec les méthodes habituelles.

Les binaires Linux liés de manière dynamique (c'est la vaste majorité des cas) demandent à ce que les bibliothèques dynamiques partgées Linux soient installées - ils peuvent être exécutés par le noyau FreeBSD, mais ne peuvent pas utiliser les bibliothèques FreeBSD; c'est semblable au principe

des binaires 32bits qui ne peuvent pas utiliser les bibliothèques natives 64bits. Il existe plusieurs méthodes pour mettre à disposition ces bibliothèques: on peut les copier à partir d'une installation Linux existante utilisant la même architecture, les installer à partir des paquets binaires FreeBSD, ou les installer en utilisant deboostrap(8) (à partir de sysutils/debootstrap), etc.

10.3. Système de base CentOS à partir des paquets binaires FreeBSD

Cette méthode n'est pas encore applicable sous arm64.

La méthode la plus simple pour installer les bibliotèques Linux est d'installer la version pré-compilée ou la version compilée à partir du catalogue des logiciels portés emulators/linux_base-c7, qui placera le système de base dérivé de CentOS 7 dans le répertoire /compat/linux:

```
# pkg install linux_base-c7
```

FreeBSD fournit les paquets des binaires Linux de certaines applications. Par exemple, pour installer Sublime Text 4, avec les bibliothèques Linux nécessaires, exécuter la commande suivante:

```
# pkg install linux-sublime-text4
```

10.4. Système de base Debian / Ubuntu avec debootstrap(8)

Une autre solution pour disposer des bibliothèques partagées Linux est l'utilisation de sysutils/debootstrap. Cela a pour avantage de disposer d'une distribution complète Debian ou Ubuntu. Pour l'utiliser, suivez les instructions données sur le Wiki FreeBSD: FreeBSD Wiki - Linux Jails.

Après cette installation, utilisez chroot(8) dans le répertoire nouvellement créé et installez le logiciel suivant la manière classique sous la distribution Linux installée, par exemple:

```
# chroot /compat/ubuntu /bin/bash
root@hostname:/# apt update
```

Il est possible d'utiliser debootstrap dans le répertoire /compat/linux, mais cela est déconseillé pour éviter les colisions avec les fichiers installés à partir des logiciels portés ou pré-compilés FreeBSD. A la place, utilisez un nom de répertoire dérivé du nom ou de la version de la distribution, e.g., /compat/ubuntu. Si l'instance debootstrap est destinée à fournir des bibliothèques partagées Linux sans utiliser explicitement chroot ou les jails, on peut faire pointer le noyau dessus en modifiant le paramètre sysctl `compat.linux.emul_path` et en ajoutant une ligne comme ce qui suit au fichier /etc/sysctl.conf:

```
compat.linux.emul_path="/compat/ubuntu"
```

Ce paramètre sysctl contrôle le mécanisme de traduction du chemin du noyau, consultez linux(4) pour plus de détails. Veuillez noter que ce changement peut être à l'origine de problèmes pour les applications Linux installées à partir des paquets binaires FreeBSD; une des raisons est que beaucoup de ces applications sont toujours en 32bits, alors qu'Ubuntu semble abandonner le support des bibliothèques 32bits.

10.5. Sujets avancés

La couche de compatibilité Linux est un travail en constante progression. Consultez FreeBSD Wiki - Linuxulator pour plus d'informations.

Tous les paramètres sysctl(8) relatifs à Linux peuvent être trouvés dans la page de manuel linux(4).

Certaines applications ont besoin que des systèmes de fichiers spécifiques soient montés. Cela est normalement géré par la procédure /etc/rc.d/linux, mais peut être désactivé en ajoutant la ligne suivante au fichier /etc/rc.conf:

```
linux_mounts_enable="NO"
```

Les systèmes de fichiers montés par la procédure rc ne fonctionneront pas pour les processus Linux à l'intérieur de jail ou chroot; si nécessaire, configurez-les dans /etc/fstab:

```
devfs      /compat/linux/dev      devfs      rw,late                    0  0
tmpfs      /compat/linux/dev/shm  tmpfs      rw,late,size=1g,mode=1777  0  0
fdescfs    /compat/linux/dev/fd   fdescfs    rw,late,linrdlnk           0  0
linprocfs  /compat/linux/proc     linprocfs  rw,late                    0  0
linsysfs   /compat/linux/sys      linsysfs   rw,late                    0  0
```

Depuis qu'à été ajouté le support pour l'exécution des binaires Linux 32 et 64 bits à la couche de compatibilité Linux (sur les hôtes 64 bits de type x86), il n'est plus possible d'ajouter l'émulation en statique dans un noyau personnalisé.

10.5.1. Installer des bibliothèques supplémentaires à la main

Pour un système de base dont l'arborescence a été créée avec debootstrap(8), utilisez les instructions données plus haut.

Si une application Linux se plaint de l'absence d'une bibliothèque partagée après avoir configuré la compatibilité binaire Linux, déterminez quelle est la bibliothèque partagée nécessaire au binaire Linux et installez-la à la main.

A partir d'un système Linux utilisant un processeur de même architecture, la commande `ldd` peut être utilisée pour déterminer quelles sont les bibliothèques partagées dont l'application a besoin.

Par exemple, pour contrôler quelles bibliothèques partagées sont nécessaires à `linuxdoom`, exécuter cette commande à partir d'un système Linux où est installé Doom:

```
% ldd linuxdoom
libXt.so.3 (DLL Jump 3.1) => /usr/X11/lib/libXt.so.3.1.0
libX11.so.3 (DLL Jump 3.1) => /usr/X11/lib/libX11.so.3.1.0
libc.so.4 (DLL Jump 4.5pl26) => /lib/libc.so.4.6.29
```

Ensuite, copier tous les fichiers mentionnés dans la dernière colonne, du système sous Linux vers /compat/linux sur le système FreeBSD. Une fois copiés, créer les liens symboliques vers les noms de fichiers donnés dans la première colonne. Cet exemple donnera lieu aux fichiers suivants sur le système FreeBSD:

```
/compat/linux/usr/X11/lib/libXt.so.3.1.0
/compat/linux/usr/X11/lib/libXt.so.3 -> libXt.so.3.1.0
/compat/linux/usr/X11/lib/libX11.so.3.1.0
/compat/linux/usr/X11/lib/libX11.so.3 -> libX11.so.3.1.0
/compat/linux/lib/libc.so.4.6.29
/compat/linux/lib/libc.so.4 -> libc.so.4.6.29
```

Si une bibliothèque Linux partagée existe avec le même numéro de version majeure que celle indiquée par la première colonne du résultat de la commande `ldd`, il est inutile de la copier vers le nom de fichier donné par la dernière colonne, la bibliothèque déjà existante devrait fonctionner. Il est cependant recommandé de copier malgré tout la bibliothèque partagée si c'est une version récente. L'ancienne version peut être supprimée, du moment que le lien symbolique pointe sur la nouvelle.

Par exemple, les bibliothèques suivantes existent déjà sur le système FreeBSD:

```
/compat/linux/lib/libc.so.4.6.27
/compat/linux/lib/libc.so.4 -> libc.so.4.6.27
```

et `ldd` indique qu'un binaire a besoin d'une version plus récente:

```
libc.so.4 (DLL Jump 4.5pl26) -> libc.so.4.6.29
```

Etant donné que la bibliothèque existante n'a qu'une ou deux versions de retard sur le dernier digit, le programme devrait fonctionner avec la version légèrement plus ancienne. Il est, néanmoins, plus sûr de remplacer la libc.so existante avec la version plus récente:

```
/compat/linux/lib/libc.so.4.6.29
/compat/linux/lib/libc.so.4 -> libc.so.4.6.29
```

Généralement, vous ne devrez chercher à savoir de quelles bibliothèques partagées dépendent les

binaires Linux que les premières fois que vous installerez des programmes Linux sur le système FreeBSD. Au bout d'un moment, il y aura un ensemble suffisant de bibliothèques partagées Linux sur le système pour être en mesure d'exécuter les binaires Linux nouvellement importés sans effort supplémentaire.

10.5.2. Marquage des binaires Linux ELF

Le noyau FreeBSD utilise plusieurs méthodes pour déterminer si le binaire à exécuter est pour Linux: il contrôle le marquage dans l'entête ELF du fichier, recherche les chemins connus vers l'interpréteur ELF et contrôle les notes dans le fichier ELF; enfin, par défaut, les exécutables ELF non marqués sont considérés comme étant pour Linux. Si toutes ces méthodes échouent, une tentative pour exécuter le binaire pourra générer une erreur:

```
% ./mon-binaire-elf-linux
ELF binary type not known
Abort
```

Pour que le noyau FreeBSD puisse distinguer un binaire ELF FreeBSD d'un binaire Linux, vous devez employer l'utilitaire brandelf(1):

```
% brandelf -t Linux mon-binaire-elf-linux
```

10.5.3. Installer une application Linux basée sur RPM

Pour installer une application Linux basée sur RPM, installer en premier le logiciel précompilé ou porté archivers/rpm4. Une fois installé, `root` peut utiliser la commande suivante pour installer un .rpm:

```
# cd /compat/linux
# rpm2cpio  /path/to/linux.archive.rpm | cpio -id
```

Si nécessaire, utiliser `brandelf` sur les binaires ELF installés. Il faut noter que cela empêchera une desinstallation propre.

10.5.4. Configurer le résolveur de noms de domaines

Si le DNS ne fonctionne pas, ou si cette erreur apparaît

```
resolv+: "bind" is an invalid keyword resolv+:
"hosts" is an invalid keyword
```

Vous devrez configurer un fichier /compat/linux/etc/host.conf contenant:

```
order hosts, bind
```

```
multi on
```

Cela indique qu'il faut tout d'abord regarder dans le fichier /etc/hosts puis interroger le DNS. Quand le fichier /compat/linux/etc/host.conf n'existe pas, les applications Linux trouvent le fichier /etc/host.conf et se plaignent de sa syntaxe FreeBSD incompatible. Supprimez `bind` si un serveur de noms n'est pas configuré avec le fichier /etc/resolv.conf.

10.5.5. Divers

Cette section décrit comment la compatibilité binaire avec Linux fonctionne, et est basée sur un courrier électronique de Terry Lambert tlambert@primenet.com envoyé à la liste de diffusion pour la discussion de sujets non-techniques en rapport avec FreeBSD (Message ID: `199906020108.SAA07001@usr09.primenet.com`).

FreeBSD possède une abstraction appelée "chargeur de classe d'exécution". C'est une portion de l'appel système execve(2).

Historiquement, le chargeur UNIX examinait le nombre magique (généralement les 4 ou 8 premiers octets du fichier) pour voir si c'était un binaire connu par le système, et si c'était le cas, invoquait le chargeur binaire.

Si ce n'était pas le type de binaire du système, l'appel execve(2) retournait un échec, et l'interpréteur de commandes tentait de l'exécuter comme une commande d'interpréteur. Cette hypothèse était celle par défaut "quel que soit l'interpréteur de commandes actuel".

Plus tard, une modification a été faite sur sh(1) pour examiner les deux premiers caractères, et s'ils étaient `:\n`, alors elle invoquait l'interpréteur de commandes csh(1) à la place.

FreeBSD possède désormais une liste de chargeurs, avec un chargeur par défaut, `#!`, pour exécuter les interpréteurs ou les procédures de commandes.

Pour le support de l'ABI Linux, FreeBSD voit le nombre magique comme un binaire ELF. Le chargeur ELF recherche une *marque* spécifique, qui se trouve dans une section de commentaires dans l'image ELF, et qui n'est pas présente dans les binaires SVR4/Solaris™ ELF.

Pour que les binaires Linux puissent fonctionner, ils doivent être *marqués* sous le type `Linux` avec brandelf(1):

```
# brandelf -t Linux file
```

Lorsque le chargeur ELF voit le marquage `Linux`, le chargeur remplace un pointeur dans la structure `proc`. Tous les appels système sont indexés par l'intermédiaire de ce pointeur (dans un système UNIX traditionnel, cela serait la structure `sysent[]`, contenant les appels système). De plus, le processus est marqué pour une gestion spéciale du vecteur d'interruption ("trap") pour le signal de code "trampoline", et plusieurs autres corrections (mineures) qui sont gérées par le noyau Linux.

Le vecteur d'appel système Linux contient, entre autres, une liste des entrées `sysent[]` dont les adresses résident dans le noyau.

Quand un appel système est effectué par le binaire Linux, le code "trap" déréférence de la structure `proc` le pointeur de la fonction de l'appel système, et utilise les points d'entrée Linux, et non pas FreeBSD, de l'appel système.

Le mode Linux *redéfinit dynamiquement* l'origine des requêtes. C'est, en effet, équivalent à l'option `union` de montage des systèmes de fichiers. Tout d'abord, une tentative est faite pour rechercher le fichier dans le répertoire /compat/linux/chemin-origine. Si cela échoue, la recherche est effectuée dans le répertoire /chemin-origine. Cela permet de s'assurer que les binaires nécessitant d'autres binaires puissent s'exécuter. Par exemple, l'ensemble des outils Linux peuvent tourner sous l'ABI Linux. Cela signifie également que les binaires Linux peuvent charger et exécuter les binaires FreeBSD, s'il n'y a pas de binaires Linux correspondant présents, et vous pourriez placer une commande uname(1) dans l'arborescence /compat/linux pour vous assurer que les binaires Linux ne puissent pas dire qu'ils ne tournent pas sous Linux.

En effet, il y a un noyau Linux dans le noyau FreeBSD. Les diverses fonctions sous-jacentes qui implémentent tous les services fournis par le noyau sont identiques entre les deux tables d'entrées des appels systèmes FreeBSD et Linux: les opérations sur les systèmes de fichiers, les opérations sur la mémoire virtuelle, la gestion des signaux, iet l'IPC System V. La seule différence est que les binaires FreeBSD utilisent les fonctions *glue* de FreeBSD, et les binaires Linux celles de Linux. Les fonctions *glue* de FreeBSD sont liées en statique dans le noyau, les fonctions *glue* Linux peuvent être liées statiquement, ou l'on peut y accéder via un module du noyau.

Techniquement, ce n'est pas vraiment de l'émulation, c'est l'implémentation d'une interface binaire pour les applications (ABI). Cela est parfois appelé "émulation Linux" parce que l'implémentation a été faite à une époque où il n'y avait pas vraiment d'autres mots pour décrire ce qui était en développement. Dire que FreeBSD exécutait les binaires Linux n'était pas vrai, jusqu'à ce le code de support Linux soit compilé ou le module soit chargé.

Chapitre 11. WINE

11.1. Synopsis

WINE, qui signifie Wine Is Not an Emulator, car c'est en fait un programme faisant office de surcouche d'interprétation des instructions système. Celui-ci permet l'installation et l'utilisation de programmes à l'origine prévus pour fonctionner sous Windows® sur FreeBSD (mais aussi sous d'autres systèmes d'exploitation).

Il fonctionne par l'interception des appels systèmes, ou des requêtes venant d'un programme vers le système d'exploitation, et transforme les appels systèmes Windows® en appels systèmes que FreeBSD peut comprendre. Il fera également en sorte de traduire dans le sens inverse les nouvelles instructions afin que le programme Windows® fonctionne comme espéré. Alors oui dans un certain sens, il *émule* bien un environnement Windows®, car il fournit bons nombres des ressources nécessaires au bon fonctionnement des applications Windows®.

Cependant, il ne s'agit pas d'un émulateur au sens strict du terme. En effet, dans la plupart des émulateurs, le fonctionnement est sensiblement différent. Ces derniers simulent des composants physiques informatiques afin de faire tourner des logiciels. C'est le cas notamment des solutions de virtualisation (comme: emulators/qemu). L'un des bénéfices notables de cette approche est la capacité d'installation d'un système d'exploitation entier. Cela signifie, que du point de vue des applications exécutées au sein de cet émulateur, tout se passe comme sur un véritable système non émulé. De cette manière les programmes ont de bonnes chances de fonctionner comme escomptés. Le mauvais côté inhérent à cette approche est tout simplement qu'un programme simulant du matériel informatique est forcément plus lent que ledit matériel qu'il tente de reproduire. Le système émulé (appelé *invité*) a besoin des ressources de la machine physique (appelée *hôte*), et réserve ces ressources tant qu'il fonctionne.

D'un autre côté, le projet WINE, est plus économe en ressources système. Il fera en sorte de traduire des instructions systèmes à la volée. Ce n'est en théorie pas aussi rapide qu'un véritable système Windows®, mais la différence de vitesse d'exécution reste minime. D'un autre côté, WINE essaie d'interpréter au mieux les différentes évolutions des systèmes Windows® pour rester compatible avec les applications originellement conçues pour ces systèmes. C'est une tâche complexe, ce qui veut dire qu'il faut garder en tête le fait que de nombreuses applications puissent ne pas fonctionner comme espéré sous WINE, ne marchent pas du tout, voire ne s'installent même pas.

De cette manière, WINE constitue une autre option dans le but d'essayer de faire fonctionner un programme Windows® sous FreeBSD. Il peut servir de première solution, si cela fonctionne, car cela peut permettre de lancer l'application escomptée sans pour autant monopoliser toutes les ressources du système hôte FreeBSD.

Ce chapitre va décrire:

- Comment installer WINE sur système un FreeBSD.
- Comment WINE fonctionne et quelles sont ses différences vis-à-vis des autres alternatives comme la virtualisation.
- Comment adapter WINE aux besoins spécifiques de certaines applications.

- Comment installer des interfaces graphiques pour assister à la configuration de WINE.
- Des astuces et des solutions à utiliser sous FreeBSD.
- La prise en compte de WINE au sein d'un environnement multi-utilisateur.

Avant de lire ce chapitre, il serait utile de:

- Comprendre quelques bases d'UNIX®.
- Savoir installer FreeBSD.
- Savoir configurer une connexion réseau.
- Savoir installer des applications.

11.2. WINE généralités et concepts

WINE est un système complexe, avant de pouvoir s'en servir au mieux sur FreeBSD, il convient de comprendre ce que c'est et comment il fonctionne.

11.2.1. WINE qu'est-ce que c'est?

Comme nous l'avons déjà vu dans le Synopsis de ce chapitre, WINE constitue une surcouche de compatibilité logicielle permettant l'utilisation d'applications Windows® sur d'autres systèmes d'exploitation. En théorie, cela signifie que ces programmes pourront être exécutés sous des systèmes comme FreeBSD, macOS et Android.

Lorsque WINE lance un exécutable Windows®, il se passe deux choses:

- Tout d'abord, WINE implémente un environnement qui imite celui de diverses versions de Windows®. Par exemple, si une application demande l'accès à une ressource de la machine comme la RAM, WINE possède une interface mémoire qui ressemble et se comporte (en tout cas pour l'application en question) comme Windows®.
- Ensuite, une fois que l'application utilise cette interface, WINE reçoit les requêtes d'adressage mémoire et les transforme en instructions compatibles avec le système hôte. À l'inverse, lorsque l'application sous WINE veut obtenir des données, elles sont converties pour être exploitées par cette application Windows®.

11.2.2. WINE et le système FreeBSD

L'installation de WINE sur un système FreeBSD entraînera celle de différents composants:

- Les applications FreeBSD permettant l'exécution de tâches comme lancer un exécutable Windows®, configurer le sous-système WINE, ou compiler un programme avec une compatibilité WINE.
- Un grand nombre de dépendances implémentant les fonctionnalités centrales de Windows® (par exemple /lib/wine/api-ms-core-memory-l1-1-1.dll.so, qui fait partie de l'interface mémoire mentionnée un petit peu plus haut).
- Un certain nombre d'exécutables Windows®, qui sont (ou en tout cas imitent) les programmes courants (comme /lib/wine/notepad.exe.so, qui fournit l'éditeur de texte standard de

Windows®).

- Des composants additionnels de Windows®, en particulier les polices de caractères (comme Tahoma, qui se trouve share/wine/fonts/tahoma.ttf à la racine de l'installation).

11.2.3. Programmes avec interface graphique et programmes en mode texte/terminal sous WINE

Comme dans le monde de FreeBSD, les terminaux sont extrêmement courants, il est naturel de penser que WINE possède une excellente prise en charge des programmes en mode texte. Cependant, la majorité des applications pour Windows®, surtout les applications les plus populaires, sont conçues pour une utilisation avec une interface utilisateur graphique. De ce fait, les outils de WINE sont conçus pour lancer par défaut des programmes possédant une interface graphique.

Néanmoins, il existe trois méthodes disponibles pour lancer ces programmes en interface utilisateur console:

- L'approche *sortie directe* qui affichera directement sur la sortie standard d'un terminal.
- La *wineconsole* qui est un outil qui peut être utilisé avec les options *user* ou *curses* afin d'utiliser certaines améliorations que fournit le système de WINE pour les applications consoles.

Ces méthodes sont détaillées en profondeur sur cette page : Wiki du projet WINE.

11.2.4. Projets dérivés de WINE

WINE est en lui-même un projet open source mature, de ce fait, ce n'est pas étonnant qu'il serve de base à d'autres solutions logicielles plus complexes.

11.2.4.1. Implémentations commerciales de WINE

Un certain nombre d'entreprises ont utilisé WINE comme base centrale d'un de leur propre produit propriétaire (sachant que la licence LGPL permet ceci). Voici deux solutions populaires basées sur le projet WINE:

- CrossOver de Codeweavers

Cette solution propose des installations en un clic de différentes versions de WINE contenant différentes améliorations et optimisations (l'entreprise contribue au projet WINE en partageant certaines de ses améliorations). La principale préoccupation de Codeweavers est de faire en sorte que la plupart des applications les plus populaires puissent s'installer et s'exécuter parfaitement.

Bien que l'entreprise ait par le passé produit une version native de CrossOver pour FreeBSD, ce n'est plus le cas depuis longtemps. Certaines références en ligne sont encore disponibles (comme ici sur un forum dédié), cela fait cependant un certains temps qu'elles ne sont plus mises à jour.

- Proton de Steam

Steam qui distribue principalement des jeux vidéo utilise aussi WINE afin de permettre l'installation et l'exécution de jeux prévus pour Windows® sur d'autres systèmes d'exploitation.

Cela vise surtout à la base les systèmes de type Linux, bien qu'une certaine prise en charge de macOS existe également.

Tandis que Steam ne propose pas de version FreeBSD de leur client, il existe plusieurs options pour utiliser la versions Linux® du client en utilisant la surcouche de compatibilité Linux de FreeBSD.

11.2.4.2. Programmes d'accompagnement de WINE

Aux solutions propriétaires, nous pouvons ajouter d'autres projet ayant publié des applications conçues pour fonctionner en tandem avec la version standard et open source de WINE. Le but de ces solutions va de rendre l'installation de WINE plus facile à la simplification de l'installation des programmes les plus populaires.

Ces solutions sont abordées avec plus de détails dans une partie ultérieure de ce chapitre: interfaces graphiques pour la gestion de WINE , avec notamment:

- winetricks
- Homura

11.2.5. Les alternatives à WINE

Pour les utilisateurs de FreeBSD, certaines alternatives à WINE existent:

- Le double-amorçage: Une solution évidente est de directement lancer les programmes conçus pour Windows® sur ce dernier. Cela veut bien sûr dire qu'il faudra quitter FreeBSD afin de démarrer sous Windows®, aussi cette méthode n'est pas envisageable si l'accès aux programmes des deux systèmes en simultané est nécessaire.
- Les machines virtuelles: les machines virtuelles (ou VMs), comme mentionné plus tôt dans ce chapitre, sont des procédés logiciels qui émulent un ensemble complet de matériels informatiques, sur lequel un autre système d'exploitation (comprenant Windows®) peut être installé et utilisé. Les outils modernes rendent les VMs simples à créer et à gérer, mais cette méthode a un coût. En effet, une bonne portion des ressources du système hôte doit être allouée à chaque VM, sachant que ces ressources ne pourront pas être libérées tant que la VM est en fonctionnement. Il existe plusieurs solutions de gestion de machines virtuelles disponibles sous FreeBSD, les solutions open source comme qemu, bhyve et VirtualBox en sont un bon exemple. Voir le chapitre sur la Virtualisation pour plus de détails.
- L'accès distant: Comme beaucoup d'autres systèmes de type UNIX®, FreeBSD est capable d'utiliser un ensemble d'applications permettant aux utilisateurs d'accéder à des ordinateurs Windows® à distance afin d'utiliser leurs programmes et données. En plus des clients comme xrdp qui sont compatibles avec le protocole de bureau distant (RDP) standard de Windows®, il existe d'autres standards open source comme vnc pouvant aussi être utilisé (si un serveur compatible est présent à l'autre bout).

11.3. Installer WINE sur FreeBSD

WINE peut être installé grâce à l'outil de gestion de logiciels pré-compilés de FreeBSD (pkg), ou bien en compilant le programme depuis le catalogue de logiciels portés.

11.3.1. WINE les prérequis

Avant de procéder à l'installation de WINE lui-même, il convient d'avoir préinstallé ce qui suit:

- Une interface utilisateur graphique

La plupart des programmes Windows® s'attendent à pouvoir interagir avec une interface graphique. Si WINE est installé sans une interface graphique déjà présente, ses dépendances comprendront également le compositeur Wayland, et de ce fait, une interface graphique sera effectivement installée aux côtés de WINE. Cela dit, il vaut mieux installer au préalable une interface graphique de votre choix, configurée et fonctionnelle avant de procéder à l'installation de WINE.

- wine-gecko

Pendant une longue période Windows® avait, par défaut, pré-installé le navigateur Web: Internet Explorer. Par conséquent, certaines applications s'exécuteront en partant du principe qu'il y aura toujours quelque chose capable d'afficher des pages Web. Dans le but de fournir cette fonctionnalité, la surcouche logicielle de WINE inclue un navigateur Internet basique utilisant le moteur de rendu Web Gecko issu du projet Mozilla. Lorsque WINE sera lancé pour la première fois, une fenêtre de dialogue apparaîtra pour proposer le téléchargement et l'installation de Gecko. Il existe un certain nombre de raisons pour vouloir procéder ainsi (cela sera abordé plus loin). Mais, il peut aussi être installé avant même d'installer WINE ou en parallèle de l'installation de ce dernier.

Pour installer ce programme en version pré-compilée, il faut procéder comme ce qui suit:

```
# pkg install wine-gecko
```

ou alors, il est aussi possible de le compiler depuis le catalogue de logiciels portés:

```
# cd /usr/ports/emulator/wine-gecko
# make install
```

- wine-mono

MONO est une implémentation open source de la plateforme de développement .NET de Microsoft. Installer MONO devrait rendre plus facile l'installation et l'utilisation des applications écrites en .NET sous FreeBSD.

Pour l'installer la version pré-compilée:

```
# pkg install wine-mono
```

Pour compiler MONO à partir du catalogue de logiciels portés:

```
# cd /usr/ports/emulator/wine-mono
```

```
# make install
```

11.3.2. Installer WINE depuis le dépôt de paquets de FreeBSD

Une fois les prérequis installés, il suffit de procéder à l'installation de WINE via la commande suivante:

```
# pkg install wine
```

ou alors, WINE peut être compilé depuis le catalogue de logiciels portés avec les commandes suivantes:

```
# cd /usr/ports/emulator/wine
# make install
```

11.3.3. Préoccupations concernant les différences entre les versions 32 et 64 bits de WINE

Comme la plupart des applications, les programmes Windows®, sont, eux aussi, passés de l'ancienne architecture 32 bits à l'architecture 64 bits. La plupart des logiciels récents sont écrits pour des systèmes d'exploitation 64 bits, cependant, les systèmes d'exploitation modernes peuvent parfois continuer d'utiliser des programmes plus anciens en 32 bits. FreeBSD ne diffère en rien sur ce point, il supporte effectivement les architectures 64 bits depuis les versions 5.X du système.

Ainsi, le fait que les programmes les plus anciens ne soient plus pris en charge, peut justifier l'emploi d'émulateurs. Les utilisateurs se tournent bien souvent vers WINE afin de pouvoir jouer à des jeux et utiliser divers programmes qui ne fonctionnent plus correctement sur du matériel moderne. Heureusement, FreeBSD prend en charge les trois cas de figures:

- Pour une machine moderne 64 bits sur laquelle vous désirez lancer une application 64 bits Windows®, il suffit de procéder à l'installation des outils WINE comme détaillés dans les rubriques précédentes. En procédant ainsi, le système installera automatiquement la version 64 bits de Wine.
- Si jamais, un utilisateur possède une vieille machine prenant en charge exclusivement les architectures 32 bits, il peut installer une version 32 bits de FreeBSD et ensuite procéder à l'installation de WINE comme indiqué précédemment.

11.4. Lancer un premier programme WINE sous FreeBSD

Maintenant que WINE est installé, la prochaine étape est d'essayer WINE en tentant de lancer un programme simple. Une manière simple de faire cela est de télécharger une application autonome, par exemple, un programme qu'il suffit d'extraire de son archive et de lancer directement sans aucun autre processus d'installation plus complexe.

Ces applications de types "portables" constituent de bons choix pour procéder à ce genre de tests, tout comme les programmes pouvant s'exécuter en s'appuyant sur un unique fichier exécutable.

11.4.1. Lancer un programme WINE en ligne de commande

Il existe deux méthodes différentes pour lancer des programmes Windows depuis un émulateur de terminal. La première et la plus directe, est de naviguer dans le répertoire contenant l'exécutable du programme en question (.EXE) et de taper ce qui suit:

```
% wine program.exe
```

Pour les applications qui acceptent des arguments en ligne de commande, il suffit de les ajouter après l'exécutable comme habituellement:

```
% wine program2.exe -file file.txt
```

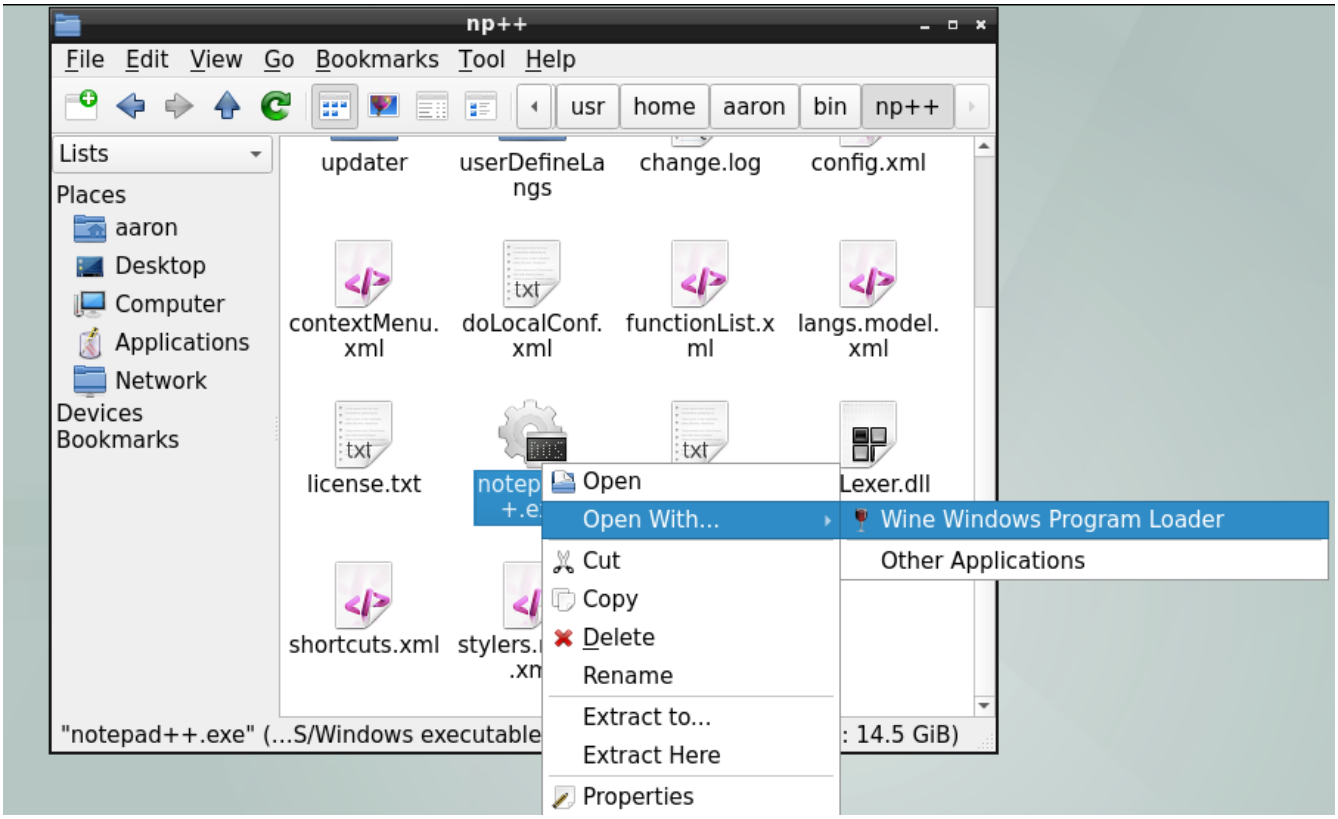
Il est aussi possible de fournir le chemin complet vers l'exécutable afin de l'utiliser dans un script, par exemple:

```
% wine /home/user/bin/program.exe
```

11.4.2. Lancer un programme WINE depuis une interface graphique

Après l'installation de WINE, les environnements graphiques doivent être configurés pour associer les fichiers exécutables Windows® (.EXE) avec WINE. Il sera ensuite possible de parcourir le système avec un gestionnaire de fichiers, puis de lancer une application Windows® de la même manière que n'importe quel autre programme (avec un clic ou en double-cliquant selon la manière dont est configurée l'interface graphique).

Sur la plupart des environnements de bureau, il suffit de vérifier que l'association est correcte en faisant un clic droit sur le fichier, puis de chercher une option de lancement correspondante dans le menu. Une des options (normalement celle par défaut) devrait être lancer avec **Wine - Chargeur de programmes Windows**, comme dans la capture d'écran ci-dessous:



Dans l'éventualité où le programme ne se lancerait pas comme escompté, essayez de le lancer depuis un terminal afin de voir si un éventuel message d'erreur apparaît, vous donnant ainsi un indice pour débloquer la situation. Dans le cas où WINE ne serait pas l'application par défaut pour ouvrir les fichiers .EXE après l'installation, veuillez vérifier les associations MIME pour cette extension de fichier dans l'environnement de bureau courant, l'interface système ou bien le gestionnaire de fichiers.

11.5. Configurer WINE après installation

Après avoir compris ce qu'était WINE et comment il fonctionne dans les grandes lignes, la prochaine étape consiste savoir l'utiliser de manière efficiente sur FreeBSD et de s'habituer à ses configurations. Ce qui va suivre détaillera le concept clé de *préfixe WINE*, et comment il est utilisé pour contrôler la façon dont les applications fonctionnent via WINE.

11.5.1. Les préfixes WINE

Un *préfixe* WINE est un répertoire, il se trouve généralement (par défaut) ici: $HOME/.wine mais peut aussi se situer ailleurs. Le préfixe est un ensemble de configurations et de fichiers utilisés par WINE pour configurer et utiliser l'environnement Windows® dont a besoin une application donnée. Par défaut, une installation toute fraîche de WINE va mettre en place la structure suivante lors de la première utilisation par un utilisateur:

- .update-timestamp: contient la date de la dernière modification de file /usr/share/wine/wine.inf. WINE utilise cela pour déterminer si un préfixe n'est plus à jour et le met à jour automatiquement si besoin.
- dosdevices/: contient la correspondance entre les ressources de Windows® et les ressources du système hôte (FreeBSD) afin de rendre possible les interactions entre les deux systèmes. Par

exemple, après une nouvelle installation de WINE, ce répertoire devrait contenir au moins deux éléments permettant l'accès au système de fichiers de FreeBSD en utilisant le modèle de Windows®, c'est-à-dire avec les lecteurs associés à des lettres:

  - c:@ : un lien vers drive_c décrit juste après.
  - z:@ : un lien vers le répertoire racine du système hôte.

- drive_c/: émule le disque principal d'un système Windows® (c'est-à-dire: C:). Il contient une arborescence de répertoires et fichiers imitant celui d'un système Windows® standard. Un préfixe WINE fraîchement créé devrait contenir les répertoires Windows® 10 comme *Users* et *Windows* qui contiennent le système d'exploitation lui-même. Par la suite, les applications qui seront installées au sein de ce préfixe se situeront soit dans *Program Files* ou *Program Files (x86)*, en fonction de leurs architectures respectives.
- system.reg: Ce fichier de registres contient les informations sur l'installation de Windows®, qui est dans le cas de WINE, l'environnement se trouvant dans drive_c.
- user.reg: Ce fichier de registres contient les configurations personnelles de l'utilisateur courant, générées par divers programmes ou bien via l'utilisation de l'éditeur de registres.
- userdef.reg: Ce fichier de registres comprends un ensemble de configurations par défaut pour les utilisateurs nouvellement crées.

11.5.2. Créer et utiliser un préfixe WINE

Alors que WINE créera par défaut un préfixe dans le répertoire utilisateur $HOME/.wine/, il est possible de mettre en place plusieurs préfixes. Il existe plusieurs raisons de procéder ainsi:

- La raison la plus courante à cela est d'émuler différentes versions de Windows®, en fonctions des besoins en compatibilité de divers logiciels.
- Il est également courant de rencontrer certaines applications ne fonctionnant pas correctement dans un environnement WINE par défaut, nécessitant ainsi une configuration spéciale. Il est généralement pratique d'isoler ce genre de programmes dans leur propre préfixe taillé sur mesure, de cette manière cela n'impactera pas le fonctionnement d'autres applications Windows®.
- De façon similaire, cela peut aussi servir dans l'optique de tests. En effet, on peut très bien dupliquer le préfixe par défaut pour réaliser divers tests de compatibilité sans risquer de compromettre le préfixe principal.

Pour créer un préfixe depuis le terminal, tapez la commande suivante:

```
% WINEPREFIX="/home/username/.wine-new" winecfg
```

Ce qui lancera l'utilitaire de configuration des préfixes `winecfg` (nous verrons ceci de façon plus approfondie dans la section ultérieure). En définissant un chemin de répertoire pour la variable `WINEPREFIX`, un nouveau préfixe sera créé à cet endroit, à supposer qu'un préfixe ayant un nom identique ne se trouve pas déjà là.

En fournissant la même variable au programme principal de WINE, le logiciel Windows® s'exécutera au sein de ce nouveau préfixe :

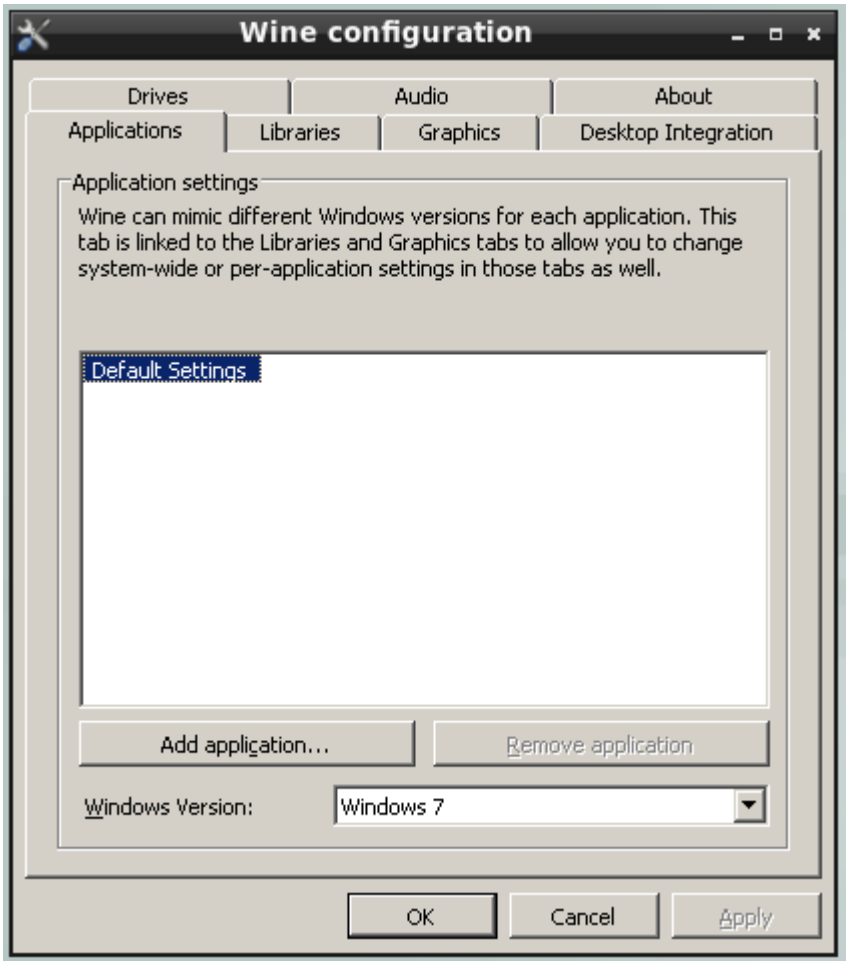
```
% WINEPREFIX="/home/username/.wine-new" wine program.exe
```

11.5.3. Configuration des préfixes WINE à l'aide de winecfg

Comme expliqué plus haut, WINE inclut `winecfg` un outil qui permet la configuration des préfixes depuis une interface graphique. Il comprend plusieurs fonctionnalités qui sont détaillées dans les sections suivantes. Quand `winecfg` est lancé depuis un préfixe, ou bien lancé en combinaison avec l'emplacement d'un préfixe dans la variable `WINEPREFIX`, cela autorisera la configuration de préfixe ainsi sélectionné comme décrit plus loin.

Les sélections faites dans l'onglet *Applications* affecterons la portée des changements effectués dans les onglets *Libraries* et *Graphics*, cela signifie que les changements apportés seront cantonnés aux applications sélectionnées. Voir Utiliser Winecfg sur le Wiki de WINE pour plus d'informations.

11.5.3.1. Applications



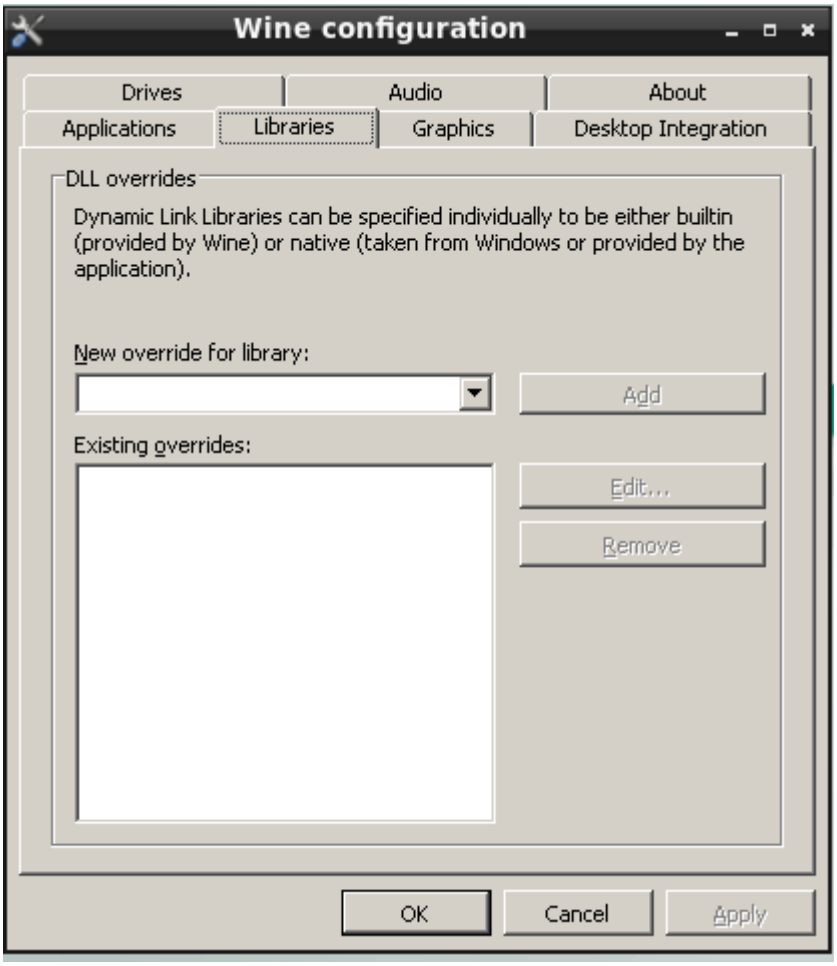
L'onglet *Applications* permet d'associer des programmes avec une version particulière de Windows®. Au premier démarrage de WINE, cet onglet contiendra simplement une seule entrée: *Default Settings*. Cela correspond à toutes les configurations par défaut du préfixe, cette entrée (comme l'implique le bouton *Remove application* désactivé) ne peut être pas supprimée du préfixe.

Mais, des applications additionnelles peuvent être ajoutées en suivant le procédé ci-dessous:

1. Cliquez sur le bouton *Add application*;

2. Utilisez la fenêtre qui apparaît alors pour sélectionner l'exécutable du programme voulu;
3. Sélectionnez la version de Windows® qui sera utilisée pour le programme sélectionné.

11.5.3.2. Bibliothèques (onglet *Libraries*)



WINE fourni par défaut un ensemble de bibliothèques open source reproduisant les mêmes fonctionnalités que leurs équivalent Windows®. Cependant, comme vu précédemment dans ce chapitre, le projet WINE fait en sorte de s'adapter au rythme des mise à jour de ces bibliothèques. De ce fait, les versions fournies avec WINE peuvent ne pas disposer de certaines fonctionnalités attendues par les programmes Windows® les plus récents.

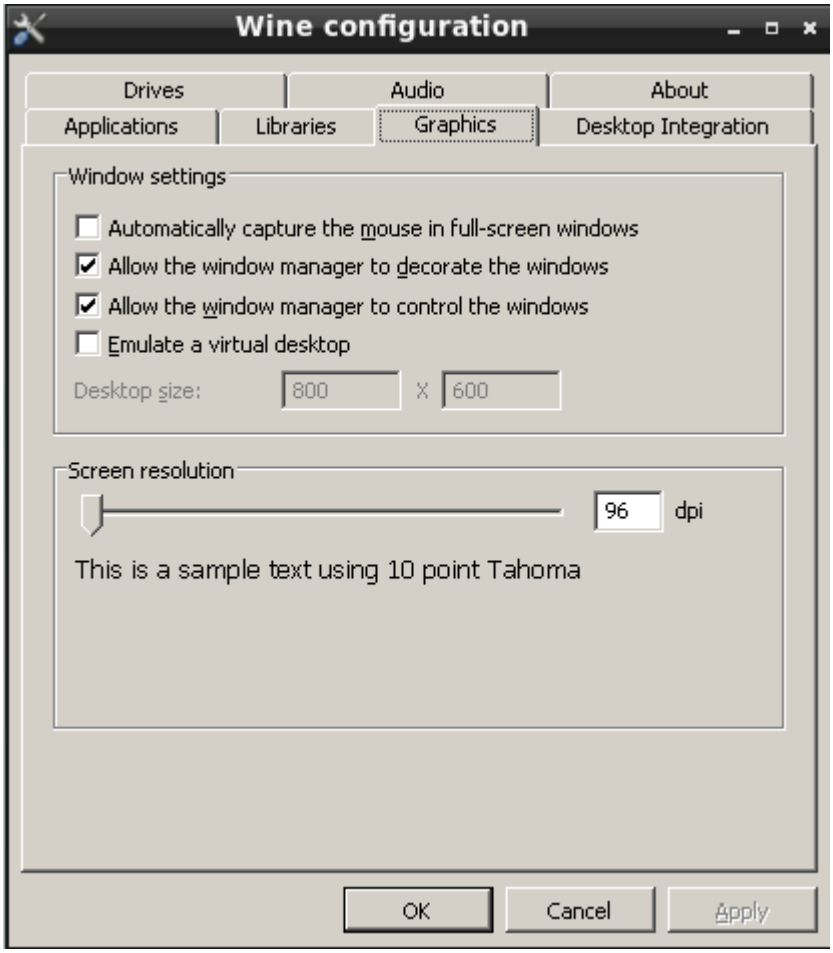
Il est toutefois possible, grâce à `winecfg`, de remplacer spécifiquement les bibliothèques de bases de WINE, tout particulièrement si une installation de Windows® est disponible sur la machine hôte. Pour chaque dépendance ayant besoin d'être remplacée, il suffit de procéder comme indiqué en dessous:

1. Ouvrez le menu déroulant *New override for library* et sélectionnez la bibliothèque à remplacer;
2. Cliquez sur le bouton *Add*;
3. Le nouveau remplacement apparaîtra dans la liste *Existing overrides*, notez les mentions *native, builtin* entre parenthèses;
4. Cliquez pour sélectionner une bibliothèque;
5. Cliquez sur le bouton *Edit*;
6. Servez-vous de la fenêtre de dialogue pour sélectionner la bibliothèque à utiliser à la place de

celle intégrée par défaut dans WINE.

Faites attention à bien sélectionner un fichier qui correspond à la version de la bibliothèque intégrée à WINE, dans le cas contraire, les programmes pourraient ne pas fonctionner comme attendu.

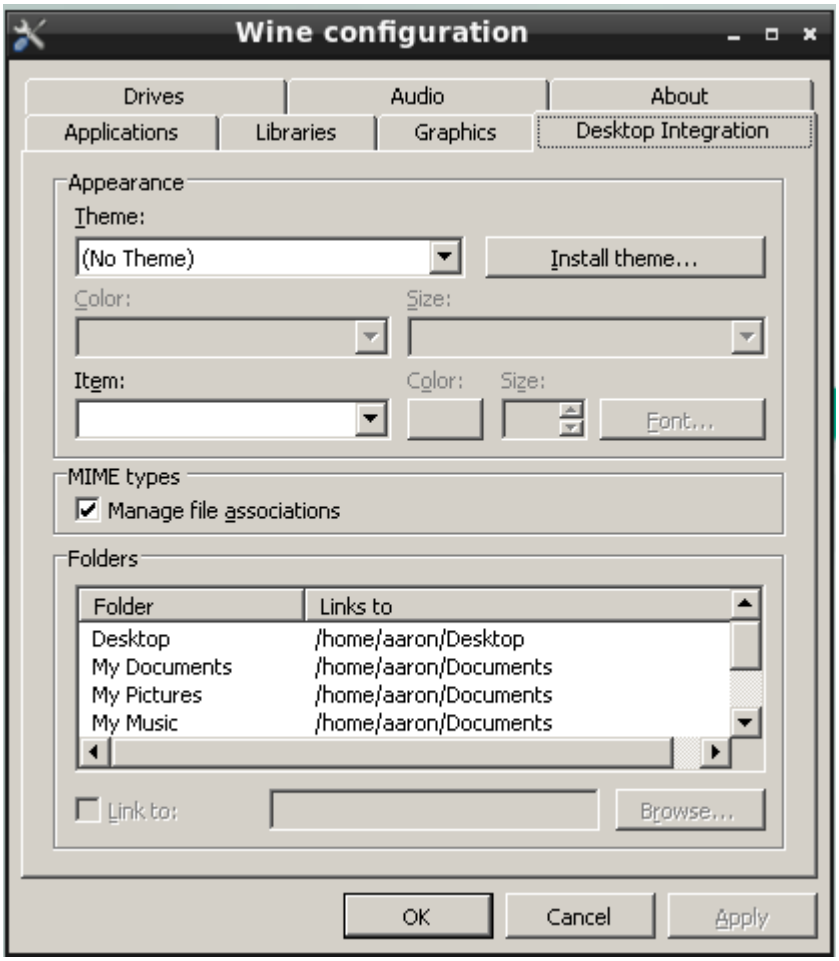
11.5.3.3. Configuration graphique (onglet *Graphics*)



L'onglet *Graphics* fournit des options permettant à la fenêtre du programme lancé via WINE de fonctionner avec des performances optimales sous FreeBSD:

- Capture automatique de la souris lorsqu'il s'agit d'une fenêtre en plein écran;
- Autoriser le gestionnaire de fenêtre de FreeBSD à prendre en charge la décoration des fenêtres, comme la barre de titre des applications WINE par exemple;
- Autoriser le gestionnaire de fenêtre de FreeBSD à contrôler les fenêtres des applications WINE, cela concerne les fonctionnalités telles que redimensionner une fenêtre;
- Créer un bureau virtuel émulé dans lequel seront lancés tous les programmes WINE. Une fois cette option cochée, il est possible de définir la taille de ce bureau virtuel via les zones de saisie en face de *Desktop size*;
- Définir la définition de l'écran pour les programmes lancés via WINE.

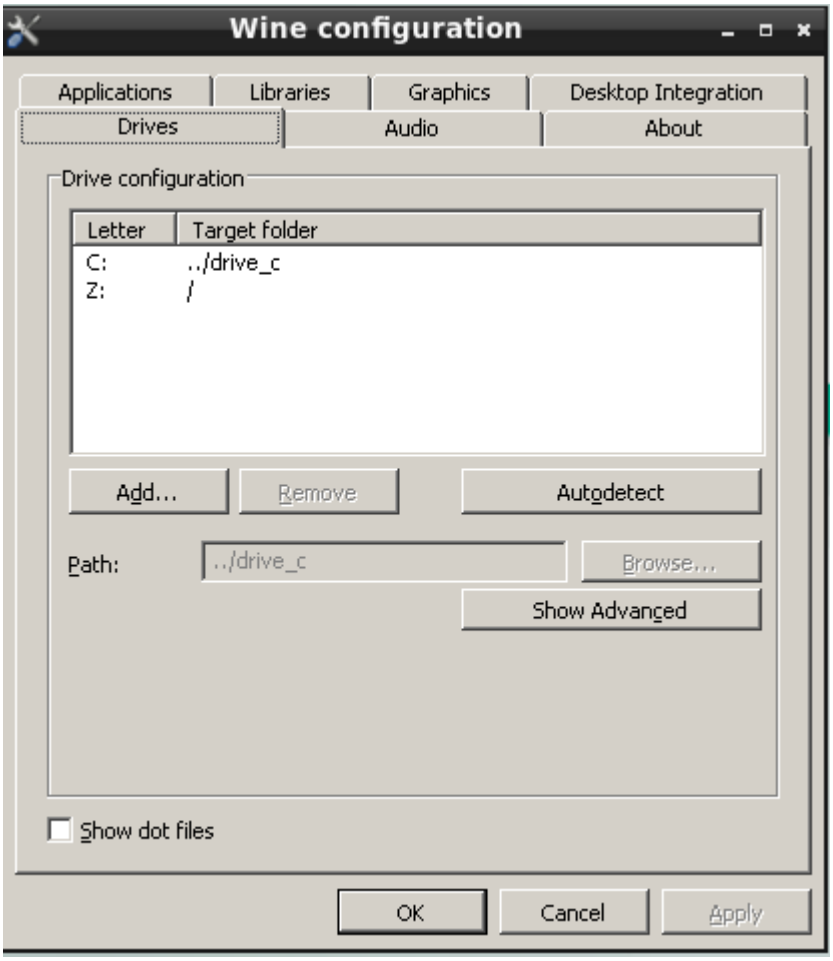
11.5.3.4. Intégration avec l'environnement de bureau (onglet *Desktop Integration*)



Cet onglet permet la configuration des éléments suivants:

- Les paramètres de thème et d'aspect visuel pour les programmes lancés via WINE;
- Si le sous-système WINE doit gérer les associations MIME (utilisé pour déterminer quelle application ouvre tel type de fichier particulier) de manière interne ou non;
- La correspondance des répertoires de la machine FreeBSD hôte avec les répertoires utiles au sein de l'environnement Windows®. Afin de changer les associations présentes par défaut, sélectionnez l'élément voulu et cliquez sur *Browse*, puis sélectionnez un répertoire dans la fenêtre qui apparaît.

11.5.3.5. Disques (onglet *Drives*)



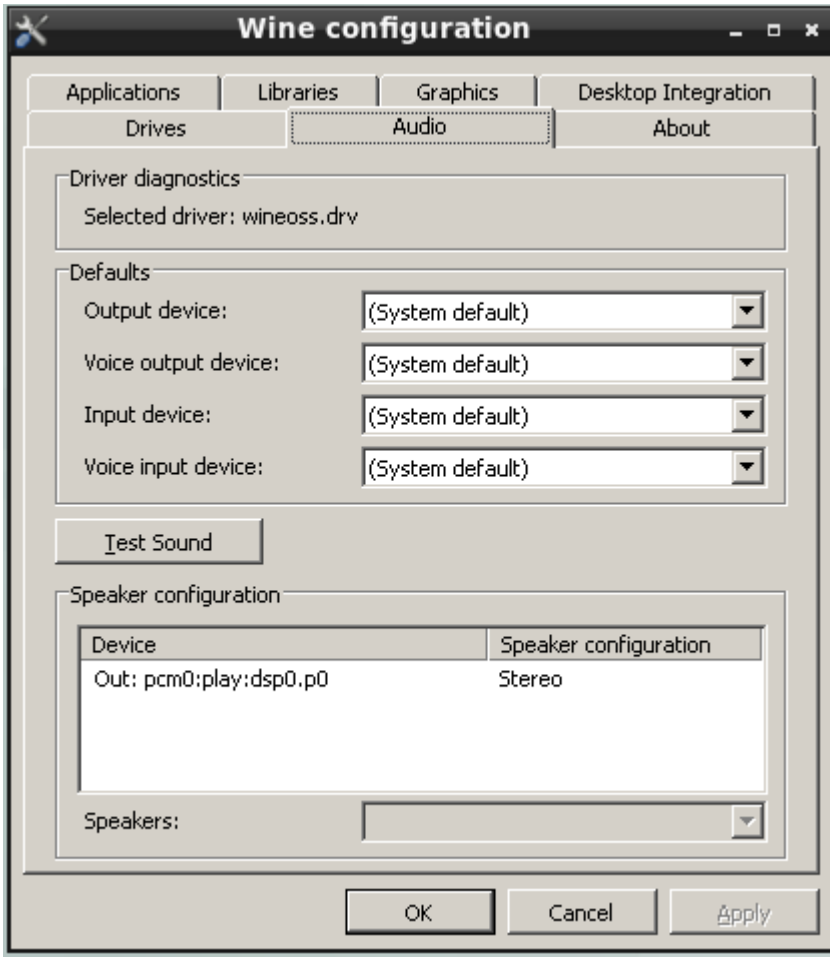
L'onglet *Drives* permet de créer un lien d'un répertoire du système hôte FreeBSD vers une lettre de lecteurs de l'environnement Windows®. Les valeurs par défaut devraient être familières, car elles affichent le contenu de dosdevices/ dans le préfixe WINE courant. Les changements effectués dans cet onglet se répercuteront dans dosdevices, et les liens correctement formatés présents dans ce répertoire apparaîtront dans cet onglet également.

Pour créer une nouvelle entrée, par exemple pour un CD-ROM (monté dans /mnt/cdrom), il suffit réaliser les étapes suivantes:

1. Cliquez sur le bouton *Add*;
2. Dans la nouvelle fenêtre, choisissez une lettre de lecteur disponible;
3. Cliquez sur *OK*;
4. Remplissez la zone de saisie *Path* soit en tapant le chemin vers la ressource, soit en cliquant sur *Browse* pour sélectionner la ressource en question.

Par défaut, WINE détecte le type de ressource liée, mais cela peut être changé manuellement si besoin. Voir la section correspondante dans le Wiki de WINE pour plus de détails sur les options avancées.

11.5.3.6. Audio



Cet onglet comprend des options configurable afin de router le son depuis les programmes Windows® vers le système de son natif de FreeBSD, notamment:

- La sélection du pilote;
- La sélection du périphérique audio par défaut;
- Un test audio.

11.5.3.7. A propos (onglet *About*)

Le dernier onglet contient des informations à propos du projet WINE, comme un lien vers le site Web. Cet onglet contient par ailleurs des champs de saisies pour les informations de l'utilisateur (complètement optionnel), bien que ces informations ne soient envoyées absolument nulle part au contraire d'autres systèmes d'exploitation.

11.6. Interfaces graphiques de gestion de WINE

Bien que WINE soit fourni avec `winecfg`, un outil de configuration par interface graphique, ce dernier sert surtout à: configurer dans les grandes ligne un préfixe WINE existant. Cependant, il existe des applications plus avancées qui pourront assister les installations de certaines applications de même qu'optimiser leur environnement WINE lié. La section qui suit, inclut une sélection des outils de ce type les plus populaires.

11.6.1. Winetricks

Le programme `winetricks` est un assistant multiplate-forme et complet pour WINE. Il n'est pas développé par le projet WINE, mais est maintenu par un groupe de contributeurs sur Github. Il contient "recettes" automatisées pour faire fonctionner un certain nombre d'applications communes sous WINE, en optimisant à la fois les paramètres et en installant certaines DLL automatiquement.

11.6.1.1. Installer winetricks

Pour installer winetricks sur FreeBSD en version pré-compilée, utilisez la commande suivante

(notez que cela nécessite que le paquet i386-wine ou bien i386-wine-devel soit installé, par conséquent ils seront installés automatiquement avec d'autres dépendances):

```
# pkg install i386-wine winetricks
```

Pour compiler `winetricks` depuis les sources, tapez les commandes suivantes:

```
# cd /usr/ports/emulators/i386-wine
# make install
# cd /usr/ports/emulators/winetricks
# make install
```

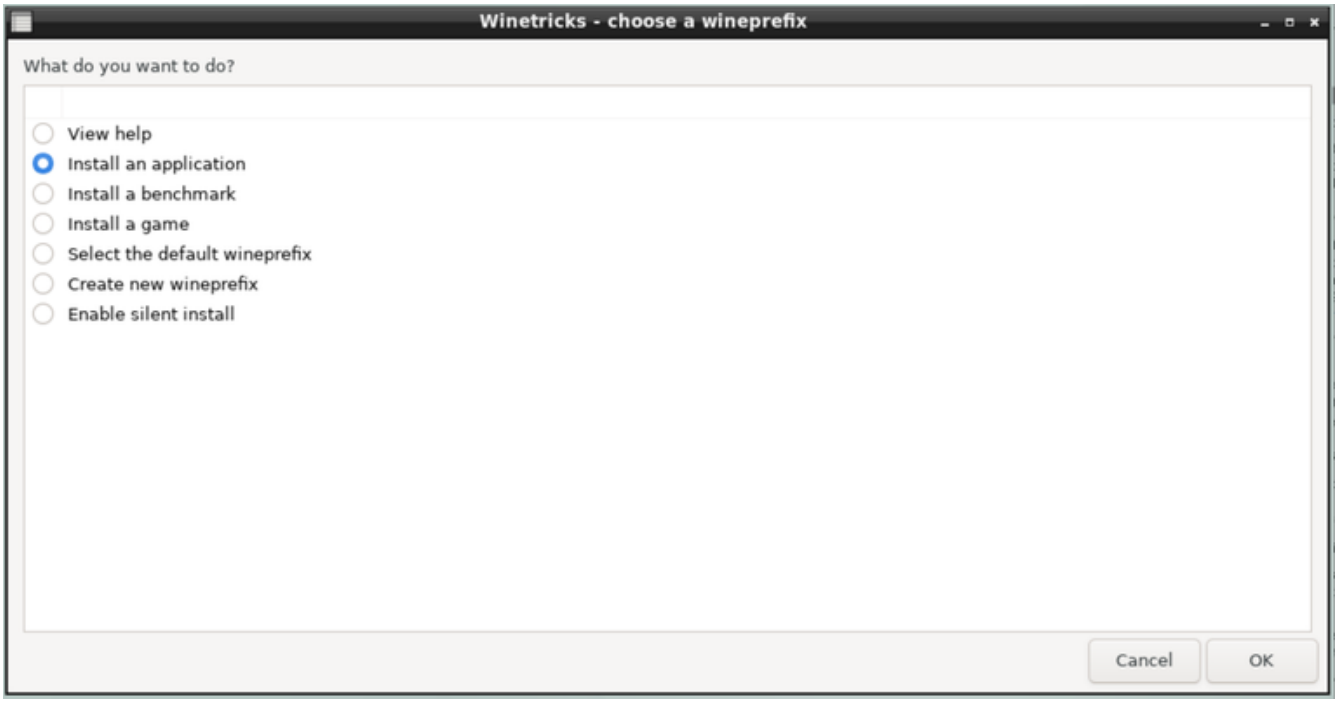
Si une installation manuelle est requise, référez-vous la page suivante pour des instructions: Github.

11.6.1.2. Utiliser winetricks

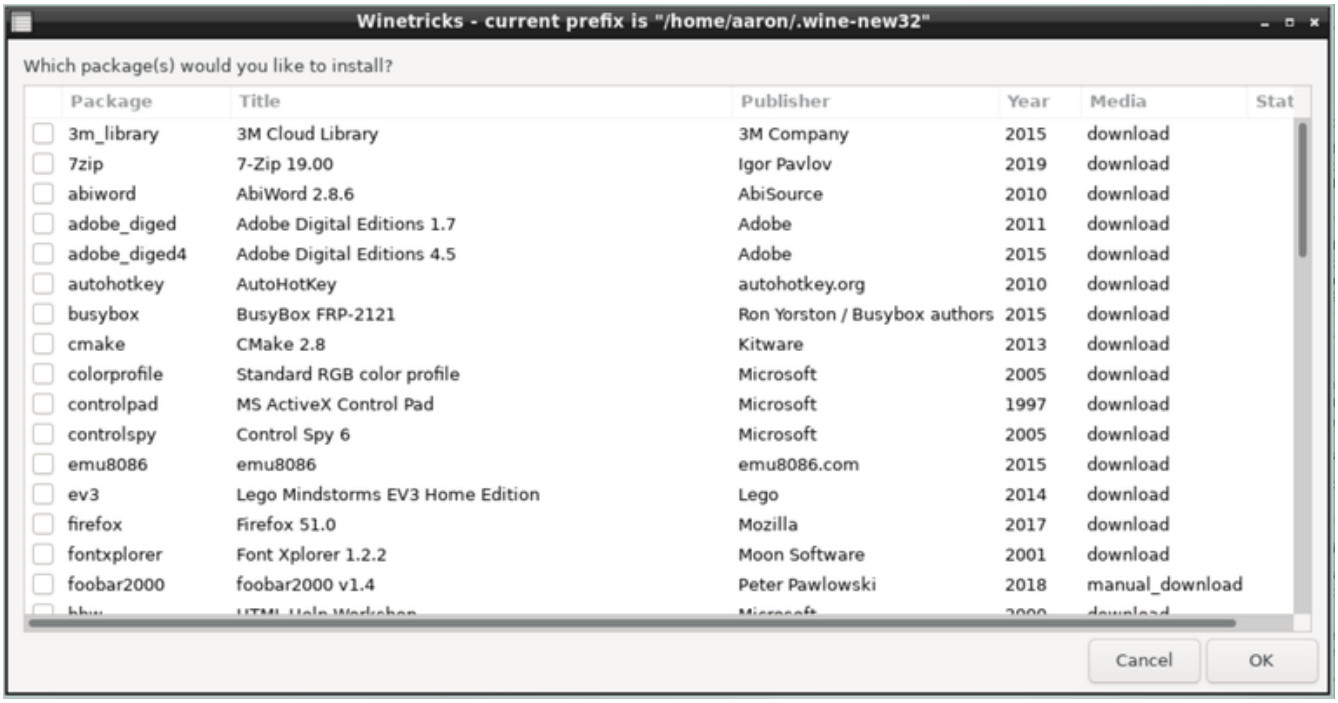
Lancer `winetricks` avec la commande suivante:

```
% winetricks
```

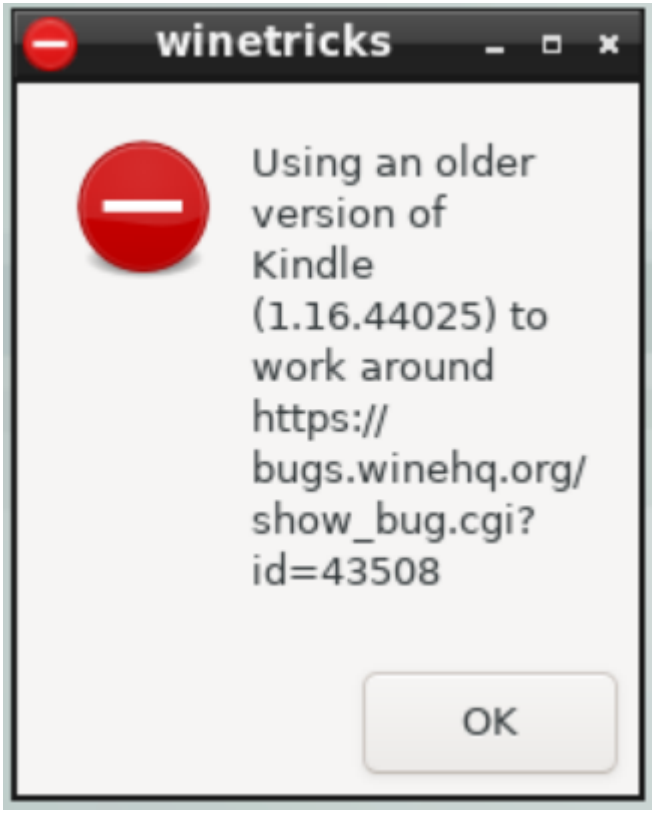
Notez qu'un préfixe WINE en 32 bits doit être présent pour lancer effectivement `winetricks`. Lancer `winetricks` aura pour effet de faire apparaître une fenêtre proposant un certain nombre de choix, comme celle-ci:



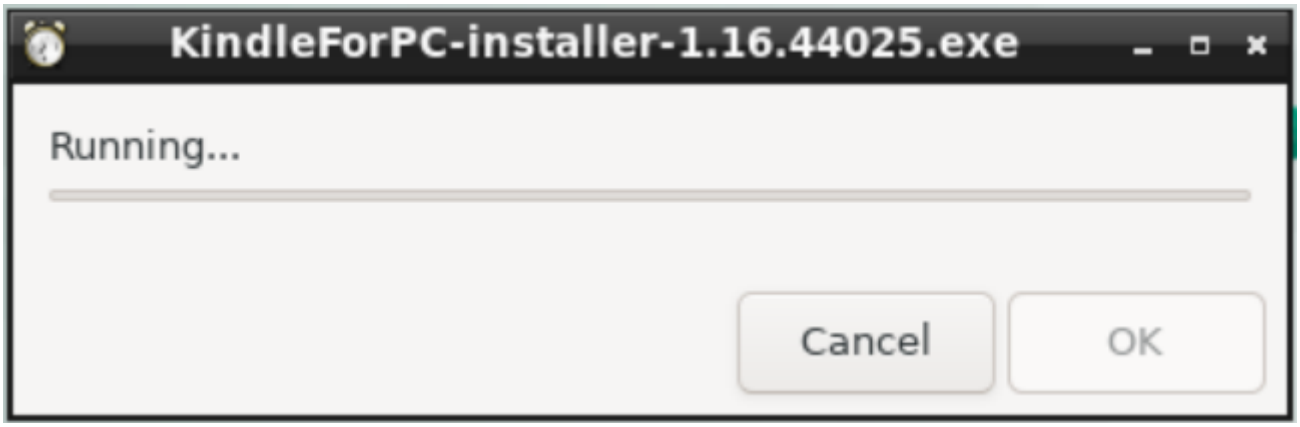
Sélectionner soit *Install an application*, soit *Install a benchmark*, ou encore *Install a game* affichera une liste avec une liste d'options prises en charge, comme ci-dessous pour les applications:



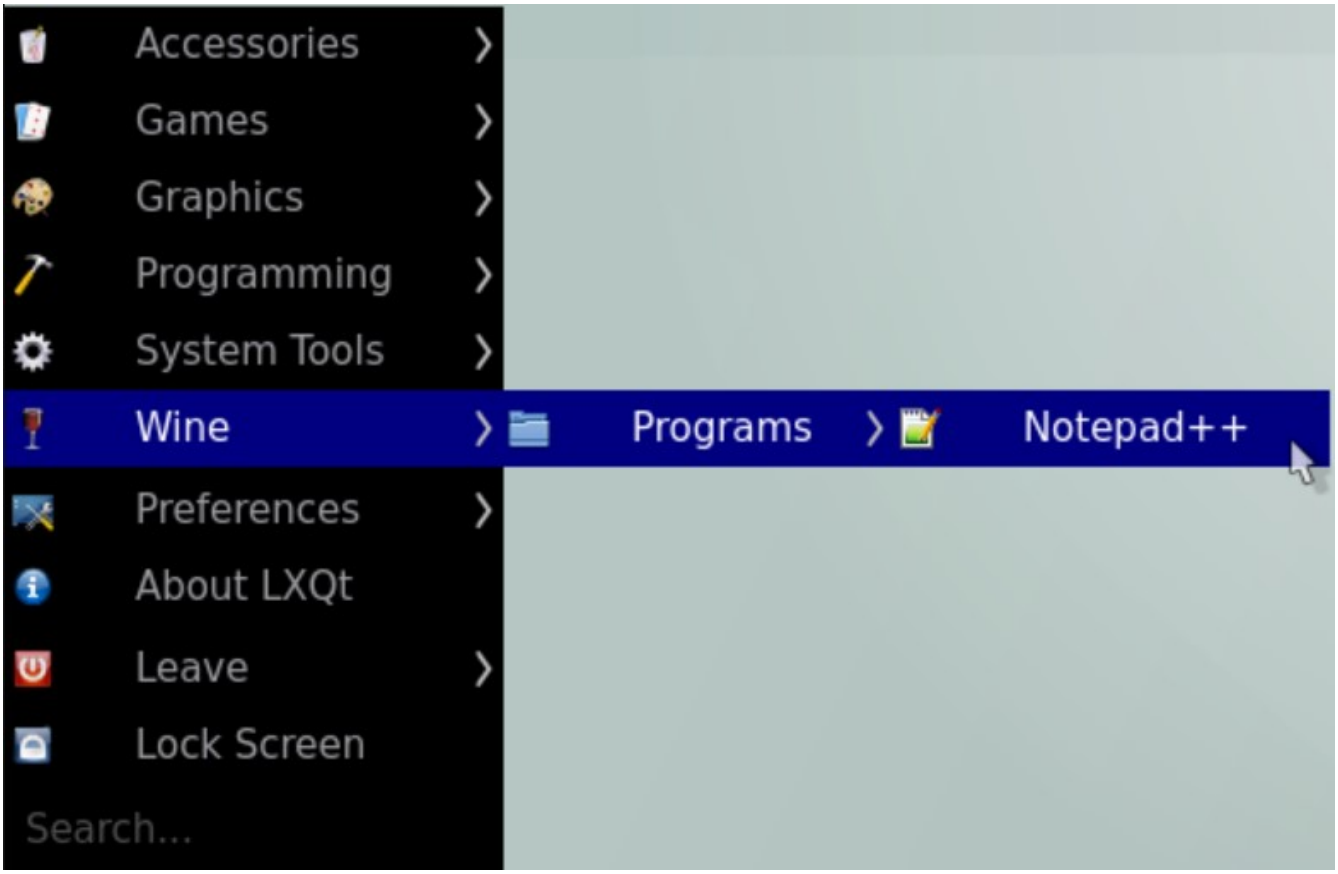
Sélectionner un ou plusieurs éléments et cliquer sur *OK* démarrera automatiquement leur(s) processus d'installation. Au début, certains messages qui ont l'air d'être des erreurs peuvent apparaître, mais il s'agit en fait d'informations et d'alertes mentionnant la manière de contourner certains problèmes éventuels pour certaines applications:



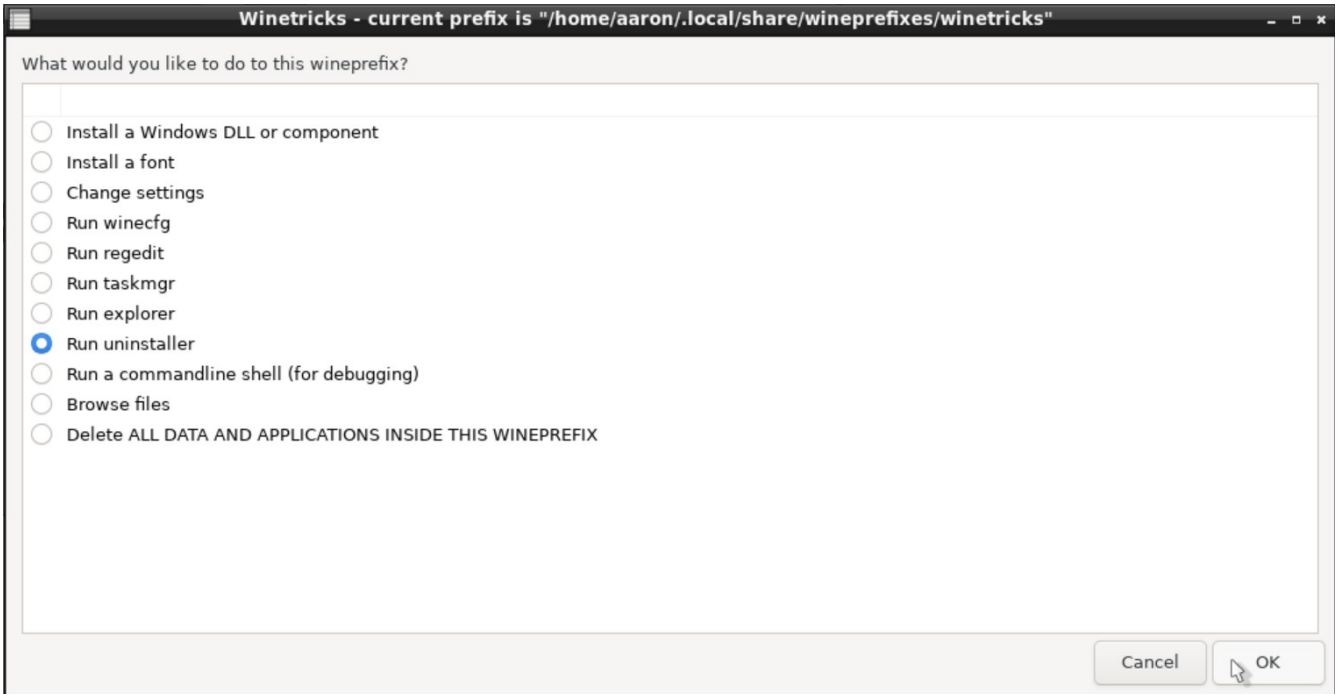
Une fois ces messages contournés, l'installation des applications en question sera effectivement lancée:



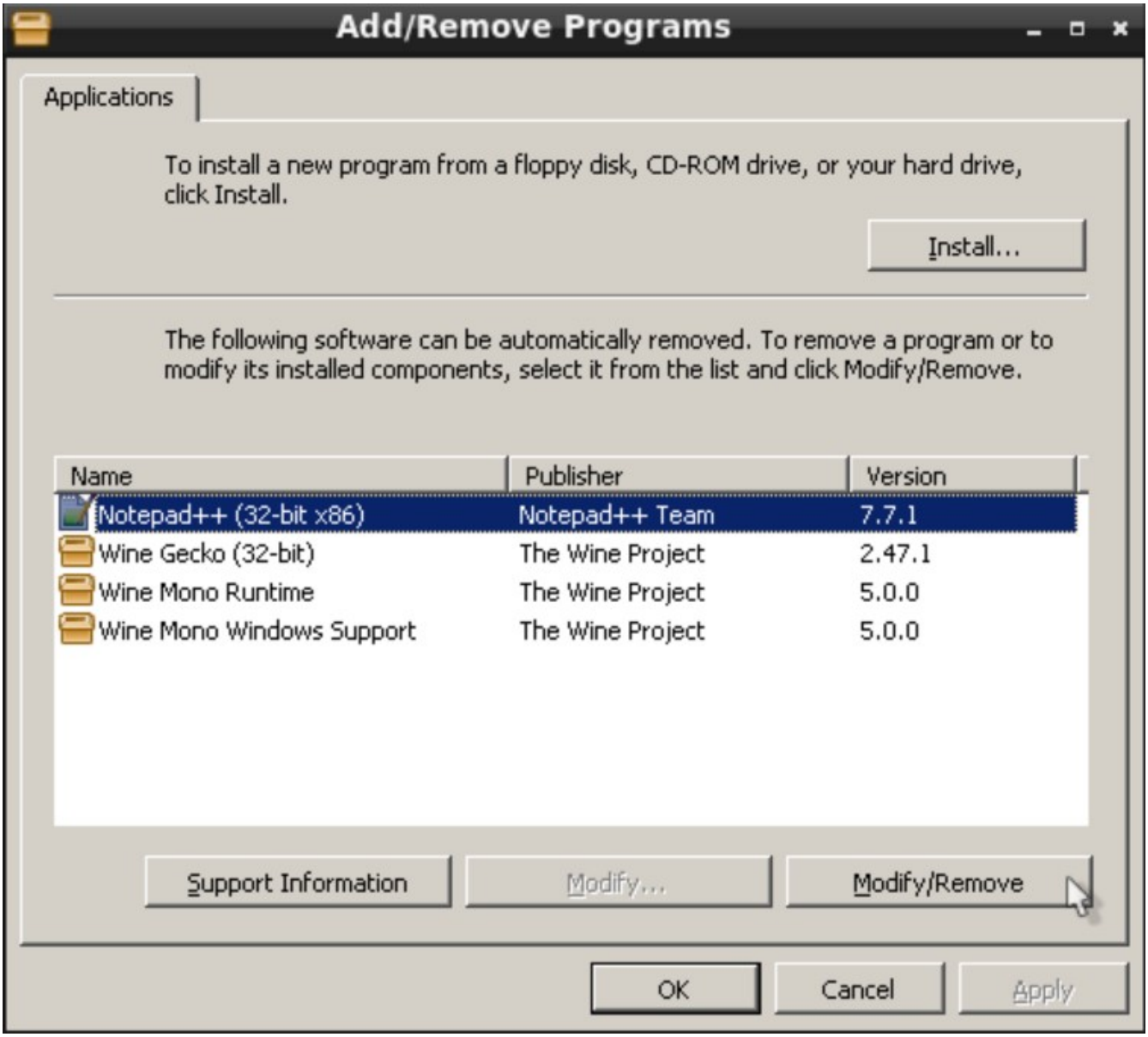
Une fois l'installation terminée, le nouveau logiciel Windows® devrait être disponible depuis le menu de l'environnement de bureau (comme ici, avec l'environnement de bureau LXQT):



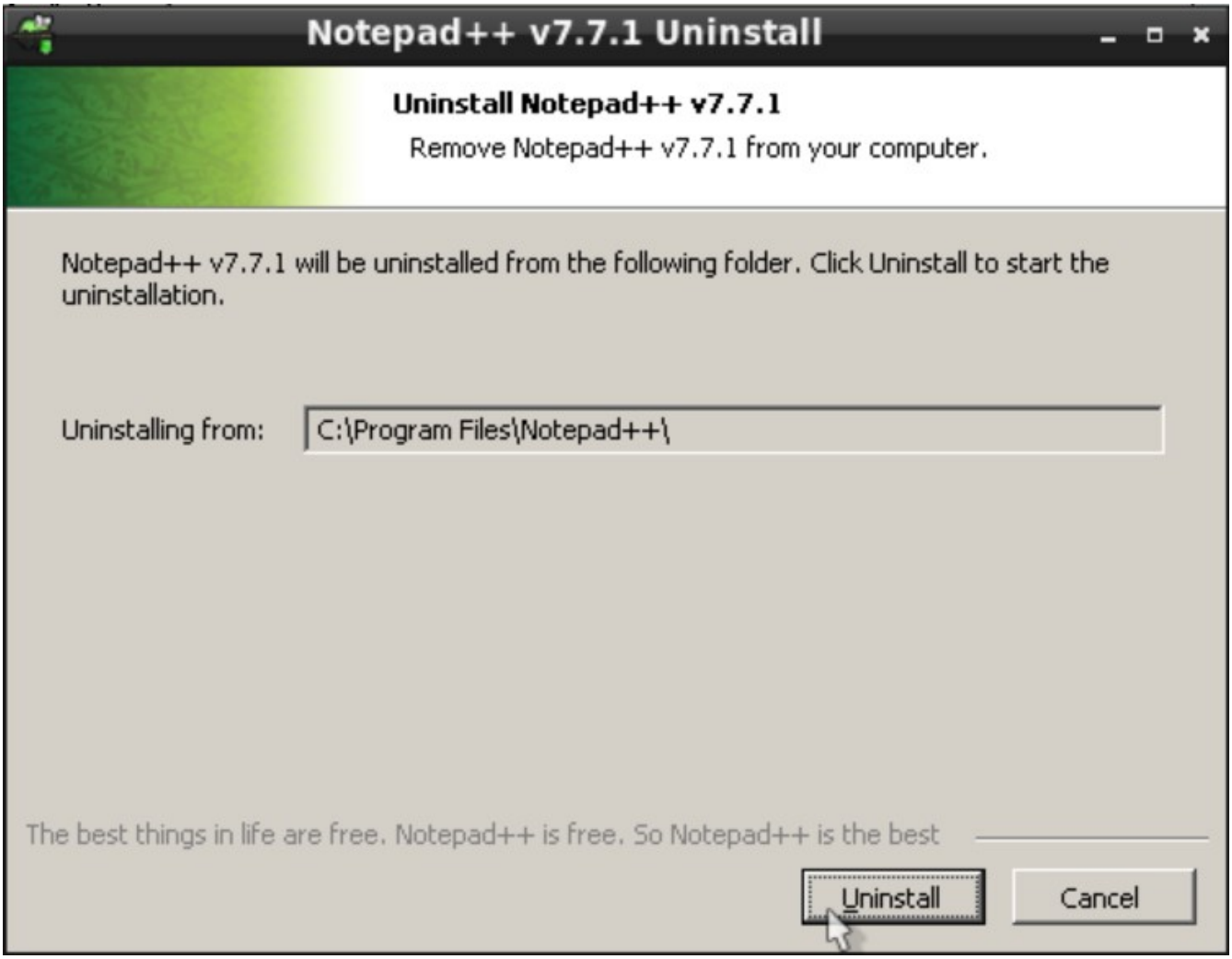
Pour supprimer l'application, lancez de nouveau `winetricks` et sélectionnez *Run an uninstaller*:



Une fenêtre Windows® apparaîtra pour lister tous les programmes et composants installés au sein de ce préfixe. Choisissez l'application à supprimer, puis cliquez sur le bouton *Modify/Remove*:



Cela lancera l'installateur interne de l'application en question, qui devrait également comprendre une option pour la désinstallation:



11.6.2. Homura

Homura est une application qui ressemble à `winetricks`, mais ce dernier s'inspire surtout de Lutris, qui est un système axé sur le jeu vidéo pour les plateformes Linux. Bien que cela soit centré sur le jeu vidéo, il y a aussi des applications n'étant pas des jeux qui sont disponibles pour l'installation au sein d'Homura.

11.6.2.1. Installer Homura

Pour installer la version compilée d'Homura, tapez la commande suivante:

```
# pkg install homura
```

Homura est aussi disponible via le catalogue de logiciels portés de FreeBSD. Cependant, au contraire de WINE ou `winetricks`, il se trouve dans la section *games* plutôt que dans la section *emulators*.

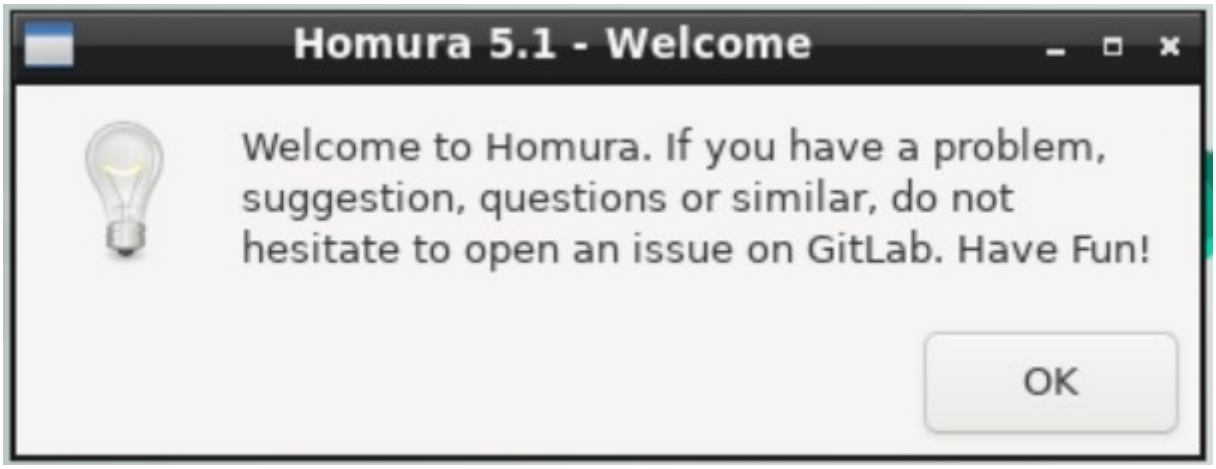
```
# cd /usr/ports/games/homura
# make install
```

11.6.2.2. Utiliser Homura

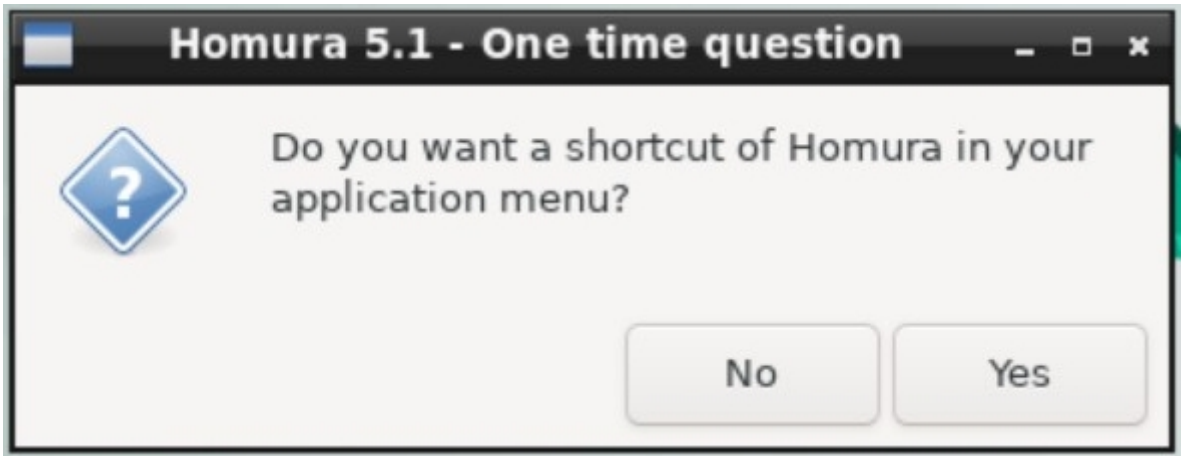
L'utilisation d'Homura est relativement similaire à celle de `winetricks`. Lorsque vous le lancez pour la première fois, via une ligne de commande (ou via un lanceur de votre environnement de bureau):

```
% Homura
```

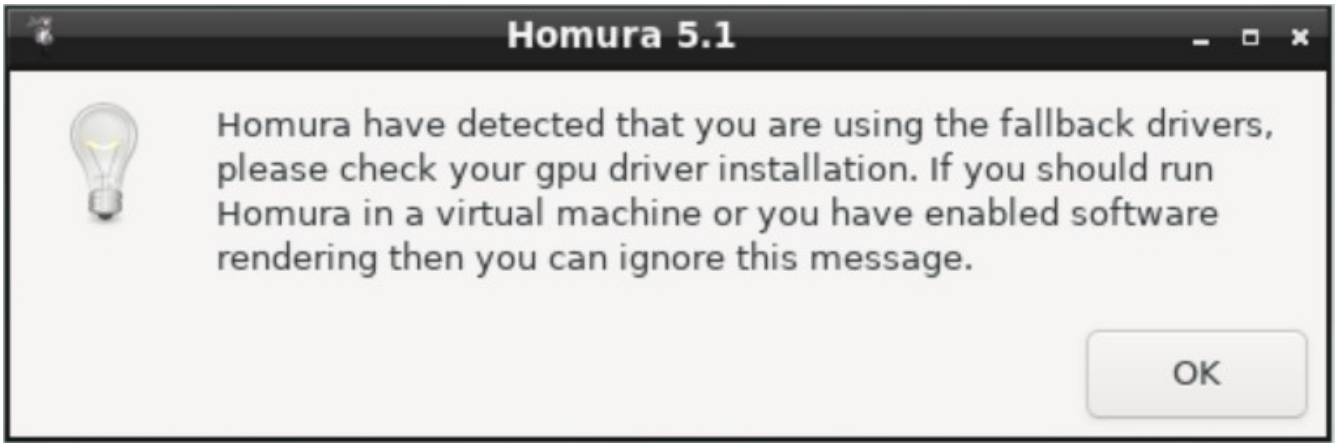
Cela devrait afficher le message d'accueil du programme. Cliquez sur *OK* pour continuer.



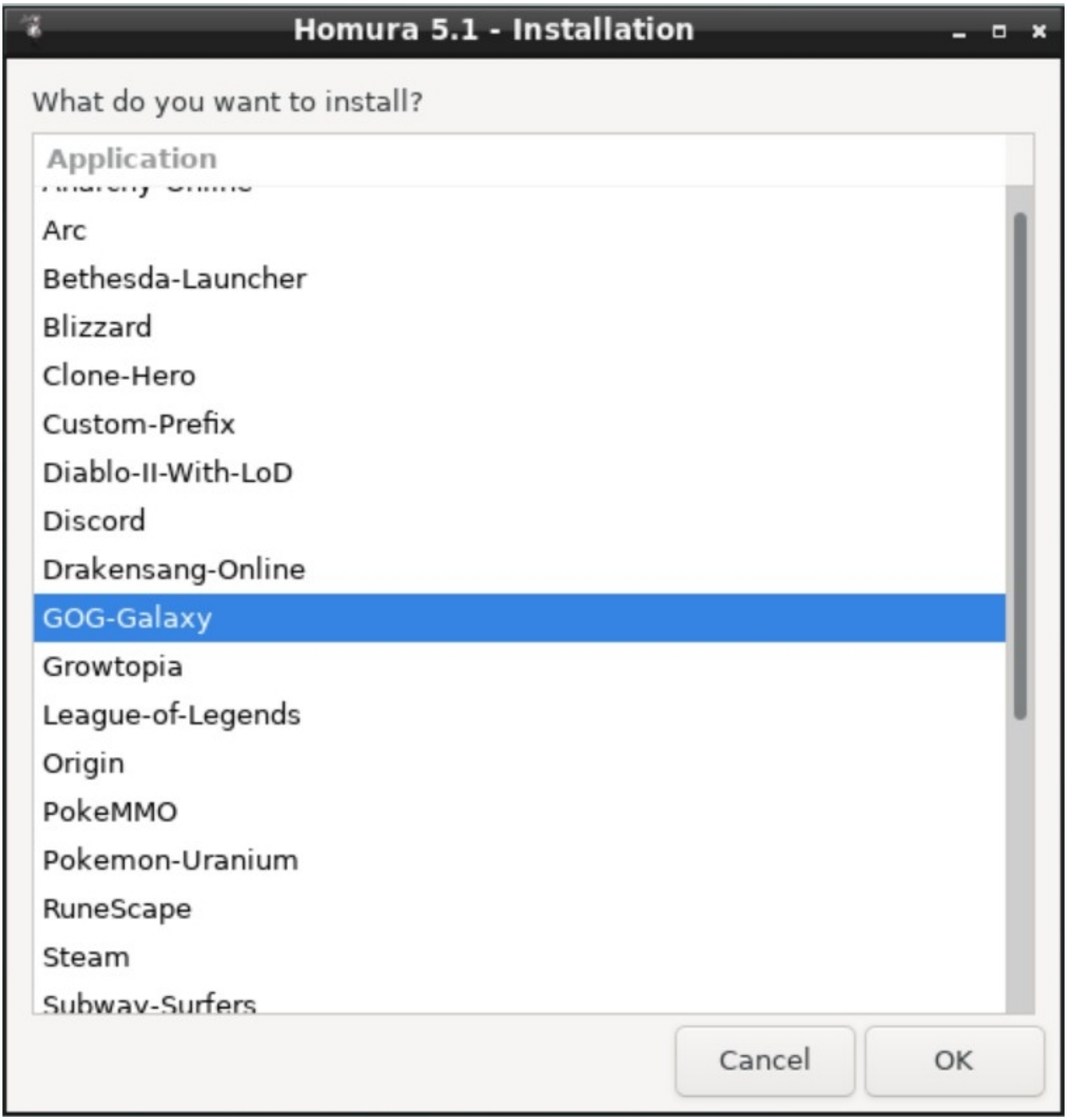
Le logiciel proposera la création d'un raccourci dans le menu des environnements de bureaux compatibles:



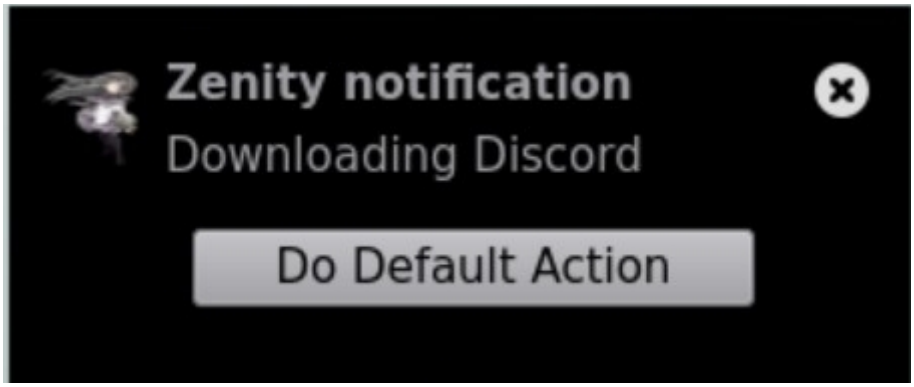
En fonction de la configuration de la machine FreeBSD hôte, il se peut qu'Homura affiche un message vous incitant à rapidement installer les pilotes natifs pour votre carte graphique.



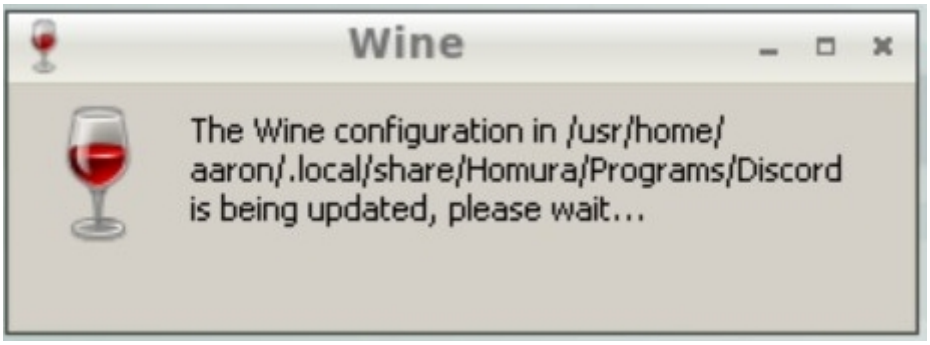
La fenêtre principale de l'application devrait désormais apparaître, elle correspond plus ou moins à une sorte de menu principal avec toutes ses options. Nombre de ces éléments sont identiques à ceux trouvés dans `winetricks`, néanmoins, Homura en propose également des nouveaux, comme une option utile pour ouvrir le répertoire des données (*Open Homura Folder*) ou de lancer un programme particulier au sein du préfixe (*Run a executable in prefix*).



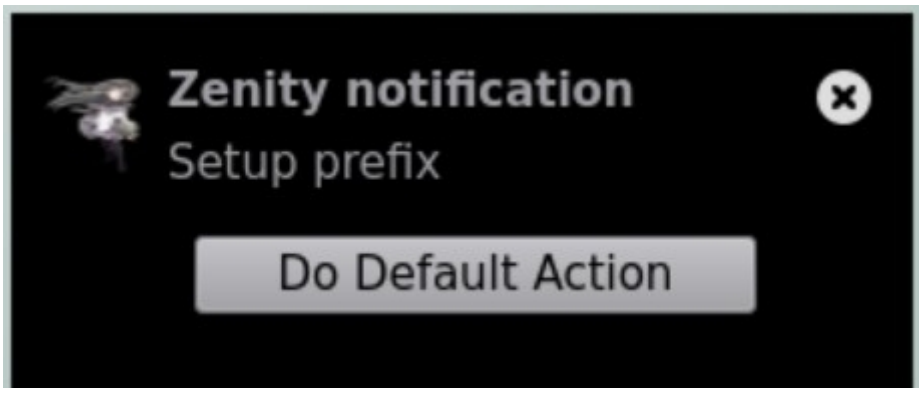
Pour choisir une application prise en charge et l'installer, sélectionnez *Installation*, puis cliquez sur *OK*. Cela affichera une liste d'applications qu'Homura pourra installer automatiquement. Choisissez-en une, puis cliquez sur *OK* pour en commencer l'installation.



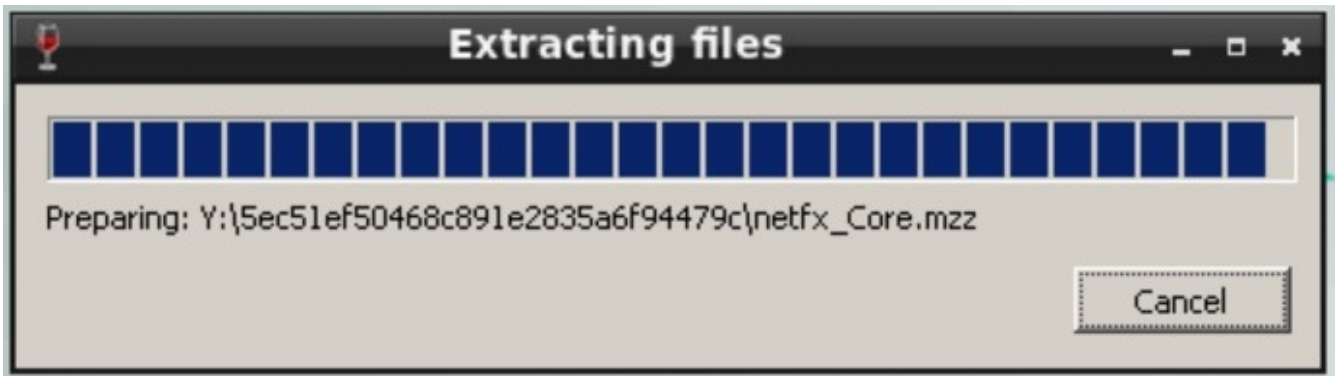
Homura commencera d'abord par télécharger l'application en question. Dans un environnement de bureau le prenant en charge, une notification est susceptible d'apparaître.



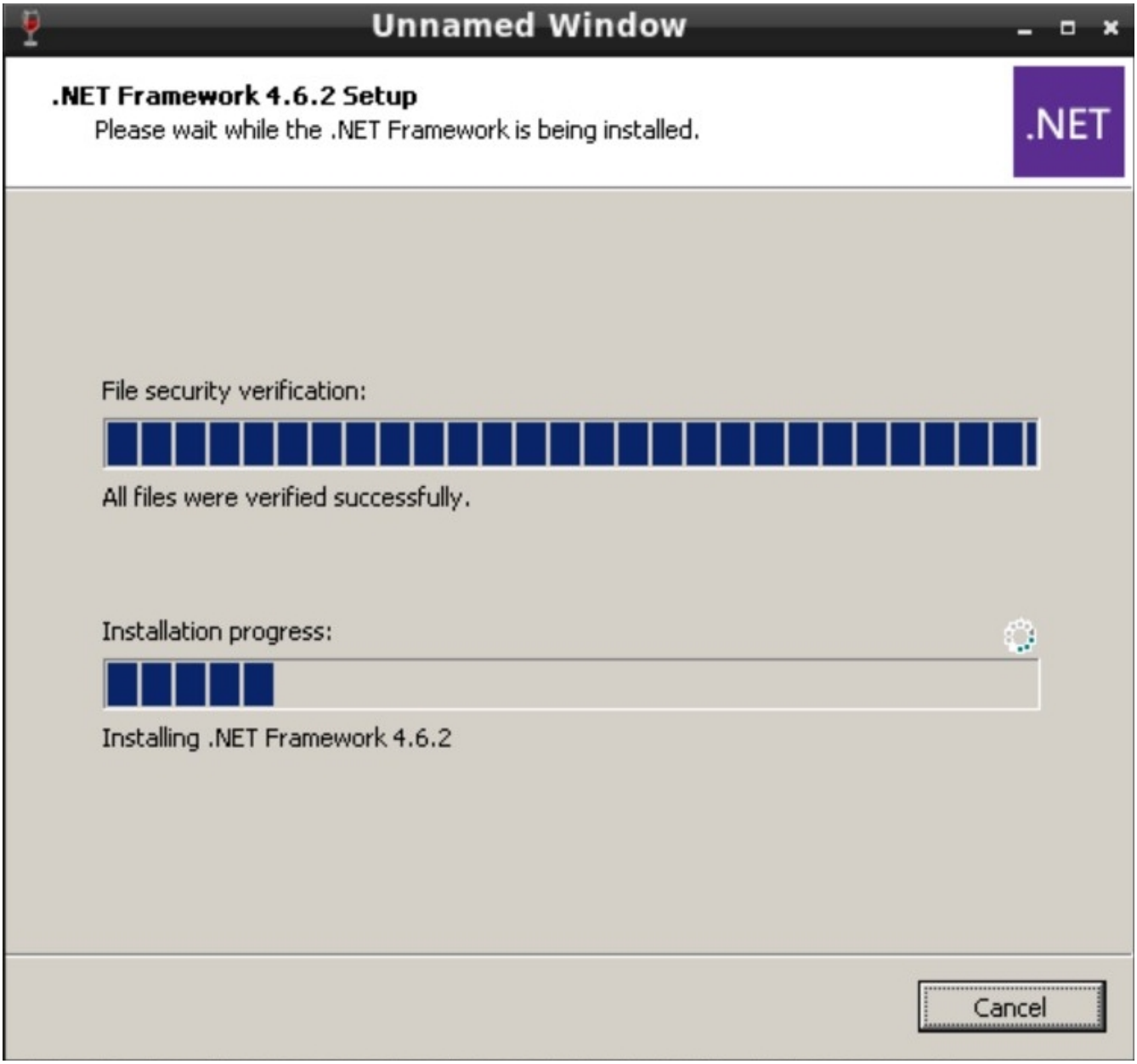
De plus, le programme se chargera de générer un nouveau préfixe pour l'application. Une fenêtre standard de WINE devrait apparaître avec ce message:



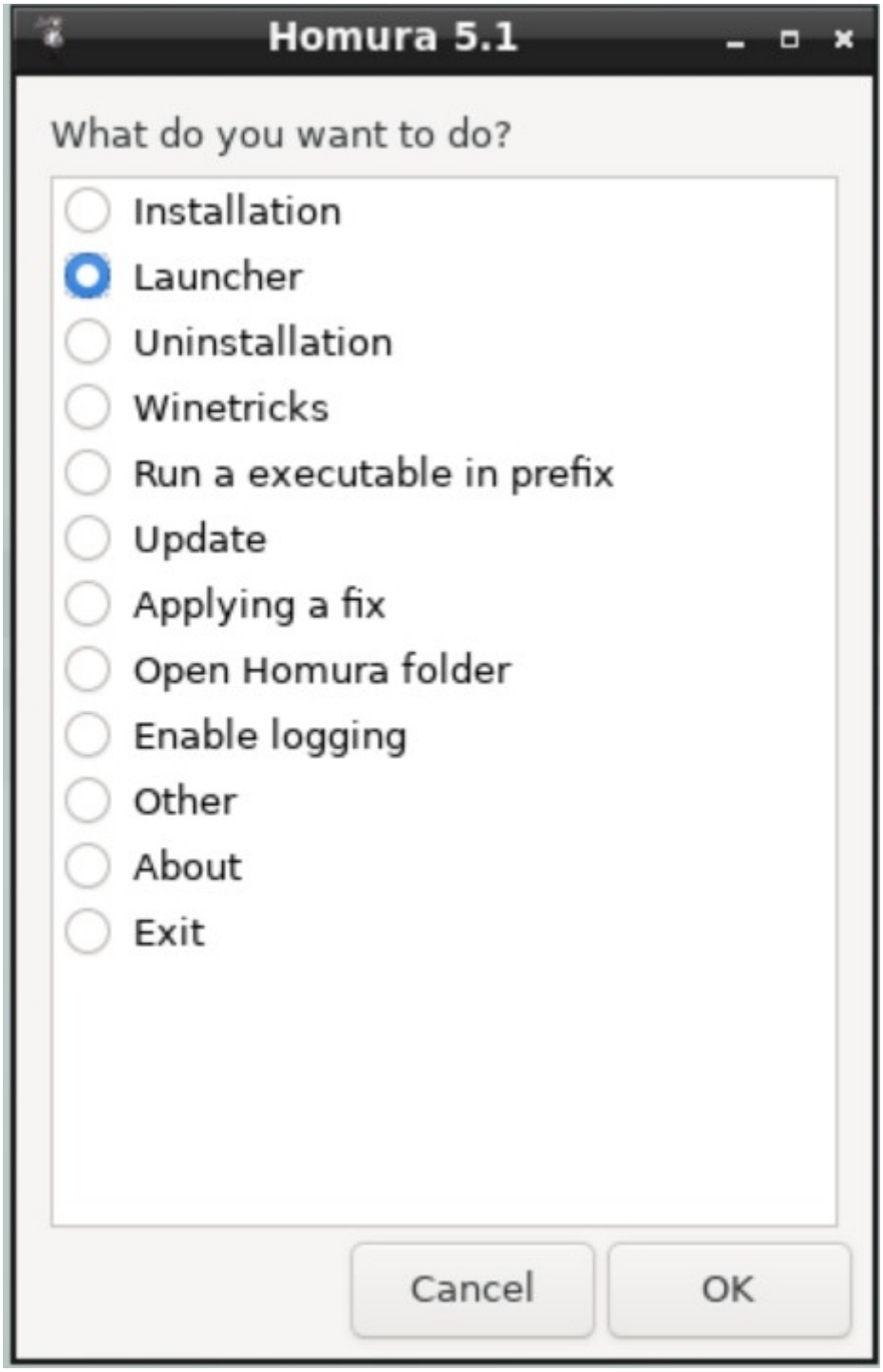
Ensuite, Homura se chargera d'installer tous les prérequis pour ledit programme. Ce qui peut impliquer le téléchargement et l'extraction d'un certain nombre de fichiers, les détails de ces actions apparaîtront dans une fenêtre comme ceci:



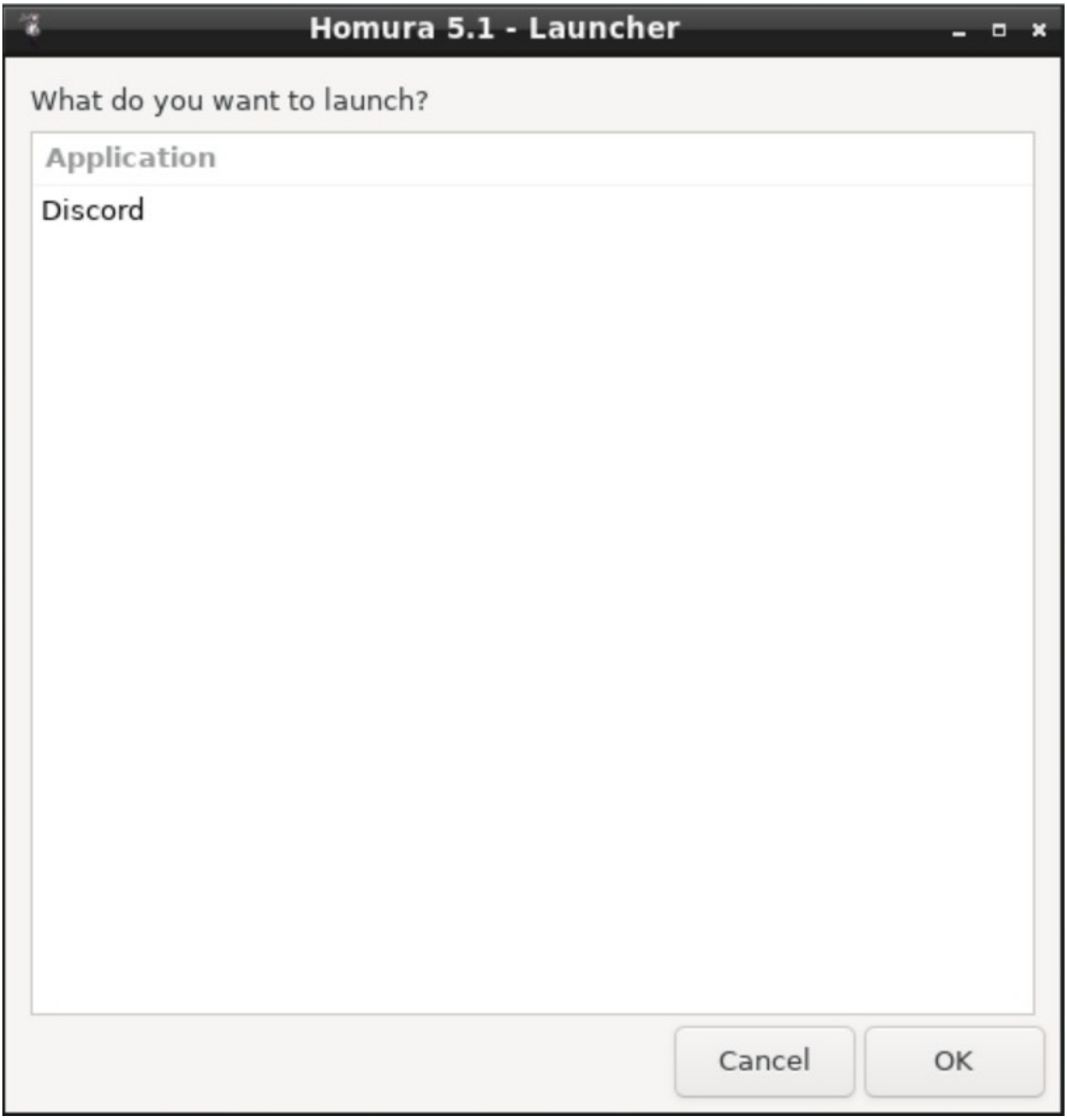
Les paquets téléchargés seront automatiquement extraits et installés en fonction des besoins.



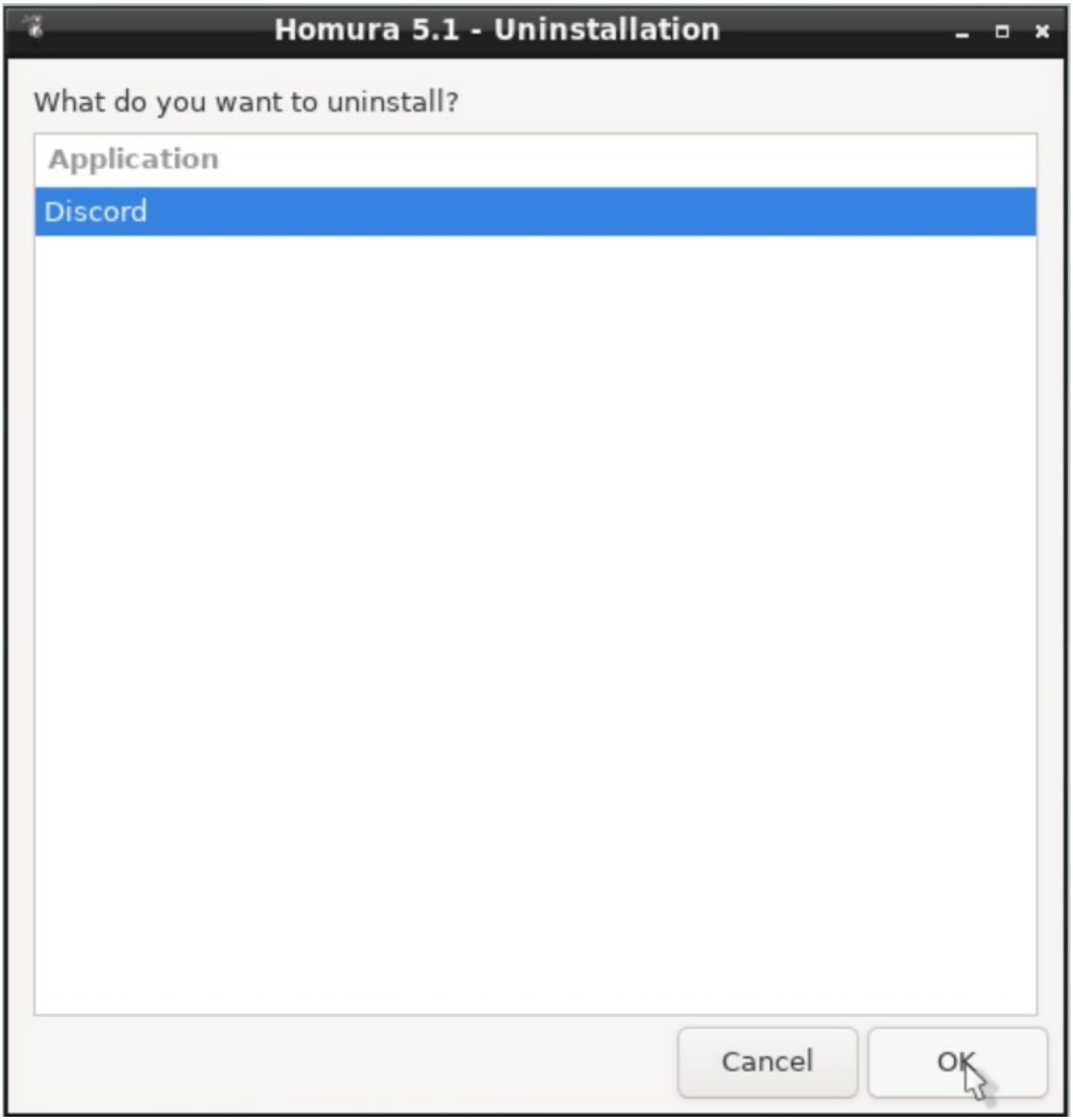
L'installation peut se solder par une simple notification de bureau ou un message dans le terminal, en fonction de la manière dont Homura a été lancé. Mais dans tous les cas, Homura devrait de nouveau afficher son écran principal. Afin de vérifier si l'installation a effectivement été menée à bien, choisissez *Launcher*, puis cliquez sur *OK*.



Cela affichera une liste des programmes installés.



Pour lancer le nouveau programme, sélectionnez le depuis la liste, puis cliquez sur *OK*. Afin de procéder à la désinstallation d'une application, choisissez *Uninstallation* depuis le menu principal, ce qui devrait afficher une liste similaire. Choisissez un programme à supprimer, puis cliquez sur *OK*.



11.6.3. Utiliser plusieurs outils graphiques de gestion

Il est à noter que l'installation d'un outil n'exclut pas l'utilisation d'un autre. Il est totalement possible, et même intéressant, d'avoir plusieurs outils installés en même temps, comme ils offrent le support de différents programmes.

Cependant, assurez-vous au préalable qu'ils n'accèdent pas au même préfixe WINE. Chacun de ces logiciels applique des solutions de contournement et appliquent des changements aux registres en fonction de problèmes connus au sein de WINE afin de permettre la bonne exécution d'un programme. Utiliser `wintricks` et Homura sur le même préfixe WINE pourrait compromettre ces changements et rendre ainsi certaines applications instables.

11.7. WINE sur un système FreeBSD avec plusieurs utilisateurs

11.7.1. Problèmes avec l'utilisation d'un préfixe WINE commun

Comme la plupart des systèmes d'exploitation de type UNIX®, FreeBSD est conçu de sorte que plusieurs utilisateurs puissent être connectés et peuvent travailler sur la même machine en même temps. D'un autre côté, Windows® est aussi un système multi-utilisateurs, mais dans le sens où il peut y avoir plusieurs comptes utilisateur sur un même système. Mais, l'objectif est qu'un seul utilisateur à la fois se serve de la machine physique (ordinateur portable ou fixe).

Les récentes versions grand public de Windows® ont amélioré l'utilisation du système dans le cas d'un scénario multi-utilisateurs. Mais le système reste largement structuré pour une utilisation mono-utilisateur. De plus, les mesures prises par le projet WINE afin de créer un environnement compatible Windows® impliquent, contrairement à aux applications FreeBSD (y compris WINE lui-même), qu'il s'approchera d'un environnement mono-utilisateur.

Ce qui veut dire, dans cette optique, que chaque utilisateur devra gérer son propre ensemble de configurations, ce qui est potentiellement une bonne chose. Cela dit, il peut être avantageux d'installer certaines applications une seule fois, notamment les plus lourdes, comme les suites de bureautique ou les jeux vidéo. Deux raisons évidentes pour vouloir procéder ainsi: la maintenance (les mises à jour ne devront être effectuées qu'une seule fois) et l'efficacité en termes d'espace disque (pas de duplications de fichiers).

Il existe deux stratégies dans le but de minimiser l'impact de plusieurs utilisateurs WINE sur le système.

11.7.2. Installer des applications sur un disque dur commun

Comme montré dans la section sur la configuration de WINE, ce dernier fourni la possibilité d'intégrer des disques supplémentaires à un préfixe donné. De cette manière, les applications peuvent être installées à un endroit commun, alors que les utilisateurs pourront toujours avoir un préfixe avec leurs configurations propres (selon le programme). C'est un bon choix, s'il y a peu d'applications devant être partagées entre les utilisateurs, et s'il y a des programmes qui n'ont besoin que de configurations minimes de leur préfixe pour leur permettre de fonctionner.

Les étapes pour procéder comme ceci sont les suivantes:

1. Premièrement, mettre en place un répertoire partagé sur le système avec lequel seront stockés les fichiers, comme /mnt/windows-drive_d/. Créer un nouveau dossier, cela est détaillé dans la page de manuel de mkdir(1).
2. Puis, définir les permissions pour ce nouveau répertoire afin d'autoriser l'accès uniquement aux utilisateurs voulus. Une manière de procéder est de créer un nouveau groupe, "windows" par exemple, ajouter les utilisateurs en question à ce groupe (voir la sous-section sur les groupes dans la section Gestion des comptes et des utilisateurs de ce manuel), puis définir les permissions du répertoire sur `770` (la section sur les permissions sous FreeBSD illustre ce processus).

3. Enfin, ajouter ce répertoire au préfixe de l'utilisateur en utilisant `winecfg` comme décrit plus haut, dans la section sur la configuration de WINE.

Une fois ceci terminé, les applications pourrons être installées à cet emplacement, et ensuite être lancées en utilisant la lettre de lecteur assignée (ou bien en utilisant le chemin standard façon UNIX®. Cependant, comme noté plus haut, un seul utilisateur devrait utiliser ces applications (qui pourraient accéder à des fichiers dans leur répertoire d'installation) à la fois. Il se peut que certaines applications présentent un comportement inattendu lorsqu'elles seront exécutées par un utilisateur qui n'en n'est pas le propriétaire, malgré le fait que ce dernier appartienne bien au groupe ayant les permissions "lecture/écriture/exécution" pour tout le répertoire.

11.7.3. Utiliser une installation commune de WINE

Si jamais beaucoup d'applications doivent être partagées, ou bien qu'elles nécessitent des réglages spéciaux pour fonctionner correctement, une autre approche peut être requise. Dans cette méthode, un autre utilisateur est créé tout spécialement dans le but de stocker les préfixes WINE et les applications installées. Chaque utilisateur voulu sera autorisé à lancer les programmes en tant que ce nouvel utilisateur en utilisant la commande sudo(8). Cela a pour résultat, que ces utilisateurs peuvent désormais lancer une application WINE comme ils le feraient en temps normal, cela agira simplement comme si cette dernière était lancée par l'utilisateur nouvellement crée, et donc utilisera le préfixe centralisé contenant les configurations ainsi que les programmes. Pour parvenir à cela, il faut suivre les étapes suivantes:

Créez un nouvel utilisateur avec la commande suivante en tant que `root`:

```
# adduser
```

Entrez le nom d'utilisateur (par exemple *windows*) et le nom complet ("Microsoft Windows"). Ensuite acceptez les options par défauts pour les questions restantes. Puis, installez l'utilitaire `sudo` en version pré-compilé avec la commande suivante:

```
# pkg install sudo
```

Une fois l'installation terminée, éditez /etc/sudoers comme ce qui suit:

```
# User alias specification

# define which users can run the wine/windows programs
User_Alias WINDOWS_USERS = user1,user2

# define which users can administrate (become root)
User_Alias ADMIN = user1

# Cmnd alias specification

# define which commands the WINDOWS_USERS may run
Cmnd_Alias WINDOWS = /usr/bin/wine,/usr/bin/winecfg
```

```
# Defaults
Defaults:WINDOWS_USERS env_reset
Defaults:WINDOWS_USERS env_keep += DISPLAY
Defaults:WINDOWS_USERS env_keep += XAUTHORITY
Defaults    !lecture,tty_tickets,!fqdn

# User privilege specification
root    ALL=(ALL) ALL

# Members of the admin user_alias, defined above, may gain root privileges
ADMIN ALL=(ALL) ALL

# The WINDOWS_USERS may run WINDOWS programs as user windows without a password
WINDOWS_USERS ALL = (windows) NOPASSWD: WINDOWS
```

Cela permet aux utilisateurs nommés dans la section *User_Alias* de lancer les programmes listés à la section *Cmnd Alias* en utilisant les ressources listées dans la section *Defaults* (sur l'affichage en cours d'utilisation) comme s'il s'agissait de l'utilisateur listé dans la dernière ligne du fichier. Autrement dit, les utilisateurs désignés comme *WINDOWS_USERS* peuvent lancer les applications WINE et `winecfg` comme étant l'utilisateur *windows*. De plus, cette configuration signifie que les utilisateurs membres de ce groupe n'auront pas à entrer le mot de passe pour l'utilisateur *windows*.

Ensuite, il faut donner l'accès à l'affichage pour l'utilisateur *windows*, sachant que c'est sous cet utilisateur que les programmes WINE seront lancés:

```
% xhost +local:windows
```

C'est une commande qui devrait être ajoutée à la liste des commandes lancées à la connexion ou au démarrage de l'environnement de bureau. Une fois que tout ceci est prêt, un utilisateur configuré comme un de `WINDOW_USERS` dans sudoers peut lancer les programmes en utilisant le préfixe en commun avec la commande suivante:

```
% sudo -u windows wine program.exe
```

Il faut noter cela dit, que si plusieurs utilisateurs accèdent à cet environnement partagé en même temps, cela présente toujours un risque. Cependant, il faut aussi garder en tête que cet environnement partagé peut contenir plusieurs préfixes WINE. De cette manière, un administrateur peut créer, tester et vérifier un ensemble de programmes, chacun dans son propre préfixe. Dans le même temps, un utilisateur peut jouer à un jeu pendant qu'un autre utilise une suite bureautique sans pour autant multiplier des installations redondantes.

11.8. WINE sur FreeBSD Foire Aux Questions

La section suivante détaille les questions posées fréquemment, les trucs et astuces, ou bien les problèmes souvent rencontrés avec WINE sur FreeBSD, avec leurs réponses respectives.

11.8.1. Installation et utilisation basique

11.8.1.1. Comment installer la version 32 bits et la versions 64 bits sur le même système?

Comme déjà mentionné, les paquets wine et i386-wine entrent en conflit s'ils sont installés normalement sur le même système. Néanmoins, plusieurs types d'installations peuvent être mis en place en utilisant des mécanismes comme chroots/jails, ou en compilant WINE directement depuis les sources (hors catalogue de logiciels portés de FreeBSD).

11.8.1.2. Peut-on utiliser un programme DOS sous WINE ?

Théoriquement oui, car ce sont des programmes en interfaces console comme nous l'avons vu plus haut. Cela dit, il existe une méthode plus adaptée à cela, il suffit d'utiliser DOSBox. Bien sûr, cela ne coûte rien d'essayer. Créez simplement un nouveau préfixe WINE, installez le programme et si cela ne marche pas, supprimez le préfixe.

11.8.1.3. Est-ce que le paquet emulators/wine-devel doit être installé pour pouvoir utiliser la version en développement de WINE à la place de la version stable?

Oui, cette version installe la version développement de WINE. Comme avec les versions 32 et 64 bits de WINE, la version développement ne peux pas être installée en même temps que la version stable sans mesures additionnelles.

Notez qu'il existait aussi une version "Staging" de WINE, contenant les mises à jour les plus récentes du projet. Cette version était disponible dans le catalogue de logiciels portés de FreeBSD, mais a depuis été supprimée. Cette version est toujours compilable depuis les sources cela dit.

11.8.2. Optimisation de l'installation

11.8.2.1. Comment les pilotes (de carte graphique par exemple) Windows® sont pris en charge?

Les pilotes de périphériques se chargent de transférer des commandes depuis une application vers le matériel de la machine. WINE émule un environnement Windows®, ce qui inclut les pilotes, qui utilisent ensuite les pilotes natifs de FreeBSD pour effectuer ce transfert. Il n'est pas recommandé d'installer des pilotes Windows®, car WINE est conçu de manière à interagir avec les pilotes du système hôte. Si par exemple, des pilotes de cartes graphiques améliorent ses performances, veuillez plutôt installer la version FreeBSD et non leur équivalent Windows®.

11.8.2.2. Est-il possible d'améliorer l'apparence des polices de caractères Windows®?

Un utilisateur sur le forum FreeBSD propose cette configuration pour régler l'apparence des polices Windows® qui sont par défaut légèrement pixélisées.

Selon ce post sur le forum FreeBSD, ajouter ce qui suit au fichier .config/fontconfig/fonts.conf devrait ajouter de l'anti-crenélage et rendre le texte plus lisible.

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd>"
```

```
<fontconfig>

  <!-- antialias all fonts -->
  <match target="font">
    <edit name="antialias" mode="assign"><bool>true</bool></edit>>
    <edit name="hinting" mode="assign"><bool>true</bool></edit>>
    <edit name="hintstyle" mode="assign"><const>hintslight</const></edit>>
    <edit name="rgba" mode="assign"><const>rgb</const></edit>>
  </match>
</fontconfig>
```

11.8.2.3. Installer Windows® ailleurs sur le système peut-il aider WINE à fonctionner?

C'est possible, en fonction de l'application devant être exécutée. Comme mentionné dans la section sur `winecfg`, certaines DLLs intégrées par défaut avec WINE et d'autres bibliothèques peuvent être remplacés en fournissant le chemin de versions alternatives. Si la partition ou le disque Windows® est montée et accessible pour l'utilisateur sous FreeBSD, il est alors possible de remplacer certaines DLL de WINE par les versions natives du système Windows®, diminuant potentiellement le risque de fonctionnement inattendus de certaines applications.

11.8.3. Spécifique à une application

11.8.3.1. Quel est le meilleur endroit pour savoir si une application fonctionne sous WINE?

La première étape pour savoir si une application est compatible doit être le site WINE AppDB. Il s'agit d'un site qui répertorie les programmes fonctionnant ou non sous WINE sur toutes les plateformes supportées, et les solutions pour les faire fonctionner, solutions qui sont souvent applicables sur d'autres plateformes.

11.8.3.2. Y a-t-il quelque chose permettant à un jeu vidéo de mieux fonctionner?

Peut-être. Beaucoup de jeux Windows® se basent sur DirectX, une surcouche graphique propriétaire de Microsoft. Cependant, il existe des projets open source qui tentent d'implémenter une prise en charge pour cette technologie.

Le projet *dxvk*, est une tentative d'implémenter DirectX en utilisant le sous-système graphique Vulkan compatible avec FreeBSD. Bien que ce système soit avant tout conçu pour fonctionner pour la version Linux de WINE; il est apparemment possible d'utiliser ce système sur FreeBSD selon certains utilisateurs du forum FreeBSD.

De plus, des initiatives sont en cours pour intégrer WINE Proton. Cela devrait amener la version de Valve, développeur de la plateforme de jeux vidéo Steam, sur FreeBSD. Proton est une version de WINE spécialement conçue pour que nombre de jeux Windows® puissent tourner avec un minimum de manipulation de la part de l'utilisateur.

11.8.3.3. Où les utilisateurs de WINE sous FreeBSD se ressemblent pour échanger des conseils et astuces?

Il existe pas mal d'endroits où les utilisateurs FreeBSD discutent de problèmes liés à WINE, qui

peuvent être utilisés pour rechercher des solutions:

- Le forum FreeBSD, tout particulièrement les sections *Installation and Maintenance of Ports or Packages* ou *Emulation and virtualization*.
- Les canaux IRC de FreeBSD, dont #freebsd (pour un support général), #freebsd-games, ou autres.
- Le serveur discord: The BSD World, notamment les canaux *bsd-desktop*, *bsd-gaming*, *bsd-wine*, et autres.

11.8.4. Les ressource provenant d'autres systèmes d'exploitation

Il existe un certain nombre de ressources relatives au fonctionnement de WINE sous d'autres systèmes d'exploitation qui peuvent cependant s'avérer utiles pour les utilisateurs de FreeBSD:

- Le Wiki de WINE sur lequel se trouve des tonnes d'informations relatives à l'utilisation de WINE, qui sont bien souvent applicables à tous les systèmes d'exploitation pris en charge par WINE;
- De plus, la documentation d'autre systèmes d'exploitation peut aussi s'avérer utile comme la page WINE sur le Wiki de la distribution Arch Linux, bien que certaines applications tierces (i.e., "companion applications") ne soient bien évidemment pas disponibles sous FreeBSD;
- Enfin, Codeweavers (le développeur d'une version commerciale de WINE) est un contributeur actif au projet WINE. Souvent, les réponses aux questions sur leur forum peuvent également être utiles pour dépanner des problèmes avec la version open source de WINE.

Partie III: Administration Système

Les chapitres restant couvrent tous les aspects de l'administration système de FreeBSD. Chaque chapitre débute en décrivant ce qui sera appris à la lecture du chapitre, et détaille également ce que le lecteur est sensé connaître avant de l'aborder.

Ces chapitres sont conçus pour être consultés dès qu'une information est nécessaire. Il n'est pas nécessaire de les lire suivant un ordre particulier, ni tous les lire avant de pouvoir utiliser FreeBSD.

Chapitre 12. Configuration et optimisation

12.1. Synopsis

La configuration correcte d'un système peut sensiblement réduire la quantité de travail impliquée dans la maintenance et la mise à jour. Ce chapitre décrit certains des aspects de la configuration des systèmes FreeBSD.

Ce chapitre décrira également certains paramètres qui peuvent être modifiés pour configurer un système FreeBSD pour des performances optimales.

Après la lecture de ce chapitre, vous saurez:

- Les bases de la configuration du fichier rc.conf et des fichiers de démarrage /usr/local/etc/rc.d.
- Comment configurer et tester une carte réseau.
- Comment configurer des hôtes virtuels sur vos périphériques réseau.
- Comment utiliser les divers fichiers de configuration du répertoire /etc.
- Comment optimiser FreeBSD en utilisant les variables `sysctl`.
- Comment optimiser les performances des disques et modifier les limitations du noyau.

Avant de lire ce chapitre, vous devrez:

- Comprendre les fondements d'UNIX® et de FreeBSD (Quelques bases d'UNIX).
- Etre familier avec la configuration et la compilation du noyau (Configurer le noyau de FreeBSD).

12.2. Configuration principale

L'emplacement principal pour les données de configuration du système est le fichier /etc/rc.conf. Ce fichier contient une large gamme d'informations de configuration, principalement utilisées au démarrage du système pour configurer ce dernier. Son nom le sous-entend; c'est l'information de configuration pour les fichiers rc*.

Un administrateur devrait ajouter des entrées dans le fichier rc.conf pour remplacer les valeurs par défaut du fichier /etc/defaults/rc.conf. Les fichiers de valeurs par défaut ne devraient pas être copiés directement tels quels dans /etc - ils contiennent des valeurs par défaut, et non pas des exemples. Tout changement spécifique au système devrait être fait dans le fichier rc.conf.

Un certain nombre de stratégies peuvent être appliquées dans le cas d'applications en grappe pour séparer la configuration d'un site de celle d'un système afin de réduire le travail d'administration. L'approche recommandée est de placer la configuration propre au site dans le fichier /etc/rc.conf.local. Par exemple:

- /etc/rc.conf:

```
sshd_enable="YES"
```

```
keyrate="fast"
defaultrouter="10.1.1.254"
```

- /etc/rc.conf.local:

```
hostname="node1.example.org"
ifconfig_fxp0="inet 10.1.1.1/8"
```

Le fichier rc.conf peut être distribué à l'ensemble des systèmes en utilisant `rsync` ou un programme semblable, tandis que le fichier rc.conf.local reste unique.

Mettre à jour le système en employant sysinstall(8) ou `make world` n'écrasera pas le fichier rc.conf, les informations de configuration du système ne seront donc pas perdues.

Le fichier de configuration /etc/rc.conf est analysé par sh(1). Cela permet aux administrateurs système d'ajouter un certain niveau de logique à ce fichier, ce qui peut aider à créer des scénaris de configuration complexes. Veuillez consulter rc.conf(5) pour plus d'information sur ce sujet.

12.3. Configuration des applications

Généralement, les applications installées ont leurs propres fichiers de configuration, avec leur propre syntaxe, etc... Il est important que ces fichiers soient séparés du système de base, de sorte qu'ils soient facilement localisables et gérables par les outils de gestion des logiciels installés.

Ces fichiers sont généralement installés dans le répertoire /usr/local/etc. Dans le cas où une application possède un grand nombre de fichiers de configuration, un sous-répertoire sera créé pour les héberger.

Normalement, quand un logiciel porté ou pré-compilé est installé, des exemples de fichiers de configuration sont également installés. Ces derniers sont généralement identifiés par un suffixe ".default". Si aucun fichier de configuration n'existe pour l'application, on les créera en copiant les fichiers .default.

Par exemple, considérez le contenu du répertoire /usr/local/etc/apache:

```
-rw-r--r--  1 root  wheel   2184 May 20  1998 access.conf
-rw-r--r--  1 root  wheel   2184 May 20  1998 access.conf.default
-rw-r--r--  1 root  wheel   9555 May 20  1998 httpd.conf
-rw-r--r--  1 root  wheel   9555 May 20  1998 httpd.conf.default
-rw-r--r--  1 root  wheel  12205 May 20  1998 magic
-rw-r--r--  1 root  wheel  12205 May 20  1998 magic.default
-rw-r--r--  1 root  wheel   2700 May 20  1998 mime.types
-rw-r--r--  1 root  wheel   2700 May 20  1998 mime.types.default
-rw-r--r--  1 root  wheel   7980 May 20  1998 srm.conf
-rw-r--r--  1 root  wheel   7933 May 20  1998 srm.conf.default
```

Les tailles des fichiers indiquent que seul le fichier srm.conf a été modifié. Une mise à jour, plus

tard, du logiciel Apache ne devrait pas écraser le fichier modifié.

12.4. Démarrer des services

Nombreux sont les utilisateurs qui choisissent d'installer des logiciels tierce partie sous FreeBSD à partir du catalogue des logiciels portés. Dans de nombreuses situations, il peut être nécessaire de configurer le logiciel de manière à ce qu'il soit lancé au démarrage du système. Des services comme mail/postfix ou www/apache22 sont deux exemples de logiciels parmi tant d'autres qui peuvent être lancés à l'initialisation du système. Cette section explique les procédures disponibles pour démarrer certains logiciels tierce partie.

Sous FreeBSD, la plupart des services offerts, comme cron(8), sont lancés par l'intermédiaire des procédures de démarrage du système. Ces procédures peuvent varier en fonction de la version de FreeBSD, ou du fournisseur; cependant, l'aspect le plus important à considérer est que leur configuration de démarrage peut être gérée à l'aide de procédures de démarrage simples.

12.4.1. Configuration étendue des applications

Maintenant que FreeBSD dispose du système rc.d, la configuration du démarrage des applications est plus simple, et propose plus de possibilités. En utilisant les mots clés présentés dans la section sur le système rc.d, les applications peuvent désormais être paramétrées pour démarrer après certains services, par exemple le DNS, des paramètres supplémentaires peuvent être passés par l'intermédiaire de rc.conf au lieu d'utiliser des paramètres fixes dans les procédures de démarrage, etc. Une procédure de base pourra ressembler à ce qui suit:

```
#!/bin/sh
#
# PROVIDE: utility
# REQUIRE: DAEMON
# KEYWORD: shutdown

. /etc/rc.subr

name=utility
rcvar=utility_enable

command="/usr/local/sbin/utility"

load_rc_config $name

#
# DO NOT CHANGE THESE DEFAULT VALUES HERE
# SET THEM IN THE /etc/rc.conf FILE
#
utility_enable=${utility_enable-"NO"}
pidfile=${utility_pidfile-"/var/run/utility.pid"}

run_rc_command "$1"
```

Cette procédure s'assurera que l'application utility sera lancée après le le service DAEMON. Elle fournie également une méthode de suivi du PID, ou encore ID (identifiant) de processus.

Cette application pourra alors avoir la ligne suivante la concernant dans le fichier /etc/rc.conf:

```
utility_enable="YES"
```

Cette méthode permet également une manipulation plus aisée des arguments en ligne de commande, l'inclusion des fonctions offertes par défaut dans /etc/rc.subr, offre une compatibilité avec l'utilitaire rcorder(8) et fournie une configuration plus aisée par l'intermédiaire du fichier rc.conf.

12.4.2. Utiliser des services pour démarrer d'autres services

Certains services, comme les serveurs POP3, IMAP, etc., peuvent être démarrés en utilisant inetd(8). Cela implique d'installer le service à partir du catalogue des logiciels portés et avec une ligne de configuration ajoutée au fichier /etc/inetd.conf, ou en décommentant une des lignes de configuration déjà présentes. L'utilisation d'inetd et sa configuration sont décrits en profondeur dans la section concernant inetd.

Dans certains cas, il peut être plus approprié d'utiliser le "daemon" cron(8) pour démarrer des services. Cette approche présente un certain nombre d'avantages parce que `cron` exécute ces processus sous les privilèges du propriétaire de la table crontab. Cela permet aux utilisateurs normaux de lancer et maintenir certaines applications.

L'utilitaire `cron` offre une fonction unique, `@reboot`, qui peut être utilisée en remplacement de la date d'exécution. Cela provoquera l'exécution de la tâche quand cron(8) est lancé, normalement lors de l'initialisation du système.

12.5. Configuration de l'utilitaire `cron`

Un des utilitaires les plus importants de FreeBSD est cron(8). L'utilitaire `cron` tourne en arrière plan et contrôle constamment le fichier /etc/crontab. L'utilitaire `cron` consulte également le répertoire /var/cron/tabs, à la recherche de nouveaux fichiers crontab. Ces fichiers crontab conservent les informations sur les tâches que `cron` est censé exécuter à des moments donnés.

L'utilitaire `cron` utilise deux types différents de fichiers de configuration, le fichier crontab système et les crontabs des utilisateurs. Ces deux formats diffèrent à partir du sixième champ. Dans le fichier crontab système, `cron` exécutera la commande en tant que l'utilisateur indiqué dans le sixième champ. Dans le fichier crontab d'un utilisateur, toutes les commandes sont exécutées sous l'utilisateur qui a créé ce fichier crontab, aussi le sixième champ est le dernier champ; c'est un aspect sécurité important. Le dernier champ est toujours la commande à exécuter.

Les fichiers crontab utilisateur permettent aux utilisateurs de planifier l'exécution de tâches sans avoir besoin des privilèges du super-utilisateur `root`. Les commandes contenues dans le fichier crontab d'un utilisateur s'exécutent avec les privilèges de l'utilisateur auquel appartient ce fichier.

> Le super-utilisateur `root` peut posséder un fichier crontab utilisateur comme tout autre utilisateur. Ce fichier est différent de /etc/crontab (le crontab système). Etant donné que le fichier crontab système invoque les commandes spécifiées en tant que `root`, il n'y a généralement pas besoin d'un fichier crontab utilisateur pour `root`.

Examinons le fichier /etc/crontab (fichier crontab système):

```
# /etc/crontab - root's crontab for FreeBSD
#
# $FreeBSD: src/etc/crontab,v 1.32 2002/11/22 16:13:39 tom Exp $
#①
#
SHELL=/bin/sh
PATH=/etc:/bin:/sbin:/usr/bin:/usr/sbin ②
HOME=/var/log
#
#
#minute heure   date    mois    jour    utilisateur commande ③
#
#
*/5 *   *   *   *   root    /usr/libexec/atrun ④
```

① Comme pour la plupart des fichiers de configuration de FreeBSD, le caractère `#` indique un commentaire. Un commentaire peut être ajouté dans le fichier comme rappel de ce que fait une action bien précise et pourquoi elle est effectuée. Les commentaires ne peuvent être situés sur la même ligne qu'une commande ou sinon ils seront interprétés comme faisant partie de la commande; ils doivent se trouver sur une nouvelle ligne. Les lignes vides sont ignorées.

② Tout d'abord, les variables d'environnement doivent être définies. Le caractère égal (`=`) est utilisé pour définir tout paramètre concernant l'environnement, comme dans notre exemple où il a été utilisé pour les variables `SHELL`, `PATH`, et `HOME`. Si la ligne concernant l'interpréteur de commande est omise, `cron` utilisera celui par défaut, qui est `sh`. Si la variable `PATH` est omise, il n'y aura pas de valeur par défaut utilisée et l'emplacement des fichiers devra être absolu. Si `HOME` est omise, `cron` utilisera le répertoire personnel de l'utilisateur qui l'invoque.

③ Cette ligne définie un total de sept champs. Sont listés ici les valeurs `minute`, `heure`, `date`, `mois`, `jour`, `utilisateur`, et `commande`. Ces champs sont relativement explicites. `minute` représente l'heure en minute à laquelle la commande sera exécutée. L'option `heure` est semblable à l'option `minute`, mais en heures. Le champ `date` précise le jour dans le mois. `mois` est similaire à `heure` et `minute` mais désigne le mois. L'option `jour` représente le jour de la semaine. Tous ces champs doivent être des valeurs numériques, et respecter un format horaire de vingt quatre heures. Le champ `utilisateur` est spécial, et n'existe que dans le fichier /etc/crontab. Ce champ précise sous quel utilisateur sera exécutée la commande. Le dernier champ désigne la commande à exécuter.

④ Cette dernière ligne définie les valeurs discutées ci-dessus. Nous avons ici `*/5` suivi de plusieurs caractères `\*`. Ces caractères `*` signifient "premier-dernier", et peuvent être interprétés comme voulant dire à *chaque* instance. Aussi, d'après cette ligne, il apparaît que la commande `atrun` sera invoquée par l'utilisateur `root` toutes les cinq minutes indépendamment du jour ou du mois. Pour plus d'informations sur la commande `atrun`, consultez la page de manuel de atrun(8).

N'importe quel nombre d'indicateur peut être passé à ces commandes; cependant, les commandes qui s'étendent sur de multiples lignes doivent être "cassées" avec le caractère, contre-oblique `\`, de continuation de lignes.

Ceci est la configuration de base pour chaque fichier crontab, bien qu'il y ait une différence dans celui présenté ici. Le sixième champ, où est précisé le nom d'utilisateur, n'existe que dans le fichier système /etc/crontab. Ce champ devrait être omis pour les fichiers crontab d'utilisateur.

12.5.1. Installer un fichier crontab

Ne pas utiliser la procédure décrite ci-dessous pour éditer et installer le fichier crontab système. Utilisez directement votre éditeur: l'utilitaire `cron` remarquera le changement au niveau de ce fichier et utilisera immédiatement la nouvelle version. Consultez cette entrée de la FAQ pour plus d'information.

Pour installer un fichier crontab utilisateur fraîchement rédigé, tout d'abord utilisez votre éditeur favori pour créer un fichier dans le bon format, ensuite utilisez l'utilitaire `crontab`. L'usage le plus typique est:

```
# crontab fichier-crontab
```

Dans cet exemple, fichier-crontab est le nom d'un fichier crontab qui a été précédemment créé.

Il existe également une option pour afficher les fichiers crontab installés, passez simplement le paramètre `-l` à `crontab` et lisez ce qui est affiché.

Pour les utilisateurs désirant créer leur fichier crontab à partir de zéro, sans utiliser de modèle, l'option `crontab -e` est disponible. Cela invoquera l'éditeur par défaut avec un fichier vide. Quand le fichier est sauvegardé, il sera automatiquement installé par la commande `crontab`.

Afin d'effacer le fichier crontab utilisateur complètement, utiliser la commande `crontab` avec l'option `-r`.

12.6. Utilisation du système rc(8) sous FreeBSD

En 2002, le système rc.d de NetBSD pour l'initialisation du système a été intégré à FreeBSD. Les utilisateurs noteront les fichiers présents dans le répertoire /etc/rc.d. Plusieurs de ces fichiers sont destinés aux services de base qui peuvent être contrôlés avec les options `start`, `stop`, et `restart`. Par exemple, sshd(8) peut être relancé avec la commande suivante:

```
# /etc/rc.d/sshd restart
```

Cette procédure est similaire pour d'autres services. Bien sûr, les services sont généralement lancés automatiquement au démarrage dès qu'ils sont spécifiés dans le fichier rc.conf(5). Par exemple, activer le "daemon" de translation d'adresses au démarrage est aussi simple que d'ajouter la ligne suivante au fichier /etc/rc.conf:

```
natd_enable="YES"
```

Si une ligne `natd_enable="NO"` est déjà présente, modifiez alors le `NO` par `YES`. Les procédures rc chargeront automatiquement les autres services dépendants lors du prochain redémarrage comme décrit ci-dessous.

Comme le système rc.d est à l'origine destiné pour lancer/arrêter les services au démarrage/à l'arrêt du système, les options standards `start`, `stop` et `restart` ne seront effectives que si les variables appropriées sont positionnées dans le fichier /etc/rc.conf. Par exemple, la commande `sshd restart` ci-dessus ne fonctionnera que si `sshd_enable` est fixée à `YES` dans /etc/rc.conf. Pour lancer, arrêter ou redémarrer un service indépendemment des paramétrages du fichier /etc/rc.conf, les commandes doivent être précédées par "one". Par exemple pour redémarrer `sshd` indépendemment du paramétrage du fichier /etc/rc.conf, exécutez la commande suivante:

```
# /etc/rc.d/sshd onerestart
```

Il est facile de contrôler si un service est activé dans le fichier /etc/rc.conf en exécutant la procédure rc.d appropriée avec l'option `rcvar`. Ainsi, un administrateur peut contrôler que `sshd` est réellement activé dans /etc/rc.conf en exécutant:

```
# /etc/rc.d/sshd rcvar
# sshd
$sshd_enable=YES
```

La seconde ligne (`# sshd`) est la sortie de la commande `sshd` et non pas une console `root`.

Pour déterminer si un service est actif, une option appelée `status` est disponible. Par exemple pour vérifier que `sshd` a réellement été lancé:

```
# /etc/rc.d/sshd status
sshd is running as pid 433.
```

Dans certains cas, il est également possible de recharger un service avec l'option `reload`. Le système tentera d'envoyer un signal à un service individuel, le forçant à recharger ses fichiers de configuration. Dans la plupart des cas cela signifie envoyer un signal `SIGHUP` au service. Le support de cette fonctionnalité n'est pas disponible pour chaque service.

Le système rc.d n'est pas uniquement utilisée pour les services réseaux, elle participe à la majeure partie de l'initialisation du système. Prenez par exemple le fichier bgfsck. Quand cette procédure est exécutée, il affichera le message suivant:

```
Starting background file system checks in 60 seconds.
```

Donc ce fichier est utilisé pour les vérifications du système de fichiers en arrière plan, qui sont uniquement effectuées lors de l'initialisation du système.

De nombreux services système dépendent d'autres services pour fonctionner correctement. Par exemple, NIS et les autres services basés sur les RPCs peuvent échouer s'ils sont lancés après le lancement du service `rpcbind` (portmapper). Pour résoudre ce problème, l'information concernant les dépendances et autres méta-données est inclue dans les commentaires au début de chaque procédure de démarrage. Le programme rcorder(8) est alors utilisé pour analyser ces commentaires lors de l'initialisation du système en vue de déterminer l'ordre dans lequel les services système seront invoqués pour satisfaire les dépendances.

Les mots suivants doivent être présents en tête de tous les fichiers de démarrage (ils sont nécessaires pour que rc.subr(8) active les procédures de démarrages):

- `PROVIDE`: indique les services que fournit ce fichier.

Les mots clés suivants peuvent être ajoutés au début de chaque fichier de démarrage. Ils ne sont pas strictement nécessaires, mais sont utiles comme aide pour rcorder(8):

- `REQUIRE`: liste les fichiers dont dépend ce service. Ce fichier sera exécuté *après* les services indiqués.
- `BEFORE`: liste les services qui dépendent du service présent. Ce fichier sera exécuté *avant* les services indiqués.

En utilisant avec soin ces mots clés pour chaque fichier de démarrage, un administrateur dispose d'un niveau de contrôle très fin de l'ordre d'exécution des procédures de démarrage sans les inconvénients des "runlevels" comme sur d'autres systèmes d'exploitation UNIX®.

Des informations supplémentaires concernant le système rc.d peuvent être trouvées dans les pages de manuel rc(8) et rc.subr(8). Si vous êtes intéressé par l'écriture de vos propres procédures rc.d ou pour l'amélioration des procédures existantes, vous trouverez cette article utile.

12.7. Configuration des cartes réseaux

De nos jours il est impossible de penser à un ordinateur sans penser connexion à un réseau. Installer et configurer une carte réseau est une tâche classique pour tout administrateur FreeBSD.

12.7.1. Déterminer le bon pilote de périphérique

Avant de commencer, vous devez connaître le modèle de la carte dont vous disposez, le circuit qu'elle utilise, et si c'est une carte PCI ou ISA. FreeBSD supporte une large variété de cartes PCI et ISA. Consultez la liste de compatibilité matérielle pour votre version de FreeBSD afin de voir si votre carte est supportée.

Une fois que vous êtes sûrs que votre carte est supportée, vous devez déterminer le bon pilote de périphérique pour la carte. Les fichiers /usr/src/sys/conf/NOTES et /usr/src/sys/arch/conf/NOTES vous donneront la liste des pilotes de périphériques pour cartes réseaux avec des informations sur les cartes/circuits supportés. Si vous avez des doutes au sujet du bon pilote, lisez la page de manuel du pilote. La page de manuel vous donnera plus d'information sur le matériel supporté et même les

éventuels problèmes qui pourront apparaître.

Si vous possédez une carte courante, la plupart du temps vous n'aurez pas à chercher trop loin pour trouver un pilote. Les pilotes pour les cartes réseaux courantes sont présents dans le noyau GENERIC, aussi votre carte devrait apparaître au démarrage, comme suit:

```
dc0: <82c169 PNIC 10/100BaseTX> port 0xa000-0xa0ff mem 0xd3800000-0xd38
000ff irq 15 at device 11.0 on pci0
miibus0: <MII bus> on dc0
bmtphy0: <BCM5201 10/100baseTX PHY> PHY 1 on miibus0
bmtphy0:  10baseT, 10baseT-FDX, 100baseTX, 100baseTX-FDX, auto
dc0: Ethernet address: 00:a0:cc:da:da:da
dc0: [ITHREAD]
dc1: <82c169 PNIC 10/100BaseTX> port 0x9800-0x98ff mem 0xd3000000-0xd30
000ff irq 11 at device 12.0 on pci0
miibus1: <MII bus> on dc1
bmtphy1: <BCM5201 10/100baseTX PHY> PHY 1 on miibus1
bmtphy1:  10baseT, 10baseT-FDX, 100baseTX, 100baseTX-FDX, auto
dc1: Ethernet address: 00:a0:cc:da:da:db
dc1: [ITHREAD]
```

Dans cet exemple, nous voyons que deux cartes utilisant le pilote de périphérique dc(4) sont présentes sur le système.

Si le pilote de votre carte n'est pas présent dans le noyau GENERIC, vous devrez charger le module approprié pour pouvoir utiliser votre carte. Cela peut être effectué de deux manières différentes:

- La méthode la plus simple est de charger le module pour votre carte réseau avec kldload(8), ou automatiquement au démarrage du système en ajoutant la ligne appropriée au fichier /boot/loader.conf. Tous les pilotes de cartes réseau ne sont pas disponibles sous forme de modules; les cartes ISA sont un bon exemple de périphériques pour lesquels les modules n'existent pas.
- Alternativement, vous pouvez compiler en statique le support pour votre carte dans votre noyau. Consultez /usr/src/sys/conf/NOTES, /usr/src/sys/arch/conf/NOTES et la page de manuel du pilote de périphérique pour savoir ce qu'il faut ajouter au fichier de configuration de votre noyau. Pour plus d'information sur la recompilation de votre noyau, veuillez lire le Configurer le noyau de FreeBSD. Si votre carte a été détectée au démarrage par votre noyau (GENERIC) vous n'avez pas à compiler un nouveau noyau.

12.7.1.1. Utilisation des pilotes NDIS de Windows®

Malheureusement il y a toujours de nombreux fabricants qui ne fournissent pas à la communauté des logiciels libres les informations concernant les pilotes pour leurs cartes considérant de telles informations comme des secrets industriels. Par conséquent, il ne reste aux développeurs de FreeBSD et d'autres systèmes d'exploitation libres que deux choix: développer les pilotes en passant par un long et pénible processus de "reverse engineering" ou utiliser les pilotes binaires existants disponibles pour la plateforme Microsoft® Windows®. La plupart des développeurs, y compris ceux impliqués dans FreeBSD, ont choisi cette dernière approche.

Grâce aux contributions de Bill Paul (wpaul), il existe un support "natif" pour la spécification d'interface des pilotes de périphérique réseau (Network Driver Interface Specification-NDIS). Le NDISulator FreeBSD (connu également sous le nom de Project Evil) prend un pilote binaire réseau Windows® et lui fait penser qu'il est en train de tourner sous Windows®. Etant donné que le pilote ndis(4) utilise un binaire Windows®, il ne fonctionne que sur les systèmes i386™ et amd64. Les périphériques PCI, CardBus, PCMCIA (PC-Card), et USB sont supportés.

Pour utiliser le NDISulator, trois choses sont nécessaires:

1. les sources du noyau;
2. le pilote binaire Windows® XP (extension .SYS);
3. le fichier de configuration du pilote Windows® XP (extension .INF).

Recherchez les fichiers spécifiques à votre carte. Généralement, ils peuvent être trouvés sur les CDs livrés avec la carte ou sur le site du fabricant. Dans les exemples qui suivent nous utiliseront les fichiers W32DRIVER.SYS et W32DRIVER.INF.

Le type de pilote doit correspondre à la version de FreeBSD. Pour FreeBSD/i386, utiliser un pilote Windows® 32bits. Pour FreeBSD/amd64, un pilote Windows® 64bits est nécessaire.

L'étape suivante est de compiler le pilote binaire dans un module chargeable du noyau. En tant que `root`, utilisez ndisgen(8):

```
# ndisgen /path/to/W32DRIVER.INF /path/to/W32DRIVER.SYS
```

L'utilitaire ndisgen(8) est interactif, il sollicitera l'utilisateur pour d'éventuelles informations complémentaires si nécessaire. Un nouveau module noyau est créé dans le répertoire courant. Utiliser kldload(8) pour charger le nouveau module:

```
# kldload ./W32DRIVER_SYS.ko
```

Avec le module généré, vous devez également charger les modules ndis.ko et if_ndis.ko. Cela devrait être fait automatiquement quand vous chargez un module qui dépend de ndis(4). Si vous désirez les charger manuellement, utilisez les commandes suivantes:

```
# kldload ndis
# kldload if_ndis
```

La première commande charge le pilote d'interface NDIS, la seconde charge l'interface réseau.

Contrôlez maintenant la sortie de dmesg(8) à la recherche d'une quelconque erreur au chargement. Si tout s'est bien passé, vous devriez obtenir une sortie ressemblant à ce qui suit:

```
ndis0: <Wireless-G PCI Adapter> mem 0xf4100000-0xf4101fff irq 3 at device 8.0 on pci1
ndis0: NDIS API version: 5.0
ndis0: Ethernet address: 0a:b1:2c:d3:4e:f5
```

```
ndis0: 11b rates: 1Mbps 2Mbps 5.5Mbps 11Mbps
ndis0: 11g rates: 6Mbps 9Mbps 12Mbps 18Mbps 36Mbps 48Mbps 54Mbps
```

A partir de là vous pouvez traiter le périphérique ndis0 comme n'importe quelle interface réseau (par exemple dc0).

Vous pouvez configurer le système pour charger les modules NDIS au démarrage du système de la même manière que pour n'importe quel autre module. Tout d'abord, copiez le module généré, W32DRIVER_SYS.ko, dans le répertoire /boot/modules. Ajoutez ensuite la ligne suivante au fichier /boot/loader.conf:

```
W32DRIVER_SYS_load="YES"
```

12.7.2. Configuration de la carte réseau

Une fois que le bon pilote de périphérique pour la carte réseau est chargé, la carte doit être configurée. Comme beaucoup d'autres choses, la carte aura pu être configurée à l'installation par sysinstall.

Pour afficher la configuration des interfaces réseaux de votre système, entrer la commande suivante:

```
% ifconfig
dc0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80008<VLAN_MTU,LINKSTATE>
        ether 00:a0:cc:da:da:da
        inet 192.168.1.3 netmask 0xffffff00 broadcast 192.168.1.255
        media: Ethernet autoselect (100baseTX <full-duplex>)
        status: active
dc1: flags=8802<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80008<VLAN_MTU,LINKSTATE>
        ether 00:a0:cc:da:da:db
        inet 10.0.0.1 netmask 0xffffff00 broadcast 10.0.0.255
        media: Ethernet 10baseT/UTP
        status: no carrier
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x4
        inet6 ::1 prefixlen 128
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
```

Dans cet exemple, les périphériques suivants ont été affichés:

- dc0: La première interface Ethernet
- dc1: La seconde interface Ethernet
- lo0: L'interface "en boucle" ("loopback")

FreeBSD utilise le nom du pilote de périphérique suivi par un chiffre représentant l'ordre dans lequel la carte est détectée au démarrage du noyau pour nommer la carte. Par exemple sis2 serait la troisième carte sur le système utilisant le pilote de périphérique sis(4).

Dans cet exemple, le périphérique dc0 est actif et en fonctionnement. Les indicateurs importants sont:

1. `UP` signifie que la carte est configurée et prête.
2. La carte possède une adresse Internet (`inet`) (dans ce cas-ci `192.168.1.3`).
3. Elle a un masque de sous-réseau valide (`netmask`; `0xffffff00` est équivalent à `255.255.255.0`).
4. Elle a une adresse de diffusion valide (dans ce cas-ci `192.168.1.255`).
5. L'adresse MAC de la carte (`ether`) est `00:a0:cc:da:da:da`
6. La sélection du média est sur le mode d'autosélection (`media: Ethernet autoselect (100baseTX full-duplex)`). Nous voyons que dc1 a été configurée pour utiliser un matériel de type `10baseT/UTP`. Pour plus d'information sur le type de matériel disponible pour un pilote de périphérique, référez-vous à sa page de manuel.
7. La liaison (`status`) est `active`, i.e. la porteuse est détectée. Pour dc1, nous lisons `status: no carrier`. Cela est normal lorsqu'aucun câble n'est branché à la carte.

Si le résultat de la commande ifconfig(8) est similaire à:

```
dc0: flags=8843<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80008<VLAN_MTU,LINKSTATE>
        ether 00:a0:cc:da:da:da
        media: Ethernet autoselect (100baseTX <full-duplex>)
        status: active
```

cela indiquerait que la carte n'a pas été configurée.

Pour configurer votre carte, vous avez besoin des privilèges de l'utilisateur `root`. La configuration de la carte réseau peut être faite à partir de la ligne de commande avec ifconfig(8) mais vous aurez à répéter cette opération à chaque redémarrage du système. Le fichier /etc/rc.conf est l'endroit où ajouter la configuration de la carte réseau.

Ouvrez le fichier /etc/rc.conf dans votre éditeur favori. Vous devez ajouter une ligne pour chaque carte réseau présente sur le système, par exemple dans notre cas, nous avons ajouté ces lignes:

```
ifconfig_dc0="inet 192.168.1.3 netmask 255.255.255.0"
ifconfig_dc1="inet 10.0.0.1 netmask 255.255.255.0 media 10baseT/UTP"
```

Vous devez remplacer dc0, dc1, et ainsi de suite, avec le périphérique correspondant pour vos cartes, et les adresses avec celles désirées. Vous devriez lire les pages de manuel du pilote de périphérique et d'ifconfig(8) pour plus de détails sur les options autorisées et également la page de manuel de rc.conf(5) pour plus d'information sur la syntaxe de /etc/rc.conf.

Si vous avez configuré le réseau à l'installation, des lignes concernant la/les carte(s) réseau pourront être déjà présentes. Contrôler à deux fois le fichier /etc/rc.conf avant d'y ajouter des lignes.

Vous devrez également éditer le fichier /etc/hosts pour ajouter les noms et les adresses IP des diverses machines du réseau local, si elles ne sont pas déjà présentes. Pour plus d'information référez-vous à la page de manuel hosts(5) et au fichier /usr/shared/examples/etc/hosts.

S'il n'y a pas de serveur DHCP et qu'un accès à Internet est nécessaire, configurez manuellement la passerelle par défaut et le serveur de noms:

```
# echo 'defaultrouter="your_default_router"' >> /etc/rc.conf
# echo 'nameserver your_DNS_server' >> /etc/resolv.conf
```

12.7.3. Test et dépannage

Une fois les modifications nécessaires du fichier /etc/rc.conf effectuées, vous devrez redémarrer votre système. Cela permettra la prise en compte de la ou les modifications au niveau des interfaces, et permettra de vérifier que le système redémarre sans erreur de configuration. Sinon, une autre méthode pour faire prendre en compte les modifications au niveau de la gestion du réseau consiste à utiliser la commande:

```
# service netif restart
```

Si une passerelle par défaut a été configurée dans /etc/rc.conf, lancez également cette commande:

```
# service routing restart
```

Une fois que le système a été redémarré, vous testez les interfaces réseau.

12.7.3.1. Tester la carte Ethernet

Pour vérifier qu'une carte Ethernet est configurée correctement, vous devez essayer deux choses. Premièrement, "pinguer" l'interface, puis une autre machine sur le réseau local.

Tout d'abord testons l'interface:

```
% ping -c5 192.168.1.3
PING 192.168.1.3 (192.168.1.3): 56 data bytes
64 bytes from 192.168.1.3: icmp_seq=0 ttl=64 time=0.082 ms
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=0.074 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.076 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=0.108 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=64 time=0.076 ms
```

```
--- 192.168.1.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.074/0.083/0.108/0.013 ms
```

Nous devons maintenant "pinguer" une autre machine sur le réseau:

```
% ping -c5 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=0.726 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.766 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.700 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.747 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.704 ms

--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.700/0.729/0.766/0.025 ms
```

Vous pourrez utiliser le noms de la machine à la place de `192.168.1.2` si vous avez configuré le fichier /etc/hosts.

12.7.3.2. Dépannage

Le dépannage de matériels ou de logiciels est toujours une tâche relativement pénible, mais qui peut être rendue plus aisée en vérifiant en premier lieu certaines choses élémentaires. Votre câble réseau est-il branché? Avez-vous correctement configuré les services réseau? Le coupe-feu est-il bien configuré? Est-ce que la carte réseau est supportée par FreeBSD? Consultez toujours les notes concernant le matériel avant d'envoyer un rapport de bogue. Mettez à jour votre version de FreeBSD vers la dernière version STABLE. Consultez les archives des listes de diffusion, et faites même des recherches sur l'Internet.

Si la carte fonctionne mais les performances sont mauvaises, une lecture de la page de manuel tuning(7) peut valoir la peine. Vous pouvez également vérifier la configuration du réseau puisque des paramètres réseau incorrects peuvent donner lieu à des connexions lentes.

Certains utilisateurs peuvent voir apparaître un ou deux messages `device timeout`, ce qui est normal pour certaines cartes. Si ces messages se multiplient, assurez-vous que la carte n'est pas en conflit avec un autre périphérique. Contrôlez à deux fois les câbles de connexion. Peut-être que vous avez juste besoin d'une autre carte.

Parfois, des utilisateurs sont confrontés à des messages d'erreur `watchdog timeout`. La première chose à faire dans ce cas est de vérifier votre câble réseau. De nombreuses cartes demandent un slot PCI supportant le "Bus Mastering". Sur certaines cartes mère anciennes, seul un slot PCI le permet (la plupart du temps le slot 0). Consultez la documentation de la carte réseau et de la carte mère pour déterminer si cela peut être à l'origine du problème.

Les messages `No route to host` surviennent si le système est incapable de router un paquet vers la

machine de destination. Cela peut arriver s'il n'y a pas de route par défaut de définie, ou si le câble réseau est débranché. Vérifiez la sortie de la commande `netstat -nr` et assurez-vous qu'il y a une route valide en direction de la machine que vous essayez d'atteindre. Si ce n'est pas le cas, lisez la Administration réseau avancée.

Les messages d'erreur `ping: sendto: Permission denied` sont souvent dus à un coupe-feu mal configuré. Si `ipfw` est activé dans le noyau mais qu'aucune règle n'a été définie, alors la politique par défaut est de refuser tout trafic, même les requêtes "ping"! Lisez Firewalls pour plus d'informations.

Parfois les performances de la carte ne sont pas bonnes, ou en dessous de la moyenne. Dans ce cas il est recommandé de passer la sélection du média du mode `autoselect` au mode adéquat. Alors que cela fonctionne généralement pour la plupart du matériel, il se peut que cela ne résolve pas le problème pour tout de monde. Encore une fois, contrôlez les paramétrages réseau et consultez la page de manuel tuning(7).

12.8. Hôtes virtuels

Une utilisation très courante de FreeBSD est l'hébergement de sites virtuels, où un serveur apparaît pour le réseau comme étant plusieurs serveurs différents. Ceci est possible en assignant plusieurs adresses réseau à une interface.

Une interface réseau donnée possède une adresse "réelle", et peut avoir n'importe quel nombre d'adresses "alias". Ces alias sont normalement ajoutés en plaçant les entrées correspondantes dans le fichier /etc/rc.conf.

Une entrée d'alias pour l'interface fxp0 ressemble à:

```
ifconfig_fxp0_alias0="inet xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx"
```

Notez que les entrées d'alias doivent commencer avec alias0 et continuer en ordre croissant, (par exemple, _alias1, _alias2, et ainsi de suite). Le processus de configuration s'arrêtera au premier nombre absent.

Le calcul des masques de réseau est important, mais heureusement assez simple. Pour une interface donnée, il doit y avoir une adresse qui représente correctement le masque de réseau de votre réseau. Tout autre adresse appartenant à ce réseau devra avoir un masque de réseau avec chaque bit à `1` (exprimé soit sous la forme `255.255.255.255` soit `0xffffffff`).

Par exemple, considérez le cas où l'interface fxp0 est connectée à deux réseaux, le réseau `10.1.1.0` avec un masque de réseau de `255.255.255.0` et le réseau `202.0.75.16` avec un masque de `255.255.255.240`. Nous voulons que le système apparaisse de `10.1.1.1` jusqu'à `10.1.1.5` et à `202.0.75.17` jusqu'à `202.0.75.20`. Comme noté plus haut, seule la première adresse dans un intervalle réseau donné (dans ce cas, `10.0.1.1` et `202.0.75.17`) devrait avoir un masque de sous-réseau réel; toutes les autres adresses (`10.1.1.2` à `10.1.1.5` et `202.0.75.18` jusqu'à `202.0.75.20`) doivent être configurées avec un masque de sous-réseau de `255.255.255.255`.

Les entrées suivantes du fichier /etc/rc.conf configurent la carte correctement pour cet

arrangement:

```
ifconfig_fxp0="inet 10.1.1.1 netmask 255.255.255.0"
ifconfig_fxp0_alias0="inet 10.1.1.2 netmask 255.255.255.255"
ifconfig_fxp0_alias1="inet 10.1.1.3 netmask 255.255.255.255"
ifconfig_fxp0_alias2="inet 10.1.1.4 netmask 255.255.255.255"
ifconfig_fxp0_alias3="inet 10.1.1.5 netmask 255.255.255.255"
ifconfig_fxp0_alias4="inet 202.0.75.17 netmask 255.255.255.240"
ifconfig_fxp0_alias5="inet 202.0.75.18 netmask 255.255.255.255"
ifconfig_fxp0_alias6="inet 202.0.75.19 netmask 255.255.255.255"
ifconfig_fxp0_alias7="inet 202.0.75.20 netmask 255.255.255.255"
```

12.9. Fichiers de configuration

12.9.1. Organisation du répertoire /etc

Il existe un certain nombre de répertoires dans lesquels se trouvent les informations de configuration. Ceux-ci incluent:

/etc	Information de configuration générique du système; les données ici sont spécifiques au système.
/etc/defaults	Version par défaut des fichiers de configuration du système.
/etc/mail	Configuration de sendmail(8), et autres fichiers de configuration d'agent de transmission du courrier électronique.
/etc/ppp	Configuration pour les programmes PPP utilisateur et intégré au noyau.
/etc/namedb	Emplacement par défaut pour les données de named(8). Normalement named.conf et les fichiers de zone sont stockés dans ce répertoire.
/usr/local/etc	Fichiers de configuration pour les applications installées. Peut contenir des sous-répertoires pour chaque application.
/usr/local/etc/rc.d	Procédures de lancement/d'arrêt pour les applications installées.
/var/db	Fichiers de bases de données automatiquement générés, spécifiques au système, comme la base de données des logiciels installés, la base de données de localisation des fichiers, et ainsi de suite.

12.9.2. Nom d'hôtes

12.9.2.1. /etc/resolv.conf

/etc/resolv.conf gère comment le résolveur de FreeBSD accède au système de nom de domaine d'Internet (DNS).

Les entrées la plus classiques du fichier resolv.conf sont:

`nameserver`	L'adresse IP du serveur de noms auquel le résolveur devrait envoyer ses requêtes. Les serveurs sont sollicités dans l'ordre listé avec un maximum de trois.
`search`	Liste de recherche pour la résolution de nom de machine. Ceci est normalement déterminé par le domaine de l'hôte local.
`domain`	Le nom du domaine local.

Un fichier resolv.conf typique:

```
search example.com
nameserver 147.11.1.11
nameserver 147.11.100.30
```

Seule une des options `search` et `domain` devrait être utilisée.

Si vous utilisez DHCP, dhclient(8) réécrit habituellement resolv.conf avec l'information reçue du serveur DHCP.

12.9.2.2. /etc/hosts

/etc/hosts est une simple base de données texte, une réminiscence des débuts d'Internet. Il travaille en conjonction avec les serveurs DNS et NIS pour fournir les correspondances nom vers adresse IP. Les ordinateurs locaux reliés par l'intermédiaire d'un réseau local peuvent être ajoutés dans ce fichier pour une résolution de noms simple plutôt que de configurer un serveur named(8). De plus /etc/hosts peut être utilisé pour fournir un enregistrement local de correspondances de nom, réduisant ainsi le besoin de requêtes vers l'extérieur pour les noms auxquels on accède couramment.

```
# $FreeBSD$
#
#
# Host Database
#
# This file should contain the addresses and aliases for local hosts that
# share this file.  Replace 'my.domain' below with the domainname of your
# machine.
```

```
#
# In the presence of the domain name service or NIS, this file may
# not be consulted at all; see /etc/nsswitch.conf for the resolution order.
#
#
::1         localhost localhost.my.domain
127.0.0.1       localhost localhost.my.domain
#
# Imaginary network.
#10.0.0.2       myname.my.domain myname
#10.0.0.3       myfriend.my.domain myfriend
#
# According to RFC 1918, you can use the following IP networks for
# private nets which will never be connected to the Internet:
#
#   10.0.0.0    -   10.255.255.255
#   172.16.0.0  -   172.31.255.255
#   192.168.0.0 -   192.168.255.255
#
# In case you want to be able to connect to the Internet, you need
# real official assigned numbers.  Do not try to invent your own network
# numbers but instead get one from your network provider (if any) or
# from your regional registry (ARIN, APNIC, LACNIC, RIPE NCC, or AfriNIC.)
#
```

/etc/hosts suit le format simple suivant:

```
[Internet address] [official hostname] [alias1] [alias2] ...
```

Par exemple:

```
10.0.0.1 myRealHostname.example.com myRealHostname foobar1 foobar2
```

Consultez la page de manuel hosts(5) pour plus d'informations.

12.9.3. Configuration des fichiers de trace

12.9.3.1. syslog.conf

syslog.conf est le fichier de configuration du programme syslogd(8). Il indique quel type de messages `syslog` sera enregistré dans des fichiers de traces particuliers.

```
# $FreeBSD$
#
#       Spaces ARE valid field separators in this file. However,
#       other *nix-like systems still insist on using tabs as field
#       separators. If you are sharing this file between systems, you
```

```
#       may want to use only tabs as field separators here.
#       Consult the syslog.conf(5) manual page.
*.err;kern.debug;auth.notice;mail.crit          /dev/console
*.notice;kern.debug;lpr.info;mail.crit;news.err /var/log/messages
security.*                                      /var/log/security
mail.info                                       /var/log/maillog
lpr.info                                        /var/log/lpd-errs
cron.*                                          /var/log/cron
*.err                                           root
*.notice;news.err                               root
*.alert                                         root
*.emerg                                         *
# uncomment this to log all writes to /dev/console to /var/log/console.log
#console.info                                   /var/log/console.log
# uncomment this to enable logging of all log messages to /var/log/all.log
#*.*                                            /var/log/all.log
# uncomment this to enable logging to a remote log host named loghost
#*.*                                            @loghost
# uncomment these if you're running inn
# news.crit                                     /var/log/news/news.crit
# news.err                                      /var/log/news/news.err
# news.notice                                   /var/log/news/news.notice
!startslip
*.*                                             /var/log/slip.log
!ppp
*.*                                             /var/log/ppp.log
```

Consultez la page de manuel syslog.conf(5) pour plus d'informations.

12.9.3.2. newsyslog.conf

newsyslog.conf est le fichier de configuration de newsyslog(8), un programme qui est normalement programmé cron(8) pour s'exécuter périodiquement. newsyslog(8) détermine quand les fichiers de traces doivent être archivés ou réorganisés. logfile devient logfile.0, logfile.0 devient à son tour logfile.1, et ainsi de suite. D'autre part, les fichiers de traces peuvent être archivés dans le format gzip(1), ils se nommeront alors: logfile.0.gz, logfile.1.gz, et ainsi de suite.

newsyslog.conf indique quels fichiers de traces doivent être gérés, combien doivent être conservés, et quand ils doivent être modifiés. Les fichiers de traces peuvent être réorganisés et/ou archivés quand ils ont soit atteint une certaine taille, soit à une certaine période/date.

```
# configuration file for newsyslog
# $FreeBSD$
#
# filename          [owner:group]    mode count size when [ZB] [/pid_file] [sig_num]
/var/log/cron                         600  3     100  *     Z
/var/log/amd.log                      644  7     100  *     Z
/var/log/kerberos.log                 644  7     100  *     Z
/var/log/lpd-errs                     644  7     100  *     Z
/var/log/maillog                      644  7     *    @T00  Z
```

```
/var/log/sendmail.st                    644  10    *    168   B
/var/log/messages                       644  5     100  *     Z
/var/log/all.log                        600  7     *    @T00  Z
/var/log/slip.log                       600  3     100  *     Z
/var/log/ppp.log                        600  3     100  *     Z
/var/log/security                       600  10    100  *     Z
/var/log/wtmp                           644  3     *    @01T05 B
/var/log/daily.log                      640  7     *    @T00  Z
/var/log/weekly.log                     640  5     1    $W6D0 Z
/var/log/monthly.log                    640  12    *    $M1D0 Z
/var/log/console.log                    640  5     100  *     Z
```

Consultez la page de manuel newsyslog(8) pour plus d'informations.

12.9.4. sysctl.conf

sysctl.conf ressemble à rc.conf. Les valeurs sont fixées sous la forme `variable=value`. Les valeurs spécifiées sont positionnées après que le système soit passé dans le mode multi-utilisateurs. Toutes les variables ne sont pas paramétrables dans ce mode.

Pour désactiver l'enregistrement des signaux fatals de fin de processus et empêcher les utilisateurs de voir les processus lancés par les autres, les variables suivantes peuvent être paramétrées dans sysctl.conf:

```
# Do not log fatal signal exits (e.g., sig 11)
kern.logsigexit=0

# Prevent users from seeing information about processes that
# are being run under another UID.
security.bsd.see_other_uids=0
```

12.10. Optimisation avec sysctl(8)

sysctl(8) est une interface qui vous permet d'effectuer des changements de paramétrage sur un système FreeBSD en fonctionnement. Cela comprend de nombreuses options avancées de la pile TCP/IP et du système de mémoire virtuelle qui peuvent améliorer dramatiquement les performances pour un administrateur système expérimenté. Plus de cinq cent variables système peuvent être lues et modifiées grâce à sysctl(8).

sysctl(8) remplit deux fonctions: lire et modifier les paramétrages du système.

Pour afficher toutes les variables lisibles:

```
% sysctl -a
```

Pour lire une variable particulière, par exemple, `kern.maxproc`:

```
% sysctl kern.maxproc
kern.maxproc: 1044
```

Pour fixer une variable particulière, utilisez la syntaxe intuitive *variable=valeur* :

```
# sysctl kern.maxfiles=5000
kern.maxfiles: 2088 -> 5000
```

Les valeurs des variables sysctl sont généralement des chaînes de caractères, des nombres, ou des booléens (un variable booléenne étant `1` pour oui ou un `0` pour non).

Si vous voulez fixer automatiquement certaines variables à chaque démarrage de la machine, ajoutez-les au fichier /etc/sysctl.conf. Pour plus d'information consultez la page de manuel sysctl.conf(5) et la sysctl.conf.

12.10.1. Variables sysctl(8) en lecture seule

Dans certains cas, il peut être nécessaire de modifier des variables sysctl(8) en lecture seule. Bien que cela soit parfois inévitable, cela ne peut être fait qu'au (re)démarrage de la machine.

Par exemple sur certains modèles d'ordinateurs portables le périphérique cardbus(4) ne sondera pas le système à la recherche des zones mémoires, et échouera avec des erreurs du type:

```
cbb0: Could not map register memory
device_probe_and_attach: cbb0 attach returned 12
```

Des cas comme le précédent demandent généralement la modification de paramètres sysctl(8) par défaut qui sont en lecture seule. Pour palier à ces situations un utilisateur peut placer un paramétrage ("OID"-Object IDentifier) sysctl(8) dans le fichier local /boot/loader.conf.local. Les paramétrages par défaut se trouvent dans le fichier /boot/defaults/loader.conf.

Pour corriger le problème précédent, il faudrait que l'utilisateur ajoute la ligne `hw.pci.allow_unsupported_io_range=1` dans le fichier précédemment indiqué. Désormais le périphérique cardbus(4) devrait fonctionner normalement.

12.11. Optimiser les disques

12.11.1. Les variables sysctl

12.11.1.1. `vfs.vmiodirenable`

La variable sysctl `vfs.vmiodirenable` peut être positionnée soit à 0 (désactivée) soit à 1 (activée); elle est a 1 par défaut. Cette variable spécifie comment les répertoires sont cachés par le système. La plupart des répertoires sont petits, utilisant juste un simple fragment du système de fichiers (typiquement 1KO) et moins dans le cache en mémoire (typiquement 512 octets). Avec cette variable désactivée (à 0), le cache en mémoire ne cachera qu'un nombre fixe de répertoires même

si vous disposez d'une grande quantité de mémoire. Activée (à 1), cette variable sysctl permet au cache en mémoire d'utiliser le cache des pages de mémoire virtuelle pour cacher les répertoires, rendant toute la mémoire disponible pour cacher les répertoires. Cependant, la taille minimale de l'élément mémoire utilisé pour cacher un répertoire est une page physique (typiquement 4KO) plutôt que 512 octets. Nous recommandons de conserver de cette option activée si vous faites fonctionner des services qui manipulent un grand nombre de fichiers. De tels services peuvent être des caches web, d'importants systèmes de courrier électronique, et des systèmes serveurs de groupe de discussion. Conserver cette option activée ne réduira généralement pas les performances même avec la mémoire gaspillée mais vous devriez faire des expériences pour le déterminer.

12.11.1.2. vfs.write_behind

La variable sysctl `vfs.write_behind` est positionnée par défaut à `1` (activée). Elle demande au système de fichiers d'effectuer les écritures lorsque des grappes complètes de données ont été collectées, ce qui se produit généralement lors de l'écriture séquentielle de gros fichiers. L'idée est d'éviter de saturer le cache tampon avec des tampons sales quand cela n'améliorera pas les performances d'E/S. Cependant, cela peut bloquer les processus et dans certaines conditions vous pouvez vouloir désactiver cette fonction.

12.11.1.3. vfs.hirunningspace

La variable sysctl `vfs.hirunningspace` détermine combien d'opérations d'écriture peuvent être mises en attente à tout moment au niveau des contrôleurs disques du système. La valeur par défaut est normalement suffisante mais sur les machines avec de nombreux disques, vous pouvez vouloir l'augmenter jusqu'à quatre ou cinq *méga-octets*. Notez que fixer une valeur trop élevée (dépassant la limite d'écriture du cache tampon) peut donner lieu à de très mauvaises performances. Ne fixez pas cette valeur à une valeur élevée arbitraire! Des valeurs d'écriture élevées peuvent ajouter des temps de latence aux opérations d'écriture survenant au même moment.

Il existent d'autres variables sysctl relatives aux caches tampons et aux pages VM. Nous ne recommandons pas de modifier ces valeurs, le système VM effectue un très bon travail d'auto-optimisation.

12.11.1.4. vm.swap_idle_enabled

La variable `vm.swap_idle_enabled` est utile dans le cas de systèmes multi-utilisateurs importants où il y a beaucoup d'utilisateurs s'attachant et quittant le système et de nombreux processus inactifs. De tels systèmes tendent à générer une pression assez importante et continue sur les réserves de mémoire libres. Activer cette fonction et régler l'hystéresis de libération de l'espace de pagination (en secondes d'inactivité) par l'intermédiaire des variables `vm.swap_idle_threshold1` et `vm.swap_idle_threshold2`, vous permet de diminuer la priorité des pages mémoire associées avec les processus inactifs plus rapidement qu'avec l'algorithme normal de libération. Cela aide le "daemon" de libération des pages. N'activez cette option que si vous en besoin, parce que la concession que vous faites est d'utiliser l'espace de pagination pour les pages mémoire plus tôt qu'à l'accoutumé, consommant par conséquent plus d'espace de pagination et de bande passante disque. Sur un petit système, cette option aura un effet limité mais dans le cas d'un système important qui fait appel à l'espace de pagination de façon modérée, cette option permettra au système VM de transférer l'ensemble des processus de et vers la mémoire aisément.

12.11.1.5. hw.ata.wc

FreeBSD 4.3 a flirté avec la désactivation du cache en écriture des disques IDE. Cela réduisit la bande passante en écriture des disques IDE mais fut considéré comme nécessaire en raison de sérieux problèmes de cohérence de données introduits par les fabricants de disques durs. Le problème est que les disques IDE mentent sur le moment où une écriture est réellement terminée. Avec le cache en écriture IDE activé, les disques durs IDE non seulement n'écriront pas les données dans l'ordre, mais parfois retarderont l'écriture de certains blocs indéfiniment sous une charge disque importante. Un crash ou une coupure secteur pourra être à l'origine de sérieuses corruptions du système de fichiers. Par précaution le paramétrage par défaut de FreeBSD fut modifié. Malheureusement, le résultat fut une telle perte de performances que nous avons réactivé le cache en écriture après cette version de FreeBSD. Vous devriez contrôler la valeur par défaut sur votre système en examinant la variable sysctl `hw.ata.wc`. Si le cache en écriture des disques IDE est désactivé, vous pouvez le réactiver en positionnant la variable à 1. Cela doit être fait à partir du chargeur au démarrage. Tenter de le faire après le démarrage du noyau n'aura aucun effet.

Pour plus d'informations, veuillez consulter la page de manuel ata(4).

12.11.1.6. SCSI_DELAY (kern.cam.scsi_delay)

L'option de configuration du noyau `SCSI_DELAY` peut être utilisée pour réduire le temps de démarrage du système. Le délai par défaut est important et peut être responsable de plus de `15` secondes d'attente lors du processus de démarrage. Réduire ce délai à `5` secondes est généralement suffisant (tout particulièrement avec les disques modernes). L'option de démarrage `kern.cam.scsi_delay` devrait être utilisée. Cette option de démarrage et celle de configuration du noyau acceptent des valeurs en *millisecondes* et *non pas* en *secondes*.

12.11.2. Les "Soft Updates"

Le programme tunefs(8) peut être utilisé pour régler finement un système de fichiers. Ce programme dispose de nombreuses options différentes, mais pour l'instant nous nous intéresserons uniquement à l'activation et la désactivation des "Soft Updates", ce qui fait avec:

```
# tunefs -n enable /filesystem
# tunefs -n disable /filesystem
```

Un système de fichiers ne peut être modifié avec tunefs(8) tant qu'il est monté. Un bon moment pour activer les "Soft Updates" est avant que les partitions ne soient montées en mode mono-utilisateur.

Les "Soft Updates" améliorent de façon drastique les performances sur les méta-données, principalement la création et la suppression de fichier, par l'utilisation d'un cache mémoire. Nous recommandons d'activer les "Soft Updates" sur tous vos systèmes de fichiers. Il y a deux inconvénients aux "Soft Updates" que vous devez connaître: tout d'abord, les "Soft Updates" garantissent la cohérence du système de fichiers en cas de crash mais pourront facilement être en retard de quelques secondes (voir même une minute!) dans la mise à jour du disque. Si votre système plante il se peut que vous perdiez plus de travail que dans d'autres cas. Deuxièmement, les "Soft Updates" retardent la libération des blocs du système de fichiers. Si vous avez un système de

fichiers (comme le système de fichiers racine) qui est presque plein, effectuer une mise à jour majeure, comme un `make installworld`, peut mener à un manque d'espace sur le système de fichiers et faire échouer la mise à jour.

12.11.2.1. Plus de détails à propos des "Soft Updates"

Il y a deux approches traditionnelles pour écrire les méta-données d'un système de fichiers sur le disque (mise à jour des méta-données et mise à jour des éléments sans données comme les inodes ou les répertoires).

Historiquement, le comportement par défaut était d'écrire les mises à jour des méta-données de façon synchrone. Si un répertoire a été modifié, le système attendait jusqu'à ce que le changement soit effectivement écrit sur le disque. Les tampons des données de fichier (contenu du fichier) passaient par le cache mémoire et étaient copiés sur le disque plus tard de façon asynchrone. L'avantage de cette implémentation est qu'elle est effectuée sans risque. S'il y a un problème durant une mise à jour, les méta-données sont toujours dans un état consistant. Un fichier est soit créé complètement soit pas du tout. Si les blocs de données d'un fichier n'ont pas trouvé leur chemin du cache mémoire vers le disque au moment du crash, fsck(8) est capable de s'en apercevoir et de réparer le système de fichiers en fixant la taille du fichier à 0. De plus, l'implémentation est claire et simple. L'inconvénient est que la modification des méta-données est lente. Un `rm -r`, par exemple, touche à tous les fichiers dans un répertoire séquentiellement, mais chaque modification du répertoire (effacement d'un fichier) sera écrite de façon synchrone sur le disque. Cela comprend les mises à jour du répertoire lui-même, de la table des inodes, et éventuellement celles sur des blocs indirects alloués par le fichier. Des considérations semblables s'appliquent à la création d'importantes hiérarchies ((`tar -x`).

Le deuxième cas est la mise à jour asynchrone des méta-données. C'est le comportement par défaut de Linux/ext2fs et de l'usage de `mount -o async` pour l'UFS des systèmes BSD. Toutes les mises à jour des méta-données passent également par l'intermédiaire d'un cache mémoire, c'est à dire, qu'elles seront mélangées aux mises à jour des données du contenu du fichier. L'avantage de cette implémentation est qu'il n'y a pas besoin d'attendre jusqu'à l'écriture sur le disque de chaque mise à jour de méta-données, donc toutes les opérations qui sont à l'origine d'une grande quantité de mise à jour de méta-données fonctionnent bien plus rapidement que dans le cas synchrone. De plus, l'implémentation est toujours claire et simple, il y a donc peu de risque qu'un bogue se cache dans le code. L'inconvénient est qu'il n'y a aucune garantie du tout sur la cohérence du système de fichiers. S'il y a un problème durant une opération qui met à jour une grande quantité de méta-données (comme une coupure secteur, ou quelqu'un appuyant sur le bouton reset), le système de fichiers sera laissé dans un état imprévisible. Il n'y a aucune opportunité d'examiner l'état du système de fichiers quand le système est à nouveau relancé; les blocs de données d'un fichier pourraient déjà avoir été inscrits sur le disque alors que la mise à jour de la table des inodes ou du répertoire associé n'a pas été faite. Il est en fait impossible d'implémenter un `fsck` qui est capable de nettoyer le chaos résultant (parce que l'information nécessaire n'est pas disponible sur le disque). Si le système de fichiers a été endommagé irrémédiablement, le seul choix est de le recréer avec newfs(8) et de récupérer les données à partir de sauvegardes.

La solution commune pour ce problème fut d'implémenter une *région de trace*, dont on fait souvent référence sous le terme de *journalisation*, bien que ce terme ne soit pas toujours utilisé de façon cohérente et est occasionnellement utilisé pour d'autres formes de transaction avec trace. Les mises à jour des méta-données sont toujours écrites de façon synchrone, mais seulement sur une petite

région du disque. Elles seront plus tard déplacées vers leur emplacement correct. Parce que la région de trace est une petite région contiguë sur le disque, il n'y a pas de grandes distances de déplacement pour les têtes des disques, même durant les opérations importantes, donc ces opérations sont plus rapides que les mises à jour synchrones. De plus la complexité de l'implémentation est relativement limitée, donc le risque de présence de bogues est faible. Un inconvénient est que toutes les méta-données sont écrites deux fois (une fois dans la région de trace et une fois sur l'emplacement correct) donc pour un fonctionnement normal, une baisse des performances pourra en résulter. D'autre part, dans le cas d'un crash, toutes les opérations sur les méta-données en attente peuvent rapidement être annulées ou complétées à partir de la zone de trace après le redémarrage du système, ayant pour résultat un démarrage rapide du système de fichiers.

Kirk McKusick, le développeur du FFS de Berkeley, a résolu le problème avec les "Soft Updates": toutes les mises à jour des méta-données sont conservées en mémoire et inscrites sur le disque selon une séquence ordonnée ("mise à jour ordonnée des méta-données"). Ceci a pour effet, dans le cas d'un nombre d'opérations sur les méta-données important, que les dernières mises à jour sur un élément "attrapent" les premières si ces dernières sont encore en mémoire et n'ont pas encore été inscrites sur le disque. Donc toutes les opérations sur, par exemple, un répertoire sont généralement effectuées en mémoire avant que la mise à jour ne soit écrite sur le disque (les blocs de données sont ordonnés en fonction de leur position de sorte à ce qu'ils ne soient pas sur le disque avant leur méta-données). Si le système crash, cela provoque un "retour dans les traces" implicite: toutes les opérations qui n'ont pas trouvé leur chemin vers le disque apparaissent comme si elles n'avaient jamais existé. Un état cohérent du système de fichiers est maintenu et apparaît comme étant celui de 30 ou 60 secondes plus tôt. L'algorithme utilisé garantie que toutes les ressources utilisées soient marquées avec leur bons "bitmaps": blocs et inodes. Après un crash, les seules erreurs d'allocation de ressources qui apparaissent sont les ressources qui ont été marquées comme "utilisées" et qui sont en fait "libre". fsck(8) reconnaît cette situation, et libère les ressources qui ne sont plus utilisées. On peut ignorer sans risque l'état "sale" d'un système de fichiers après un crash en forçant son montage avec `mount -f`. Afin de libérer les ressources qui peuvent être inutilisées, fsck(8) doit être exécuté plus tard. C'est l'idée qu'il y a derrière le "*background fsck*" (fsck en tâche de fond): au démarrage du système, seule un "*snapshot*" (photographie) du système de fichiers est prise. La commande `fsck` peut être exécutée plus tard sur ce système de fichiers. Tous les systèmes de fichiers peuvent être montés "sales", donc le système passe en mode multi-utilisateurs. Ensuite, les `fsck` en tâche de fond seront programmés pour tous les systèmes de fichiers pour lesquels c'est nécessaire, pour libérer les ressources qui peuvent être inutilisées (les systèmes qui n'utilisent pas les "Soft Updates" ont toujours besoin du `fsck` en avant plan).

L'avantage est que les opérations sur les méta-données sont presque aussi rapides que les mises à jour asynchrones (i.e. plus rapide qu'avec le "*logging*" - traçage, qui doit écrire les méta-données deux fois). Les inconvénients sont la complexité du code (impliquant un haut risque de bogues dans une zone qui est hautement sensible en raison de risque perte de données utilisateur), et une plus grande consommation en mémoire. De plus il y a quelques particularités que l'on peut rencontrer lors de l'utilisation. Après un crash, l'état du système apparaît être en quelque sorte "plus vieux". Dans des situations où l'approche synchrone classique aurait donné lieu à des fichiers de taille nulle restant après le `fsck`, ces fichiers n'existent pas du tout avec un système de fichiers utilisant les "Soft Updates" parce que ni les méta-données ni les contenus de fichiers n'ont jamais été inscrits sur le disque. L'espace disque n'est pas rendu tant que les mises à jour n'ont pas été inscrites sur le disque, ce qui peut se produire quelques temps après l'exécution de `rm`. Cela peut être à l'origine de

problèmes quand on installe une grande quantité de données sur un système de fichiers qui ne dispose pas de suffisamment d'espace pour contenir tous les fichiers deux fois.

12.12. Optimisation des limitations du noyau

12.12.1. Limitations sur les fichiers et les processus

12.12.1.1. `kern.maxfiles`

Le paramètre `kern.maxfiles` peut être augmenté ou diminué en fonction des besoins du système. Cette variable indique le nombre maximal de descripteurs de fichier sur votre système. Quand la table de descripteurs de fichier est pleine, le message `file: table is full` s'affichera régulièrement dans le tampon des messages système, qui peut être visualisé avec la commande `dmesg`.

Chaque fichier ouvert, chaque "socket", ou chaque emplacement en pile utilise un descripteur de fichier. Un serveur important peut facilement demander plusieurs milliers de descripteurs de fichiers, en fonction du type et du nombre de services s'exécutant en même temps.

Sous les anciennes versions de FreeBSD, la valeur par défaut de `kern.maxfile` est fixée par l'option `maxusers` dans votre fichier de configuration du noyau. `kern.maxfiles` augmente proportionnellement avec la valeur de `maxusers`. Quand vous compilez un noyau sur mesure, il est bon de paramétrer cette option en fonction de l'utilisation de votre système. Ce nombre fixe la plupart des limites pré-définies du noyau. Même si une machine de production pourra ne pas avoir en réalité 256 utilisateurs connectés simultanément, les ressources requises pourront être semblables pour un serveur web important.

La variable `kern.maxusers` est automatiquement ajustée au démarrage en fonction de la quantité de mémoire disponible dans le système, sa valeur peut être connue durant le fonctionnement du système en examinant la valeur de la variable sysctl en lecture seule: `kern.maxusers`. Certains systèmes auront besoin de valeurs plus élevées ou plus faibles pour `kern.maxusers` et pourront donc la fixer au chargement du système; des valeurs de 64, 128, ou 256 ne sont pas inhabituelles. Nous recommandons de ne pas dépasser 256 à moins que vous ayez besoin d'un grand nombre de descripteurs de fichiers; plusieurs des variables dont la valeur par défaut dépend de `kern.maxusers` peuvent être fixées individuellement au démarrage ou en fonctionnement dans le fichier /boot/loader.conf (voir la page de manuel loader.conf(5) ou le fichier /boot/defaults/loader.conf pour des exemples) ou comme décrit en d'autres endroits dans ce document.

Sous les anciennes versions, le système auto-ajuste ce paramètre pour vous si vous le fixez explicitement à `0`. En paramétrant cette option, vous devrez fixer `maxusers` à 4 au moins, en particulier si vous utilisez le système X Window ou compilez des logiciels. La raison de cela est que la valeur la plus importante que dimensionne `maxusers` est le nombre maximal de processus, qui est fixé à `20 + 16 * maxusers`, donc si vous positionnez `maxusers` à 1, alors vous ne pouvez avoir que 36 processus en simultanés, comprenant les 18, environ, que le système lance au démarrage et les 15, à peu près, que vous créerez probablement au démarrage du système X Window. Même une tâche simple comme la lecture d'une page de manuel lancera jusqu'à neuf processus pour la filtrer, la décompresser, et l'afficher. Fixer `maxusers` à 64 autorisera jusqu'à 1044 processus simultanés, ce qui devrait suffire dans la plupart des cas. Si, toutefois, vous obtenez le message d'erreur tant redouté quand vous tentez d'exécuter un nouveau programme, ou gérez un serveur avec un grand nombre

d'utilisateurs en simultanés (comme ftp.FreeBSD.org), vous pouvez toujours augmenter cette valeur et recompiler le noyau.

maxusers ne limite *pas* le nombre d'utilisateurs qui pourront ouvrir une session sur votre machine. Cette valeur dimensionne simplement différentes tables à des valeurs raisonnables en fonction du nombre maximal d'utilisateur que vous aurez vraisemblablement sur votre système et combien de processus chacun d'entre eux pourra utiliser.

12.12.1.2. kern.ipc.somaxconn

La variable sysctl kern.ipc.somaxconn limite la taille de la file d'attente acceptant les nouvelles connexions TCP. La valeur par défaut de 128 est généralement trop faible pour une gestion robuste des nouvelles connexions dans un environnement de serveur web très chargé. Pour de tels environnements, il est recommandé d'augmenter cette valeur à 1024 ou plus. Le "daemon" en service peut de lui-même limiter la taille de la file d'attente (e.g. sendmail(8), ou Apache) mais disposera, la plupart du temps, d'une directive dans son fichier de configuration pour ajuster la taille de la file d'attente. Les files d'attentes de grandes tailles sont plus adaptées pour éviter les attaques par déni de service ().

12.12.2. Limitations réseau

L'literal du noyau NMBCLUSTERS fixe la quantité de "Mbuf";s disponibles pour le système. Un serveur à fort trafic avec un nombre faible de "Mbuf";s sous-emploiera les capacités de FreeBSD. Chaque "cluster" représente approximativement 2 Ko de mémoire, donc une valeur de 1024 représente 2 mégaoctets de mémoire noyau réservée pour les tampons réseau. Un simple calcul peut être fait pour déterminer combien sont nécessaires. Si vous avez un serveur web qui culmine à 1000 connexions simultanées, et que chaque connexion consomme un tampon de réception de 16Ko et un tampon d'émission de 16 Ko, vous avez approximativement besoin de 32 Mo de tampon réseau pour couvrir les besoin du serveur web. Un bon principe est de multiplier ce nombre par 2, soit 2x32 Mo / 2 Ko = 64 Mo / 2 Ko =32768. Nous recommandons des valeurs comprises entre 4096 et 32768 pour les machines avec des quantités de mémoire plus élevées. Vous ne devriez, dans aucun circonstance, spécifier de valeur élevée arbitraire pour ce paramètre étant donné que cela peut être à l'origine d'un plantage au démarrage. L'option -m de netstat(1) peut être utilisée pour observer l'utilisation des "clusters".

La variable kern.ipc.nmbclusters configurable au niveau du chargeur est utilisée pour ajuster cela au démarrage. Seules les anciennes versions de FreeBSD vous demanderont d'utiliser l'option de configuration du noyau NMBCLUSTERS.

Pour les serveurs chargés qui font une utilisation intensive de l'appel système sendfile(2), il peut être nécessaire d'augmenter le nombre de tampons sendfile(2) par l'intermédiaire de l'option de configuration du noyau NSFBUFS ou en fixant sa valeur dans le fichier /boot/loader.conf (consultez la page de manuel loader(8) pour plus de détails). Un indicateur de la nécessité d'ajuster ce paramètre est lorsque des processus sont dans l'état sfbufa. La variable sysctl kern.ipc.nsfbufs est un aperçu en lecture seule de la variable du noyau. Ce paramètre s'ajuste de façon optimale avec kern.maxusers, il peut être cependant nécessaire de l'ajuster en fonction des besoins.

Même si une "socket" a été marquée comme étant non-bloquante, un appel de sendfile(2) sur la "socket" non-bloquante peut résulter en un blocage de l'appel sendfile(2) jusqu'à ce que suffisamment de `struct sf_buf` soient libérées.

12.12.2.1. `net.inet.ip.portrange.*`

Les variables `net.inet.ip.portrange.*` contrôlent les intervalles de ports automatiquement alloués aux "socket"s TCP et UDP. Il y a trois intervalles: un intervalle bas, un intervalle par défaut, et intervalle un haut. La plupart des programmes réseau utilisent l'intervalle par défaut qui est contrôlé par `net.inet.ip.portrange.first` et `net.inet.ip.portrange.last`, qui ont pour valeur par défaut respectivement 1024 et 5000. Ces intervalles de ports sont utilisés pour les connexions sortantes, et il est possible de se trouver à court de ports dans certaines conditions. Cela arrive le plus souvent quand votre système fait tourner un proxy web très chargé. L'intervalle de ports n'est pas un problème quand vous exécutez des serveurs qui ne gèrent principalement que des connexions entrantes, comme un server web classique, ou qui ont un nombre de connexions sortantes limitées comme un relai de messagerie. Pour les cas où vous risquez d'être à court de ports, il est recommandé d'augmenter légèrement `net.inet.ip.portrange.last`. Une valeur de `10000`, `20000` ou `30000` doit être suffisante. Vous devriez également penser au problème du coupe-feu lors du changement de l'intervalle des ports. Certains coupes-feu peuvent bloquer de grands intervalles de ports (en général les ports inférieurs) et s'attendent à ce que les systèmes utilisent les intervalles supérieurs pour les connexions sortantes - pour cette raison il n'est pas conseillé de diminuer `net.inet.ip.portrange.first`.

12.12.2.2. Le produit délai-bande passante TCP

La limitation du produit délai-bande passante TCP est semblable au TCP/Vegas sous NetBSD. Elle peut être activée en positionnant à `1` la variable `net.inet.tcp.inflight.enable`. Le système tentera alors de calculer le produit délai-bande passante pour chaque connexion et limitera la quantité de données en attente à la quantité juste nécessaire au maintient d'un flux de sortie optimal.

Cette fonctionnalité est utile si vous diffusez des données par l'intermédiaire de modems, de connexions Ethernet Gigabit, ou même de liaisons hauts débits WAN (ou toute autre liaison avec un produit délai-bande passante élevé), tout particulièrement si vous utilisez également le dimensionnement des fenêtres d'émission ou que vous avez configuré une fenêtre d'émission importante. Si vous activez cette option, vous devriez également vous assurer que `net.inet.tcp.inflight.debug` est positionnée à `0` (désactive le débogage), et pour une utilisation en production, fixer `net.inet.tcp.inflight.min` à au moins `6144` peut être bénéfique. Notez, cependant, que fixer des minima élevés peut désactiver la limitation de bande passante selon la liaison. La fonction de limitation diminue la quantité de données accumulées dans les files d'attente intermédiaire de routage et de commutation, et diminue également la quantité de données présentes dans les files d'attente de l'interface de la machine locale. Avec moins de paquets dans les files d'attente, les connexions interactives, tout particulièrement sur des modems lents, seront en mesure de fonctionner avec des *temps d'aller-retour* plus faible. Mais cette fonctionnalité n'affecte que la transmission de données (transmission côté serveur). Ceci n'a aucun effet sur la réception de données (téléchargement).

Modifier `net.inet.tcp.inflight.stab` n'est *pas* recommandé. Ce paramètre est fixé par défaut à la valeur 20, représentant au maximum 2 paquets ajoutés à la fenêtre de calcul du produit délai-

bande passante. La fenêtre supplémentaire est nécessaire pour stabiliser l'algorithme et améliorer la réponse aux changements de conditions, mais il peut en résulter des temps de "ping" plus élevés sur les liaisons lentes (mais cependant inférieurs à ce que vous obtiendriez sans l'algorithme de limitation). Dans de tels cas, vous pouvez essayer de réduire ce paramètre à 15, 10, ou 5, et vous pouvez avoir à réduire le paramètre `net.inet.tcp.inflight.min` (par exemple à 3500) pour obtenir l'effet désiré. Ces paramètres ne doivent être réduits qu'en dernier ressort.

12.12.3. Mémoire virtuelle

12.12.3.1. `kern.maxvnodes`

Un vnode est la représentation interne d'un fichier ou d'un répertoire. Augmenter le nombre de vnodes disponibles pour le système d'exploitation diminue les accès disque. Cela est normalement géré par le système d'exploitation et n'a pas besoin d'être modifié. Dans certains cas où les accès aux disques sont un goulot d'étranglement pour le système et que ce dernier est à cours de vnodes, ce nombre aura besoin d'être augmenté. La quantité de RAM libre et inactive sera prise en compte.

Pour connaître le nombre de vnodes actuellement utilisés:

```
# sysctl vfs.numvnodes
vfs.numvnodes: 91349
```

Pour connaître le maximum de vnodes utilisables:

```
# sysctl kern.maxvnodes
kern.maxvnodes: 100000
```

Si l'utilisation actuelle des vnodes est proche du maximum, augmenter de 1000 `kern.maxvnodes` est probablement une bonne idée. Gardez un oeil sur le nombre `vfs.numvnodes`. S'il approche à nouveau le maximum, `kern.maxvnodes` devra être augmenté de manière plus conséquente. Une modification dans votre utilisation de la mémoire devrait être visible dans top(1). Une plus grande quantité de mémoire devrait être annoncée comme active.

12.13. Ajouter de l'espace de pagination

Peu importe comment vous l'avez pensé, parfois un système ne fonctionne pas comme prévu. Si vous trouvez que vous avez besoin de plus d'espace de pagination, il est assez simple d'en rajouter. Vous avez trois manières d'augmenter votre espace de pagination: ajouter un nouveau disque dur, activer la pagination sur NFS, et créer un fichier de pagination sur une partition existante.

Pour des informations sur comment chiffrer l'espace de pagination, quelles options existent pour mener à bien cette tâche et pourquoi on devrait le faire, veuillez vous référer à la Chiffrage de l'espace de pagination du Manuel.

12.13.1. Espace de pagination sur un nouveau disque dur ou une partition existante

Ajouter un nouveau disque pour l'espace de pagination donne de meilleures performances qu'utiliser une partition sur un disque existant. La configuration des partitions et des disques durs est expliquée dans la Ajouter des disques tandis que la Choix du partitionnement aborde l'organisation des partitions et les problèmes relatifs à la taille de la partition de l'espace de pagination.

Utiliser la commande `swapon` pour ajouter une partition de pagination au système. Par exemple:

```
# swapon /dev/ada1s1b
```

Il est possible d'utiliser n'importe quelle partition actuellement non-montée, même si cette dernière contient des données. Utiliser `swapon` sur une partition contenant des données écrasera et effacera ces données. Assurez-vous que la partition à utiliser comme espace de pagination est bien celle prévue à cet effet avant d'exécuter `swapon`.

Pour ajouter cette partition de pagination automatiquement au démarrage, ajouter une entrée au fichier /etc/fstab:

```
/dev/ada1s1b    none    swap    sw  0   0
```

Consulter fstab(5) pour plus d'explications sur les entrées du fichier /etc/fstab. Plus d'informations sur `swapon` sont disponibles dans swapon(8).

12.13.2. Espace de pagination sur NFS

L'espace de pagination sur NFS n'est recommandé que si vous n'avez pas de disque dur local sur lequel avoir l'espace de pagination; la pagination sur NFS sera limitée par la bande passante du réseau et sera un fardeau supplémentaire pour le serveur NFS.

12.13.3. Fichiers de pagination

Vous pouvez créer un fichier d'une taille spécifique pour l'utiliser comme fichier de pagination. Dans notre exemple nous utiliserons un fichier de 64MO appelé /usr/swap0. Vous pouvez, bien sûr, utiliser le nom de votre choix.

Exemple 15. Créer un fichier de pagination sous FreeBSD

1. Le noyau GENERIC inclut déjà le pilote de disque mémoire (md(4)) nécessaire à cette opération. Lors de la compilation d'un noyau sur mesures, assurez-vous d'inclure la ligne suivante dans le fichier de configuration:

```
device   md
```

Pour plus d'information sur la compilation du noyau, veuillez vous référer à la Configurer le noyau de FreeBSD.

2. Créez un fichier de pagination (/usr/swap0):

```
# dd if=/dev/zero of=/usr/swap0 bs=1024k count=64
```

3. Fixez les bonnes permissions sur /usr/swap0:

```
# chmod 0600 /usr/swap0
```

4. Activez le fichier de pagination dans /etc/rc.conf:

```
swapfile="/usr/swap0"   # Set to name of swapfile if aux swapfile desired.
```

5. Redémarrez la machine ou activez directement le fichier de pagination:

```
# mdconfig -a -t vnode -f /usr/swap0 -u 0  swapon /dev/md0
```

12.14. Gestion de l'énergie et des ressources

Il est important d'utiliser les ressources matérielles d'une manière efficace. Avant l'apparition de l'ACPI, il était difficile pour les systèmes d'exploitation de gérer l'utilisation de l'alimentation et la température d'un système. Le matériel était géré par le BIOS et donc l'utilisateur avait moins de contrôle et de visibilité sur le paramétrage de la gestion de l'énergie. Une configuration limitée était accessible via l'*Advanced Power Management (APM)*. La gestion de l'énergie et des ressources est un des éléments clés d'un système d'exploitation moderne. Par exemple, vous pourrez vouloir qu'un système d'exploitation surveille certaines limites (et éventuellement vous alerte), au cas où la température de votre système augmente de façon inattendue.

Dans cette section, nous fournirons une information complète au sujet de l'ACPI. Il sera fait référence à des documents supplémentaires en fin de section pour plus de détails.

12.14.1. Qu'est-ce que l'ACPI?

L'"interface de configuration et d'alimentation avancée" (ACPI, Advanced Configuration and Power Interface) est une norme créée par un ensemble de constructeurs pour fournir une interface standard à la gestion des ressources et de l'énergie. C'est un élément clé dans le contrôle et la configuration par le système d'exploitation de de la gestion d'énergie, i.e., il permet plus de contrôle et flexibilité au système d'exploitation. Les systèmes modernes ont "repoussé" les limites des

interfaces "Plug and Play" antérieures à l'apparition de l'ACPI. L'ACPI est le descendant direct de l'APM (Advanced Power Management - gestion avancée de l'énergie).

12.14.2. Les imperfections de la gestion avancée de l'énergie (APM)

Le système de *gestion avancée de l'énergie (APM)* gère l'utilisation de l'énergie par un système en fonction de son activité. Le BIOS APM est fourni par le fabricant (du système) et est spécifique à la plateforme matérielle. Un pilote APM au niveau du système d'exploitation gère l'accès à l'*interface logicielle APM* qui autorise la gestion des niveaux de consommation. L'APM devrait être toujours utilisé pour les systèmes fabriqués en ou avant 2000.

L'APM présente quatre problèmes majeurs. Tout d'abord la gestion de l'énergie est effectuée par le BIOS (spécifique au constructeur), et le système d'exploitation n'en a aucune connaissance. Un exemple de ce problème, est lorsque l'utilisateur fixe des valeurs pour le temps d'inactivité d'un disque dur dans le BIOS APM, qui une fois dépassé, provoque l'arrêt du disque (par le BIOS) sans le consentement du système d'exploitation. Deuxièmement, la logique de l'APM est interne au BIOS, et agit indépendamment du système d'exploitation. Cela signifie que les utilisateurs ne peuvent corriger les problèmes de leur BIOS APM qu'en flashant un nouveau BIOS; c'est une opération dangereuse, qui si elle échoue peut laisser le système dans un état irrécupérable. Troisièmement, l'APM est une technologie spécifique au constructeur, ce qui veut dire qu'il y a beaucoup de redondances (duplication des efforts) et de bogues qui peuvent être trouvées dans le BIOS d'un constructeur, et qui peuvent ne pas être corrigées dans d'autres BIOS. Et pour terminer, le dernier problème est le fait que le BIOS APM n'a pas suffisamment d'espace pour implémenter une politique sophistiquée de gestion de l'énergie, ou une politique qui peut s'adapter parfaitement aux besoins de la machine.

Le *BIOS Plug and Play (PNPBIOS)* n'était pas fiable dans de nombreuses situations. Le PNPBIOS est une technologie 16 bits, le système d'exploitation doit utiliser une émulation 16 bits afin de faire l'"interface" avec les méthodes PNPBIOS.

Le pilote APM FreeBSD est documenté dans la page de manuel apm(4).

12.14.3. Configurer l'ACPI

Le pilote acpi.ko est par défaut chargé par le loader(8) au démarrage et ne devrait *pas* être compilé dans le noyau. La raison derrière cela est que les modules sont plus facile à manipuler, par exemple pour passer à une autre version du module acpi.ko sans avoir à recompiler le noyau. Cela présente l'avantage de rendre les tests aisés. Une autre raison est que lancer l'ACPI après qu'un système ait terminé son lancement donne souvent lieu à des dysfonctionnements. Si des problèmes surviennent, vous pouvez désactiver l'ACPI. Ce pilote ne devrait et ne peut être déchargé car le bus système l'utilise pour différentes intéraction avec le matériel. L'ACPI peut être déactivé en ajoutant `hint.acpi.0.disabled="1"` dans le fichier /boot/loader.conf ou directement à l'invite du chargeur (loader(8)).

L'ACPI et l'APM ne peuvent coexister et devraient être utilisé séparément. Le dernier chargé s'arrêtera s'il détecte l'autre en fonctionnement.

L'ACPI peut être utilisé pour mettre en veille un système avec acpiconf(8), les options `-s` et `1-5`. La plupart des utilisateurs n'auront besoin que de `1` ou `3` (système suspendu en RAM). L'option `5`

provoquera un arrêt de l'alimentation par logiciel, effet identique à un:

```
# halt -p
```

D'autres options sont disponibles via sysctl(8). Consultez les pages de manuel acpi(4) et acpiconf(8) pour plus d'informations.

12.15. Utiliser et déboguer l'ACPI sous FreeBSD

L'ACPI est une nouvelle méthode de recherche des périphériques, de gestion de l'énergie, et fourni un accès standardisé à différents matériels gérés auparavant par le BIOS. Des progrès ont été fait vers un fonctionnement de l'ACPI sur tous les systèmes, mais des bogues dans le "bytecode" du *langage machine ACPI* (*ACPI Machine Language*-AML), des imperfections dans les sous-systèmes du noyau FreeBSD, et des bogues dans l'interpréteur ACPI-CA d'Intel® continuent d'apparaître.

Ce document est destiné à vous permettre d'aider les développeurs du système ACPI sous FreeBSD à identifier la cause originelle des problèmes que vous observez et à déboguer et développer une solution. Merci de lire ce document et nous espérons pouvoir résoudre les problèmes de votre système.

12.15.1. Soumettre des informations de débogage

Avant de soumettre un problème, assurez-vous d'utiliser la dernière version de votre BIOS, et si elle est disponible, la dernière version du firmware du contrôleur utilisé.

Pour ceux désirant soumettre directement un problème, veuillez faire parvenir les informations suivantes à la liste freebsd-acpi@FreeBSD.org:

- Description du comportement défectueux, en ajoutant le type et le modèle du système et tout ce qui peut causer l'apparition du bogue. Notez également le plus précisément possible quand le bogue a commencé à se manifester s'il est nouveau.
- La sortie de dmesg(8) après un `boot -v`, y compris tout message généré lors de la manifestation du bogue.
- La sortie de dmesg(8) après un `boot -v` avec l'ACPI désactivé, si cette désactivation corrige le problème.
- La sortie de `sysctl hw.acpi`. C'est également un bon moyen de déterminer quelles fonctionnalités sont offertes par votre système.
- Une URL où peut être trouvé votre *code source ACPI* (ACPI Source Language-ASL). N'envoyez pas directement l'ASL sur la liste de diffusion, ce fichier peut être très gros. Vous pouvez générer une copie de votre ASL en exécutant la commande suivante:

  ```
  # acpidump -dt > name-system.asl
  ```

(Remplacez *name* par votre nom d'utilisateur et *system* par celui du constructeur/modèle. Par exemple: njl-FooCo6000.asl)

La plupart des développeurs lisent la liste liste de diffusion à propos de la branche FreeBSD-CURRENT mais soumettez également les problèmes rencontrés à la liste liste de diffusion concernant ACPI sous FreeBSD afin d'être sûr qu'ils seront vus. Soyez patient, nous avons tous un travail à plein temps qui nous attend ailleurs. Si votre bogue n'est pas immédiatement apparent, nous vous demanderons probablement de soumettre un PR par l'intermédiaire de send-pr(1). Quand vous remplirez un PR, veillez à inclure les mêmes informations que celles précisées précédemment. Cela nous aidera à cerner et à résoudre le problème. N'envoyez pas de PR sans avoir contacté auparavant la liste liste de diffusion concernant ACPI sous FreeBSD étant donné que nous utilisons les PRs comme pense-bêtes de problèmes existants, et non pas comme mécanisme de rapport. Il se peut que votre problème puisse avoir déjà été signalé par quelqu'un d'autre.

12.15.2. Information de fond

L'ACPI est présent sur tous les ordinateurs modernes compatibles avec l'une des architectures ia32 (x86), ia64 (Itanium), et amd64 (AMD). La norme complète définit des fonctionnalités comme la gestion des performances du CPU, des contrôles des niveaux d'énergie, des zones de températures, divers systèmes d'utilisation des batteries, des contrôleurs intégrés, et l'énumération du bus. La plupart des systèmes n'implémentent pas l'intégralité des fonctionnalités de la norme. Par exemple, un ordinateur de bureau n'implémentera généralement que la partie énumération de bus alors qu'un ordinateur portable aura également le support de la gestion du refroidissement et de la batterie. Les ordinateurs portables disposent également des modes de mise en veille et de réveil, avec toute la complexité qui en découle.

Un système compatible ACPI dispose de divers composants. Les fabricants de BIOS et de circuits fournissent des tables de description (FADT) fixes en mémoire qui définissent des choses comme la table APIC (utilisée par les systèmes SMP), les registres de configuration, et des valeurs de configuration simples. De plus, est fournie une table de "bytecode" (la *table différenciée de description du système-Differentiated System Description Table* DSDT) qui spécifie sous forme d'une arborescence l'espace des noms des périphériques et des méthodes.

Le pilote ACPI doit analyser les tables, implémenter un interpréteur pour le "bytecode", et modifier les pilotes de périphériques et le noyau pour qu'ils acceptent des informations en provenance du sous-système ACPI. Pour FreeBSD, Intel® fourni un interpréteur (ACPI-CA) qui est partagé avec Linux et NetBSD. L'emplacement du code source de l'interpréteur ACPI-CA est src/sys/contrib/dev/acpica. Le code "glu" permettant à ACPI-CA de fonctionner sous FreeBSD se trouve dans src/sys/dev/acpica/Osd. Et enfin, les pilotes qui gèrent les différents périphériques ACPI se trouvent dans src/sys/dev/acpica.

12.15.3. Problèmes courants

Pour un fonctionnement correct de l'ACPI, il faut que toutes les parties fonctionnent correctement. Voici quelques problèmes courants, par ordre de fréquence d'apparition, et quelques contournements ou corrections possibles.

12.15.3.1. Problèmes avec la souris

Dans certains cas le réveil après une mise en veille sera à l'origine d'un dysfonctionnement de la souris. Une solution connue est d'ajouter la ligne `hint.psm.0.flags="0x3000"` au fichier /boot/loader.conf. Si cela ne fonctionne pas, pensez à envoyer un rapport de bogue comme décrit plus haut.

12.15.3.2. Mise en veille/réveil

L'ACPI dispose de trois modes de mise en veille en RAM (STR-Suspend To RAM), `S1` à `S3`, et un mode de mise en veille vers le disque dur (`STD`-Suspend To Disk), appelé `S4`. Le mode `S5` est un arrêt "soft" et est le mode dans lequel se trouve votre système quand il est branché mais pas allumé. Le mode `S4` peut être implémenté de deux manières différentes. Le mode `S4`BIOS est une mise en veille vers le disque assistée par le BIOS. Le mode `S4`OS est implémenté intégralement par le système d'exploitation.

Commencez par examiner la sortie de `sysctl hw.acpi` à la recherche d'éléments concernant les modes de mise en veille. Voici les résultats pour un Thinkpad:

```
hw.acpi.supported_sleep_state: S3 S4 S5
hw.acpi.s4bios: 0
```

Cela signifie que nous pouvons utiliser `acpiconf -s` pour tester les modes `S3`, `S4`OS, et `S5`. Si `s4bios` était égal à `1`, nous disposerions d'un support `S4`BIOS à la place de `S4`OS.

Quand vous testez la mise en veille et le réveil, commencez avec le mode `S1`, pour voir s'il est supporté. Ce mode doit fonctionner dans la plupart des cas puisqu'il nécessite peu de support. Le mode `S2` n'est pas implémenté, mais si vous en disposez, il est similaire au mode `S1`. La chose suivante à essayer est le mode `S3`. C'est le mode STR le plus avancé et il nécessite un support du pilote important pour réinitialiser correctement votre matériel. Si vous avez des problèmes au réveil de la machine, n'hésitez pas à contacter la liste liste de diffusion concernant ACPI sous FreeBSD mais ne vous attendez pas à ce que le problème soit résolu puisqu'il y a de nombreux pilotes/matériels qui nécessitent plus de tests et de développement.

Un problème courant avec la mise en veille/le réveil est que de nombreux pilotes de périphériques ne sauvegardent pas, ne restaurent pas, ou ne réinitialisent pas leurs logiciel, registres ou mémoire proprement. En premier lieu pour débogguer le problème, essayez:

```
# sysctl debug.bootverbose=1
# sysctl debug.acpi.suspend_bounce=1
# acpiconf -s 3
```

Ce test émule le cycle de mise en veille/réveil de tous les pilotes de périphériques sans réellement passer dans l'état `S3`. Dans certains cas, les problèmes comme la perte de l'état du périphérique, le dépassement du délai du chien de garde du périphérique, les tentatives répétées, peuvent être capturés avec cette méthode. Notez que le système n'entrera pas vraiment dans l'état `S3`, ce qui signifie que les périphériques peuvent ne pas perdre leur alimentation, et nombreux fonctionneront correctement même si les méthodes de mise en veille/réveil sont totalement

absentes, contrairement au cas d'un véritable état `S3`.

Les cas plus difficiles nécessitent un matériel supplémentaire, tel qu'un port série et un câble pour débogguer à l'aide d'une console série, un port firewire et un câble pour l'utilisation de dcons(4), et des compétences en debogguage du noyau.

Pour isoler le problème, retirez du noyau tous les pilotes de périphériques possibles. Si cela fonctionne, vous pouvez alors identifier le pilote fautif en chargeant les pilotes un à un jusqu'à l'apparition du problème. Généralement les pilotes binaires comme nvidia.ko, les pilotes d'affichage X11, ou les pilotes USB seront victimes de la plupart des problèmes tandis que ceux concernant les interfaces Ethernet fonctionneront normalement. Si vous pouvez charger/décharger les pilotes de périphériques correctement, vous pouvez automatiser cela en ajoutant les commandes appropriées dans les fichiers /etc/rc.suspend et /etc/rc.resume. Il y a un exemple en commentaire pour décharger ou charger un pilote. Essayez de fixer `hw.acpi.reset_video` à zéro (`0`) si votre affichage est corrompu après un réveil de la machine. Essayez des valeurs plus grandes ou plus faibles pour `hw.acpi.sleep_delay` pour voir si cela aide.

Une autre méthode est d'essayer de charger une distribution Linux récente avec le support ACPI et tester la mise en veille et le réveil sur le même matériel. Si cela fonctionne sous Linux, c'est probablement donc un problème de pilotes FreeBSD et déterminer quel pilote est responsable des dysfonctionnements nous aidera à corriger le problème. Notez que les personnes qui maintiennent l'ACPI sous FreeBSD ne s'occupe pas généralement des autres pilotes de périphériques (comme le son, le système ATA, etc.), aussi tout rapport concernant un problème de pilote devrait probablement en fin de compte être posté sur la liste liste de diffusion à propos de la branche FreeBSD-CURRENT et communiqué au responsable du pilote. Si vous vous sentez une âme d'aventurier, commencez à ajouter des printf(3)s de débogage dans un pilote problématique pour déterminer à quel moment dans sa fonction de réveil il se bloque.

Enfin, essayez de désactiver l'ACPI et d'activer l'APM à la place, pour voir si la mise en veille et le réveil fonctionnent avec l'APM, tout particulièrement dans le cas de matériel ancien (antérieur à 2000). Cela prend du temps aux constructeurs de mettre en place le support ACPI et le matériel ancien aura sûrement des problèmes de BIOS avec l'ACPI.

12.15.3.3. Blocages du système (temporaires ou permanents)

La plupart des blocages système sont le résultat d'une perte d'interruptions ou d'une tempête d'interruptions. Les circuits ont beaucoup de problèmes en fonction de la manière dont le BIOS configure les interruptions avant le démarrage, l'exactitude de la table APIC (MADT), et le routage du *System Control Interrupt* (SCI).

Les tempêtes d'interruptions peuvent être distinguées des pertes d'interruptions en contrôlant la sortie de la commande `vmstat -i` en examinant la ligne mentionnant `acpi0`. Si le compteur s'incrémente plusieurs fois par seconde, vous êtes victime d'une tempête d'interruptions. Si le système semble bloqué, essayez de basculer sous DDB (`CTRL` + `ALT` + `ESC` sous la console) et tapez `show interrupts`.

Votre plus grand espoir quand vous faites face à des problèmes d'interruptions est d'essayer de désactiver le support APIC avec la ligne `hint.apic.0.disabled="1"` dans le fichier loader.conf.

12.15.3.4. Paniques

Les paniques sont relativement rares dans le cas de l'ACPI et sont au sommet des priorités en matière de problèmes à corriger. Le premier point est d'isoler les étapes nécessaires à la reproduction de la panique (si possible) et d'obtenir une trace de débogage. Suivez l'aide sur l'activation de `options DDB` et la configuration d'une console série (lire la Entering the DDB Debugger from the Serial Line) ou la configuration d'une partition dump(8). Vous pouvez obtenir une trace de débogage sous DDB avec la commande `tr`. Si vous devez recopier à la main la trace de débogage, assurez-vous de relever les cinq dernières lignes et les cinq premières ligne de la trace.

Ensuite essayez d'isoler le problème en démarrant avec l'ACPI désactivé. Si cela fonctionne, vous pouvez isoler le sous-système ACPI en utilisant différentes valeurs pour l'option `debug.acpi.disable`. Consultez la page de manuel acpi(4) pour des exemples.

12.15.3.5. Le système redémarre après une mise en veille ou un arrêt

Tout d'abord, essayez de fixer `hw.acpi.disable_on_poweroff="0"` dans loader.conf(5). Cela empêche l'ACPI de désactiver divers événements lors du processus d'arrêt. Certains systèmes ont besoin d'avoir cette valeur fixée à `1` (valeur par défaut) pour la même raison. Cela corrige généralement le problème d'un système démarrant spontanément après une mise en veille ou un arrêt.

12.15.3.6. Autres problèmes

Si vous rencontrez d'autres problèmes avec l'ACPI (impossible de travailler avec une station d'amarrage, périphériques non détectés, etc.), veuillez envoyer un courrier descriptif à la liste de diffusion; cependant, certains de ces problèmes peuvent être relatifs à des partie incomplètes du sous-système ACPI et qui pourront prendre du temps à être implémentées. Soyez patient et prêt à tester les correctifs que nous pourront éventuellement vous envoyer.

12.15.4. ASL, `acpidump`, et IASL

Le problème le plus courant est le fait que les constructeurs fournissent des "bytecodes" erronés (ou plus simplement bogués!). Cela se manifeste généralement sur la console par des messages du noyau du type:

```
ACPI-1287: *** Error: Method execution failed [\\_SB_.PCI0.LPC0.FIGD._STA] \\
(Node 0xc3f6d160), AE_NOT_FOUND
```

La plupart du temps vous pouvez corriger ces problèmes en mettant à jour votre BIOS avec la dernière version disponible. La majorité des messages sur la console sont inoffensifs mais si vous avez d'autres problèmes comme l'état de la batterie qui ne fonctionne pas, ce sont de bonnes raisons pour commencer à jeter un oeil à ces problèmes dans l'AML. Le "bytecode", connu sous le nom d'AML, est compilé à partir d'un langage source appelé ASL. L'AML se trouve dans une table appelée DSDT. Pour obtenir une copie de votre ASL, utilisez acpidump(8). Vous devriez utiliser de paire les options `-t` (qui affiche le contenu des tables fixes) et `-d` (qui désassemble l'AML en ASL). Consultez la section Soumettre des informations de déboguage pour un exemple de syntaxe.

Le tout premier test que vous pouvez effectuer est de recompiler votre ASL à la recherche

d'erreurs. Les avertissements peuvent être généralement ignorés mais les erreurs sont des bogues qui normalement empêchent l'ACPI de fonctionner correctement. Pour recompiler votre ASL, utilisez la commande suivante:

```
# iasl your.asl
```

12.15.5. Correction de votre ASL

A long terme, notre objectif est que tout le monde puisse avoir un système ACPI fonctionnant sans aucune intervention de l'utilisateur. Actuellement, nous sommes toujours en train de développer des solutions pour contourner les erreurs courantes faites par les fabricants de BIOS. L'interpréteur de Microsoft® (acpi.sys et acpiec.sys) ne contrôle pas de façon stricte la conformité avec la norme, et par conséquent de nombreux fabricants de BIOS qui testent l'ACPI uniquement sous Windows® ne corrigent donc jamais leur ASL. Nous espérons poursuivre à identifier et documenter avec exactitude les comportements non-standards autorisés par l'interpréteur de Microsoft® et les reproduire de manière à permettre à FreeBSD de fonctionner sans obliger les utilisateurs à corriger leur ASL. Comme solution et pour nous aider à identifier ces comportements, vous pouvez corriger manuellement votre ASL. Si cela fonctionne pour vous, veuillez nous envoyer un diff(1) de l'ancien et du nouveau ASL de façon à ce que nous puissions corriger le comportement incorrect dans ACPI-CA et rendre donc inutile à l'avenir votre correctif.

Voici une liste des messages d'erreur courants, leur cause, et comment les corriger:

12.15.5.1. Dépendances _OS

Certains AMLs supposent que le monde n'est fait de que différentes versions de Windows®. Vous pouvez demander à FreeBSD de s'annoncer comme étant n'importe quel système d'exploitation pour voir si cela corrige les problèmes que vous pouvez rencontrer. Une manière simple de faire cela est de fixer la variable `hw.acpi.osname="Windows 2001"` dans /boot/loader.conf ou avec une autre chaîne de caractères que vous trouvez dans l'ASL.

12.15.5.2. `Missing Return statements`

Certaines méthodes ne renvoient pas explicitement une valeur comme la norme le demande. Bien qu'ACPI-CA ne gère pas cela, FreeBSD contourne ce problème en renvoyant implicitement la valeur. Vous pouvez également ajouter des "Return statements" explicites où cela est nécessaire si vous connaissez la valeur à renvoyer. Pour forcer `iasl` à compiler l'ASL, utilisez l'option `-f`.

12.15.5.3. Remplacer l'AML par défaut

Après avoir personnalisé votre.asl, vous voudrez le compiler, pour cela exécutez:

```
# iasl your.asl
```

Vous pouvez ajouter l'option `-f` pour forcer la création de l'AML, même s'il y a des erreurs lors de la compilation. Rappelez-vous que certaines erreurs (e.g., `missing Return statements`) sont automatiquement contournées par l'interpréteur.

DSDT.aml est le fichier de sortie par défaut pour `iasl`. Vous pouvez le charger à la place de la version boguée de votre BIOS (qui est toujours présent dans la mémoire flash) en éditant le fichier /boot/loader.conf comme suit:

```
acpi_dsdt_load="YES"
acpi_dsdt_name="/boot/DSDT.aml"
```

Assurez-vous de bien copier votre fichier DSDT.aml dans le répertoire /boot.

12.15.6. Obtenir d'ACPI une sortie de débogage

Le pilote ACPI dispose d'une fonction de débogage très flexible. Elle vous permet de spécifier un ensemble de sous-systèmes ainsi que le niveau de verbosité. Les sous-systèmes que vous désirez déboguer sont indiqués sous la forme de "couches" et sont divisés en composants ACPI-CA (ACPI_ALL_COMPONENTS) et en supports matériel ACPI (ACPI_ALL_DRIVERS). La verbosité de la sortie de débogage est spécifiée par un "niveau" et des intervalles de ACPI_LV_ERROR (rapporte juste les erreurs) à ACPI_LV_VERBOSE (tout). Le "niveau" est un masque de bits séparés par des espaces, aussi de nombreuses options peuvent être fixées à la fois. Dans la pratique, vous voudrez utiliser un console série pour afficher la sortie si les informations de débogage sont si importantes qu'elles dépassent le tampon des messages de la console. Une liste complète des couches individuelles et des niveaux peut être trouvée dans la page de manuel acpi(4).

L'affichage des informations de débogage n'est pas activé par défaut. Pour l'activer, ajoutez la ligne `options ACPI_DEBUG` à votre fichier de configuration du noyau si l'ACPI est compilé dans le noyau. Vous pouvez ajouter la ligne `ACPI_DEBUG=1` à votre fichier /etc/make.conf pour l'activer de façon globale. Si l'ACPI est sous forme de module, vous pouvez recompiler votre module acpi.ko comme suit:

```
# cd /sys/modules/acpi/acpi
&& make clean &&
make ACPI_DEBUG=1
```

Installez acpi.ko dans le répertoire /boot/kernel et indiquez le niveau et la couche désirée dans loader.conf. L'exemple suivant active les messages de débogage pour tous les composants ACPI-CA et tous les pilotes de matériel ACPI (CPU, LID, etc.). Il n'affichera que les messages d'erreur, c'est le niveau le moins verbeux.

```
debug.acpi.layer="ACPI_ALL_COMPONENTS ACPI_ALL_DRIVERS"
debug.acpi.level="ACPI_LV_ERROR"
```

Si l'information que vous voulez est déclenchée par un événement particulier (disons par exemple une mise en veille suivi d'un réveil), vous pouvez abandonner les modifications dans loader.conf et utiliser à la place `sysctl` pour indiquer la couche et le niveau après le démarrage et préparer votre système pour cet événement particulier. Les variables `sysctl` sont appelées de la même manière que dans le fichier loader.conf.

12.15.7. Références

Plus d'information au sujet de l'ACPI peut être trouvé aux emplacements suivants:

- La liste de diffusion liste de diffusion concernant ACPI sous FreeBSD
- Les archives de la liste de diffusion ACPI http://lists.freebsd.org/pipermail/freebsd-acpi/
- Les archives de l'ancienne liste de diffusion ACPI http://home.jp.FreeBSD.org/mail-list/acpi-jp/
- La spécification ACPI
- Les pages de manuel: acpi(4), acpi_thermal(4), acpidump(8), iasl(8), acpidb(8)
- Ressource sur le débogage de la DSDT. (Utilise un exemple basé sur du matériel Compaq mais qui est en général intéressant.)

Chapitre 13. Processus de démarrage de FreeBSD

13.1. Synopsis

L'action de démarrer un ordinateur et de charger le système d'exploitation est désignée sous le nom de "processus de bootstrap", ou simplement démarrage. Le processus de démarrage de FreeBSD fournit une grande flexibilité en adaptant ce qui se passe quand vous démarrez le système, vous permettant de choisir parmi les différents systèmes d'exploitation installés sur l'ordinateur, ou même parmi les différentes versions du même système d'exploitation ou du noyau installées.

Ce chapitre détaille les options de configuration que vous pouvez paramétrer et comment personnaliser le processus de démarrage de FreeBSD. Cela inclut tout ce qui se produit jusqu'au démarrage du noyau FreeBSD, la détection des périphériques, et le démarrage d'init(8). Si vous n'êtes pas tout à fait sûr du moment auquel cela arrive, cela se produit à l'instant où la couleur du texte passe d'un blanc lumineux au gris.

Après la lecture de ce chapitre, vous connaîtrez:

- Quels sont les composants du système de démarrage de FreeBSD, et comment ils agissent les uns sur les autres.
- Les options que vous pouvez passer aux composants du système de démarrage de FreeBSD pour contrôler le processus.
- Les bases du système device.hints(5).

x86 seulement

Ce chapitre ne décrit que le processus de démarrage de FreeBSD pour les systèmes Intel x86.

13.2. Le problème du démarrage

Allumer un ordinateur et démarrer le système d'exploitation pose un intéressant dilemme. Par définition, l'ordinateur ne sait rien faire jusqu'à ce que le système d'exploitation soit lancé. Ceci inclut l'exécution des programmes à partir du disque. Donc si l'ordinateur ne peut pas exécuter de programme à partir du disque sans le système d'exploitation, et que les programmes du système d'exploitation sont sur le disque, comment le système d'exploitation est-il démarré?

On peut faire le parallèle avec un événement du livre Les aventures du Baron Munchausen. Le personnage tombe dans une bouche d'égout avec une partie du corps hors de la bouche, et il s'en sort en attrapant les fixations de ses bottes ("bootstraps"), et en se soulevant ainsi. Dans les premiers jours de l'informatique le terme *bootstrap* fut appliqué au mécanisme utilisé pour charger le système d'exploitation, terme qui a été raccourci en "booting" (que l'on traduit par démarrage en Français).

Sur l'architecture x86 c'est le BIOS ("Basic Input/Output System") qui est responsable du

chargement du système d'exploitation. Pour effectuer cela, le BIOS recherche sur le disque dur le "Master Boot Record" - Secteur Principal de Démarrage (MBR), qui doit être placé à un endroit bien précis sur le disque. Le BIOS dispose de suffisamment de connaissances pour charger et exécuter le MBR, et suppose que le MBR peut alors effectuer le reste des tâches impliquées dans le chargement du système d'exploitation, probablement avec l'aide du BIOS.

Pour parler du code contenu dans le MBR, on fait souvent référence aux termes de *gestionnaire de démarrage gestionnaire d'amorce*, tout particulièrement quand il y a intéraction avec l'utilisateur. Dans ce cas le code de ce gestionnaire occupe un espace plus important sur la première *piste* du disque ou du système de fichier du système d'exploitation (le gestionnaire de démarrage est parfois également appelé gestionnaire de chargement ou chargeur, "boot loader", sous FreeBSD ce terme est utilisé pour une étape ultérieur du démarrage). Parmi les gestionnaire de démarrage populaire, se trouvent boot0 (également connu sous le nom de Boot Easy, le gestionnaire de démarrage standard de FreeBSD), Grub, GAG, et LILO (seul boot0 peut tenir entièrement dans l'espace du MBR.).

Si vous n'avez qu'un seul système d'exploitation installé sur vos disques alors le MBR PC standard sera suffisant. Ce MBR recherche la première tranche ("slice") amorçable (souvent appelée active) sur le disque, et puis exécute le code sur cette tranche pour charger le reste du système d'exploitation. Le MBR installé par fdisk(8) par défaut se comporte de cette manière. Il est basé sur /boot/mbr.

Si vous avez installé plusieurs systèmes d'exploitation sur vos disques alors vous pouvez installer un gestionnaire d'amorce différent, qui permet d'afficher une liste des différents systèmes d'exploitation, et vous permet de sélectionner celui à partir duquel démarrer. Ceci est abordé dans la sous-section suivante.

Le reste du système de démarrage de FreeBSD est divisé en trois étapes. La première étape est exécutée par le MBR, qui en sait juste assez pour mettre l'ordinateur dans un état spécifique et lancer la deuxième étape. La seconde étape peut en faire un peu plus, avant de lancer la troisième étape. La troisième étape termine la tâche de chargement du système d'exploitation. La tâche a été séparée en trois étapes parce que le standard PC impose des limites sur la taille des programmes qui peuvent être exécutés aux étapes une et deux. L'enchaînement des tâches permet à FreeBSD de fournir un chargeur plus flexible.

Le noyau est ensuite démarré et commence à sonder le système à la recherche de périphériques et les initialise. Une fois le processus de démarrage du noyau achevé, le noyau passe la main au processus init(8), qui alors vérifie que les disques sont utilisables. init(8) commence ensuite la configuration des ressources au niveau utilisateur, monte les systèmes de fichiers, initialise les cartes réseaux pour communiquer sur le réseau, et lance tous les processus qui sont habituellement exécutés au démarrage d'un système FreeBSD.

13.3. Le gestionnaire de démarrage et les étapes de démarrage

13.3.1. Le gestionnaire de démarrage

Le code contenu dans le MBR ou gestionnaire de démarrage ou d'amorce est parfois appelé *étape*

zéro du processus de démarrage. Cette section discute de deux gestionnaires de démarrage précédemment mentionnés: boot0 et LILO.

Le gestionnaire d'amorce boot0: Le MBR installé par l'installateur FreeBSD ou par boot0cfg(8) est basé sur /boot/boot0. (boot0 est très simple, puisque le programme dans le ne peut pas occuper plus de 446 octets en raison de la table de partition principale et l'identifiant `0x55AA` à la fin du MBR). Si vous avez installé boot0 et plusieurs systèmes d'exploitation sur vos disques durs alors vous verrez un affichage semblable à celui-ci au démarrage:

Exemple 16. Ecran de boot0

```
F1 DOS
F2 FreeBSD
F3 Linux
F4 ??
F5 Drive 1

Default: F2
```

D'autres systèmes d'exploitation, en particulier Windows®, sont connus pour écraser le MBR existant avec le leur. Si cela vous arrive, ou que vous désirez remplacer le MBR existant avec le MBR de FreeBSD alors utilisez la commande suivante:

```
# fdisk -B -b /boot/boot0 device
```

où *device* est le périphérique à partir duquel vous démarrez, comme ad0 pour le premier disque IDE, ad2 pour le premier disque IDE sur le second contrôleur IDE, da0 pour le premier disque SCSI, et ainsi de suite. Ou, si vous voulez une configuration sur mesure du MBR, employez boot0cfg(8).

Le gestionnaire de démarrage LILO: Pour installer ce gestionnaire de manière à ce qu'il amorce également FreeBSD, démarrez tout d'abord Linux et ajoutez ce qui suit au fichier de configuration /etc/lilo.conf:

```
other=/dev/hdXY
table=/dev/hdX
loader=/boot/chain.b
label=FreeBSD
```

Dans ce qui précède, précisez la partition primaire et le disque FreeBSD en utilisant les paramètres propres à Linux, en remplaçant *X* avec la lettre correspondant au disque Linux et *Y* avec le numéro de la partition primaire Linux. Si vous utilisez un disque SCSI, vous changerez */dev/hd* pour quelque chose de semblable à */dev/sd*. La ligne `loader=/boot/chain.b` peut être omise si vous avez les deux systèmes d'exploitation sur le même disque. Lancez maintenant la commande `/sbin/lilo -v` pour entériner vos modifications; des messages de contrôle devraient s'afficher, vérifiant ces modifications.

13.3.2. Etape une, /boot/boot1, et étape deux, /boot/boot2

Conceptuellement la première et la seconde étapes font partie du même programme, sur le même emplacement du disque. Mais en raison de contraintes d'espace elles ont été divisées en deux, mais vous les installerez toujours de paire. Elles sont copiées, à partir du fichier combiné /boot/boot, par l'installateur ou bsdlabel (voir plus bas).

On les trouve en dehors des systèmes de fichiers, sur la première piste de la tranche de démarrage, à partir du premier secteur. C'est l'endroit où boot0, ou tout autre gestionnaire de démarrage s'attend à trouver le code à exécuter pour continuer le processus de démarrage. Le nombre de secteurs utilisés est facilement déterminé à partir de la taille du fichier /boot/boot.

boot1 est très simple, puisqu'il est limité à 512 octets, et en sait juste assez du *bsdlabel* de FreeBSD, qui contient l'information sur la tranche, pour trouver et lancer boot2.

boot2 est légèrement plus sophistiqué, et en connaît assez sur le système de fichiers de FreeBSD pour y trouver des fichiers, et il peut également fournir une interface simple pour sélectionner un noyau ou un chargeur à exécuter.

Comme le chargeur est beaucoup plus sophistiqué, et dispose d'une interface de configuration du démarrage facile d'emploi, boot2 l'exécute habituellement, bien que précédemment, c'est lui qui lançait directement le noyau.

Exemple 17. Ecran de boot2

```
>> FreeBSD/i386 BOOT
Default: 0:ad(0,a)/boot/loader
boot:
```

Si vous avez un jour besoin de remplacer boot1 et boot2, utilisez bsdlabel(8):

```
# bsdlabel -B diskslice
```

où *diskslice* est le disque et la tranche à partir de laquelle vous démarrez, comme ad0s1 pour la première tranche sur le premier disque IDE.

Mode dangereusement dédié

Si vous utilisez juste le nom du disque, comme ad0, dans la commande bsdlabel(8) vous créerez un disque dangereusement dédié, sans tranches. Ce n'est presque certainement pas ce que vous voulez faire, donc vérifiez à deux fois la commande bsdlabel(8) avant d'appuyer sur `Entrée`.

13.3.3. Etape trois, /boot/loader

Le chargeur est la dernière étape du processus de démarrage en trois temps, et il réside sur le système de fichiers, c'est habituellement le fichier /boot/loader.

Le chargeur a pour objet de fournir une méthode de configuration conviviale, en utilisant un jeu de commandes faciles d'emploi, doublé d'un interpréteur plus puissant, avec un ensemble de commandes plus complexes.

13.3.3.1. Déroulement des opérations du chargeur

A l'initialisation, le chargeur recherchera la console et les disques, et déterminera à partir de quel disque démarrer. Il positionnera les variables en conséquence, et un interpréteur sera lancé pour lequel l'utilisateur pourra passer des commandes par l'intermédiaire d'une procédure ou de façon interactive.

Le chargeur lira ensuite /boot/loader.rc, qui lui ira lire dans /boot/defaults/loader.conf les valeurs par défaut des variables à positionner et dans /boot/loader.conf les variantes locales de ces dernières. loader.rc se sert de ces variables pour charger les modules et le noyau sélectionnés.

Finalement, par défaut, le chargeur attend 10 secondes l'appui sur une ou plusieurs touches, et démarre le noyau s'il n'est pas interrompu. S'il est interrompu, une invite est alors affichée à l'utilisateur, un jeu de commandes simples permet à l'utilisateur de modifier des variables, charger ou décharger des modules, et enfin démarrer ou redémarrer.

13.3.3.2. Commandes intégrées au chargeur

Voici les commandes du chargeur les plus utilisées. Pour une information complète sur toutes les commandes disponibles, veuillez consulter la page loader(8).

autoboot *secondes*

Démarre le noyau si elle n'est pas interrompue dans le laps de temps donné en secondes. Elle affiche un compte à rebours, et le délai par défaut est de 10 secondes.

boot [-options] [nom_du_noyau]

Démarre immédiatement le noyau dont le nom est indiqué, avec les options données, s'il y en a.

boot-conf

Passe par la même configuration automatique des modules basée sur des variables comme ce qui se produit au démarrage. Cela n'a de sens que si vous utilisez `unload` en premier, et modifiez certaines variables, généralement `kernel`.

help [sujet]

Affiche les messages d'aide contenus dans /boot/loader.help. Si le sujet donné est `index`, alors c'est la liste de tous les sujets existants qui est donnée.

include *nom_du_fichier ...*

Traite le fichier dont le nom est donné. Le fichier est lu, et interprété ligne par ligne. Une erreur stoppe immédiatement le traitement.

load [-t type] *nom_du_fichier*

Charge le noyau, le module, ou le fichier du type donné, dont le nom est passé en paramètre. Les arguments qui suivent le nom du fichier sont passés au fichier.

ls [-l] [chemin_d_accès]

Affiche la liste des fichiers du répertoire donné, ou du répertoire racine, si le chemin d'accès n'est pas précisé. Si l'option `-l` est utilisée, les tailles des fichiers seront également listées.

lsdev [-v]

Liste tous les périphériques depuis lesquels il sera possible de charger des modules. Si l'option `-v` est utilisée, plus de détails seront donnés.

lsmod [-v]

Affiche la liste des modules chargés. Si l'option `-v` est utilisée, plus de détails seront donnés.

more *nom_du_fichier*

Affiche les fichiers indiqués, avec une pause toutes `LINES` lignes.

reboot

Redémarre immédiatement le système.

set *variable*

Positionne les variables d'environnement du chargeur.

unload

Retire de la mémoire tous les modules chargés.

13.3.3.3. Exemples d'utilisation du chargeur

Voici quelques exemples pratiques d'utilisation du chargeur:

- Pour simplement démarrer votre noyau habituel, mais en mode mono-utilisateur:

```
boot -s
```

- Pour décharger votre noyau et modules habituels, puis charger votre ancien (ou un autre) noyau:

```
unload
load kernel.old
```

Vous pouvez utiliser kernel.GENERIC pour faire référence au noyau générique du disque d'installation, ou kernel.old pour désigner votre noyau précédent (quand vous avez mis à jour ou configuré votre propre noyau, par exemple).

Utilisez ce qui suit pour charger vos modules habituels avec un autre noyau:

```
unload
set kernel="kernel.old"
boot-conf
```

- Pour charger une procédure de configuration du noyau (une procédure qui automatise ce que vous faites normalement avec l'outil de configuration du noyau au démarrage):

```
load -t userconfig_script /boot/kernel.conf
```

13.4. Interaction avec le noyau au démarrage

Une fois que le noyau est chargé, soit par le chargeur (habituellement) soit par boot2 (en court-circuitant le chargeur), il examine les options de démarrage s'il y en a, et adapte son comportement en conséquence.

13.4.1. Options de démarrage du noyau

Voici les options de démarrage les plus courantes:

`-a`
: A l'initialisation du noyau, demande quel est le périphérique où se trouve le système de fichiers racine.

`-C`
: Démarre depuis le CDROM.

`-c`
: Exécute UserConfig, l'outil de configuration du noyau au démarrage.

`-s`
: Démarre en mode mono-utilisateur.

`-v`
: Donne plus de détails lors du lancement du noyau.

Il existe d'autres options de démarrage, lisez la page de manuel boot(8) pour plus d'informations.

13.5. "Device Hints"-Paramétrage des périphériques

C'est une caractéristique de FreeBSD 5.0 et des versions suivantes qui n'existe pas dans les versions précédentes.

Lors du démarrage du système, le chargeur (loader(8)) lira le fichier device.hints(5). Ce fichier stocke les informations de démarrage du noyau connues sous le nom de variables, et parfois appelées "device hints". Ces "device hints" sont utilisés par les pilotes de périphérique pour la configuration des périphériques.

Les "device hints" peuvent être spécifiés à l'invite du chargeur. Des variables peuvent être ajoutées en utilisant la commande `set`, retirées avec la commande `unset`, et affichées avec la commande `show`.

Les variables positionnées dans le fichier /boot/device.hints peuvent être écrasées à cet endroit. Les "device hints" entrés au niveau du chargeur ne sont pas permanents et seront oubliés au prochain redémarrage.

Une fois le système démarré, la commande kenv(1) peut être utilisée pour afficher toutes les variables.

La syntaxe du fichier /boot/device.hints est d'une variable par ligne, en utilisant le caractère "#" comme signe de mise en commentaire. Les lignes sont présentées comme suit:

```
hint.pilote.unité.motclé="valeur"
```

La syntaxe à utiliser avec le chargeur est:

```
set hint.pilote.unité.motclé=valeur
```

où `pilote` est le pilote de périphérique, `unité` est le numéro de l'unité et `motclé` est le mot-clé correspondant à la variable. Le mot-clé pourra être une des options suivantes:

- `at`: spécifie le bus auquel le périphérique est attaché.
- `port`: spécifie l'adresse de départ de l'E/S à utiliser.
- `irq`: spécifie le numéro de la requête d'interruption à utiliser.
- `drq`: spécifie le numéro du canal DMA.
- `maddr`: spécifie l'adresse mémoire physique occupée par le périphérique.
- `flags`: fixe les bits des indicateurs pour le périphérique.
- `disabled`: si positionnée à `1` le périphérique est désactivé.

Les pilotes de périphérique pourront accepter (ou nécessiter) plus de variables non listées ici, il est recommandé de lire leur page de manuel. Pour plus d'information, consultez les pages de manuel device.hints(5), kenv(1), loader.conf(5), et loader(8).

13.6. Init: Initialisation de la gestion des processus

Une fois que le noyau a démarré, il passe le contrôle au processus utilisateur init(8), qui se trouve dans /sbin/init, ou au programme défini dans la variable d'environnement `init_path` du chargeur.

13.6.1. Séquence de redémarrage automatique

La séquence de redémarrage automatique vérifie que les systèmes de fichiers sont cohérents. S'ils ne le sont pas, et que fsck(8) ne peut pas corriger les incohérences, init(8) place le système dans le mode mono-utilisateur pour que l'administrateur système règle directement le problème.

13.6.2. Mode mono-utilisateur

Ce mode peut être atteint depuis la séquence de redémarrage automatique, ou quand l'utilisateur démarre avec l'option `-s` ou en positionnant la variable `boot_single` du chargeur.

On peut également y parvenir en appelant la commande shutdown(8) sans les options de redémarrage (`-r`) ou d'arrêt (`-h`), à partir du mode multi-utilisateur.

Si la `console` système est positionnée dans le mode `insecure` dans le fichier /etc/ttys, alors le système demande le mot de passe de `root` avant de passer en mode mono-utilisateur.

Exemple 18. Une console non sécurisée dans /etc/ttys

```
# name  getty                           type    status          comments
#
# If console is marked "insecure", then init will ask for the root password
# when going to single-user mode.
console none                            unknown off insecure
```

Une console `insecure` (non sécurisée) signifie que vous considérez que la console n'est pas sécurisée, et vous désirez que seul quelqu'un connaissant le mot passe de `root` puisse utiliser le mode mono-utilisateur, et cela ne signifie pas que vous utilisez une console sans sécurité. Donc, si vous voulez de la sécurité, choisissez `insecure`, et non `secure`.

13.6.3. Mode multi-utilisateur

Si init(8) trouve vos systèmes de fichiers en état de marche, ou dès que l'utilisateur quitte le mode mono-utilisateur, le système entre dans le mode multi-utilisateur, dans lequel il commence la configuration de ses ressources.

13.6.3.1. Configuration des ressources (rc)

Le système de configuration des ressources lit les valeurs par défaut dans /etc/defaults/rc.conf, et les valeurs propres à la machine dans /etc/rc.conf, puis ensuite monte les systèmes de fichiers mentionnés dans /etc/fstab, démarre les services réseau, divers autres "démons" système, et enfin exécute les procédures de démarrage des logiciels installés localement.

La page de manuel rc(8) est une bonne référence au sujet du système de configuration des ressources, de même que la lecture des procédures de démarrage elles-mêmes.

13.7. Séquence d'arrêt du système

Lors de l'arrêt manuel du système, via shutdown(8), init(8) tentera d'exécuter la procédure /etc/rc.shutdown, et ensuite enverra à tous les processus le signal `TERM`, suivi du signal `KILL` à tous ceux qui ne se terminent pas à temps.

Pour éteindre une machine FreeBSD et cela sur des architectures ou des systèmes supportant la gestion par logiciel de l'énergie, utilisez simplement la commande `shutdown -p now` pour arrêter et couper l'alimentation de la machine. Pour juste redémarrer un système FreeBSD, utilisez `shutdown -r now`. Vous devez être super-utilisateur (`root`) ou un membre du groupe `operator` pour pouvoir exécuter shutdown(8). Les commandes halt(8) et reboot(8) peuvent également être utilisées, veuillez consulter leur page de manuel ainsi que celle de shutdown(8) pour plus d'informations.

La gestion de l'énergie nécessite d'avoir le support acpi(4) dans son noyau ou chargé en tant que module.

Chapitre 14. Gestion des comptes et des utilisateurs

14.1. Synopsis

FreeBSD permet à de nombreux utilisateurs d'utiliser l'ordinateur en même temps. Evidemment, seul un de ces utilisateurs peut être assis devant l'écran et le clavier à un instant donné , mais n'importe quel nombre d'utilisateurs peut ouvrir une session par l'intermédiaire du réseau pour mener à bien son travail. Pour utiliser le système chaque utilisateur doit posséder un compte.

Après la lecture de ce chapitre, vous connaîtrez:

- Les différences entre les divers comptes utilisateur sur un système FreeBSD.
- Comment ajouter des comptes utilisateur.
- Comment supprimer des comptes utilisateur.
- Comment modifier les paramètres d'un compte, comme le nom complet de l'utilisateur, ou l'interpréteur de commandes préféré.
- Comment fixer des limites par compte, pour contrôler les ressources comme la mémoire et le temps CPU auxquels les comptes et les groupes de comptes sont autorisés à accéder.
- Comment utiliser les groupes pour rendre la gestion de comptes plus aisée.

Avant de lire ce chapitre, vous devrez:

- Comprendre les fondements d'UNIX® et de FreeBSD (Quelques bases d'UNIX).

14.2. Introduction

Tout accès au système est effectué par l'intermédiaire de comptes, et tous les processus sont exécutés par des utilisateurs, la gestion des comptes et des utilisateurs est capitale sur les systèmes FreeBSD.

Chaque compte sur un système FreeBSD est associé avec un certain nombre d'informations utilisé pour identifier le compte.

"User name" - nom d'utilisateur

Le nom d'utilisateur comme il sera tapé à l'invite `login:`. Les noms d'utilisateur doivent être uniques sur le système; vous ne pouvez pas avoir deux utilisateurs avec le même nom d'utilisateur. Il y a un certain nombre de règles pour la création de noms d'utilisateur valides, documentées dans passwd(5); vous utiliserez généralement des noms d'utilisateurs de huit lettres ou moins et en minuscules.

"Password" - mot de passe

Chaque compte est associé à un mot de passe. Le mot de passe peut être vide, dans ce cas aucun mot de passe ne sera requis pour accéder au système. Ceci est une très mauvaise idée; chaque compte devrait avoir un mot de passe.

"User ID (UID)" - identifiant utilisateur

L'UID est un nombre compris entre 0 et 65535, utilisé pour identifier de façon unique un utilisateur sur le système. Au niveau interne, FreeBSD utilise l'UID pour identifier les utilisateurs-toute commande qui vous permet de spécifier un utilisateur convertira le nom d'utilisateur en son UID avant de le traiter. Cela signifie que vous pouvez avoir plusieurs comptes avec des noms d'utilisateurs différents mais le même UID. En ce qui concerne FreeBSD ces comptes ne sont qu'un seul et unique utilisateur. Il est peu probable que vous ayez jamais à faire cela.

"Group ID (GID)" - identifiant de groupe

Le GID est un nombre compris entre 0 et 65535, utilisé pour identifier de façon unique le groupe principal auquel appartient l'utilisateur. Les groupes sont un mécanisme pour contrôler l'accès aux ressources qui est basé sur le GID de l'utilisateur plutôt que sur son UID. Un utilisateur peut également appartenir à plus d'un groupe.

"Login class" - classe de session

Les classes de session sont une extension du mécanisme de groupe qui apporte une flexibilité supplémentaire quand on adapte le système aux différents utilisateurs.

"Password change time" - durée de vie d'un mot de passe

Par défaut FreeBSD n'oblige pas les utilisateurs à changer leur mot de passe régulièrement. Vous pouvez forcer cela en fonction de l'utilisateur, en obligeant certains ou tous les utilisateurs à changer leur mot de passe après qu'une certaine période de temps se soit écoulée.

"Account expiry time" - date d'expiration d'un compte

Par défaut FreeBSD ne désactive pas de comptes après une certaine période. Si vous créez des comptes qui auront une durée de vie limitée, par exemple, dans une école où il existe des comptes pour les étudiants, alors vous pouvez spécifier la date d'expiration des comptes. Après la durée d'expiration écoulée le compte ne pourra plus être utilisé pour ouvrir de session sur le système, bien que les répertoires et les fichiers attachés au compte seront conservés.

"User's full name" - nom complet d'utilisateur

Le nom d'utilisateur identifie uniquement le compte sur FreeBSD, mais ne reflète pas nécessairement le nom réel de l'utilisateur. Cette information peut être associée avec le compte.

"Home directory" - répertoire utilisateur

Le répertoire utilisateur est le chemin complet vers un répertoire sur le système dans lequel se retrouve l'utilisateur quand il ouvre une session sur le système. Une convention commune est de mettre tous les répertoires d'utilisateurs sous /home/username ou /usr/home/username. L'utilisateur pourra stocker ses fichiers personnel dans son répertoire utilisateur et dans tout sous-répertoire qu'il pourra y créer.

"User shell" - interpréteur de commandes de l'utilisateur

L'interpréteur de commandes fournit aux utilisateurs l'environnement par défaut pour communiquer avec le système. Il existe plusieurs différents types d'interpréteurs de commandes, et les utilisateurs expérimentés auront leur préférence, qui peut se refléter dans le paramétrage de leur compte.

Il y a trois principales sortes de comptes: le super-utilisateur, les utilisateurs système, et les comptes utilisateur. Le compte super-utilisateur, normalement appelé `root`, est utilisé pour gérer le système sans aucune limitation de privilèges. Les utilisateurs système exécutent des services. Et enfin, les comptes utilisateur sont utilisés par de véritables utilisateurs, qui ouvrent des sessions, lisent leur courrier électronique, et ainsi de suite.

14.3. Le compte super-utilisateur

Le compte super-utilisateur, habituellement appelé `root`, est préconfiguré pour simplifier l'administration système, et ne devrait pas être utilisé pour des tâches quotidiennes comme l'envoi et la réception de courrier électronique, l'exploration du système, ou la programmation.

Cela parce que le super-utilisateur, à la différence des comptes utilisateurs ordinaires, peut agir sans aucune limite, et une mauvaise utilisation du compte super-utilisateur peut être à l'origine de résultats catastrophiques. On ne peut pas endommager par erreur le système avec un compte utilisateur, il est donc généralement préférable d'utiliser des comptes utilisateur ordinaires chaque fois que c'est possible, à moins d'avoir particulièrement besoin de droits supplémentaires.

Vous devriez toujours vérifier et revérifier les commandes que vous tapez en tant que super-utilisateur, parce qu'un espace en trop ou un caractère manquant peuvent signifier la perte définitive de données.

Donc, la première chose que vous devriez faire, après la lecture de ce chapitre, est de vous créer un compte utilisateur sans privilèges si vous n'en avez pas déjà. Cela s'applique aussi bien à une machine multi-utilisateurs qu'à une machine mono-utilisateur. Plus loin dans ce chapitre, nous expliquerons comment créer de nouveaux comptes, et comment passer d'un compte utilisateur ordinaire au compte du super-utilisateur.

14.4. Comptes système

Les utilisateurs système sont ceux utilisés pour exécuter des services comme le DNS, le courrier électronique, les serveurs web, et ainsi de suite. La raison de cela est la sécurité; si tous les services s'exécutaient avec les droits du super-utilisateur, ils pourraient agir sans aucune restriction.

Des exemples d'utilisateurs système sont `daemon`, `operator`, `bind` (pour le serveur de noms de domaine), `news`, et `www`.

`nobody` est l'utilisateur sans privilèges générique du système. Cependant, il est important de garder à l'esprit que plus grand est le nombre de services utilisant `nobody`, plus grand sera le nombre de fichiers et de processus associés à cet utilisateur, et par conséquent plus grand sera le nombre de privilèges de cet utilisateur.

14.5. Comptes utilisateur

Les comptes utilisateur sont le principal moyen pour les véritables utilisateurs d'accéder au système, ces comptes isolent l'utilisateur du reste de l'environnement, empêchant les utilisateurs d'endommager le système et ou les comptes d'autres utilisateurs, tout en leur permettant de personnaliser leur environnement sans incidence pour les autres utilisateurs.

Chaque personne accédant à votre système ne devrait posséder que son propre et unique compte. Cela vous permet de savoir qui fait quoi, empêche un utilisateur de désorganiser l'environnement d'un autre ou de lire du courrier électronique qui ne lui est pas destiné, et ainsi de suite.

Chaque utilisateur peut configurer son propre environnement en fonction de ses besoins, pour utiliser d'autres interpréteurs de commandes, éditeurs, raccourcis de clavier, et langues.

14.6. Modifier des comptes

Il existe une variété de différentes commandes disponibles dans l'environnement UNIX® pour manipuler les comptes utilisateur. Les commandes les plus communes sont récapitulées ci-dessous, suivis par des exemples détaillés de leur utilisation.

Commande	Résumé
adduser(8)	L'application en ligne de commande recommandée pour ajouter de nouveaux utilisateurs.
rmuser(8)	L'application en ligne de commande recommandée pour supprimer des utilisateurs.
chpass(1)	Un outil flexible pour modifier les informations de la base de données utilisateur.
passwd(1)	L'outil simple en ligne de commande pour changer les mots de passe utilisateur.
pw(8)	Un puissant et flexible outil pour modifier tous les aspects des comptes utilisateurs.

14.6.1. adduser

adduser(8) est un programme simple pour ajouter de nouveaux utilisateurs. Il crée les entrées dans les fichiers système passwd et group. Il crée également le répertoire utilisateur pour le nouvel utilisateur, y copie les fichiers de configuration par défaut ("dotfiles") à partir de /usr/shared/skel, et peut éventuellement envoyer à l'utilisateur un courrier électronique de bienvenue.

Exemple 19. Ajouter un utilisateur sous FreeBSD

```
# adduser
Username: jru
Full name: J. Random User
Uid (Leave empty for default):
Login group [jru]:
Login group is jru. Invite jru into other groups? []: wheel
Login class [default]:
Shell (sh csh tcsh zsh nologin) [sh]: zsh
Home directory [/home/jru]:
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]:
```

```
Use a random password? (yes/no) [no]:
Enter password:
Enter password again:
Lock out the account after creation? [no]:
Username   : jru
Password   : ****
Full Name  : J. Random User
Uid        : 1001
Class      :
Groups     : jru wheel
Home       : /home/jru
Shell      : /usr/local/bin/zsh
Locked     : no
OK? (yes/no): yes
adduser: INFO: Successfully added (jru) to the user database.
Add another user? (yes/no): no
Goodbye!
#
```

Le mot de passe que vous tapez n'apparaît pas à l'écran, et il n'y a pas non plus d'astérisques affichés. Assurez-vous de ne pas vous tromper dans le mot de passe.

14.6.2. `rmuser`

Vous pouvez utiliser rmuser(8) pour supprimer complètement un utilisateur du système. rmuser(8) effectue les opérations suivantes:

1. Supprime les entrées appartenant à l'utilisateur de la crontab(1) (s'il y en a).
2. Supprime les tâches at(1) appartenant à l'utilisateur.
3. Tue tous les processus appartenant à l'utilisateur.
4. Supprime l'utilisateur du fichier de mots de passe local.
5. Supprime le répertoire l'utilisateur (s'il lui appartient).
6. Supprime les courriers électroniques en attente pour l'utilisateur dans /var/mail.
7. Supprime tous les fichiers temporaires appartenant à l'utilisateur des zones de stockages temporaires comme /tmp.
8. Et enfin, supprime l'utilisateur de tous les groupes auxquels il appartient dans /etc/group.

Si un groupe est vide de ce fait et que le nom du groupe est le même que celui de l'utilisateur, le groupe est supprimé; c'est la réciproque de la création par adduser(8) d'un groupe propre pour chaque utilisateur.

rmuser(8) ne peut pas être employé pour supprimer des comptes super-utilisateur, car cela entraînerait presque toujours des destructions massives.

Par défaut, la commande travaille en mode interactif, pour garantir que vous soyez sûr de ce que vous faites.

Exemple 20. Suppression interactive de compte avec `rmuser`

```
# rmuser jru
Matching password entry:
jru:*:1001:1001::0:0:J. Random User:/home/jru:/usr/local/bin/zsh
Is this the entry you wish to remove? y
Remove user's home directory (/home/jru)? y
Updating password file, updating databases, done.
Updating group file: trusted (removing group jru -- personal group is empty) done.
Removing user's incoming mail file /var/mail/jru: done.
Removing files belonging to jru from /tmp: done.
Removing files belonging to jru from /var/tmp: done.
Removing files belonging to jru from /var/tmp/vi.recover: done.
#
```

14.6.3. chpass

chpass(1) modifie les informations de la base de données des utilisateurs comme les mots de passe, les interpréteurs de commandes, et les informations personnelles.

Seuls les administrateurs système, comme le super-utilisateur, peuvent modifier les informations concernant les autres utilisateurs et les mots de passe à l'aide de chpass(1).

Utilisé sans options, en dehors du nom facultatif de l'utilisateur, chpass(1) ouvre un éditeur affichant les informations de l'utilisateur. Quand l'utilisateur quitte l'éditeur, la base de données utilisateur est mise à jour avec les nouvelles informations.

On vous demandera votre mot de passe en quittant l'éditeur si vous n'êtes pas le super-utilisateur.

Exemple 21. `chpass` *interactif par le super-utilisateur*

```
#Changing user database information for jru.
Login: jru
Password: *
Uid [#]: 1001
Gid [# or name]: 1001
Change [month day year]:
Expire [month day year]:
Class:
Home directory: /home/jru
Shell: /usr/local/bin/zsh
Full Name: J. Random User
Office Location:
```

```
Office Phone:
Home Phone:
Other information:
```

Un utilisateur ordinaire ne peut modifier qu'une partie de ces informations, et seulement celles qui le concernent.

Exemple 22. chpass interactif par un utilisateur ordinaire

```
#Changing user database information for jru.
Shell: /usr/local/bin/zsh
Full Name: J. Random User
Office Location:
Office Phone:
Home Phone:
Other information:
```

chfn(1) et chsh(1) sont juste des liens vers chpass(1), comme le sont ypchpass(1), ypchfn(1), et ypchsh(1). NIS est supporté automatiquement, aussi spécifier yp avant la commande n'est pas nécessaire. Si cela vous semble confus, ne vous inquiétez pas, NIS sera abordé dans le chapitre Serveurs réseau.

14.6.4. passwd

passwd(1) est la méthode habituelle pour modifier son mot de passe, ou celui d'un autre utilisateur si vous êtes le super-utilisateur.

Pour prévenir des modifications accidentelles ou non autorisées, le mot de passe original doit être entré avant de pouvoir fixer un nouveau mot de passe.

Exemple 23. Modifier votre mot de passe

```
% passwd
Changing local password for jru.
Old password:
New password:
Retype new password:
passwd: updating the database...
passwd: done
```

Exemple 24. Modifier le mot de passe d'un autre utilisateur en tant que super-utilisateur

```
# passwd jru
```

```
Changing local password for jru.
New password:
Retype new password:
passwd: updating the database...
passwd: done
```

Comme pour chpass(1), yppasswd(1) est juste un lien vers passwd(1), donc NIS fonctionnera avec l'une des deux commandes.

14.6.5. pw

pw(8) est un utilitaire en ligne de commande pour créer, supprimer, modifier, et lister utilisateurs et groupes. Il fonctionne comme une interface aux fichiers d'utilisateurs et de groupe. pw(8) possède un ensemble puissant d'options qui le rende adapté à une utilisation dans des procédures, mais les nouveaux utilisateurs pourront le trouver plus compliqué que les autres commandes présentées ici.

14.7. Mettre en place des restrictions pour les utilisateurs

Si vous avez plusieurs utilisateurs sur votre système, la possibilité de limiter leur utilisation du système peut venir à l'esprit. FreeBSD fournit plusieurs méthodes à l'administrateur système pour limiter la quantité de ressources système qu'un utilisateur peut utiliser. Ces limites sont généralement divisées en deux parties: les quotas disque, et les autres limites de ressource.

Les quotas limitent l'utilisation des disques par les utilisateurs, et ils fournissent un moyen de vérifier rapidement cette utilisation sans avoir à faire des calculs à chaque fois. Les quotas sont abordés dans la Quotas d'utilisation des disques.

Les autres limites de ressource comprennent les moyens de limiter l'utilisation du CPU, de la mémoire, et les autres ressources qu'un utilisateur peut consommer. Elles sont définies en employant des classes de session et sont abordées ici.

Les classes de session sont définies dans /etc/login.conf. La sémantique précise sort du cadre de cette section, mais est décrite en détail dans la page de manuel login.conf(5). Il est suffisant de dire que chaque utilisateur est assigné à une classe (`default` par défaut), et que chaque classe dispose d'un ensemble de capacités associées. La forme utilisée pour ces capacités est une paire `nom=valeur` où *nom* est un identifiant connu et *valeur* est une chaîne arbitraire dépendante du nom. Paramétrer des classes et des capacités est plutôt direct et également décrit dans login.conf(5).

Le système ne lit normalement pas directement le fichier /etc/login.conf, mais plutôt la base de données /etc/login.conf.db qui fournit plus rapidement les réponses au système. Pour générer /etc/login.conf.db à partir du fichier /etc/login.conf, exécutez la commande suivante:

```
# cap_mkdb /etc/login.conf
```

Les limites de ressource sont différentes des capacités standards des classes en deux points. Premièrement, pour chaque limite, il existe une limite douce (actuelle) et limite dure. Une limite douce peut être ajustée par l'utilisateur ou une application, mais jamais dépasser la limite dure. Cette dernière peut être abaissée par l'utilisateur, mais jamais augmentée. Deuxièmement, la plupart des limites de ressource s'applique par processus à un utilisateur spécifique, et non pas à l'utilisateur dans sa totalité. Notez, cependant, que ces différences sont exigées par la manipulation spécifique des limites, et non pas par l'implémentation du système des capacités des classes de session utilisateur (i.e., elles ne sont *vraiment* pas un cas particulier des capacités des classes de session).

Sans plus attendre, ci-dessous sont présentées les limites de ressource les plus souvent utilisées (le reste, avec les autres capacités des classes de session, peut être trouvé dans login.conf(5)).

`coredumpsize`

La limite sur la taille du fichier core généré par un programme est, pour d'évidentes raisons, subordonnée aux autres limites sur l'utilisation du disque (e.g., `filesize`, ou les quotas de disque). Néanmoins, elle est souvent employée comme méthode moins sévère pour contrôler la consommation d'espace disque: puisque les utilisateurs ne génèrent pas de fichier core eux-mêmes, et souvent ne les suppriment pas, paramétrer cela peut leur éviter de manquer d'espace disque si un programme important (e.g., emacs) plante.

`cputime`

C'est la quantité maximale de temps CPU qu'un processus d'un utilisateur peut consommer. Les processus la dépassant seront tués par le noyau.

C'est une limite sur le *temps* CPU consommé, non sur le pourcentage comme affiché par certains champs de top(1) et ps(1). Une limite sur ce dernier est, au moment de l'écriture de ces lignes, impossible, et serait plutôt inutile: un compilateur-probablement une tâche légitime-peut aisément utiliser presque 100% du CPU pendant un certain temps.

`filesize`

C'est la taille maximale du plus gros fichier qu'un utilisateur peut posséder. Contrairement aux quotas, cette limite ne s'applique qu'aux fichiers individuellement, et non pas sur l'ensemble lui-même de tous les fichiers que possède un utilisateur.

`maxproc`

C'est le nombre maximal de processus que peut exécuter un utilisateur en même temps. Ceci inclut les processus de premier plan et de tâche de fond. Pour d'évidentes raisons, il ne doit pas être plus grand que les limites du système spécifiées par la variable sysctl(8) `kern.maxproc`. Notez en outre qu'une valeur trop basse peut gêner la productivité de l'utilisateur: il est souvent utile d'ouvrir plusieurs sessions à la fois ou d'exécuter des opérations sous forme de "pipeline". Certaines tâches, comme compiler un gros programme, engendrent également de multiples processus (e.g., make(1), cc(1), et autres préprocesseurs).

`memorylocked`

C'est la quantité maximale de mémoire qu'un processus peut avoir demandé de verrouiller en mémoire principale (e.g., voir mlock(2)). Certains programmes système critiques, comme amd(8), sont verrouillés en mémoire principale de sorte qu'en cas de dépassement de la mémoire de pagination, ils ne contribuent pas aux ennuis du système.

`memoryuse`

C'est la quantité maximale de mémoire qu'un processus peut consommer à un instant donné. Cela inclus la mémoire principale et celle de pagination. Ce n'est pas le remède miracle pour restreindre la consommation de mémoire, mais c'est un bon début.

`openfiles`

C'est le nombre maximal de fichiers qu'un processus peut avoir ouvert. Sous FreeBSD, des fichiers sont également employés pour représenter les sockets et les canaux IPC, par conséquent faites attention à ne fixer une valeur trop basse. La limite générale du système pour cela est définie par la variable sysctl(8) `kern.maxfiles`.

`sbsize`

C'est une limite sur la quantité de mémoire réseau, et donc de "mbufs", qu'un utilisateur peut consommer. Ceci est à l'origine une réponse à une vielle attaque par refus de service en créant de nombreuses sockets, mais peut être généralement employée pour limiter les communications réseau.

`stacksize`

C'est la taille maximale de la pile d'un processus. Seule, cela n'est pas suffisant pour limiter la quantité de mémoire que peut utiliser un programme, par conséquent, cette limite devra être utilisée en même temps que d'autres limitations.

Il y a quelques éléments à se rappeler quand on fixe des limites de ressource. Quelques astuces générales, suggestions, et commentaires divers:

- Les processus lancés au démarrage du système par /etc/rc sont assignés à la classe `daemon`.
- Bien que le fichier /etc/login.conf qui est fourni avec le système est une bonne source de valeurs raisonnables pour la plupart des limites, seul vous, l'administrateur, peut savoir ce qui est approprié à votre système. Fixer une limite trop haute peut laisser la porte ouverte aux abus, alors qu'une limite trop basse peut être un frein à la productivité.
- Les utilisateurs du système X Window (X11) devraient se voir allouer plus de ressources que les autres utilisateurs. X11 par lui-même utilise beaucoup de ressources, mais il encourage également les utilisateurs à exécuter plus de programmes simultanément.
- Souvenez-vous que de nombreuses limites ne s'appliquent qu'aux processus individuels, et non pas à l'utilisateur globalement. Par exemple, paramétrer `openfiles` à 50 signifie que chaque processus que l'utilisateur exécute pourra ouvrir jusqu'à 50 fichiers. Ainsi, la quantité totale de fichiers qu'un utilisateur peut ouvrir est la valeur `openfiles` multipliée par la valeur `maxproc`. Ceci s'applique également à la consommation de mémoire.

Pour de plus amples informations sur les limites et les classes de session et les capacités en général, veuillez consulter les pages de manuel appropriées: cap.mkdb(1), getrlimit(2), login.conf(5).

14.8. Groupes

Un groupe est simplement une liste d'utilisateurs. Les groupes sont identifiés par leur nom et leur GID (identificateur de groupe). Dans FreeBSD (et la plupart des systèmes UNIX®), les deux éléments que le noyau utilise pour décider si un processus est autorisé à faire quelque chose sont son ID utilisateur et la liste des groupes auxquels il appartient. Différent d'un identificateur utilisateur, un processus est associé à une liste de groupes. Vous pourrez entendre faire références au "group ID" d'un utilisateur ou d'un processus; la plupart du temps on veut parler du premier groupe dans la liste.

La table d'équivalence nom de groupe et identificateur de groupe se trouve dans /etc/group. C'est un fichier texte avec quatre champs délimités par deux points. Le premier champ est le nom du groupe, le second est le mot de passe crypté, le troisième est l'ID du groupe, et le quatrième est une liste de membres séparés par des virgules. Ce fichier peut sans risque être édité à la main (en supposant, bien sûr, que vous ne faites pas d'erreur de syntaxe!). Pour une description complète de le syntaxe, voir la page de manuel group(5).

Si vous ne voulez pas éditer /etc/group à la main, vous pouvez utiliser la commande pw(8) pour ajouter et éditer des groupes. Par exemple, pour ajouter un groupe appelé `teamtwo` et ensuite vérifier qu'il existe bien vous pouvez utiliser:

Exemple 25. Ajouter un groupe en utilisant pw(8)

```
# pw groupadd teamtwo
# pw groupshow teamtwo
teamtwo:*:1100:
```

Le nombre `1100` ci-dessus est l'identificateur de groupe pour le groupe `teamtwo`. A cet instant `teamtwo` n'a aucun membre, et est par conséquent plutôt inutile. Changeons cela en ajoutant `jru` au groupe `teamtwo`.

Exemple 26. Ajouter quelqu'un dans un groupe en utilisant pw(8)

```
# pw groupmod teamtwo -M jru
# pw groupshow teamtwo
teamtwo:*:1100:jru
```

Le paramètre ajouté à l'option `-M` est une liste, délimitée par des virgules, d'utilisateurs qui sont membres du groupe. Des sections précédentes nous savons que le fichier des mots de passe contient également un groupe pour chaque utilisateur. Le dernier (utilisateur) est automatiquement ajouté à la liste des groupes par le système; l'utilisateur n'apparaîtra pas comme étant membre quand on utilise l'option `groupshow` avec pw(8), mais apparaîtra quand l'information est demandée par l'intermédiaire de id(1) ou un outil similaire. En d'autres termes, pw(8) manipule uniquement le fichier /etc/group, il n'essaiera jamais de lire des données supplémentaires à partir du fichier /etc/passwd.

Exemple 27. Utilisation de id(1) pour déterminer l'appartenance à un groupe

```
% id jru
uid=1001(jru) gid=1001(jru) groups=1001(jru), 1100(teamtwo)
```

Comme vous pouvez le voir, `jru` est membre des groupes `jru` et `teamtwo`.

Pour plus d'information sur pw(8), voir sa page de manuel, et pour d'information sur le format de /etc/group, consultez la page de manuel group(5).

Chapitre 15. Sécurité

15.1. Synopsis

Ce chapitre sera une introduction aux concepts de base de la sécurité système, à certaines règles empiriques, et à des sujets avancés sous FreeBSD. De nombreux sujets abordés ici peuvent être appliqués à la sécurité système et à l'Internet en général. L'Internet n'est plus un endroit "amical" dans lequel chacun désire être votre gentil voisin. Sécuriser votre système est impératif pour protéger vos données, la propriété intellectuelle, votre temps, et bien plus des mains des "hackers" et équivalents.

FreeBSD fournit un ensemble d'utilitaires et de mécanismes pour assurer l'intégrité et la sécurité de votre système et votre réseau.

Après la lecture de ce chapitre, vous connaîtrez:

- Les concepts de base de la sécurité système en ce qui concerne FreeBSD.
- Les différents mécanismes de chiffrement disponibles sous FreeBSD, comme DES et MD5.
- Comment mettre en place une authentification par mot de passe non réutilisable.
- Comment configurer l'encapsuleur TCP pour une utilisation avec inetd.
- Comment configurer KerberosIV sous les versions de FreeBSD antérieures à la 5.0.
- Comment configurer Kerberos5 sous FreeBSD.
- Comment configurer IPsec et mettre en place un VPN entre machines FreeBSD et Windows®.
- Comment configurer et utiliser OpenSSH, la version de SSH implémentée sous FreeBSD.
- Ce que sont les ACLs et comment les utiliser.
- Comment employer l'utilitaire Portaudit pour l'audit des logiciels tierce-partie installés à partir du catalogue des logiciels portés.
- Comment utiliser les avis de sécurité de FreeBSD.
- Ce qu'est la comptabilité des processus et comment l'activer sous FreeBSD.

Avant de lire ce chapitre, vous devrez:

- Comprendre les concepts de base de FreeBSD et d'Internet.

D'autres sujets relatifs à la sécurité sont abordés par ailleurs dans ce Manuel. Par exemple, le contrôle d'accès obligatoire est présenté dans le Mandatory Access Control et les coupe-feux Internet sont développés dans le Firewalls.

15.2. Introduction

La sécurité est un domaine qui débute et se termine au niveau de l'administrateur système. Alors que tous les systèmes multi-utilisateurs UNIX® BSD ont des sécurités inhérentes, la mise en place et la maintenance des mécanismes supplémentaires de sécurité pour conserver des utilisateurs

"honnêtes" est probablement une des tâches les plus vastes de l'administrateur système. La sécurité des machines est celle que vous voulez bien mettre en oeuvre, de plus les préoccupations en matière de sécurité sont plus que jamais en concurrence avec les besoins de confort des utilisateurs. Les systèmes UNIX® sont, en général, capables d'exécuter un nombre important de processus simultanément et plusieurs de ces processus fonctionnent en tant que serveur - cela signifiant que des entités extérieures peuvent se connecter et échanger avec ces processus. Comme les mini-ordinateurs et les gros ordinateurs d'hier deviennent aujourd'hui nos ordinateurs de bureau, et comme les ordinateurs sont désormais en réseau et reliés à Internet, la sécurité devient d'autant plus un problème majeur.

La sécurité système concerne également la lutte contre les diverses formes d'attaque, y compris les attaques destinées à faire planter, ou à rendre inutilisable le système, mais qui ne cherchent pas à compromettre le compte `root`. Les problèmes de sécurité peuvent être divisés en plusieurs catégories:

1. Attaques par déni de service.
2. Compte utilisateur compromis.
3. Le compte `root` compromis par l'intermédiaire de serveurs accessibles.
4. Le compte `root` compromis par l'intermédiaire de comptes utilisateur.
5. Création d'une "Backdoor" (porte dérobée).

Une attaque par déni de service ("DoS") est une action qui prive la machine de ressources nécessaires à son bon fonctionnement. Généralement, les attaques par déni de service sont des mécanismes de force brute qui tentent de faire planter ou tout au moins de rendre inutilisable la machine en saturant ses serveurs ou sa pile réseau. Certaines attaques par déni de service peuvent se servir de bogues présents dans la pile réseau pour faire planter une machine avec un seul paquet. Ces problèmes ne peuvent être corrigés que par l'application d'un correctif sur le noyau. On peut souvent remédier aux attaques sur les serveurs en fixant correctement des options pour limiter la charge que provoquent ces serveurs sur le système lors de conditions critiques. Les attaques réseau par force brute sont plus difficiles à traiter. Une attaque par paquets usurpés ("spoofed-packet"), par exemple, est quasi-impossible à arrêter, à moins de déconnecter de l'Internet votre système. Elle peut ne pas être en mesure de stopper votre machine, mais elle peut saturer votre connexion Internet.

La compromission d'un compte utilisateur est bien plus fréquente qu'une attaque de type DoS. De nombreux administrateurs utilisent toujours sur leurs machines les versions standards des serveurs telnetd, rlogind, rshd, et ftpd. Par défaut, ces serveurs ne fonctionnent pas avec des connexions chiffrées. Cela aura pour résultat si vous disposez d'un nombre d'utilisateurs conséquent qu'un ou plusieurs de ces utilisateurs ayant l'habitude de se connecter à partir d'une machine distante (ce qui représente la manière la plus courante et la plus pratique pour ouvrir une session sur un système) auront leur mot de passe "sniffé". L'administrateur système méticuleux analysera ses journaux de connexions effectuées à partir de machines distantes à la recherche d'adresses sources suspectes même pour les ouvertures de sessions ayant réussies.

Il faut toujours supposer qu'une fois l'attaquant a l'accès à un compte utilisateur, il pourra s'attaquer et avoir accès au compte `root`. Cependant, la réalité est que dans un système bien sécurisé et surveillé, l'accès à un compte utilisateur ne donne pas nécessairement à l'attaquant

l'accès au compte `root`. Cette distinction est importante car sans accès aux droits de `root`, l'attaquant ne peut généralement pas dissimuler ses traces et peut, dans le meilleur des cas, ne rien faire d'autre que mettre la pagaille dans les fichiers de l'utilisateur ou faire planter la machine. La compromission de comptes utilisateur est très fréquente parce que les utilisateurs n'ont pas l'habitude de prendre les précautions que prennent les administrateurs système.

Les administrateurs doivent garder à l'esprit qu'il existe potentiellement de nombreuses manières d'avoir accès au compte `root` sur une machine. L'attaquant peut connaître le mot de passe `root`, l'attaquant peut trouver un bogue dans un serveur tournant avec les droits de `root` et être en mesure de devenir `root` par l'intermédiaire d'une connexion réseau à ce serveur, ou l'attaquant peut connaître un bogue dans un programme suid-root qui permet de devenir `root` une fois qu'il a accédé à un compte utilisateur. Si un attaquant a trouvé un moyen de devenir `root` sur une machine, il n'aura peut-être pas besoin d'installer une "backdoor" (porte dérobée). De nombreux trous de sécurité `root` trouvés et fermés à temps demandent un travail considérable à l'attaquant pour effacer ses traces, aussi la plupart des attaquants installe des portes dérobées. Une porte dérobée offre à l'attaquant un moyen aisé d'avoir à nouveau accès aux droits de `root` sur le système, mais cela donne également à l'administrateur système intelligent un bon moyen de détecter l'intrusion. Rendre impossible à un attaquant l'installation d'une porte dérobée peut en fait être préjudiciable à votre sécurité, parce que cela ne fermera pas le trou qu'a découvert en premier lieu l'attaquant pour pénétrer sur le système.

Les solutions aux problèmes de sécurité devraient toujours être mises en place suivant l'approche multi-couches de "la pelure d'oignon", elles peuvent être classées comme suit:

1. Sécuriser les comptes `root` et d'administration.
2. Sécuriser les serveurs exécutés avec les droits de `root` et les binaires suid/sgid.
3. Sécuriser les comptes utilisateurs.
4. Sécuriser le fichier des mots de passe.
5. Sécuriser le noyau, les périphériques et les systèmes de fichiers.
6. Installer un mécanisme de détection rapide des modifications inappropriées apportées au système.
7. La paranoïa.

La section suivante de ce chapitre abordera de manière plus approfondie les points énoncés ci-dessus.

15.3. Securing FreeBSD Traduction en Cours

15.4. DES, MD5, et chiffrement

Chaque utilisateur d'un système UNIX® possède un mot de passe associé à son compte. Il semble évident que ces mots de passe ne doivent être connus que de l'utilisateur et du système d'exploitation. Afin de conserver ces mots de passe secrets, ils sont chiffrés avec ce que l'on appelle un "hachage irréversible", ce qui signifie que le mot de passe peut être aisément chiffré mais pas déchiffré. En d'autres mots, ce que nous vous disions précédemment n'est même pas vrai: le

système d'exploitation lui-même ne connaît pas *vraiment* le mot de passe. Il ne connaît que la forme *chiffrée* du mot de passe. La seule manière d'obtenir le mot de passe en *clair* est d'effectuer une recherche par force brute de tous les mots de passe possibles.

Malheureusement, la seule méthode sécurisée pour chiffrer les mots de passe quand UNIX® a vu le jour était basée sur DES, le "Data Encryption Standard" (standard de chiffrement des données). C'était un problème mineur pour les utilisateurs résidants aux Etats-Unis, mais puisque le code source de DES ne pouvait être exporté en dehors des Etats-Unis, FreeBSD dû trouver un moyen de respecter la législation américaine et de rester compatible avec les autres systèmes UNIX® qui utilisaient encore DES.

La solution fut de séparer les bibliothèques de chiffrement de façon à ce que les utilisateurs américains puissent installer les bibliothèques DES et utiliser DES, mais que les utilisateurs internationaux disposent d'une méthode de chiffrement non restreinte à l'exportation. C'est comment FreeBSD est venu à utiliser MD5 comme méthode de chiffrement par défaut. MD5 est reconnu comme étant plus sure que DES, l'installation de DES est proposée principalement pour des raisons de compatibilité.

15.4.1. Identifier votre mécanisme de chiffrement

Avant FreeBSD 4.4 libcrypt.a était un lien symbolique pointant sur la bibliothèque utilisée pour le chiffrement. FreeBSD 4.4 modifia libcrypt.a pour fournir une bibliothèque de hachage pour l'authentification des mots de passe configurable. Actuellement la bibliothèque supporte les fonctions de hachage DES, MD5 et Blowfish. Par défaut FreeBSD utilise MD5 pour chiffrer les mots de passe.

Il est relativement facile d'identifier quelle méthode de chiffrement FreeBSD utilise. Examiner les mots de passe chiffrés dans le fichier /etc/master.passwd est une méthode. Les mots de passe MD5 sont plus longs que les mots de passe DES, et commencent par les caractères `$1$`. Les mots de passe débutant par `$2$` sont chiffrés suivant la méthode Blowfish. Les mots de passe DES n'ont pas de caractéristique particulière, mais sont plus courts que les mots de passe MD5 et utilisent un alphabet de 64 caractères qui ne contient pas le caractère `$`, aussi une chaîne relativement courte qui ne commence pas par un dollar a donc de très fortes chances d'être un mot de passe DES.

Le format utilisé par les nouveaux mots de passe est contrôlé par la capacité de classe de session `passwd_format` dans /etc/login.conf, qui prend comme valeur `des`, `md5` ou `blf`. Voir la page de manuel login.conf(5) pour plus d'information sur les capacités de classe de session.

15.5. Mots de passe non réutilisables

S/Key est un système de mots de passe non réutilisables basé sur une fonction de hachage irréversible. FreeBSD utilise le hachage MD4 pour des raisons de compatibilité mais d'autres système utilisent MD5 et DES-MAC. S/Key fait partie du système de base de FreeBSD depuis la version 1.1.5 et est aussi utilisé sur un nombre toujours plus important d'autres systèmes d'exploitation. S/Key est une marque déposée de Bell Communications Research, Inc.

Depuis la version 5.0 de FreeBSD, S/Key a été remplacé par la fonction équivalente OPIE ("One-time Passwords In Everything" - Mots de passe non réutilisables dans toutes les applications). OPIE utilise le hachage MD5 par défaut.

Il existe trois types de mots de passe dont nous parlerons dans ce qui suit. Le premier est votre mot de passe UNIX® habituel ou mot de passe Kerberos; nous appellerons "mot de passe UNIX®". Le deuxième type est le mot de passe généré par les programmes S/Key `key` ou OPIE opiekey(1) et reconnu par les programmes `keyinit` ou opiepasswd(1) et l'invite de session; nous appellerons ceci un "mot de passe non réutilisable". Le dernier type de mot de passe est le mot de passe secret que vous donnez aux programmes `key`/`opiekey` (et parfois aux programmes `keyinit`/`opiepasswd`) qui l'utilisent pour générer des mots de passe non réutilisable; nous l'appellerons "mot de passe secret" ou tout simplement "mot de passe".

Le mot de passe secret n'a rien à voir avec votre mot de passe UNIX®; ils peuvent être identique, mais c'est déconseillé. Les mots de passe secret S/Key et OPIE ne sont pas limités à 8 caractères comme les anciens mots de passe UNIX®, ils peuvent avoir la longueur que vous désirez. Des mots de passe de six ou sept mots de long sont relativement communs. La plupart du temps, le système S/Key ou OPIE fonctionne de façon complètement indépendante du système de mot de passe UNIX®.

En plus du mot de passe, deux autres types de données sont importantes pour S/Key et OPIE. L'une d'elles est connue sous le nom de "germe" ("seed") ou "clé", formé de deux lettres et cinq chiffres. L'autre est ce que l'on appelle le "compteur d'itérations", un nombre compris entre 1 et 100. S/Key génère un mot de passe non réutilisable en concaténant le germe et le mot de passe secret, puis en appliquant la fonction de hachage MD4/MD5 autant de fois qu'indiqué par le compteur d'itérations, et en convertissant le résultat en six courts mots anglais. Ces six mots anglais constituent votre mot de passe non réutilisable. Le système d'authentification (principalement PAM) conserve une trace du dernier mot de passe non réutilisable utilisé, et l'utilisateur est authentifié si la valeur de hachage du mot de passe fourni par l'utilisateur est la même que celle du mot de passe précédent. Comme le hachage utilisé est irréversible, il est impossible de générer de mot de passe non réutilisable si on a surpris un de ceux qui a été utilisé avec succès; le compteur d'itérations est décrémenté après chaque ouverture de session réussie, de sorte que l'utilisateur et le programme d'ouverture de session restent en phase. Quand le compteur d'itération passe à 1, S/Key et OPIE doivent être réinitialisés.

Il y a trois programmes impliqués dans chacun des systèmes que nous aborderons plus bas. Les programmes `key` et `opiekey` ont pour paramètres un compteur d'itérations, un germe, et un mot de passe secret, et génère un mot de passe non réutilisable ou une liste de mots de passe non réutilisable. Les programmes `keyinit` et `opiepasswd` sont utilisés pour initialiser respectivement S/Key et OPIE, et pour modifier les mots de passe, les compteurs d'itérations, ou les germes; ils prennent pour paramètres soit un mot de passe secret, soit un compteur d'itérations, soit un germe, et un mot de passe non réutilisable. Le programme `keyinfo` ou `opieinfo` consulte le fichier d'identification correspondant (/etc/skeykeys ou /etc/opiekeys) et imprime la valeur du compteur d'itérations et le germe de l'utilisateur qui l'a invoqué.

Nous décrirons quatre sortes d'opérations. La première est l'utilisation du programme `keyinit` ou `opiepasswd` sur une connexion sécurisée pour initialiser les mots de passe non réutilisables pour la première fois, ou pour modifier votre mot de passe ou votre germe. La seconde opération est l'emploi des programmes `keyinit` ou `opiepasswd` sur une connexion non sécurisée, en conjonction avec `key` ou `opiekey` sur une connexion sécurisée, pour faire la même chose. La troisième est l'utilisation de `key`/`opiekey` pour ouvrir une session sur une connexion non sécurisée. La quatrième est l'emploi de `key` ou `opiekey` pour générer un certain nombre de clés qui peuvent être notées ou imprimées et emportées avec vous quand vous allez quelque part ou il n'y a aucune connexion

sécurisée.

15.5.1. Initialisation depuis une connexion sécurisée

Pour initialiser S/Key pour la première fois, changer votre mot de passe, ou changer votre germe quand vous êtes attaché sous votre compte par l'intermédiaire d'une connexion sécurisée (e.g., sur la console d'une machine ou via ssh), utilisez la commande `keyinit` sans paramètres:

```
% keyinit
Adding unfurl:
Reminder - Only use this method if you are directly connected.
If you are using telnet or rlogin exit with no password and use keyinit -s.
Enter secret password:
Again secret password:

ID unfurl s/key is 99 to17757
DEFY CLUB PRO NASH LACE SOFT
```

Pour OPIE, `opiepasswd` est utilisé à la place:

```
% opiepasswd -c
[grimreaper] ~ $ opiepasswd -f -c
Adding unfurl:
Only use this method from the console; NEVER from remote. If you are using
telnet, xterm, or a dial-in, type ^C now or exit with no password.
Then run opiepasswd without the -c parameter.
Using MD5 to compute responses.
Enter new secret pass phrase:
Again new secret pass phrase:
ID unfurl OTP key is 499 to4268
MOS MALL GOAT ARM AVID COED
```

A l'invite `Enter new secret pass phrase:` ou `Enter secret password:`, vous devez entrer un mot de passe ou une phrase. Rappelez-vous que ce n'est pas le mot de passe que vous utiliserez pour ouvrir une session, mais celui utilisé pour générer vos clés non réutilisables. La ligne commençant par "ID" liste les paramètres de votre instance: votre nom d'utilisateur, la valeur de votre compteur d'itérations et votre germe. Quand vous ouvrirez une session, le système aura mémorisé ces paramètres et vous les redonnera, vous n'avez donc pas besoin de les retenir. La dernière ligne donne le mot de passe non réutilisable correspondant à ces paramètres et à votre mot de passe secret; si vous devez vous reconnectez immédiatement, c'est ce mot de passe que vous utiliseriez.

15.5.2. Initialisation depuis une connexion non sécurisée

Pour initialiser ou changer votre mot de passe secret par l'intermédiaire d'une connexion non sécurisée, il faudra avoir déjà une connexion sécurisée sur une machine où vous pouvez exécuter `key` ou `opiekey`; ce peut être depuis une icone sur le bureau d'un Macintosh ou depuis la ligne de commande d'une machine sûre. Il vous faudra également donner une valeur au compteur

d'itération (100 est probablement une bonne valeur), et indiquer un germe ou utiliser la valeur aléatoire générée par le programme. Sur la connexion non sécurisée (vers la machine que vous initialisez), employez la commande `keyinit -s`:

```
% keyinit -s
Updating unfurl:
Old key: to17758
Reminder you need the 6 English words from the key command.
Enter sequence count from 1 to 9999: 100
Enter new key [default to17759]:
s/key 100 to 17759
s/key access password:
s/key access password:CURE MIKE BANE HIM RACY GORE
```

Pour OPIE, vous devez utiliser `opiepasswd`:

```
% opiepasswd

Updating unfurl:
You need the response from an OTP generator.
Old secret pass phrase:
        otp-md5 498 to4268 ext
        Response: GAME GAG WELT OUT DOWN CHAT
New secret pass phrase:
        otp-md5 499 to4269
        Response: LINE PAP MILK NELL BUOY TROY

ID mark OTP key is 499 gr4269
LINE PAP MILK NELL BUOY TROY
```

Pour accepter le germe par défaut (que le programme `keyinit` appelle `key`, ce qui prête à confusion), appuyez sur `Entrée`. Ensuite avant d'entrer un mot de passe d'accès, passez sur votre connexion sécurisée et donnez lui les mêmes paramètres:

```
% key 100 to17759
Reminder - Do not use this program while logged in via telnet or rlogin.
Enter secret password: <secret password>
CURE MIKE BANE HIM RACY GORE
```

Ou pour OPIE:

```
% opiekey 498 to4268
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase:
GAME GAG WELT OUT DOWN CHAT
```

Retournez maintenant sur votre connexion non sécurisée, et copiez le mot de passe non réutilisable généré par le programme adapté.

15.5.3. Générer un unique mot de passe non réutilisable

Une fois que vous avez initialisé S/Key ou OPIE, lorsque que vous ouvrez une session, une invite de ce type apparaîtra:

```
% telnet example.com
Trying 10.0.0.1...
Connected to example.com
Escape character is '^]'.

FreeBSD/i386 (example.com) (ttypa)

login: <username>
s/key 97 fw13894
Password:
```

Ou pour OPIE:

```
% telnet example.com
Trying 10.0.0.1...
Connected to example.com
Escape character is '^]'.

FreeBSD/i386 (example.com) (ttypa)

login: <username>
otp-md5 498 gr4269 ext
Password:
```

Les invites S/Key et OPIE disposent d'une fonction utile (qui n'est pas illustrée ici): si vous appuyez sur la touche `Entrée` lorsque l'on vous demande votre mot de passe, le programme active l'écho au terminal, de sorte que vous voyez ce que vous êtes en train de taper. Ceci est très utile si vous essayez de taper un mot de passe à la main, à partir d'un résultat imprimé par exemple.

A ce moment vous devez générer votre mot de passe non réutilisable pour répondre à cette invite de session. Cela doit être effectué sur une machine de confiance sur laquelle vous pouvez exécuter `key` ou `opiekey` (il y a des versions de ces programmes pour DOS, Windows et MacOS). Ces programmes ont besoin du compteur d'itérations et du germe comme paramètres. Vous pouvez les copier-coller de l'invite de session de la machine sur laquelle vous voulez ouvrir une session.

Sur le système sûr:

```
% key 97 fw13894
Reminder - Do not use this program while logged in via telnet or rlogin.
```

```
Enter secret password:
WELD LIP ACTS ENDS ME HAAG
```

Pour OPIE:

```
% opiekey 498 to4268
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase:
GAME GAG WELT OUT DOWN CHAT
```

Maintenant que vous disposez de votre mot de passe non réutilisable vous pouvez continuer et vous connecter:

```
login: <username>
s/key 97 fw13894
Password: <return to enable echo>
s/key 97 fw13894
Password [echo on]: WELD LIP ACTS ENDS ME HAAG
Last login: Tue Mar 21 11:56:41 from 10.0.0.2 ...
```

15.5.4. Générer de multiples mots de passe non réutilisables

Il faut parfois se rendre en des endroits où vous n'avez pas accès à une machine de confiance ou à une connexion sécurisée. Dans ce cas, vous pouvez utiliser la commande `key` ou `opiekey` pour générer plusieurs mots de passe non réutilisables que vous pouvez imprimer et transporter avec vous. Par exemple:

```
% key -n 5 30 zz99999
Reminder - Do not use this program while logged in via telnet or rlogin.
Enter secret password: <secret password>
26: SODA RUDE LEA LIND BUDD SILT
27: JILT SPY DUTY GLOW COWL ROT
28: THEM OW COLA RUNT BONG SCOT
29: COT MASH BARR BRIM NAN FLAG
30: CAN KNEE CAST NAME FOLK BILK
```

Ou pour OPIE:

```
% opiekey -n 5 30 zz99999
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase: <secret password>
26: JOAN BORE FOSS DES NAY QUIT
27: LATE BIAS SLAY FOLK MUCH TRIG
28: SALT TIN ANTI LOON NEAL USE
```

```
29: RIO ODIN GO BYE FURY TIC
30: GREW JIVE SAN GIRD BOIL PHI
```

L'option `-n 5` demande cinq clés en séquence, l'option `30` indique quel doit être le rang de la dernière itération. Notez que les clés sont imprimées dans l'ordre *inverse* de celui où elles seront éventuellement utilisées. Si vous êtes vraiment paranoïaque, vous pouvez les recopier à la main, sinon vous pouvez les copier-coller vers la commande `lpr`. Remarquez que chaque ligne liste le compteur d'itération et le mot de passe non réutilisable; vous trouverez peut-être utile de rayer les mots de passe au fur et à mesure de leur utilisation.

15.5.5. Restreindre l'utilisation des mots de passe UNIX®

S/Key peut placer des restrictions sur l'utilisation des mots de passe UNIX® en fonction des noms de machine, d'utilisateur, de la ligne utilisée par le terminal ou de l'adresse IP de la machine connectée à distance. Ces restrictions peuvent être trouvées dans le fichier de configuration /etc/skey.access. La page de manuel skey.access(5) donne de plus amples informations sur le format de ce fichier et elle détaille également certains avertissements relatifs à la sécurité qu'il faut lire avant de se fier à ce fichier pour sa sécurité.

S'il n'y a pas de fichier /etc/skey.access (ce qui est le cas par défaut sur les systèmes FreeBSD 4.X), tous les utilisateurs pourront se servir de mots de passe UNIX®. Si le fichier existe, alors tous les utilisateurs devront passer par S/Key, à moins qu'ils ne soient explicitement autorisés à ne pas le faire par des instructions du fichier /etc/skey.access. Dans tous les cas l'usage des mots de passe UNIX® est autorisé sur la console.

Voici un exemple de configuration du fichier skey.access qui illustre les trois types d'instructions les plus courantes:

```
permit internet 192.168.0.0 255.255.0.0
permit user fnord
permit port ttyd0
```

La première ligne (`permit internet`) autorise les utilisateurs dont l'adresse IP (ce qui rend vulnérable en cas d'usurpation) appartient au sous-réseau spécifié à employer les mots de passe UNIX®. Cela ne doit pas être considéré comme une mesure de sécurité, mais plutôt comme un moyen de rappeler aux utilisateurs autorisés qu'ils sont sur un réseau non sécurisé et doivent utiliser S/Key pour s'authentifier.

La seconde ligne (`permit user`) autorise l'utilisateur désigné, dans notre cas `fnord`, à employer n'importe quand les mots de passe UNIX®. En général, il faut se servir de cette possibilité si les personnes soit n'ont pas moyen d'utiliser le programme `key`, s'ils ont par exemple des terminaux passifs, soit s'ils sont définitivement réfractaires au système.

La troisième ligne (`permit port`) autorise tous les utilisateurs d'un terminal sur une liaison particulière à utiliser les mots de passe UNIX®; cela devrait être employé pour les connexions téléphoniques.

OPIE peut restreindre l'usage des mots de passe UNIX® sur la base de l'adresse IP lors de

l'ouverture d'une session comme peut le faire S/Key. Le fichier impliqué est /etc/opieaccess, qui est présent par défaut sous FreeBSD 5.0 et versions suivantes. Veuillez consulter la page de manuel opieaccess(5) pour plus d'information sur ce fichier et certaines considérations sur la sécurité dont vous devez être au courant en l'utilisant.

Voici un exemple de fichier opieaccess:

```
permit 192.168.0.0 255.255.0.0
```

Cette ligne autorise les utilisateurs dont l'adresse IP (ce qui rend vulnérable en cas d'usurpation) appartient au sous-réseau spécifié à employer les mots de passe UNIX® à tout moment.

Si aucune règle du fichier opieaccess ne correspond, le comportement par défaut est de refuser toute ouverture de session non-OPIE.

15.6. L'encapsuleur TCP ("TCP Wrappers")

Toute personne familière avec inetd(8) a probablement entendu parlé à un moment ou à un autre de l'encapsuleur TCP ("TCP Wrappers"). Mais peu sont ceux qui semblent saisir complètement son intérêt dans un réseau. Il semble que tout le monde désire installer un coupe-feu pour contrôler les connexions réseaux. Alors qu'un coupe-feu peut avoir de nombreuses utilisations, il existe des choses qu'un coupe-feu ne peut gérer comme renvoyer un message à l'initiateur d'une connexion. L'encapsuleur TCP en est capable ainsi que bien d'autres choses. Dans les sections suivantes plusieurs fonctionnalités de l'encapsuleur TCP seront abordées, et, dès que ce sera possible, un exemple de configuration sera proposé.

L'encapsuleur TCP étend les capacités d'inetd au niveau du support pour chaque serveur sous son contrôle. En utilisant cette méthode il est possible d'offrir le support des ouvertures de session, de retourner des messages lors des connexions, de permettre à un "daemon" de n'accepter que les connexions internes, etc. Bien que certaines de ces fonctionnalités peuvent être obtenues par l'implémentation d'un coupe-feu, ce système ajoutera non seulement une couche supplémentaire de protection mais ira plus loin dans le contrôle que ce que peut fournir un coupe-feu.

Les fonctionnalités apportées par l'encapsuleur TCP ne peuvent se substituer à l'utilisation d'un bon coupe-feu. L'encapsuleur TCP peut être utilisé de paire avec un coupe-feu ou tout autre système de sécurité et il pourra alors servir comme une couche supplémentaire de protection pour le système.

Etant donné que ce programme est une extension à la configuration du programme inetd, le lecteur est supposé avoir pris connaissance de la section de configuration d'inetd.

Bien que les programmes lancés par inetd(8) ne soient pas tout à fait des "daemons", ils sont traditionnellement appelés "daemons". C'est le terme que nous utiliserons également dans le reste de cette section.

15.6.1. Configuration initiale

Le seul pré-requis à l'utilisation de l'encapsuleur TCP sous FreeBSD est de s'assurer que le serveur inetd est lancé à partir de rc.conf avec l'option `-Ww`; c'est la configuration par défaut. Bien évidemment une configuration correcte du fichier /etc/hosts.allow est également sous-entendue, mais dans le cas contraire syslogd(8) émettra des messages d'avertissement dans les journaux du système.

Contrairement à d'autres implémentations de l'encapsuleur TCP, l'emploi du fichier hosts.deny est obsolète. Toutes les options de configuration doivent être placées dans le fichier /etc/hosts.allow.

Dans la configuration la plus simple, la politique de connexion aux "daemons" est soit de tout autoriser ou soit de tout bloquer en fonctions des options choisies dans /etc/hosts.allow. La configuration par défaut sous FreeBSD est d'autoriser les connexions à chaque "daemon" lancé à l'aide d'inetd. La modification de ce réglage par défaut sera discutée une fois que la configuration de base aura été vue.

Une configuration de base prend en général la forme `daemon : adresse : action`. Où `daemon` est le nom du "daemon" lancé par inetd. L'`adresse` peut être un nom de machine valide, une adresse IP ou une adresse IPv6 entre crochets ([ ]). Le champ `action` pourra avoir comme valeur `allow` ou `deny` pour autoriser ou interdire l'accès. Gardez à l'esprit que ce type de configuration fonctionne de manière à honorer la première règle sémantique correspondante, cela signifie que le fichier de configuration est parcouru à la recherche d'une règle correspondant à la requête. Quand une correspondance est trouvée, la règle est appliquée et la recherche s'arrête.

Plusieurs autres options existent mais elles seront exposées dans une section ultérieure. Une simple ligne de configuration peut être construite avec peu d'information. Par exemple, pour autoriser les connexions POP3 via le "daemon"mail/qpopper, les lignes suivantes doivent être ajoutées au fichier hosts.allow:

```
# This line is required for POP3 connections:
qpopper : ALL : allow
```

Après l'ajout de cette ligne, inetd devra être redémarré. Cela sera fait en utilisant la commande kill(1), ou avec le passage du paramètre restart à la commande /etc/rc.d/inetd.

15.6.2. Configuration avancée

L'encapsuleur TCP dispose également d'options avancées; elles permettrons plus de contrôle sur la manière dont sont gérées les connexions. Dans certains cas cela peut être une bonne idée de renvoyer un commentaire à certaines machines ou lors de connexions à certains "daemon"s. Dans d'autres cas, peut-être qu'un fichier journal pourrait être enregistré ou un courrier électronique pourrait être envoyé à l'administrateur. D'autres situations peuvent nécessiter l'utilisation d'un service uniquement pour les connexions locales. Tout cela est possible à l'aide des options de configuration connues sous le nom de `jokers`, caractères d'expansion et d'exécution de commandes externes. Les deux sections suivantes abordent ces situations.

15.6.2.1. Commandes externes

Imaginez une situation dans laquelle une connexion doit être refusée et que la raison de ce refus doit être envoyée à la personne qui a tenté d'établir cette connexion. Comment cela peut-il être mis en place? Ce type d'action est rendu possible par l'emploi de l'option `twist`. Quand une tentative de connexion est faite, `twist` sera appelée pour exécuter une commande ou une procédure d'interpréteur de commande. Un exemple est déjà présent dans le fichier hosts.allow:

```
# The rest of the daemons are protected.
ALL : ALL \
        : severity auth.info \
        : twist /bin/echo "You are not welcome to use %d from %h."
```

Cet exemple montre que le message "You are not allowed to use `daemon` from `hostname`." sera retourné pour tout "daemon" qui n'a pas été précédemment configuré dans le fichier d'accès. Cette fonction est très utile pour envoyer une réponse à l'initiateur de la connexion juste après le refus de la connexion. Notez que tout message à retourner *doit* être placé entre des guillemets "; il n'y a pas d'exception possible à cette règle.

Il est possible de lancer une attaque par déni de service sur le serveur si un agresseur, ou un groupe d'agresseurs sont en mesure de submerger ces "daemon"s avec des demandes de connexion.

Une autre possibilité dans ce cas est d'employer l'option `spawn`. Tout comme l'option `twist`, `spawn` interdit implicitement les connexions et peut être utilisée pour lancer une commande ou une procédure externe. Contrairement à `twist`, `spawn` n'enverra pas de réponse à la personne qui a établi la connexion. Examinons par exemple la ligne de configuration suivante:

```
# We do not allow connections from example.com:
ALL : .example.com \
    : spawn (/bin/echo %a from %h attempted to access %d  \
      /var/log/connections.log) \
    : deny
```

Cela interdira toute tentative de connexion à partir du domaine `*.example.com`, enregistrant simultanément dans le fichier /var/log/connections.log le nom de machine, l'adresse IP et le "daemon" auquel on tente d'accéder.

Il existe d'autres caractères de substitution en dehors de ceux déjà présentés, par exemple `%a`. Consultez la page de manuel hosts_access(5) pour une liste complète.

15.6.2.2. Les options jokers

Jusqu'ici l'option `ALL` a été utilisée dans tous les exemples. Il existe d'autres options pour étendre un peu plus les fonctionnalités. Par exemple, l'option `ALL` peut être utilisée pour prendre en compte chaque instance d'un "daemon", d'un domaine ou d'une adresse IP. Un autre joker disponible est l'option `PARANOID` qui peut être employée pour prendre en compte toute machine qui fournirait une

adresse IP susceptible d'être falsifiée. En d'autres termes, l'option `PARANOID` peut être utilisée pour définir l'action a effectuer dès qu'une connexion se fait à partir d'une adresse IP qui diffère de celle attachée à une machine. L'exemple suivant apporte un éclairage sur cette option:

```
# Block possibly spoofed requests to sendmail:
sendmail : PARANOID : deny
```

Dans cet exemple, toutes les requêtes de connexion à sendmail à partir d'adresses IP différentes de celle correspondant au nom de la machine seront refusées.

Utiliser l'option `PARANOID` peut gravement paralyser les serveurs si le client ou le serveur a une configuration de DNS défectueuse. Les administrateurs sont maintenant prévenus.

Pour en apprendre plus sur les jokers et leurs fonctionnalités associées, consultez la page de manuel hosts_access(5).

Avant que n'importe quelle des lignes de configuration données ci-dessus ne fonctionne, la première ligne de configuration du fichier hosts.allow devra être dé-commentée. Cela a été noté en début de section.

15.7. Kerberos

Kerberos est un protocole réseau supplémentaire qui permet aux utilisateurs de s'authentifier par l'intermédiaire d'un serveur sécurisé. Des services comme l'ouverture de session et la copie à distance, la copie sécurisée de fichiers entre systèmes et autres fonctionnalités à haut risque deviennent ainsi considérablement plus sûrs et contrôlables.

Les instructions qui suivent peuvent être utilisées comme guide d'installation de Kerberos dans la version distribuée pour FreeBSD. Vous devriez cependant vous référer aux pages de manuel correspondantes pour avoir une description complète.

15.7.1. Installation de Kerberos

Kerberos est un composant optionnel de FreeBSD. La manière la plus simple d'installer ce logiciel est de sélectionner la distribution `krb4` ou `krb5` dans sysinstall lors de l'installation de FreeBSD. Cela installera les implémentations "eBones" (KerberosIV) ou "Heimdal" (Kerberos5) de Kerberos. Ces implémentations sont distribuées car elles sont développées en dehors des USA ou du Canada et étaient par conséquent disponibles aux utilisateurs hors de ces pays durant l'ère restrictive du contrôle des exportations de code de chiffrement à partir des USA.

Alternativement, l'implémentation du MIT de Kerberos est disponible dans le catalogue des logiciels portés sous security/krb5.

15.7.2. Créer la base de données initiale

Cela se fait uniquement sur le serveur Kerberos. Vérifiez tout d'abord qu'il ne traîne pas

d'anciennes bases Kerberos. Allez dans le répertoire /etc/kerberosIV et assurez-vous qu'il ne contient que les fichiers suivants:

```
# cd /etc/kerberosIV
# ls
README      krb.conf        krb.realms
```

S'il y a d'autres fichiers (comme principal.* ou master_key), utilisez alors la commande `kdb_destroy` pour supprimer l'ancienne base de données Kerberos, ou si Kerberos ne tourne pas, effacez simplement les fichiers supplémentaires.

Vous devez maintenant éditer les fichiers krb.conf et krb.realms pour définir votre domaine Kerberos. Dans notre cas, le domaine sera `EXAMPLE.COM` et le serveur `grunt.example.com`. Nous éditons ou créons le fichier krb.conf:

```
# cat krb.conf
EXAMPLE.COM
EXAMPLE.COM grunt.example.com admin server
CS.BERKELEY.EDU okeeffe.berkeley.edu
ATHENA.MIT.EDU kerberos.mit.edu
ATHENA.MIT.EDU kerberos-1.mit.edu
ATHENA.MIT.EDU kerberos-2.mit.edu
ATHENA.MIT.EDU kerberos-3.mit.edu
LCS.MIT.EDU kerberos.lcs.mit.edu
TELECOM.MIT.EDU bitsy.mit.edu
ARC.NASA.GOV trident.arc.nasa.gov
```

Dans notre cas les autres domaines n'ont pas besoin d'être mentionnés. Ils ne sont là que pour montrer comment une machine peut avoir connaissance de plusieurs domaines. Pour plus de simplicité, vous pouvez ne pas les inclure.

La première ligne indique pour quel domaine cette machine agit. Les autre lignes définissent les autres domaines/machines. Le premier élément sur une ligne est le domaine, le second le nom de la machine qui est le "centre de distribution de clés" de ce domaine. Les mots `admin server` qui suivent un nom de machine signifient que la machine est aussi serveur d'administration de la base de données. Pour plus d'explication sur cette terminologie, consultez les pages de manuel de Kerberos.

Nous devons maintenant ajouter `grunt.example.com` au domaine `EXAMPLE.COM` et ajouter une entrée pour mettre toutes les machines du domaine DNS `.example.com` dans le domaine Kerberos `EXAMPLE.COM`. Le fichier krb.realms aura alors l'allure suivante:

```
# cat krb.realms
grunt.example.com EXAMPLE.COM
.example.com EXAMPLE.COM
.berkeley.edu CS.BERKELEY.EDU
.MIT.EDU ATHENA.MIT.EDU
.mit.edu ATHENA.MIT.EDU
```

Encore une fois, les autres domaines n'ont pas besoin d'être mentionnés. Ils ne sont là que pour montrer comment une machine peut avoir connaissance de plusieurs domaines. Pour plus de simplicité, vous pouvez ne pas les inclure.

La première ligne assigne un système *particulier* au domaine désigné. Les lignes restantes montrent comment affecter par défaut les systèmes d'un sous-domaine DNS particulier à un domaine Kerberos donné.

Nous sommes maintenant prêt pour la création de la base de données. Il n'y a à le faire que sur le serveur Kerberos (ou Centre de Distribution de Clés). Cela se fait avec la commande `kdb_init`:

```
# kdb_init
Realm name [default  ATHENA.MIT.EDU ]: EXAMPLE.COM
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.

Enter Kerberos master key:
```

Nous devons maintenant sauvegarder la clé pour que les serveurs sur la machine locale puissent la lire. Utilisons la commande `kstash` pour faire cela:

```
# kstash

Enter Kerberos master key:

Current Kerberos master key version is 1.

Master key entered. BEWARE!
```

Le mot de passe maître chiffré est sauvegardé dans /etc/kerberosIV/master_key.

15.7.3. Installer les services

Il faut ajouter deux entrées ("principals") à la base de données pour *chaque* système qui sera sécurisé par Kerberos. Ce sont `kpasswd` et `rcmd`. Ces deux entrées sont définies pour chaque système, chacune de leurs instances se voyant attribuer le nom du système.

Ces "daemons", kpasswd et rcmd permettent aux autres systèmes de changer les mots de passe Kerberos et d'exécuter des commandes comme rcp(1), rlogin(1), et rsh(1).

Ajoutons donc maintenant ces entrées:

```
# kdb_edit
Opening database...

Enter Kerberos master key:

Current Kerberos master key version is 1.
```

```
Master key entered.  BEWARE!
Previous or default values are in [brackets] ,
enter return to leave the same, or new value.

Principal name: passwd
Instance: grunt

<Not found>, Create [y] ? y

Principal: passwd, Instance: grunt, kdc_key_ver: 1
New Password:                    <---- entrez RANDOM ici
Verifying password

New Password: <---- enter RANDOM here

Random password [y] ? y

Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 2000-01-01 ] ?
Max ticket lifetime (*5 minutes) [ 255 ] ?
Attributes [ 0 ] ?
Edit O.K.
Principal name: rcmd
Instance: grunt

<Not found>, Create [y] ?

Principal: rcmd, Instance: grunt, kdc_key_ver: 1
New Password:       <---- entrez RANDOM ici
Verifying password

New Password:           <---- entrez RANDOM ici

Random password [y] ?

Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 2000-01-01 ] ?
Max ticket lifetime (*5 minutes) [ 255 ] ?
Attributes [ 0 ] ?
Edit O.K.
Principal name:         <---- ne rien entrer ici permet de quitter le programme
```

15.7.4. Créer le fichier des services

Il faut maintenant extraire les instances qui définissent les services sur chaque machine. Pour cela on utilise la commande `ext_srvtab`. Cela créera un fichier qui doit être copié ou déplacé *par un moyen sûr* dans le répertoire /etc/kerberosIV de chaque client Kerberos. Ce fichier doit être présent sur chaque serveur et client, et est crucial au bon fonctionnement de Kerberos.

```
# ext_srvtab grunt
Enter Kerberos master key:

Current Kerberos master key version is 1.

Master key entered. BEWARE!
Generating 'grunt-new-srvtab'....
```

Cette commande ne génère qu'un fichier temporaire qui doit être renommé en srvtab pour que tous les serveurs puissent y accéder. Utilisez la commande mv(1) pour l'installer sur le système d'origine:

```
# mv grunt-new-srvtab srvtab
```

Si le fichier est destiné à un client, et que le réseau n'est pas considéré comme sûr, alors copiez le fichier client-new-srvtab sur un support amovible et transportez-le par un moyen physiquement sûr. Assurez-vous de le renommer en srvtab dans le répertoire /etc/kerberosIV du client, et mettez-le bien en mode 600:

```
# mv grumble-new-srvtab srvtab
# chmod 600 srvtab
```

15.7.5. Renseigner la base de données

Nous devons maintenant créer des entrées utilisateurs dans la base de données. Tout d'abord créons une entrée pour l'utilisateur `jane`. Utilisez la commande `kdb_edit` pour cela:

```
# kdb_edit
Opening database...

Enter Kerberos master key:

Current Kerberos master key version is 1.

Master key entered.  BEWARE!
Previous or default values are in [brackets] ,
enter return to leave the same, or new value.

Principal name: jane
Instance:

<Not found>, Create [y] ? y

Principal: jane, Instance: , kdc_key_ver: 1
New Password:                <---- entrez un mot de passe sûr ici
Verifying password
```

```
New Password:                <---- réentrez le mot de passe sûr là
Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 2000-01-01 ] ?
Max ticket lifetime (*5 minutes) [ 255 ] ?
Attributes [ 0 ] ?
Edit O.K.
Principal name:        <---- ne rien entrer ici permet de quitter le programme
```

15.7.6. Tester l'ensemble

Il faut tout d'abord démarrer les "daemons" Kerberos. Notez que si vous avez correctement modifié votre fichier /etc/rc.conf, cela se fera automatiquement au redémarrage du système. Ceci n'est nécessaire que sur le serveur Kerberos. Les clients Kerberos récupéreront automatiquement les informations dont ils ont besoin via leur répertoire /etc/kerberosIV.

```
# kerberos &
Kerberos server starting
Sleep forever on error
Log file is /var/log/kerberos.log
Current Kerberos master key version is 1.

Master key entered. BEWARE!

Current Kerberos master key version is 1
Local realm: EXAMPLE.COM
# kadmind -n &
KADM Server KADM0.0A initializing
Please do not use 'kill -9' to kill this job, use a
regular kill instead

Current Kerberos master key version is 1.

Master key entered.  BEWARE!
```

Nous pouvons maintenant utiliser la commande `kinit` pour obtenir un "ticket d'entrée" pour l'utilisateur `jane` que nous avons créé plus haut:

```
% kinit jane
MIT Project Athena (grunt.example.com)
Kerberos Initialization for "jane"
Password:
```

Essayons de lister les informations associées avec la commande `klist` pour voir si nous avons vraiment tout ce qu'il faut:

```
% klist
```

```
Ticket file:    /tmp/tkt245
Principal:      jane@EXAMPLE.COM

  Issued           Expires          Principal
Apr 30 11:23:22  Apr 30 19:23:22  krbtgt.EXAMPLE.COM@EXAMPLE.COM
```

Essayons maintenant de modifier le mot de passe en utilisant la commande passwd(1) pour vérifier si le "daemon" kpasswd est autorisé à accéder à la base de données Kerberos:

```
% passwd
realm EXAMPLE.COM
Old password for jane:
New Password for jane:
Verifying password
New Password for jane:
Password changed.
```

15.7.7. Autoriser l'utilisation de la commande `su`

Kerberos permet d'attribuer à *chaque* utilisateur qui a besoin des droits du super-utilisateur son *propre* mot de passe su(1). Nous pouvons créer un identifiant qui est autorisé à utiliser su(1) pour devenir `root`. Cela se fait en associant une instance `root` un identificateur ("principal") de base. En utilisant la commande `kdb_edit` nous pouvons créer l'entrée `jane.root` dans la base de données Kerberos:

```
# kdb_edit
Opening database...

Enter Kerberos master key:

Current Kerberos master key version is 1.

Master key entered.  BEWARE!
Previous or default values are in [brackets] ,
enter return to leave the same, or new value.

Principal name: jane
Instance: root

<Not found>, Create [y] ? y

Principal: jane, Instance: root, kdc_key_ver: 1
New Password:                    <---- entrez un mot de passe SUR ici
Verifying password

New Password:            <---- réentrez le mot de passe ici

Principal's new key version = 1
```

```
Expiration date (enter yyyy-mm-dd) [ 2000-01-01 ] ?
Max ticket lifetime (*5 minutes) [ 255 ] ? 12 <--- Laissez une valeur faible!
Attributes [ 0 ] ?
Edit O.K.
Principal name:              <---- ne rien entrer ici permet de quitter le programme
```

Vérifions maintenant les caractéristiques associées pour voir si cela fonctionne:

```
# kinit jane.root
MIT Project Athena (grunt.example.com)
Kerberos Initialization for "jane.root"
Password:
```

Nous devons maintenant ajouter l'utilisateur au fichier .klogin de `root`:

```
# cat /root/.klogin
jane.root@EXAMPLE.COM
```

Essayons maintenant la commande su(1):

```
% su
Password:
```

et voyons quelles sont nos caractéristiques:

```
# klist
Ticket file:    /tmp/tkt_root_245
Principal:      jane.root@EXAMPLE.COM

  Issued           Expires          Principal
May  2 20:43:12  May  3 04:43:12  krbtgt.EXAMPLE.COM@EXAMPLE.COM
```

15.7.8. Utiliser d'autres commandes

Dans l'exemple précédent, nous avons créé une entrée principale nommée `jane` avec une instance `root`. Cette entrée reposait sur un utilisateur ayant le même nom que l'entrée principale, c'est ce que fait par défaut Kerberos; une `entrée_principale.instance` de la forme `nom_d_utilisateur`. `root` autorisera `nom_d_utilisateur.` à utiliser su(1) pour devenir `root` si le fichier .klogin du répertoire personnel de l'utilisateur `root` est correctement renseigné:

```
# cat /root/.klogin
jane.root@EXAMPLE.COM
```

De même, si un utilisateur a dans son répertoire des lignes de la forme:

```
% cat ~/.klogin
jane@EXAMPLE.COM
jack@EXAMPLE.COM
```

Cela permet à quiconque dans le domaine EXAMPLE.COM s'étant authentifié en tant que jane ou jack (via kinit, voir plus haut) d'accéder avec rlogin(1) au compte de jane ou à ses fichiers sur le système (grunt) via rlogin(1), rsh(1) ou rcp(1).

Par exemple, jane ouvre maintenant une session sur un autre système en utilisant Kerberos:

```
% kinit
MIT Project Athena (grunt.example.com)
Password:
% rlogin grunt
Last login: Mon May  1 21:14:47 from grumble
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
        The Regents of the University of California.   All rights reserved.

FreeBSD BUILT-19950429 (GR386) #0: Sat Apr 29 17:50:09 SAT 1995
```

Ou bien jack ouvre une session sur le compte de jane sur la même machine (jane ayant modifié son fichier .klogin comme décrit plus haut, et la personne an charge de Kerberos ayant défini une entrée principale *jack* sans instance):

```
% kinit
% rlogin grunt -l jane
MIT Project Athena (grunt.example.com)
Password:
Last login: Mon May  1 21:16:55 from grumble
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
        The Regents of the University of California.   All rights reserved.
FreeBSD BUILT-19950429 (GR386) #0: Sat Apr 29 17:50:09 SAT 1995
```

15.8. Kerberos5 Traduction en Cours

15.9. OpenSSL

Une des caractéristiques que de nombreux utilisateurs ignorent souvent est la présence des outils OpenSSL dans le système FreeBSD. OpenSSL fournit une couche de transport des données chiffrée par-dessus la couche de communication, lui permettant ainsi d'être liée à de nombreux services et applications réseau.

Les applications d'OpenSSL pourront être l'authentification chiffrée de clients de messagerie, les transactions via le Web comme les paiements par carte bancaire et bien plus encore. De nombreux logiciels portés tels que www/apache13-ssl, et mail/sylpheed-claws offriront un support pour

OpenSSL lors de leur compilation.

Dans la plupart des cas le catalogue des logiciels portés tentera de compiler le logiciel porté security/openssl à moins que la variable make(1) WITH_OPENSSL_BASE ne soit explicitement fixée à la valeur "yes".

La version d'OpenSSL fournie avec FreeBSD supporte les protocoles de sécurité réseau *Secure Sockets Layer v2/v3* (SSLv2/SSLv3), et *Transport Layer Security v1* (TLSv1) et peut être utilisée comme bibliothèque de chiffrement d'usage général.

Bien que OpenSSL supporte l'algorithme IDEA, il est désactivé par défaut en raison des problèmes de brevets aux USA. Pour l'utiliser, le texte de la licence devrait être consulté et si les termes de cette licence sont acceptables, la variable MAKE_IDEA doit être activée dans le fichier make.conf.

Une des utilisations les plus courantes d'OpenSSL est de fournir des certificats utilisables avec des applications logicielles. Ces certificats assurent que les références de la société ou d'un individu sont valides et non frauduleuses. Si le certificat en question n'a pas été vérifié par une des nombreuses "autorité de certification" ("Certificate Authorities") ou CAs, une alerte est généralement produite. Une autorité de certification est une société, comme VeriSign, qui signera les certificats afin de valider les références d'individus ou de sociétés. Ce processus a un coût et n'est pas obligatoire pour utiliser des certificats, cependant cela pourra mettre plus à l'aise les utilisateurs les plus paranoïaques.

15.9.1. Générer des certificats

Pour générer un certificat, la commande suivante est disponible:

```
# openssl req -new -nodes -out req.pem -keyout cert.pem
Generating a 1024 bit RSA private key
.............++++++
.....................................++++++
writing new private key to 'cert.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:PA
Locality Name (eg, city) []:Pittsburgh
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Company
Organizational Unit Name (eg, section) []:Systems Administrator
Common Name (eg, YOUR name) []:localhost.example.org
Email Address []:trhodes@FreeBSD.org
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:SOME PASSWORD
An optional company name []:Another Name
```

Notez la réponse à la question "Common Name" qui est un nom de domaine. Cette question demande l'entrée d'un serveur de noms à des fins de vérification; entrer autre chose qu'un nom de domaine produira un certificat inutilisable. D'autres options sont disponibles comme par exemple: la date d'expiration, des algorithmes de chiffrement alternatifs, etc. Une liste complète peut être obtenue en consultant la page de manuel openssl(1).

Deux fichiers doivent maintenant être présents dans le répertoire dans lequel la commande a été exécutée. La demande de certificat, req.pem, peut être envoyée à une autorité de certification qui validera les références que vous avez saisies, signera la demande et vous retournera le certificat. Le deuxième fichier s'appellera cert.pem et sera la clé privée du certificat et devra être à tout prix protégée; si ce fichier tombe dans d'autres mains, il pourra être utilisé pour imiter votre identité (ou votre serveur).

Pour les cas où une signature d'une CA n'est pas indispensable, un certificat auto-signé peut être créé. Générez tout d'abord la clé RSA:

```
# openssl dsaparam -rand -genkey -out myRSA.key 1024
```

Générez ensuite la clé de la CA:

```
# openssl gendsa -des3 -out myca.key myRSA.key
```

Utilisez cette clé pour créer le certificat:

```
# openssl req -new -x509 -days 365 -key myca.key -out new.crt
```

Deux fichiers devraient être présents maintenant dans le répertoire: un fichier de signature de l'autorité de certification, myca.key, et le certificat lui-même, new.crt. Ces fichiers doivent être placés dans un répertoire, de préférence sous /etc, qui est uniquement lisible que par `root`. Les permissions 0700 devraient convenir et peuvent être fixées à l'aide de l'utilitaire `chmod`.

15.9.2. Utilisation des certificats, un exemple

A quoi peuvent servir ces fichiers? Un bon exemple serait le chiffrage des connexions au MTAsendmail. Cela permettra de faire disparaître l'utilisation d'une authentification en clair pour les utilisateurs qui envoient du courrier via le MTA local.

Ce n'est pas la meilleure utilisation au monde étant donné que certains clients de messagerie afficheront une erreur si le certificat n'a pas été installé localement. Reportez-vous à la documentation du logiciel pour plus d'information sur

l'installation de certificats.

Les lignes suivantes doivent être ajoutées dans le fichier .mc local:

```
dnl SSL Options
define(`confCACERT_PATH',`/etc/certs')dnl
define(`confCACERT',`/etc/certs/new.crt')dnl
define(`confSERVER_CERT',`/etc/certs/new.crt')dnl
define(`confSERVER_KEY',`/etc/certs/myca.key')dnl
define(`confTLS_SRV_OPTIONS', `V')dnl
```

Où /etc/certs/ est le répertoire à utiliser pour stocker localement les certificats et les clés. La dernière condition nécessaire étant une reconstruction du fichier .cf. Cela se fait facilement en tapant `make`install à l'intérieur du répertoire /etc/mail. Suivi d'un `make`restart qui devrait relancer le "daemon"sendmail.

Si tout s'est bien passé il n'y aura pas de message d'erreur dans le fichier /var/log/maillog et sendmail apparaîtra dans la liste des processus.

Comme test simple, connectez vous au serveur de messagerie à l'aide de l'utilitaire telnet(1):

```
# telnet example.com 25
Trying 192.0.34.166...
Connected to example.com.
Escape character is '^]'.
220 example.com ESMTP Sendmail 8.12.10/8.12.10; Tue, 31 Aug 2004 03:41:22 -0400 (EDT)
ehlo example.com
250-example.com Hello example.com [192.0.34.166], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH LOGIN PLAIN
250-STARTTLS
250-DELIVERBY
250 HELP
quit
221 2.0.0 example.com closing connection
Connection closed by foreign host.
```

Si la ligne "STARTTLS" apparaît dans la sortie, cela signifie alors que tout fonctionne correctement.

15.10. IPsec

Caractères de terminaison

Dans tous les exemples de cette section, et d'autres sections, vous remarquerez qu'il y aura un "^D" à la fin de certains exemples. Cela signifie qu'il faut maintenir la touche `Ctrl` enfoncée et appuyer sur la touche `D`. Un autre caractère couramment utilisé est "^C", qui signifie de maintenir enfoncé la touche `Ctrl` et d'appuyer sur `C`.

Pour d'autres documents détaillant l'implémentation d'IPsec, jetez un oeil à http://www.daemonnews.org/200101/ipsec-howto.html et http://www.freebsddiary.org/ipsec.php.

Le mécanisme IPsec fournit des communications sécurisées sur couche IP ou à travers les *sockets*. Cette section explique comment l'utiliser. Pour des détails concernant l'implémentation d'IPsec, reportez-vous au Manuel du développeur.

L'implémentation actuelle d'IPsec supporte le mode transport et le mode tunnel. Cependant, il y a des restrictions au mode tunnel. http://www.kame.net/newsletter/ fournit des exemples plus exhaustifs.

Soyez informé que pour utiliser cette fonctionnalité, vous devez avoir les options suivantes présentes dans votre fichier de configuration du noyau:

```
options         IPSEC           #IP security
options         IPSEC_ESP       #IP security (crypto; define w/IPSEC)
```

15.10.1. Exemple en mode transport avec IPv4

Configurons une association de sécurité pour déployer un canal sécurisé entre la Machine A (10.2.3.4) et la Machine B (10.6.7.8). Notre exemple est un peu compliqué. De A vers B, nous n'utilisons que l'ancien AH. De B vers A, le nouvel AH et le nouvel ESP sont combinés.

Nous devons maintenant choisir les algorithmes correspondant à "AH"/"nouvel AH"/"ESP"/ "nouvel ESP". Reportez-vous à la page de manuel setkey(8) pour connaître les noms des algorithmes. Nous utiliserons MD5 pour AH, new-HMAC-SHA1 pour le nouvel AH, et new-DES-expIV avec 8 octets IV pour le nouvel ESP.

La longueur de la clé dépend de chaque algorithme. Par exemple, elle doit être égale à 16 octets pour MD5, 20 pour new-HMAC-SHA1, et 8 pour new-DES-expIV. Nous choisissons maintenant "MYSECRETMYSECRET", "KAMEKAMEKAMEKAMEKAME", "PASSWORD", respectivement.

Définissons maintenant le SPI (*Security Parameter Index*) pour chaque protocole. Remarquez qu'il nous faut 3 SPIs pour ce canal sécurisé puisqu'il y aura trois entêtes de sécurité (une de la Machine A vers la Machine B et deux de la Machine B vers la Machine A). Notez également que les SPIs doivent être supérieurs à 256. Nous choisirions 1000, 2000 et 3000 respectivement.

```
          (1)
   Machine A ------> Machine B
```

```
    (1)PROTO=AH
        ALG=MD5(RFC1826)
        KEY=MYSECRETMYSECRET
        SPI=1000

                (2.1)
    Machine A <------ Machine B
              <------
                (2.2)

    (2.1)
    PROTO=AH
        ALG=new-HMAC-SHA1(new AH)
        KEY=KAMEKAMEKAMEKAMEKAME
        SPI=2000

    (2.2)
    PROTO=ESP
        ALG=new-DES-expIV(new ESP)
            IV length = 8
        KEY=PASSWORD
        SPI=3000
```

Maintenant, définissons l'association de sécurité. Exécutons setkey(8) sur la Machine A et la Machine B:

```
# setkey -c
    add 10.2.3.4 10.6.7.8 ah-old  1000 -m transport -A keyed-md5 "MYSECRETMYSECRET" ;
    add 10.6.7.8 10.2.3.4 ah  2000 -m transport -A hmac-sha1 "KAMEKAMEKAMEKAMEKAME" ;
    add 10.6.7.8 10.2.3.4 esp 3000 -m transport -E des-cbc "PASSWORD" ;
    ^D
```

En fait, la communication IPsec n'aura pas lieu avant que les entrées de politique de sécurité ne soient définies. Dans notre cas, il faut le faire sur les deux machines.

```
Côté A:

# setkey -c
    spdadd 10.2.3.4 10.6.7.8 any -P out ipsec
    ah/transport/10.2.3.4-10.6.7.8/require ;
    ^D

Côté B:

# setkey -c
    spdadd 10.6.7.8 10.2.3.4 any -P out ipsec
    esp/transport/10.6.7.8-10.2.3.4/require ;
    spdadd 10.6.7.8 10.2.3.4 any -P out ipsec
```

```
    ah/transport/10.6.7.8-10.2.3.4/require ;
    ^D

   Machine A --------------------------> Machine E
   10.2.3.4                               10.6.7.8
      |                                     |
      ========= ancien AH keyed-md5 ========>

      <======== nouveau AH hmac-sha1 ========
      <======== nouveau ESP des-cbc =========
```

15.10.2. Exemple en mode transport avec IPv6

Un autre exemple utilisant IPv6.

Le mode de transport ESP est recommandé pour le port TCP numéro 110 entre la Machine-A et la Machine-B.

```
            ============ ESP ============
            |                           |
         Machine-A                   Machine-B
         fec0::10 -------------------- fec0::11
```

L'algorithme de chiffrement est blowfish-cbc avec la clé "kamekame", et l'algorithme d'authentification est hmac-sha1 avec la clé "this is the test key". Configuration de la Machine-A:

```
# setkey -c <<EOF
    spdadd fec0::10[any] fec0::11[110] tcp -P out ipsec
    esp/transport/fec0::10-fec0::11/use ;
    spdadd fec0::11[110] fec0::10[any] tcp -P in ipsec
    esp/transport/fec0::11-fec0::10/use ;
    add fec0::10 fec0::11 esp 0x10001
    -m transport
    -E blowfish-cbc "kamekame"
    -A hmac-sha1 "this is the test key" ;
    add fec0::11 fec0::10 esp 0x10002
    -m transport
    -E blowfish-cbc "kamekame"
    -A hmac-sha1 "this is the test key" ;
    EOF
```

et de la Machine-B:

```
# setkey -c <<EOF
    spdadd fec0::11[110] fec0::10[any] tcp -P out ipsec
    esp/transport/fec0::11-fec0::10/use ;
    spdadd fec0::10[any] fec0::11[110] tcp -P in ipsec
```

```
    esp/transport/fec0::10-fec0::11/use ;
    add fec0::10 fec0::11 esp 0x10001 -m transport
    -E blowfish-cbc "kamekame"
    -A hmac-sha1 "this is the test key" ;
    add fec0::11 fec0::10 esp 0x10002 -m transport
    -E blowfish-cbc "kamekame"
    -A hmac-sha1 "this is the test key" ;
    EOF
```

Remarquez la direction de SP.

15.10.3. Exemple en mode tunnel avec IPv4

Mode tunnel entre deux passerelles de sécurité

Le protocole de sécurité est l'ancien mode tunnel AH, i.e. spécifié par la RFC1826, avec keyed-md5 comme algorithme d'authentification et "this is the test" comme clé.

```
                          ======= AH =======
                          |                |
       Réseau-A       Passerelle-A     Passerelle-B       Réseau-B
      10.0.1.0/24 ---- 172.16.0.1 ----- 172.16.0.2 ---- 10.0.2.0/24
```

Configuration de la Passerelle-A:

```
# setkey -c <<EOF
    spdadd 10.0.1.0/24 10.0.2.0/24 any -P out ipsec
    ah/tunnel/172.16.0.1-172.16.0.2/require ;
    spdadd 10.0.2.0/24 10.0.1.0/24 any -P in ipsec
    ah/tunnel/172.16.0.2-172.16.0.1/require ;
    add 172.16.0.1 172.16.0.2 ah-old 0x10003 -m any
    -A keyed-md5 "this is the test" ;
    add 172.16.0.2 172.16.0.1 ah-old 0x10004 -m any
    -A keyed-md5 "this is the test" ;

EOF
```

Si le numéro de port n'est pas précisé comme ci-dessus, alors `[any]` est utilisé. `-m` définit le mode de SA à utiliser. `-m any` signifie tout mode de protocole de sécurité. Vous pouvez utiliser cette SA à la fois en mode transport et en mode tunnel.

et de la Passerelle-B:

```
# setkey -c <<EOF
    spdadd 10.0.2.0/24 10.0.1.0/24 any -P out ipsec
    ah/tunnel/172.16.0.2-172.16.0.1/require ;
    spdadd 10.0.1.0/24 10.0.2.0/24 any -P in ipsec
```

```
    ah/tunnel/172.16.0.1-172.16.0.2/require ;
    add 172.16.0.1 172.16.0.2 ah-old 0x10003 -m any
    -A keyed-md5 "this is the test" ;
    add 172.16.0.2 172.16.0.1 ah-old 0x10004 -m any
    -A keyed-md5 "this is the test" ;

EOF
```

Etablir une SA regroupée entre deux passerelles de sécurité

On désire le mode de transport AH et le mode tunnel ESP entre Passerelle-A et Passerelle-B. Dans ce cas, on applique d'abord le mode tunnel ESP puis le mode de transport AH.

```
                          ========== AH =========
                          |  ======= ESP =====  |
                          |  |              |  |
   Réseau-A         Passerelle-A        Passerelle-B        Réseau-B
fec0:0:0:1::/64 --- fec0:0:0:1::1 ---- fec0:0:0:2::1 --- fec0:0:0:2::/64
```

15.10.4. Exemple en mode tunnel avec IPv6

L'algorithme de chiffrement est 3des-cbc, et l'algorithme d'authentification est hmac-sha1. L'algorithme d'authentification pour AH est hmac-md5. Configuration de la Passerelle-A:

```
# setkey -c <<EOF
    spdadd fec0:0:0:1::/64 fec0:0:0:2::/64 any -P out ipsec
    esp/tunnel/fec0:0:0:1::1-fec0:0:0:2::1/require
    ah/transport/fec0:0:0:1::1-fec0:0:0:2::1/require ;
    spdadd fec0:0:0:2::/64 fec0:0:0:1::/64 any -P in ipsec
    esp/tunnel/fec0:0:0:2::1-fec0:0:0:1::1/require
    ah/transport/fec0:0:0:2::1-fec0:0:0:1::1/require ;
    add fec0:0:0:1::1 fec0:0:0:2::1 esp 0x10001 -m tunnel
    -E 3des-cbc "kamekame12341234kame1234"
    -A hmac-sha1 "this is the test key" ;
    add fec0:0:0:1::1 fec0:0:0:2::1 ah 0x10001 -m transport
    -A hmac-md5 "this is the test" ;
    add fec0:0:0:2::1 fec0:0:0:1::1 esp 0x10001 -m tunnel
    -E 3des-cbc "kamekame12341234kame1234"
    -A hmac-sha1 "this is the test key" ;
    add fec0:0:0:2::1 fec0:0:0:1::1 ah 0x10001 -m transport
    -A hmac-md5 "this is the test" ;

    EOF
```

Etablir des SAs avec les différentes extrémités

On désire un mode tunnel ESP entre Machine-A et Passerelle-A. L'algorithme de chiffrement est cast128-cbc, et l'algorithme d'authentification pour ESP est hmac-sha1. Le mode de transport ESP

est recommandé entre Machine-A et Machine-B. L'algorithme de chiffrement est rc5-cbc, et l'algorithme d'authentification pour ESP est hmac-md5.

```
            ================= ESP =================
            |  ======= ESP =======                |
            |  |                 |                |
          Machine-A        Passerelle-A         Machine-B
        fec0:0:0:1::1 ---- fec0:0:0:2::1 ---- fec0:0:0:2::2
```

Configuration de la Machine-A:

```
# setkey -c <<EOF
    spdadd fec0:0:0:1::1[any] fec0:0:0:2::2[80] tcp -P out ipsec
    esp/transport/fec0:0:0:1::1-fec0:0:0:2::2/use
    esp/tunnel/fec0:0:0:1::1-fec0:0:0:2::1/require ;
    spdadd fec0:0:0:2::1[80] fec0:0:0:1::1[any] tcp -P in ipsec
    esp/transport/fec0:0:0:2::2-fec0:0:0:l::1/use
    esp/tunnel/fec0:0:0:2::1-fec0:0:0:1::1/require ;
    add fec0:0:0:1::1 fec0:0:0:2::2 esp 0x10001
    -m transport
    -E cast128-cbc "12341234"
    -A hmac-sha1 "this is the test key" ;
    add fec0:0:0:1::1 fec0:0:0:2::1 esp 0x10002
    -E rc5-cbc "kamekame"
    -A hmac-md5 "this is the test" ;
    add fec0:0:0:2::2 fec0:0:0:1::1 esp 0x10003
    -m transport
    -E cast128-cbc "12341234"
    -A hmac-sha1 "this is the test key" ;
    add fec0:0:0:2::1 fec0:0:0:1::1 esp 0x10004
    -E rc5-cbc "kamekame"
    -A hmac-md5 "this is the test" ;

    EOF
```

15.11. OpenSSH

OpenSSH est un ensemble d'outils de connexion réseau utilisés pour accéder à des machines distantes de façon sécurisée. Ils peuvent être utilisés comme remplaçants directs de `rlogin`, `rsh`, `rcp`, et `telnet`. De plus, OpenSSH peut sécuriser n'importe quelle connexion TCP/IP via un tunnel. OpenSSH chiffre tout le trafic de façon à déjouer les écoutes réseau, les prises de contrôle de connexion, et aux attaques au niveau du réseau.

OpenSSH est maintenu par le projet OpenBSD, et est basé sur SSH v1.2.12 avec tous les récentes corrections et mises à jour. Il est compatible avec les protocoles SSH 1 et 2. OpenSSH est présent dans le système de base depuis FreeBSD 4.0.

15.11.1. Les avantages à utiliser OpenSSH

Normalement, quand on utilise telnet(1) ou rlogin(1), les données sont envoyées sur le réseau en clair, sous forme non chiffrée. Des "renifleurs de paquets" placés n'importe où entre le client et le serveur peuvent prendre connaissance de votre nom d'utilisateur, de votre mot de passe et des données transmises lors de votre session. OpenSSH offre une variété de méthodes d'authentification et de chiffrage pour éviter ce genre de problème.

15.11.2. Activer sshd

Assurez-vous d'ajouter la ligne suivante à votre fichier rc.conf:

```
sshd_enable="YES"
```

Cela chargera le "daemon" ssh à l'initialisation suivante du système. Alternativement, vous pouvez tout simplement exécuter le "daemon" sshd directement en tapant `sshd` sur la ligne de commande.

15.11.3. Client SSH

L'utilitaire ssh(1) fonctionne de la même manière que rlogin(1):

```
# ssh user@example.com
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Host 'example.com' added to the list of known hosts.
user@example.com's password: *******
```

L'ouverture de session se poursuit comme si elle avait lancée par rlogin(1) ou telnet(1). Le système SSH utilise un système d'empreinte de clé pour vérifier l'authenticité du serveur quand le client se connecte. L'utilisateur est invité à entrer `yes` uniquement à la première connexion. Lors des futures connexions, l'empreinte de la clé sauvegardé est vérifiée. Le client SSH vous avertira si l'empreinte sauvée diffère de l'empreinte reçue lors de futures tentatives de connexion. Les empreintes sont sauvées dans le fichier ~/.ssh/known_hosts, ou ~/.ssh/known_hosts2 pour les empreintes du protocole SSH 2.

Par défaut, les serveurs OpenSSH sont configurés pour accepter les connexions dans les deux protocoles SSH 1 et 2. Le client peut, cependant, choisir entre les deux. Le protocole 2 est connu pour être plus robuste et plus sécurisé que son prédécesseur.

`ssh` peut être forcé à utilisé l'un des protocole en passant l'argument `-1` ou `-2` pour le protocole 1 ou 2 respectivement.

15.11.4. Copie sécurisée

La commande scp(1) fonctionne de la même manière que rcp(1); elle copie un fichier vers ou à partir d'une machine distante à la différence qu'elle le fait d'une façon sécurisé.

```
#  scp user@example.com:/COPYRIGHT COPYRIGHT
user@example.com's password: *******
COPYRIGHT            100% |*****************************|  4735
00:00
#
```

Puisque l'empreinte a déjà été sauvée pour cette machine dans l'exemple précédent, cela se vérifie ici quand on utilise scp(1).

Les arguments passés à scp(1) sont similaires à ceux de cp(1), avec le ou les fichiers en premier argument, et la destination en second. Puisque que le fichier est copié via le réseau, par l'intermédiaire de SSH, un ou plusieurs des arguments prennent la forme `utilisateur@machine_distante:chemin_du_fichier`.

15.11.5. Configuration

Les fichiers de configuration général au système pour le "daemon" et le client OpenSSH résident dans le répertoire /etc/ssh.

ssh_config permet de paramétrer le client, tandis que sshd_config s'occupe de la configuration du "daemon".

De plus, les options `sshd_program` (/usr/sbin/sshd par défaut), et `sshd_flags` du fichier rc.conf peut fournir un niveau supplémentaire de configuration.

15.11.6. ssh-keygen

Au lieu d'utiliser des mots de passe, ssh-keygen(1) peut être employé pour générer des clés RSA pour authentifier un utilisateur:

```
% ssh-keygen -t rsa1
Initializing random number generator...
Generating p:  .++ (distance 66)
Generating q:  ..............................++ (distance 498)
Computing the keys...
Key generation complete.
Enter file in which to save the key (/home/user/.ssh/identity):
Enter passphrase:
Enter the same passphrase again:
Your identification has been saved in /home/user/.ssh/identity.
...
```

ssh-keygen(1) créera une paire de clés publique et privée à utiliser pour l'authentification. La clé privée est stockée dans le fichier ~/.ssh/identity, alors que la clé publique l'est dans le fichier ~/.ssh/identity.pub. La clé publique doit être placée dans le fichier ~/.ssh/authorized_keys sur la machine distante pour que cela fonctionne.

Ceci autorisera les connexions sur la machine distante en utilisant l'authentification RSA à la place

des mots de passe.

L'option `-t rsa1` créera des clés RSA pour le protocole SSH 1. Si vous désirez utiliser des clés RSA avec le protocole SSH 2, vous devez employer la commande `ssh-keygen -t rsa`.

Si une phrase d'authentification est utilisée avec ssh-keygen(1), l'utilisateur se verra demandé d'entrer un mot de passe à chaque utilisation de la clé privé.

Une clé DSA SSH protocole 2 peut être créée pour le même objectif en utilisant la commande `ssh-keygen -t dsa`. Cela créera une paire de clés DSA pour les sessions SSH utilisant le protocole 2. La clé publique est conservée dans ~/.ssh/id_dsa.pub, tandis que la clé privée se trouve dans ~/.ssh/id_dsa.

Les clés publiques DSA sont placées dans le fichier ~/.ssh/authorized_keys sur la machine distante.

ssh-agent(1) et ssh-add(1) sont des utilitaires employés pour la gestion de multiples clés privées protégées par mots de passe.

Les divers fichiers et options peuvent être différents selon la version d'OpenSSH dont vous disposez, pour éviter les problèmes vous devez consultez la page de manuel ssh-keygen(1).

15.11.7. Tunnels SSH

OpenSSH a la capacité de créer un tunnel pour encapsuler un autre protocole dans une session chiffrée.

La commande suivante demande à ssh(1) de créer un tunnel pour telnet:

```
% ssh -2 -N -f -L 5023:localhost:23 user@foo.example.com
%
```

La commande `ssh` est utilisée avec les options suivantes:

`-2`

Force `ssh` à utiliser la version du protocole (à ne pas utiliser si vous travaillez avec de vieux serveurs SSH).

`-N`

N'exécute aucune commande à distance, ou mode se place en mode tunnel. Si cette option est omise `ssh` initiera une session normale.

`-f`

Force `ssh` à s'exécuter en arrière-plan.

`-L`

Spécifie un tunnel local de la manière `port_local:machine_distante:port_distant`.

`user@foo.example.com`

Le serveur SSH distant.

Un tunnel SSH fonctionne grâce à l'allocation d'une "socket" qui écoute sur le port spécifié de la machine `localhost`. Il transfère ensuite toute connexion reçue sur la/le machine/port local(e) via la connexion SSH vers la machine et le port distants spécifiés.

Dans l'exemple, le port *5023* sur la machine locale transfère toute connexion sur ce port vers le port *23* de la machine distante (le `localhost` de la commande). Puisque le port *23* est celui de telnet, cela créerai une session telnet sécurisée par l'intermédiaire d'un tunnel SSH.

Cela peut être utilisé pour encapsuler n'importe quel nombre de protocoles TCP non sécurisé comme SMTP, POP3, FTP, etc.

Exemple 28. Utiliser SSH pour créer un tunnel sécurisé pour SMTP

```
% ssh -2 -N -f -L 5025:localhost:25 user@mailserver.example.com
user@mailserver.example.com's password: *****
% telnet localhost 5025
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mailserver.example.com ESMTP
```

Ceci peut être utilisé en conjonction avec ssh-keygen(1) et des comptes utilisateurs supplémentaires pour la création et l'accès au tunnel SSH sans trop de problème. Des clés peuvent être utilisées à la place de la saisie d'un mot de passe, et les tunnels peuvent être exécutés sous un utilisateur séparé.

15.11.7.1. Exemples pratiques de tunnels SSH

15.11.7.1.1. Accès sécurisé à un serveur POP3

Au travail, il y a un serveur SSH qui accepte les connexions de l'extérieur. Sur le même réseau d'entreprise réside un serveur de courrier électronique faisant fonctionner un serveur POP3. Le réseau ou le chemin entre chez vous et le bureau peut ou peut ne pas être complètement sûr. Pour cette raison, vous devez récupérer votre courrier électronique d'une façon sécurisée. La solution est de créer une connexion SSH vers le serveur SSH de votre entreprise, et d'utiliser ce tunnel vers le serveur de courrier.

```
% ssh -2 -N -f -L 2110:mail.example.com:110 user@ssh-server.example.com
user@ssh-server.example.com's password: ******
```

Quand le tunnel est configuré et fonctionne, vous pouvez demander à votre client de courrier électronique d'envoyer ses requêtes POP3 sur le port 2110 de la machine locale: `localhost`. Les connexions seront transférées de façon sécurisé à travers le tunnel jusqu'à `mail.example.com`.

15.11.7.1.2. Passer à travers un coupe-feu restrictif

Certains administrateurs réseau imposent des règles draconiennes au niveau du coupe-feu, filtrant non seulement les connexions entrantes, mais également les connexions sortantes. Il se peut que vous n'ayez accès qu'aux ports 22 et 80 de machines distantes pour SSH ou la navigation Internet.

Vous pouvez vouloir accéder à un autre (n'ayant peut-être aucun rapport avec votre travail) service, comme un serveur Ogg Vorbis pour écouter de la musique. Si le serveur Ogg Vorbis diffuse ("streaming") ses données à partir d'un port différent des ports 22 ou 80, vous ne serez alors pas en mesure d'y accéder.

La solution est de créer une connexion SSH vers une machine à l'extérieur du réseau protégé par le coupe-feu, et l'utiliser pour créer un tunnel vers le serveur Ogg Vorbis.

```
% ssh -2 -N -f -L 8888:music.example.com:8000 user@unfirewalled-system.example.org
user@unfirewalled-system.example.org's password: *******
```

Vous pouvez maintenant faire pointer votre client pour la récupération du flux de données sur le port 8888 de la machine locale, qui sera transféré jusqu'au port 8000 de la machine `music.example.com`, passant ainsi outre les restrictions du coupe-feu.

15.11.8. Lectures supplémentaires

OpenSSH

ssh(1) scp(1) ssh-keygen(1) ssh-agent(1) ssh-add(1)

sshd(8) sftp-server(8)

15.12. Listes de contrôle d'accès au système de fichiers

Avec les améliorations des systèmes de fichiers comme les "snapshots", FreeBSD 5.0 et versions suivantes offrent une nouveauté en matière de sécurité: les listes de contrôle d'accès au système de fichiers (ACLs - "Access Control Lists").

Les listes de contrôle d'accès étendent le système de permission standard d'UNIX d'une manière hautement compatible (POSIX.1e). Cette caractéristique permet à un administrateur d'utiliser avantageusement un modèle de sécurité plus sophistiqué.

Pour activer le support ACL pour les systèmes de fichiers UFS, ce qui suit:

```
options UFS_ACL
```

doit être compilé dans le noyau. Si cette option n'a pas été ajoutée, un avertissement sera affiché lors d'une tentative de montage d'un système de fichiers supportant les ACLs. Cette option est présente dans le noyau GENERIC. Les ACLs reposent sur des attributs étendus rajoutés au système de fichiers. Les attributs étendus sont nativement supportés par la prochaine génération du système de fichiers UNIX, UFS2.

Un supplément de travail d'administration est requis pour configurer les attributs étendus sous UFS1 par rapport à UFS2. Les performances des attributs étendus sous UFS2 sont sensiblement meilleures également. Il en résulte donc, que l'UFS2 est généralement recommandé par rapport à l'UFS1 pour une utilisation des listes de contrôle d'accès.

Les ACLs sont activés grâce l'option utilisée lors du montage, `acls`, qui peut être ajouté dans le fichier /etc/fstab. Cette option de montage peut être également automatiquement fixée d'une manière définitive en utilisant tunefs(8) pour modifier l'indicateur ACL du "superblock" dans l'entête du système de fichiers. Il est en général préférable d'utiliser cet indicateur pour plusieurs raisons:

- L'option de montage pour les ACLs ne peut être modifiée par un simple remontage (mount(8) `-u`), mais uniquement par un umount(8) complet et suivi d'un mount(8). Cela signifie que les ACLs ne peuvent être activées sur le système de fichiers racine après le démarrage. Cela signifie également que vous ne pouvez pas modifier la disposition d'un système de fichier une fois que c'est activé.
- Positionner l'indicateur du "superblock" fera que le système de fichiers sera toujours monté avec les ACLs activées même s'il n'y a pas d'entrée dans le fichier fstab, ou s'il y a une réorganisation des périphériques. Cela prévient le montage accidentel du système de fichiers sans les ACLs activées, ce qui peut provoquer une activation impropre des ACLs et par conséquent des problèmes de sécurité.

Nous pourrions modifier le comportement des ACLs pour permettre l'activation de l'indicateur sans le besoin d'un nouveau mount(8) complet, mais nous considérons qu'il est préférable d'éviter un montage accidentel sans les ACLs activées, parce que vous pouvez vous "tirer facilement dans les pieds" si vous activez les ACLs, puis les désactivez, et ensuite les réactivez à nouveau sans réinitialiser les attributs étendus. En général, une fois que vous avez activé les ACLs sur un système de fichiers, elles ne devraient pas être désactivées étant donné que les protections de fichiers résultantes peuvent ne pas être compatible avec celles prévues par les utilisateurs du système, et réactiver les ACLs peut réaffecter les précédentes ACLs aux fichiers qui ont depuis eût leur permissions modifiées, avec pour résultat un comportement imprévisible.

Les systèmes de fichiers avec les ACLs activées présenteront un signe `+` au niveau de leurs permissions quand elles seront affichées. Par exemple:

```
drwx------  2 robert  robert  512 Dec 27 11:54 private
drwxrwx---+ 2 robert  robert  512 Dec 23 10:57 directory1
drwxrwx---+ 2 robert  robert  512 Dec 22 10:20 directory2
drwxrwx---+ 2 robert  robert  512 Dec 27 11:57 directory3
drwxr-xr-x  2 robert  robert  512 Nov 10 11:54 public_html
```

Ici nous voyons que les répertoires directory1, directory2, et directory3 utilisent les ACLs. Ce n'est pas le cas du répertoire public_html.

15.12.1. Utilisation des ACLs

Les ACLs peuvent être affichées par l'utilitaire getfacl(1). Par exemple pour voir les ACLs sur le fichier test, on utilisera la commande:

```
% getfacl test
    #file:test
    #owner:1001
    #group:1001
    user::rw-
    group::r--
    other::r--
```

Pour modifier le paramétrage des ACLs sur ce fichier, invoquez la commande setfacl(1). Intéressons-nous à la ligne:

```
% setfacl -k test
```

L'indicateur `-k` supprimera toutes les ACLs actuellement définies pour un fichier ou un système de fichiers. Une méthode plus adaptée est d'utiliser l'option `-b` étant donné qu'elle conserve les champs de base nécessaires au bon fonctionnement des ACLs.

```
% setfacl -m u:trhodes:rwx,group:web:r--,o::--- test
```

Dans la commande ci-dessus, l'option `-m` a été utilisée pour modifier les entrées ACL par défaut. Comme il n'y avait pas d'entrées pré-définies, puisqu'elles ont été supprimées par la commande précédente, cela restaurera les options par défaut et prendra en compte les options précisées. Prenez soin de noter que si vous ajoutez un utilisateur ou un groupe qui n'existe pas sur le système, une erreur `Invalid argument` sera affichée sur la sortie standard.

15.13. Surveillance des problèmes de sécurité relatifs aux programmes tierce-partie

Ces dernières années, le monde de la sécurité a fait beaucoup de progrès dans la manière d'évaluer les vulnérabilités. Le risque d'une intrusion dans le système augmente avec l'installation et la configuration d'utilitaires tierce-partie et cela pour quasiment n'importe quel système d'exploitation disponible aujourd'hui.

L'évaluation des vulnérabilités est un facteur clé de la politique de sécurité, alors que FreeBSD publie des avis pour le système de base, faire de même pour les programmes tierce-partie dépasse les capacités du projet FreeBSD. Il existe un moyen d'atténuer les vulnérabilités des logiciels tierce-partie et de prévenir les administrateurs des problèmes de sécurité connus. Un outil FreeBSD connu sous le nom de Portaudit existe dans cet unique but.

Le logiciel porté ports-mgmt/portaudit consulte une base de données, mise à jour et maintenue par

l'équipe de sécurité de FreeBSD et les développeurs des logiciels portés, à la recherche de problèmes de sécurité connus.

Pour utiliser Portaudit, ce dernier doit être installé à partir du catalogue des logiciels portés:

```
# cd /usr/ports/ports-mgmt/portaudit && make install clean
```

Lors du processus d'installation, les fichiers de configuration de periodic(8) seront mis à jour, autorisant l'ajout des résultats de Portaudit dans l'exécution quotidienne du rapport de sécurité. Assurez-vous que les rapports de sécurité quotidiens, qui sont envoyés au compte messagerie de `root`, sont bien lus. Pas plus de configuration ne sera nécessaire.

Après l'installation, un administrateur peut mettre à jour la base de données et afficher les vulnérabilités connues des logiciels installés en invoquant la commande suivante:

```
# portaudit -Fda
```

La base de données sera automatiquement mise à jour lors de l'exécution de periodic(8), cela rendant par conséquent facultative la commande précédente. Elle n'est requise que pour les exemples qui vont suivre.

Pour contrôler à n'importe quel moment les programmes tierce-partie installés à partir du catalogue des logiciels portés, un administrateur n'aura qu'à exécuter la commande suivante:

```
# portaudit -a
```

Portaudit produira pour les logiciels vulnérables quelque chose comme ceci:

```
Affected package: cups-base-1.1.22.0_1
Type of problem: cups-base -- HPGL buffer overflow vulnerability.
Reference: http://www.FreeBSD.org/ports/portaudit/40a3bca2-6809-11d9-a9e7-
0001020eed82.html

1 problem(s) in your installed packages found.

You are advised to update or deinstall the affected package(s) immediately.
```

En faisant pointer un navigateur Web sur l'URL proposée, un administrateur pourra obtenir plus d'information au sujet de la vulnérabilité en question. Cela comprendra les versions affectées, listées par version du logiciel porté FreeBSD, ainsi que des liens vers d'autres sites Web pouvant contenir des avis de sécurité.

En résumé, Portaudit est un outil puissant et extrêmement utile quand il est employé conjointement avec le logiciel Portupgrade.

15.14. Avis de sécurité de FreeBSD

Comme plusieurs systèmes d'exploitation destinés à la production, FreeBSD publie des "Avis de sécurité". Ces avis sont généralement envoyés aux listes de diffusion traitant de la sécurité et ajoutés dans l'errata une fois seulement que les versions correspondantes ont été corrigées. Cette section aura pour objectif d'expliquer ce qu'est un avis, comment le comprendre, et quelles mesures sont à prendre pour appliquer des correctifs à un système.

15.14.1. A quoi ressemble un avis de sécurité?

Les avis de sécurité de FreeBSD ressemblent à celui présenté ci-dessous qui provient de la liste de diffusion liste de diffusion des avis de sécurité pour FreeBSD.

```
=============================================================================
FreeBSD-SA-XX:XX.UTIL                                          Security Advisory
                                                               The FreeBSD Project

Topic:          denial of service due to some problem ①

Category:       core ②
Module:         sys ③
Announced:      2003-09-23 ④
Credits:        Person@EMAIL-ADDRESS ⑤
Affects:        All releases of FreeBSD ⑥
                FreeBSD 4-STABLE prior to the correction date
Corrected:      2003-09-23 16:42:59 UTC (RELENG_4, 4.9-PRERELEASE)
                2003-09-23 20:08:42 UTC (RELENG_5_1, 5.1-RELEASE-p6)
                2003-09-23 20:07:06 UTC (RELENG_5_0, 5.0-RELEASE-p15)
                2003-09-23 16:44:58 UTC (RELENG_4_8, 4.8-RELEASE-p8)
                2003-09-23 16:47:34 UTC (RELENG_4_7, 4.7-RELEASE-p18)
                2003-09-23 16:49:46 UTC (RELENG_4_6, 4.6-RELEASE-p21)
                2003-09-23 16:51:24 UTC (RELENG_4_5, 4.5-RELEASE-p33)
                2003-09-23 16:52:45 UTC (RELENG_4_4, 4.4-RELEASE-p43)
                2003-09-23 16:54:39 UTC (RELENG_4_3, 4.3-RELEASE-p39) ⑦
FreeBSD only:   NO ⑧

For general information regarding FreeBSD Security Advisories,
including descriptions of the fields above, security branches, and the
following sections, please visit
http://www.freebsd.org/security/.

I.   Background ⑨

II.  Problem Description ⑩

III. Impact ⑪

IV.  Workaround ⑫
```

```
V.   Solution ⑬

VI.  Correction details ⑭

VII. References ⑮
```

① Le champ `Topic` indique exactement quel est le problème. C'est basiquement une introduction à l'avis de sécurité en tant que tel et mentionne l'utilitaire contenant la vulnérabilité.

② Le champ `Category` fait référence à la partie du système affectée qui peut être une parmi `core`, `contrib`, ou `ports`. La catégorie `core` signifie que la vulnérabilité affecte un composant système du système d'exploitation FreeBSD. La catégorie `contrib` précise que la vulnérabilité affecte du logiciel contribué au projet FreeBSD, comme sendmail. Et enfin la catégorie `ports` indique que la vulnérabilité affecte un logiciel du catalogue des logiciels portés.

③ Le champ `Module` fait référence à l'emplacement du composant, par exemple `sys`. Dans notre exemple, nous voyons que le module `sys` est affecté, par conséquent, cette vulnérabilité concerne un composant utilisé dans le noyau.

④ Le champ `Announced` reflète la date à laquelle l'avis de sécurité a été publié, ou annoncé au monde entier. Cela signifie que l'équipe de sécurité a vérifié que le problème existait vraiment et qu'un correctif a été ajouté au référentiel des sources de FreeBSD.

⑤ Le champ `Credits` donne le crédit de la découverte du problème à la personne ou l'organisation qui a constaté et rapporté le problème.

⑥ Le champ `Affects` explique quelles versions de FreeBSD sont affectées par cette vulnérabilité. Pour le noyau, un coup d'oeil rapide à la sortie de la commande `ident` sur les fichiers affectés aidera à déterminer la révision. Pour les logiciels portés, le numéro de version est listé après le nom du logiciel dans /var/db/pkg. Si le système ne se synchronise pas avec le référentiel CVS FreeBSD et ne recompile pas les sources quotidiennement, il y a des chances qu'il soit affecté par le problème.

⑦ Le champ `Corrected` indique la date, l'heure, le fuseau horaire, et la version de publication qui a été corrigée.

⑧ Le champ `FreeBSD only` précise si cette vulnérabilité affecte juste FreeBSD, ou si elle concerne d'autres systèmes d'exploitation également.

⑨ Le champ `Background` donne une information précise sur ce qu'est l'utilitaire affecté. La plupart du temps, ce champ indique pourquoi l'utilitaire existe sous FreeBSD, son rôle, et quelques informations sur la naissance de l'utilitaire.

⑩ Le champ `Problem Description` explique en profondeur le problème de sécurité. Cela peut comprendre des informations sur le code défectueux, ou même comment l'utilitaire pourrait être utilisé pour ouvrir un faille de sécurité.

⑪ Le champ `Impact` décrit l'impact sur le système du problème de sécurité. Par exemple, cela peut aller de l'attaque par refus de service, au gain de droits supplémentaires par les utilisateurs, en passant par l'obtention des droits de super-utilisateur par l'attaquant.

⑫ Le champ `Workaround` offre une solution de contournement possible pour les administrateurs qui ne sont pas en mesure de mettre à jour le système. Cela pouvant être due à des contraintes de temps, à une disponibilité réseau, ou une tout autre raison. Cependant, la sécurité ne devrait pas être prise à la légère, et un système affecté devrait soit être corrigé soit implémenter une

solution de contournement du problème de sécurité.

⑬ Le champ `Solution` donne les instructions sur l'application de correctifs sur le système affecté. C'est une méthode pas à pas vérifiée et testée pour obtenir un système corrigé et fonctionnant de manière sécurisée.

⑭ Le champ `Correction Details` liste la branche CVS ou la version de publication avec les points remplacés par des caractères souligné. Il donne également le numéro de révision des fichiers affectés sur chaque branche.

⑮ Le champ `References` donne en général d'autres sources d'informations. Cela peut être des URLs web, des ouvrages, des listes de diffusions, et des forums de discussion.

15.15. Comptabilité des processus

La comptabilité des processus est une mesure de sécurité avec laquelle un administrateur peut suivre l'utilisation des ressources du système, leur répartition entre les utilisateurs, surveiller le système et avoir un suivi minimal des commandes exécutées par un utilisateur.

Ce système possède des avantages et des inconvénients. Un de ses avantages est qu'une intrusion pourra être remontée jusqu'à son point d'entrée. Un des inconvénients est la quantité de journaux générée par cette comptabilité et l'espace disque que cela peut demander. Cette section guidera l'administrateur au travers des bases de la comptabilité des processus.

15.15.1. Activer et utiliser la comptabilité des processus

Avant de pouvoir utiliser la comptabilité des processus, il faut l'activer. Cela se fait en exécutant les commandes suivantes:

```
# touch /var/account/acct

# accton /var/account/acct

# echo 'accounting_enable="YES"' >> /etc/rc.conf
```

Une fois activée, les statistiques concernant le CPU, les commandes, etc. commenceront à être comptabilisée. Tous les journaux de comptabilisation des processus sont dans un format directement illisible pour l'utilisateur, ils pourront être examinés à l'aide de l'utilitaire sa(8). Si elle est utilisée sans paramètre, la commande `sa` affichera les informations relatives au nombre d'appels par utilisateur, le temps écoulé en minutes, la durée totale des temps CPU et utilisateur en minutes, le nombre moyen des opérations d'E/S, etc.

Pour afficher les informations sur les commandes utilisées, on emploiera l'utilitaire lastcomm(1). La commande `lastcomm` peut être employée pour afficher les commandes tapées par les utilisateurs sur des terminaux (ttys(5)) spécifiques; par exemple:

```
# lastcomm ls
    trhodes ttyp1
```

imprimera toute utilisation de la commande `ls` par l'utilisateur `trhodes` sur le terminal `ttyp1`.

De nombreuses autres options utiles existent et sont détaillées dans les pages de manuel lastcomm(1), acct(5) et sa(8).

Chapitre 16. Jails

16.1. Synopsis

Ce chapitre expliquera ce que sont les environnements jail (prisons) et comment les utiliser. Les environnements jail, souvent présentés comme une amélioration et un remplacement des *environnements chrootés* sont des outils très puissants pour les administrateurs système, mais certaines de leurs fonctionnalités de base peuvent être également utiles aux utilisateurs avancés.

Après avoir lu ce chapitre, vous connaîtrez:

- Ce qu'est un environnement jail, et quelle utilité il peut avoir sur une installation FreeBSD.
- Comment construire, démarrer et arrêter un environnement jail.
- Les bases de l'administration d'un environnement jail, de l'intérieur et de l'extérieur de l'environnement.

D'autres sources d'information utiles concernant les environnements jail sont:

- La page de manuel jail(8). C'est la référence pour l'emploi de l'utilitaire `jail` - l'outil d'administration qui peut être utilisé sous FreeBSD pour démarrer, arrêter, et contrôler les environnements jail FreeBSD.
- Les listes de diffusion et leurs archives. Les archives de la liste de diffusion pour les questions d'ordre général à propos de FreeBSD et d'autres listes hébergées par le serveur des listes de diffusion FreeBSD contiennent déjà quantité d'information sur les environnements jail. Il sera toujours conseillé de chercher dans les archives ou de poster une nouvelle question sur la liste de diffusion freebsd-questions.

16.2. Termes relatifs aux environnements jail

Pour faciliter la compréhension des parties du système FreeBSD relatives aux jails, leurs mécanismes internes et la manière dont ils interagissent avec le reste de FreeBSD, les termes suivants seront utilisés tout au long de ce chapitre:

chroot(2) (commande)

Un appel système FreeBSD, qui modifie le répertoire racine d'un processus et de tout ses descendants.

chroot(2) (environnement)

Environnement des processus pour lesquels l'emplacement de la racine du système de fichier a été modifiée ("chrootée"). Cela comprend les ressources comme la partie du système de fichiers qui est visible, les identifiants utilisateur et groupe qui sont disponibles, les interfaces réseaux et autres mécanismes IPC, etc.

jail(8) (commande)

L'utilitaire système d'administration qui permet le lancement de processus à l'intérieur d'un environnement jail.

hôte (système, processus, utilisateur, etc.)

Le système de contrôle d'un environnement jail. Le système hôte a accès à toutes les ressources matérielles disponibles, et peut contrôler des processus à l'extérieur et à l'intérieur d'un environnement jail. Une des différences importantes entre le système hôte et l'environnement jail est que les limitations qui s'appliquent aux processus du super-utilisateur à l'intérieur de l'environnement jail ne s'appliquent pas aux processus du système hôte.

hébergé (système, processus, utilisateur, etc.)

Un processus, un utilisateur ou toute autre entité, dont l'accès aux ressources est limité par un environnement jail FreeBSD.

16.3. Introduction

Comme l'administration système est une tâche difficile et déroutante, de nombreux outils ont été développés pour rendre la vie de l'administrateur plus simple. Ces outils apportent pour la plupart des améliorations dans la manière dont sont installés, configurés et maintenus les systèmes. Une partie des tâches dévolues à l'administrateur est la sécurisation du système, de façon à ce que le système puisse se consacrer aux tâches qui lui sont confiées sans toutefois mettre en péril sa propre sécurité.

Un de ces outils pouvant être employé pour augmenter la sécurisation d'un système FreeBSD sont les environnements *jail*. Les environnements jail ont été introduits sous FreeBSD 4.X par Poul-Henning Kamp <phk@FreeBSD.org>, mais ils ont été fortement améliorés sous FreeBSD 5.X pour en faire des sous-systèmes flexibles et puissants. Des développements sont toujours en cours pour l'amélioration de leur utilité, performances, fiabilité et sécurité.

16.3.1. Qu'est-ce qu'un environnement jail?

Les systèmes BSD disposent de l'environnement chroot(2) depuis l'époque de 4.2BSD. L'utilitaire chroot(8) peut être employé pour changer le répertoire racine d'un ensemble de processus, créant ainsi un environnement sécurisé et séparé du reste du système. Les processus créés dans l'environnement chrooté ne peuvent accéder aux fichiers et aux ressources extérieures à cet environnement. Pour cette raison, si un attaquant compromet un service tournant dans un environnement chrooté, cela ne devrait pas lui permettre de compromettre l'intégralité du système. L'utilitaire chroot(8) est parfait pour des tâches simples qui ne demandent pas trop de flexibilité ou de fonctionnalités avancées et complexes. Depuis l'apparition du concept d'environnement chrooté, de nombreuses manières de s'échapper de ces environnements ont été découvertes, et bien que cela ait été corrigé dans les versions récentes du noyau FreeBSD, il est clair que l'environnement chroot(2) n'est pas la solution idéale pour la sécurisation des services. Un nouveau sous-système devait être implémenté.

Ceci est une des raisons principales à l'origine du développement de l'environnement *jail*.

Les environnements jail améliorent de plusieurs manières le concept d'environnement chroot(2). Dans un environnement chroot(2) traditionnel, les processus ne sont limités que dans la partie du système de fichiers à laquelle ils ont accès. Le reste des ressources système (comme l'ensemble des utilisateurs système, les processus en cours d'exécution, ou le réseau) est partagé par les processus de l'environnement chrooté et les processus du système hôte. L'environnement jail étend ce modèle

en virtualisant non seulement l'accès au système de fichiers mais également l'ensemble des utilisateurs, la partie réseau du noyau FreeBSD et quelques autres éléments du système. Un ensemble plus complet de contrôles fins pour optimiser l'accès à un environnement jail est décrit dans la Optimisation et administration.

Un environnement jail est caractérisé par quatre éléments:

- Une arborescence de répertoires - le point d'accès à l'environnement jail. Une fois à l'intérieur de l'environnement jail, un processus ne peut s'échapper hors de cette arborescence. Les traditionnels problèmes de sécurité qui grèvent l'architecture chroot(2) d'origine n'affecteront pas les environnements jail FreeBSD.
- Un nom de machine - le nom de machine qui sera utilisé à l'intérieur de l'environnement jail. Les environnements jails sont principalement utilisés pour l'hébergement de services réseaux, par conséquent choisir un nom évocateur pour chaque environnement peut être d'une grande aide pour l'administrateur système.
- Une adresse IP - elle sera assignée à l'environnement jail et ne peut, en aucun cas, être modifiée pendant toute la durée de vie de l'environnement. L'adresse IP d'un environnement jail est en général un alias d'une interface réseau existante, mais cela n'est pas forcément nécessaire.
- Une commande - le chemin d'accès d'un exécutable à exécuter à l'intérieur de l'environnement jail. Il est relatif au répertoire racine de l'environnement jail, et peut beaucoup varier, en fonction du type d'environnement jail mis en oeuvre.

En dehors de cela les environnements jail peuvent avoir leur propre ensemble d'utilisateurs et leur propre utilisateur `root`. Naturellement les pouvoirs de l'utilisateur `root` sont limités à l'environnement jail et, du point de vue du système hôte, l'utilisateur `root` de l'environnement jail n'est pas un utilisateur omnipotent. De plus, l'utilisateur `root` d'un environnement jail n'est pas autorisé à effectuer des opérations critiques au niveau du système en dehors de son environnement jail(8). Plus d'information au sujet des possibilités et des restrictions de l'utilisateur `root` sera donnée dans la Optimisation et administration ci-après.

16.4. Création et contrôle de l'environnement jail

Certains administrateurs divisent les environnements jail en deux catégories: les environnements jails "complets", qui ressemblent à un véritable système FreeBSD, et les environnements jails de "service", qui sont dédiés à une application ou un seul service, et tournant éventuellement avec des privilèges. Cette séparation est juste conceptuelle et n'affecte pas la création de l'environnement jail. La page de manuel jail(8) est très claire quant à la procédure de création d'un environnement jail:

```
# setenv D /here/is/the/jail
# mkdir -p $D ①
# cd /usr/src
# make world DESTDIR=$D ②
# cd etc/ [9]
# make distribution DESTDIR=$D ③
# mount_devfs devfs $D/dev ④
```

① Sélectionner un emplacement pour l'environnement est le meilleur point de départ. C'est l'endroit où l'environnement jail se trouvera dans le système de fichiers de la machine hôte. Un bon choix peut être /usr/jail/jailname, où *jailname* est le nom de machine identifiant l'environnement jail. Le système de fichiers /usr/ dispose généralement de suffisamment d'espace pour le système de fichiers de l'environnement jail, qui est pour les environnements "complets", essentiellement, une copie de chaque fichier présent dans une installation par défaut du système de base de FreeBSD.

② Cette commande peuplera l'arborescence du répertoire choisi comme emplacement pour l'environnement jail avec les binaires, les bibliothèques, les pages de manuel, etc. nécessaires. Tout sera fait selon le style FreeBSD habituel - en premier lieu tout est compilé, puis ensuite installé à l'emplacement voulu.

③ La cible `distribution` pour make installe tous les fichiers de configuration nécessaires. Ou pour faire simple, cette commande installe tous les fichiers installables du répertoire /usr/src/etc/ vers le répertoire /etc de l'environnement jail: $D/etc/.

④ Le montage du système de fichiers devfs(8) à l'intérieur d'un environnement jail n'est pas requis. Cependant, toutes, ou presque toutes les applications nécessitent l'accès à au moins un périphérique, en fonction du rôle de l'application. Il est vraiment important de contrôler l'accès aux périphériques depuis l'intérieur d'un environnement jail, comme un mauvais paramétrage pourrait permettre à quelqu'un de malintentionné de faire de "mauvaises" choses dans l'environnement jail. Le contrôle sur devfs(8) est géré par l'intermédiaire d'un ensemble de règles qui est décrit dans les pages de manuel devfs(8) et devfs.conf(5).

Une fois l'environnement jail installé, il peut être lancé en employant l'utilitaire jail(8). Cet outil requiert obligatoirement quatre arguments qui sont décrits dans la Qu'est-ce qu'un environnement jail?. D'autres arguments peuvent également être utilisés, pour par exemple exécuter le processus avec les droits d'un utilisateur particulier. L'argument `command` dépend du type d'environnement; pour un *système virtuel*, /etc/rc est un bon choix puisque la séquence de démarrage d'un véritable système FreeBSD sera dupliquée. Pour un environnement jail de type *service*, cela dépendra du service ou de l'application qui sera exécuté dans l'environnement jail.

Les environnements jails sont souvent lancés au démarrage de la machine et le système rc de FreeBSD propose une méthode simple pour cela.

1. Une liste des environnements jail autorisés à être lancés au démarrage du système devrait être ajoutée au fichier rc.conf(5):

```
jail_enable="YES"   # Utiliser NO pour désactiver le lancement des
environnements jail
jail_list="www"     # Liste des noms des environnements jail séparés par une
espace
```

2. Pour chaque environnement listé dans `jail_list`, un ensemble de paramètres rc.conf(5), qui décrivent l'environnement jail, devrait être ajouté:

```
jail_www_rootdir="/usr/jail/www"     # le répertoire racine de l'environnement
```

```
jail
jail_www_hostname="www.example.org"  # le nom de machine de l'environnement
jail
jail_www_ip="192.168.0.10"           # son adresse IP
jail_www_devfs_enable="YES"          # monter devfs dans l'environnement jail
jail_www_devfs_ruleset="www_ruleset" # les règles devfs à appliquer à
l'environnement jail
```

Le démarrage par défaut des environnements jails, configuré dans rc.conf(5), exécutera la procédure /etc/rc de l'environnement jail, ce qui suppose que l'environnement est un système virtuel complet. Pour les environnements jail de service, la commande de démarrage par défaut de l'environnement devrait être modifiée en configurant correctement l'option `jailjailnameexec_start`.

Pour une liste complète des options disponibles, veuillez consulter la page de manuel rc.conf(5).

La procedure /etc/rc.d/jail peut être utilisée pour démarrer ou arrêter un environnement jail à la main si une entrée pour l'environnement existe dans le fichier rc.conf:

```
# /etc/rc.d/jail start www
# /etc/rc.d/jail stop www
```

Il n'existe pas pour le moment de méthode propre pour arrêter un environnement jail(8). C'est dû au fait que les commandes normalement employées pour arrêter proprement un système ne peuvent être utilisées à l'intérieur d'un environnement jail. La meilleur façon d'arrêter un environnement jail est de lancer la commande suivante à l'intérieur de l'environnement ou en utilisant le programme jexec(8) depuis l'extérieur de l'environnement:

```
# sh /etc/rc.shutdown
```

Plus d'information à ce sujet peut être trouvé dans la page de manuel de jail(8).

16.5. Optimisation et administration

Il existe plusieurs options qui peuvent être configurées pour n'importe quel environnement jail, et de nombreuses manières de combiner un système FreeBSD hôte avec des environnements jail pour donner naissance à des applications haut-niveau. Cette section présente:

- Certaines des options disponibles pour l'optimisation du fonctionnement et des restrictions de sécurité implémentées par une installation jail.
- Des applications de haut niveau pour la gestion des environnements jail, qui sont disponibles dans le catalogue des logiciels portés, et peuvent être utilisées pour implémenter des environnements jail complets.

16.5.1. Outils systèmes pour l'optimisation d'un environnement jail sous FreeBSD

L'optimisation de la configuration d'un environnement jail se fait principalement par le paramétrage de variables sysctl(8). Une sous-catégorie spécifique de sysctl(8) existe pour toutes les options pertinentes: la hiérarchie `security.jail.*` d'options du noyau FreeBSD. Ci-dessous est donnée une liste des principales variables relatives aux environnements jail avec leur valeur par défaut. Leurs noms sont explicites, mais pour plus d'information, veuillez vous référer aux pages de manuel jail(8) et sysctl(8).

- `security.jail.set_hostname_allowed: 1`
- `security.jail.socket_unixiproute_only: 1`
- `security.jail.sysvipc_allowed: 0`
- `security.jail.enforce_statfs: 2`
- `security.jail.allow_raw_sockets: 0`
- `security.jail.chflags_allowed: 0`
- `security.jail.jailed: 0`

Ces variables peuvent être utilisées par l'administrateur du *système hôte* pour ajouter ou retirer certaines limitations imposées par défaut à l'utilisateur `root`. Notez que certaines limitations ne peuvent être retirées. L'utilisateur `root` n'est pas autorisé à monter ou démonter des systèmes de fichiers à partir d'un environnement jail(8). L'utilisateur `root` d'un environnement jail ne peut charger ou modifier des règles devfs(8), paramétrer des règles de pare-feu, ou effectuer des tâches d'administration qui nécessitent la modification de données du noyau, comme le paramétrage du niveau de sécurité `securelevel` du noyau.

Le système de base de FreeBSD contient un ensemble d'outils basiques pour afficher les informations au sujet des environnements jail actifs, pour s'attacher à un environnement jail pour lancer des commandes d'administration. Les commandes jls(8) et jexec(8) font partie du système de base de FreeBSD et peuvent être utilisées pour effectuer les tâches simples suivantes:

- Afficher une liste des environnements jail actifs et leur identifiant (JID), leur adresse IP, leur nom de machine et leur emplacement.
- S'attacher à un environnement jail actif, à partir de son système hôte, et exécuter une commande à l'intérieur de l'environnement ou effectuer des tâches d'administration à l'intérieur de environnement lui-même. C'est tout particulièrement utile quand l'utilisateur `root` veut arrêter proprement un environnement. L'utilitaire jexec(8) peut également être employé pour lancer un interpréteur de commandes dans un environnement jail pour faire de l'administration; par exemple:

```
# jexec 1 tcsh
```

16.5.2. Outils d'administration haut niveau du catalogue des logiciels portés de FreeBSD

Parmi les nombreux utilitaires tierce-partie pour l'administration des environnements jail, un des plus complet et utile est sysutils/jailutils. C'est un ensemble de petites applications qui aident à la gestion des environnements jail(8). Veuillez consulter sa page Web pour plus d'information.

Chapitre 17. Mandatory Access Control Traduction en Cours

17.1. Synopsis

17.2. Key Terms in this Chapter

17.3. Explanation of MAC

17.4. Understanding MAC Labels

17.5. Module Configuration

17.6. The MAC bsdextended Module

17.7. The MAC ifoff Module

17.8. The MAC portacl Module

17.9. MAC Policies with Labeling Features

17.10. The MAC partition Module

17.11. The MAC Multi-Level Security Module

17.12. The MAC Biba Module

17.13. The MAC LOMAC Module

17.14. Implementing a Secure Environment with MAC

17.15. Another Example: Using MAC to Constrain a Web Server

17.16. Troubleshooting the MAC Framework

Chapitre 18. Audit des événements relatifs à la sécurité du système

18.1. Synopsis

FreeBSD dispose d'un support pour l'audit d'événements relatifs à la sécurité du système. L'audit d'événements permet un enregistrement fiable et configurable d'une grande variété d'événements système en rapport avec la sécurité, parmi lesquels les ouvertures de session, les modifications de la configuration, et les accès aux fichiers et au réseau. Ces enregistrements ou journaux peuvent être d'une très grande aide pour la surveillance d'un système, pour la détection d'intrusion, et les analyses post-mortem. FreeBSD implémente l'API et le format de fichiers BSM (*Basic Security Module*) publiés par Sun™ qui sont interopérables avec les implémentations d'audits de Solaris™ de Sun™ et de Mac OS® X d'Apple®.

Ce chapitre se concentre sur l'installation et la configuration de l'audit des événements. Il explique les stratégies utilisées pour l'audit, et propose un exemple de configuration.

Après la lecture de ce chapitre, vous saurez:

- Ce qu'est l'audit d'événements et comment cela fonctionne.
- Comment configurer l'audit d'événements sous FreeBSD pour les utilisateurs et les processus.
- Comment lire une trace d'audit en utilisant les outils de réduction et de lecture.

Avant de lire ce chapitre, vous devrez:

- Comprendre les fondements d'UNIX® et de FreeBSD (Quelques bases d'UNIX).
- Etre familier avec la configuration et la compilation du noyau (Configurer le noyau de FreeBSD).
- Avoir quelques notions de sécurité et savoir comment les appliquer à FreeBSD (Sécurité).

La fonctionnalité d'audit connaît des limitations. Tous les événements systèmes en rapport avec la sécurité ne peuvent pas être soumis à un audit, et que certains mécanismes d'ouverture de session, comme les gestionnaires de procédures de connexions basés sur Xorg et des "démons" tiers, ne permettent pas une configuration correcte de l'audit pour les ouvertures de session utilisateur.

Le système d'audit des événements permet la génération d'enregistrements détaillés de l'activité du système. Sur un système occupé, un fichier journal d'audit peut être très important quand le système est configuré pour un haut niveau de détail, dépassant plusieurs gigaoctets par semaine sur certaines configurations. Les administrateurs système devraient prendre en compte les besoins en espace disque associés avec les configurations d'audit à haut niveau de détail. Par exemple, il peut être recommandé de dédier un système de fichiers à /var/audit de manière à ce que les autres systèmes de fichiers ne soient pas affectés si le système de fichiers pour les audits est plein.

18.2. Mots-clés

Les termes suivants sont relatifs à l'audit des événements:

- *événement*: un événement pouvant être audité est n'importe quel événement pouvant faire l'objet d'un suivi par le système d'audit. La création d'un fichier, la mise en place d'une connection réseau, ou une ouverture de session sont des exemples d'événements relatifs à la sécurité. Les événements sont considérés soit comme "attribuables", quand on peut les relier à un utilisateur authentifié, soit "non-attribuables" quand on ne peut pas les relier à un utilisateur authentifié. Des événements comme ceux qui apparaissent avant l'authentification durant le processus d'ouverture de session, tels que les tentatives avec un mauvais mot de passe, sont des exemples d'événements non-attribuables.
- *classe*: désigne à l'aide d'un nom particulier des ensembles d'événements en rapport les uns avec les autres et sont utilisées dans les expressions de sélection des événements. Les classes d'événement généralement utilisées sont la "création de fichiers" (fc) l'"exécution" (ex) et l'"ouverture/fermeture de session" (lo).
- *enregistrement*: une entrée du fichier de trace d'audit décrivant un événement relatif à la sécurité. Les enregistrements contiennent le type d'événement, des informations sur l'auteur (l'utilisateur) de l'action, la date et l'heure, des informations sur tout objet ou argument en relation avec l'action, et une condition de succès ou d'échec.
- *trace d'audit*: un fichier journal consistant en une série d'enregistrements décrivant les événements relatifs à la sécurité. Les traces sont organisées de manière chronologiques par rapport à l'horaire de fin des événements. Seuls les processus autorisés peuvent ajouter des enregistrements aux fichiers journaux d'audit.
- *expression de sélection*: une chaîne de caractères contenant une liste de préfixes et de classes d'événement d'audit utilisés pour désigner des événements.
- *préselection*: le processus par lequel le système identifie quels événements intéressent l'administrateur. La configuration de la présélection utilise une série d'expressions de sélection pour déterminer quelles classes d'événement sont à auditer et pour quels utilisateurs, ainsi que le paramétrage global qui s'applique aux processus authentifiés et non-authentifiés.
- *réduction*: le processus par lequel les enregistrements de traces d'audit existantes sont sélectionnés pour être conservés, imprimés ou analysés. Ou encore le processus qui supprime de la trace d'audit les enregistrements non-désirés. En utilisant le principe de réduction, les administrateurs peuvent mettre en place des stratégies pour la conservation des données d'audit. Par exemple, les traces d'audit détaillées peuvent être conservées pendant un mois, mais passé ce délai, les traces seront réduites afin de ne préserver pour archivage que les informations relatives aux ouvertures de sessions.

18.3. Configuration de l'audit

Le support pour l'audit des événements est installé avec le système de base de FreeBSD. Le support présent dans le noyau GENERIC par défaut, et auditd(8) peut être activé en ajoutant la ligne suivante au fichier /etc/rc.conf:

```
auditd_enable="YES"
```

Puis, le daemon d'audit peut être lancé:

```
# service auditd start
```

Les utilisateurs préférant compiler un noyau sur mesure doivent ajouter la ligne suivante dans le fichier de configuration du noyau:

```
options     AUDIT
```

18.3.1. Expressions de sélection des événements

Les expressions de sélection sont utilisées à plusieurs endroits dans la configuration du système d'audit pour déterminer quels événements doivent être suivis. Les expressions contiennent une liste de classes d'événements devant correspondre. Les expressions de sélection sont évaluées de gauche à droite, et deux expressions sont combinées en ajoutant l'une à la suite de l'autre.

Classes d'événements par défaut résume les classes d'événements présentes par défaut

Tableau 4. Classes d'événements par défaut

Classe	Description	Action
all	tout	correspond à toutes les classes d'événements.
aa	authentification et autorisation	
ad	administration	Actions d'administration du système.
ap	application	Action définie par l'application.
cl	fermeture de fichiers	Enregistre les utilisations de l'appel système `close`.
ex	exécution	Enregistre les exécutions de programmes. L'audit des arguments en ligne de commande et des variables d'environnement est contrôlé par via audit_control(5) en utilisant les paramètres `argv` et `envv` pour l'entrée `policy`.
fa	accès à aux attributs des fichiers	enregistre l'accès aux attributs des objets comme stat(1), pathconf(2).

Classe	Description	Action
fc	création de fichiers	Enregistre les événements ayant pour résultat la création d'un fichier.
fd	suppression de fichiers	Enregistre les événements pour lesquels une suppression de fichier a lieu.
fm	modification des attributs d'un fichier	Enregistre les événements lors desquels une modification des attributs d'un fichier intervient, comme l'utilisation de chown(8), chflags(1), et flock(2).
fr	lecture de fichiers	Enregistre les événements qui donnent lieu à la lecture de données, l'ouverture de fichiers pour la lecture.
fw	écriture de fichiers	Enregistre les événements qui donnent lieu à l'écriture de données ou à l'écriture ou la modification de fichiers.
io	ioctl	Enregistre l'utilisation de l'appel système `ioctl`.
ip	ipc	Enregistre les différentes utilisations de communication inter-processus, dont les utilisations des tubes POSIX et les opérations IPC Système V.
lo	login_logout	Enregistre les ouvertures et fermeture de session (login(1) et logout(1)).
na	non attributable	Enregistre les événements non-attribuables.
no	classe invalide	Ne correspond à aucun des événements surveillés.
nt	réseau	Enregistre les événements relatifs au réseau, comme l'utilisation des fonctions connect(2) et accept(2).
ot	autre	Enregistre les événements divers.

Classe	Description	Action
pc	processus	Enregistre les opérations sur les processus, comme l'utilisation des fonctions exec(3) et exit(3).

Ces classes d'événement peuvent être personnalisées en modifiant les fichiers de configuration audit_class et audit_event.

Chaque classe d'audit peut être combinée avec un préfixe indiquant si les opérations réussies/échouées sont sélectionnées, et si l'entrée ajoute ou supprime une sélection pour la classe ou le type concerné. Prefixes pour les classes d'audit résume les préfixes disponibles.

Tableau 5. Prefixes pour les classes d'audit

Prefixe	Action
+	Enregistre les événements réussis de cette classe.
-	Enregistre les événements de cette classe qui ont échoué.
^	N'enregistre ni les événements réussis ni les échecs de cette classe.
^+	Ne pas enregistrer les événements réussis de cette classe.
^-	Ne pas enregistrer les événements de cette classe qui ont échoué.

Si aucun préfixe n'est présent, les succès et le échecs de l'événement seront enregistrés.

L'exemple suivant d'expression de sélection permet la sélection des ouvertures et fermetures de session réussies ou échouées, et uniquement les exécutions ayant réussies:

```
lo,+ex
```

18.3.2. Fichiers de configuration

Les fichiers de configuration suivants pour l'audit d'événements en rapport avec la sécurité se trouvent dans le répertoire /etc/security.

- audit_class: contient les définitions des classes d'audit.
- audit_control: contrôle les caractéristiques du système d'audit comme les classes d'audit par défaut, l'espace disque minimal à conserver sur le volume réservé aux journaux, la taille maximale des traces d'audit.
- audit_event: les noms et la description des événements systèmes audités ainsi qu'une liste de classes auxquelles appartiennent chaque événement.
- audit_user: les classes d'événement à auditer pour des utilisateurs spécifiques, qui s'ajoutent

aux paramètres généraux fixés par défaut à l'ouverture de session.

- audit_warn: une procédure modifiable utilisée par auditd(8) pour générer des messages d'alerte lors des situations exceptionnelles comme un espace disque faible pour les fichiers journaux d'audit ou quand il y a eu rotation de ces fichiers journaux.

Les fichiers de configuration de l'audit devraient être modifiés et gérés avec prudence étant donné que des erreurs dans la configuration pourraient donner lieu à un enregistrement incorrect des événements.

Dans la plupart des cas, les administrateurs ne devront modifier que audit_control et audit_user. Le premier contrôle les propriétés et les stratégies au niveau du système et le second peut être utilisé pour affiner l'audit pour chaque utilisateur.

18.3.2.1. Le fichier audit_control

Un certain nombre de paramètres par défaut pour le système d'audit sont spécifiés dans le fichier audit_control:

```
dir:/var/audit
dist:off
flags:lo,aa
minfree:5
naflags:lo,aa
policy:cnt,argv
filesz:2M
expire-after:10M
```

L'option `dir` est utilisée pour déclarer un ou plusieurs répertoires dans lesquels seront stockés les fichiers journaux. Si l'on mentionne plus d'un répertoire, ces derniers seront utilisés dans l'ordre à mesure qu'ils se remplissent. Il est classique de configurer le système d'audit pour le stockage des fichiers journaux sur un système de fichiers dédié, afin d'éviter toute interférence entre le système d'audit et d'autres systèmes si le système de fichiers est plein.

Si le champ `dist` est fixé à `on` ou `yes`, des liens matériel seront créés pour tous les fichiers de trace d'audit de /var/audit/dist.

Le champ `flags` fixe le masque général de présélection utilisé par défaut pour les événements attribuables. Dans l'exemple ci-dessus, les ouvertures et fermetures de sessions réussies ou échouées ainsi que les authentifications et autorisations sont enregistrées pour tous les utilisateurs.

L'option `minfree` définit le pourcentage minimal d'espace libre du système de fichiers sur lequel les traces d'audit sont stockées.

L'entrée `naflags` indique les classes à surveiller pour les événements non-attribués, comme les processus d'ouverture et de fermeture de session et les authentifications et autorisations.

L'entrée `policy` donne une liste d'indicateurs de stratégie contrôlant divers aspect du comportement de l'audit séparés par une virgule. L'indicateur `cnt` indique que le système devrait

continuer à fonctionner en dépit d'un échec dans l'audit (l'emploi de cet indicateur est hautement recommandé). L'autre indicateur `argv`, provoque l'audit des arguments passés à l'appel système execve(2) lors de l'audit de l'exécution des commandes.

L'entrée `filez` indique la taille maximale en octets autorisée pour un fichier de trace avant qu'il soit interrompu et que le système provoque sa rotation. La valeur par défaut, `0`, désactive la rotation automatique des journaux. Si la taille de fichier est inférieure à 512K, elle sera ignorée et un message sera généré.

Le champ `expire-after` indique quand un fichier de trace expirera et sera supprimé.

18.3.2.2. Le fichier audit_user

L'administrateur peut spécifier des exigences supplémentaires qu niveau de l'audit pour des utilisateurs spécifiques dans le fichier audit_user. Chaque ligne paramètre l'audit pour un utilisateur par l'intermédiaire de deux champs: le champ `alwaysaudit`, qui indique l'ensemble des événements qui devraient toujours être surveillés pour l'utilisateur, le champ, `neveraudit`, indique un ensemble d'événements qui ne devrait jamais être audité pour cet utilisateur.

L'exemple suivant d'entrées permet le suivi des ouvertures et fermetures de sessions et l'exécution de commandes avec succès de l'utilisateur `root`, et audite la création de fichiers et l'exécution de commandes avec succès pour l'utilisateur `www`. Si utilisé avec le fichier audit_control par défaut, l'entrée `lo` pour `root` est redondante, et les événements relatifs aux ouvertures et aux fermetures de sessions seront également enregistrés pour l'utilisateur `www`.

```
root:lo,+ex:no
www:fc,+ex:no
```

18.4. Travailler avec les traces d'audit

Etant donné que les traces d'audit sont stockées sous le format binaire BSM ("Basic Security Module"), plusieurs outils sont disponibles pour modifier ou convertir en texte ces fichiers de trace. Pour convertir les fichiers de trace en en texte simple, utiliser la commande `praudit`. Pour réduire le fichier de trace en vue d'une analyse, d'un archivage, ou d'une impression, utiliser la commande `auditreduce`. Cet utilitaire supporte une variété de paramètres de sélection, parmi lesquels le type d'événement, la classe de l'événement, l'utilisateur, la date ou l'heure de l'événement, et le chemin d'accès ou l'objet sur lequel on agit.

Par exemple, pour afficher sous forme de texte brut l'intégralité du contenu du fichier journal d'audit précisé:

```
# praudit /var/audit/AUDITFILE
```

Où *AUDITFILE* est le journal à afficher.

Les traces d'audit consistent en une série d'enregistrements constitués de champs que la commande `praudit` affiche de manière séquentielle, un par ligne. Chaque champ est spécifique,

comme `header` (l'entête de l'enregistrement), ou `path` (le chemin d'accès). Ce qui suit est un exemple d'événement `execve`:

```
header,133,10,execve(2),0,Mon Sep 25 15:58:03 2006, + 384 msec
exec arg,finger,doug
path,/usr/bin/finger
attribute,555,root,wheel,90,24918,104944
subject,robert,root,wheel,root,wheel,38439,38032,42086,128.232.9.100
return,success,0
trailer,133
```

Cet audit représente un appel réussi à `execve`, lors de l'exécution de la commande `finger doug`. Le champ `exec arg` contient la ligne de commande présentée par l'interpréteur de commandes au noyau. Le champ `path` contient le chemin d'accès à l'exécutable comme le voit le noyau. Le champ `attribute` décrit le binaire et précise les permissions sur le fichier. Le champ `subject` conserve l'identifiant (ID) de l'utilisateur audité, les identifiants groupe et utilisateur effectifs, les identifiants groupe et utilisateur réels, l'ID du processus, l'ID de la session, l'ID du port, et l'adresse correspondant à la session. Notez que l'ID de l'utilisateur pour l'audit diffère de l'ID réel de l'utilisateur étant donné que l'utilisateur `robert` est passé en `root` avant l'exécution de la commande, mais l'audit se fait par rapport à l'utilisateur authentifié original. Le champ `return` indique la réussite de l'exécution et le champ `trailer` termine l'enregistrement.

Le format de sortie XML est également supporté et peut être sélectionné en utilisant l'argument `-x`.

Comme les journaux d'audit peuvent être très gros, un sous-ensemble d'enregistrements peut être sélectionné en utilisant `auditreduce`. Cet exemple sélectionne tous les enregistrements produits pour l'utilisateur `trhodes` et stockés dans le fichier *AUDITFILE*:

```
# auditreduce -u trhodes /var/audit/AUDITFILE | praudit
```

Les membres du groupe `audit` sont autorisés à lire les traces d'audit présentes dans le répertoire /var/audit. Par défaut, ce groupe est vide, par conséquent seul l'utilisateur `root` peut lire les traces d'audit. Des utilisateurs peuvent être ajoutés au groupe `audit` afin de déléguer les droits de lecture des audits. Comme la possibilité de suivre le contenu des fichiers journaux de l'audit donne un aperçu significatif du comportement des utilisateurs et des processus, il est donc recommandé de déléguer avec prudence les droits de lecture des audits.

18.4.1. Surveillance en direct à l'aide de tubes d'audit

Les tubes ("pipes") d'audit sont des pseudo-périphériques "clonables" qui autorisent aux applications l'accès au flux d'enregistrement des audits en cours. C'est de tout premier intérêt pour les auteurs d'applications de détection des intrusions et de surveillance du système. Cependant, le tube d'audit est un moyen pratique pour l'administrateur pour autoriser la surveillance en direct sans avoir à faire face aux problèmes de permissions ou de rotation des fichiers journaux interrompant le flux des enregistrements des événements. Pour suivre le flux des enregistrements de l'audit en cours:

```
# praudit /dev/auditpipe
```

Par défaut, les fichiers spéciaux de périphériques correspondant aux tubes d'audit ne sont accessibles qu'à l'utilisateur `root`. Pour les rendre accessibles aux membres du groupe `audit`, ajoutez une règle `devfs` au fichier /etc/devfs.rules:

```
add path 'auditpipe*' mode 0440 group audit
```

Consultez la page de manuel devfs.rules(5) pour plus d'information sur la configuration du système de fichiers devfs.

Il est relativement simple de produire un effet de boucle sans fin, dans lequel la consultation de chaque événement enregistré par le système d'audit provoque la génération de nouveaux événements d'audit. Par exemple, si toutes les entrées/sorties réseau sont surveillées, et que `praudit` est exécuté depuis une session SSH, alors un flux continu d'événements sera généré suivant une fréquence importante, chaque événement affiché générant un autre événement. Pour cette raison, il est recommandé d'exécuter `praudit` sur un tube par l'intermédiaire de sessions sans surveillance précise des entrées/sorties.

18.4.2. Rotation et compression des fichiers de trace d'audit

Les traces d'audit sont écrites par le noyau, et sont gérées par le "démon" d'audit, auditd(8). Les administrateurs ne devraient donc pas tenter d'utiliser newsyslog.conf(5) ou tout autre outil pour assurer la rotation directe des journaux d'audit. A la place, l'utilitaire `audit` devrait être employé pour stopper l'audit, reconfigurer le système d'audit et effectuer la rotation des journaux. La commande suivante provoque la création d'un nouveau fichier journal d'audit par le "démon" et signale au noyau d'utiliser le nouveau fichier pour les enregistrements. L'ancien fichier journal sera fermé et renommé et pourra, à partir de cet instant, être manipulé par l'administrateur:

```
# audit -n
```

Si auditd(8) ne tourne pas, cette commande échouera et un message d'erreur sera généré.

Ajouter la ligne suivante au fichier /etc/crontab provoquera cette rotation toutes les douze heures:

```
0     */12      *       *       *       root    /usr/sbin/audit -n
```

La modification sera prise en compte une fois que aurez sauvegardé le fichier /etc/crontab.

La rotation automatique du fichier d'une trace d'audit basée sur la taille du fichier est possible à l'aide de l'option `filesz` de audit_control comme décrit dans Le fichier audit_control.

18.4.3. Compresser les traces d’audit

Les fichiers de trace d’audit peuvent devenir très gros, il est souvent désirable de les compresser ou sinon de les archiver une fois qu’ils ont été fermés par le "démon" d’audit. La procédure audit_warn peut être employée pour effectuer des opérations personnalisées pour une variété d’événements relatifs à l’audit, y compris l’arrêt propre des traces d’audit lors de leur rotation. Par exemple, ce qui suit peut être ajouté au fichier /etc/security/audit_warn pour compresser les traces d’audit à leur fermeture:

```
#
# Compression des fichiers de trace d'audit à leur fermeture.
#
if [ "$1" = closefile ]; then
        gzip -9 $2
fi
```

D’autres activités d’archivage pourront inclure la copie des fichiers de trace vers un serveur central, la suppression d’anciennes traces, ou la réduction des traces pour supprimer les enregistrements inutiles. Cette procédure ne sera exécutée que lorsque les fichiers de trace d’audit auront été proprement arrêtés, et ne sera pas exécutée sur les traces interrompues en cours d’utilisation suite à un arrêt incorrect du système.

Chapitre 19. Stockage des données

19.1. Synopsis

Ce chapitre couvre l'utilisation des disques sous FreeBSD. Cela comprend les disques mémoire, les disques réseau, les périphériques standards de stockage SCSI/IDE, et les périphériques utilisant l'interface USB.

Après la lecture de ce chapitre, vous connaîtrez:

- La terminologie qu'utilise FreeBSD pour décrire l'organisation des données sur un disque physique (les partitions et les tranches).
- Comment ajouter des disques durs supplémentaires sur votre système.
- Comment configurer FreeBSD pour l'utilisation de périphériques de stockage USB.
- Comment configurer des systèmes de fichiers virtuels, comme les disques mémoires.
- Comment utiliser les quotas pour limiter l'usage de l'espace disque.
- Comment chiffrer des disques pour les sécuriser contre les attaques.
- Comment créer et graver des CDs et DVDs sous FreeBSD.
- Les différents supports disponibles pour les sauvegardes.
- Comment utiliser les programmes de sauvegarde disponibles sous FreeBSD.
- Comment faire des sauvegardes sur disquettes.
- Ce que sont les "snapshots" (instantanés) de systèmes de fichiers et comment les utiliser efficacement.

Avant de lire ce chapitre, vous devrez:

- Savoir comment configurer et installer un nouveau noyau FreeBSD (Configurer le noyau de FreeBSD).

19.2. Noms des périphériques

Ce qui suit est une liste des périphériques de stockage physiques, et des noms de périphériques associés.

Tableau 6. Conventions de nom pour les disques physiques

Type de disque	Nom du périphérique
Disques durs IDE	`ad`
Lecteurs de CDROMs IDE	`acd`
Disques durs SCSI et périphériques de stockage USB	`da`
Lecteurs de CDROMs SCSI	`cd`

Type de disque	Nom du périphérique
mcd pour les CD-ROMs Mitsumi, scd pour les CD-ROMs Sony	
Lecteurs de disquette	fd
Lecteurs de bande SCSI	sa
Lecteurs de bande IDE	ast
Disques flash	fla pour les périphériques Flash DiskOnChip®
Disques RAID	aacd pour l'AdvancedRAID Adaptec®, mlxd et mlyd pour les Mylex®, amrd le MegaRAID® d'AMI, idad pour le Smart RAID de Compaq, twed pour le 3ware® RAID.

19.3. Ajouter des disques

Supposons que nous voulions ajouter un second disque SCSI à une machine qui n'a pour l'instant qu'un seul disque. Commençons par arrêter l'ordinateur et installer le disque en suivant les instructions données par le constructeur de l'ordinateur, du contrôleur et du disque. Comme il y a de nombreuses façon de procéder, ces détails dépassent le cadre de ce document.

Ouvrons maintenant une session sous le compte root. Après avoir installé le disque, consultez le fichier /var/run/dmesg.boot pour vérifier que le nouveau disque a été reconnu. Dans notre exemple, le disque que nous venons d'ajouter sera le périphérique da1 et nous le monterons sur le répertoire /1 (si vous ajoutez un disque IDE, le nom de périphérique sera ad1).

FreeBSD tourne sur des ordinateurs compatibles IBM-PC, il doit tenir compte des partitions PC BIOS. Ces dernières sont différentes des partitions BSD traditionnelles. Un disque PC peut avoir jusqu'à quatre partitions. Si le disque va être réservé uniquement à FreeBSD, vous pouvez utiliser le mode *dédié*. Sinon, FreeBSD devra utiliser une des partitions PC BIOS. FreeBSD appelle les partitions PC BIOS *tranches* ("slices") pour les distinguer des partitions BSD traditionnelles. Vous pouvez aussi des tranches sur un disque dédié à FreeBSD, mais utilisé sur une machine où un autre système d'exploitation est également installé. C'est une bonne manière pour éviter de perturber l'utilitaire fdisk des autres système d'exploitation différents de FreeBSD.

Dans le cas d'une tranche, le disque ajouté deviendra le périphérique /dev/da1s1e. Ce qui se lit: disque SCSI, numéro d'unité 1 (second disque SCSI), tranche 1 (partition PC BIOS 1), et partition BSD e. Dans le cas du mode dédié, le disque sera ajouté en tant que /dev/da1e.

En raison de l'utilisation d'entiers codés sur 32 bits pour stocker le nombre de secteurs, bsdlabel(8) est limité à 2^32-1 secteurs par disque ou 2TB dans la plupart des cas. Le format fdisk(8) n'autorise pas de secteur au delà de 2^32-1 et une largeur de plus de 2^32-1, limitant donc les partitions à 2TB et les disques à 4TB en général. Le format sunlabel(8) est limité à 2^32-1 secteur par partition et 8 partitions pour un total de 16TB d'espace. Pour des disques plus importants, les partitions gpt(8) peuvent être utilisées.

19.3.1. Utiliser sysinstall(8)

1. Naviguer dans sysinstall

   Vous pouvez utiliser `sysinstall` et ses menus simples d'emploi pour partitionner et libeller le nouveau disque. Ouvrez une session sous le compte super-utilisateur `root` ou utilisez la commande su(1). Lancez `sysinstall` et sélectionnez Configure. A l'intérieur du menu FreeBSD Configuration Menu, descendez et sélectionnez l'option Fdisk.

2. L'éditeur de partition fdisk

   Une fois dans l'utilitaire fdisk, nous pouvons taper `A` pour utiliser tout le disque pour FreeBSD. Lorsque l'on vous demande si vous voulez garder la possibilité de pouvoir coopérer avec d'autres systèmes d'exploitation ("remain cooperative with any future possible operating systems"), répondez par l'affirmative (`YES`). Enregistrez les modifications sur le disque avec `W`. Quittez maintenant l'éditeur fdisk en tapant `q`. La prochaine question concernera le secteur de démarrage ("Master Boot Record"). Comme vous ajoutez un disque à un système déjà opérationnel, choisissez **[None]**.

3. L'éditeur de label du disque

   Ensuite, vous devez quitter puis relancer sysinstall. Suivez les instructions précédentes, en choisissant cette fois l'option Label. Vous entrerez dans l'éditeur de label du disque (`Disk Label Editor`). C'est là que vous allez créer les partitions BSD traditionnelles. Un disque peut avoir jusqu'à huit partitions, libellées de `a` à `h`. Certains de ces labels ont des significations particulières. La partition `a` est la partition racine (/). Seul votre disque système (e.g., celui à partir duquel vous démarrez) doit avoir une partition `a`. La partition `b` est utilisée pour la pagination, vous pouvez avoir plusieurs disques avec des partitions de pagination. La partition `c` désigne la totalité du disque en mode dédié, ou toute la tranche FreeBSD dans le cas contraire. Les autres partitions sont à usage général.

   L'éditeur de label de sysinstall définit par défaut la partition `e` comme première partition qui n'est ni racine, ni de pagination. Dans l'éditeur de label, créez un seul système de fichiers avec l'option `C`. Quand on vous demande si ce sera un système de fichiers (FS) ou une partition de pagination, choisissez `FS` et indiquez un point de montage (e.g., /mnt). Lorsque vous ajoutez un disque sur un système déjà installé, sysinstall ne créera pas d'entrées dans /etc/fstab, donc le nom que vous donnez au point de montage n'a pas d'importance.

   Vous pouvez maintenant écrire le nouveau label sur le disque et y créer un système de fichiers. Faites-le en tapant `W`. Ignorez les erreurs de sysinstall disant que la nouvelle partition ne peut être montée. Quittez maintenant l'éditeur de label et sysinstall.

4. Dernière étape

   La dernière étape consiste à éditer le fichier /etc/fstab pour y ajouter une entrée pour votre nouveau disque.

19.3.2. Utiliser les utilitaires en ligne de commande

19.3.2.1. Utiliser les tranches - "slices"

Cette configuration permettra de faire fonctionner correctement votre disque dure avec d'autres systèmes d'exploitation qui pourraient être installé sur votre machine, et ne perturbera pas les utilitaires `fdisk` de ces autres systèmes d'exploitation. C'est la méthode recommandée pour l'installation de nouveau disques. N'utilisez le mode *dédié* que si vous avez une bonne raison de le faire!

```
# dd if=/dev/zero of=/dev/da1 bs=1k count=1
# fdisk -BI da1 #Initialize your new disk
# bsdlabel -B -w da1s1 auto #Label it.
# bsdlabel -e da1s1 # Edit the disklabel just created and add any partitions.
# mkdir -p /1
# newfs /dev/da1s1e # Repeat this for every partition you created.
# mount /dev/da1s1e /1 # Mount the partition(s)
# vi /etc/fstab # Add the appropriate entry/entries to your /etc/fstab.
```

Si vous avez un disque IDE, remplacez da par ad.

19.3.2.2. Mode dédié

Si le nouveau disque n'est pas destiné a être partagé avec un autre système d'exploitation, vous pouvez utiliser le mode *dédié*. Rappelez-vous que ce mode peut perturber les systèmes d'exploitation Microsoft; cependant, ils ne toucheront pas au disque. OS/2® d'IBM, au contraire, "s'approprie" toute partition qu'il trouve et ne reconnaît pas.

```
# dd if=/dev/zero of=/dev/da1 bs=1k count=1
# bsdlabel -Bw da1 auto
# bsdlabel -e da1               # create the `e' partition
# newfs -d0 /dev/da1e
# mkdir -p /1
# vi /etc/fstab             # add an entry for /dev/da1e
# mount /1
```

Un autre méthode est:

```
# dd if=/dev/zero of=/dev/da1 count=2
# bsdlabel /dev/da1 | bsdlabel -BR da1 /dev/stdin
# newfs /dev/da1e
# mkdir -p /1
# vi /etc/fstab                 # add an entry for /dev/da1e
# mount /1
```

19.4. RAID

19.4.1. RAID logiciel

19.4.1.1. Configuration du pilote de disque concaténé (CCD - "Concatenated Disk Driver")

Quand il est question du choix d'une solution de stockage de masse les critères de choix les plus importants à considérer sont la vitesse, la fiabilité, et le coût. Il est plutôt rare de pouvoir réunir ces trois critères; normalement un périphérique de stockage rapide et fiable est coûteux, et pour diminuer les coûts la vitesse ou la fiabilité doivent être sacrifiées.

A la conception du système décrit plus bas, le coût a été choisi comme facteur le plus important, suivi de la vitesse, et enfin la fiabilité. La vitesse de transfert des données est limitée par le réseau. Et tandis que la fiabilité est très importante, le disque CCD décrit ci-dessous est destiné au stockage de données en ligne qui sont déjà complètement sauvegardées sur CD-Rs et qui peuvent être facilement remplacées.

Définir vos propres besoins est la première étape dans le choix d'une solution de stockage de masse. Si vos critères de choix privilégient la vitesse ou la fiabilité par rapport au coût, votre solution diférera du système décrit dans cette section.

19.4.1.1.1. Installation du matériel

En plus du disque système IDE, trois disques Western Digital de 30Go, 5400 trs/min IDE forment le coeur du disque CCD décrit ci-dessous donnant approximativement 90Go de stockage en ligne. La solution idéale serait d'avoir pour chaque disque IDE son propre câble et contrôleur IDE, mais pour minimiser les coûts, des contrôleur IDE supplémentaires n'ont pas été utilisés. Aussi, les disques ont été configuré de telle façon que chaque contrôleur IDE ait un disque maître et un disque esclave.

Au redémarrage, le BIOS a été configuré pour détecter automatiquement les disques attachés. FreeBSD les a d'ailleurs détectés au redémarrage:

```
ad0: 19574MB WDC WD205BA [39770/16/63] at ata0-master UDMA33
ad1: 29333MB WDC WD307AA [59598/16/63] at ata0-slave UDMA33
ad2: 29333MB WDC WD307AA [59598/16/63] at ata1-master UDMA33
ad3: 29333MB WDC WD307AA [59598/16/63] at ata1-slave UDMA33
```

Si FreeBSD ne détecte pas les disques, assurez-vous que vous avez correctement placé les cavaliers. La plupart des disques IDE disposent également d'un cavalier "Cable Select". Ce n'est *pas* le cavalier de configuration maître/esclave. Consultez la documentation du disque pour identifier le cavalier correct.

Ensuite, réfléchissez sur la manière de les intégrer au système de fichiers. Vous devriez faire des recherches sur vinum(8) (Le gestionnaire de volume Vinum) et ccd(4). Dans cette configuration particulière, ccd(4) a été choisi.

19.4.1.1.2. Configuration du CCD

Le pilote ccd(4) vous permet de prendre plusieurs disques identiques et les concaténer en un seul système de fichiers logique. Afin d'utiliser ccd(4), vous avez besoin d'un noyau avec le support ccd(4). Ajoutez la ligne suivante à votre fichier de configuration de noyau, recompilez, et installez le noyau:

```
device   ccd
```

Le support ccd(4) peut également chargé sous la forme d'un module noyau.

Pour configurer ccd(4), vous devez tout d'abord utiliser bsdlabel(8) pour labéliser les disques:

```
bsdlabel -w ad1 auto
bsdlabel -w ad2 auto
bsdlabel -w ad3 auto
```

Cela a créé un label de disque ad1c, ad2c et ad3c qui s'étend sur l'intégralité du disque.

L'étape suivante est de modifier le type de label de disque. Vous pouvez utiliser bsdlabel(8) pour éditer les disques:

```
bsdlabel -e ad1
bsdlabel -e ad2
bsdlabel -e ad3
```

Cela ouvre le label de disque actuel de chaque disque dans l'éditeur fixé par la variable d'environnement `EDITOR`, généralement, vi(1).

Un label de disque non modifié ressemblera à quelque chose comme ceci:

```
8 partitions:
#        size   offset    fstype   [fsize bsize bps/cpg]
  c: 60074784        0    unused        0     0     0   # (Cyl.    0 - 59597)
```

Ajoutez une nouvelle partition `e` pour être utilisé par ccd(4). Cela peut être une copie de la partition `c` mais le type de système de fichiers (`fstype`) doit être `4.2BSD`. Le label de disque devait ressembler à:

```
8 partitions:
#        size   offset    fstype   [fsize bsize bps/cpg]
  c: 60074784        0    unused        0     0     0   # (Cyl.    0 - 59597)
  e: 60074784        0    4.2BSD        0     0     0   # (Cyl.    0 - 59597)
```

19.4.1.1.3. Création du système de fichiers

Maintenant que tous les disques sont labélisés, vous devez construire le ccd(4). Pour cela, utilisez ccdconfig(8), avec des options semblables à ce qui suit:

```
ccdconfig ccd0. 32. 0. /dev/ad1e. /dev/ad2e /dev/ad3e
```

- L'utilisation et la signification de chaque option est données ci-dessous:
- Le premier argument est le périphérique à configurer, dans ce cas, /dev/ccd0c. La partie /dev/ est optionnelle.
- L'entrelacement ("interleave") du système de fichiers. L'entrelacement définit la taille d'une bande de blocs disque, de 512 octets chacune normalement. Donc un entrelacement de 32 serait d'une largeur de 16384 octets.
- Paramètres pour ccdconfig(8). Si vous désirez activer les miroirs disque, vous pouvez spécifier un indicateur à cet endroit. Cette configuration ne fournit pas de miroir pour ccd(4), aussi l'indicateur est a 0 (zéro). Les derniers arguments de ccdconfig(8) sont les périphériques à placer dans le disque concaténé. Utilisez le chemin complet pour chaque périphérique.

Après avoir utilisé ccdconfig(8) le ccd(4) est configuré. Un système de fichiers peut être créé. Consultez la page de manuel de newfs(8) pour les options disponibles, ou lancez simplement:

```
newfs /dev/ccd0c
```

19.4.1.1.4. Automatiser la procédure

Généralement, vous voudrez monter le ccd(4) à chaque redémarrage. Pour cela, vous devez le configurer avant toute chose. Ecrivez votre configuration actuelle dans /etc/ccd.conf en utilisant la commande suivante:

```
ccdconfig -g  /etc/ccd.conf
```

Lors du démarrage, la procédure `/etc/rc` exécute `ccdconfig -C` si /etc/ccd.conf existe. Cela configure automatiquement le ccd(4) de façon à pouvoir être monté.

Si vous démarrez en mode mono-utilisateur, avant que vous ne puissiez monter le ccd(4), vous devez utiliser la commande suivante pour configurer l'unité:

```
ccdconfig -C
```

Pour monter automatiquement le ccd(4) placez une entrées pour le ccd(4) dans /etc/fstab, il sera ainsi monté au démarrage:

```
/dev/ccd0c              /media      ufs     rw      2       2
```

19.4.1.2. Le gestionnaire de volume Vinum

Le gestionnaire de volume Vinum est un pilote de périphérique de gestion de disques virtuels. Il sépare le disque matériel de l'interface de périphérique bloc et organise les données de telle façon qu'il en résulte une amélioration de la flexibilité, des performances et de la fiabilité, comparé à la vision traditionnelle sous forme partitionnée du stockage disque. vinum(8) implémente les modèles RAID-0, RAID-1 et RAID-5, individuellement ou combinés.

Voir le Le gestionnaire de volume Vinum pour plus d'information au sujet de vinum(8).

19.4.2. RAID Matériel

FreeBSD supporte également de nombreux contrôleurs RAID. Ces périphériques peuvent contrôler un système RAID sans nécessiter l'utilisation d'un logiciel spécifique pour FreeBSD pour gérer l'unité.

En utilisant son propre BIOS, la carte contrôle la plupart des opérations disque. Ce qui suit est une description rapide d'une configuration utilisant un contrôleur Promise IDERAID. Quand cette carte est installée et le système redémarré, une invite s'affichera posant quelques questions. Suivez les instructions à l'écran pour atteindre l'écran de configuration de la carte. A partir de là, vous avez la possibilité de combiner tous les disques attachés. En faisant cela, les disques apparaîtront sous la forme d'un unique disque sous FreeBSD. D'autres niveaux RAID peuvent être configurés en conséquence.

19.4.3. Reconstruire une unité ATA RAID1

FreeBSD vous permet de remplacer à chaud un disque défectueux dans une unité. Cela doit être fait avant redémarrage.

Vous verrez probablement dans /var/log/messages ou dans la sortie de dmesg(8) quelque chose comme:

```
ad6 on monster1 suffered a hard error.
ad6: READ command timeout tag=0 serv=0 - resetting
ad6: trying fallback to PIO mode
ata3: resetting devices .. done
ad6: hard error reading fsbn 1116119 of 0-7 (ad6 bn 1116119; cn 1107 tn 4 sn 11)
status=59 error=40
ar0: WARNING - mirror lost
```

En utilisant atacontrol(8), recherchez de plus amples informations:

```
# atacontrol list
ATA channel 0:
    Master:      no device present
    Slave:   acd0 <HL-DT-ST CD-ROM GCR-8520B/1.00> ATA/ATAPI rev 0

ATA channel 1:
    Master:      no device present
```

```
    Slave:       no device present

ATA channel 2:
    Master:  ad4 <MAXTOR 6L080J4/A93.0500> ATA/ATAPI rev 5
    Slave:       no device present

ATA channel 3:
    Master:  ad6 <MAXTOR 6L080J4/A93.0500> ATA/ATAPI rev 5
    Slave:       no device present

# atacontrol status ar0
ar0: ATA RAID1 subdisks: ad4 ad6 status: DEGRADED
```

1. Vous devrez détacher le canal ATA avec le disque défectueux de façon à pouvoir le retirer sans risque:

   ```
   # atacontrol detach ata3
   ```

2. Remplacer le disque.
3. Rattacher le canal ATA:

   ```
   # atacontrol attach ata3
   Master:  ad6 <MAXTOR 6L080J4/A93.0500> ATA/ATAPI rev 5
   Slave:   no device present
   ```

4. Rajouter le disque de rechange à l'unité:

   ```
   # atacontrol addspare ar0 ad6
   ```

5. Recontruire l'unité:

   ```
   # atacontrol rebuild ar0
   ```

6. Il est possible de contrôler l'avancée de la procédure en utilisant la commande suivante:

   ```
   # dmesg | tail -10
   [output removed]
   ad6: removed from configuration
   ad6: deleted from ar0 disk1
   ad6: inserted into ar0 disk1 as spare

   # atacontrol status ar0
   ar0: ATA RAID1 subdisks: ad4 ad6 status: REBUILDING 0% completed
   ```

7. Attendre jusqu'à la fin de cette opération.

19.5. Périphériques de stockage USB

De nombreuses solutions de stockage externes utilisent, de nos jours, le bus série universel ("Universal Serial Bus"-USB): disques durs, clés USB, graveurs de CDs, etc. FreeBSD fournit un support pour ces périphériques.

19.5.1. Configuration

Le pilote de périphériques USB de stockage de masse, umass(4), fournit le support pour les périphériques de stockage USB. Si vous utilisez le noyau GENERIC, vous n'avez rien à modifier à votre configuration. Si vous utilisez un noyau personnalisé, assurez-vous que les lignes suivantes sont présentent dans votre fichier de configuration du noyau:

```
device scbus
device da
device pass
device uhci
device ohci
device usb
device umass
```

Le pilote umass(4) utilise le sous-système SCSI pour accéder aux périphériques de stockage USB, votre périphérique USB sera vu par le système comme étant un périphérique SCSI. En fonction du contrôleur USB présent sur votre carte mère, vous n'avez besoin qu'une des lignes `device uhci` et `device ohci`, cependant avoir les deux lignes dans votre configuration du noyau est sans danger. N'oubliez pas de compiler et d'installer le nouveau noyau si vous y avez effectué des modifications.

Si votre périphérique USB est un graveur de CD ou de DVD, le pilote de périphérique SCSI CD-ROM, cd(4), doit être ajouté au noyau via la ligne:

```
device cd
```

Puisque le graveur est vu comme un disque SCSI, le pilote atapicam(4) ne devrait pas être employé dans la configuration du noyau.

Le support pour les contrôleurs USB 2.0 est fourni avec FreeBSD vous devez cependant ajouter:

```
device ehci
```

à votre fichier de configuration pour bénéficier du support USB 2.0. Notez que les pilotes uhci(4) et ohci(4) sont toujours nécessaires si vous désirez le support de l'USB 1.X.

19.5.2. Test de la configuration

La configuration est prête à être testée: branchez votre périphérique USB, et dans le tampon des messages du système (dmesg(8)), le disque devrait apparaître de cette manière:

```
umass0: USB Solid state disk, rev 1.10/1.00, addr 2
GEOM: create disk da0 dp=0xc2d74850
da0 at umass-sim0 bus 0 target 0 lun 0
da0: <Generic Traveling Disk 1.11> Removable Direct Access SCSI-2 device
da0: 1.000MB/s transfers
da0: 126MB (258048 512 byte sectors: 64H 32S/T 126C)
```

Bien évidement, le modèle, le fichier spécial de périphérique (da0) et d'autres détails peuvent être différents en fonction de votre configuration.

Comme le périphérique USB est vu comme étant un périphérique SCSI, la commande `camcontrol` peut être employée pour lister les périphériques de stockage USB attachés au système:

```
# camcontrol devlist
<Generic Traveling Disk 1.11>      at scbus0 target 0 lun 0 (da0,pass0)
```

Si le disque dispose d'un système de fichiers, vous devriez pouvoir le monter. La Ajouter des disques vous aidera à formater et créer des partitions sur le disque USB si nécessaire.

Pour rendre ce périphérique montable par un utilisateur normal, un certain nombre de paramétrages sont nécessaires. Tout d'abord, les entrées de périphériques qui sont créées lors de la connexion d'un périphérique USB doivent être accessibles à l'utilisateur. Une solution est de faire en sorte que tous les utilisateurs de ces périphériques soient membres du groupe `operator`. Cela se fait à l'aide de pw(8). Ensuite, quand ces entrées de périphériques sont créées, le groupe `operator` doit pouvoir y accéder en lecture et en écriture. Pour cela, les lignes suivantes sont ajoutées à /etc/devfs.rules:

```
[localrules=1]
add path 'da*' mode 0660 group operator
```

S'il y a déjà des disques SCSI dans le système, on doit procéder légèrement différemment. Par exemple, si le système contient déjà des disques da0 à da2 attachés au système, changez la seconde ligne pour:

```
add path 'da[3-9]*' mode 0660 group operator
```

Les disques déjà présents n'appartiendront pas au groupe `operator`.

Vous devez également activer votre ensemble de règles devfs.rules(5) dans votre fichier /etc/rc.conf:

```
devfs_system_ruleset="localrules"
```

Le noyau doit être ensuite configuré pour autoriser les utilisateurs habituels à monter des systèmes de fichiers. La méthode la plus simple est d'ajouter la ligne suivante au fichier /etc/sysctl.conf:

```
vfs.usermount=1
```

Notez que ce paramétrage ne prendra effet qu'au prochain redémarrage. Il est également possible d'utiliser sysctl(8) pour fixer cette variable.

La dernière étape est de créer un répertoire où le système de fichiers sera monté. Ce répertoire doit appartenir à l'utilisateur qui montera le système de fichiers. Une méthode adaptée et la création par `root` d'un sous-répertoire /mnt/$USER appartenant à l'utilisateur en question (remplacez *$USER* par le nom d'utilisateur de cet utilisateur):

```
# mkdir /mnt/$USER
# chown $USER:$USER /mnt/$USER
```

Supposez qu'une clé USB soit branchée et qu'un périphérique /dev/da0s1 apparaît. Comme ce type de périphériques est en général livré préformaté avec un système de fichiers de type FAT, on pourra le monter de cette manière:

```
% mount -t msdosfs -m 644 -M 755 /dev/da0s1 /mnt/$USER
```

Si vous débranchez le périphérique (le disque doit être démonté auparavant), vous devriez voir dans les messages du système quelque chose comme:

```
umass0: at uhub0 port 1 (addr 2) disconnected
(da0:umass-sim0:0:0:0): lost device
(da0:umass-sim0:0:0:0): removing device entry
GEOM: destroy disk da0 dp=0xc2d74850
umass0: detached
```

19.5.3. Lectures supplémentaires

En plus des sections Ajouter des disques et Monter et démonter des systèmes de fichiers, la lecture de différentes pages de manuel peut être également utile: umass(4), camcontrol(8), et usbdevs(8).

19.6. Création et utilisation de supports optiques (CDs)

19.6.1. Introduction

Les CDs se différencient des disques conventionnels par de nombreuses caractéristiques. Au départ,

ils n'étaient pas inscriptible par l'utilisateur. Ils sont conçu pour être lut de façon continue sans délai pour déplacer la tête de lecture entre les pistes. Ils sont également plus facile à déplacer entre systèmes que les supports de même taille à cette époque.

Les CDs possèdent des pistes, mais cela fait référence à un ensemble de données qui peuvent être lues de façon continue et non pas à une particularité physique du disque. Pour produire un CD sous FreeBSD, il faut préparer les fichiers de données qui vont constituer les pistes sur le CD, puis écrire les pistes sur le CD.

Le système de fichiers ISO 9660 a été conçu pour gérer ces différences. Malheureusement il incorpore des limites du système de fichiers qui semblaient normale alors. Mais heureusement, il fournit un mécanisme d'extension qui permet au CDs proprement gravés de passer outre ces limites tout en restant lisibles par les systèmes qui ne supportent pas ces extensions.

Le logiciel sysutils/cdrtools comprend mkisofs(8), un programme que vous pouvez utiliser pour produire un fichier de données contenant un système de fichiers ISO 9660. Il dispose d'options pour le support de diverses extensions, et est décrit ci-dessous.

L'outil a utiliser pour graver un CD varie en fonction du type de graveur de CD: ATAPI ou autre. Les graveurs ATAPI utilisent le programme `burncd` qui fait partie du système de base. Les graveurs SCSI ou USB devraient utiliser l'utilitaire `cdrecord` du logiciel porté sysutils/cdrtools port. Il est également possible d'utiliser `cdrecord` et d'autres outils pour lecteurs SCSI sur du matériel ATAPI avec le module ATAPI/CAM.

Si vous voulez un programme de gravure de CD avec une interface graphique, vous devriez jeter un oeil à X-CD-Roast ou K3b. Ces outils sont disponibles sous une version pré-compilée ou à partir des logiciels portés sysutils/xcdroast et sysutils/k3b. X-CD-Roast et K3b nécessitent le module ATAPI/CAM avec des périphériques ATAPI.

19.6.2. mkisofs

L'utilitaire mkisofs(8), qui fait partie du logiciel porté sysutils/cdrtools, produit un système de fichiers ISO 9660 qui est une image de l'arborescence des répertoires dans un système de fichiers UNIX®. L'utilisation la plus simple est:

```
# mkisofs -o fichierimage.iso /chemin/vers/arborescence
```

Cette commande créera un *fichierimage.iso* contenant un système de fichiers ISO 9660 qui est une copie de l'arborescence */chemin/vers/arborescence*. Durant le processus de création, les noms de fichiers seront modifiés de façon à respecter les limitations de la norme ISO 9660, et rejettera les fichiers ayant des noms non acceptables pour un système de fichiers ISO.

De nombreuses options sont disponibles pour passer outre ces restrictions. En particulier, `-R` qui autorise les extensions Rock Ridge communes aux systèmes UNIX®, `-J` qui active les extensions Joliet utilisées par les systèmes Microsoft, et `-hfs` peut être utilisé pour créer des systèmes de fichiers HFS utilisés par Mac OS®.

Pour des CDs qui sont destinés à n'être utilisé que sur des systèmes FreeBSD, l'option `-U` peut être utilisée pour désactiver toutes les restrictions au niveau des noms de fichiers. Quand elle est

utilisée avec l'option `-R`, cela produit une image de système de fichiers qui est identique à l'arborescence FreeBSD d'origine, cependant ce système de fichiers pourra violer la norme ISO 9660 de nombreuses façon.

La dernière option d'usage général est l'option `-b`. Elle est utilisée pour indiquer l'emplacement de l'image de démarrage à utiliser dans la création d'un CD démarrable "El Torito". Cette option prend en argument le chemin vers une image de démarrage à partir de la racine de l'arborescence qui va être copiée sur le CD. Par défaut, mkisofs(8) créé une image ISO dans un mode appelé "émulation de disquette", et s'attend donc à une image de démarrage de 1200, 1440 ou 2880 Ko en taille. Certains chargeurs, comme celui utilisé par les disques d'installation de FreeBSD, n'utilisent pas ce mode d'émulation, dans ce cas l'option `-no-emul-boot` devrait être utilisée. Aussi, si /tmp/monboot contient un système FreeBSD avec une image de démarrage dans /tmp/monboot/boot/cdboot, vous pourrez produire l'image d'un système de fichiers ISO 9660 dans /tmp/bootable.iso de cette façon:

```
# mkisofs -R -no-emul-boot -b boot/cdboot -o /tmp/bootable.iso /tmp/monboot
```

Cela étant fait, si vous avez le pilote md configuré dans votre noyau, vous pouvez monter le système de fichiers avec:

```
# mdconfig -a -t vnode -f /tmp/bootable.iso -u 0
# mount -t cd9660 /dev/md0 /mnt
```

A ce moment vous pouvez vérifier que /mnt et /tmp/monboot sont identique.

Il existe de nombreuses autres options que vous pouvez utiliser avec mkisofs(8) pour régler finement son comportement. En particulier: les modifications d'une organisation ISO 9660 et la création de disques Joliet et HFS. Voir la page de manuel mkisofs(8) pour plus de détails.

19.6.3. burncd

Si vous disposez d'un graveur de CD ATAPI, vous pouvez utiliser la commande `burncd` pour graver une image ISO sur un CD. `burncd` fait partie du système de base, installé sous /usr/sbin/burncd. Son utilisation est très simple, car il dispose de peu d'options:

```
# burncd -f cddevice data fichierimage.iso fixate
```

Gravera une copie de *fichierimage.iso* sur *cddevice*. Le périphérique par défaut est /dev/acd0. Consultez burncd(8) pour les options pour fixer la vitesse d'écriture, éjecter le CD après gravure, et graver des données audios.

19.6.4. cdrecord

Si vous n'avez pas de graveur de CD ATAPI, vous devrez utiliser `cdrecord` pour graver vos CDs. `cdrecord` ne fait pas partie du système de base; vous devez l'installer soit à partir du logiciel porté sysutils/cdrtools ou de la version pré-compilée appropriée. Des modifications du système de base peuvent provoquer le dysfonctionnement des versions binaires de ce programme, et donner lieu à

une production de "dessous de bouteille". Vous devrez par conséquent soit mettre à jour le logiciel porté quand vous mettez à jour votre système, soit si vous suivez la branche -STABLE, mettre à jour le logiciel porté lorsqu'une nouvelle version est disponible.

Bien que `cdrecord` dispose de nombreuses options, l'usage de base est même plus simple qu'avec `burncd`. La gravure d'une image ISO 9660 se fait avec:

```
# cdrecord dev=device fichierimage.iso
```

La partie délicate dans l'utilisation de `cdrecord` est la recherche de la valeur à utiliser pour l'option `dev`. Pour déterminer le bon paramètre à utiliser, utilisez l'indicateur `-scanbus` de `cdrecord`, qui produira des résultats du type:

```
# cdrecord -scanbus
Cdrecord-Clone 2.01 (i386-unknown-freebsd7.0) Copyright (C) 1995-2004 Jörg Schilling
Using libscg version 'schily-0.1'
scsibus0:
        0,0,0     0) 'SEAGATE ' 'ST39236LW       ' '0004' Disk
        0,1,0     1) 'SEAGATE ' 'ST39173W        ' '5958' Disk
        0,2,0     2) *
        0,3,0     3) 'iomega  ' 'jaz 1GB         ' 'J.86' Removable Disk
        0,4,0     4) 'NEC     ' 'CD-ROM DRIVE:466' '1.26' Removable CD-ROM
        0,5,0     5) *
        0,6,0     6) *
        0,7,0     7) *
scsibus1:
        1,0,0   100) *
        1,1,0   101) *
        1,2,0   102) *
        1,3,0   103) *
        1,4,0   104) *
        1,5,0   105) 'YAMAHA  ' 'CRW4260        ' '1.0q' Removable CD-ROM
        1,6,0   106) 'ARTEC   ' 'AM12S          ' '1.06' Scanner
        1,7,0   107) *
```

Cela donne la valeur `dev` appropriée pour les périphériques listés. Recherchez votre graveur de CD dans la liste, et utilisez les trois chiffres séparés par une virgule comme valeur pour `dev`. Dans notre cas le périphérique de gravure est 1,5,0, donc l'entrée appropriée serait `dev=1,5,0`. Il existe des manières plus simple de spécifier cette valeur, consultez la page de manuel cdrecord(1) pour des détails. C'est également la documentation à consulter pour des informations sur la gravure de pistes audios, le contrôle de la vitesse, et d'autres choses.

19.6.5. Dupliquer des CDs Audio

Vous pouvez dupliquer un CD audio en effectuant l'extraction des données audio du CD vers un ensemble de fichiers, puis graver ces fichiers sur un CD vierge. Le processus est légèrement différent entre lecteurs ATAPI et SCSI.

Procedure: Lecteurs SCSI

1. Utiliser `cdda2wav` pour effectuer l'extraction audio.

```
% cdda2wav -v255 -D2,0 -B -Owav
```

2. Utiliser `cdrecord` pour graver les fichiers .wav.

```
% cdrecord -v dev=2,0 -dao -useinfo  *.wav
```

   Assurez-vous que *2,0* est choisi correctement, comme décrit dans cdrecord.

Procedure: Lecteurs ATAPI

1. Le pilote CD ATAPI rend disponible chaque piste sous la forme /dev/acddtnn, où *d* est le numéro de lecteur, et *nn* est le numéro de la piste écrit sur deux digits décimaux. Donc la première piste sur le premier lecteur est /dev/acd0t01, la seconde est /dev/acd0t02, la troisième /dev/acd0t03, et ainsi de suite.

   Assurez-vous que les fichiers appropriés existent sous /dev. Si ces entrées sont absentes, forcez le système à lire le disque à nouveau:

```
# dd if=/dev/acd0 of=/dev/null count=1
```

2. Extraire chaque piste en utilisant dd(1). Vous devez également préciser une taille de bloc durant l'extraction des fichiers.

```
# dd if=/dev/acd0t01 of=piste1.cdr bs=2352
# dd if=/dev/acd0t02 of=piste2.cdr bs=2352
...
```

3. Graver les fichiers récupérés en utilisant `burncd`. Vous devez spécifier que ce sont des fichiers audio, et que `burncd` devra fermer le disque une fois terminé.

```
# burncd -f /dev/acd0 audio piste1.cdr piste2.cdr ... fixate
```

19.6.6. Dupliquer des CDs de données

vous pouvez copier un CD de données vers un fichier image équivalent au fichier créé avec mkisofs(8), et vous pouvez l'utiliser pour dupliquer n'importe quel CD de données. L'exemple présenté ici suppose que votre lecteur de CDROM est les périphérique acd0. Remplacez-le avec le

périphérique correct.

```
# dd if=/dev/acd0 of=fichier.iso bs=2048
```

Vous disposez maintenant d'une image, vous pouvez la graver comme décrit plus haut.

19.6.7. Utiliser des CDs de données

Maintenant que vous avez créé une CDROM de données standard, vous voulez probablement le monter et lire les données présentes. Par défaut, mount(8) suppose que le système de fichier à monter est de type `UFS`. Si vous essayez quelque chose comme:

```
# mount /dev/cd0 /mnt
```

vous obtiendrez une erreur du type `Incorrect super block`, et pas de montage. Le CDROM n'est pas un système de fichiers de type `UFS`, aussi toute tentative de montage de ce type échouera. Vous devez juste préciser à mount(8) que le système de fichiers est du type `ISO9660`, et tout fonctionnera. Cela se fait en spécifiant l'option `-t cd9660` option à mount(8). Par exemple, si vous désirez monter un CDROM, contenu dans le lecteur /dev/cd0, sous /mnt, vous devrez exécuter:

```
# mount -t cd9660 /dev/cd0 /mnt
```

Notez que votre nom de lecteur (/dev/cd0 dans cet exemple) pourra être différent, en fonction de l'interface utilisée par votre lecteur de CDROM. De plus l'option `-t cd9660` ne fait qu'exécuter la commande mount_cd9660(8). L'exemple précédent pourrait être réduit à:

```
# mount_cd9660 /dev/cd0 /mnt
```

Vous pouvez généralement utiliser des CDROMs de données de n'importe quelle provenance de cette façon. Les disques avec certaines extensions ISO 9660 pourront se comporter de façon étrange, cependant. Par exemple, les disques Joliet conservent tous les noms de fichiers en utilisant des caractères Unicodes sur 2 octets. Le noyau FreeBSD ne comprend pas l'Unicode, mais le pilote CD9660 de FreeBSD est en mesure de convertir au vol les caractères Unicode. Si des caractères non-anglais apparaissent sous la forme de points d'interrogation, vous devrez préciser la table de caractères locale que vous utilisez avec l'option `-C`. Pour plus d'information, consultez la page de manuel mount_cd9660(8).

Pour pouvoir effectuer cette conversion de caractères à l'aide de l'option `-C`, le module cd9660_iconv.ko devra être chargé. Cela peut être fait soit en ajoutant au fichier loader.conf la ligne:

```
cd9660_iconv_load="YES"
```

> puis en redémarrant la machine, soit en chargeant directement le module avec kldload(8).

Occasionnellement, vous pourrez obtenir le message `Device not configured` (périphérique non configuré) lors d'une tentative de montage d'un CDROM. Cela veut généralement dire que le lecteur de CDROM pense qu'il n'y a pas de disque dans le lecteur, ou que le lecteur n'est pas visible sur le bus. Cela peut demander plusieurs secondes à un lecteur de CDROM de s'apercevoir qu'il a été chargé, soyez donc patient.

Parfois, un lecteur de CDROM SCSI peut être manquant parce qu'il n'a pas eu suffisamment de temps pour répondre à la réinitialisation du bus. Si vous avez un lecteur de CDROM SCSI, veuillez ajouter l'option suivante à la configuration de votre noyau et recompiler votre noyau.

```
options SCSI_DELAY=15000
```

Ceci demande à votre bus SCSI une pause de 15 seconds au démarrage, pour donner à votre lecteur de CDROM une chance de répondre la réinitialisation du bus.

19.6.8. Graver des CDs de données brutes

Il est possible de graver directement un fichier sur CD, sans créer de système de fichiers ISO 9660. Certaines personnes le font dans le cas de sauvegardes. Cela est beaucoup plus rapide que de graver un CD standard:

```
# burncd -f /dev/acd1 -s 12 data archive.tar.gz fixate
```

Afin de récupérer les données gravées sur un tel CD, vous devez lire les données à partir du fichier spécial de périphériques en mode caractère:

```
# tar xzvf /dev/acd1
```

Vous ne pouvez monter ce disque comme vous le feriez avec un CDROM classique. Un tel CDROM ne pourra être lu sous un autre système d'exploitation en dehors de FreeBSD. Si vous voulez être en mesure de monter le CD, ou d'en partager les données avec un autre système d'exploitation, vous devez utiliser mkisofs(8) comme décrit plus haut.

19.6.9. Utilisation du pilote de périphérique ATAPI/CAM

Ce pilote permet d'accéder aux périphériques ATAPI (lecteurs de CD-ROM, graveurs CD-RW, lecteur de DVD etc...) par l'intermédiaire du sous-système SCSI, et autorise l'utilisation d'applications comme sysutils/cdrdao ou cdrecord(1).

Pour utiliser ce pilote, vous devrez ajouter la ligne suivante au fichier /boot/loader.conf:

```
atapicam_load="YES"
```

puis redémarrez votre machine.

Si vous préférez compiler en statique dans le noyau le support atapicam(4), vous devrez ajouter au fichier de configuration du noyau la ligne:

```
device atapicam
```

Vous avez également besoin des lignes suivantes dans votre fichier de configuration:

```
device ata
device scbus
device cd
device pass
```

qui devraient être déjà présentes. Puis recompilez, installez votre nouveau noyau, et enfin redémarrez votre machine.

Lors du démarrage, votre graveur devrait apparaître, comme suit:

```
acd0: CD-RW <MATSHITA CD-RW/DVD-ROM UJDA740> at ata1-master PIO4
cd0 at ata1 bus 0 target 0 lun 0
cd0: <MATSHITA CDRW/DVD UJDA740 1.00> Removable CD-ROM SCSI-0 device
cd0: 16.000MB/s transfers
cd0: Attempt to query device size failed: NOT READY, Medium not present - tray closed
```

Le lecteur doit être accessible via le nom de périphérique /dev/cd0, par exemple pour monter un CD-ROM sous /mnt, tapez juste ce qui suit:

```
# mount -t cd9660 /dev/cd0 /mnt
```

En tant que `root`, vous pouvez exécuter la commande suivante pour obtenir l'adresse SCSI du graveur:

```
# camcontrol devlist
<MATSHITA CDRW/DVD UJDA740 1.00>   at scbus1 target 0 lun 0 (pass0,cd0)
```

Donc `1,0,0` sera l'adresse SCSI à utiliser avec cdrecord(1) et tout autre application SCSI.

Pour plus d'information concernant ATAPI/CAM et le système SCSI, consultez les pages de manuel atapicam(4) et cam(4).

19.7. Création et utilisation de supports optiques (DVDs)

19.7.1. Introduction

Comparé au CD, le DVD est la génération technologique suivante de support optique de stockage de données. Un DVD peut contenir plus de données qu'un CD et est de nos jour le standard pour la publication de vidéos.

Cinq formats physiques enregistrables peuvent être définis pour ce que nous appellerons un DVD enregistrable:

- DVD-R: Ce fut le premier format DVD enregistrable disponible. La norme DVD-R est définie par le Forum DVD. Ce format n'est pas réinscriptible.
- DVD-RW: C'est la version réinscriptible du standard DVD-R. Un DVD-RW peut supporter environ 1000 réécritures.
- DVD-RAM: C'est également un format réinscriptible supporté par le Forum DVD. Un DVD-RAM peut être vu comme un disque dur extractible. Cependant, ce support n'est pas compatible avec la plupart des lecteurs DVD-ROM et DVD-Vidéo; seuls quelques graveurs de DVDs supportent le DVD-RAM. Consultez la Utiliser un disque DVD-RAM pour plus d'information sur l'utilisation d'un DVD-RAM.
- DVD+RW: C'est un format réinscriptible défini par l' Alliance DVD+RW. Un DVD+RW supporte environ 1000 réécritures.
- DVD+R: Ce format est la version non-réinscriptible du format DVD+RW.

Un DVD enregistrable simple couche peut contenir jusqu'à 4 700 000 000 octets ce qui équivaut en fait à 4.38 Go ou 4485 Mo (1 kilo-octet représente 1024 octets).

Une différence doit être faite entre un support physique et son application. Par exemple un DVD-Vidéo est une organisation de fichiers particulière qui peut être écrite sur n'importe quel type de DVD enregistrable: DVD-R, DVD+R, DVD-RW etc. Avant de choisir le type de support, vous devez vous assurer que le graveur et le lecteur de DVD-Vidéo (lecteur de salon ou un lecteur de DVD-ROM sur un micro-ordinateur) sont compatibles avec le support.

19.7.2. Configuration

Le programme growisofs(1) sera utilisé pour effectuer la gravure des DVDs. Cette commande fait partie des utilitaires dvd+rw-tools (sysutils/dvd+rw-tools). Les outils dvd+rw-tools supportent l'ensemble des supports DVD.

Ces utilitaires utilisent le sous-système SCSI pour accéder aux périphériques, par conséquent le support ATAPI/CAM doit être ajouté à votre noyau. Si votre graveur utilise l'interface USB, cet ajout est inutile et vous devriez lire la Périphériques de stockage USB sur la configuration de périphériques USB.

Vous devez également activer l'accès aux périphériques ATAPI par DMA, cela peut être fait en ajoutant la ligne suivante au fichier /boot/loader.conf:

```
hw.ata.atapi_dma="1"
```

Avant de tenter d'utiliser les utilitaires dvd+rw-tools vous devriez consulter les notes de compatibilité matérielle des dvd+rw-tools pour des informations concernant votre graveur de DVDs.

Si vous désirez une interface graphique, vous devriez jeter un oeil à K3b (sysutils/k3b) qui offre une interface conviviale à growisofs(1) et à d'autres outils de gravure.

19.7.3. Graver des DVDs de données

La commande growisofs(1) est une interface à mkisofs, elle invoquera mkisofs(8) pour la création du système de fichiers et effectuera la gravure des données sur le DVD. Cela signifie que vous n'avez pas besoin de créer une image des données avant le processus de gravure.

Pour écrire les données du répertoire /path/to/data, utilisez la commande suivante:

```
# growisofs -dvd-compat -Z /dev/cd0 -J -R /path/to/data
```

Les options `-J -R` sont passées à mkisofs(8) pour la création du système de fichiers (dans le cas présent: un système de fichiers ISO 9660 avec les extensions Joliet et Rock Ridge), consultez la page de manuel de mkisofs(8) pour plus de détails.

L'option `-Z` est utilisée pour la session d'écriture initiale dans tous les cas: multi-sessions ou pas. Le périphérique correspondant au graveur, */dev/cd0*, doit être adapté en fonction de votre configuration. Le paramètre `-dvd-compat` provoquera la fermeture du disque, rien ne pourra être écrit à la suite de l'enregistrement. En retour cela devrait donner lieu à une plus grande compatibilité avec les lecteurs de DVD-ROMs.

Il est également possible de graver une image de système de fichiers, par exemple pour graver l'image *imagefile.iso*, nous lancerons:

```
# growisofs -dvd-compat -Z /dev/cd0=imagefile.iso
```

La vitesse d'écriture devrait être détectée et positionnée automatiquement en fonction du support et du graveur utilisé. Si vous voulez forcer la vitesse de gravure, utilisez le paramètre `-speed=`. Pour plus d'informations, lisez la page de manuel de growisofs(1).

19.7.4. Graver un DVD-Vidéo

Un DVD-Vidéo est un système de fichiers particulier basé sur les spécifications IS0 9660 et micro-UDF (M-UDF). Le DVD-Vidéo présente également une arborescence de données spécifique, c'est la

raison pour laquelle vous devez utiliser un programme particulier tel que multimedia/dvdauthor pour créer le DVD.

Si vous disposez déjà d'une image du système de fichiers du DVD-Vidéo, gravez-la de la même façon que pour une autre image, reportez-vous aux sections précédentes pour un exemple. Si vous avez réalisé vous-même l'arborescence du DVD et que le résultat est dans, par exemple, le répertoire /path/to/video, la commande suivante devrait être utilisée pour graver le DVD-Vidéo:

```
# growisofs -Z /dev/cd0 -dvd-video /path/to/video
```

L'option `-dvd-video` sera passée à mkisofs(8) et lui demandera de créer un système de fichiers de DVD-Vidéo. De plus, l'option `-dvd-video` implique l'option `-dvd-compat` de growisofs(1).

19.7.5. Utiliser un DVD+RW

Contrairement à un CD-RW, un DVD+RW vierge doit être formaté avant la première utilisation. Le programme growisofs(1) s'en chargera automatiquement quand cela sera nécessaire, ce qui est la méthode *recommandée*. Cependant vous pouvez utiliser la commande `dvd+rw-format` pour formater le DVD+RW:

```
# dvd+rw-format /dev/cd0
```

Vous devez effectuer cette opération qu'une seule fois, gardez à l'esprit que seuls des DVD+RW vierges doivent être formatés. Ensuite vous pouvez graver le DVD+RW de la manière vue dans les sections précédentes.

Si vous voulez graver de nouvelles données (graver un système de fichiers totalement nouveau et pas juste ajouter des données) sur un DVD+RW, vous n'avez pas besoin de l'effacer, vous avez juste à récrire sur l'enregistrement précédent (en effectuant une nouvelle session initiale), comme ceci:

```
# growisofs -Z /dev/cd0 -J -R /path/to/newdata
```

Le format DVD+RW offre la possibilité d'ajouter facilement des données à un enregistrement précédent. L'opération consiste à fusionner une nouvelle session avec la session existante, ceci n'est pas une gravure multisession, growisofs(1) *augmentera* le système de fichiers ISO 9660 présent sur le disque.

Par exemple, si nous voulons ajouter des données à notre DVD+RW précédent, nous devons utiliser cela:

```
# growisofs -M /dev/cd0 -J -R /path/to/nextdata
```

Les mêmes options de mkisofs(8) utilisées lors de la gravure de la session initiale doivent être à nouveau utilisées lors des écritures ultérieures.

Vous pouvez ajouter l'option `-dvd-compat` si vous désirez une meilleure compatibilité avec les lecteurs de DVD-ROM. Dans le cas d'un DVD+RW cela ne vous empêchera pas de rajouter des données par la suite.

Si pour une quelconque raison vous voulez vraiment effacer le disque, faites ce qui suit:

```
# growisofs -Z /dev/cd0=/dev/zero
```

19.7.6. Utiliser un DVD-RW

Un DVD-RW accepte deux formats de disque: le format séquentiel incrémental et le format "restricted overwrite". Par défaut les disques DVD-RW sont fournis sous le format séquentiel.

Un DVD-RW vierge peut être directement gravé sans le besoin d'une opération de formatage préalable, cependant un DVD-RW non-vierge au format séquentiel doit être effacé avant de pouvoir y écrire une nouvelle session initiale.

Pour effacer un DVD-RW en mode séquentiel, exécutez:

```
# dvd+rw-format -blank=full /dev/cd0
```

Une opération d'effacement complète (`-blank=full`) prendra environ une heure avec un support 1x. Un effacement rapide peut être effectué en utilisant l'option `-blank` si le DVD-RW est destiné à être enregistré suivant le mode d'écriture Disk-At-Once (DAO). Pour écrire le DVD-RW suivant le mode DAO, utilisez la commande:

```
# growisofs -use-the-force-luke=dao -Z /dev/cd0=imagefile.iso
```

L'option `-use-the-force-luke=dao` ne devrait pas être nécessaire puisque growisofs(1) tente de détecter les supports effacés rapidement et engage une écriture DAO.

En fait le mode "restricted overwrite" devrait être utilisé avec tout DVD-RW, ce format est plus flexible que le format séquentiel incrémental par défaut.

Pour écrire des données sur un DVD-RW en mode séquentiel, utilisez les mêmes instructions que pour tout autre format de DVD:

```
# growisofs -Z /dev/cd0 -J -R /path/to/data
```

Si vous voulez ajouter des données à votre enregistrement précédent, vous devrez utiliser la commande `-M` de growisofs(1). Cependant, si vous effectuez un ajout de données sur un DVD-RW en mode séquentiel, une nouvelle session sera créée sur le disque avec pour résultat de donner naissance à un disque multi-sessions.

Un DVD-RW dans le format "restricted overwrite" n'a pas besoin d'être effacé avant une nouvelle session initiale, vous avez juste à récrire sur le disque avec l'option `-Z`, ceci est similaire à un DVD+RW. Il est également possible d'augmenter un système de fichiers ISO 9660 existant écrit sur le disque de la même manière que pour un DVD+RW en utilisant l'option `-M`. Le résultat sera un DVD avec une seule session.

Pour faire passer un DVD-RW dans le format "restricted overwrite", la commande suivante doit être utilisée:

```
# dvd+rw-format /dev/cd0
```

Pour revenir au format séquentiel, utilisez:

```
# dvd+rw-format -blank=full /dev/cd0
```

19.7.7. Multi-sessions

Très peu de lecteurs de DVD-ROMs supportent les DVDs multi-sessions, ils ne liront, dans le meilleur des cas, que la première session. Les DVD+R, DVD-R et DVD-RW en mode séquentiel peuvent accepter de multiples sessions, la notion de multiples sessions n'existe pas pour les formats DVD+RW et DVD-RW en mode "restricted overwrite".

Utiliser la commande suivante après une session initiale (non fermée) sur un DVD+R, DVD-R, ou DVD-RW en mode séquentiel, ajoutera une nouvelle session sur le disque:

```
# growisofs -M /dev/cd0 -J -R /path/to/nextdata
```

L'utilisation de cette ligne de commande avec un DVD+RW ou un DVD-RW en mode "restricted overwrite" aura pour effet d'ajouter les données en fusionnant la nouvelle session avec celle déjà présente. Le résultat sera un disque mono-session. C'est la méthode utilisée pour ajouter des données sur ces médias après une écriture initiale.

De l'espace sur le médium est utilisé entre chaque session pour la fin et le début des sessions. Par conséquent, tout ajout de données devrait se faire suivant une quantité importante de données pour optimiser l'espace sur le disque. Le nombre de sessions est limité à 154 pour un DVD+R, environ 2000 pour un DVD-R, et 127 pour un DVD+R double couche.

19.7.8. Pour plus d'informations

Pour obtenir plus d'informations sur un DVD, la commande `dvd+rw-mediainfo /dev/cd0` peut être exécutée avec le disque dans le lecteur.

Plus d'informations sur les utilitaires dvd+rw-tools peuvent être trouvées dans la page de manuel de growisofs(1), sur le site Web de dvd+rw-tools et dans les archives de la liste de diffusion cdwrite.

La sortie de la commande `dvd+rw-mediainfo` sur le résultat de la gravure ou le disque posant problème est obligatoire avec tout rapport de problème. Sans cette sortie, il sera quasiment impossible de vous aider.

19.7.9. Utiliser un disque DVD-RAM

19.7.9.1. Configuration

Les graveurs de DVD-RAM sont fournis soit avec une interface SCSI soit une interface ATAPI. Dans le cas des périphériques ATAPI, l'accès DMA doit être activé, cela peut être fait en ajoutant la ligne suivante au fichier /boot/loader.conf:

```
hw.ata.atapi_dma="1"
```

19.7.9.2. Préparer le disque

Comme précisé dans l'introduction de cette section, un DVD-RAM peut être vu comme un disque dur extractible. Comme tout autre disque dur le DVD-RAM doit être "préparé" avant la première utilisation. Dans l'exemple, l'intégralité de l'espace sur le disque sera utilisé par un système de fichiers UFS2 standard:

```
# dd if=/dev/zero of=/dev/acd0 count=2
# bsdlabel -Bw acd0
# newfs /dev/acd0
```

Le périphérique DVD acd0 doit être modifié en fonction de la configuration.

19.7.9.3. Utiliser le disque

Une fois les opérations précédentes effectuées sur le DVD-RAM, il peut être monté comme un disque dur classique:

```
# mount /dev/acd0 /mnt
```

Après cela, on pourra lire et écrire sur le DVD-RAM.

19.8. Création et utilisation de disquettes

Sauvegarder des données sur disquette est parfois utile, par exemple quand on a pas d'autre support de stockage amovible de disponible ou quand on doit transférer de petites quantités de données sur un autre ordinateur.

Cette section expliquera comment utiliser des disquettes sous FreeBSD. Elle couvrira principalement le formatage et l'utilisation de disquettes DOS de 3.5pouces, mais les concepts exposés sont identiques pour d'autres formats de disquettes.

19.8.1. Formater des disquettes

19.8.1.1. Le périphérique

On accède aux disquettes par l'intermédiaire d'entrées dans /dev, comme pour tout autre périphérique. Pour accéder directement à la disquette, utilisez simplement /dev/fdN.

19.8.1.2. Le formatage

Une disquette doit subir un formatage bas niveau avant d'être utilisable. Il est généralement réalisé par le constructeur, mais le formatage est une bonne manière de contrôler l'intégrité du support. Bien qu'il soit possible de forcer une plus grande (ou plus petite) capacité, 1440Ko est celle pour laquelle sont conçues la plupart des disquettes.

Pour effectuer un formatage bas niveau d'une disquette vous devez utiliser fdformat(1). L'utilitaire attend le nom du périphérique en argument.

Notez tout message d'erreur, sachant que cela peut aider à déterminer si la disquette est bonne ou défectueuse.

19.8.1.2.1. Formatage des disquettes

Utilisez un des périphériques /dev/fdN.size, pour formater la disquette. Insérez une disquette 3.5pouces dans votre lecteur et tapez:

```
# /usr/sbin/fdformat -f 1440 /dev/fd0
```

19.8.2. Le label de disque

Après le formatage bas niveau du disque, vous devrez y placer un label de disque. Ce label sera détruit plus tard, mais il est nécessaire au système pour déterminer par la suite la taille et la géométrie du disque.

Le nouveau label de disque prendra l'intégralité du disque, et contiendra l'information correcte sur la géométrie de la disquette. Les différentes géométries possibles pour le label sont listées dans /etc/disktab.

Vous pouvez maintenant exécuter bsdlabel(8) de la façon suivante:

```
# /sbin/bsdlabel -B -w /dev/fd0 fd1440
```

19.8.3. Le système de fichiers

La disquette est maintenant fin prête pour un formatage haut niveau. Cette opération placera un nouveau système de fichiers sur la disquette, qui permettra à FreeBSD d'écrire et de lire sur le disque. Après la création du nouveau système de fichiers, le label disque est détruit, aussi si vous désirez reformater le disque, vous devrez recréer le label de disque à nouveau.

Le système de fichiers de la disquette peut soit être de l'UFS soit utiliser le système FAT. Le système FAT est généralement un meilleur choix pour les disquettes.

Pour placer un nouveau système de fichier sur la disquette faites ceci:

```
# /sbin/newfs_msdos /dev/fd0
```

La disquette est maintenant prête à être utilisée.

19.8.4. Utilisation de la disquette

Pour utiliser la disquette, montez-la avec mount_msdosfs(8). On peut également utiliser emulators/mtools du catalogue des logiciels portés.

19.9. Créer et utiliser les bandes magnétiques

Les principaux types de bandes sont les 4mm, 8mm, QIC, les mini-cartouches et les DLTs.

19.9.1. Bandes 4mm (DDS: "Digital Data Storage")

Les bandes 4mm sont en train de remplacer les bandes QIC comme le format usuel de sauvegarde pour les stations de travail. Cette tendance s'est accélérée quand Conner a racheté Archive, un des leaders de la fabrication des lecteurs QIC, et a arrêté la production de ces derniers. Les lecteurs 4mm sont petits et silencieux mais n'ont pas la réputation de fiabilité des lecteurs 8mm. Les cartouches sont moins coûteuse et plus petites (3 x 2 x 0.5 pouces, 76 x 51 x 12 mm) que les cartouches 8mm. Les cartouches 4mm, tout comme les 8mm, ont une durée de vie faible car elles utilisent un procédé de lecture/écriture en hélice.

Le débit de ces lecteurs va de ~150 Ko/s à ~500 Ko/s au maximum. Leur capacité de varie de 1.3 Go à 2.0 Go. La compression matérielle, disponible sur la plupart des lecteurs, double approximativement leur capacité. Les unités multi-lecteurs peuvent avoir jusqu'à 6 lecteurs dans une seule tour avec changement automatique de bande. La capacité totale atteint 240 Go.

Le standard DDS-3 supporte maintenant des capacités de bande jusqu'à 12 Go (ou 24 Go compressés).

Les lecteurs 4mm, comme les lecteurs 8mm, utilisent un procédé de lecture/écriture en hélice. Tous les avantages et les inconvénients de ce procédé s'appliquent aux deux types de lecteurs.

Les bandes doivent être changées après 2000 utilisations ou 100 sauvegardes complètes.

19.9.2. Bandes 8mm (Exabyte)

Les unités de bandes 8mm sont les lecteurs de bandes SCSI les plus courant; c'est le meilleur choix de bandes amovibles. Presque chaque site dispose d'une unité Exabyte 2 Go 8mm. Les lecteurs 8mm sont fiables, pratiques et silencieux. Les cartouches sont bon marché et d'encombrement faible (4.8 x 3.3 x 0.6 pouces; 122 x 84 x 15 mm). Un des inconvénients de la bande 8mm est la durée de vie relativement courte des bandes et des têtes de lectures en raison de la grande vitesse de défilement

de la bande devant les têtes.

Leur débit va de ~250 Ko/s à ~500 Ko/s. Leur capacité commence à 300 Mo jusqu'à 7 Go. La compression matérielle, disponible sur la plupart des lecteurs, double approximativement la capacité. Ces lecteurs sont disponibles sous forme d'unité simple ou multiple accueillant 6 lecteurs et 120 bandes. Les bandes sont changées automatiquement par l'unité. Ils peuvent gérer une capacité de stockage de plus de 840 Go.

Le lecteur Exabyte "Mammoth" supporte 12 Go sur une seule bande (24 Go compressé) et coûte approximativement le double d'un lecteur classique.

L'enregistrement des données sur la bande utilise un procédé en hélice, les têtes sont positionnées en biais par rapport à la bande (environ 6 degrés). La bande fait un angle de 270 degrés avec le cylindre sur lequel se trouvent les têtes. Ce cylindre tourne en même temps que la bande défile. Il en résulte donc une grande densité de données et des pistes très serrées qui vont de biais d'un bord à l'autre de la bande.

19.9.3. QIC

Les bandes et les lecteurs QIC-150 sont, peut-être, le format le plus courant. Les lecteurs QIC sont les moins chers des supports de sauvegarde "sérieux". Leur inconvénient par contre est le coût des bandes. Les bandes QIC sont chères comparées aux bandes 8mm ou 4mm, jusqu'à 5 fois le coût au Go. Mais, si une demi-douzaine de bandes vous suffit, le format QIC peut être le bon choix. QIC est le format le *plus* répandu. Chaque site dispose d'un lecteur QIC d'une densité ou d'une autre. C'est là la difficulté, il existe de nombreuses densités pour des bandes physiquement semblables (parfois même identiques). Les lecteurs QIC ne sont pas silencieux. Ces lecteurs se positionnent bruyamment avant d'enregistrer des données et ont les entend clairement lors de lecture, écriture ou recherche. Les bandes QIC sont volumineuses: 6 x 4 x 0.7 pouces (152 x 102 x 17 mm).

Leur débit va de ~150 Ko/s à ~500 Ko/s. Leur capacité varie de 40 Mo à 15 Go. La compression matérielle est disponible sur de nombreux lecteurs récents. Les lecteurs QIC sont de moins en moins utilisés, ils sont supplantés par les lecteurs DAT.

Les données sont enregistrées sur des pistes sur la bande. Les pistes sont parallèles à la bande et vont d'une extrémité à l'autre. Le nombre de piste, et par conséquent la largeur des pistes, varie avec la capacité de la bande. La plupart des nouveaux lecteurs fournissent au moins une compatibilité descendante en lecture (mais aussi en écriture). Le format QIC a une bonne réputation de sécurité des données (la mécanique est plus simple et plus robuste que les lecteurs à système en hélice).

Les bandes devraient être changée après 5000 sauvegardes.

19.9.4. DLT

Les DLT ont le taux de transfert le plus élevé de tous les types de lecteurs décrits ici. La bande d'1/2" (12.5mm) est contenue dans une seule cartouche (4 x 4 x 1 pouces; 100 x 100 x 25 mm). La cartouche est munie d'une trappe basculante le long d'un côté de la cartouche. Le lecteur ouvre cette trappe pour saisir l'amorce de la bande. Cette amorce comporte une découpe ovale que le lecteur utilise pour "crocheter" la bande. La bobine d'entraînement est située dans le lecteur. Tous

les autres types de cartouches décrits ici (les bandes 9 pistes sont la seule exception) ont les bobines de stockage et d'entraînement dans la cartouche elle-même.

Leur débit est d'environ 1.5 Mo/s, trois fois celui des lecteurs 4mm, 8mm, ou QIC. La capacité d'une bande varie de 10 Go à 20 Go pour une unité simple. Les lecteurs sont disponibles en unités multi-bandes avec changeurs et multi-lecteurs contenant de 5 à 900 bandes et 1 à 20 lecteurs, fournissant une capacité de stockage allant de 50 Go à 9 TO.

Avec la compression, le format DLT type IV supporte jusqu'à une capacité de 70 Go.

Les données sont enregistrées sur la bande sur des pistes parallèles à la direction de défilement (comme pour les bandes QIC). Deux pistes sont écrites à la fois. La durée de vie des têtes de lecture/écriture est relativement longue; une fois que la bande s'arrête, il n'y a pas de déplacement des têtes par rapport à la bande.

19.9.5. AIT

AIT est le nouveau format de Sony, il peut supporter jusqu'à 50 Go par bande (avec compression). Les bandes contiennent un circuit mémoire qui contient un index du contenu de la bande. Cet index peut être lu rapidement par le lecteur pour déterminer l'emplacement de fichiers sur la bande, au lieu des nombreuses minutes nécessaires aux autres types de bande. Des programmes comme SAMS:Alexandria peuvent contrôler quarante ou plus ensemble de bandes AIT, communiquant directement avec le circuit mémoire de la bande pour en afficher le contenu à l'écran, déterminer quels fichiers ont été sauvegardé sur quelle bande, localiser la bonne bande, la charger, et en restaurer les données.

Les ensembles de ce type reviennent aux alentour des 20000 dollars, les rendant inaccessibles à l'amateur éclairé.

19.9.6. Utiliser une bande neuve pour la première fois

La première fois que vous essayez de lire ou d'écrire sur une bande vierge, l'opération échoue. Les messages affichés par la console devraient être du type:

```
sa0(ncr1:4:0): NOT READY asc:4,1
sa0(ncr1:4:0):  Logical unit is in process of becoming ready
```

La bande ne contient pas de bloc d'identification (bloc numéro 0). Tous les lecteurs QIC depuis l'adoption du standard QIC-525 écrivent un bloc d'identification sur la bande. Il y a alors deux solutions:

- `mt fsf 1` fait écrire au lecteur un bloc d'identification sur la bande.
- Utiliser le bouton en face avant pour éjecter la bande.

  Ré-insérer la bande et utiliser dump(8) pour écrire dessus.

  dump(8) produira l'erreur `DUMP: End of tape detected` et la console affichera: `HARDWARE FAILURE info:280 asc:80,96`.

Rembobiner la bande avec: `mt rewind`.

Les manipulations ultérieures sur la bande fonctionneront.

19.10. Sauvegardes sur disquettes

19.10.1. Puis-je utiliser des disquettes pour la sauvegarde des mes données?

Les disquettes ne sont pas des supports adaptés à la réalisation de sauvegardes étant donné que:

- Le support n'est pas fiable, spécialement sur de longues périodes de temps.
- Les opérations de sauvegarde et de restauration sont très lentes.
- Elles ont une capacité très limitée (le jour où l'on pourra sauvegarder l'intégralité d'un disque dur sur une douzaine de disquette n'est pas encore arrivé).

Cependant, si vous n'avez pas d'autres méthodes pour sauvegarder vos données alors les disquettes sont mieux que pas de sauvegardes du tout.

Si vous devez utiliser les disquettes, alors assurez-vous que vous en utiliser des disquettes de bonne qualité. Les disquettes qui traînent sur le bureau depuis quelques années sont un mauvais choix. Idéalement utilisez de des disquettes neuves en provenance d'un fabricant renommé.

19.10.2. Alors, comment je sauvegarde mes données sur disquettes?

La meilleur façon de sauvegarder sur disquette est d'utiliser la commande tar(1) avec l'option `-M` (volume multiple), qui autorise la répartition des sauvegardes sur plusieurs disquettes.

Pour sauvegarder tous les fichiers du répertoire courant et des sous-répertoires (en tant que `root`):

```
# tar Mcvf /dev/fd0 *
```

Quand la première disquette est pleine tar(1) vous réclamera d'introduire le volume suivant (parce que tar(1) est indépendant du support il parle en terme de volume; dans notre contexte cela signifie disquette).

```
Prepare volume 2 for /dev/fd0 and hit return:
```

Cette opération est répétée (avec incrémentation du numéro de volume) jusqu'à ce que les fichiers spécifiés soient sauvegardés.

19.10.3. Puis-je sauvegarder mes sauvegardes?

Malheureusement, tar(1) ne permettra pas l'utilisation de l'option `-z` pour les archives multi-volumes. Vous pourrez, bien sûr, utiliser gzip(1) sur tous les fichiers, les archiver avec tar(1) sur disquettes, puis décompresser les fichiers avec gunzip(1)!

19.10.4. Comment puis-je restaurer mes sauvegardes?

Pour restaurer une archive complète utiliser:

```
# tar Mxvf /dev/fd0
```

Vous pouvez utiliser deux manières pour restaurer uniquement certains fichiers. Tout d'abord, vous pouvez commencer avec la première disquette et utiliser:

```
# tar Mxvf /dev/fd0 nomdufichier
```

tar(1) vous demandera d'insérer les disquettes suivantes jusqu'à trouver le fichier recherché.

Alternativement, si vous savez sur quelle disquette le fichier se trouve alors vous pouvez simplement insérer cette disquette et utiliser la commande précédente. Notez que si le premier fichier sur la disquette est la suite d'un fichier de la précédente disquette alors tar(1) vous avertira qu'il ne peut le restaurer, même si vous ne le voulez pas!

19.11. Stratégies de sauvegarde

La première chose a faire lors de la mise en place d'un plan de sauvegarde est de s'assurer que l'ensemble des problèmes suivants sera couvert:

- Panne d'un disque
- Suppression accidentelle de fichiers
- Corruption aléatoire de fichiers
- Destruction complète de la machine (par exemple suite à un incendie), avec destruction des sauvegardes stockées sur le même site.

Il est parfaitement possible que certains systèmes utilisent une technique différente pour chacun des problèmes évoqués ci-dessus. En dehors des systèmes personnels avec des données peu importantes, il est peu probable qu'une seule technique puisse répondre à l'ensemble de ces risques.

Quelques-unes des techniques à notre disposition sont:

- Des archives de tout le système, sauvegardées sur un support fiable et à l'extérieur du site. C'est une protection réelle contre tous les problèmes précédemment cités, mais cette méthode est lente et peu pratique lors des restaurations. Vous pouvez conserver des copies de ces sauvegardes sur site et/ou en ligne, mais il y aura toujours des difficultés lors de la restauration des fichiers, en particulier pour les utilisateurs sans droits.
- Instantané de systèmes de fichiers. Cet outil n'est vraiment utile que dans le cas d'une suppression accidentelle de fichiers, mais il l'est *vraiment* dans ce cas; de plus cette méthode est rapide et simple à employer.
- Copies de l'intégralité des systèmes de fichiers et/ou des disques (par une utilisation régulière de

rsync(1) sur l'intégralité de la machine par exemple). C'est le procédé en général le plus utile dans le cas des réseaux avec des besoins spécifiques. Dans le cas d'une protection contre les pannes disques, cette méthode est normalement inférieure à un système RAID. Pour la restauration de fichiers supprimés accidentellement, c'est comparable aux instantanés UFS, c'est plus une question de préférence.

- RAID. Réduit ou évite les périodes où le système est inutilisable quand un disque tombe en panne. Avec l'inconvénient d'avoir à faire face à des pannes disques plus fréquentes (parce que vous utilisez plus de disques), mais avec cependant une moindre urgence.
- Le contrôle des empreintes de fichiers. L'utilitaire mtree(8) est très utile dans ce cas. Bien que cela ne soit pas une technique de sauvegarde des données, ce contrôle aidera à garantir que vous serez averti quand vous devrez ressortir vos sauvegardes. C'est tout particulièrement important dans le cas de sauvegardes hors site, et ces empreintes devraient être vérifiées régulièrement.

Il est relativement simple de trouver d'autres solutions, nombreuses sont celles qui sont des variations des techniques présentées ci-dessus. Des besoins spécifiques conduiront généralement à des solutions spécifiques (par exemple sauvegarder une base de données durant son utilisation demande une étape intermédiaire spécifique au logiciel de base de données). L'important est de connaître les dangers contre lesquels vous désirez vous protéger, et comment vous ferez face à chacun d'entre eux.

19.12. Sauvegardes

Les trois principaux programmes de sauvegarde sont: dump(8), tar(1), et cpio(1).

19.12.1. Dump et Restore

dump(8) et restore(8) sont les programmes de sauvegarde traditionnels d'UNIX®. Ils opèrent sur le disque comme sur une suite de blocs disque, en dessous du niveau d'abstraction que constituent les fichiers, liens et répertoires créés par les systèmes de fichiers. Le programme dump(8) sauvegarde l'intégralité d'un système de fichiers d'un périphérique. Il est incapable de sauvegarder seulement une partie d'un système de fichiers ou une arborescence de répertoires s'étalant sur plus d'un système de fichiers. Le programme dump(8) n'écrit pas de fichiers ou des répertoires sur la bande, mais écrit plutôt les blocs de données brutes dont sont constitués les fichiers et les répertoires.

Si vous utilisez dump(8) sur votre répertoire racine, vous ne sauvegarderez pas /home, /usr ou beaucoup d'autres répertoires puisque que ces derniers sont généralement des points de montages pour d'autres systèmes de fichiers ou des liens symboliques vers ces systèmes de fichiers.

L'utilitaire dump(8) a quelques particularités datant de ses débuts sous la version 6 d'ATT UNIX (circa 1975). Les paramètres par défaut conviennent aux bandes 9 pistes (6250 bpi), et non aux supports à haute densité d'aujourd'hui (jusqu'à 62182 ftpi). Il faut surcharger ces valeurs par défaut sur la ligne de commande pour utiliser la capacité des bandes actuelles.

Il est également possible de sauvegarder les données par l'intermédiaire d'un réseau sur un lecteur de bande se trouvant sur une autre ordinateur à l'aide des commandes `rdump` et `rrestore`. Ces deux

programmes utilisent rcmd(3) et ruserok(3) pour accéder à l'unité de bandes distante. Cependant, l'utilisateur effectuant une sauvegarde doit être présent dans le fichier .rhosts sur la machine distante. Les arguments de rdump(8) et rrestore(8) doivent être compatibles avec une utilisation sur la machine distante. Quand on sauvegarde une machine FreeBSD sur un lecteur Exabyte installé sur un ordinateur Sun appelé komodo, utilisez:

```
# /sbin/rdump 0dsbfu 54000 13000 126 komodo:/dev/nsa8 /dev/da0a 2>&1
```

Attention: il y a des conséquences pour la sécurité à utiliser l'authentification .rhosts. Evaluez soigneusement votre situation.

Il est également possible d'utiliser dump(8) et restore(8) d'une façon plus sécurisée sur ssh(1).

Exemple 29. Utiliser dump(8) sur ssh

```
# /sbin/dump -0uan -f - /usr | gzip -2 | ssh -c blowfish \
          targetuser@targetmachine.example.com dd of=/mybigfiles/dump-usr-l0.gz
```

Ou en utilisant une fonction interne de dump, positionner la variable d'environnement RSH:

Exemple 30. Utiliser dump sur ssh avec la variable RSH positionnée

```
# RSH=/usr/bin/ssh /sbin/dump -0uan -f
targetuser@targetmachine.example.com:/dev/sa0 /usr
```

19.12.2. tar

Le programme tar(1) date aussi de la Version 6 d'ATT UNIX (circa 1975). tar(1) travaille en coopération avec le système de fichiers; il permet d'écrire des fichiers et des répertoires sur bandes. tar(1) ne supporte pas toutes les options permises par cpio(1), mais ne demande pas l'inhabituelle concaténation de commandes qu'utilise cpio(1)

Sous FreeBSD 5.3 et versions suivantes, GNU tar et la version par défaut bsdtar sont disponibles. La version GNU peut être invoquée avec la commande gtar. Elle supporte les sauvegardes sur des périphériques distants et cela avec la même syntaxe que rdump(8). Pour sauvegarder avec tar(1) sur une unité Exabyte connectée sur une machine Sun appelée komodo, utilisez:

```
# /usr/bin/gtar cf komodo:/dev/nsa8 . 2>&1
```

La même opération peut être effectuée avec bsdtar en utilisant un tuyau et rsh(1) pour envoyer les données sur un lecteur de bande distant:

```
# tar cf - . | rsh hostname dd of=tape-device obs=20b
```

Si vous êtes inquiet au sujet de la sécurité de sauvegardes par réseau, vous devriez utiliser la commande ssh(1) à la place de rsh(1).

19.12.3. cpio

cpio(1) est le programme UNIX® original pour l'échange de fichiers par bandes magnétiques. cpio(1) dispose d'options (parmi beaucoup d'autres) pour intervertir les octets, utiliser de nombreux différents formats, et envoyer les données à d'autres programmes. Cette dernière caractéristique fait de cpio(1) un excellent choix pour les supports d'installation. cpio(1) ne sait pas parcourir une arborescence de répertoires et il faut lui passer la liste des fichiers via stdin.

cpio(1) ne supporte pas les sauvegardes par le réseau. Vous pouvez utiliser un tuyau et rsh(1) pour envoyer les données sur un lecteur de bande distant:

```
# for f in directory_list; do
find $f >> backup.list
done
# cpio -v -o --format=newc < backup.list | ssh user@host "cat > backup_device"
```

Où *directory_list* est la liste des répertoires que vous désirez sauvegarder, *user@host* est l'ensemble utilisateur/nom de machine qui effectuera les sauvegardes, et *backup_device* représente l'unité où seront écrites les sauvegardes (e.g., /dev/nsa0).

19.12.4. pax

pax(1) est la réponse IEEE/POSIX® à tar(1) et cpio(1). Au fil des ans les différentes versions de tar(1) et cpio(1) sont devenues légèrement incompatibles. Aussi, plutôt que de batailler pour les standardiser entièrement, POSIX® a défini un nouvel utilitaire d'archivage. pax(1) tente de lire et d'écrire nombre des divers formats tar(1) et cpio(1), en plus de ses propres nouveaux formats. Son ensemble de commandes ressemble plus à celui de cpio(1) qu'à celui de tar(1).

19.12.5. Amanda

Amanda (Advanced Maryland Network Disk Archiver-Système Avancé d'Archivage de Disques en Réseau du Maryland) est un système d'archivage client/serveur plutôt qu'un simple programme. Un serveur Amanda archivera sur une seule unité de bandes un nombre quelconque d'ordinateurs disposant de clients Amanda et un accès réseau au serveur Amanda. Un problème classique sur les sites qui ont de nombreux disques volumineux est que le temps nécessaire pour sauvegarder directement les données sur la bande dépasse le temps alloué à cette tâche. Amanda résout ce problème. Amanda peut utiliser un "disque intermédiaire" pour sauvegarder plusieurs systèmes de fichiers à la fois. Amanda des "jeux d'archive": un ensemble de bandes utilisé pour une période donnée pour créer une sauvegarde complète de tous les systèmes de fichiers listé dans le fichier de configuration d'Amanda. Le "jeu d'archive" contient également les sauvegardes nocturnes incrémentales (ou différentielles) de tous les systèmes de fichiers. Pour restaurer une système de

fichiers endommagé, il faut la sauvegarde complète la plus récente et les sauvegardes incrémentales.

Le fichier de configuration permet un contrôle en finesse des sauvegardes et du trafic réseau qu'Amanda génère. Amanda utilisera n'importe quel des programmes de sauvegarde décrits plus haut pour écrire les données sur bande. Amanda est disponible sous forme de logiciel porté ou de logiciel pré-compilé, il n'est pas installé par défaut.

19.12.6. Ne rien faire

"Ne rien faire" n'est pas un logiciel, mais c'est la stratégie de sauvegarde la plus utilisée. Il n'y a aucun investissement initial. Il n'y a pas de de planification des sauvegardes à suivre. Juste dire non. Si quelque chose arrive à vos données, souriez et débrouillez-vous!

Si votre temps et vos données ne valent pas grand chose, alors "Ne rien faire" est le programme de sauvegarde le mieux adapté à votre ordinateur. Mais prenez garde, UNIX® est un outil utile, et vous pouvez vous rendre compte au bout de six mois que vous disposez d'une collection de fichiers qui vous sont utiles.

"Ne rien faire" est la bonne méthode de sauvegarde pour /usr/obj et les autres répertoires qui peuvent facilement être recréés par votre ordinateur. Un exemple est les fichiers qui constituent la version HTML ou PostScript® de ce manuel. Ces fichiers ont été générés à partir de fichiers SGML. Faire des sauvegardes des fichiers HTML ou PostScript® n'est pas nécessaire. Les fichiers source SGML sont sauvegardés régulièrement.

19.12.7. Quel est le meilleur programme de sauvegarde?

dump(8) *Point.* Elizabeth D. Zwicky a soumis à rude épreuve tous les programmes de sauvegarde dont nous avons parlé. Le choix de dump(8) s'impose pour préserver toutes vos données et les particularités des systèmes de fichiers UNIX®. Elizabeth a créé des systèmes de fichiers avec une grande variété de particularités inhabituelles (et quelques unes pas tellement inhabituelles) et a testé chacun des programmes en faisant une sauvegarde et une restauration de ces systèmes de fichiers. Parmi les spécificités testées: fichiers avec des trous, fichiers avec des trous et des blocs de caractères "null", fichiers dont les noms comportent des caractères inhabituels, les fichiers illisibles ou impossible à modifier, les périphériques, fichiers dont la taille change pendant la sauvegarde, fichiers créés ou détruits en cours de sauvegarde et bien plus. Elle a présenté les résultats de ces tests au LISA V en Octobre 1991. Voir les tests d'endurance des programmes de sauvegarde et d'archivage.

19.12.8. Procédure de restauration d'urgence

19.12.8.1. Avant le désastre

Il y a quatre étapes à mettre en oeuvre en prévision d'un désastre éventuel.

Tout d'abord, imprimez le label de chacun de vos disques (par exemple `bsdlabel da0 | lpr`), votre table des systèmes de fichiers (/etc/fstab) et tous les messages de démarrage, en deux exemplaires.

Deuxièmement, vérifiez que vos disquettes de démarrage et de reprise d'urgence (boot.flp et

fixit.flp) incluent tous vos périphériques. La méthode la plus simple pour vérifier est de redémarrer avec la disquette de démarrage dans le lecteur et contrôler les messages de démarrage. Si tous vos périphériques sont listés et opérationnels, passez à la troisième étape.

Sinon, vous devez créer deux disquettes de démarrage sur-mesure avec un noyau qui puisse monter tous vos disques et accéder à votre unité de bandes. Ces disquettes doivent contenir: fdisk(8), bsdlabel(8), newfs(8), mount(8), et le programme de sauvegarde que vous utilisez. L'édition de liens de ces programmes doit être statique. Si vous utilisez dump(8), la disquette doit contenir restore(8).

Troisièmement, faites régulièrement des sauvegardes sur bandes. Toutes les modifications effectuées après votre dernière sauvegarde peuvent irrémédiablement perdues. Protégez vos bandes de sauvegarde en écriture.

Quatrièmement, testez les disquettes (soit boot.flp et fixit.flp soit les deux disquettes sur-mesure que vous avez créées à la seconde étape) et vos bandes de sauvegarde. Prenez note de la procédure. Conservez ces notes avec la disquette de démarrage, les impressions et les bandes de sauvegarde. Vous serez si préoccupé quand vous devrez restaurer que ces notes peuvent vous éviter de détruire vos bandes de sauvegarde (Comment? Au lieu de `tar xvf /dev/sa0`, vous pourriez taper accidentellement `tar cvf /dev/sa0`, ce qui écraserait votre bande de sauvegarde).

Par mesure de sécurité, créez une disquette de démarrage et deux bandes de sauvegarde à chaque fois. Conservez-les dans un lieu éloigné. Un endroit éloigné n'est PAS le sous-sol du même bâtiment. Un certain nombre de compagnies du World Trade Center l'ont appris à leurs dépends. Un endroit éloigné doit être physiquement séparé de vos ordinateurs et de vos disques par une distance significative.

Exemple 31. Procédure de création d'une disquette de démarrage

```
#!/bin/sh
#
# create a restore floppy
#
# format the floppy
#
PATH=/bin:/sbin:/usr/sbin:/usr/bin

fdformat -q fd0
if [ $? -ne 0 ]
then
     echo "Bad floppy, please use a new one"
     exit 1
fi

# place boot blocks on the floppy
#
bsdlabel -w -B /dev/fd0c fd1440

#
# newfs the one and only partition
```

```
#
newfs -t 2 -u 18 -l 1 -c 40 -i 5120 -m 5 -o space /dev/fd0a

#
# mount the new floppy
#
mount /dev/fd0a /mnt

#
# create required directories
#
mkdir /mnt/dev
mkdir /mnt/bin
mkdir /mnt/sbin
mkdir /mnt/etc
mkdir /mnt/root
mkdir /mnt/mnt          # for the root partition
mkdir /mnt/tmp
mkdir /mnt/var

#
# populate the directories
#
if [ ! -x /sys/compile/MINI/kernel ]
then
     cat &lt;&lt; EOM
The MINI kernel does not exist, please create one.
Here is an example config file:
#
# MINI - A kernel to get FreeBSD onto a disk.
#
machine         "i386"
cpu             "I486_CPU"
ident           MINI
maxusers        5

options         INET                    # needed for _tcp _icmpstat _ipstat
                                        #            _udpstat _tcpstat _udb
options         FFS                     #Berkeley Fast File System
options         FAT_CURSOR              #block cursor in syscons or pccons
options         SCSI_DELAY=15           #Be pessimistic about Joe SCSI device
options         NCONS=2                 #1 virtual consoles
options         USERCONFIG              #Allow user configuration with -c XXX

config          kernel  root on da0 swap on da0 and da1 dumps on da0

device          isa0
device          pci0

device          fdc0    at isa? port "IO_FD1" bio irq 6 drq 2 vector fdintr
device          fd0 at fdc0 drive 0
```

```
device          ncr0

device          scbus0

device          sc0 at isa? port "IO_KBD" tty irq 1 vector scintr
device          npx0    at isa? port "IO_NPX" irq 13 vector npxintr

device          da0
device          da1
device          da2

device          sa0

pseudo-device   loop            # required by INET
pseudo-device   gzip            # Exec gzipped a.out's
EOM
     exit 1
fi

cp -f /sys/compile/MINI/kernel /mnt

gzip -c -best /sbin/init > /mnt/sbin/init
gzip -c -best /sbin/fsck > /mnt/sbin/fsck
gzip -c -best /sbin/mount > /mnt/sbin/mount
gzip -c -best /sbin/halt > /mnt/sbin/halt
gzip -c -best /sbin/restore > /mnt/sbin/restore

gzip -c -best /bin/sh > /mnt/bin/sh
gzip -c -best /bin/sync > /mnt/bin/sync

cp /root/.profile /mnt/root

cp -f /dev/MAKEDEV /mnt/dev
chmod 755 /mnt/dev/MAKEDEV

chmod 500 /mnt/sbin/init
chmod 555 /mnt/sbin/fsck /mnt/sbin/mount /mnt/sbin/halt
chmod 555 /mnt/bin/sh /mnt/bin/sync
chmod 6555 /mnt/sbin/restore

#
# create the devices nodes
#
cd /mnt/dev
./MAKEDEV std
./MAKEDEV da0
./MAKEDEV da1
./MAKEDEV da2
./MAKEDEV sa0
./MAKEDEV pty0
```

```
cd /

#
# create minimum file system table
#
cat &lt; /mnt/etc/fstab &lt;&lt;EOM
/dev/fd0a    /    ufs    rw  1  1
EOM

#
# create minimum passwd file
#
cat &lt; /mnt/etc/passwd &lt;&lt;EOM
root:*:0:0:Charlie &amp;:/root:/bin/sh
EOM

cat &lt; /mnt/etc/master.passwd &lt;&lt;EOM
root::0:0::0:0:Charlie &amp;:/root:/bin/sh
EOM

chmod 600 /mnt/etc/master.passwd
chmod 644 /mnt/etc/passwd
/usr/sbin/pwd_mkdb -d/mnt/etc /mnt/etc/master.passwd

#
# umount the floppy and inform the user
#
/sbin/umount /mnt
echo "The floppy has been unmounted and is now ready."
```

19.12.8.2. Après le désastre

La question cruciale est: votre matériel a-t-il survécu? Vous avez régulièrement fait des sauvegardes, vous n'avez donc pas besoin de vous inquiéter pour les fichiers et les programmes.

Si le matériel a subi des dégâts, remplacez tout d'abord ce qui a été endommagé avant de tenter d'utiliser l'ordinateur.

Si votre matériel est en état, contrôlez vos disquettes. Si vous utilisez une disquette de démarrage personnalisée, démarrez en mode mono-utilisateur (tapez `-s` à l'invite `boot:`). Sautez le paragraphe suivant.

Si vous utilisez les disquettes boot.flp et fixit.flp, continuez à lire. Mettre la disquette boot.flp dans le premier lecteur et démarrez l'ordinateur. Le menu d'installation d'origine s'affiche à l'écran. Choisissez l'option Fixit—Repair mode with CDROM or floppy.. Insérez la disquette fixit.flp quand on vous la demande. restore(8) et les autres programmes dont vous avez besoin sont situés dans le répertoire /mnt2/rescue (/mnt2/stand pour les versions de FreeBSD antérieures à la 5.2).

Restaurez chaque système de fichiers séparément.

Essayez mount(8) (e.g. `mount /dev/da0a /mnt`) sur la partition racine de votre premier disque. Si le label du disque est endommagé, utilisez bsdlabel(8) pour repartitionner et libeller le disque conformément au label que vous avez imprimé et mis de côté. Utilisez newfs(8) pour recréer les systèmes de fichiers. Remontez la partition racine de la disquette en lecture/écriture (`mount -u -o rw /mnt`). Utilisez votre programme de restauration et vos bandes de sauvegardes pour restaurer les données de ce système de fichiers (e.g. `restore vrf /dev/sa0`). Démontez le système de fichiers (e.g. `umount /mnt`). Répétez l'opération pour chacun des systèmes de fichiers endommagés.

Une fois que le système fonctionne à nouveau, faites une sauvegarde sur de nouvelles bandes. Ce qui a causé la panne ou la perte de données peut se reproduire. Une heure de perdue maintenant peut vous épargner d'autres ennuis plus tard.

19.13. Systèmes de fichiers réseaux, en mémoire et sauvegardés sur fichier

En plus des disques que vous introduisez physiquement dans votre ordinateur: disquettes, CD, disques durs, et ainsi de suite; d'autres formes de disques sont gérées par FreeBSD - les *disques virtuels*.

Ceux-ci comprennent les systèmes de fichiers réseaux comme le NFS et Coda, les systèmes de fichiers en mémoire et les systèmes de fichiers sauvegardé dans un fichier.

En fonction de la version de FreeBSD que vous utilisez, vous devrez utiliser des outils différents pour la création et l'utilisation de systèmes de fichiers en mémoire ou sauvegardé dans un fichier.

Utilisez devfs(5) pour allouer de façon transparente pour l'utilisateur les fichiers spéciaux de périphériques.

19.13.1. Système de fichiers sauvegardé dans un fichier

L'utilitaire mdconfig(8) est utilisé pour configurer et activer les disques mémoires, md(4), sous FreeBSD. Pour utiliser mdconfig(8), vous devez charger le module md(4) ou en ajouter le support dans votre fichier de configuration du noyau:

```
device md
```

La commande mdconfig(8) supporte trois sortes de disques virtuels en mémoire: les disques mémoire alloués avec malloc(9), les disques mémoires utilisant un fichier ou l'espace de pagination comme espace disque. Une des utilisations possibles est le montage d'images de disquettes ou de CDs conservées sous forme de fichier.

Pour monter l'image d'un système de fichiers:

Exemple 32. Utilisation de `mdconfig` pour monter une image d'un système de fichiers

```
# mdconfig -a -t vnode -f diskimage -u 0
```

```
# mount /dev/md0 /mnt
```

Pour créer l'image d'un nouveau système de fichiers avec mdconfig(8):

Exemple 33. Création d'un nouveau disque sauvegardé sur fichier avec `mdconfig`

```
# dd if=/dev/zero of=newimage bs=1k count=5k
5120+0 records in
5120+0 records out
# mdconfig -a -t vnode -f newimage -u 0
# bsdlabel -w md0 auto
# newfs md0a
/dev/md0a: 5.0MB (10224 sectors) block size 16384, fragment size 2048
        using 4 cylinder groups of 1.25MB, 80 blks, 192 inodes.
super-block backups (for fsck -b #) at:
 160, 2720, 5280, 7840
# mount /dev/md0a /mnt
# df /mnt
Filesystem 1K-blocks Used Avail Capacity  Mounted on
/dev/md0a       4710    4  4330     0%    /mnt
```

Si vous ne préciser pas de numéro d'unité avec l'option `-u`, mdconfig(8) utilisera le mécanisme d'allocation automatique de md(4) pour sélectionner un périphérique libre. Le nom de l'unité allouée s'affichera sur la sortie standard comme par exemple md4. Pour plus de détails concernant mdconfig(8), référez-vous à la page de manuel.

L'outil mdconfig(8) est très utile, cependant son utilisation demande de nombreuses lignes de commandes pour créer un système de fichiers sauvegardé sur fichier. FreeBSD vient avec un outil appelé mdmfs(8), ce programme configure un disque md(4) en utilisant mdconfig(8), y ajoute dessus un système de fichiers UFS en utilisant newfs(8), et le monte avec mount(8). Par exemple, si vous désirez créer et monter la même image de système de fichiers que précédemment, tapez simplement ce qui suit:

Exemple 34. Création et montage d'un disque sauvegardé sur fichier avec `mdmfs`

```
# dd if=/dev/zero of=newimage bs=1k count=5k
5120+0 records in
5120+0 records out
# mdmfs -F newimage -s 5m md0 /mnt
# df /mnt
Filesystem 1K-blocks Used Avail Capacity  Mounted on
/dev/md0        4718    4  4338     0%    /mnt
```

Si vous utilisez l'option `md` sans numéro d'unité, mdmfs(8) utilisera la fonction automatique de sélection d'unité de md(4) pour choisir un périphérique non utilisé. Pour plus de détails au sujet de

mdmfs(8), référez-vous à la page de manuel.

19.13.2. Système de fichiers en mémoire

Pour un système de fichiers en mémoire la "sauvegarde sur l'espace de pagination" devrait être normalement utilisée. Utiliser l'espace de pagination ne signifie pas que le disque en mémoire sera par défaut sur l'espace de pagination, mais plutôt que le disque mémoire sera alloué sur une zone de mémoire qui pourra être sauvegardée sur l'espace de pagination si nécessaire. Il est également possible de créer un disque en mémoire dont la mémoire est allouée à l'aide de malloc(9), mais ce type de configuration, tout particulièrement dans le cas de disques de grande taille, peut donner lieu à une panique du système si le noyau se trouve à cours de mémoire.

Exemple 35. Création d'un disque mémoire avec `mdconfig`

```
# mdconfig -a -t swap -s 5m -u 1
# newfs -U md1
/dev/md1: 5.0MB (10240 sectors) block size 16384, fragment size 2048
        using 4 cylinder groups of 1.27MB, 81 blks, 192 inodes.
        with soft updates
super-block backups (for fsck -b #) at:
 160, 2752, 5344, 7936
# mount /dev/md1 /mnt
# df /mnt
Filesystem 1K-blocks Used Avail Capacity  Mounted on
/dev/md1        4718    4  4338     0%    /mnt
```

Exemple 36. Création d'un disque mémoire avec `mdmfs`

```
# mdmfs -s 5m md2 /mnt
# df /mnt
Filesystem 1K-blocks Used Avail Capacity  Mounted on
/dev/md2        4846    2  4458     0%    /mnt
```

19.13.3. Détacher un disque mémoire du système

Quand un système de fichiers en mémoire ou sauvegardé dans un fichier n'est pas utilisé, vous devriez rendre au système toutes les ressources. La première chose à faire est de démonter le système de fichiers, ensuite utiliser mdconfig(8) pour détacher le disque du système et rendre les ressources.

Par exemple pour détacher et libérer toutes les ressources utilisées par /dev/md4:

```
# mdconfig -d -u 4
```

Il est possible d'afficher des informations sur les périphériques md(4) configurés en utilisant la commande `mdconfig -l`.

19.14. Instantané ("Snapshot") d'un système de fichiers

FreeBSD en association avec les Soft Updates offre une nouvelle caractéristique: les instantanés de systèmes de fichiers ("file system snapshots").

Les instantanés permettent à un utilisateur de créer des images d'un système de fichiers précis, et de les traiter comme un fichier. Les instantanés doivent être créés dans le système de fichiers sur lequel on veut effectuer l'opération, et un utilisateur ne pourra pas créer plus de 20 instantanés par système de fichiers. Les instantanés actifs sont enregistrés dans le superbloc, ils sont donc conservés durant les opérations de démontage et de remontage lors des redémarrages du système. Quand un instantané n'est plus requis, il peut être supprimé avec la commande standard rm(1). Les instantanés peuvent être supprimés dans n'importe quel ordre, cependant tout l'espace utilisé pourra ne pas être à nouveau disponible car un autre instantané réclamera éventuellement les blocs libérés.

L'indicateur inaltérable `snapshot` est positionné lors de la création initiale de l'instantané. La commande unlink(1) fait une exception pour les fichiers d'instantanés puisqu'elle autorise leur suppression.

Les instantanés sont créés avec la commande mount(8). Pour placer un instantané de /var dans le fichier /var/snapshot/snap utilisez la commande suivante:

```
# mount -u -o snapshot /var/snapshot/snap /var
```

Alternativement, vous pouvez utiliser mksnap_ffs(8) pour créer un instantané:

```
# mksnap_ffs /var /var/snapshot/snap
```

Les fichiers d'instantanés peuvent être localisés sur un système de fichiers (e.g. /var) en utilisant la commande find(1):

```
# find /var -flags snapshot
```

Une fois un instantané créé, ce dernier pourra avoir de nombreux usages:

- Certains administrateurs utiliseront un instantané pour des besoins de sauvegarde, car l'instantané peut être transféré sur CD ou bande.
- Un contrôle d'intégrité du système fichiers, fsck(8), pourra être effectué sur l'instantané. En supposant que le système de fichiers était propre quand il a été monté, vous devriez toujours obtenir un résultat positif (et non différent). C'est essentiellement que effectue le processus de fsck(8) en tâche de fond ("background fsck(8)").

- Lancer l'utilitaire dump(8) sur l'instantané. Une image cohérente du système de fichiers avec les paramètres temporels de l'instantané sera produite. dump(8) peut également à partir d'un instantané, créer une image et puis supprimer l'instantané en une seule fois en utilisant l'indicateur `-L` dans la ligne de commande.
- Monter l'instantané comme une image figée du système de fichiers. Pour monter l'instantané /var/snapshot/snap lancer:

```
# mdconfig -a -t vnode -f /var/snapshot/snap -u 4
# mount -r /dev/md4 /mnt
```

Vous pouvez maintenant parcourir l'arborescence de votre système de fichiers /var figé monter sous /mnt. Tout sera au départ dans le même état que lors de la création de l'instantané. La seule exception est que les instantanés antérieurs apparaîtront sous la forme de fichiers vides. Quand l'utilisation d'un instantané est terminée, il peut être démonté avec:

```
# umount /mnt
# mdconfig -d -u 4
```

Pour plus d'informations sur les `softupdates` et les instantanés de systèmes de fichiers, et également de la documentation technique, vous pouvez consulter le site Web de Marshall Kirk McKusick à l'adresse http://www.mckusick.com/

19.15. Quotas d'utilisation des disques

Les quotas sont une option du système d'exploitation qui vous permet de limiter la quantité d'espace disque et/ou le nombre de fichiers auxquels ont droit un utilisateur ou tous les utilisateurs d'un même groupe, sur un système de fichiers donné. On les utilise la plupart du temps sur les systèmes en temps partagé où il est souhaitable de limiter la quantité de ressources allouée à un utilisateur ou à un groupe. Cela évitera qu'un utilisateur ou un groupe d'utilisateur consomme tout l'espace disque.

19.15.1. Configurer votre système pour pouvoir utiliser les quotas d'utilisation des disques

Avant d'essayer de mettre en place des quotas disque, il est nécessaire de s'assurer que le noyau est configuré pour les quotas. Cela se fait en ajoutant la ligne suivante dans votre fichier de configuration du noyau:

```
options QUOTA
```

Cette option n'est pas activée par défaut dans le noyau GENERIC de base, vous devrez donc configurer, compiler et installer un noyau sur-mesure pour utiliser les quotas disque. Reportez-vous au chapitre Configurer le noyau de FreeBSD pour plus d'informations sur la configuration du noyau.

Ensuite vous devrez activer les quotas disques dans le fichier /etc/rc.conf. Pour cela, ajoutez la ligne:

```
enable_quotas="YES"
```

Pour un contrôle plus fin des quotas au démarrage du système, il existe une variable supplémentaire de configuration. Normalement au démarrage, l'intégrité des quotas sur chaque système de fichiers est vérifiée par le programme quotacheck(8). Ce programme s'assure que les données de la base de données des quotas correspondent bien aux données présentes sur le système de fichiers. C'est un processus consommateur en temps qui affectera considérablement la durée de démarrage du système. Si vous désirez passer cette étape, une variable dans /etc/rc.conf est prévue à cet effet:

```
check_quotas="NO"
```

Vous devez enfin éditer le fichier /etc/fstab pour activer les quotas système de fichiers par système de fichiers. C'est là que vous pouvez soit activer les quotas par utilisateur ou par groupe soit les pour les deux sur tous vos systèmes de fichiers.

Pour activer les quotas par utilisateur sur un système de fichiers, ajouter l'option `userquota` dans le champ d'options sur l'entrée de /etc/fstab pour le système de fichiers sur lequel vous voulez activer les quotas. Par exemple:

```
/dev/da1s2g   /home    ufs rw,userquota 1 2
```

De même, pour activer les quotas par groupe, utilisez l'option `groupquota` à la place de `userquota`. Pour activer à la fois les quotas par utilisateur et par groupe, modifiez l'entrée de la façon suivante:

```
/dev/da1s2g    /home    ufs rw,userquota,groupquota 1 2
```

Par défaut, les fichiers où sont définis les quotas dans le répertoire racine du système de fichiers sous les noms quota.user et quota.group, respectivement pour les quotas utilisateur et les quotas par groupe. Consultez la page de manuel fstab(5) pour plus d'information. Bien que la page de manuel fstab(5) indique que vous pouvez spécifier un autre emplacement pour ces fichiers, cela n'est pas recommandé parce que les divers utilitaires qui gèrent les quotas ne semblent pas les prendre correctement en compte.

A ce point vous devriez redémarrer votre système avec votre nouveau noyau. La procédure /etc/rc exécutera automatiquement les commandes nécessaires pour créer les fichiers de quotas initiaux pour tous les quotas que vous avez définis dans /etc/fstab, vous n'avez donc pas besoin de créer à la main de fichiers de quotas vides.

Vous ne devriez pas avoir à exécuter les commandes quotacheck(8), quotaon(8), ou quotaoff(8) manuellement. Cependant, vous pouvez lire leur page de manuel pour vous familiariser avec leur rôle.

19.15.2. Définir les quotas

Une fois que vous avez activé les quotas sur votre système, assurez-vous que cela fonctionne correctement. Une manière simple de le faire est d'exécuter:

```
# quota -v
```

Vous devriez obtenir une ligne résumant l'utilisation disque avec les quotas actuellement définis pour chaque système de fichiers sur lesquels il y a des quotas.

Vous êtes maintenant prêt à définir les quotas avec la commande edquota(8).

Vous disposez de différentes options pour instaurer les quotas d'espace disque alloué à un utilisateur ou à un groupe, et le nombre de fichiers qu'ils peuvent créer. Vous pouvez baser les limitations sur l'espace disque alloué (quotas en nombre de blocs) ou sur le nombre de fichiers (quotas en inode) ou les deux. Ces options peuvent être divisées en deux catégories: les limites strictes ou souples.

Une limite stricte ne peut être dépassée. Une fois qu'un utilisateur atteint sa limite stricte, il ne pourra plus rien allouer sur le système de fichiers en question. Par exemple, si l'utilisateur a droit à une limite stricte de 500 Ko sur un système de fichiers et en utilise 490 Ko, il ne pourra allouer que 10 Ko supplémentaires. Une tentative d'allouer 11 Ko échouerait.

Une limite souple peut être dépassée pour une période de temps restreinte. C'est ce que l'on appelle le délai de grâce, qui est d'une semaine par défaut. Si un utilisateur dépasse cette limite au delà du délai de grâce, cette limite devient stricte, et plus aucune allocation ne sera possible. Quand l'utilisateur redescend en dessous de la limite souple, le délai de grâce est à nouveau réaccordé.

Ce qui suit est un exemple de ce que vous pourrez voir en utilisant la commande edquota(8). Quand vous invoquez la commande edquota(8), vous vous retrouvez dans l'éditeur défini par la variable d'environnement `EDITOR`, ou sous vi si la variable d'environnement `EDITOR` n'est pas positionnée, ce qui vous permet d'éditer les quotas.

```
# edquota -u test
```

```
Quotas for user test:
/usr: kbytes in use: 65, limits (soft = 50, hard = 75)
        inodes in use: 7, limits (soft = 50, hard = 60)
/usr/var: kbytes in use: 0, limits (soft = 50, hard = 75)
        inodes in use: 0, limits (soft = 50, hard = 60)
```

Vous verrez normalement deux lignes pour chaque système de fichiers sur lequel il y a des quotas. Une ligne pour les quotas de blocs, et une autre pour la limite d'inode. Modifiez simplement les valeurs que vous voulez mettre à jour. Par exemple, pour augmenter la limite de blocs accordée à cet utilisateur de 50 pour la limite souple et de 75 pour la limite stricte à 500 pour la limite souple et 600 pour la limite stricte, modifiez:

```
/usr: kbytes in use: 65, limits (soft = 50, hard = 75)
```

en:

```
/usr: kbytes in use: 65, limits (soft = 500, hard = 600)
```

Les nouveaux quotas seront en service dès que vous quitterez l'éditeur.

Il est parfois souhaitable de définir des quotas pour une plage d'UIDs (identifiants utilisateur). Cela peut être réalisé avec l'option `-p` de la commande edquota(8). Définissez d'abord les quotas pour un seul utilisateur, et puis exécutez `edquota -p protouser startuid-enduid`. Par exemple, si l'utilisateur `test` dispose des quotas désirés, la commande suivante peut être utilisée pour appliquer ces quotas pour les UIDs de 10000 à 19999:

```
# edquota -p test 10000-19999
```

Pour plus d'informations consultez la page de manuel edquota(8).

19.15.3. Consulter les quotas et l'utilisation des disques

Vous pouvez soit utiliser la commande quota(1) soit la commande repquota(8) pour consulter les quotas et l'utilisation des disques. La commande quota(1) peut être employée pour connaître les quotas et l'utilisation des disques pour un utilisateur et un groupe. Un utilisateur ne peut consulter que ses propres quotas et ceux d'un groupe auquel il appartient. Seul le super-utilisateur peut consulter les quotas et l'usage disque de tous les utilisateurs et groupes. La commande repquota(8) permet d'obtenir un résumé de tous les quotas et l'utilisation disque pour les systèmes de fichiers sur lesquels il y a des quotas.

Ce qui suit est un extrait de la sortie de la commande `quota -v` pour un utilisateur pour lequel on a défini des quotas sur deux systèmes de fichiers.

```
Disk quotas for user test (uid 1002):
     Filesystem  usage   quota   limit   grace   files   quota   limit   grace
           /usr      65*     50      75   5days       7      50      60
       /usr/var       0      50      75               0      50      60
```

Sur le système de fichiers /usr dans l'exemple ci-dessus, l'utilisateur occupe 15 Ko de plus que la limite de 50 Ko qui lui est allouée et dispose d'un délai de grâce de 5 jours. Notez l'astérisque * qui indique que l'utilisateur dépasse actuellement son quota.

Normalement les systèmes de fichiers sur lesquels l'utilisateur n'occupe pas d'espace n'apparaissent pas dans la sortie de la commande quota(1), même s'il a des quotas sur ces systèmes de fichiers. L'option `-v` listera ces systèmes de fichiers, comme /usr/var dans l'exemple ci-dessus.

19.15.4. Quotas avec NFS

Les quotas sont gérés par le sous-système de gestion des quotas sur le serveur NFS. Le démon rpc.rquotad(8) fournit les informations sur les quotas à la commande quota(1) des clients NFS, permettant aux utilisateurs sur ces machines de consulter l'utilisation des quotas qui leur sont alloués.

Activez `rpc.rquotad` dans /etc/inetd.conf de la façon suivante:

```
rquotad/1      dgram rpc/udp wait root /usr/libexec/rpc.rquotad rpc.rquotad
```

Puis redémarrez `inetd`:

```
# kill -HUP `cat /var/run/inetd.pid`
```

19.16. Chiffrer les partitions d'un disque

FreeBSD offre d'excellentes protections contre un accès non autorisé aux données par l'intermédiaire du réseau. Les permissions sur les fichiers et le contrôle d'accès obligatoire - "Mandatory Access Control" (MAC) (voir Mandatory Access Control) empêchent l'accès aux données pour des tiers non autorisés quand le système d'exploitation est actif et l'ordinateur en fonctionnement. Cependant, des permissions renforcés sont inutiles si l'attaquant a un accès physique à un ordinateur et peut simplement déplacer le disque dur sur un autre système pour copier et analyser les données sensibles.

Indépendamment de la manière dont une personne malveillante s'est trouvé en possession d'un disque dur ou a arrêté un ordinateur, le chiffrage de disque basé sur GEOM (gbde) ("GEOM Based Disk Encryption") et le système de chiffrage `geli` de FreeBSD sont en mesure de protéger les données des systèmes de fichiers contre des attaquants très motivés et aux ressources importantes. A la différence des méthodes de chiffrage lourdes qui chiffrent uniquement les fichiers individuels, gbde et `geli` chiffrent de manière transparente l'intégralité du système de fichiers. Aucun texte en clair ne touche les plateaux du disque.

19.16.1. Chiffrage des disques avec gbde

1. Devenir `root`

   La configuration de gbde requiert les privilèges du super-utilisateur.

   ```
   % su -
   Password:
   ```

2. Ajouter le support gbde(4) au fichier de configuration du noyau

   Ajoutez la ligne suivante à votre fichier de configuration du noyau:

```
options GEOM_BDE
```

Recompilez le noyau comme décrit dans Configurer le noyau de FreeBSD.

Redémarrez avec le nouveau noyau.

3. Au lieu de recompiler le noyau, on peut utiliser `kldload` pour charger le support gbde(4):

```
# kldload geom_bde
```

19.16.1.1. Préparation du disque dur chiffré

L'exemple suivant suppose que vous ajoutez un nouveau disque dur à votre système et qui contiendra une seule partition chiffrée. Cette partition sera montée sous /private. gbde peut également être utilisé pour chiffrer les répertoires /home et /var/mail, mais cela demande une configuration plus complexe qui dépasse le cadre de cette introduction.

1. Ajouter le nouveau disque

   Installez le nouveau disque comme expliqué dans Ajouter des disques. Pour les besoins de cet exemple, une nouvelle partition disque a été ajoutée en tant que /dev/ad4s1c. Les périphériques du type /dev/ad0s1* représentent les partitions FreeBSD standards sur le système exemple.

```
# ls /dev/ad*
/dev/ad0        /dev/ad0s1b     /dev/ad0s1e     /dev/ad4s1
/dev/ad0s1      /dev/ad0s1c     /dev/ad0s1f     /dev/ad4s1c
/dev/ad0s1a     /dev/ad0s1d     /dev/ad4
```

2. Créer un répertoire pour héberger les fichiers de verrouillage de GBDE

```
# mkdir /etc/gbde
```

   Le fichier de verrouillage de gbde contient l'information nécessaire à gbde pour accéder aux partitions chiffrées. Sans accès au fichier de verrouillage, gbde sera incapable de déchiffrer les données contenues sur la partition chiffrée sans une aide manuelle significative ce qui n'est pas supporté par le logiciel. Chaque partition chiffrée utilise un fichier de verrouillage propre.

3. Initialiser la partition gbde

   Une partition gbde doit être initialisée avant d'être utilisable. Cette initialisation doit être effectuée une seule fois:

```
# gbde init /dev/ad4s1c -i -L /etc/gbde/ad4s1c
```

gbde(8) lancera votre éditeur, vous permettant de fixer diverses options de configuration dans un gabarit. Pour une utilisation de UFS1 ou UFS2, fixez l'option `sector_size` à 2048:

```
$FreeBSD: src/sbin/gbde/template.txt,v 1.1 2002/10/20 11:16:13 phk Exp $
#
# La taille d'un secteur est la plus petite unité de donnée
# qui peut être lue ou écrite.
# Une valeur trop petite diminue les performances et l'espace
# disponible.
# Une valeur trop grande peut empêcher des systèmes de
# fichiers de fonctionner correctement.  512 est la valeur minimale
# et sans risque.  Pour l'UFS, utiliser la taille d'un fragment
#
sector_size     =       2048
[...]
```

gbde(8) vous demandera de taper deux fois la phrase d'authentification qui devra être utilisée pour sécuriser les données. La phrase d'authentification doit être la même dans les deux cas. La capacité de gbde à protéger vos données dépend de la qualité de la phrase d'authentification que vous avez choisie.

La commande `gbde init` crée un fichier de verrouillage pour votre partition gbde qui dans cet exemple est stocké sous /etc/gbde/ad4s1c.

Les fichiers de verrouillage de gbde *doivent* être conservés de pair avec le contenu des partitions chiffrées. Alors que la suppression seule d'un fichier de verrouillage ne peut empêcher une personne déterminée de déchiffrer une partition gbde, sans le fichier de verrouillage, le propriétaire légitime sera incapable d'accéder aux données de la partition chiffrée sans beaucoup de travail ce qui est totalement non supporté par gbde(8) et son concepteur.

4. Attacher la partition chiffrée au noyau

```
# gbde attach /dev/ad4s1c -l /etc/gbde/ad4s1c
```

On vous demandera de fournir la phrase d'authentification que vous avez choisie lors de l'initialisation de la partition chiffrée. Le nouveau périphérique chiffré apparaîtra dans /dev en tant que /dev/nom_périphérique.bde:

```
# ls /dev/ad*
/dev/ad0        /dev/ad0s1b     /dev/ad0s1e     /dev/ad4s1
/dev/ad0s1      /dev/ad0s1c     /dev/ad0s1f     /dev/ad4s1c
/dev/ad0s1a     /dev/ad0s1d     /dev/ad4        /dev/ad4s1c.bde
```

5. Créer un système de fichiers sur le périphérique chiffré

Une fois que le périphérique chiffré a été attaché au noyau, vous pouvez créer un système de fichiers sur le périphérique. Pour créer un système de fichiers sur le périphérique, utilisez newfs(8). Puisqu'il est plus rapide d'initialiser un nouveau système de fichiers UFS2 qu'un nouveau système UFS1, l'utilisation de newfs(8) avec l'option -O2 est recommandé.

```
# newfs -U -O2 /dev/ad4s1c.bde
```

La commande newfs(8) peut être effectuée sur une partition gbde attachée qui est identifiée par une extension *.bde au niveau du nom de périphérique.

6. Monter la partition chiffrée

   Créez un point de montage pour le système de fichiers chiffré.

   ```
   # mkdir /private
   ```

   Montez le système de fichiers chiffré.

   ```
   # mount /dev/ad4s1c.bde /private
   ```

7. Vérifiez que le système de fichiers chiffré est disponible

   Le système de fichiers chiffré devrait être visible par df(1) et prêt à être utilisé:

   ```
   % df -H
   Filesystem        Size   Used  Avail Capacity  Mounted on
   /dev/ad0s1a      1037M    72M   883M     8%    /
   /devfs            1.0K   1.0K     0B   100%    /dev
   /dev/ad0s1f       8.1G    55K   7.5G     0%    /home
   /dev/ad0s1e      1037M   1.1M   953M     0%    /tmp
   /dev/ad0s1d       6.1G   1.9G   3.7G    35%    /usr
   /dev/ad4s1c.bde   150G   4.1K   138G     0%    /private
   ```

19.16.1.2. Montage des systèmes de fichiers chiffrés

Après chaque démarrage, tout système de fichiers chiffré doit être rattaché au noyau, contrôlé pour les erreurs, et monté, avant que les systèmes de fichiers ne puissent être utilisés. Les commandes nécessaires doivent être exécutées en tant que `root`.

1. Attacher la partition gdbe au noyau

   ```
   # gbde attach /dev/ad4s1c -l /etc/gbde/ad4s1c
   ```

On vous demandera de fournir la phrase d'authentification que vous avez choisie lors de l'initialisation de la partition gbde chiffrée.

2. Contrôler les erreurs du système de fichiers

   Puisque les systèmes de fichiers chiffrés ne peuvent être encore listés dans le fichier /etc/fstab pour un montage automatique, on doit donc contrôler les systèmes de fichiers pour d'éventuelles erreurs en exécutant manuellement fsck(8) avant le montage.

   ```
   # fsck -p -t ffs /dev/ad4s1c.bde
   ```

3. Monter le système de fichiers chiffré

   ```
   # mount /dev/ad4s1c.bde /private
   ```

   Le système de fichiers est maintenant disponible à l'utilisation.

19.16.1.2.1. Montage automatique de partitions chiffrées

Il est possible de créer une procédure pour automatiquement attacher, contrôler, et monter une partition chiffrée, mais pour des raisons de sécurité la procédure ne devrait pas contenir le mot de passe gbde(8). A la place, il est recommandé que de telles procédures soient exécutées manuellement tout en fournissant le mot de passe via la console ou ssh(1).

Comme autre possibilité, une procédure rc.d est fournie. Des arguments peuvent être passés à cette procédure par l'intermédiaire de rc.conf(5),, par exemple:

```
gbde_autoattach_all="YES"
gbde_devices="ad4s1c"
```

Cela impose la saisie de la phrase d'authentification gbde au démarrage. Après avoir entré la phrase d'authentification correctement, la partition chiffrée gbde sera montée automatiquement. Cela peut être très utile quand gbde est utilisé sur des ordinateurs portables.

19.16.1.3. Les protections cryptographiques utilisées par gbde

gbde(8) chiffre la partie utile des secteurs en utilisant le chiffrage AES 128 bits en mode CBC. Chaque secteur sur le disque est chiffré avec une clé AES différente. Pour plus d'informations sur l'architecture cryptographique de gbde, y compris comment les clés pour chaque secteur sont des dérivés de la phrase d'authentification donnée par l'utilisateur, voir la page de manuel gbde(4).

19.16.1.4. Problèmes de compatibilité

sysinstall(8) est incompatible avec les périphériques gbde-chiffrés. Tous les périphériques *.bde doivent être détachés du noyau avant de lancer sysinstall(8) ou ce dernier plantera durant son processus initial de recherche des périphériques. Pour détacher le périphérique chiffré utilisé dans

notre exemple, utilisez la commande suivante:

```
# gbde detach /dev/ad4s1c
```

Notez également qu'étant donné que vinum(4) n'utilise pas le sous-système geom(4), vous ne pouvez utiliser gbde avec des volumes vinum.

19.16.2. Chiffrage des disques avec `geli`

Depuis FreeBSD 6.0, une nouvelle classe GEOM pour le chiffrage des données est disponible: `geli`. Cette classe est développée par Paweł Jakub Dawidek <pjd@FreeBSD.org>. L'outil `geli` est différent de `gbde`; il offre des fonctionnalités différentes et utilise une méthode différente pour chiffrer les données.

Les caractéristiques les plus importantes de geli(8) sont:

- Utilisation du système crypto(9) - quand du matériel destiné au chiffrement est disponible dans la machine, `geli` l'utilisera automatiquement.
- Support de plusieurs algorithmes de chiffrement (actuellement AES, Blowfish, et 3DES).
- Permettre le chiffrage de la partition racine. La phrase d'authentification utilisée pour accéder à la partition racine chiffrée sera demandée au démarrage du système.
- Permettre l'emploi de deux clés indépendantes (par exemple une "clé utilisateur" et une "clé entreprise").
- `geli` est rapide-il effectue un simple chiffrement de secteur à secteur.
- Permettre la sauvegarde et la restauration des clés principales. Quand un utilisateur doit détruire ses clés, il sera possible d'accéder à nouveau aux données en restaurant les clés à partir de la sauvegarde.
- Permettre d'attacher un disque avec une clé aléatoire à usage unique - utile pour les partitions de pagination et les systèmes de fichiers temporaires.

Plus de caractéristiques concernant `geli` peuvent être trouvées dans la page de manuel de geli(8).

Les points suivants décriront comment activer le support pour `geli` dans le noyau FreeBSD et expliqueront comment créer et utiliser un *provider* (ou partition) chiffré `geli`.

Afin de pouvoir employer `geli`, vous devez utiliser FreeBSD 6.0-RELEASE ou une version ultérieure. Les privilèges du super-utilisateur seront également nécessaire puisque il faudra effectuer des modifications au niveau du noyau.

1. Ajouter le support `geli` au noyau

   Ajoutez les lignes suivantes au fichier de configuration du noyau:

   ```
   options GEOM_ELI
   ```

```
device crypto
```

Recompilez le noyau comme décrit dans la Configurer le noyau de FreeBSD.

Sinon, le module `geli` peut être chargé au démarrage. Ajoutez la ligne suivante au fichier /boot/loader.conf:

```
geom_eli_load="YES"
```

Le système geli(8) devrait désormais être supporté par le noyau.

2. Générer la clé principale

L'exemple suivant décrira la méthode pour générer un fichier clé qui sera utilisé comme partie de la clé principale pour le *provider* chiffré monté sous le répertoire /private. Le fichier clé fournira des données aléatoires qui seront employées pour chiffrer la clé principale. La clé principale sera également protégée par une phrase d'authentification. La taille des secteurs du *provider* sera de 4Ko. De plus, sera décrit comment attacher au système le *provider* geli, créer un système de fichiers dessus, utiliser ce système de fichiers et enfin comment le détacher.

Il est recommandé d'utiliser une taille de secteur plus grande (comme 4Ko) pour de meilleures performances.

La clé principale sera protégée avec une phrase d'authentification et la source de données pour le fichier clé sera /dev/random. La taille des secteurs de /dev/da2.eli, partition que nous appelons *provider*, sera de 4Ko.

```
# dd if=/dev/random of=/root/da2.key bs=64 count=1
# geli init -s 4096 -K /root/da2.key /dev/da2
Enter new passphrase:
Reenter new passphrase:
```

Il n'est pas obligatoire d'utiliser la phrase d'authentification et le fichier clé; chacune de ces méthodes de sécurisation de la clé principale peut être utilisée séparément.

Si à la place du fichier clé un "-" est passé, l'entrée standard sera utilisée. Cet exemple montre comment on peut utiliser plus d'un fichier clé:

```
# cat keyfile1 keyfile2 keyfile3 | geli init -K - /dev/da2
```

3. Attacher le *provider* avec la clé générée

```
# geli attach -k /root/da2.key /dev/da2
Enter passphrase:
```

Le nouveau périphérique sera appelé /dev/da2.eli.

```
# ls /dev/da2*
/dev/da2  /dev/da2.eli
```

4. Créer le nouveau système de fichiers

```
# dd if=/dev/random of=/dev/da2.eli bs=1m
# newfs /dev/da2.eli
# mount /dev/da2.eli /private
```

Le système de fichiers chiffré devrait être maintenant visible par df(1) et disponible à l'utilisation:

```
# df -H
Filesystem     Size   Used  Avail Capacity  Mounted on
/dev/ad0s1a    248M    89M   139M    38%    /
/devfs         1.0K   1.0K     0B   100%    /dev
/dev/ad0s1f    7.7G   2.3G   4.9G    32%    /usr
/dev/ad0s1d    989M   1.5M   909M     0%    /tmp
/dev/ad0s1e    3.9G   1.3G   2.3G    35%    /var
/dev/da2.eli   150G   4.1K   138G     0%    /private
```

5. Démonter et détacher le *provider*

Une fois l'utilisation de la partition chiffrée achevée et que la partition /private n'est plus nécessaire, il est prudent de penser à démonter et détacher la partition `geli` chiffrée:

```
# umount /private
# geli detach da2.eli
```

Plus d'information sur l'utilisation de geli(8) peut être trouvée dans sa page de manuel.

19.16.2.1. Utiliser la procédure rc.d de geli

La commande geli est fournie avec une procédure rc.d qui peut être employée pour simplifier l'utilisation de `geli`. Un exemple de configuration de `geli` à l'aide de rc.conf(5) sera:

```
geli_devices="da2"
geli_da2_flags="-p -k /root/da2.key"
```

Ces lignes configureront /dev/da2 comme *provider* `geli` avec une clé principale /root/da2.key, de plus `geli` n'utilisera pas de phrase d'authentification pour attacher le *provider* (notez que ceci n'est utilisable que si l'option `-P` a été passée durant la phase `geli init`). Le système détachera du noyau

le *provider* `geli` avant l'arrêt du système.

Plus d'information sur la configuration du système rc.d est fournie dans la section rc.d de ce Manuel.

19.17. Chiffrage de l'espace de pagination

Sous FreeBSD, le chiffrement de l'espace de pagination est simple à mettre en place et est possible depuis FreeBSD 5.3-RELEASE. En fonction de la version de FreeBSD utilisée, différentes options sont disponibles et la configuration peut légèrement varier. Depuis FreeBSD 6.0-RELEASE, les systèmes de chiffrage gbde(8) ou geli(8) peuvent être utilisé à cet effet. Avec les versions antérieures, seul gbde(8) est disponible. Les deux systèmes utilisent la procédure rc.d nommée encswap.

La section précédente, Chiffrer les partitions d'un disque, contient une courte explication sur les différents systèmes de chiffrage.

19.17.1. Pourquoi l'espace de pagination devrait être chiffré?

Comme pour le chiffrage des partitions d'un disque, chiffrer l'espace de pagination a pour but la protection des informations sensibles. Imaginez une application qui, par exemple, traite des mots de passe. Tant que ces mots de passe résident en mémoire tout va pour le mieux. Cependant, si le système d'exploitation commence à transférer des pages mémoires vers l'espace de pagination en vue de libérer de la mémoire pour d'autres applications, les mots de passe peuvent être écrits en clair sur les plateaux du disque et seront faciles à récupérer par une personne malveillante. Chiffrer l'espace de pagination peut être une solution contre ce scénario.

19.17.2. Préparation

Pour le reste de cette section, ad0s1b sera la partition réservée à l'espace de pagination.

Jusqu'ici l'espace de pagination n'a jamais été chiffré. Il est fort possible qu'il y ait déjà des mots de passe ou toute autre donnée sensible de présents en clair sur les plateaux du disque. Afin d'y remédier, les données de la partition de pagination doivent être écrasées avec des données aléatoires:

```
# dd if=/dev/random of=/dev/ad0s1b bs=1m
```

19.17.3. Chiffrer de l'espace de pagination avec gbde(8)

Si FreeBSD 6.0-RELEASE ou une version plus récente est utilisée, le suffixe `.bde` doit être ajouté au nom de périphérique sur la ligne du fichier /etc/fstab correspondant à cet espace de pagination:

```
# Device                Mountpoint      FStype  Options         Dump    Pass#
/dev/ad0s1b.bde         none            swap    sw              0       0
```

Pour les systèmes antérieurs à FreeBSD 6.0-RELEASE, la ligne suivante doit également être ajoutée à /etc/rc.conf:

```
gbde_swap_enable="YES"
```

19.17.4. Chiffrage de l'espace de pagination avec geli(8)

La procédure pour le chiffrage de l'espace de pagination avec geli(8) est similaire à celle pour l'utilisation de gbde(8). Le suffixe `.eli` doit être ajouté au nom de périphérique sur la ligne du fichier /etc/fstab correspondant à cet espace de pagination:

```
# Device                Mountpoint      FStype  Options         Dump    Pass#
/dev/ad0s1b.eli         none            swap    sw              0       0
```

Par défaut, geli(8) utilise l'algorithme AES avec une longueur de clé de 256bits.

Les valeurs par défaut peuvent être modifiées en utilisant l'option `geli_swap_flags` dans le fichier /etc/rc.conf. La ligne suivante demande à la procédure rc.d encswap de créer des partitions de pagination en utilisant l'algorithme Blowfish avec une clé de 128 bits de longueur, une taille de secteur de 4 kilo-octets et avec l'option "detach on last close" (détacher après démontage de la partition) activée:

```
geli_swap_flags="-a blowfish -l 128 -s 4096 -d"
```

Veuillez vous référer à la description de la commande `onetime` dans la page de manuel geli(8) pour une liste des options possibles.

19.17.5. Vérifier que cela fonctionne

Une fois que le système a été redémarré, le fonctionnement correct de l'espace de pagination peut être vérifié en utilisant la commande `swapinfo`.

Si gbde(8) est utilisé:

```
% swapinfo
Device          1K-blocks     Used    Avail Capacity
/dev/ad0s1b.bde    542720        0   542720     0%
```

Si geli(8) est utilisé:

```
% swapinfo
Device          1K-blocks     Used    Avail Capacity
/dev/ad0s1b.eli    542720        0   542720     0%
```

Chapitre 20. GEOM: architecture modulaire de gestion des disques

20.1. Synopsis

Ce chapitre couvre l'utilisation des disques via le système GEOM sous FreeBSD. Cela comprend les utilitaires principaux de contrôle des niveaux RAID qui utilisent GEOM pour la configuration. Ce chapitre n'abordera pas en profondeur la manière dont GEOM gère et contrôle les E/S, les systèmes sous-jacents, ou le code utilisé. Ces informations sont fournies par la page de manuel geom(4) et ses nombreuses références. Ce chapitre n'est pas non plus un guide de référence sur les configurations RAID. Seuls les niveaux de RAID supportés par GEOM seront abordés.

Après la lecture de ce chapitre, vous saurez:

- Quel type de support RAID est disponible avec GEOM.
- Comment utiliser les utilitaires de base pour configurer, gérer et manipuler les différents niveaux de RAID.
- Comment dupliquer, entrelacer, et connecter à distance des disques via le système GEOM.
- Comment dépanner les disques attachés au système GEOM.

Avant de lire ce chapitre, vous devrez:

- Comprendre comment FreeBSD gère les disques (Stockage des données).
- Savoir comment configurer et installer un nouveau noyau FreeBSD (Configurer le noyau de FreeBSD).

20.2. Introduction à GEOM

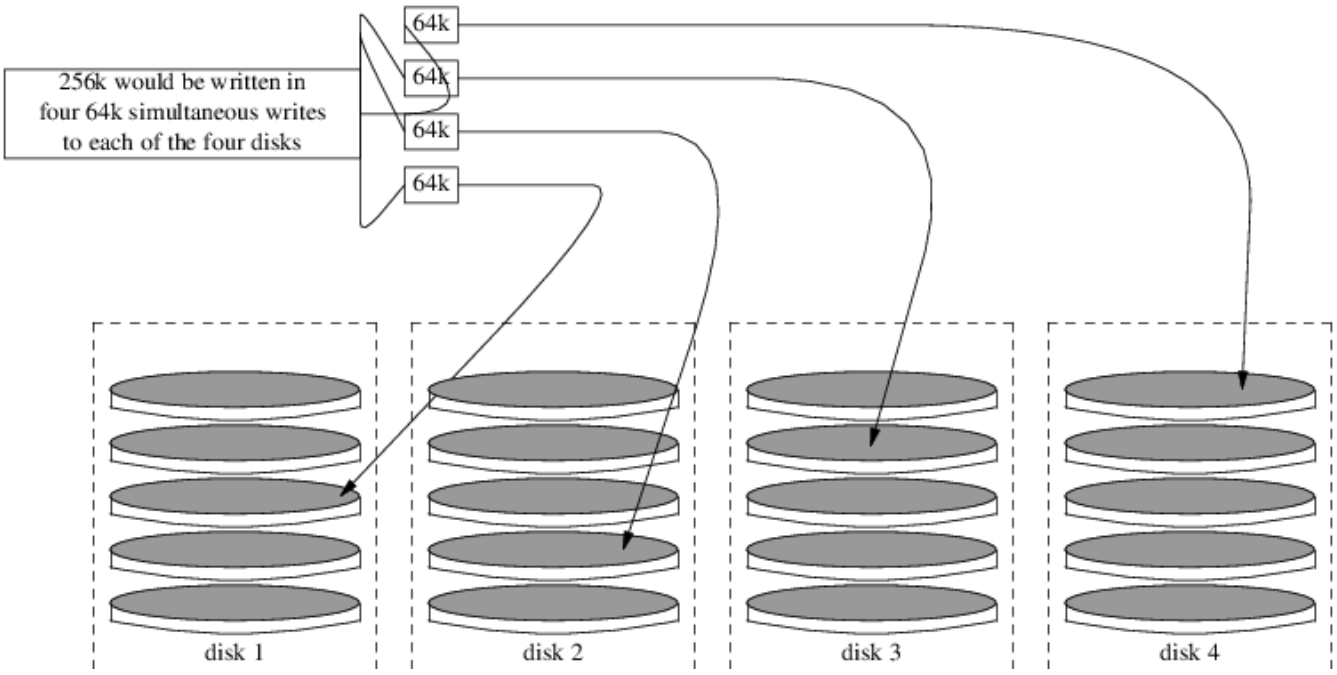
GEOM autorise l'accès et le contrôle de classes - secteur principaux de démarrage ("Master Boot Records"), labels BSD, etc. - par l'intermédiaire d'interfaces, ou de fichiers spéciaux du répertoire /dev. En supportant plusieurs configurations RAID logicielles, GEOM offrira un accès transparent au système d'exploitation et à ses utilitaires.

20.3. RAID0 - "Striping"

Le "striping" (ou entrelacement) est utilisé pour combiner plusieurs disques en un seul volume de stockage. Dans de nombreux cas, cette configuration est réalisée à l'aide de contrôleurs matériels. Le sous-système GEOM offre le support pour le niveau RAID0, également connu sous le nom de "striping".

Dans un système RAID0, les données sont divisées en blocs répartis sur l'ensemble des disques de la "grappe". Au lieu de devoir attendre l'écriture de 256k sur un disque, un système RAID0 peut écrire en simultané 64k sur quatre disques différents, offrant alors des performances d'accès supérieures. Ces performances peuvent être encore améliorées en utilisant plusieurs contrôleurs de disques.

Chaque disque d'une bande ("stripe") RAID0 doit avoir la même taille, puisque les requêtes d'E/S sont entrelacées de manière à lire ou écrire sur plusieurs disques en parallèle.



Procedure: Création d'un système entrelacé à partir de disques ATA non formatés

1. Chargez le module geom_stripe:

```
# kldload geom_stripe
```

2. Assurez-vous de l'existence d'un point de montage. Si ce volume doit devenir une partition racine, utilisez alors un autre point de montage comme /mnt.

```
# mkdir /mnt
```

3. Déterminez les noms de périphériques pour les disques qui seront entrelacé, et créez le nouveau périphérique entrelacé. Par exemple, pour entrelacer deux disques ATA non utilisés et non partitionnés, par exemple /dev/ad2 et /dev/ad3:

```
# gstripe label -v st0 /dev/ad2 /dev/ad3
```

4. Créez un label standard, également connu sous le nom de table des partitions, sur le nouveau volume et installez le code d'amoraçage par défaut:

```
# bsdlabel -wB /dev/stripe/st0
```

5. Cette opération doit avoir créé deux autres périphériques dans le répertoire /dev/stripe en plus du périphérique st0: st0a et st0c. A ce stade, un système de fichiers peut être créé sur

st0a en utilisant la commande `newfs`:

```
# newfs -U /dev/stripe/st0a
```

Des nombres défileront à l'écran, l'opération sera s'achèvera après quelques secondes. Le volume a été créé et est prêt à être monté.

Pour monter manuellement une grappe de disques entrelacés fraîchement créée:

```
# mount /dev/stripe/st0a /mnt
```

Pour monter automatiquement au démarrage ce système de fichiers entrelacé, ajoutez les informations concernant ce volume dans le fichier /etc/fstab:

```
# echo "/dev/stripe/st0a /mnt ufs rw 2 2" \
    >> /etc/fstab
```

Le module geom_stripe doit également être automatiquement chargé lors de l'initialisation du système en ajoutant une ligne au fichier /boot/loader.conf:

```
# echo 'geom_stripe_load="YES"'  /boot/loader.conf
```

20.4. RAID1 - "mirroring"

Le "mirroring" est une technologie utilisée par de nombreuses entreprises et beaucoup de particuliers pour sauvegarder les données sans interruption des activités. Quand un miroir existe, cela signifie que le disque B est une copie du disque A. Ou, autre cas, que les disques C+D sont une copie des disques A+B. Indépendamment de la configuration des disques, l'aspect important est que les données d'un disque ou d'une partition sont dupliquées. Ultérieurement, ces données pourront être plus facilement restaurées, sauvegardées sans interrompre le système ou les accès, et pourront même être stockées physiquement de manière sure.

Pour commencer, vérifiez que le système dispose de deux disques de taille identique, cet exemple suppose que ce sont des disques SCSI (da(4)).

Installez FreeBSD sur le premier disque avec uniquement deux partitions. Une partition sera la partition de pagination d'une taille double à celle de la RAM et l'espace restant sera alloué au système de fichiers racine (/). Il est possible d'avoir des partitions séparées pour les autres points de montage, cependant cela augmentera énormément le niveau de difficulté en raison des modifications manuelles nécessaires des paramètres de bsdlabel(8) et fdisk(8).

Redémarrez et attendez l'initialisation complète du système. Ensuite, ouvrez une session sous l'utilisateur `root`.

Créez le périphérique /dev/mirror/gm et liez-le avec /dev/da1:

```
# gmirror label -vnb round-robin gm0 /dev/da1
```

Le système devrait répondre par:

```
Metadata value stored on /dev/da1.
Done.
```

Initialisez GEOM, cela devrait charger le module du noyau /boot/kernel/geom_mirror.ko:

```
# gmirror load
```

Cette commande devrait créer le fichier spécial de périphérique gm0 sous le répertoire /dev/mirror.

Installez un label `fdisk` et un code de d'amorce génériques sur le nouveau périphérique gm0:

```
# fdisk -vBI /dev/mirror/gm0
```

Installez maintenant un label générique `bsdlabel`:

```
# bsdlabel -wB /dev/mirror/gm0s1
```

S'il existe plusieurs "slices" et plusieurs partitions, il faudra modifier les paramètres des deux commandes précédentes. Elles doivent correspondre aux tailles des partitions et "slices" sur l'autre disque.

Utilisez l'utilitaire newfs(8) pour créer un système de fichiers UFS sur le périphérique gm0s1a:

```
# newfs -U /dev/mirror/gm0s1a
```

Le système devrait alors afficher un certain nombre d'informations et de nombres. C'est bon signe. Contrôlez l'affichage à la recherche de messages d'erreur et montez le périphérique sur le point de montage /mnt:

```
# mount /dev/mirror/gm0s1a /mnt
```

Transférez maintenant toutes les données du disque de démarrage vers ce nouveau système de fichiers. Dans notre exemple nous utilisons à cet effet les commandes dump(8) et restore(8), cependant la commande dd(1) conviendrait également.

```
# dump -L -0 -f- / |(cd /mnt && restore -r -v -f-)
```

Cela doit être effectué pour chaque système de fichiers. Placez simplement le système de fichiers approprié au bon endroit quand vous exécutez la commande précédente.

Editez ensuite le fichier /mnt/etc/fstab et supprimez ou mettez en commentaires le fichier de pagination . Modifiez les autres paramètres du système de fichiers pour utiliser le nouveau disque comme présenté l'exemple suivant:

```
# Device                Mountpoint      FStype  Options         Dump    Pass#
#/dev/da0s2b             none            swap    sw              0       0
/dev/mirror/gm0s1a       /               ufs     rw              1       1
```

Créez maintenant un fichier boot.config sur la partition racine actuelle et celle nouvellement créée. Ce fichier "aidera" le BIOS à déterminer correctement sur quel disque démarrer:

```
# echo "1:da(1,a)/boot/loader" > /boot.config
```

```
# echo "1:da(1,a)/boot/loader" > /mnt/boot.config
```

Nous l'avons ajouter sur les deux partitions racines afin d'assurer un démarrage correct. Si pour une raison quelconque le système ne pourrait le lire à partir de la nouvelle partition racine, une version de secours est disponible.

Assurez-vous que le module geom_mirror.ko sera chargé au démarrage du système en lançant la commande suivante:

```
# echo 'geom_mirror_load="YES"'  /mnt/boot/loader.conf
```

Redémarrez le système:

```
# shutdown -r now
```

Si tout s'est bien passé, le système a dû démarrer à partir du périphérique gm0s1a et une invite d'ouverture de session doit être affichée. En cas de problème, consultez la section suivante consacrée au dépannage. Ajoutez maintenant le disque da0 au périphérique gm0:

```
# gmirror configure -a gm0
# gmirror insert gm0 /dev/da0
```

L'option `-a` demande à gmirror(8) d'utiliser une synchronisation automatique, c'est à dire dupliquer

automatiquement toute écriture disque. La page de manuel explique comment reconstruire et remplacer les disques, avec la différence qu'elle utilise data à la place de gm0.

20.4.1. Dépannage

20.4.1.1. Le système refuse de démarrer

Si le démarrage du système s'interrompt à une invite semblable à:

```
ffs_mountroot: can't find rootvp
Root mount failed: 6
mountroot
```

Redémarrez la machine à l'aide du bouton de mise en marche ou de "reset". Au menu de démarrage, sélectionnez la sixième option (6). Le système basculera alors vers une invite du chargeur (loader(8)). Chargez manuellement le module du noyau:

```
OK? load geom_mirror
OK? boot
```

Si cela fonctionne, cela signifie que pour une raison quelconque le module n'a pas été correctement chargé. Ajoutez la ligne:

```
options GEOM_MIRROR
```

dans le fichier de configuration du noyau, recompilez-le puis réinstallez-le. Cela devrait corriger le problème.

20.5. Périphériques réseau "GEOM Gate"

GEOM supporte l'utilisation de périphériques distants, comme les disques durs, les CD-ROMs, les fichiers, etc. via l'utilisation des outils "gate". Ce mécanisme est semblable à NFS.

Pour commencer, un fichier d'export doit être créé. Ce fichier précise qui est autorisé à accéder aux ressources partagées et quel niveau d'accès est offert. Par exemple, pour partager la quatrième tranche du premier disque SCSI, le fichier /etc/gg.exports suivant est adapté:

```
192.168.1.0/24 RW /dev/da0s4d
```

Cette ligne autorisera l'accès au système de fichiers présent sur la partition da0s4d à toutes les machines du réseau local.

Pour exporter ce périphérique, assurez-vous tout d'abord qu'il n'est pas déjà monté et lancez le "démon" ggated(8):

```
# ggated
```

Maintenant pour monter le périphérique sur la machine cliente, tapez les commandes suivantes:

```
# ggatec create -o rw 192.168.1.1 /dev/da0s4d
ggate0
# mount /dev/ggate0 /mnt
```

A partir d'ici, on peut accéder au périphérique par l'intermédiaire du point de montage /mnt.

Il est à noter que toutes ces opérations échoueront si le disque est déjà monté soit sur la machine serveur soit sur tout autre machine du réseau.

Quand le périphérique n'est plus utilisé, il peut être démonté sans risque avec la commande umount(8) de la même manière que pour tout autre disque.

20.6. Ajouter un label à un disque

Lors de l'initialisation du système, le noyau FreeBSD créé les fichiers spéciaux de périphériques à mesure que les périphériques sont détectés. Cette méthode de détection des périphériques soulève quelques problèmes, par exemple que se passe-t-il si un nouveau disque est ajouté par l'intermédiaire de l'interface USB? Il est très probable qu'un disque flash se verra proposer le nom de périphérique da0 et le périphérique original da0 déplacé en da1. Cela sera à l'origine de problèmes de montage des systèmes de fichiers s'ils sont listés dans /etc/fstab, en fait cela pourra tout simplement empêcher le démarrage du système.

Une solution à ce problème est d'"enchaîner" les périphériques SCSI afin que tout nouveau périphérique ajouté sur la carte SCSI se voit assigné un numéro de périphérique non-utilisé. Mais qu'en est-il des périphériques USB qui peuvent remplacer le premier disque SCSI? Cela se produit parce que les périphériques USB sont en général détectés avant la carte SCSI. Une solution est de brancher ces périphériques qu'après le démarrage du système. Une autre méthode serait de n'utiliser qu'un seul disque ATA et de ne jamais lister de périphériques SCSI dans le fichier /etc/fstab.

Une meilleure solution existe. En employant l'utilitaire `glabel`, un administrateur ou un utilisateur peut attribuer un label à chacun de ses disques et utiliser ces labels dans /etc/fstab. Comme `glabel` conserve le label sur le dernier secteur du support concerné, le label persistera après redémarrage du système. En utilisant ce label comme un véritable périphérique, le système de fichiers pourra toujours être monté indépendamment du fichier spécial de périphérique utilisé pour y accéder.

Cela se fait sans préciser qu'un label sera permanent. L'utilitaire `glabel` peut être utilisé pour créer des labels persistants et des labels éphémères. Seul le label persistant sera conservé après redémarrage du système. Consultez la page de manuel de glabel(8) pour plus d'information sur les différences entre labels.

20.6.1. Types et exemples de labels

Il existe deux types de label, un label générique et un label de système de fichiers. La différence entre les labels est le système d'auto-détection associé avec les labels permanents, et le fait que ce type de label sera persistant après redémarrage du système. A ces labels est attribué un sous-répertoire spécifique de /dev dont le nom sera basé sur le type de système de fichiers. Par exemple, les labels de systèmes de fichiers UFS2 seront créés dans le répertoire /dev/ufs2.

Un label générique disparaîtra au redémarrage suivant. Ces labels seront créés dans le répertoire /dev/label et sont parfaits pour faire des expériences.

Les labels permanents peuvent être placés sur le système de fichiers en utilisant les utilitaires `tunefs` ou `newfs`. Pour créer un label permanent pour un système de fichier UFS2 sans endommager de données, utilisez la commande suivante:

```
# tunefs -L home /dev/da3
```

Si le système de fichiers est plein, cette opération pourra entraîner une corruption des données; si le système de fichiers est plein, alors la première chose à faire sera de supprimer les fichiers inutiles et non pas l'ajout de labels.

Un nouveau label devrait désormais apparaître dans /dev/ufs2 et pourra être ajouté à /etc/fstab:

```
/dev/ufs2/home      /home           ufs     rw              2       2
```

Le système de fichiers ne doit pas être monté lors de l'utilisation de `tunefs`.

Le système de fichiers peut, maintenant, être normalement monté:

```
# mount /home
```

La commande suivante peut être employée pour supprimer le label:

```
# glabel destroy home
```

A partir de cet instant, aussi longtemps que le module du noyau geom_label.ko est chargé au démarrage avec /boot/loader.conf ou que l'option `GEOM_LABEL` est présente dans le noyau, le fichier spécial de périphérique peut changer sans effet négatif pour le système.

Les systèmes de fichiers peuvent également être créés avec un label par défaut en utilisant l'option `-L` avec `newfs`. Consultez la page de manuel de newfs(8) pour plus d'information.

Chapitre 21. The Z File System (ZFS) Traduction en Cours

21.1. What Makes ZFS Different

21.2. Quick Start Guide

21.3. `zpool` Administration

21.4. `zfs` Administration

21.5. Delegated Administration

21.6. Additional Resources

21.7. ZFS Features and Terminology

Chapitre 22. Autres systèmes de fichiers

22.1. Synopsis

Les systèmes de fichiers sont partie intégrante de n'importe quel système d'exploitation. Ils permettent aux utilisateurs de lire et stocker des fichiers, de donner accès aux données, et rendre utiles les disques durs. Les systèmes d'exploitation diffèrent par leur système de fichiers natifs. Traditionnellement, le système de fichiers natif de FreeBSD était l'*Unix File System* UFS qui a été modernisé sous le nom UFS2. Depuis la version FreeBSD 7.0, le système de fichiers Z ou *Z File System* (ZFS) est également disponible en tant que système de fichiers natif. Consultez The Z File System (ZFS) pour plus d'information.

En plus de ses systèmes de fichiers natifs, FreeBSD supporte une multitude d'autres systèmes de fichiers donnant ainsi un accès local aux données d'autres systèmes d'exploitation, comme les données présentes sur des périphériques USB, les disques flash et des disques durs. Cela comprend également le support pour le système de fichiers étendu de Linux® ou *Extended File System* (EXT).

Il y a différents niveaux de support de FreeBSD pour les différents systèmes de fichiers. Certains nécessitent le chargement d'un module du noyau et d'autres l'installation d'un ensemble d'outils. Le support de certains systèmes de fichiers est complet en lecture et en écriture alors que pour d'autres il est limité à la lecture.

Après la lecture de ce chapitre, vous connaîtrez:

- La différence entre les systèmes de fichiers natifs et supportés.
- Quels systèmes de fichiers sont supporté par FreeBSD.
- Comment activer, configurer, accéder, et utiliser des systèmes de fichiers non-natifs.

Avant de lire ce chapitre, vous devez:

- Comprendre UNIX® et les bases de FreeBSD.
- Etre familier avec les bases de la configuration et compilation du noyau.
- Etre à l'aise avec l'installation de logiciels sous FreeBSD.
- Avoir quelques connaissances sur les disques, les stockage de données, et les noms de périphériques sous FreeBSD.

22.2. Systèmes de fichiers Linux®

FreeBSD offre un support intégré pour plusieurs systèmes de fichiers Linux®. Cette section montre comment charger le support et comment monter les systèmes de fichiers Linux® supportés.

22.2.1. ext2

Le support du noyau pour les systèmes de fichiers ext2 est disponible depuis FreeBSD 2.2. Sous FreeBSD 8.X et versions antérieures, le code était sous licence GPL. Depuis FreeBSD 9.0, le code a été récrit et est désormais sous licence BSD.

Le pilote ext2fs(5) permet au noyau FreeBSD de lire et écrire sur les systèmes de fichiers ext2.

Ce pilote peut également être utilisé pour accéder à des systèmes de fichiers ext3 et ext4. Le système de fichiers ext2fs(5) supporte complètement l'écriture et la lecture de systèmes de fichiers ext4 à partir de FreeBSD 12.0-RELEASE. De plus, les attributs étendus et les ACLs sont également supportés, mais ce n'est pas le cas de la journalisation et du chiffrement. A partir de FreeBSD 12.1-RELEASE, le support DTrace sera aussi disponible. Les versions de FreeBSD antérieures peuvent accéder à de l'ext4 en lecture et en écriture en utilisant sysutils/fusefs-ext2.

Pour accéder à un système de fichiers ext, tout d'abord chargez le module du noyau:

```
# kldload ext2fs
```

Puis, montez le volume ext en indiquant son nom de partition sous FreeBSD et un point de montage. Cette exemple monte /dev/ad1s1 sur /mnt:

```
# mount -t ext2fs /dev/ad1s1 /mnt
```

Chapitre 23. Le gestionnaire de volume Vinum

23.1. Synopsis

Peu importe les disques dont vous disposez, ils seront toujours limités:

- Ils pourront être trop petits.
- Ils pourront être trop lents.
- Ils pourront être peu fiables.

23.2. Les disques sont trop petits

Vinum est un *gestionnaire de volume*, un pilote de disque virtuel qui permet de résoudre ces trois problèmes. Regardons-les plus en détails. De nombreuses solutions à ces problèmes ont été proposées et implémentées:

Les disques deviennent de plus en plus gros, mais tout comme les besoins en stockage. Vous vous apercevrez souvent que vous avez besoin d'un système de fichiers plus grand que les disques que vous avez à votre disposition. Bien évidemment, ce problème n'est plus aussi aigu qu'il l'était il y a de cela dix ans, mais il existe toujours. Certains systèmes l'ont résolu en créant un périphérique abstrait qui stocke ses données sur plusieurs disques.

23.3. Les goulots d'étranglement d'accès aux données

Les systèmes modernes ont fréquemment besoin d'accéder aux données d'une manière hautement concourante. Par exemple, d'importants serveurs FTP ou HTTP peuvent supporter des milliers de sessions concourantes et avoir de multiple connexions à 100 Mbit/s vers le monde extérieur, et cela bien au-delà du taux de transfert soutenu de la plupart des disques.

Les disques actuels peuvent effectuer des transfert séquentiels de données jusqu'à une vitesse de 70 MO/s, mais ce chiffre a peu d'importance dans un environnement où plusieurs processus indépendants accèdent à un disque, où l'on pourra n'atteindre qu'une fraction de cette valeur. Dans de tels cas il est plus intéressant de voir le problème du point de vue du sous-système des disques: le paramètre important est la charge que provoque un transfert sur le sous-système, en d'autres termes le temps d'occupation du disque impliqué dans le transfert.

Dans n'importe quel transfert, le disque doit tout d'abord positionner les têtes de lecture, attendre le passage du premier secteur sous la tête de lecture, puis effectuer le transfert. Ces actions peuvent être considérées comme étant atomiques: cela n'a aucun sens de les interrompre.

Considérons un transfert typique d'environ 10 KO: la génération actuelle de disques hautes performances peuvent positionner leurs têtes en environ 3.5 ms. Les disques les plus véloces tournent à 15000 tr/minute, donc le temps de latence moyen de rotation (un demi-tour) est de 2 ms. A 70 MO/s, le transfert en lui-même prend environ 150 µs, presque rien comparé au temps de

positionnement. Dans un tel cas, le taux de transfert effectif tombe à un peu plus de 1 MO/s et est clairement hautement dépendant de la taille du transfert.

La solution classique et évidente à ce goulot d'étranglement est "plus de cylindres": plutôt que d'utiliser un gros disque, on utilise plusieurs disques plus petits avec le même espace de stockage. Chaque disque est en mesure d'effectuer un transfert indépendamment des autres, aussi le taux de sortie augmente d'un facteur proche du nombre de disques utilisés.

L'amélioration du taux réel de sortie est, naturellement, inférieure au nombre de disques impliqués: bien que chaque disque soit capable de transférer en parallèle, il n'y a aucun moyen de s'assurer que les requêtes sont distribuées équitablement entre les disques. Inévitablement la charge d'un disque sera plus importante que celle d'un autre.

La répartition de la charge sur les disques dépend fortement de la manière dont les données sont partagées entre les disques. Dans la discussion suivant, il sera pratique de penser au stockage disque en tant qu'un grand nombre de secteurs qui sont adressables par l'intermédiaire d'un nombre, plutôt que comme les pages d'un livre. La méthode la plus évidente est de diviser le disque virtuel en groupes de secteurs consécutifs de taille égale aux disques physiques individuels et de les stocker de cette manière, plutôt que de les prendre comme un gros livre et de le déchirer en petites sections. Cette méthode est appelée *concaténation* et a pour avantage que les disques n'ont pas besoin d'avoir de rapport spécifique au niveau de leur taille respective. Cela fonctionne bien quand l'accès au disque virtuel est réparti de façon identique sur son espace d'adressage. Quand l'accès est limité à une petite zone, l'amélioration est moins marquée. Organisation par concaténation décrit la séquence dans laquelle les unités sont assignées dans une organisation par concaténation.

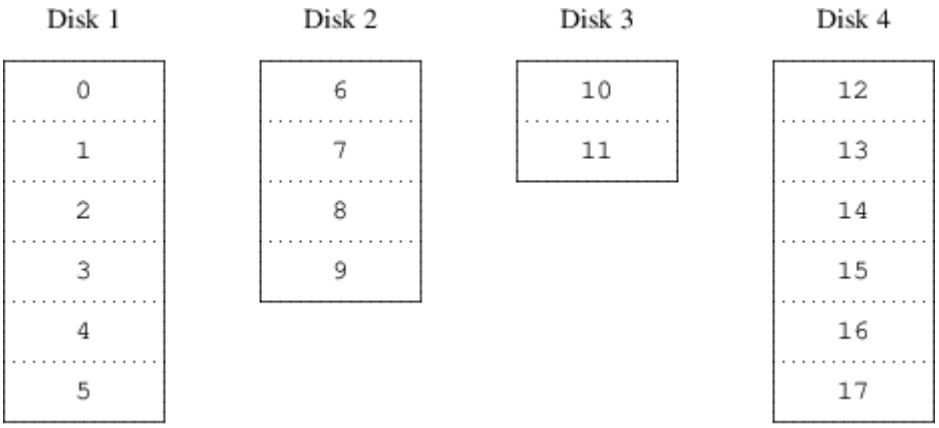


Figure 61. Organisation par concaténation

Une organisation alternative est de diviser l'espace adressable en composants plus petits, de même taille et de les stocker séquentiellement sur différents périphériques. Par exemple, les 256 premiers secteurs peuvent être stockés sur le premier disque, les 256 secteurs suivants sur le disque suivant et ainsi de suite. Après avoir atteint le dernier disque, le processus se répète jusqu'à ce que les disques soient pleins. Cette organisation est appelée *striping* (découpage en bande ou segmentation) ou RAID-0.

La segmentation exige légèrement plus d'effort pour localiser les données, et peut causer une charge additionnelle d'E/S quand un transfert est réparti sur de multiples disques, mais il peut également fournir une charge plus constante sur les disques. Organisation segmentée illustre l'ordre dans lequel les unités de stockage sont assignées dans une organisation segmentée.

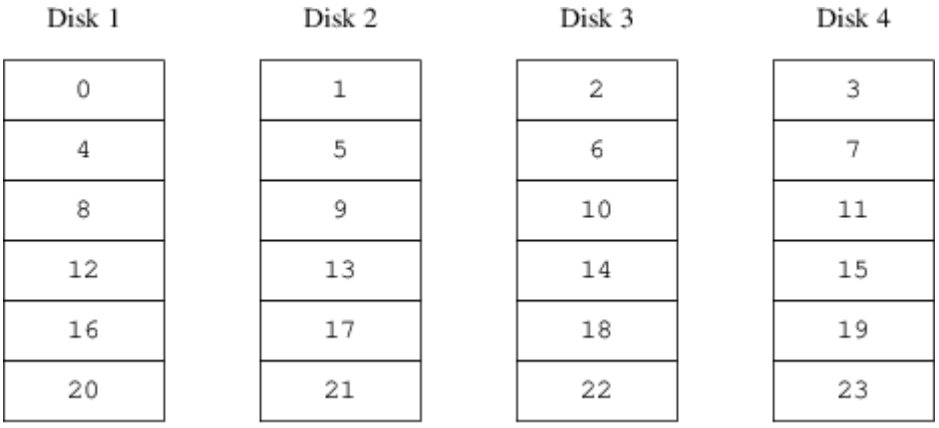


Figure 62. Organisation segmentée

23.4. Intégrité des données

Le dernier problème avec les disques actuels est qu'ils ne sont pas fiables. Bien que la fiabilité des disques s'est énormément améliorée depuis quelques années, ils sont toujours le composant principal d'un serveur le plus susceptible de tomber en panne. Et quand cela arrive, les résultats peuvent être catastrophiques: remplacer un disque en panne et restaurer les données peut prendre plusieurs jours.

La méthode originelle d'approche de ce problème fut le mode *miroir*, en conservant deux copies des données sur un matériel différent. Depuis l'avènement de la technologie RAID, cette technique est également nommée RAID niveau 1 ou RAID-1. Toute opération d'écriture sur le volume écrit sur les deux unités; une lecture peut être acquittée par l'une ou l'autre, aussi si l'un des disque tombe en panne, les données sont toujours accessibles sur l'autre disque.

Le mode miroir présente deux problèmes:

- Le prix. Il demande au moins deux fois autant d'espace disque qu'une solution non-redondante.
- L'impact sur la performance. Les écritures doivent être effectuées sur les deux disques, elles prennent donc deux fois plus de bande passante que sur un volume sans miroir. Les lectures de souffrent pas de baisse de performance: elles semblent même plus rapides.

Une alternative est l'utilisation de la *parité*, implémentée sous les niveaux RAID 2, 3, 4 et 5. De ces niveaux RAID-5 est le plus intéressant. Comme implémenté dans Vinum, c'est une variante de l'organisation segmentée qui dédie un bloc de chaque segment à la parité des autres blocs. Comme implémenté dans Vinum, un volume RAID-5 est identique à un volume segmenté, sauf qu'il implémente RAID-5 en incluant un bloc de parité dans chaque unité. Comme l'exige RAID-5, l'emplacement de ce bloc de parité varie d'une unité à l'autre. Le nombre de blocs de données indique le nombre relatif de blocs.

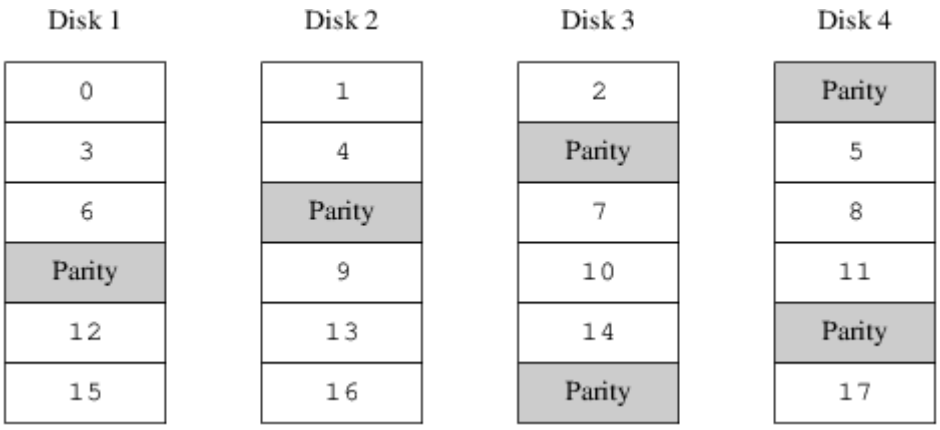


Figure 63. Organisation RAID-5

Comparé au mode miroir, RAID-5 a pour avantage de demander un espace de stockage significativement plus faible. L'accès en lecture est semblable à celui de l'organisation segmentée, mais l'accès en écriture est bien plus lent, approximativement 25% des performances en lecture. Si un disque tombe en panne, l'ensemble peut continuer à fonctionner dans un mode dégradé: une lecture sur un disque restant accessible se poursuit normalement, mais une lecture du disque perdu est recalculée à partir du bloc correspondant sur l'ensemble des disques restants.

23.5. Objets Vinum

Afin de résoudre ces problèmes, Vinum implémente une hiérarchie d'objets à quatre niveaux:

- L'objet le plus visible est le disque virtuel, appelé *volume*. Les volumes ont essentiellement les mêmes propriétés qu'un disque UNIX™, bien qu'il y ait quelques différences mineures. Ils n'ont aucune limitation de taille.
- Les volumes sont composés de *plexes*, chacune d'entre elles représente l'ensemble de l'espace d'adressable d'un volume. Ce niveau dans la hiérarchie permet ainsi la redondance. Pensez aux plexes comme différents disques dans un ensemble miroir, chacun contenant les mêmes données.
- Comme Vinum existe dans le système de stockage disque d'UNIX™, il serait possible d'utiliser les partitions UNIX™ pour construire des blocs pour des plexes à disques multiples, mais en fait cela ne serait pas suffisamment flexible: les disques UNIX™ ne peuvent avoir qu'un nombre limités de partitions. Au lieu de cela Vinum subdivise une simple partition UNIX™ (le *disque*) en zones contiguës appelées *sous-disques*, qui sont utilisés comme bloc pour construire les plexes.
- Les sous-disques résident sur le *disque* Vinum, en fait les partitions UNIX™. Les disques Vinum peuvent contenir un nombre quelconque de sous-disque. A l'exception d'une petite zone au début du disque, qui est utilisée pour stocker les informations de configuration et d'état, l'intégralité du disque est disponible pour le stockage des données.

Les sections suivantes décrivent la façon dont ces objets fournissent les fonctionnalités requises pour Vinum.

23.5.1. Considérations sur la taille des volumes

Les plexes peuvent comprendre de multiple sous-disques répartis sur tous les disques dans la configuration Vinum. Par conséquent, la taille d'un disque ne limite pas la taille d'une plex, et donc

d'un volume.

23.5.2. Stockage de données redondant

Vinum implémente le mode miroir en attachant de multiples plexes à un volume. Un volume peut contenir entre une et huit plexes.

Bien qu'une plex représente les données complètes d'un volume, il est possible que des parties de la représentation soient physiquement manquantes, soit en raison de la mise en place (en définissant un sous-disque comme ne faisant pas partie de la plex) ou par accident (en raison de la panne d'un disque). Tant qu'au moins une plex peut fournir les données de l'intégralité de la plage d'adresse d'un volume, le volume est totalement fonctionnel.

23.5.3. Problèmes de performance

Vinum implémente la concaténation et la segmentation au niveau de la plex:

- Une *plex concaténée* utilise alternativement l'espace d'adresse de chaque sous-disque.
- Une *plex segmentée* segmente les données sur chaque sous-disque. Les sous-disques doivent avoir la même taille, et il doit y avoir au moins deux sous-disques pour distinguer la plex d'une plex concaténée.

23.5.4. Quelle organisation de plex?

La version de Vinum fournie avec FreeBSD 12.0 implémente deux type de plexes:

- Les plexes concaténées sont les plus flexibles: elles peuvent contenir un nombre quelconque de de sous-disques, et les sous-disques peuvent être de taille différentes. La plex peut être étendue en ajoutant des sous-disques supplémentaires. Elles demandent moins de temps CPU que les plexes segmentées, bien que la différence en charge CPU ne soit pas mesurable. D'autre part, elles sont plus susceptibles d'échauffement, là où un disque est très actif et les autres sont au repos.
- Le plus grand avantage des plexes segmentées (RAID-0) est qu'elles réduisent les problèmes d'échauffement: en choisissant tailles de segments optimales (environ 256 KO), vous pouvez également réduire la charge des disques. Les inconvénients de cette approche sont un code (infimement) plus complexe et des restrictions sur les sous-disques: ils doivent être de la même taille, et agrandir une plex en ajoutant de nouveaux sous-disques est si complexe que Vinum ne l'implémente pas actuellement. Vinum impose une restriction triviale supplémentaire: une plex segmentée doit avoir au moins deux sous-disques, puisque sinon elle ne serait distinguable d'une plex concaténée.

Organisations de plex Vinum résume les avantages et inconvénients de chaque type d'organisation de plex.

Tableau 7. Organisations de plex Vinum

Type de plex	Nombre minimal de sous-disques	Possibilité d'ajout de sous-disques	Doivent être de même taille	Application
concaténée	1	oui	non	Stockage de grandes quantités de données avec le maximum de flexibilité en terme de placement et des performances modérées
segmentée	2	non	oui	Haute performance combinée avec un accès hautement concourant

23.6. Quelques exemples

Vinum maintient une *base de données de configuration* qui décrit les objets connus pour un système individuel. Initialement, l'utilisateur créé la base de données de configuration à partir d'un ou plusieurs fichiers de configuration avec l'aide de l'utilitaire vinum(8). Vinum conserve une copie de sa base de données de configuration sur chaque tranche (que Vinum nomme *device*) sous son contrôle. Cette base données est mise à jour à chaque changement d'état, aussi un redémarrage reconstitue exactement l'état de chaque objet Vinum.

23.6.1. Le fichier de configuration

Le fichier de configuration décrit les objets Vinum. La définition d'un simple volume pourrait être:

```
drive a device /dev/da3h
volume myvol
  plex org concat
    sd length 512m drive a
```

Ce fichier décrit quatre objets Vinum:

- La ligne *drive* une partition disque (*drive*) et son emplacement relatif par rapport au matériel sous-jacent. On lui donne le nom symbolique *a*. Cette séparation entre le nom symbolique et le nom du périphérique permet aux disques d'être déplacés d'un emplacement à un autre sans confusion possible.
- La ligne *volume* décrit un volume. Le seul attribut nécessaire est le nom, dans notre cas *myvol*.
- La ligne *plex* définit une plex. Le seul paramètre requit est l'organisation, dans ce cas *concat*. Aucun nom n'est nécessaire: le système génère automatiquement un nom à partir du nom de

volume en ajoutant le suffixe *.px*, où *x* est le nombre de plexes dans le volume. Donc cette plex sera appelée *myvol.p0*.

- La ligne *sd* décrit un sous-disque. Les spécifications minimales sont le nom du disque sur lequel le stocker et la taille du sous-disque. Comme pour les plexes, aucun nom n'est nécessaire: le système assignera automatiquement des noms dérivés du nom de la plex en ajoutant le suffixe *.sx*, où *x* est le nombre de sous-disques dans la plex. Donc Vinum donnera le nom *myvol.p0.s0* à ce sous-disque.

Après avoir traité ce fichier vinum(8) affiche ce qui suit:

```
      #  vinum - create config1
      Configuration summary
      Drives:         1 (4 configured)
      Volumes:        1 (4 configured)
      Plexes:         1 (8 configured)
      Subdisks:       1 (16 configured)

    D a                   State: up       Device /dev/da3h        Avail: 2061/2573
MB (80%)

    V myvol               State: up       Plexes:       1 Size:        512 MB

    P myvol.p0          C State: up       Subdisks:     1 Size:        512 MB

    S myvol.p0.s0         State: up       PO:        0  B Size:        512 MB
```

Cette sortie affiche une brève liste du format vinum(8). Elle est représentée graphiquement dans Un simple volume Vinum.

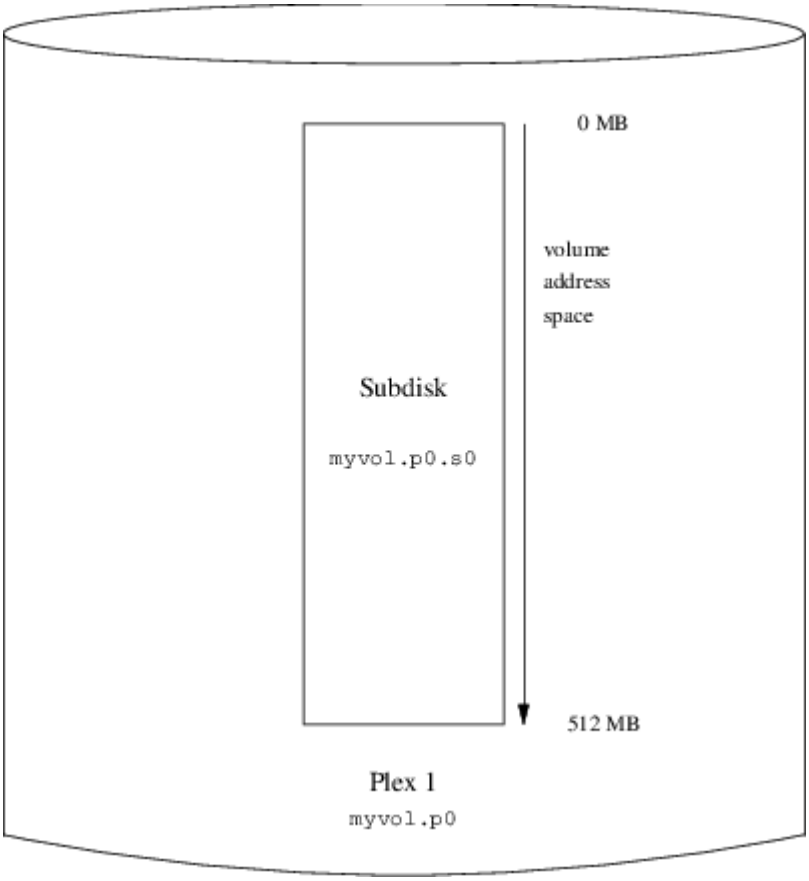


Figure 64. Un simple volume Vinum

Cette figure, et celles qui suivent, représentent un volume qui contient les plexes, qui à leur tour contiennent les sous-disques. Dans cet exemple trivial, le volume contient une plex, et la plex contient un sous-disque.

Ce volume particulier ne présente aucun avantage spécifique par rapport à une partition de disque conventionnelle. Il contient une seule plex, donc il n'est pas redondant. La plex contient un seul sous-disque, il n'y a donc pas de différence dans l'organisation du stockage des données par rapport à une partition de disque conventionnelle. Les sections suivantes présenteront diverses méthodes de configuration plus intéressantes.

23.6.2. Robustesse accrue: le mode miroir

La robustesse d'un volume peut être augmentée par le mode miroir. Quand on implémente un volume en mode miroir, il est important de s'assurer que les sous-disques de chaque plex sont sur des disques différents, de sorte qu'une panne disque ne mette hors service les deux plexes. La configuration suivante place en mode miroir un volume:

```
drive b device /dev/da4h
volume mirror
  plex org concat
    sd length 512m drive a
  plex org concat
    sd length 512m drive b
```

Dans cet exemple, il n'était pas nécessaire de spécifier une définition de disque *a* à nouveau,

puisque Vinum garde trace de tous les objets dans sa base de données de configuration. Après le traitement de cette définition, la configuration ressemble à:

```
    Drives:         2 (4 configured)
    Volumes:        2 (4 configured)
    Plexes:         3 (8 configured)
    Subdisks:       3 (16 configured)

    D a                     State: up       Device /dev/da3h        Avail: 1549/2573
MB (60%)
    D b                     State: up       Device /dev/da4h        Avail: 2061/2573
MB (80%)

    V myvol                 State: up       Plexes:       1 Size:        512 MB
    V mirror                State: up       Plexes:       2 Size:        512 MB

    P myvol.p0            C State: up       Subdisks:     1 Size:        512 MB
    P mirror.p0           C State: up       Subdisks:     1 Size:        512 MB
    P mirror.p1           C State: initializing     Subdisks:     1 Size:        512
MB

    S myvol.p0.s0           State: up       PO:        0  B Size:        512 MB
    S mirror.p0.s0          State: up       PO:        0  B Size:        512 MB
    S mirror.p1.s0          State: empty    PO:        0  B Size:        512 MB
```

Un volume Vinum en mode miroir présente la structure sous forme graphique.

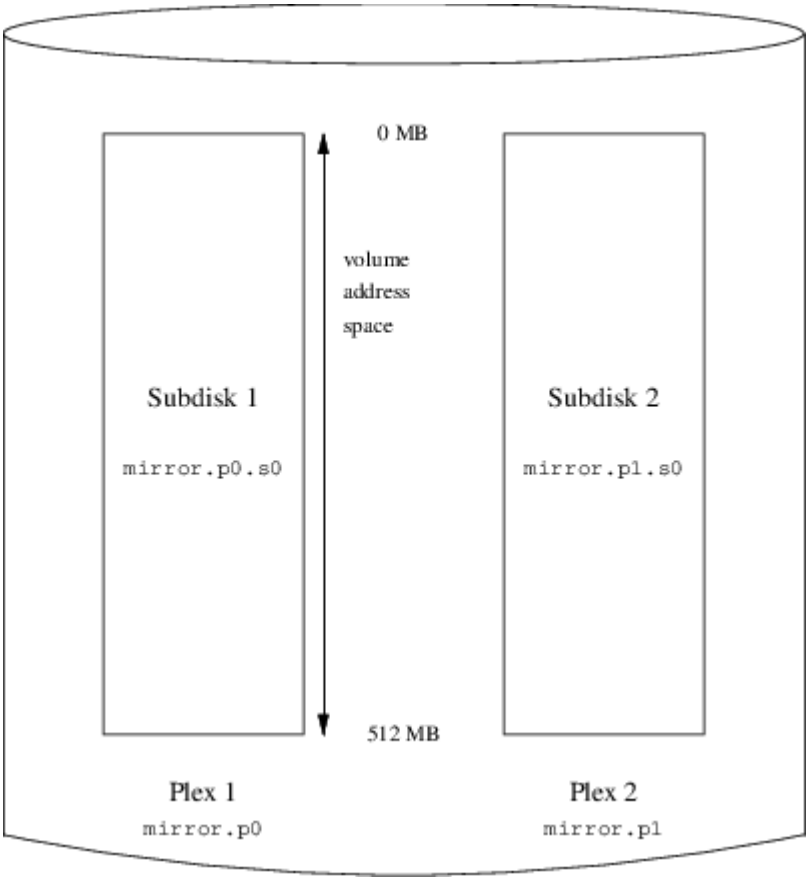


Figure 65. Un volume Vinum en mode miroir

Dans cet exemple, chaque plex contient un espace d'adressage de 512 MO. Comme dans l'exemple précédent, chaque plex contient seulement un seul sous-disque.

23.6.3. Optimiser les performances

Le volume en mode miroir de l'exemple précédent est plus résistant aux pannes qu'un volume sans miroir, mais ses performances sont moindres: chaque écriture sur le volume demande d'écrire sur les deux disques, utilisant alors une plus grande proportion de la bande passante disque totale. Des considérations sur les performances demandent une approche différente: à la place d'un miroir, les données sont segmentées sur autant de disques que possible. La configuration suivante montre un volume avec une plex segmentée sur quatre disques:

```
drive c device /dev/da5h
drive d device /dev/da6h
volume stripe
plex org striped 512k
  sd length 128m drive a
  sd length 128m drive b
  sd length 128m drive c
  sd length 128m drive d
```

Comme précédemment, il n'est pas nécessaire de définir les disques qui sont déjà connus de Vinum. Après traitement de cette définition, la configuration ressemble à:

```
    Drives:         4 (4 configured)
    Volumes:        3 (4 configured)
    Plexes:         4 (8 configured)
    Subdisks:       7 (16 configured)

    D a                     State: up       Device /dev/da3h        Avail: 1421/2573
MB (55%)
    D b                     State: up       Device /dev/da4h        Avail: 1933/2573
MB (75%)
    D c                     State: up       Device /dev/da5h        Avail: 2445/2573
MB (95%)
    D d                     State: up       Device /dev/da6h        Avail: 2445/2573
MB (95%)

    V myvol                 State: up       Plexes:       1 Size:        512 MB
    V mirror                State: up       Plexes:       2 Size:        512 MB
    V striped               State: up       Plexes:       1 Size:        512 MB

    P myvol.p0            C State: up       Subdisks:     1 Size:        512 MB
    P mirror.p0           C State: up       Subdisks:     1 Size:        512 MB
    P mirror.p1           C State: initializing     Subdisks:     1 Size:        512
MB
    P striped.p1            State: up       Subdisks:     1 Size:        512 MB

    S myvol.p0.s0           State: up       PO:        0  B Size:        512 MB
    S mirror.p0.s0          State: up       PO:        0  B Size:        512 MB
    S mirror.p1.s0          State: empty    PO:        0  B Size:        512 MB
    S striped.p0.s0         State: up       PO:        0  B Size:        128 MB
    S striped.p0.s1         State: up       PO:      512 kB Size:        128 MB
    S striped.p0.s2         State: up       PO:     1024 kB Size:        128 MB
    S striped.p0.s3         State: up       PO:     1536 kB Size:        128 MB
```

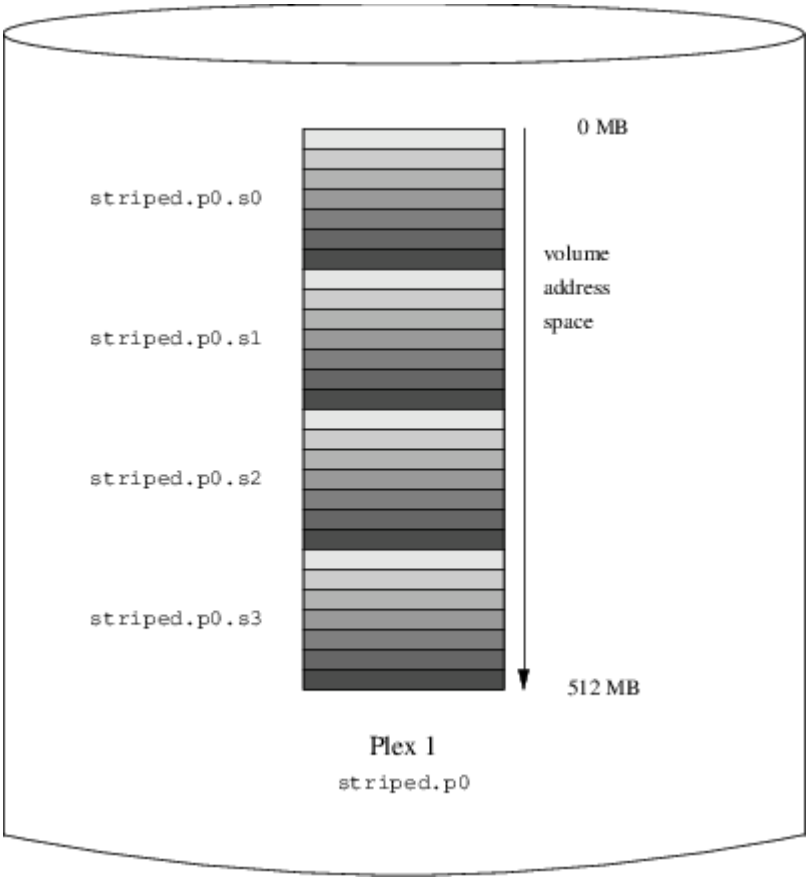


Figure 66. Un volume Vinum segmenté

Ce volume est représenté sur Un volume Vinum segmenté. La couleur des segments indique leur position dans l'espace d'adresses de la plex: le segment le plus clair vient en premier, le plus sombre en dernier.

23.6.4. Robustesse et performances

Avec suffisamment de matériel, il est possible de créer des volumes qui présenteront une robustesse et des performances accrues comparés aux partitions UNIX™ standards. Un fichier de configuration pourrait être:

```
volume raid10
  plex org striped 512k
    sd length 102480k drive a
    sd length 102480k drive b
    sd length 102480k drive c
    sd length 102480k drive d
    sd length 102480k drive e
  plex org striped 512k
    sd length 102480k drive c
    sd length 102480k drive d
    sd length 102480k drive e
    sd length 102480k drive a
    sd length 102480k drive b
```

Les sous-disques de la seconde plex sont décalés de deux disques par rapport à ceux de la première

plex: cela aide à s'assurer que les écritures ne vont pas sur les même sous-disques même si un transfert s'effectue sur les deux disques.

Un volume Vinum en mode miroir segmenté représente la structure de ce volume.

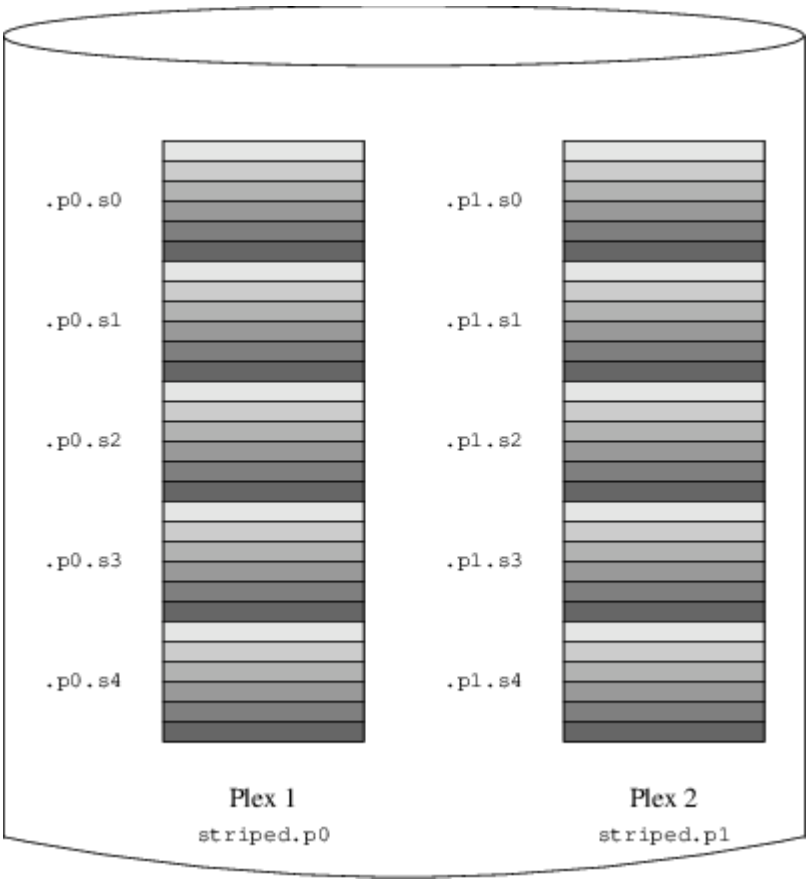


Figure 67. Un volume Vinum en mode miroir segmenté

23.7. Appellation des objets

Comme décrit précédemment, Vinum assigne des noms par défaut aux plexes et aux sous-disques, bien qu'ils peuvent être imposés. Ne pas conserver les noms par défaut n'est pas recommandé: une expérience avec le gestionnaire de volume VERITAS, qui autorise les noms arbitraires pour les objets, a montré que cette flexibilité n'apporte pas d'avantage significatif, et peut être à l'origine de confusion.

Les noms pourront contenir tout caractère non vide, mais il est recommandé de se cantonner aux lettres, chiffres ou le caractère souligné. Les noms de volumes, plexes et sous-disques peuvent contenir jusqu'à 64 caractères, et le nom des disques 32 caractères.

On assigne à chaque objet Vinum un fichier spécial de périphérique dans la hiérarchie /dev/vinum. La configuration présentée plus haut aurait fait à Vinum créer les fichiers spéciaux de périphérique suivants:

- Les périphériques de contrôle /dev/vinum/control et /dev/vinum/controld, qui sont respectivement utilisés par vinum(8)et le "daemon" Vinum.
- Les entrées des périphériques en mode bloc et caractères par chaque volume. Ce sont les périphériques principaux utilisés par Vinum. Les noms de périphériques en mode bloc sont le

nom du volume, alors que les noms de périphériques en mode caractère suivent la tradition BSD de faire précéder le nom de la lettre *r*. Donc la configuration précédent inclurait les périphériques en mode bloc /dev/vinum/myvol, /dev/vinum/mirror, /dev/vinum/striped, /dev/vinum/raid5 et /dev/vinum/raid10, et les périphériques en mode caractères /dev/vinum/rmyvol, /dev/vinum/rmirror, /dev/vinum/rstriped, /dev/vinum/rraid5 et /dev/vinum/rraid10. Un problème évident apparaît ici: il est possible d'avoir deux volumes appelés *r* et *rr*, mais il y aurait un conflit lors de la création du fichier spécial de périphérique /dev/vinum/rr: c'est le périphérique en mode caractère du volume *r* ou le périphérique en mode bloc du volume *rr*? Actuellement Vinum ne résout pas ce conflit: le premier volume défini obtiendra le nom.

- Un répertoire /dev/vinum/drive avec des entrées pour chaque disque. Ces entrées sont en fait des liens symboliques vers les fichiers spéciaux de périphérique de disque correspondants.
- Un répertoire /dev/vinum/volume avec des entrées pour chaque volume. Il contient des sous-répertoires pour chaque plex, qui à leur tour contiennent des sous-répertoires pour leurs sous-disques.
- Les répertoires /dev/vinum/plex, /dev/vinum/sd, et /dev/vinum/rsd, qui contiennent les fichiers spéciaux de périphérique en mode bloc pour chaque plex et les fichiers spéciaux de périphérique en mode bloc et caractère pour chaque sous-disque.

Par exemple, considérons le fichier de configuration suivant:

```
drive drive1 device /dev/sd1h
drive drive2 device /dev/sd2h
drive drive3 device /dev/sd3h
drive drive4 device /dev/sd4h
volume s64 setupstate
  plex org striped 64k
    sd length 100m drive drive1
    sd length 100m drive drive2
    sd length 100m drive drive3
    sd length 100m drive drive4
```

Après traitement de ce fichier, vinum(8) crée la structure suivante dans /dev/vinum:

```
brwx------  1 root  wheel   25, 0x40000001 Apr 13 16:46 Control
brwx------  1 root  wheel   25, 0x40000002 Apr 13 16:46 control
brwx------  1 root  wheel   25, 0x40000000 Apr 13 16:46 controld
drwxr-xr-x  2 root  wheel       512 Apr 13 16:46 drive
drwxr-xr-x  2 root  wheel       512 Apr 13 16:46 plex
crwxr-xr--  1 root  wheel   91,   2 Apr 13 16:46 rs64
drwxr-xr-x  2 root  wheel       512 Apr 13 16:46 rsd
drwxr-xr-x  2 root  wheel       512 Apr 13 16:46 rvol
brwxr-xr--  1 root  wheel   25,   2 Apr 13 16:46 s64
drwxr-xr-x  2 root  wheel       512 Apr 13 16:46 sd
drwxr-xr-x  3 root  wheel       512 Apr 13 16:46 vol

/dev/vinum/drive:
```

```
total 0
lrwxr-xr-x  1 root  wheel  9 Apr 13 16:46 drive1 - /dev/sd1h
lrwxr-xr-x  1 root  wheel  9 Apr 13 16:46 drive2 - /dev/sd2h
lrwxr-xr-x  1 root  wheel  9 Apr 13 16:46 drive3 - /dev/sd3h
lrwxr-xr-x  1 root  wheel  9 Apr 13 16:46 drive4 - /dev/sd4h

/dev/vinum/plex:
total 0
brwxr-xr--  1 root  wheel   25, 0x10000002 Apr 13 16:46 s64.p0

/dev/vinum/rsd:
total 0
crwxr-xr--  1 root  wheel   91, 0x20000002 Apr 13 16:46 s64.p0.s0
crwxr-xr--  1 root  wheel   91, 0x20100002 Apr 13 16:46 s64.p0.s1
crwxr-xr--  1 root  wheel   91, 0x20200002 Apr 13 16:46 s64.p0.s2
crwxr-xr--  1 root  wheel   91, 0x20300002 Apr 13 16:46 s64.p0.s3

/dev/vinum/rvol:
total 0
crwxr-xr--  1 root  wheel   91,   2 Apr 13 16:46 s64

/dev/vinum/sd:
total 0
brwxr-xr--  1 root  wheel   25, 0x20000002 Apr 13 16:46 s64.p0.s0
brwxr-xr--  1 root  wheel   25, 0x20100002 Apr 13 16:46 s64.p0.s1
brwxr-xr--  1 root  wheel   25, 0x20200002 Apr 13 16:46 s64.p0.s2
brwxr-xr--  1 root  wheel   25, 0x20300002 Apr 13 16:46 s64.p0.s3

/dev/vinum/vol:
total 1
brwxr-xr--  1 root  wheel   25,   2 Apr 13 16:46 s64
drwxr-xr-x  3 root  wheel       512 Apr 13 16:46 s64.plex

/dev/vinum/vol/s64.plex:
total 1
brwxr-xr--  1 root  wheel   25, 0x10000002 Apr 13 16:46 s64.p0
drwxr-xr-x  2 root  wheel       512 Apr 13 16:46 s64.p0.sd

/dev/vinum/vol/s64.plex/s64.p0.sd:
total 0
brwxr-xr--  1 root  wheel   25, 0x20000002 Apr 13 16:46 s64.p0.s0
brwxr-xr--  1 root  wheel   25, 0x20100002 Apr 13 16:46 s64.p0.s1
brwxr-xr--  1 root  wheel   25, 0x20200002 Apr 13 16:46 s64.p0.s2
brwxr-xr--  1 root  wheel   25, 0x20300002 Apr 13 16:46 s64.p0.s3
```

Bien qu'il soit recommandé de ne pas donner de nom spécifique aux plexes et sous-disques, les disques Vinum doivent avoir un nom. Cela rend possible de déplacer un disque à un emplacement différent et qu'il soit toujours reconnu automatiquement. Les noms de disques peuvent avoir jusqu'à 32 caractères.

23.7.1. Création de systèmes de fichiers

Les volumes apparaissent pour le système comme des disques, avec une seule exception. Contrairement aux disques UNIX™, Vinum ne partitionne pas les volumes, qui ne contiennent donc pas de table de partitionnement. Cela a demandé de modifier certains utilitaires disque, en particulier newfs(8), qui auparavant tentait d'interpréter la dernière lettre du nom de volume Vinum comme un identifiant de partition. Par exemple, un disque peut avoir un nom comme /dev/ad0a$ ou /dev/da2h. Ces noms représentent respectivement la première partition (a) sur le premier (0) disque IDE (ad) la la huitième partition (h) sur le troisième (2) disque SCSI (da). En revanche, un volume Vinum pourra être appelé /dev/vinum/concat, un nom qui n'a pas de relation avec un nom de partition.

Normalement, newfs(8) interprète le nom du disque et se plaint s'il ne peut le comprendre. Par exemple:

```
# newfs /dev/vinum/concat
newfs: /dev/vinum/concat: can't figure out file system partition
```

Afin de créer un système de fichiers sur ce volume, utilisez l'option -v de newfs(8):

```
# newfs -v /dev/vinum/concat
```

23.8. Configuration de Vinum

Le noyau GENERIC ne contient pas le support Vinum. Il est possible de compiler un noyau spécial qui inclut vinum, mais cela n'est pas recommandé. La méthode standard de lancement de Vinum est d'utiliser un module du noyau (kld). Vous n'avez même pas besoin d'utiliser kldload(8) pour Vinum: quand vous lancez vinum(8), il contrôle si le module a été chargé ou non, si ce n'est pas le cas, il le charge automatiquement.

23.8.1. Démarrage

Vinum stocke l'information de configuration sur les tranches des disques sous la même forme que dans les fichiers de configuration. En lisant à partir de la base de données de configuration, Vinum reconnaît un certain nombre de mots clés qui ne sont pas autorisés dans les fichiers de configuration. Par exemple, une configuration de disque pourrait contenir le texte suivant:

```
volume myvol state up
volume bigraid state down
plex name myvol.p0 state up org concat vol myvol
plex name myvol.p1 state up org concat vol myvol
plex name myvol.p2 state init org striped 512b vol myvol
plex name bigraid.p0 state initializing org raid5 512b vol bigraid
sd name myvol.p0.s0 drive a plex myvol.p0 state up len 1048576b driveoffset 265b
plexoffset 0b
sd name myvol.p0.s1 drive b plex myvol.p0 state up len 1048576b driveoffset 265b
```

```
plexoffset 1048576b
sd name myvol.p1.s0 drive c plex myvol.p1 state up len 1048576b driveoffset 265b
plexoffset 0b
sd name myvol.p1.s1 drive d plex myvol.p1 state up len 1048576b driveoffset 265b
plexoffset 1048576b
sd name myvol.p2.s0 drive a plex myvol.p2 state init len 524288b driveoffset 1048841b
plexoffset 0b
sd name myvol.p2.s1 drive b plex myvol.p2 state init len 524288b driveoffset 1048841b
plexoffset 524288b
sd name myvol.p2.s2 drive c plex myvol.p2 state init len 524288b driveoffset 1048841b
plexoffset 1048576b
sd name myvol.p2.s3 drive d plex myvol.p2 state init len 524288b driveoffset 1048841b
plexoffset 1572864b
sd name bigraid.p0.s0 drive a plex bigraid.p0 state initializing len 4194304b driveoff
set 1573129b plexoffset 0b
sd name bigraid.p0.s1 drive b plex bigraid.p0 state initializing len 4194304b driveoff
set 1573129b plexoffset 4194304b
sd name bigraid.p0.s2 drive c plex bigraid.p0 state initializing len 4194304b driveoff
set 1573129b plexoffset 8388608b
sd name bigraid.p0.s3 drive d plex bigraid.p0 state initializing len 4194304b driveoff
set 1573129b plexoffset 12582912b
sd name bigraid.p0.s4 drive e plex bigraid.p0 state initializing len 4194304b driveoff
set 1573129b plexoffset 16777216b
```

Ici les différences évidentes sont la présence d'une information explicite sur l'emplacement et le nom (les deux sont également autorisés, mais leur utilisation est déconseillée à l'utilisateur) et de l'information sur les états (qui ne sont pas disponibles à l'utilisateur). Vinum ne stocke pas d'informations au sujet des disques dans la configuration: il localise les disques en recherchant les disques configurés pour les partitions dans le label Vinum. Cela permet à Vinum d'identifier correctement les disques même s'ils ont un identifiant de disque UNIX™ différent.

23.8.1.1. Démarrage automatique

Afin de lancer automatiquement Vinum au démarrage du système, assurez-vous d'avoir la ligne suivante dans votre fichier /etc/rc.conf:

```
start_vinum="YES"       # set to YES to start vinum
```

Si vous n'avez pas de fichier /etc/rc.conf, créez en un avec cette ligne. Cela provoquera le chargement du module Vinum au démarrage du système, et le lancement de tout objet mentionné dans la configuration. Cela est fait avant de monter les systèmes de fichiers, il est donc possible d'utiliser automatiquement fsck(8) sur des systèmes de fichiers puis de les monter sur des volumes Vinum.

quand vous démarrez avec la commande `vinum start`, Vinum lit la base de données de configuration à partir d'un des disques Vinum. Dans des circonstances normales, chaque disque contient une copie identique de la base de données de configuration, il importe donc peu quel disque est lu. Après un crash, Vinum doit déterminer quel disque a été mis à jour le plus

récemment et lire la configuration à partir de ce disque. Il met ensuite à jour la configuration si nécessaire à partir de disques progressivement de plus en plus anciens.

Chapitre 24. Virtualisation

24.1. Synopsis

Un logiciel de virtualisation permet l'exécution simultanée de plusieurs systèmes d'exploitation sur la même machine. De tels logiciels pour PCs impliquent l'utilisation d'un système d'exploitation hôte qui exécute le logiciel de virtualisation et qui supporte un certain nombre de systèmes d'exploitation invités.

Après avoir lu ce chapitre, vous connaîtrez:

- La différence entre un système d'exploitation hôte et un système d'exploitation invité.
- Comment installer FreeBSD sur un ordinateur Apple® Macintosh® à base Intel®.
- Comment installer FreeBSD sur Linux® avec Xen™.
- Comment installer FreeBSD sur Microsoft® Windows® avec Virtual PC.
- Comment optimiser un système FreeBSD pour obtenir les meilleures performances en virtualisation.

Avant de lire ce chapitre, vous devrez

- Comprendre les fondements d'UNIX® et de FreeBSD (Quelques bases d'UNIX).
- Savoir comment installer FreeBSD (Installer FreeBSD).
- Savoir comment configurer votre connexion au réseau (Administration réseau avancée).
- Savoir comment installer des logiciels tierce-partie (Installer des applications. les logiciels pré-compilés et les logiciels portés).

24.2. FreeBSD comme système d'exploitation invité

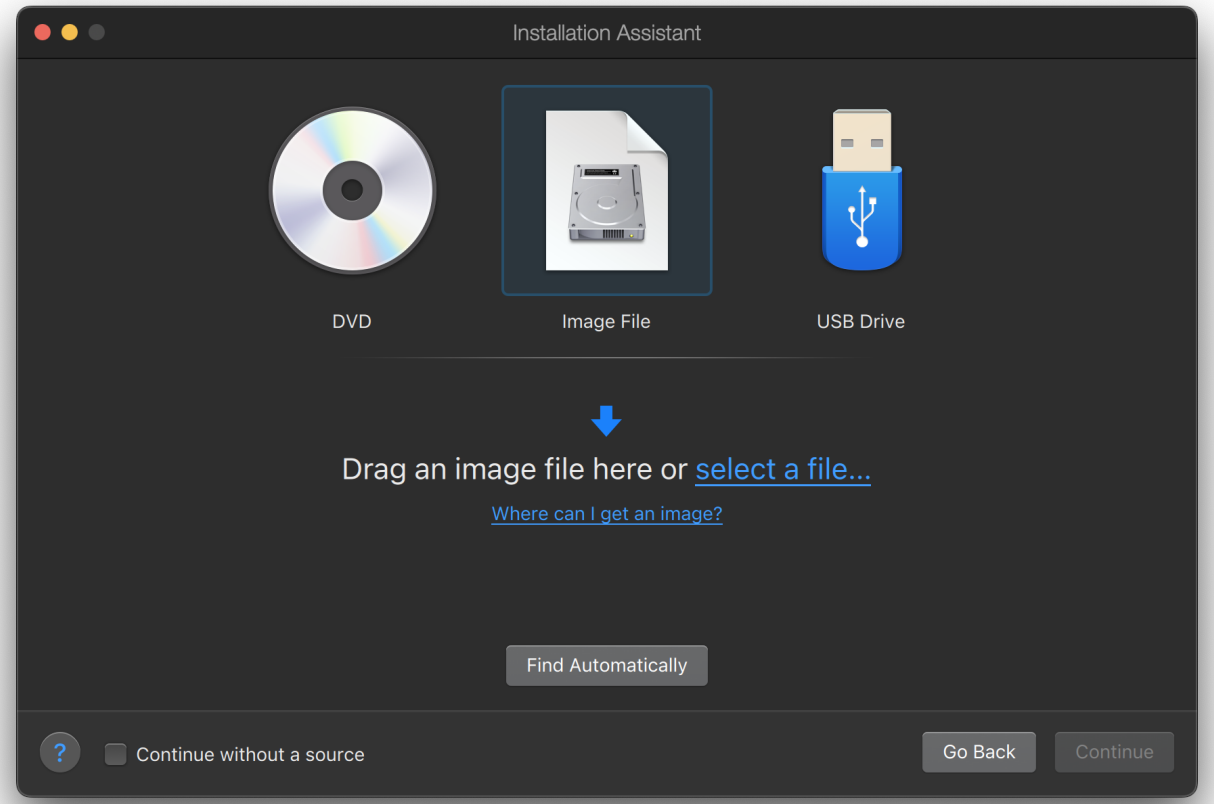
24.2.1. Parallels sur Mac OS®

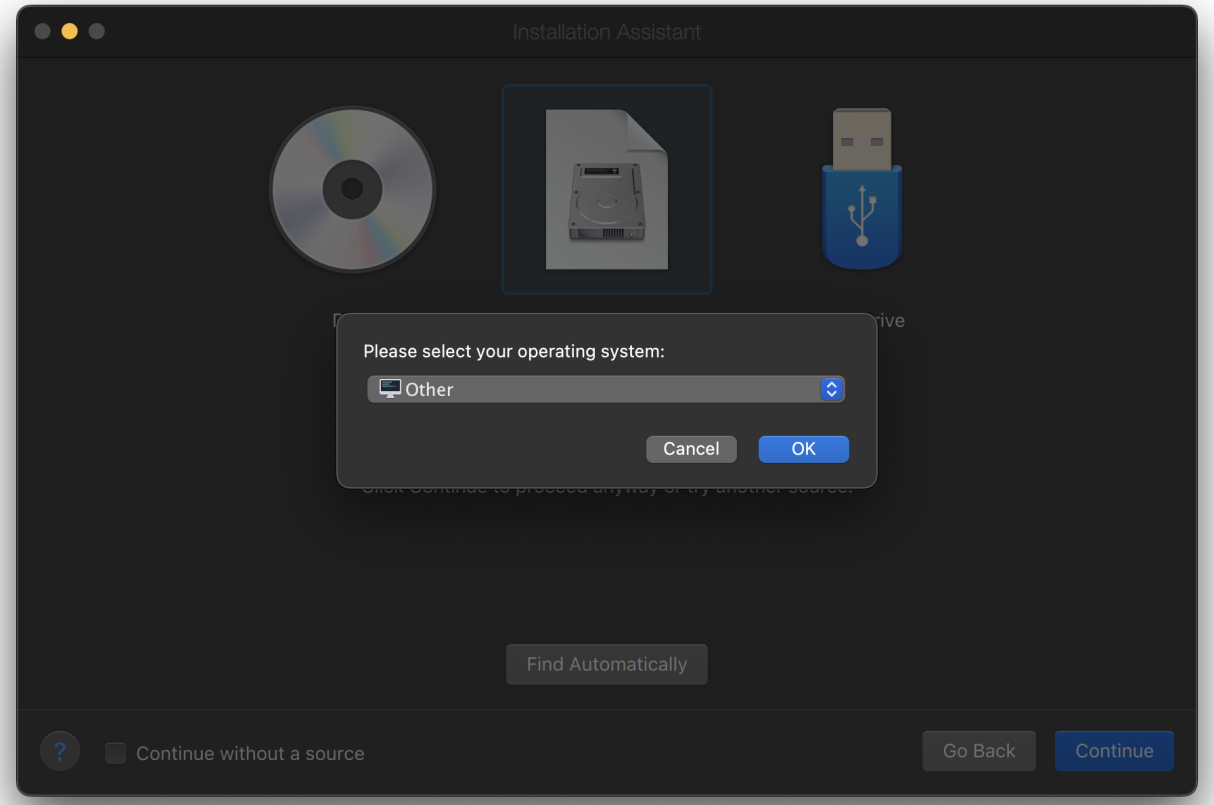
Parallels Desktop pour Mac® est un logiciel commercial pour les ordinateurs Apple® Mac® à base Intel® tournant sous Mac OS® 10.4.6 our versions supérieures. FreeBSD est totalement supporté en tant que système d'exploitation invité. Une fois que Parallels a été installé sur Mac OS® X, l'utilisateur doit configurer une machine virtuelle et installer le système d'exploitation invité qu'il désire.

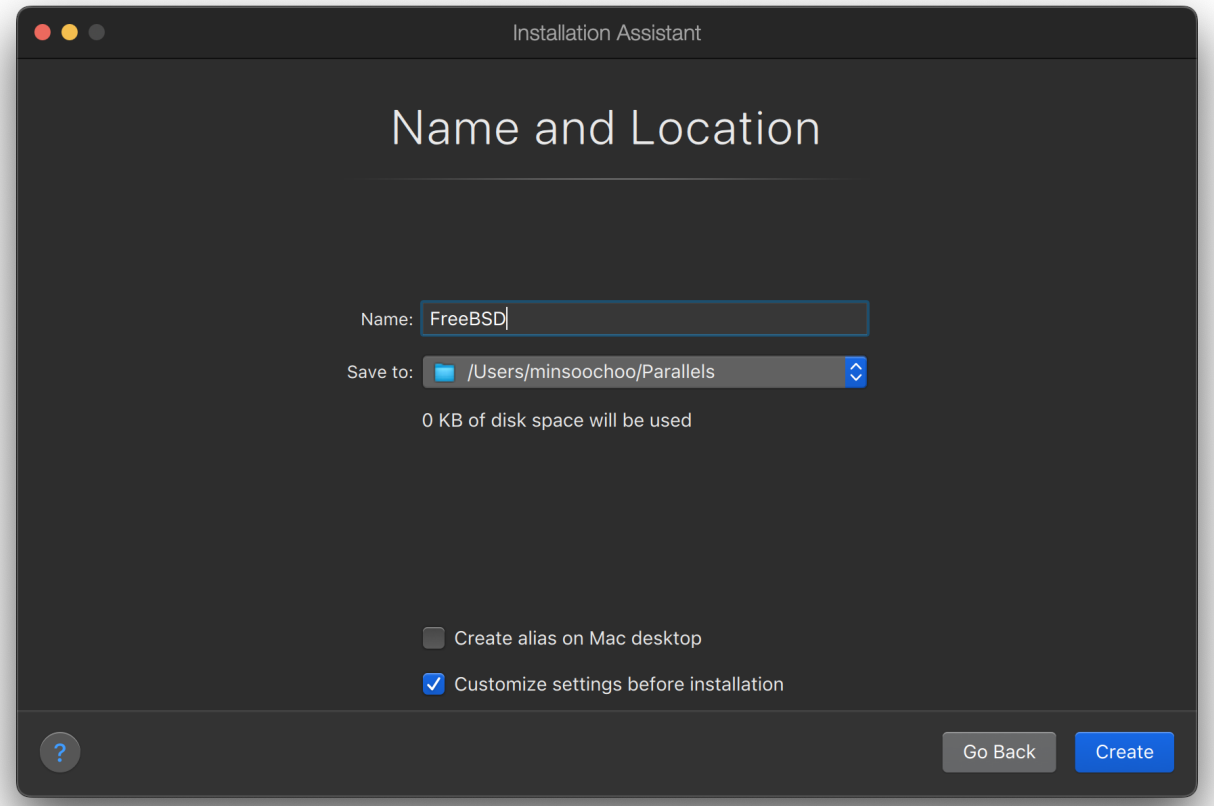
24.2.1.1. Installer FreeBSD sur Parallels/Mac OS® X

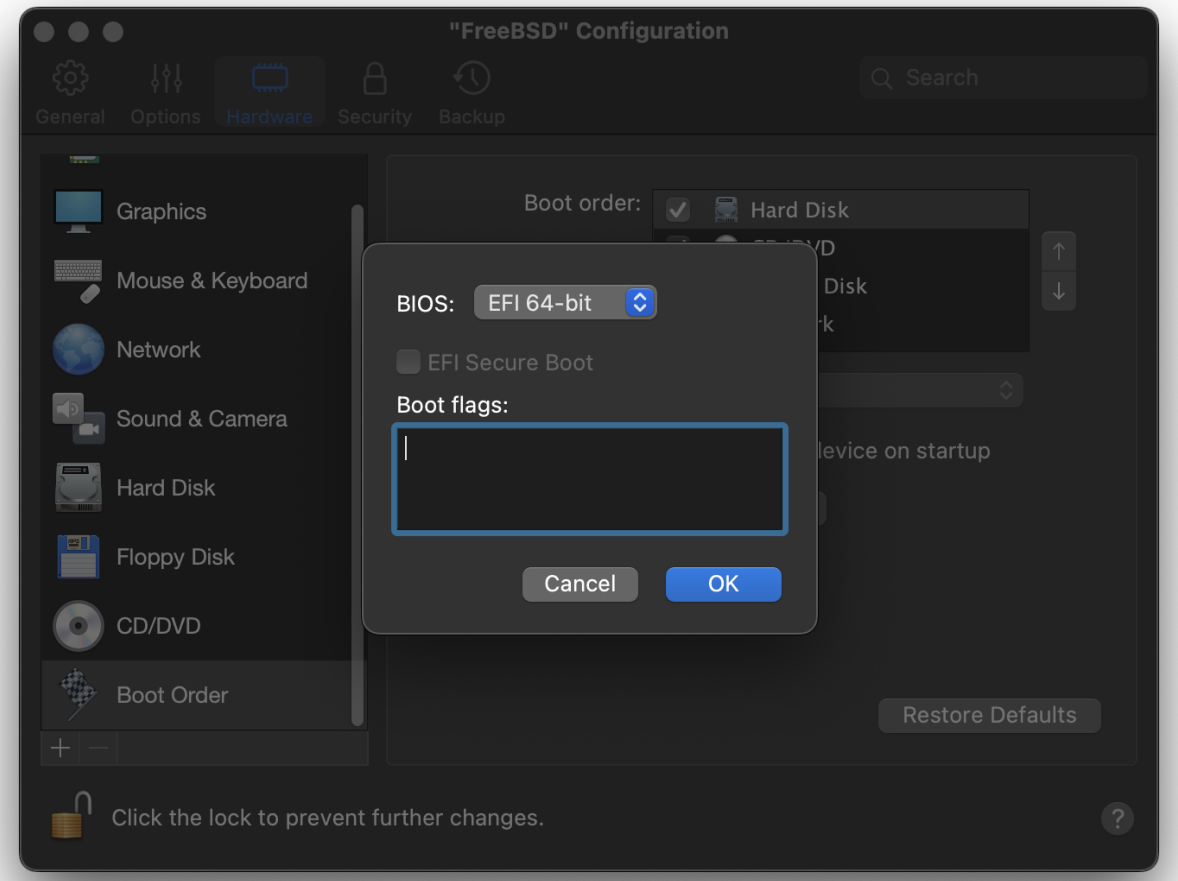
La première étape pour installer FreeBSD sur Mac OS® X/Parallels est de créer une machine virtuelle pour l'installation de FreeBSD. Sélectionnez FreeBSD comme **Système d'exploitation invité** quand on vous le demandera:

Et choisissez une taille de disque dur et de mémoire vive en fonction de l'utilisation que vous projetez pour votre FreeBSD virtuel. 4Go de disque et 512Mo de RAM conviennent pour la plupart des utilisations de FreeBSD sous Parallels:

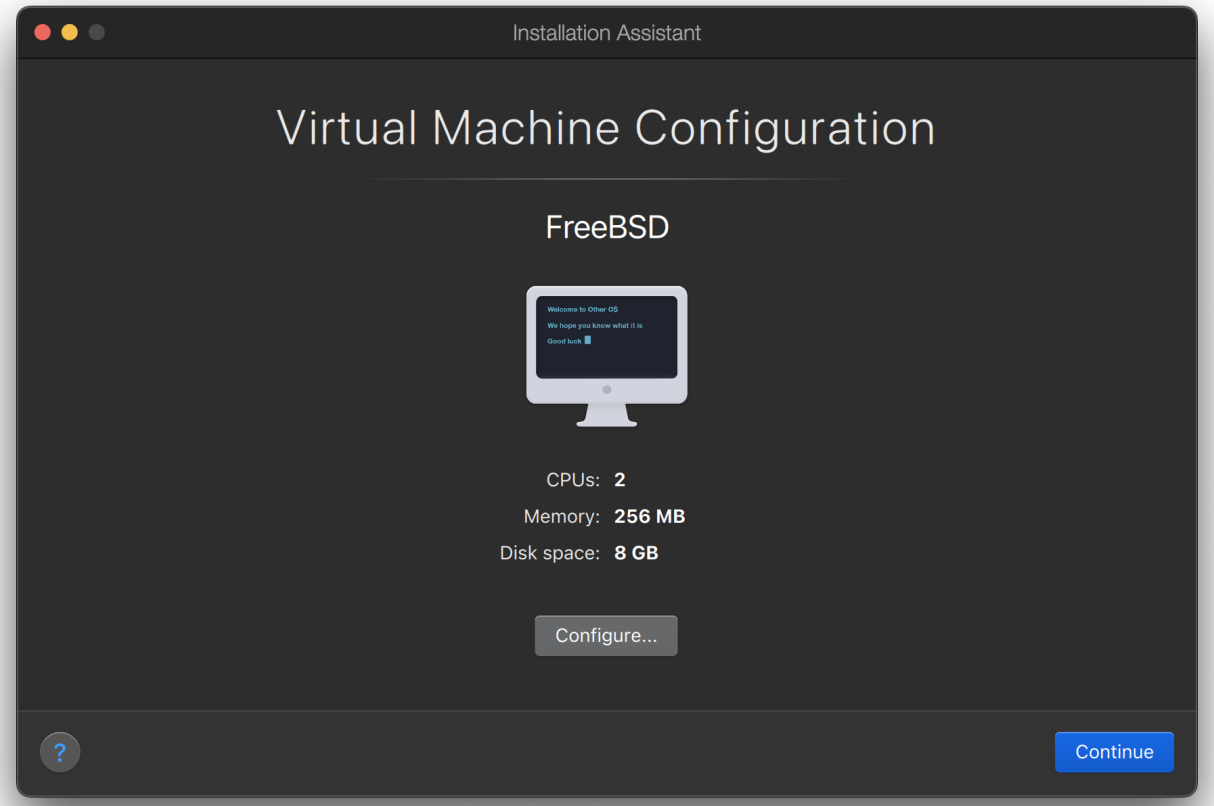

Installation Assistant
DVD
Image File
USB Drive
Drag an image file here or select a file...
Where can I get an image?
Find Automatically
Continue without a source
Go Back
Continue


Installation Assistant
Please select your operating system:
Other
Cancel
OK
Find Automatically
Continue without a source
Go Back
Continue

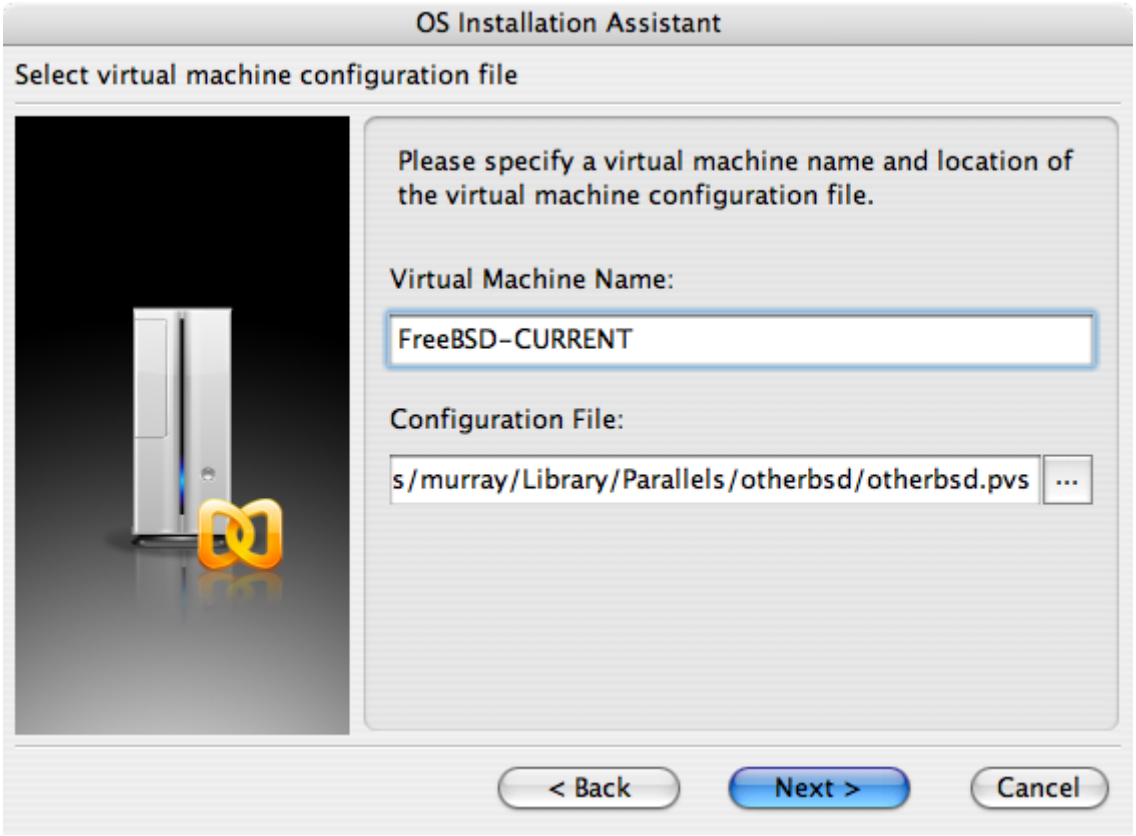

Installation Assistant
Name and Location
Name:
FreeBSD
Save to:
/Users/minsoochoo/Parallels
0 KB of disk space will be used
Create alias on Mac desktop
Customize settings before installation
Go Back
Create

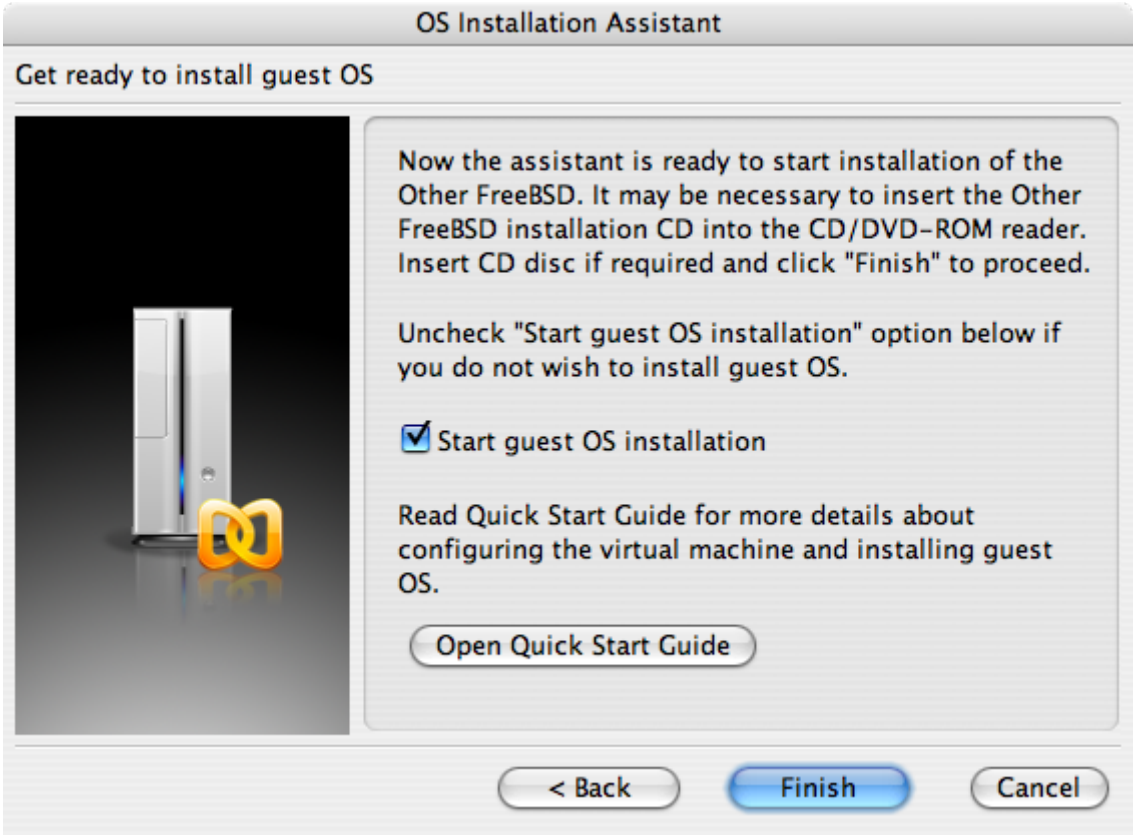


Sélectionnez le type de réseau et une carte réseau:

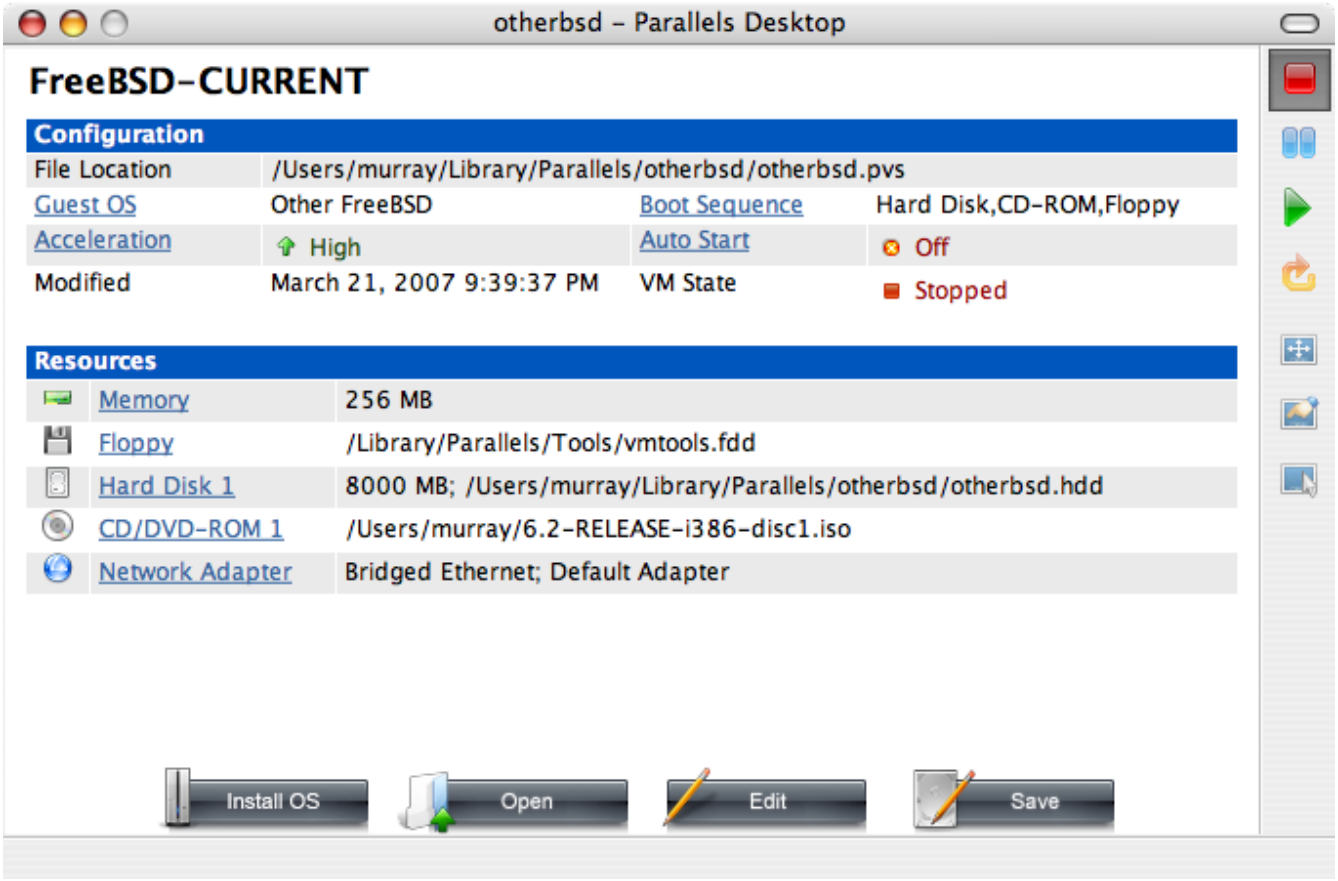

Installation Assistant
Virtual Machine Configuration
FreeBSD
Welcome to Other OS
We hope you know what it is
Good luck
CPUs: 2
Memory: 256 MB
Disk space: 8 GB
Configure...
Continue

Sauvegardez et achevez la configuration:

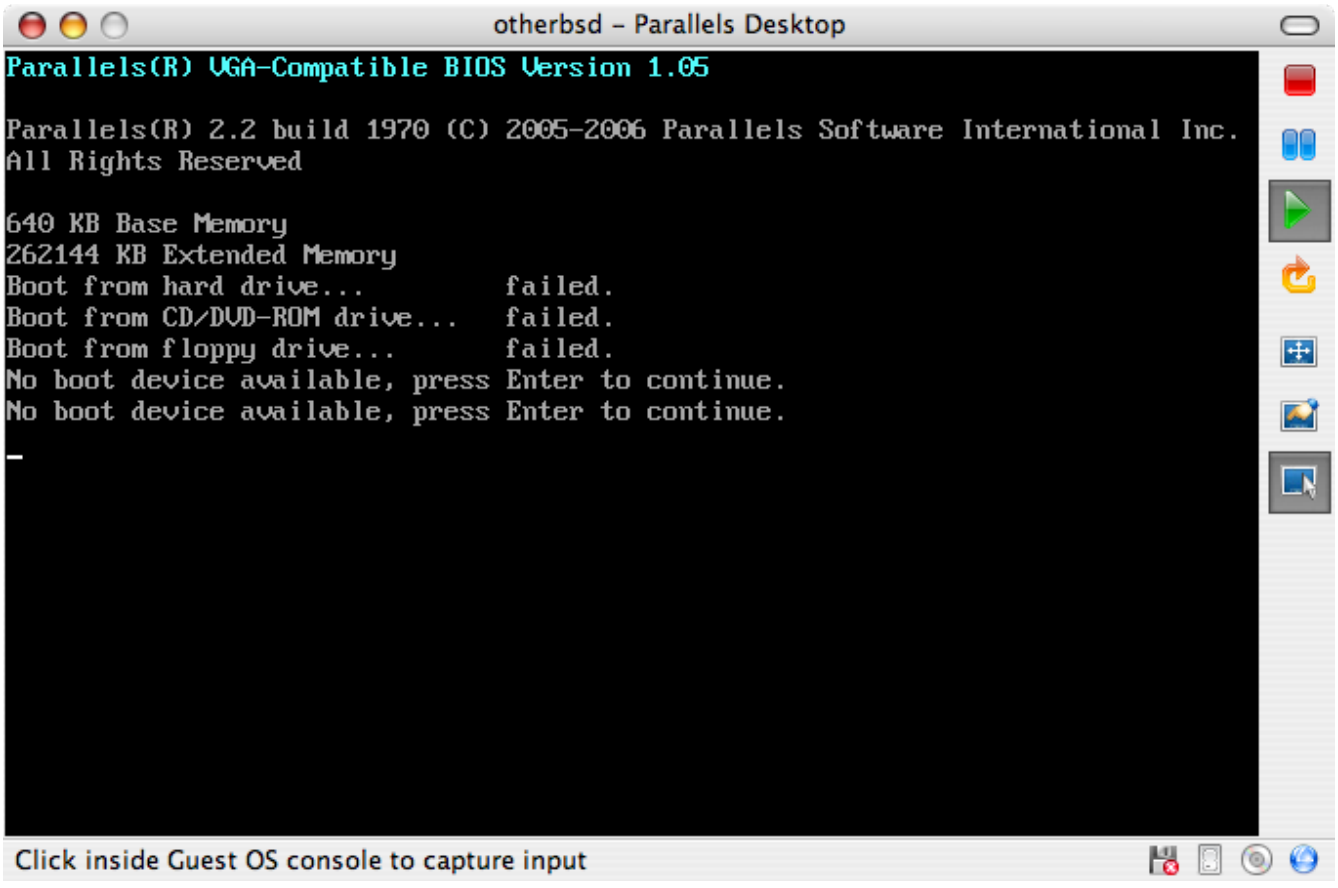




Une fois votre machine virtuelle créée, vous devrez y installer FreeBSD. Le meilleur moyen est d'utiliser un CDROM FreeBSD officiel ou une image ISO récupérée sur un site FTP officiel. Quand vous avez l'image ISO adéquate sur votre système de fichiers Mac® ou un CDROM dans le lecteur de CD du Mac®, cliquez sur l'icône disque située dans le coin droit en bas de votre fenêtre Parallels. Une fenêtre s'ouvrira pour vous permettre d'associer le lecteur de CDROM de votre machine virtuelle avec un fichier ISO ou le véritable lecteur de CDROM de votre ordinateur.

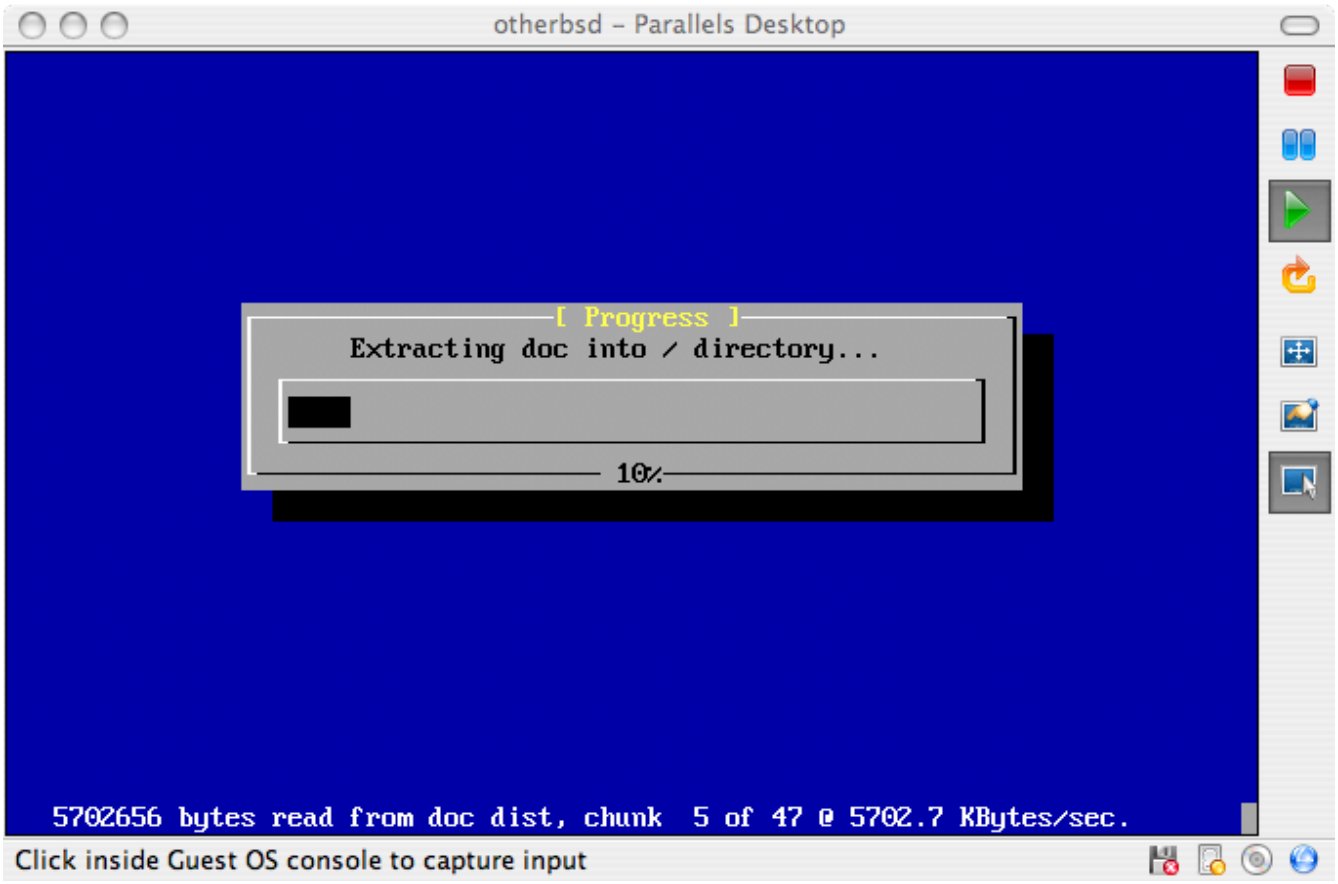


Dès que vous avez effectué cette association, redémarrez votre machine virtuelle FreeBSD en cliquant sur l'icône de redémarrage. Parallels redémarrera avec un BIOS particulier qui vérifiera si vous disposez d'un CDROM tout comme le ferait un BIOS classique.

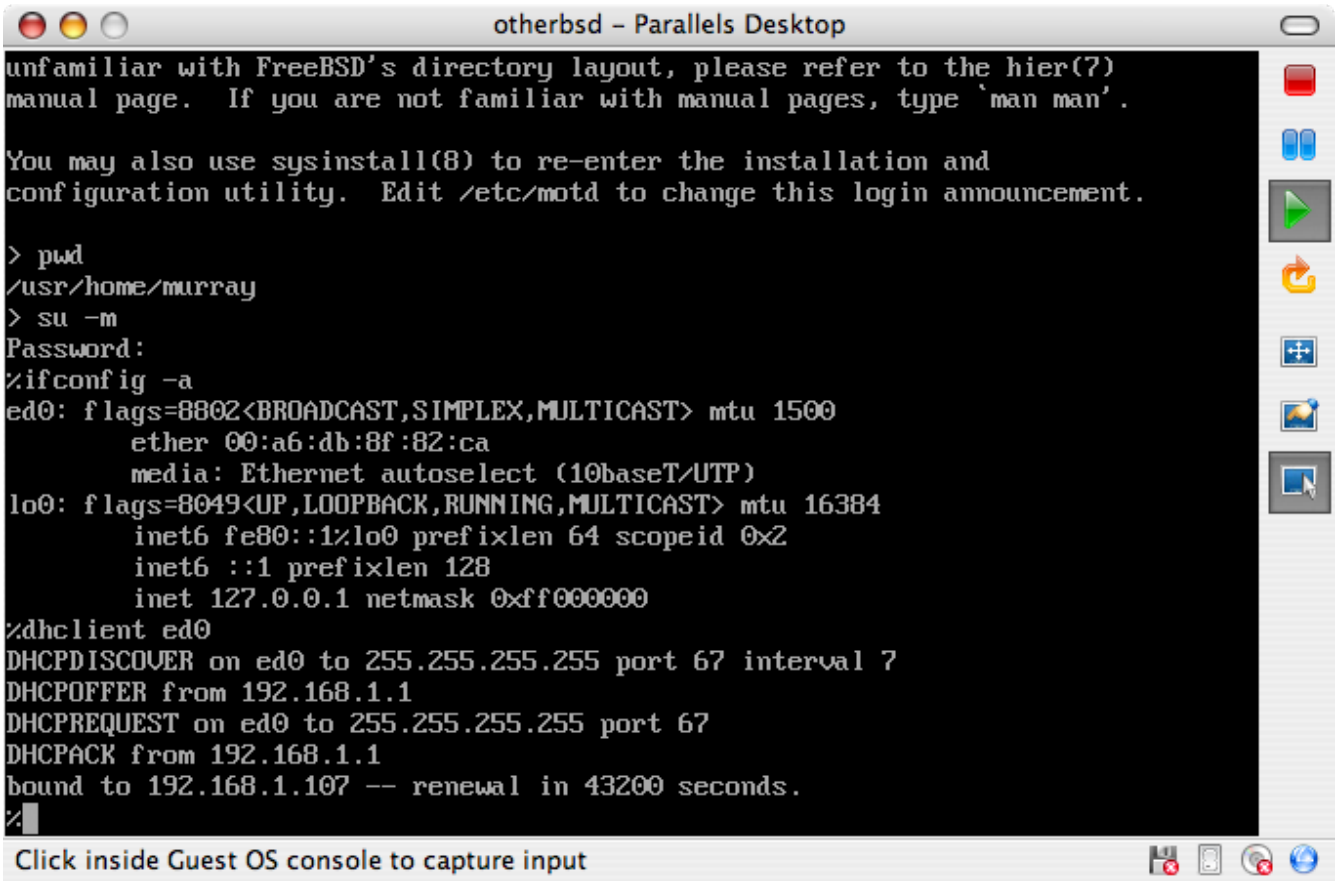


Dans notre cas il trouvera le disque d'installation de FreeBSD et lancera une installation normale

avec sysinstall comme décrit dans le Installer FreeBSD. Vous pouvez installer X11 mais ne tentez pas de le configurer pour le moment.



Quand l'installation est terminée, redémarrez votre machine virtuelle FreeBSD.



24.2.1.2. Configurer FreeBSD sur Mac OS® X/Parallels

Après avoir installé avec succès FreeBSD sur Mac OS® X avec Parallels, il reste plusieurs points à configurer pour optimiser le système virtuel.

1. Paramétrer les variables du chargeur

   L'étape la plus importante est la diminution du paramètre `kern.hz` afin de réduire l'utilisation du CPU de FreeBSD sous l'environnement Parallels. Pour cela, il faut ajouter la ligne suivante au fichier /boot/loader.conf:

   ```
   kern.hz=100
   ```

   Sans ce paramétrage, un système d'exploitation invité FreeBSD inactif sous Parallels utilisera environ 15% du CPU sur un iMac® à mono-processeur. Après ce changement l'utilisation du processeur sera plus proche d'un petit 5%.

2. Créer un nouveau fichier de configuration du noyau

   Vous pouvez retirer tous les pilotes de périphériques SCSI, FireWire et USB. Parallels fournit une carte réseau virtuelle utilisant le pilote ed(4), aussi tous les autres pilotes réseau exceptés ed(4) et miibus(4) peuvent être retirés du noyau.

3. Configuration du réseau

   La configuration réseau la plus simple utilise DHCP pour connecter votre machine virtuelle sur le même réseau local que votre machine Mac® hôte. Cette configuration se fait en ajoutant la ligne `ifconfig_ed0="DHCP"` au fichier /etc/rc.conf. Des configurations réseau plus avancées sont décrites dans le Administration réseau avancée.

24.2.2. FreeBSD avec Xen™ sur Linux

L'hyperviseur Xen™ est un logiciel libre de para-virtualisation qui est supporté par l'entreprise commerciale XenSource. Les systèmes d'exploitation invités sont appelés domaines domU, et le système d'exploitation hôte est appelé dom0. La première étape pour faire tourner un FreeBSD virtuel sous Linux® est d'installer Xen™ pour le domaine dom0 Linux®. Le système d'exploitation hôte sera une distribution Linux® Slackware.

24.2.2.1. Configuration de Xen™ 3 sur un dom0 Linux®

1. Télécharger Xen™ 3.0 auprès de XenSource

   Récupérez l'archive xen-3.0.4_1-src.tgz auprès de http://www.xensource.com/.

2. Extraire l'archive

   ```
   # cd xen-3.0.4_1-src
   ```

```
# KERNELS="linux-2.6-xen0 linux-2.6-xenU" make world
# make install
```

Pour recompiler le noyau pour le domaine dom0:

```
# cd xen-3.0.4_1-src/linux-2.6.16.33-xen0
  # make menuconfig
  # make
  # make install
```

D'anciennes versions de Xen™ peuvent nécessiter l'utilisation de la commande `make ARCH=xen menuconfig`

3. Ajouter une entrée au menu de Grub (menu.lst)

   Editez /boot/grub/menu.lst et ajoutez les lignes suivantes:

```
title Xen-3.0.4
root (hd0,0)
kernel /boot/xen-3.0.4-1.gz dom0_mem=262144
module /boot/vmlinuz-2.6.16.33-xen0 root=/dev/hda1 ro
```

4. Redémarrer votre ordinateur sous Xen™

   Tout d'abord, éditez /etc/xen/xend-config.sxp, et ajoutez la ligne suivante:

```
(network-script 'network-bridge netdev=eth0')
```

   Nous pouvons maintenant lancer Xen™:

```
# /etc/init.d/xend start
# /etc/init.d/xendomains start
```

   Notre domaine dom0 fonctionne:

```
# xm list
Name                                      ID   Mem VCPUs      State   Time(s)
Domain-0                                   0   256     1     r-----  54452.9
```

24.2.2.2. Domaine domU FreeBSD 7-CURRENT

Téléchargez le noyau pour domU FreeBSD pour Xen™ 3.0 et l'image disque auprès de http://www.fsmware.com/

- kernel-current
- mdroot-7.0.bz2
- xmexample1.bsd

Placez le fichier de configuration xmexample1.bsd dans le répertoire /etc/xen/ et modifiez les entrées relatives à l'emplacement du noyau et de l'image disque. Cela devrait donner quelque chose comme:

```
kernel = "/opt/kernel-current"
memory = 256
name = "freebsd"
vif = [ '' ]
disk = [ 'file:/opt/mdroot-7.0,hda1,w' ]
#on_crash    = 'preserve'
extra = "boot_verbose"
extra += ",boot_single"
extra += ",kern.hz=100"
extra += ",vfs.root.mountfrom=ufs:/dev/xbd769a"
```

Le fichier mdroot-7.0.bz2 doit être décompressé.

Ensuite, la section __xen_guest du fichier kernel-current doit être modifiée pour y ajouter le paramètre VIRT_BASE dont a besoin Xen™ 3.0.3:

```
# objcopy kernel-current -R __xen_guest
# perl -e 'print "LOADER=generic,GUEST_OS=freebsd,GUEST_VER=7.0,XEN_VER=xen-
3.0,BSD_SYMTAB,VIRT_BASE=0xC0000000\x00"' > tmp
# objcopy kernel-current --add-section __xen_guest=tmp
```

```
# objdump -j __xen_guest -s kernel-current

kernel-current:     file format elf32-i386

Contents of section __xen_guest:
 0000 4c4f4144 45523d67 656e6572 69632c47  LOADER=generic,G
 0010 55455354 5f4f533d 66726565 6273642c  UEST_OS=freebsd,
 0020 47554553 545f5645 523d372e 302c5845  GUEST_VER=7.0,XE
 0030 4e5f5645 523d7865 6e2d332e 302c4253  N_VER=xen-3.0,BS
 0040 445f5359 4d544142 2c564952 545f4241  D_SYMTAB,VIRT_BA
 0050 53453d30 78433030 30303030 3000      SE=0xC0000000.
```

Nous sommes maintenant prêt à créer et lancer notre domU:

```
# xm create /etc/xen/xmexample1.bsd -c
Using config file "/etc/xen/xmexample1.bsd".
Started domain freebsd
```

```
WARNING: loader(8) metadata is missing!
Copyright (c) 1992-2006 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.
FreeBSD 7.0-CURRENT #113: Wed Jan  4 06:25:43 UTC 2006
    kmacy@freebsd7.gateway.2wire.net:/usr/home/kmacy/p4/freebsd7_xen3/src/sys/i386-
xen/compile/XENCONF
WARNING: DIAGNOSTIC option enabled, expect reduced performance.
Xen reported: 1796.927 MHz processor.
Timecounter "ixen" frequency 1796927000 Hz quality 0
CPU: Intel(R) Pentium(R) 4 CPU 1.80GHz (1796.93-MHz 686-class CPU)
  Origin = "GenuineIntel"  Id = 0xf29  Stepping = 9
  Features
=0xbfebfbff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,APIC,SEP,MTRR,PGE,MCA,CMOV,PAT,PSE36,CL
FLUSH,
  DTS,ACPI,MMX,FXSR,SSE,SSE2,SS,HTT,TM,PBE>
  Features2=0x4400<CNTX-ID,<b14>>
real memory  = 265244672 (252 MB)
avail memory = 255963136 (244 MB)
xc0: <Xen Console> on motherboard
cpu0 on motherboard
Timecounters tick every 10.000 msec
[XEN] Initialising virtual ethernet driver.
xn0: Ethernet address: 00:16:3e:6b:de:3a
[XEN]
Trying to mount root from ufs:/dev/xbd769a
WARNING: / was not properly dismounted
Loading configuration files.
No suitable dump device was found.
Entropy harvesting: interrupts ethernet point_to_point kickstart.
Starting file system checks:
/dev/xbd769a: 18859 files, 140370 used, 113473 free (10769 frags, 12838 blocks, 4.2%
fragmentation)
Setting hostname: demo.freebsd.org.
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
      inet6 ::1 prefixlen 128
      inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
      inet 127.0.0.1 netmask 0xff000000
Additional routing options:.
Mounting NFS file systems:.
Starting syslogd.
/etc/rc: WARNING: Dump device does not exist.  Savecore not run.
ELF ldconfig path: /lib /usr/lib /usr/lib/compat /usr/X11R6/lib /usr/local/lib
a.out ldconfig path: /usr/lib/aout /usr/lib/compat/aout /usr/X11R6/lib/aout
Starting usbd.
usb: Kernel module not available: No such file or directory
Starting local daemons:.
Updating motd.
Starting sshd.
Initial i386 initialization:.
Additional ABI support: linux.
```

```
Starting cron.
Local package initialization:.
Additional TCP options:.
Starting background file system checks in 60 seconds.

Sun Apr  1 02:11:43 UTC 2007

FreeBSD/i386 (demo.freebsd.org) (xc0)

login:
```

Le domaine domU devrait exécuter le noyau FreeBSD 7.0-CURRENT:

```
# uname -a
FreeBSD demo.freebsd.org 7.0-CURRENT FreeBSD 7.0-CURRENT #113: Wed Jan  4 06:25:43 UTC
2006
kmacy@freebsd7.gateway.2wire.net:/usr/home/kmacy/p4/freebsd7_xen3/src/sys/i386-
xen/compile/XENCONF  i386
```

Le réseau peut maintenant être configuré sur le domaine domU. Le domaine domU FreeBSD utilisera une interface spécifique appelée xn0:

```
# ifconfig xn0 10.10.10.200 netmask 255.0.0.0
# ifconfig
xn0: flags=843<UP,BROADCAST,RUNNING,SIMPLEX> mtu 1500
    inet 10.10.10.200 netmask 0xff000000 broadcast 10.255.255.255
    ether 00:16:3e:6b:de:3a
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
      inet6 ::1 prefixlen 128
      inet6 fe80::1%lo0 prefixlen 64 scopeid 0x2
      inet 127.0.0.1 netmask 0xff000000
```

Sur le domaine dom0 Slackware, des interfaces réseaux relatives à Xen™ devraient apparaître:

```
# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:07:E9:A0:02:C2
          inet addr:10.10.10.130  Bcast:0.0.0.0  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:815 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1400 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:204857 (200.0 KiB)  TX bytes:129915 (126.8 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:99 errors:0 dropped:0 overruns:0 frame:0
```

```
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:9744 (9.5 KiB)  TX bytes:9744 (9.5 KiB)

peth0     Link encap:Ethernet  HWaddr FE:FF:FF:FF:FF:FF
          UP BROADCAST RUNNING NOARP  MTU:1500  Metric:1
          RX packets:1853349 errors:0 dropped:0 overruns:0 frame:0
          TX packets:952923 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2432115831 (2.2 GiB)  TX bytes:86528526 (82.5 MiB)
          Base address:0xc000 Memory:ef020000-ef040000

vif0.1    Link encap:Ethernet  HWaddr FE:FF:FF:FF:FF:FF
          UP BROADCAST RUNNING NOARP  MTU:1500  Metric:1
          RX packets:1400 errors:0 dropped:0 overruns:0 frame:0
          TX packets:815 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:129915 (126.8 KiB)  TX bytes:204857 (200.0 KiB)

vif1.0    Link encap:Ethernet  HWaddr FE:FF:FF:FF:FF:FF
          UP BROADCAST RUNNING NOARP  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:157 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:140 (140.0 b)  TX bytes:158 (158.0 b)

xenbr1    Link encap:Ethernet  HWaddr FE:FF:FF:FF:FF:FF
          UP BROADCAST RUNNING NOARP  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:112 (112.0 b)  TX bytes:0 (0.0 b)
```

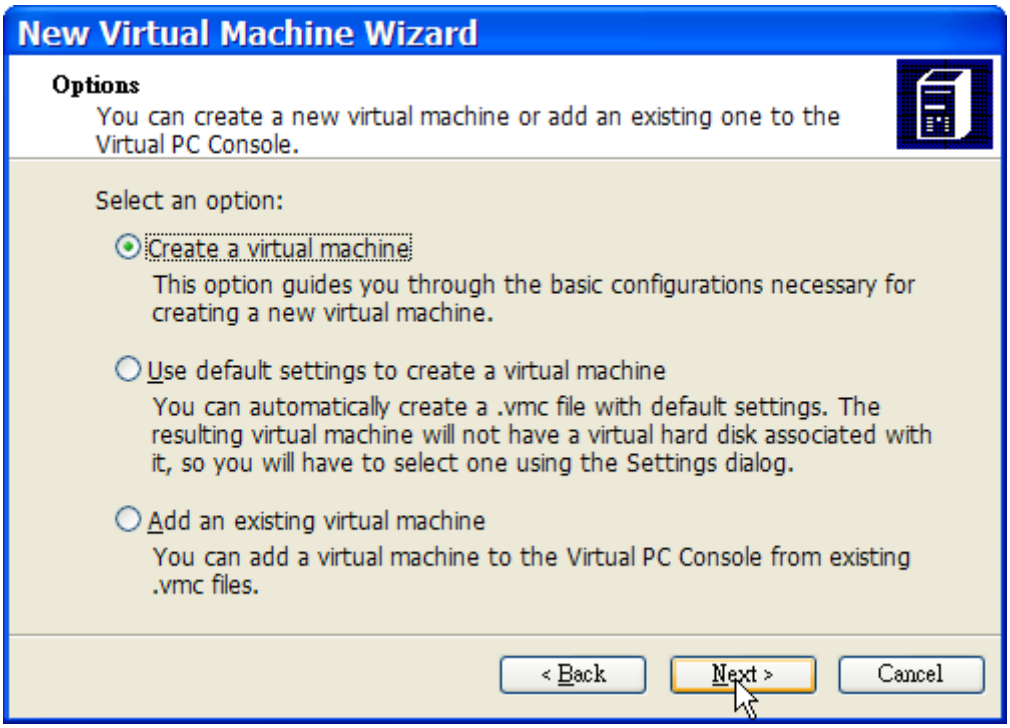
```
# brctl show
bridge name     bridge id           STP enabled         interfaces
xenbr1          8000.feffffffffff   no                  vif0.1
                                                        peth0
                                                        vif1.0
```

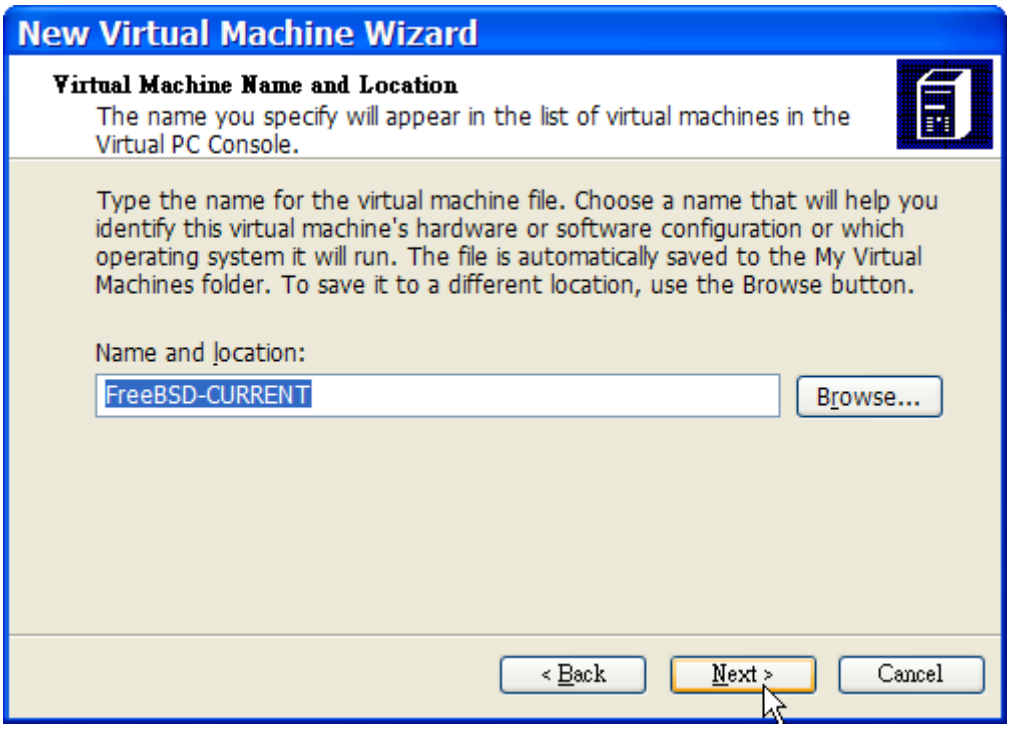
24.2.3. Virtual PC sur Windows®

Virtual PC pour Windows® est un logiciel Microsoft® librement téléchargeable. Consultez la page concernant la configuration minimale requise. Une fois Virtual PC installé sous Microsoft® Windows®, l'utilisateur doit configurer une machine virtuelle puis installer le système d'exploitation invité désiré.

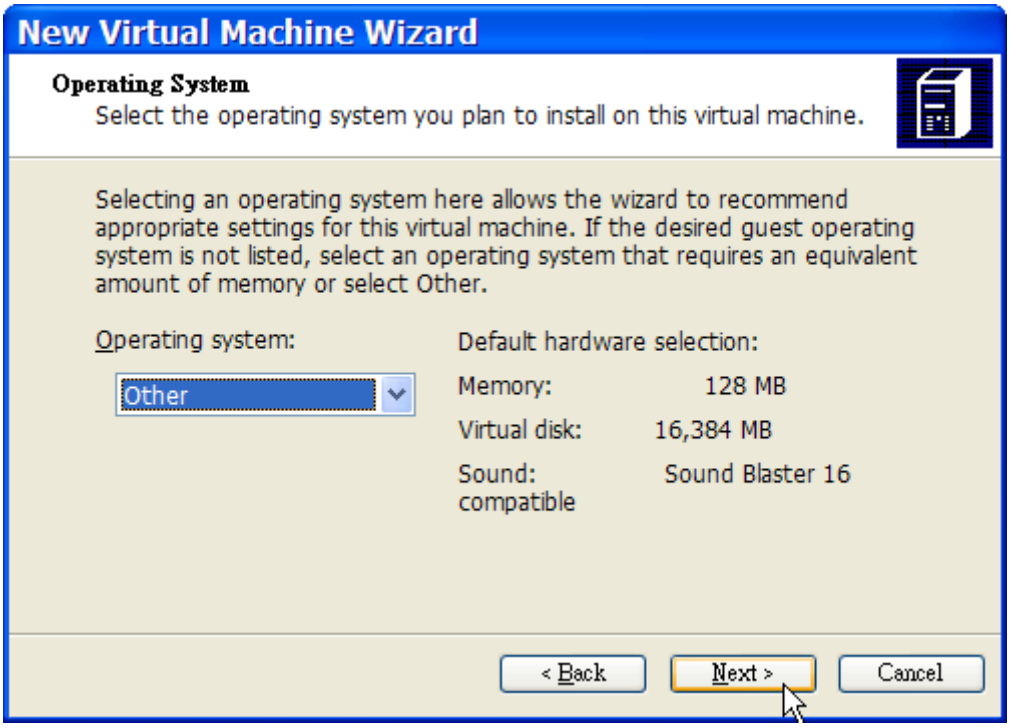
24.2.3.1. Installer FreeBSD sous Virtual PC/Microsoft® Windows®

La première étape de l'installation de FreeBSD sous Microsoft® Windows®/Virtual PC est la création d'une nouvelle machine virtuelle pour permettre l'installation de FreeBSD. Sélectionnez Create a virtual machine:

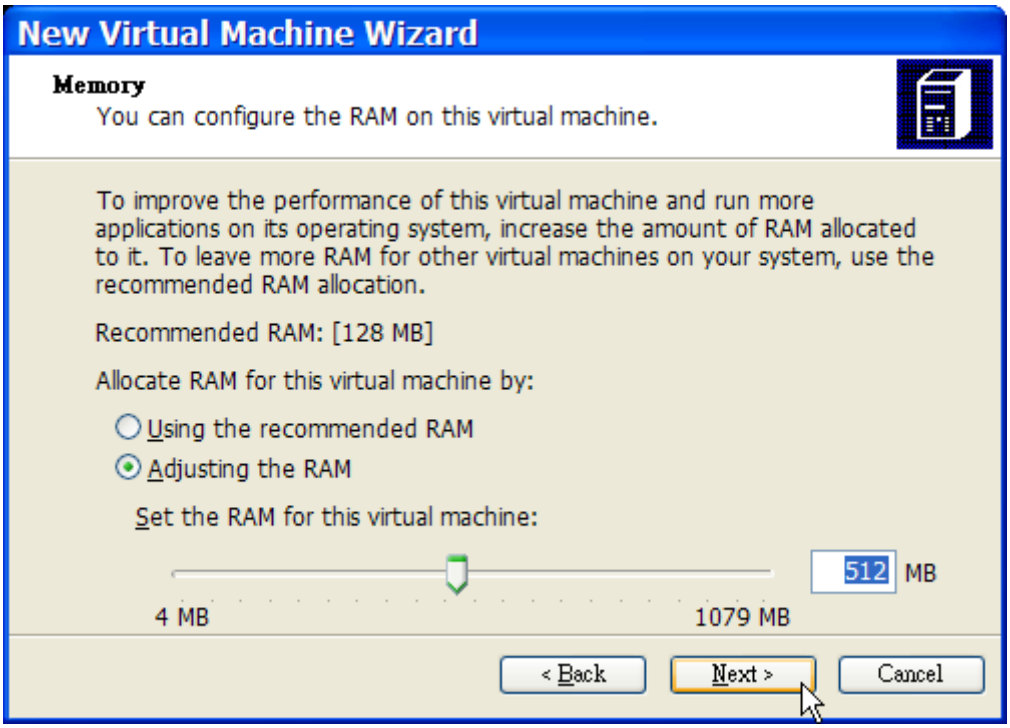


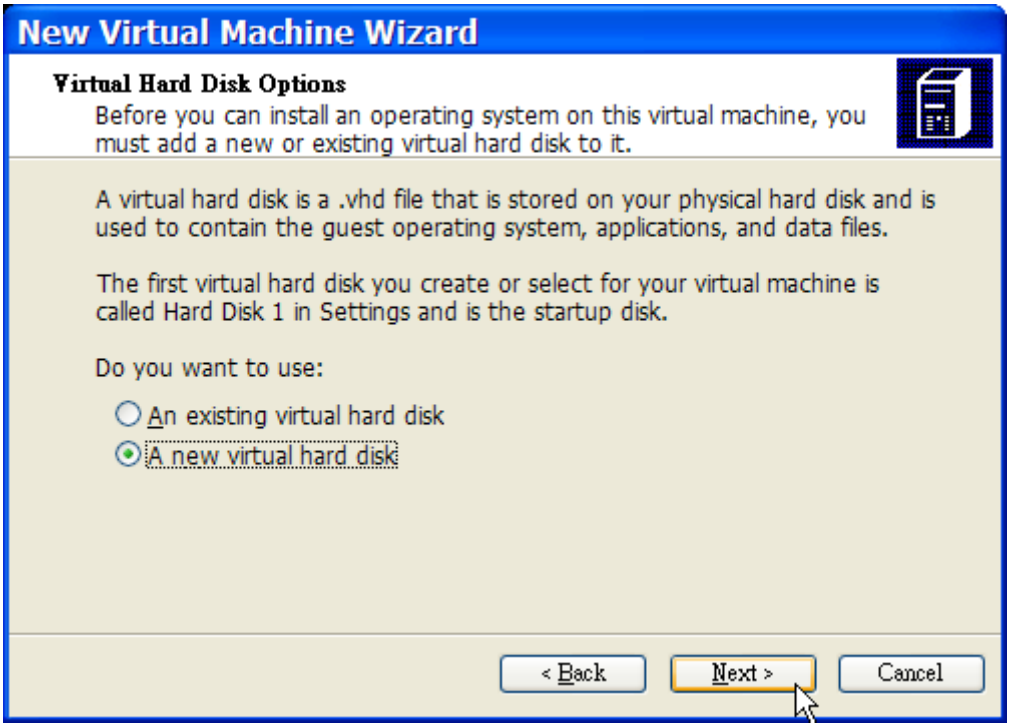


Puis sélectionnez Other pour Operating system:

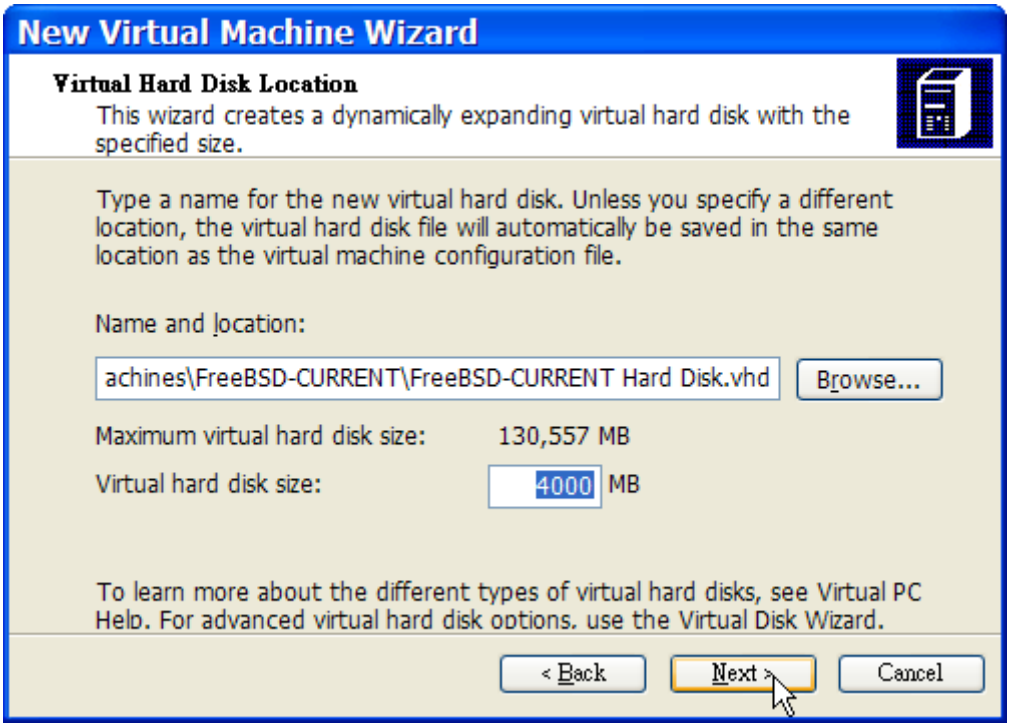


Choisissez ensuite une quantité raisonnable d'espace disque et de mémoire en fonction de vos projets pour cette installation de FreeBSD. 4Go d'espace de disque et 512Mo de mémoire vive conviennent pour la plupart des utilisateurs de FreeBSD sous Virtual PC:

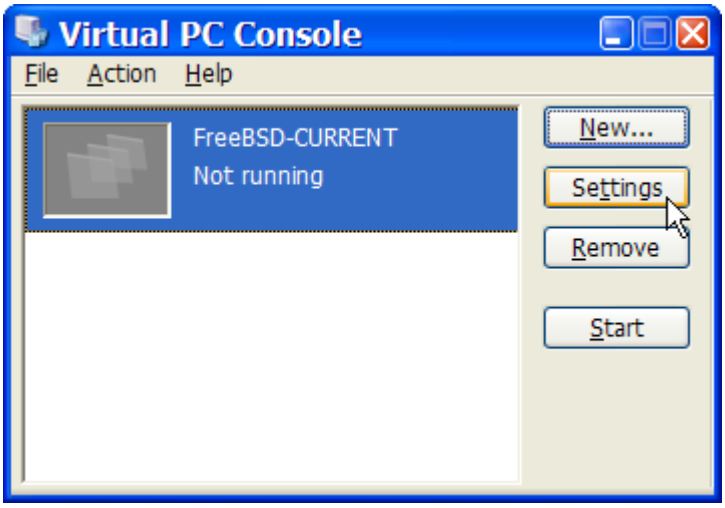


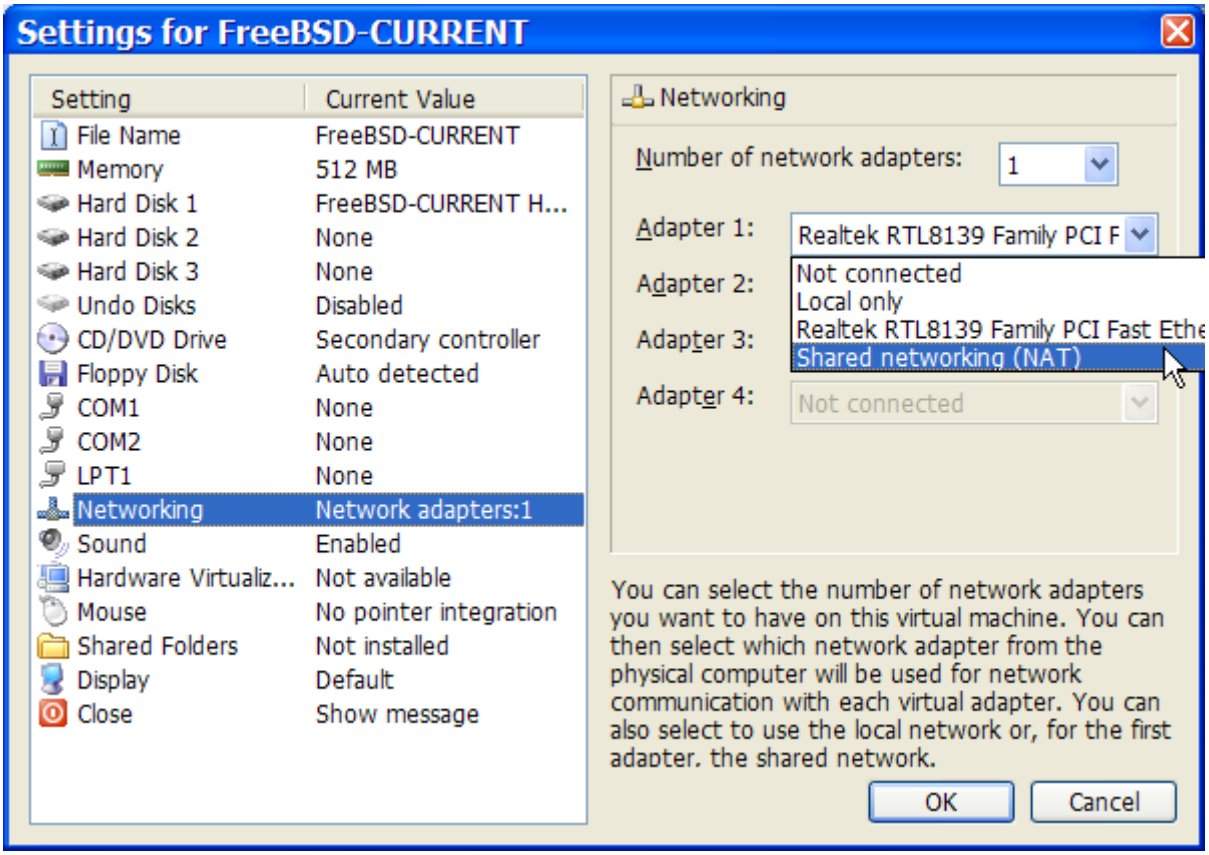


Sauvegardez et poursuivez la configuration:

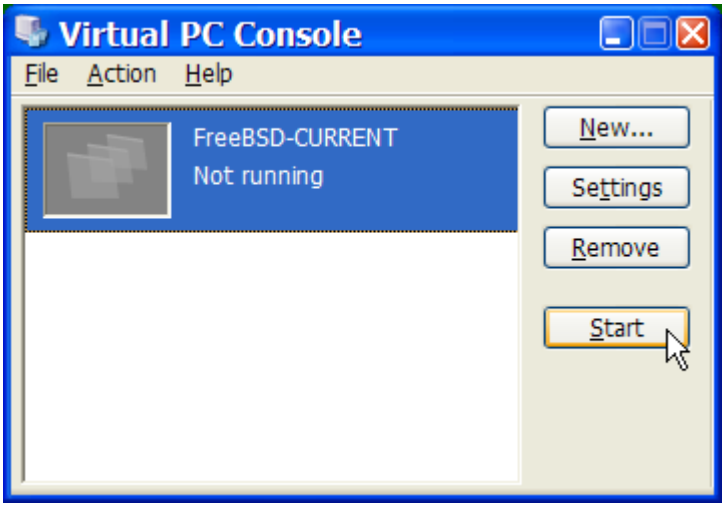


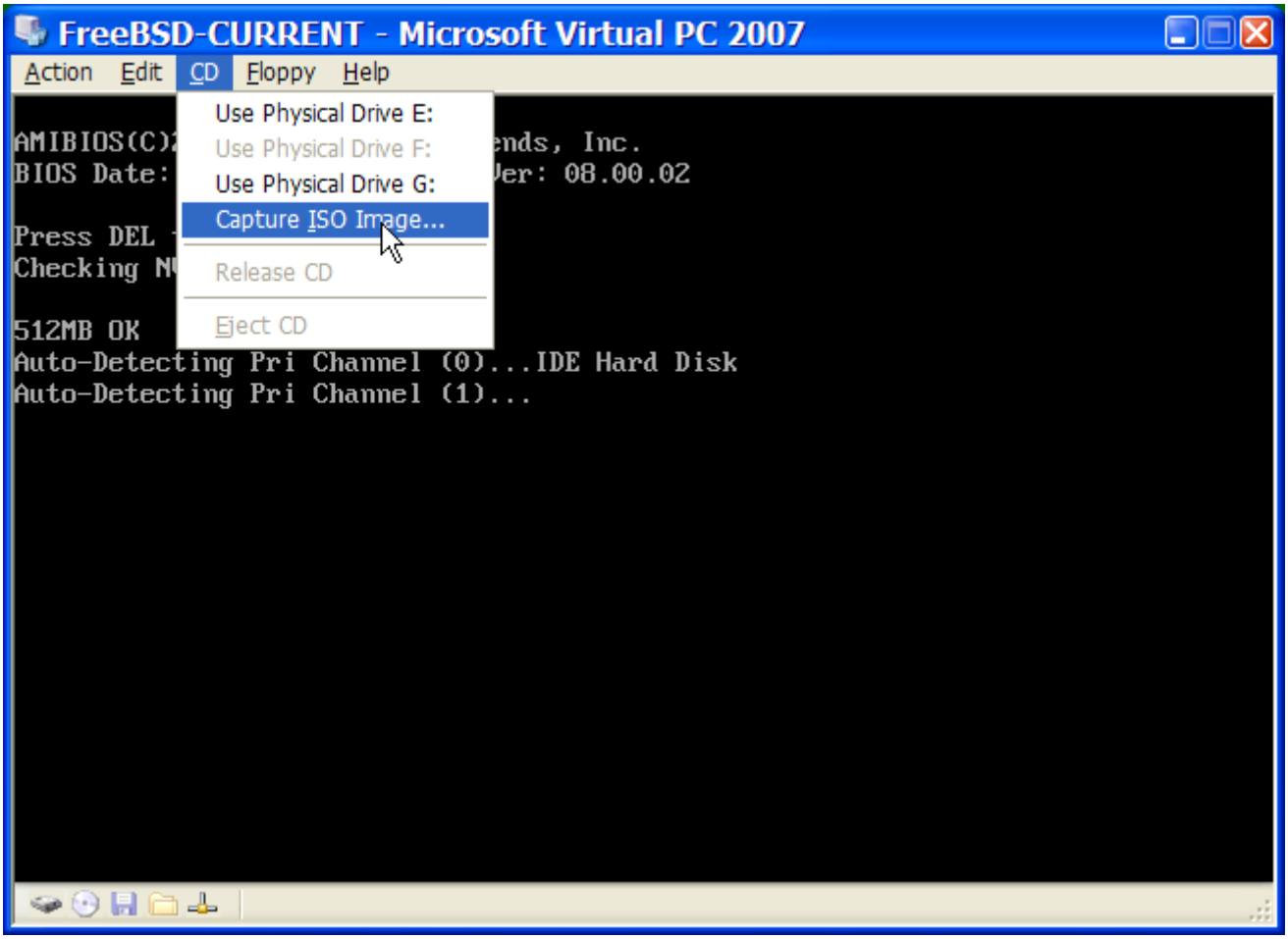
Sélectionnez votre machine virtuelle FreeBSD, cliquez sur **Settings**, puis précisez le type de réseau et l'interface réseau:



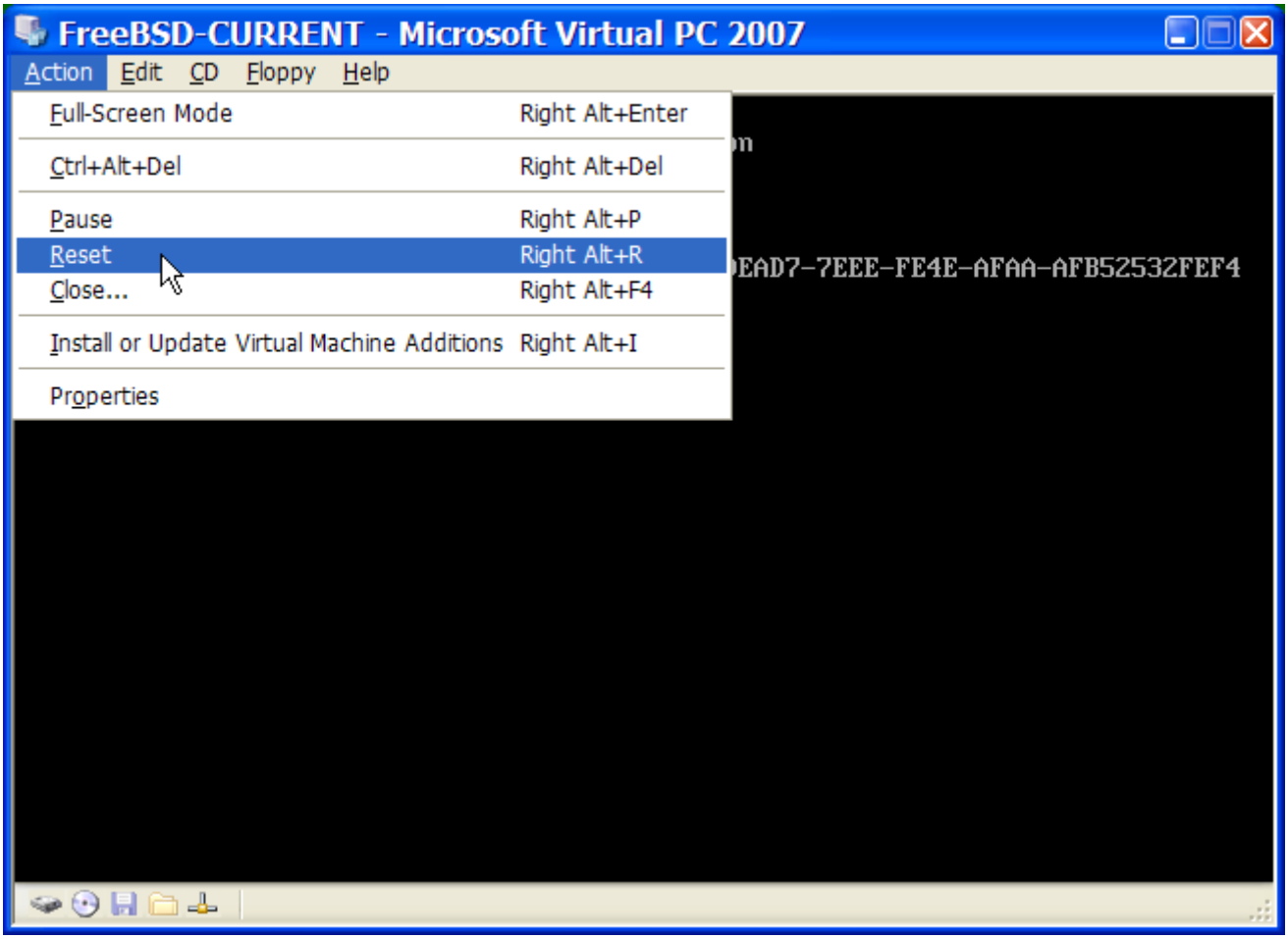


Une fois votre machine virtuelle FreeBSD créée, vous devrez y installer FreeBSD. La meilleure manière étant d'utiliser un CDROM FreeBSD officiel ou une image ISO téléchargée depuis un site FTP officiel. Quand vous avez l'image ISO appropriée sur votre système de fichiers Windows® ou sur un CDROM dans votre lecteur de CD, double-cliquez sur votre machine virtuelle FreeBSD pour démarrer. Puis cliquez sur **CD** et sélectionnez **Capture ISO Image...** dans la fenêtre Virtual PC. Une fenêtre apparaîtra et vous permettra d'associer le lecteur de CDROM de votre machine virtuelle avec une image ISO ou votre lecteur de CDROM réel.

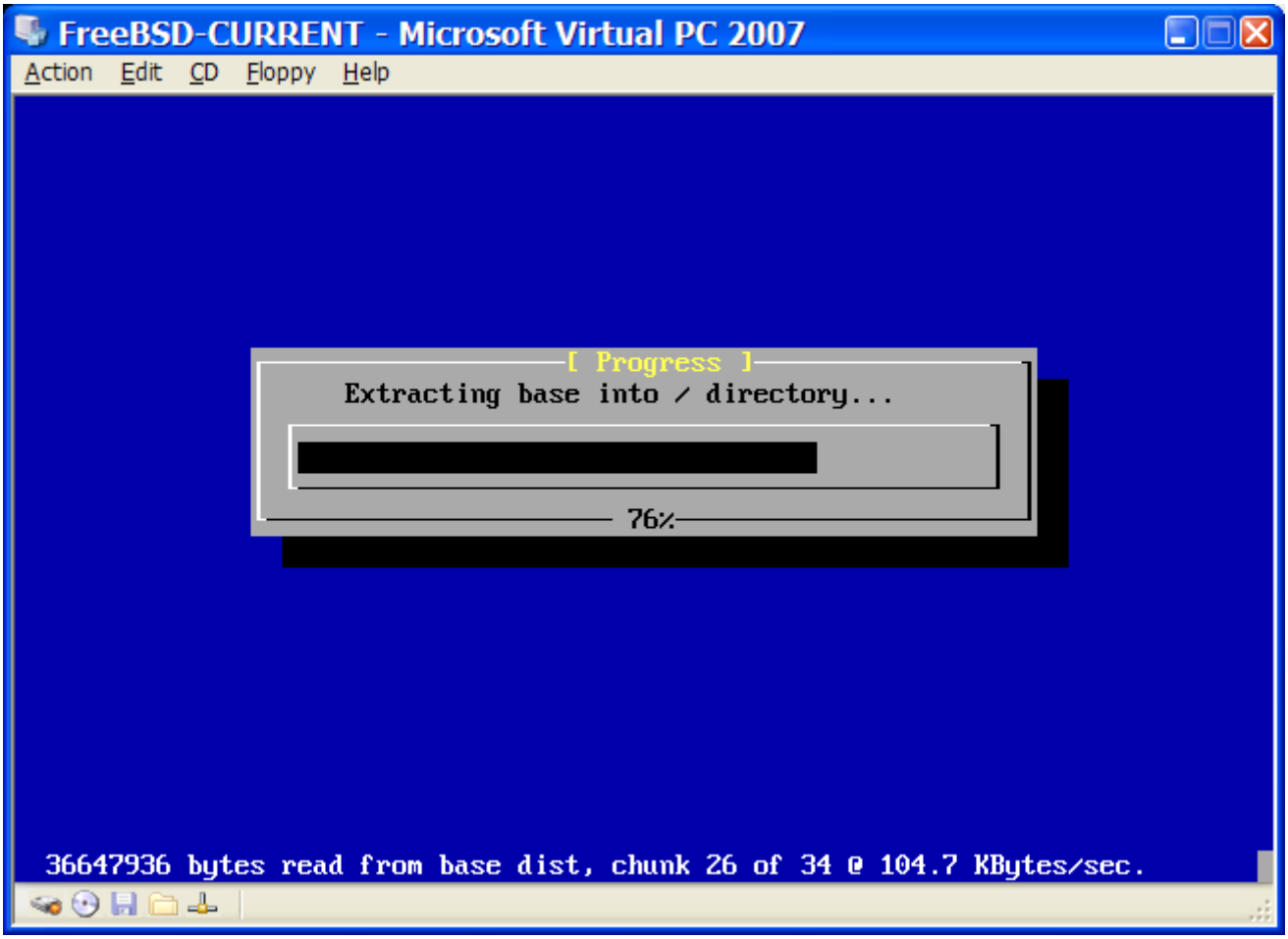




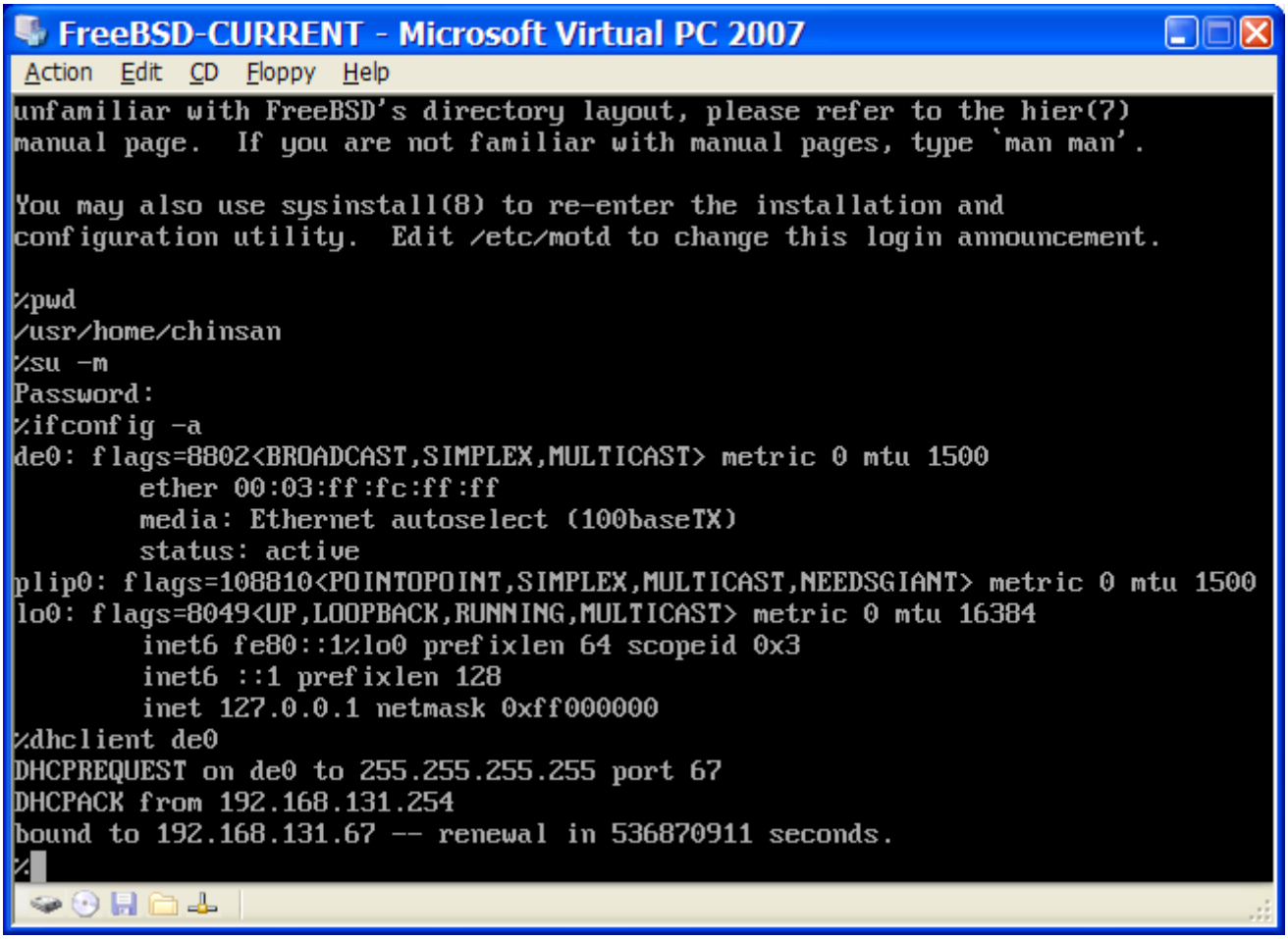
L'association avec votre CDROM source effectuée, redémarrez votre machine virtuelle FreeBSD en cliquant sur **Action** puis sur **Reset**. Virtual PC redémarrera, son BIOS vérifiera tout d'abord que vous disposez d'un CDROM comme le ferait n'importe quel BIOS normal.



Dans ce cas, le support d'installation FreeBSD sera trouvé et une installation classique basée sur sysinstall débutera comme décrit dans le Installer FreeBSD. Vous pouvez installez X11 mais ne tentez pas pour le moment de le configurer.



Quand vous avez achevé l'installation, pensez à éjecter le CDROM ou l'image ISO. Enfin, redémarrez dans votre machine virtuelle FreeBSD fraîchement installée.



24.2.3.2. Configuration de FreeBSD sous Microsoft® Windows®/Virtual PC

Après avoir installé avec succès FreeBSD sur Microsoft® Windows® avec Virtual PC, il reste plusieurs points à configurer pour optimiser le système virtuel.

1. Paramétrer les variables du chargeur

   L'étape la plus importante est la diminution du paramètre `kern.hz` afin de réduire l'utilisation du CPU de FreeBSD sous l'environnement Virtual PC. Pour cela, il faut ajouter la ligne suivante au fichier /boot/loader.conf:

   ```
   kern.hz=100
   ```

   Sans ce paramétrage, un système d'exploitation invité FreeBSD inactif sous Virtual PC utilisera environ 40% du CPU pour un micro-ordinateur monoprocesseur. Après ce changement l'utilisation du processeur sera plus proche d'un petit 3%.

2. Créer un nouveau fichier de configuration du noyau

   Vous pouvez retirer tous les pilotes de périphériques SCSI, FireWire, et USB. Virtual PC fournit une interface réseau virtuelle utilisant le pilote de(4), aussi tous les autres pilotes réseau en dehors de de(4) et miibus(4) peuvent être supprimés du noyau.

3. Configuration du réseau

La configuration réseau la plus simple utilise DHCP pour connecter votre machine virtuelle sur le même réseau local que votre machine Mac® hôte. Cette configuration se fait en ajoutant la ligne `ifconfig_de0="DHCP"` au fichier /etc/rc.conf. Des configurations réseau plus avancées sont présentées dans le Administration réseau avancée.

24.2.4. VMware sur Windows®/Mac®/Linux®

Cette section n'est pas encore écrite.

24.3. FreeBSD comme système d'exploitation hôte

Actuellement, FreeBSD en tant que système d'exploitation hôte n'est officiellement supporté par aucun logiciel de virtualisation, de nombreuses personnes utilisent d'anciennes versions de VMware pour cela. Des efforts sont actuellement déployés pour faire fonctionner Xen™ en tant qu'environnement hôte sur FreeBSD.

Chapitre 25. Localisation - Utilisation et configuration de l'I18N/L10N

25.1. Synopsis

FreeBSD est un projet à très large audience avec des utilisateurs et des contributeurs provenant du monde entier. Ce chapitre discute des fonctions d'internationalisation et de localisation de FreeBSD qui permettent aux non-anglophones de travailler. Il y a de nombreux aspects de l'implémentation i18n au niveau système et application, et quand ce sera possible nous renverrons le lecteur à des sources de documentation plus spécifiques.

Après la lecture de ce chapitre, vous connaîtrez:

- Comment les différentes langues et "locales" sont codées sur les systèmes d'exploitation modernes.
- Comment paramétrer les "locales" pour votre interpréteur de commandes.
- Comment configurer la console pour d'autres langues que l'anglais.
- Comment employer le système X Window efficacement avec différentes langues.
- Où trouver plus d'informations sur l'écriture d'applications conformes à la norme i18n.

Avant de lire ce chapitre, vous devrez:

- Savoir comment installer des logiciels tiers (Installer des applications. les logiciels pré-compilés et les logiciels portés).

25.2. Les bases

25.2.1. Qu'est-ce que I18N/L10N?

Les développeurs ont raccourci le terme internationalisation en I18N, en comptant le nombre de lettres entre la première et la dernière du mot internationalisation. L10N utilise le même principe, et provient du mot "localisation". Combinées ensemble, les méthodes I18N/L10N, les protocoles, et les applications conformes permettent aux utilisateurs d'utiliser la langue de leur choix.

Les applications I18N sont programmées en utilisant des kits I18N par dessous les bibliothèques. Cela permet aux développeurs d'écrire un simple fichier et traduire les menus et textes affichés dans chaque langue. Nous encourageons fortement les programmeurs à suivre cette convention.

25.2.2. Pourquoi devrais-je employer l'I18N/L10N?

I18N/L10N est utilisé à chaque fois que vous désirez afficher, entrer, ou traiter des données dans des langues autres que l'anglais.

25.2.3. Quelles sont les langues supportées par l'I18N?

I18N et L10N ne sont pas spécifiques à FreeBSD. Actuellement, on peut choisir parmi la plupart des langues principales du monde, y compris mais pas seulement: le chinois, l'allemand, le japonais, le coréen, le français, le russe, le vietnamien et d'autres.

25.3. Utiliser la localisation

Dans toute sa splendeur, I18N n'est pas spécifique à FreeBSD et est une convention. Nous vous encourageons à aider FreeBSD à suivre cette convention.

Le paramétrage des "locales" est basé sur trois termes principaux: le code de la langue, le code du pays, et le codage des caractères. Les noms de "locales" sont construits à partir de ces trois éléments comme suit:

```
CodeLangue_CodePays.CodageCaractères
```

25.3.1. Codage de la langue et du pays

Afin de localiser un système FreeBSD pour une langue spécifique (ou tout autre UNIX® supportant l'I18N), l'utilisateur doit déterminer les codes spécifiques pour le pays et la langue (les codes pays indiquent aux applications quelle variation d'une langue donnée utiliser). De plus, les navigateurs Web, les serveurs SMTP/POP, les serveurs Web… agissent en fonction de ces codes. Ce qui suit est un exemple de codes langue/pays:

Code langue/pays	Description
en_US	Anglais - Etats Unis
ru_RU	Russe pour la Russie
zh_TW	Chinois traditionnel pour Taiwan

25.3.2. Codage des caractères

Certaines langues utilisent les codages non-ASCII sur 8 bits ou codent des caractères sur plusieurs octets, voir multibyte(3) pour plus de détails. Les vieilles applications ne les reconnaissent pas ou les remplacent à tord par des caractères de contrôle. Les applications récentes reconnaissent normalement les caractères 8 bits. En fonction de l'implémentation, les utilisateurs devront peut être compiler une application avec le support des caractères sur 8 bits ou multi-octets, ou la configurer correctement. Afin d'accepter l'usage et le traitement de tels caractères, le catalogue des logiciels portés de FreeBSD fournit pour certains programmes une version dans chaque langue. Référez-vous à la documentation I18N de chaque logiciel porté respectif.

Spécifiquement, l'utilisateur doit consulter la documentation de l'application pour décider de comment la configurer correctement ou comment passer les valeurs correctes à la procédure configure, au Makefile ou au compilateur.

Quelques éléments à garder à l'esprit sont:

- Les jeux de caractères au codage simple des caractères de la bibliothèque C (voir multibyte(3)), par exemple ISO8859-1, ISO8859-15, KOI8-R, et CP437.
- Les codages étendus ou multi-octets, e.g. EUC, Big5.

Vous pouvez contrôler la liste des jeux de caractères actuellement actifs dans le registre de l'IANA.

FreeBSD utilise à la place un codage des "locales" compatible avec X11.

25.3.3. Applications I18N

Dans le système de logiciels portés et pré-compilés de FreeBSD, les applications I18N ont été nommées avec `I18N` dans leur nom pour une identification aisée. Cependant, elles ne supportent pas toujours la langue désirée.

25.3.4. Configurer les "locales"

Généralement il est suffisant d'exporter le nom de la "locale" grâce à la variable `LANG` sous l'interpréteur de commandes utilisé lors de la session. Cela pourra être fait dans le fichier ~/.login_conf de l'utilisateur ou le fichier de configuration de l'interpréteur de commandes de l'utilisateur (~/.profile, ~/.bashrc, ~/.cshrc). Il n'est pas nécessaire de configurer toutes les autres variables de localisation comme `LC_CTYPE`, `LC_CTIME`. Veuillez consulter la documentation de FreeBSD spécifique à votre langue pour plus d'informations.

Vous devrez configurer les deux variables d'environnement suivantes dans vos fichiers de configuration:

- `LANG` pour la famille de fonctions POSIX® setlocale(3)
- `MM_CHARSET` pour le jeu de caractères MIME des applications

Cela comprend la configuration de l'interpréteur de commandes, la configuration spécifique des applications, et celle de X11.

25.3.4.1. Méthodes de configuration des "locales"

Il existe deux méthodes pour configurer les "locales", elles sont décrites ci-dessous. La première (celle qui est recommandée) est d'assigner les variables d'environnement dans une classe de session, et la seconde est d'ajouter le paramétrage des variables d'environnement dans les fichiers d'initialisation de l'interpréteur de commandes du système.

25.3.4.1.1. Méthode utilisant les classes de session utilisateur

Cette méthode permet d'assigner une fois pour toute les variables d'environnement nécessaires pour le nom des "locales" et le jeu de caractères MIME et cela pour toutes les sessions au lieu de le faire à chaque nouvelle session par l'intermédiaire de la configuration des fichiers d'initialisation de l'interpréteur de commandes. La configuration au niveau utilisateur peut être faite par l'utilisateur lui-même et la configuration au niveau administrateur demande les privilèges de super-utilisateur.

25.3.4.1.1.1. Configuration au niveau utilisateur

Voici un exemple minimal d'un fichier .login_conf dans le répertoire personnel d'un utilisateur, fichier qui a les deux variables fixées pour le codage Latin-1:

```
me:\
    :charset=ISO-8859-1:\
    :lang=de_DE.ISO8859-1:
```

Voici un exemple de fichier .login_conf qui fixe les variables pour le chinois traditionnel dans le codage BIG-5. Notez les nombreuses variables supplémentaires paramétrées parce que certains logiciels ne respectent pas les variables des "locales" correctement pour le chinois, le japonais, et le coréen.

```
#Users who do not wish to use monetary units or time formats
#of Taiwan can manually change each variable
me:\
    :lang=zh_TW.Big5:\
    :setenv=LC_ALL=zh_TW.Big:\
    :setenv=LC_COLLATE=zh_TW.Big5:\
    :setenv=LC_CTYPE=zh_TW.Big5:\
    :setenv=LC_MESSAGES=zh_TW.Big5:\
    :setenv=LC_MONETARY=zh_TW.Big5:\
    :setenv=LC_NUMERIC=zh_TW.Big5:\
    :setenv=LC_TIME=zh_TW.Big5:\
    :charset=big5:\
    :xmodifiers="@im=gcin": #Set gcin as the XIM Input Server
```

Voir la configuration au niveau administrateur et la page de manuel login.conf(5) pour plus de détails.

25.3.4.1.2. Configuration au niveau administrateur

Vérifiez que que la classe de session d'utilisateur dans /etc/login.conf fixe la bonne langue. Soyez sûr que ces paramètres apparaissent dans /etc/login.conf:

```
nom_langue:intitulé_comptes:\
    :charset=jeu_caractères_MIME:\
    :lang=nom_locale:\
    :tc=default:
```

Donc si l'on reste sur notre exemple précédent utilisant le Latin-1, cela donnera quelque chose comme:

```
german:German Users Accounts:\
    :charset=ISO-8859-1:\
    :lang=de_DE.ISO8859-1:\
```

```
    :tc=default:
```

Avant de modifier les classes de session des utilisateurs, exécutez la commande suivante:

```
# cap_mkdb /etc/login.conf
```

pour rendre visible à l'intégralité du système la nouvelle configuration du fichier /etc/login.conf.

25.3.4.1.3. Modifier les classes de session avec vipw(8)

Utilisez `vipw` pour ajouter de nouveaux utilisateurs, et créer une entrée ressemblant à celle-ci:

```
utilisateur:mot_de_passe:1111:11:langue:0:0:Nom
d'utilisateur:/home/utilisateur:/bin/sh
```

25.3.4.1.4. Modifier les classes de session avec adduser(8)

Utilisez `adduser` pour ajouter de nouveaux utilisateurs, et faites ce qui suit:

- Paramétrez `defaultclass = langue` dans /etc/adduser.conf. Gardez à l'esprit que vous devez dans ce cas entrer une classe par `default` (défaut) pour tous les utilisateurs d'autres langues.
- Une variante est d'entrer la langue spécifiée à chaque fois que adduser(8) affiche

  ```
  Enter login class: default []:
  ```

- Une autre alternative est d'employer ce qui suit pour chaque utilisateur de langue différente que vous désirez ajouter:

  ```
  # adduser -class langue
  ```

25.3.4.1.5. Modifier les classes de session avec pw(8)

Si vous utilisez pw(8) pour ajouter de nouveaux utilisateurs, appelez la fonction de cette manière:

```
# pw useradd nom_utilisateur -L langue
```

25.3.4.1.6. Méthode utilisant les fichiers d'initialisation de l'interpréteur de commandes

Cette méthode n'est pas recommandée parce qu'elle demande une configuration différente pour chaque interpréteur de commandes choisi. Utilisez la méthode utilisant les classes de session utilisateur à la place.

Pour ajouter le nom de la "locale" et le jeu de caractère MIME, positionnez juste les deux variables d'environnement comme montré ci-dessous dans les fichiers d'initialisation de l'interpréteur de

commandes /etc/profile et/ou /etc/csh.login. Nous utiliserons la langue allemande comme exemple ci-dessous:

Dans /etc/profile:

```
LANG=de_DE.ISO8859-1; export LANG
MM_CHARSET=ISO-8859-1; export MM_CHARSET
```

Ou dans /etc/csh.login:

```
setenv LANG de_DE.ISO8859-1
setenv MM_CHARSET ISO-8859-1
```

Alternativement, vous pouvez ajouter les instructions précédentes à /usr/shared/skel/dot.profile (similaire à ce qui fut utilisé dans /etc/profile ci-dessus), ou /usr/shared/skel/dot.login (similaire à ce qui fut utilisé dans /etc/csh.login ci-dessus).

Pour X11:

Dans $HOME/.xinitrc:

```
LANG=de_DE.ISO8859-1; export LANG
```

Ou:

```
setenv LANG de_DE.ISO8859-1
```

En fonction de votre interpréteur de commandes (vois ci-dessus).

25.3.5. Configuration de la console

Pour tous les ensembles de jeu de caractères utilisés par la bibliothèque C, positionnez les bonnes polices de caractères pour la console dans /etc/rc.conf pour la langue en question avec:

```
font8x16=nom_police
font8x14=nom_police
font8x8=nom_police
```

Le *nom_police* provient ici du répertoire /usr/shared/syscons/fonts, sans le suffixe .fnt.

Vérifiez également que vous avez paramétré les bonnes tables de clavier et de correspondance d'affichage pour votre jeu de caractères C par l'intermédiaire de `sysinstall` (/stand/sysinstall sous les versions de FreeBSD antérieures à la 5.2). Une fois dans sysinstall, sélectionnez Configure, puis Console. Alternativement, vous pouvez ajouter ce qui suit au fichier /etc/rc.conf:

```
scrnmap=table_correspondance_affichage
keymap=nom_table_clavier
keychange="numéro_touche_fonction séquence"
```

La *table_correspondance_affichage* ici provient du répertoire /usr/shared/syscons/scrnmaps sans le suffixe .scm. Une table de correspondance d'affichage avec une police de correspondance est généralement nécessaire pour passer de 8 à 9 bits la matrice de caractère d'une carte VGA dans une zone pseudo-graphique, i.e., déplacer les lettres en dehors de cette zone si la police d'écran utilise une colonne de 8 bits.

Si vous avez le "daemon" moused activé par défaut grâce à la ligne suivante dans votre /etc/rc.conf:

```
moused_enable="YES"
```

alors lisez les informations sur le curseur de souris dans le paragraphe suivant.

Par défaut le curseur du pilote syscons(4) de la console occupe la zone d'adresses 0xd0-0xd3 dans le jeu de caractères. Si votre langue utilise cette zone, vous devez déplacer la zone du curseur en dehors. Pour effectuer cela sous FreeBSD, ajoutez la ligne suivante dans /etc/rc.conf:

```
mousechar_start=3
```

Le *nom_table_clavier* provient ici du répertoire /usr/shared/syscons/keymaps sans le suffixe .kbd. Si vous n'êtes pas sûr de la table de clavier à utiliser, vous pouvez employer kbdmap(1) pour tester la table sans avoir à redémarrer.

Le `keychange` est généralement utilisé pour programmer les touches de fonction pour correspondre avec le type de terminal sélectionné parce que les séquences de touches de fonction ne peuvent être définies dans la table de clavier.

Soyez également sûr de configurer le type de console correct dans le fichier /etc/ttys pour toutes les entrées `ttyv*`. Les correspondances actuellement pré-définies sont:

Jeu de caractères	Type de terminal
ISO8859-1 ou ISO8859-15	`cons25l1`
ISO8859-2	`cons25l2`
ISO8859-7	`cons25l7`
KOI8-R	`cons25r`
KOI8-U	`cons25u`
CP437 (jeu de caractères VGA par défaut)	`cons25`
US-ASCII	`cons25w`

Pour les langues au caractères étendus ou multi-octets, utilisez le logiciel porté adéquat de votre

répertoire /usr/ports/langue. Certains logiciels apparaissent comme utilisant la console alors que le système lui voit un vtty série, par conséquent vous devez réserver suffisamment de vttys pour X11 et la console pseudo-série. Voici une liste partielle des applications pour utiliser d'autres langues sous la console:

Langue	Emplacement
Chinois traditionnel (BIG-5)	chinese/big5con
Japonais	japanese/kon2-16dot ou japanese/mule_freewnn
Coréen	korean/han

25.3.6. Configuration d'X11

Bien qu'X11 ne fasse pas partie du projet FreeBSD, nous avons inclus quelques éléments d'informations ici pour les utilisateurs de FreeBSD. Pour plus de détails, référez-vous au site Web d'Xorg ou à celui du serveur X11 que vous utilisez.

Dans le fichier ~/.Xresources, vous pouvez en plus adapter les paramètres I18N spécifiques des applications (e.g., polices de caractères, menus, etc...).

25.3.6.1. Affichage des polices de caractères

Installez le serveur Xorg (x11-servers/xorg-server) ou le serveur XFree86™ (x11-servers/XFree86-4-Server), puis installez les polices de caractères TrueType® de la langue concernée. Un paramétrage correct des "locales" devrait vous permettre de visualiser les menus dans la langue que vous avez choisie etc.

25.3.6.2. Saisie de caractères non-anglais

Le protocole "X11 Input Method" - méthode de saisie pour X11 (XIM) est un nouveau standard pour tous les clients X11. Toutes les applications X11 devraient être écrites en tant que clients XIM qui reçoivent les entrées de serveurs de saisie XIM. Il existe différents serveurs XIM disponibles pour différentes langues.

25.3.7. Configuration de l'imprimante

Certains jeux de caractères de la bibliothèque C sont généralement codés en dur dans les imprimantes. Les jeux de caractères étendus ou multi-octets demandent une configuration spéciale et nous recommandons d'utiliser apsfilter. Vous pouvez également convertir le document en format PostScript® ou PDF en utilisant des convertisseurs spécifiques à la langue.

25.3.8. Noyau et systèmes de fichiers

Le système de fichiers rapide de FreeBSD (FFS) est complètement sur 8 bits, et peut donc être utilisé avec n'importe quel jeu de caractères de la bibliothèque C (voir multibyte(3)), mais il n'y a aucun jeu de caractères de stocké dans le système de fichiers; i.e., c'est du 8 bits brut et le système ne sait rien sur l'ordre du codage. Officiellement, le FFS ne supporte encore aucun jeu de caractères étendus ou multi-octets. Cependant, certains jeux de caractères étendus ou multi-octets disposent de correctifs indépendants pour FFS activant un tel support. Ce sont seulement des solutions

temporaires non portables ou des "bidouilles" et nous avons décidé de ne pas les inclure dans l'arborescence des sources. Référez-vous aux sites Internet des langues respectives pour plus d'informations et pour les correctifs.

Le support FreeBSD du système fichiers MS-DOS® a la capacité paramétrable de faire la conversion entre jeux de caractères MS-DOS®, Unicode et les jeux de caractères choisis pour le système de fichiers FreeBSD. Voir la page de manuel mount_msdosfs(8) pour plus de détails.

25.4. Compiler des programmes I18N

De nombreux logiciels ont été portés pour FreeBSD avec le support I18N. Certains d'entre eux sont identifiés avec -I18N dans le nom du logiciel porté. Ces derniers et beaucoup d'autres programmes intègrent le support I18N et ne nécessitent aucune considération spéciale.

Cependant, certaines applications comme MySQL nécessitent d'avoir un fichier Makefile configuré avec le jeu de caractères spécifiques. Ceci est en général fait dans le Makefile ou effectué en passant une valeur à configure dans les sources.

25.5. Localiser FreeBSD pour des langues spécifiques

25.5.1. Russe (codage KOI8-R)

Pour plus d'informations sur le codage KOI8-R, consultez les Références KOI8-R (Jeu de caractères russes pour Internet).

25.5.1.1. Configuration des "locales"

Ajoutez les lignes suivantes dans votre fichier ~/.login_conf:

```
me:My Account:\
    :charset=KOI8-R:\
    :lang=ru_RU.KOI8-R:
```

Voir plus haut dans ce chapitre pour des exemples de configuration des "locales".

25.5.1.2. Configuration de la console

- Ajoutez la ligne suivante à votre fichier /etc/rc.conf:

  ```
  mousechar_start=3
  ```

- Ajoutez également les paramétres suivants dans /etc/rc.conf:

  ```
  keymap="ru.utf-8"
  scrnmap="utf-82cp866"
  font8x16="cp866b-8x16"
  ```

```
font8x14="cp866-8x14"
font8x8="cp866-8x8"
```

- Pour chaque entrée `ttyv*` dans /etc/ttys, utilisez `cons25r` comme type de terminal.

Voir plus haut dans ce chapitre pour des exemples de configuration de la console.

25.5.1.3. Configuration de l'imprimante

Comme la plupart des imprimantes avec un jeu de caractères russes ont un "code page" matériel CP866, un filtre de sortie spécial pour la conversion du KOI8-R vers le CP866 est nécessaire. Un tel filtre est installé par défaut sous /usr/libexec/lpr/ru/koi2alt. Une entrée de /etc/printcap pour imprimante russe devra ressembler à:

```
lp|Russian local line printer:\
    :sh:of=/usr/libexec/lpr/ru/koi2alt:\
    :lp=/dev/lpt0:sd=/var/spool/output/lpd:lf=/var/log/lpd-errs:
```

Consultez la page de manuel printcap(5) pour plus de détails.

25.5.1.4. Système de fichiers MS-DOS® et noms de fichiers russes

L'exemple suivant d'entrée du fichier fstab(5) active le support des noms de fichiers russes sur les systèmes de fichiers MS-DOS® montés:

```
/dev/ad0s2      /dos/c  msdos   rw,-Wkoi2dos,-Lru_RU.KOI8-R 0 0
```

L'option `-L` la "locale" utilisée, et `-W` fixe la table de conversion de caractères. Pour utiliser l'option `-W` assurez-vous de monter /usr avant la partition MS-DOS®, car en effet les tables de conversion sont situées dans le répertoire /usr/libdata/msdosfs. Pour plus d'informations, consultez la page de manuel mount_msdosfs(8).

25.5.1.5. Configuration de X11

1. Effectuez tout d'abord la configuration des "locales" comme décrit plus haut dans ce chapitre.
2. Si vous utilisez Xorg, installez le paquetage x11-fonts/xorg-fonts-cyrillic.

   Contrôlez la section `"Files"` de votre fichier /etc/X11/xorg.conf. Les lignes suivantes doivent être ajoutées *avant* toute autre entrée `FontPath`:

   ```
   FontPath   "/usr/X11R6/lib/X11/fonts/cyrillic/misc"
   FontPath   "/usr/X11R6/lib/X11/fonts/cyrillic/75dpi"
   FontPath   "/usr/X11R6/lib/X11/fonts/cyrillic/100dpi"
   ```

   Si vous utilisez un mode vidéo haute résolution, intervertissez les lignes 75 dpi et 100 dpi.

Consultez le catalogue des logiciels portés pour plus de fontes cyrilliques.

3. Pour mettre en service un clavier russe, ajoutez ce qui suit à la section `"Keyboard"` de votre fichier xorg.conf:

```
Option "XkbLayout"   "us,ru"
Option "XkbOptions"  "grp:toggle"
```

Vérifiez également que `XkbDisable` est désactivé (mis en commentaire).

Pour l'option `grp:caps_toggle` le passage de russe à latin se fera par l'intermédiaire de `Right Alt`, pour `grp:ctrl_shift_toggle`, le passage se fera à l'aide de la séquence `Ctrl` + `Shift`. L'ancienne fonctionnalitée de la touche `CapsLock` est toujours disponible via `Shift` + `CapsLock` (en mode latin uniquement). Pour l'option `grp:toggle` le passage du russe au latin se fera par l'intermédiaire de la touche `Right Alt`. L'option `grp:caps_toggle` ne fonctionne pas sous Xorg pour une raison inconnue.

Si vous disposez de touches "Windows®" sur votre clavier, et que vous constatez que certaines touches non-alphabétiques ne sont pas appariées correctement en mode russe, ajoutez la ligne suivante à votre fichier xorg.conf:

```
Option "XkbVariant" ",winkeys"
```

Le clavier russe XKB peut ne pas fonctionner avec des applications non localisées.

localisées. Pour être un minimum localisée, une application devrait appeler la fonction `XtSetLanguageProc (NULL, NULL, NULL);` assez tôt dans le programme.

Consulter KOI8-R pour X Window pour plus d'instructions sur la localisation des applications pour X11.

25.5.2. Localisation du chinois traditionnel pour Taiwan

Le projet FreeBSD taiwanais dispose d'un guide sur FreeBSD en chinois à l'adresse http://netlab.cse.yzu.edu.tw/~statue/freebsd/zh-tut/ utilisant de nombreuses applications du répertoire chinese du catalogue des logiciels portés. Le rédacteur du guide sur FreeBSD en chinois est Shen Chuan-Hsing statue@freebsd.sinica.edu.tw.

Chuan-Hsing Shen statue@freebsd.sinica.edu.tw a créé la collection FreeBSD chinoise (CFC) de logiciels en utilisant le document `zh-L10N-tut` taiwanais. Les logiciels pré-compilés et les fichiers de procédures sont disponibles à l'adresse ftp://freebsd.csie.nctu.edu.tw/pub/taiwan/CFC/.

25.5.3. Localisation pour la langue allemande (valable également pour tous les langues respectant le standard ISO 8859-1)

Slaven Rezic eserte@cs.tu-berlin.de a rédigé un guide sur l'utilisation des "umlauts" sur une machine FreeBSD. Le guide est écrit en allemand et est disponible sur http://user.cs.tu-berlin.de/~eserte/FreeBSD/doc/umlaute/umlaute.html.

25.5.4. Localisation pour le japonais et le coréen

Pour le japonais, référez-vous à http://www.jp.FreeBSD.org/, et pour le coréen à http://www.kr.FreeBSD.org/.

25.5.5. Documentation FreeBSD dans d'autres langues que l'anglais

Certains contributeurs à FreeBSD ont traduit des parties de la documentation FreeBSD dans d'autres langues. Les traductions sont disponibles grâce à des liens sur le site principal ou dans /usr/shared/doc.

Chapitre 26. Mise à jour de FreeBSD

26.1. Synopsis

FreeBSD est en constant développement entre deux versions. Certains utilisateurs préfèrent utiliser les versions publiées officiellement alors que d'autres voudront rester à jour avec les tous derniers développements. Mêmes les versions officielles sont souvent mises à jour avec les correctifs de problèmes critiques et de sécurité. Indépendamment de la version utilisée, FreeBSD fournit tous les outils nécessaires à la mise à jour de votre système, et permet également des mises à jour aisées entre versions. Ce chapitre vous aidera à décider si vous voulez suivre les développements, ou vous en tenir aux versions publiées. Les outils de base pour le maintien à jour de votre système seront également présentés.

Après la lecture de ce chapitre, vous connaîtrez:

- Quels utilitaires peuvent être employés pour mettre à jour le système et le catalogue des logiciels portés.
- Comment maintenir votre système à jour avec freebsd-update, CVSup, CVS, ou CTM.
- Comment comparer l'état d'un système installé avec une copie de confiance.
- La différence entre les deux branches de développement: FreeBSD-STABLE et FreeBSD-CURRENT.
- Comment recompiler et réinstaller l'intégralité du système de base avec la commande `make buildworld` (etc.).

Avant de lire ce chapitre, vous devrez:

- Correctement configurer votre connexion réseau (Administration réseau avancée).
- Savoir comment installer des logiciels tiers (Installer des applications. les logiciels pré-compilés et les logiciels portés).

Tout au long de ce chapitre, la commande `cvsup` sera utilisée pour récupérer et mettre à jour les sources de FreeBSD. Pour l'utiliser, vous devrez installer un logiciel porté ou pré-compilé tel que net/cvsup-without-gui. Si vous utilisez FreeBSD 6.2-RELEASE ou une version ultérieure, vous pouvez remplacer cette commande par csup(1), qui fait désormais partie du système de base.

26.2. Mise à jour de FreeBSD

Appliquer des correctifs de sécurité est une part importante de la maintenance de logiciels informatiques tout particulièrement dans le cas du système d'exploitation. Pendant très longtemps sous FreeBSD, ce processus n'était pas aisé. Les correctifs devaient être appliqués au code source, le code ensuite recompilé sous forme de binaires, et enfin les binaires devaient être ré-installés.

Ce processus n'est plus de mise comme FreeBSD dispose désormais d'un utilitaire appelé simplement `freebsd-update`. Cet utilitaire fournit deux fonctions distinctes. Tout d'abord, il permet

l'application de mises à jour de correction et de sécurité sur le système de base de FreeBSD sans nécessiter une compilation et une ré-installation. En second lieu, l'utilitaire supporte les mises à jour mineures et majeures des versions publiées.

Les mise à jour binaires sont disponibles pour toutes les architectures actuellement supportées par l'équipe de sécurité. Avant de mettre à jour vers une nouvelle version, les annonces concernant la version devront être passées en revue sachant qu'elles peuvent contenir des informations importantes au sujet de cette version. Ces annonces peuvent être consultées à l'adresse suivante: http://www.FreeBSD.org/releases/.

S'il existe une table `crontab` utilisant `freebsd-update`, elle doit être désactivée avant de démarrer les opérations qui vont suivre.

26.2.1. Le fichier de configuration

Certains utilisateurs peuvent souhaiter adapter le fichier de configuration par défaut /etc/freebsd-update.conf, permettant un meilleur contrôle du processus. Les options sont très bien documentées, mais les suivantes demandent un peu plus d'explication:

```
# Composants du système de base qui doivent être maintenus à jour.
Components src world kernel
```

Ce paramètre contrôle quelles sont les parties de FreeBSD qui seront mises à jour. Par défaut on met à jour le code source, l'intégralité du système de base et le noyau. Les composants sont les mêmes que ceux disponibles durant l'installation, par exemple, ajouter `world/games` ici permettrait d'appliquer les correctifs relatifs aux jeux. Utiliser `src/bin` permettrait la mise à jour du code source du répertoire src/bin.

La meilleure option est de laisser telle quelle la configuration par défaut car la modifier pour ajouter des éléments particuliers demandera à l'utilisateur de lister chaque élément qu'il désire mettre à jour. Cela pourrait avoir des conséquences désastreuses puisque le code source et les binaires peuvent à terme ne plus être en phase.

```
# Les chemins d'accès commençant par quelque chose correspondant à une
# entrée de type IgnorePaths seront ignorés.
IgnorePaths
```

Ajoute les chemins d'accès comme /bin ou /sbin pour préserver intacts ces répertoires durant le processus de mise à jour. Cette option peut être utilisée pour empêcher `freebsd-update` d'écraser des modifications locales.

```
# Les chemins d'accès qui commencent par quelque chose correspondant à
# une entrée de type UpdateIfUnmodified seront mis à jour que si le
# contenu du fichier n'a pas été modifié par l'utilisateur (à moins
# que les modifications ne soient fusionnées; voir plus bas).
```

```
UpdateIfUnmodified /etc/ /var/ /root/ /.cshrc /.profile
```

Met à jour les fichiers de configuration dans les répertoires désignés seulement s'ils n'ont pas été modifiés. Tout changement effectué par l'utilisateur invalidera automatiquement la mise à jour de ces fichiers. Il existe une autre option `KeepModifiedMetadata` qui indiquera à `freebsd-update` de sauvegarder les changements durant la fusion.

```
# Quand on met à jour vers une nouvelle version de FreeBSD, les fichiers
# correspondant à une entrée de type MergeChanges verront leurs
# différences locales fusionnées avec le fichier de la nouvelle
# version de FreeBSD.
MergeChanges /etc/ /var/named/etc/
```

Liste des répertoires avec des fichiers de configuration que `freebsd-update` devrait tenter de fusionner. Le processus de fusion des fichiers est l'application d'une série de correctifs diff(1) similaires à ceux de mergemaster(8) avec cependant moins d'options, les fusions sont soit acceptées, ouvrant un éditeur, soit abandonnées par `freebsd-update`. En cas de doute, sauvegardez /etc et acceptez les fusions. Consultez la section sur `mergemaster` pour plus d'information sur la commande `mergemaster`.

```
# Répertoire dans lequel stocker les mise à jour téléchargées et les
# fichiers temporaires utilisés par la mise à jour de FreeBSD.
# WorkDir /var/db/freebsd-update
```

Ce répertoire est l'endroit où tous les correctifs et les fichiers temporaires seront placés. Dans les cas où l'utilisateur effectue une mise à jour de version, cet emplacement doit disposer d'au moins un gigaoctet d'espace disponible.

```
# Lors de mises à jour entre versions de FreeBSD, doit-on lire la liste
# de composants de manière stricte (StrictComponents yes)
# ou tout simplement comme une liste de composants qui *pourraient*
# être installés et pour lesquels la mise à jour de FreeBSD devrait
# déterminer lesquels sont effectivement installés et les mettre à
# jour (StrictComponents no)?
# StrictComponents no
```

Cette option fixée à `yes`, `freebsd-update` supposera que la liste de composants est complète et n'essaiera pas d'effectuer des modifications en dehors de cette liste. Concrètement, `freebsd-update` tentera de mettre à jour chaque fichier appartenant à la liste de composants.

26.2.2. Correctifs de sécurité

Les correctifs de sécurité sont stockés sur une machine distante et peuvent être téléchargés et installés en utilisant la commande suivante:

```
# freebsd-update fetch
# freebsd-update install
```

Si des correctifs ont été appliqués au noyau le système devra être redémarré. Si tout s'est bien passé le système est corrigé et `freebsd-update` pourra être exécuté chaque nuit via un processus cron(8). Une entrée dans le fichier /etc/crontab devrait être suffisante pour accomplir cette tâche:

```
@daily                                  root    freebsd-update cron
```

Cette entrée indique qu'une fois par jour, l'utilitaire `freebsd-update` sera exécuté. De cette manière, en employant l'option `cron`, `freebsd-update` vérifiera seulement l'existence de mises à jour. Si des correctifs existent, il seront automatiquement téléchargés sur le disque local mais non-appliqués. L'utilisateur `root` sera contacté par courrier électronique, il pourra ainsi les installer manuellement.

Si quelque s'est mal passé, `freebsd-update` a la capacité d'annuler le dernier ensemble de changements avec la commande suivante:

```
# freebsd-update rollback
```

Une fois la commande achevée, le système devra être redémarré si le noyau ou un de ses modules ont été modifiés. Cela permettra à FreeBSD de charger en mémoire les nouveaux binaires.

L'utilitaire `freebsd-update` peut mettre à jour uniquement et automatiquement le noyau `GENERIC`. Si un noyau personnalisé est utilisé, il devra être recompilé et réinstallé après que la commande `freebsd-update` ait achevé l'installation du reste des mises à jour. Cependant `freebsd-update` détectera et mettra à jour le noyau `GENERIC` dans /boot/GENERIC (s'il existe), et cela même si ce n'est pas le noyau actuel (qui tourne) du système.

C'est toujours une bonne idée de conserver une copie du noyau `GENERIC` dans /boot/GENERIC. Cela sera utile pour diagnostiquer une variété de problèmes, et lors des mises à jour utilisant `freebsd-update` comme décrit dans la Mises à jour mineures et majeures.

A moins que la configuration par défaut présente dans /etc/freebsd-update.conf n'ait été modifiée, `freebsd-update` installera les sources du noyau mises à jour avec le reste des mises à jour. La recompilation et la réinstallation d'un noyau personnalisé peuvent effectuées de la manière classique.

Les mises à jour distribuées via `freebsd-update`, n'impliquent pas toujours le noyau. Il ne sera pas nécessaire de recompiler votre noyau personnalisé si les sources du noyau n'ont pas été modifiées par l'exécution de `freebsd-update install`. Cependant `freebsd-update` met toujours à jour le fichier /usr/src/sys/conf/newvers.sh. Le niveau ou la version de correctifs (comme indiqué par le nombre `-p` rapporté par `uname -r`) est obtenu à partir de ce fichier. Recompiler votre noyau personnalisé, même si rien d'autre n'a changé, permettra

> à la commande uname(1) de rapporter précisément le niveau de correctifs du système. C'est particulièrement utile quand on gère de multiples systèmes, car cela permet une évaluation rapide des mises à jour présentes sur chacun d'eux.

26.2.3. Mises à jour mineures et majeures

Ce processus supprimera les anciens fichiers objets et bibliothèques qui rendent inutilisables la plupart des applications tierce-partie. Il est recommandé que tous les logiciels portés soient supprimés et réinstallés ou mis à jour ultérieurement en utilisant l'outil ports-mgmt/portupgrade. La plupart des utilisateurs voudront lancer une compilation test à l'aide de la commande suivante:

```
# portupgrade -af
```

Cela garantira que tout sera réinstallé correctement. Notez que fixer la variable d'environnement `BATCH` à `yes` répondra `yes` à toute question lors de ce processus, supprimant ainsi la nécessité d'une intervention humaine durant le processus de compilation.

Si un noyau personnalisé est utilisé, le processus de mise à jour est un peu plus complexe. Une copie du noyau `GENERIC` est nécessaire et devrait être placée dans le répertoire /boot/GENERIC. Si le noyau `GENERIC` n'est pas présent sur le système, il peut être obtenu en utilisant une des méthodes suivantes:

- Si un noyau personnalisé a déjà été compilé, le noyau présent dans /boot/kernel.old est en fait le noyau `GENERIC`. Renommer ce répertoire en /boot/GENERIC.
- En supposant qu'un accès physique à la machine est possible, une copie du noyau `GENERIC` peut être installé à partir d'un CD-ROM. Insérer votre disque d'installation et utiliser les commandes suivantes:

  ```
  # mount /cdrom
  # cd /cdrom/X.Y-RELEASE/kernels
  # ./install.sh GENERIC
  ```

  Remplacer X.Y-RELEASE avec la version que vous utilisez. Le noyau `GENERIC` sera installé par défaut dans /boot/GENERIC.

- En dehors de ce qui précède le noyau `GENERIC` peut être recompilé et installé à partir des sources:

  ```
  # cd /usr/src
  # env DESTDIR=/boot/GENERIC make kernel
  # mv /boot/GENERIC/boot/kernel/* /boot/GENERIC
  # rm -rf /boot/GENERIC/boot
  ```

  Pour que ce noyau soit pris en compte comme `GENERIC` par `freebsd-update`, le fichier de configuration `GENERIC` devra ne pas avoir été modifié. Il est également suggéré qu'il soit compilé sans aucune option particulière (de préférence avec un fichier /etc/make.conf vide).

Redémarrer avec le noyau GENERIC n'est pas nécessaire à ce stade.

Les mises à jour de versions majeures et mineures peuvent être effectuées en passant à la commande freebsd-update la version vers laquelle on désire mettre à jour, par exemple, la commande suivante effectuera la mise à jour vers FreeBSD 8.1:

```
# freebsd-update -r 8.1-RELEASE upgrade
```

La commande freebsd-update analysera le fichier de configuration et le système afin de récupérer les informations nécessaires à la mise à jour du système. A l'écran s'affichera quels sont les composants détectés et quels sont ceux qui n'ont pas été détectés. Par exemple:

```
Looking up update.FreeBSD.org mirrors... 1 mirrors found.
Fetching metadata signature for 8.0-RELEASE from update1.FreeBSD.org... done.
Fetching metadata index... done.
Inspecting system... done.

The following components of FreeBSD seem to be installed:
kernel/smp src/base src/bin src/contrib src/crypto src/etc src/games
src/gnu src/include src/krb5 src/lib src/libexec src/release src/rescue
src/sbin src/secure src/share src/sys src/tools src/ubin src/usbin
world/base world/info world/lib32 world/manpages

The following components of FreeBSD do not seem to be installed:
kernel/generic world/catpages world/dict world/doc world/games
world/proflibs

Does this look reasonable (y/n)? y
```

A ce niveau freebsd-update tentera de télécharger tous les fichiers nécessaires à la mise à jour. Dans certains cas l'utilisateur sera interrogé sur ce qu'il faut installer ou sur comment procéder à certaines actions.

Si un noyau personnalisé est utilisé, l'étape précédente produira un avertissement semblable au suivant:

```
WARNING: This system is running a "MYKERNEL" kernel, which is not a
kernel configuration distributed as part of FreeBSD 8.0-RELEASE.
This kernel will not be updated: you MUST update the kernel manually
before running "/usr/sbin/freebsd-update install"
```

Cet avertissement peut sans risque être ignoré à ce niveau. Le noyau GENERIC mis à jour sera utilisé comme une étape intermédiaire dans le processus de mise à jour.

Une fois l'ensemble des correctifs téléchargé sur le système local, ils seront appliqués. Ce processus peut prendre plus ou moins de temps en fonction de la vitesse et de la charge de la machine. Les fichiers de configuration seront fusionnés - cette partie du processus demande l'intervention de

l'utilisateur car un fichier peut être automatiquement fusionné ou en cas de besoin un éditeur peut apparaître sur l'écran pour une fusion manuelle. Les résultats des fusions réussies seront affichés au fur et à mesure que se déroule l'opération. Un échec ou une fusion ignorée provoqueront l'arrêt du processus. Certains utilisateurs peuvent vouloir conserver une sauvegarde du répertoire /etc et fusionner plus tard à la main les fichiers importants comme master.passwd ou group.

Le système n'a pas encore été réellement modifié, les fusions et l'application des correctifs ont lieu dans un autre répertoire. Quand tous les correctifs ont été appliqués avec succès, que tous les fichiers de configuration ont été fusionnés et que le processus s'est déroulé sans problème, les modifications devront être appliquées définitivement au système par l'utilisateur.

Une fois les opérations précédentes achevées, la mise à jour peut être appliquée en utilisant la commande suivante:

```
# freebsd-update install
```

Le noyau et les modules seront corrigés les premiers. A ce moment la machine doit être obligatoirement redémarrée. Si le système utilisait un noyau personnalisé, utiliser la commande nextboot(8) pour indiquer le noyau /boot/GENERIC (qui a été mis à jour) pour le prochain démarrage:

```
# nextboot -k GENERIC
```

Avant de redémarrer sur le noyau `GENERIC`, assurez-vous qu'il contient tous les pilotes nécessaires pour que votre système démarre correctement (et se connecte au réseau, si la mise à jour de la machine se fait à distance). En particulier, si le noyau précédemment utilisé contient des fonctions généralement fournies par des modules, faites en sorte de charger temporairement ces modules avec le noyau GENERIC à l'aide de /boot/loader.conf. Vous pouvez également avoir intérêt à désactiver les services non-indispensables, les montages réseaux ou disques, etc. avant que le processus de mise à jour ne soit achevé.

La machine doit maintenant être redémarrée avec le noyau mis à jour:

```
# shutdown -r now
```

Une fois la machine de nouveau active, `freebsd-update` devra être lancée à nouveau. L'état du processus de mise à jour a été sauvegardé, et donc `freebsd-update` ne recommencera pas au début, mais supprimera les anciens fichiers objet et bibliothèques partagées. Afin de poursuivre les opérations, taper la commande suivante:

```
# freebsd-update install
```

En fonction d'un changement ou non de numérotation d'une ou plusieurs bibliothèques, il pourra y avoir deux phases d'installation au lieu de trois.

Tous les logiciels tierce-partie doivent être maintenant recompilés et réinstallés. Cela est nécessaire comme certains logiciels peuvent dépendre de bibliothèques qui ont été supprimées lors du processus de mise à jour. La commande ports-mgmt/portupgrade peut être employée pour automatiser la chose. Les commandes suivantes peuvent être utilisées pour initier le processus:

```
# portupgrade -f ruby
# rm /var/db/pkg/pkgdb.db
# portupgrade -f ruby18-bdb
# rm /var/db/pkg/pkgdb.db /usr/ports/INDEX-*.db
# portupgrade -af
```

Une fois cela effectué, terminer le processus de mise à jour avec un dernier appel à `freebsd-update`. Taper la commande suivante pour régler les derniers détails:

```
# freebsd-update install
```

Si le noyau `GENERIC` a été utilisé temporairement, il est temps de compiler et d'installer un nouveau noyau personnalisé suivant la méthode habituelle.

Redémarrer la machine avec la nouvelle version de FreeBSD. Le processus de mise à jour est terminé.

26.2.4. Comparaison de l'état du système

L'utilitaire `freebsd-update` peut être utilisé pour comparer l'état du système FreeBSD installé avec une copie de confiance. Cette fonctionnalité inspecte la version actuelle des utilitaires système, des bibliothèques et des fichiers de configuration. Pour lancer la comparaison, utiliser la commande suivante:

```
# freebsd-update IDS >> outfile.ids
```

Bien que le nom de la commande soit IDS, elle ne devrait en aucun cas être considérée comme un système de détection d'intrusion du type de security/snort. Etant donné que `freebsd-update` stocke des données sur le disque, le risque de modification des données est évident. Alors que cette possibilité peut être minimisée en utilisant le paramétrage `kern.securelevel` et en stockant les données `freebsd-update` sur un système de fichiers en lecture seule quand elles ne sont pas utilisées, une bien meilleure solution serait de comparer le système avec un disque sécurisé comme un DVD ou un disque USB conservé à l'extérieur.

Le système sera analysé, et une liste de fichiers ainsi que la valeur de leur empreinte numérique sha256(1), celle de la version d'origine et celle de la version actuellement installée, seront affichés.

C'est pour cela que cet affichage est copié dans le fichier outfile.ids. L'affichage défile trop rapidement une comparaison visuelle et remplira rapidement le tampon de la console.

Ces lignes sont également très longues mais le format de sortie peut être facilement passé par une analyse syntaxique. Par exemple, pour obtenir une liste des fichiers qui diffèrent avec ceux de la version d'origine, utiliser la commande suivante:

```
# cat outfile.ids | awk '{ print $1 }' | more
/etc/master.passwd
/etc/motd
/etc/passwd
/etc/pf.conf
```

La sortie de cette commande a été tronquée, bien plus de fichiers sont concernés. Certains de ces fichiers sont naturellement modifiés, le fichier /etc/passwd a été modifié en raison de l'ajout d'utilisateurs au système. Dans certains cas, d'autres fichiers apparaîtrons, comme les modules du noyau, qui diffèrent puisque `freebsd-update` peut les avoir mis à jour. Pour exclure des fichiers ou des répertoires spécifiques, ajoutez-les au paramètre `IDSIgnorePaths` dans le fichier /etc/freebsd-update.conf.

Ce système peut prendre part à une méthode de mise à jour élaboré, en dehors de ce qui a été présenté précédemment.

26.3. Portsnap: un outil de mise à jour du catalogue des logiciels portés

Le système de base de FreeBSD dispose également d'un utilitaire pour la mise à jour du catalogue des logiciels portés: portsnap(8). Lors de son exécution, il se connectera sur un site distant, contrôlera la clé de sécurité et téléchargera une nouvelle copie du catalogue des logiciels portés. La clé est utilisée pour vérifier l'intégrité de tous les fichiers téléchargés, s'assurant qu'ils n'ont pas été modifiés au vol. Pour récupérer les tout derniers fichiers du catalogue des logiciels portés, utiliser la commande suivante:

```
# portsnap fetch
Looking up portsnap.FreeBSD.org mirrors... 3 mirrors found.
Fetching snapshot tag from portsnap1.FreeBSD.org... done.
Fetching snapshot metadata... done.
Updating from Wed Aug  6 18:00:22 EDT 2008 to Sat Aug 30 20:24:11 EDT 2008.
Fetching 3 metadata patches.. done.
Applying metadata patches... done.
Fetching 3 metadata files... done.
Fetching 90 patches.....10....20....30....40....50....60....70....80....90. done.
Applying patches... done.
Fetching 133 new ports or files... done.
```

Cet exemple nous montre que portsnap(8) a trouvé et contrôlé plusieurs mises à jour pour les

données actuelles du catalogue. Est également indiqué si l'utilitaire a été précédemment exécuté, si cela avait été une première exécution, le catalogue aurait été tout simplement téléchargé.

Lorsque portsnap(8) termine avec succès une opération de récupération (`fetch`), le catalogue des logiciels portés et ses mises à jour sont présents sur le système. A la première exécution de `portsnap` vous devez utiliser la commande `extract` pour installer les fichiers téléchargés:

```
# portsnap extract
/usr/ports/.cvsignore
/usr/ports/CHANGES
/usr/ports/COPYRIGHT
/usr/ports/GIDs
/usr/ports/KNOBS
/usr/ports/LEGAL
/usr/ports/MOVED
/usr/ports/Makefile
/usr/ports/Mk/bsd.apache.mk
/usr/ports/Mk/bsd.autotools.mk
/usr/ports/Mk/bsd.cmake.mk
...
```

Pour mettre à jour un catalogue des logiciels portés déjà installé utilisez la commande `portsnap update`:

```
# portsnap update
```

Le processus est maintenant terminé et les applications peuvent être installées ou mises à jour à l'aide du catalogue à jour.

Les opérations `fetch` et `extract` ou `update` peuvent être exécutées à la suite comme montré dans l'exemple suivant:

```
# portsnap fetch update
```

Cette commande téléchargera la dernière version du catalogue des logiciels portés et mettra à jour votre version locale située dans /usr/ports.

26.4. Updating the Documentation Set Traduction en Cours

26.4.1. Updating Documentation from Source

26.4.2. Updating Documentation from Ports

26.5. Suivre une branche de développement

Il existe deux branches de développement de FreeBSD: FreeBSD-CURRENT et FreeBSD-STABLE. Cette section détaillera un peu chacune d'elles et décrira comment garder à jour votre système avec chaque arborescence respective. FreeBSD-CURRENT sera tout d'abord traité, suivit de FreeBSD-STABLE.

26.5.1. Se synchroniser avec la version -CURRENT de FreeBSD

En lisant ces lignes, gardez à l'esprit que FreeBSD-CURRENT représente "les tout derniers" développement de FreeBSD. On attend des utilisateurs de FreeBSD-CURRENT un degré élevé de compétences techniques, et devraient être capables de résoudre des problèmes système compliqués par eux-mêmes. Si vous êtes nouveau à FreeBSD, pensez à deux fois avant de l'installer.

26.5.1.1. Qu'est-ce que FreeBSD-CURRENT?

FreeBSD-CURRENT est la toute dernière version des sources de FreeBSD en cours de développement. Cela inclut des évolutions en cours, des modifications expérimentales, et des mécanismes de transition qui feront ou ne feront pas partie de la prochaine version officielle du logiciel. Bien que de nombreux développeurs de FreeBSD compilent les sources de FreeBSD-CURRENT quotidiennement, il arrive que celles-ci ne soient pas compilables pendant une certaine période de temps. Ces problèmes sont résolus aussi rapidement que possible, mais que FreeBSD-CURRENT soit à l'origine d'un désastre ou de l'apport d'une nouvelle fonctionnalité attendue peut parfois dépendre que du moment auquel vous avez chargé le code source.

26.5.1.2. Qui a besoin de FreeBSD-CURRENT?

FreeBSD-CURRENT est mis à disposition pour 3 types de personnes:

1. Les membres de la communauté FreeBSD qui travaillent activement sur une partie de l'arborescence des sources et pour qui rester constamment à jour est une nécessité absolue.
2. Les membres de la communauté FreeBSD qui participent activement aux tests et sont disposés à passer du temps à résoudre les problèmes pour garantir que FreeBSD-CURRENT reste aussi saine que possible. Il y a également ceux qui désirent faire des suggestions dans certains domaines sur les modifications à faire et la direction générale que prend FreeBSD, et soumettent des correctifs pour les implémenter.
3. Ceux qui veulent simplement garder un oeil sur les évolutions, ou utiliser les dernières sources comme référence (e.g. pour les *lire*, et non pour les utiliser). Ces personnes font parfois des remarques ou contribuent au code.

26.5.1.3. Qu'est-ce que *n'est pas* FreeBSD-CURRENT?

1. Un raccourci pour se procurer des pré-versions parce que vous avez entendu dire qu'il y a de nouvelles fonctionnalités géniales et que vous voulez être le premier du coin à les avoir. Etre le premier à avoir la nouvelle fonctionnalité signifie être le premier à avoir les nouveaux bogues également.
2. Une moyen rapide d'avoir des corrections de bogues. N'importe quelle version de FreeBSD-CURRENT apportera probablement de nouveaux bogues comme elle corrigera ceux déjà

présents.

3. Nous ne le "supportons officiellement" en aucun cas. Nous faisons du mieux que nous pouvons pour aider les personnes qui font vraiment partie des trois groupes "légitimes" à qui s'adresse FreeBSD-CURRENT, mais nous n'avons tout simplement "pas le temps" de fournir un support technique. Ce n'est pas parce que nous sommes des personnes détestables qui n'aiment pas aider les autres (nous ne ferions pas FreeBSD si tel était le cas), nous ne pouvons simplement pas répondre à des centaines de messages par jour *et* travailler sur FreeBSD! Entre améliorer FreeBSD et répondre à de nombreuses questions sur le code expérimental, les développeurs optent pour le premier choix.

26.5.1.4. Utiliser FreeBSD-CURRENT

1. Inscrivez-vous à la liste de diffusion à propos de la branche FreeBSD-CURRENT et la messages SVN de modification pour l'arbre pour head/-current. Ce n'est pas seulement une bonne idée, c'est *indispensable*. Si vous n'êtes pas sur la liste *liste de diffusion à propos de la branche FreeBSD-CURRENT*, vous ne verrez pas les commentaires qui sont faits sur l'état courant du système et vous vous retrouverez probablement confrontés à de nombreux problèmes que d'autres ont déjà identifiés et résolus. Encore plus grave, vous manqueriez des bulletins importants potentiellement critiques pour la bonne santé de votre système.

   La liste messages SVN de modification pour l'arbre pour head/-current vous permettra de voir les courriers de trace des soumissions de toutes les modifications dès qu'elles sont faites et des informations pertinentes sur les éventuels effets de bord.

   Pour vous inscrire à ces listes, ou à une autre, rendez vous à https://lists.freebsd.org et cliquez sur la liste à laquelle vous désirez vous inscrire. Des instructions sur le reste de la procédure sont alors données. Si vous êtes intéressé par le suivi des modifications appliquées à l'ensemble de l'arborescence des sources, nous vous recommandons de vous inscrire à messages SVN de modification concernant l'intégrélité de l'arbre src (en dehors des arbres "user" et "projects").

2. Récupérez les sources sur un site miroir FreeBSD. Vous pouvez le faire de deux manières:

   a. Utilisez le programme cvsup avec le fichier supfile nommé standard-supfile disponible dans le répertoire /usr/shared/examples/cvsup. C'est la méthode recommandée, puisqu'elle permet de récupérer la totalité des sources la première fois et par la suite uniquement ce qui a été modifié. De nombreuses personnes exécutent `cvsup` depuis `cron` et maintiennent ainsi automatiquement à jour leurs sources. Vous devez personnaliser l'exemple de supfile précédent, et configurer cvsup pour votre environnement.

Le fichier d'exemple standard-supfile est destiné au suivi d'une branche de sécurité FreeBSD spécifique et non pas à celui de FreeBSD-CURRENT. Vous devrez éditer ce fichier et remplacer la ligne suivante:

```
*default release=cvs tag=RELENG_X_Y
```

Par celle-ci:

```
*default release=cvs tag=.
```

Pour une explication détaillée des étiquettes utilisables, veuillez vous référer à la section Etiquettes CVS de ce manuel.

b. Utilisez CTM. Si vous disposez d'une mauvaise connexion (connexions chères ou seulement un accès au courrier électronique) CTM est une bonne solution. Cependant, c'est une source de problèmes et peut donner lieu à des fichiers endommagés. C'est pourquoi cette méthode est rarement utilisée, ce qui augmente les chances que cela ne fonctionne pas pendant d'assez longue périodes. Nous recommandons d'utiliser CVSup à tous ceux disposant d'un modem 9600 bps ou d'une connexion plus rapide.

3. Si vous récupérez les sources pour compiler un système opérationnel, et pas simplement pour les lire, alors récupérez *tout* FreeBSD-CURRENT, et pas uniquement certaines portions. La raison de cela est que diverses parties des sources dépendent de modifications effectuées ailleurs, et si vous essayez de compiler juste une partie des source, il est quasiment certain que vous aurez des problèmes.

4. Avant de compiler FreeBSD-CURRENT, lisez attentivement le Makefile dans /usr/src. Vous devriez au moins la première fois installer un nouveau noyau et recompiler le système, comme étape nécessaire à votre processus de mise à jour. La lecture de la liste de diffusion à propos de la branche FreeBSD-CURRENT et du fichier /usr/src/UPDATING vous tiendra au courant des autres procédures de transition qui sont parfois nécessaires lorsque nous préparons la prochaine version.

5. Participez! Si vous utilisez FreeBSD-CURRENT, nous aimerions savoir ce que vous en pensez, tout particulièrement si vous avez des améliorations à nous suggérer ou des corrections de bogues à nous soumettre. Les suggestions accompagnées de code sont accueillies avec enthousiasme!

26.5.2. Se synchroniser avec la version -STABLE de FreeBSD

26.5.2.1. Qu'est-ce que FreeBSD-STABLE?

FreeBSD-STABLE est notre branche de développement à partir de laquelle sont extraites les versions majeures. Les modifications sur cette branche se font à une allure différente, et en supposant généralement qu'elles ont été tout d'abord testées sur FreeBSD-CURRENT. Cela reste cependant *toujours* une branche de développement, et cela signifie qu'à certains moments, les sources de FreeBSD-STABLE pourront être ou pas utilisables pour une quelconque raison. C'est tout simplement une autre branche de mise au point, et non pas une ressource pour l'utilisateur final.

26.5.2.2. Qui a besoin de FreeBSD-STABLE?

Si vous désirez suivre ou contribuer au processus de développement de FreeBSD, tout particulièrement si cela a rapport avec la prochaine version de FreeBSD, alors vous devriez penser à suivre FreeBSD-STABLE.

Bien qu'il soit vrai que les correctifs de sécurité vont également dans la branche FreeBSD-STABLE, vous n'avez pas *besoin* de suivre FreeBSD-STABLE pour cela. Chaque rapport de sécurité

concernant FreeBSD explique comment corriger le problème sur les versions affectées , et suivre intégralement une branche de développement juste pour des raisons de sécurité apportera également de nombreux changements non désirés.

Bien que nous tentons de nous assurer que la branche FreeBSD-STABLE soit compilable et constamment stable, cela ne peut être garanti. De plus, alors que le code est développé sous FreeBSD-CURRENT avant de l'inclure dans FreeBSD-STABLE, le nombre de personnes utilisant FreeBSD-STABLE est plus nombreux que celui utilisant FreeBSD-CURRENT, aussi il est inévitable que des bogues et des problèmes pourront parfois apparaître sous FreeBSD-STABLE alors qu'ils n'existaient pas sous FreeBSD-CURRENT.

Pour ces raisons, nous ne recommandons *pas* de suivre aveuglément FreeBSD-STABLE, et il est tout particulièrement important que vous ne mettiez pas à jour des serveurs de production sous FreeBSD-STABLE sans avoir tout d'abord testé le code dans votre environnement de travail.

Si vous ne disposez pas des ressources pour faire cela alors nous recommandons que vous utilisiez la version de FreeBSD la plus récente, et que vous utilisiez le mécanisme de mise à jour binaire pour passer d'une version à une autre.

26.5.2.3. Utiliser FreeBSD-STABLE

1. Inscrivez-vous à à la liste liste de diffusion à propos de la branche FreeBSD-STABLE;. Vous serez tenu au courant des dépendances de compilation qui peuvent apparaître dans la branche FreeBSD-STABLE ou de tout autre problème demandant une attention particulière. Les développeurs publieront également des annonces sur cette liste lorsqu'ils envisagent une correction ou modification controversée, offrant la possibilité aux utilisateurs de répondre s'ils ont des questions à soulever en rapport avec la modification proposée.

   Inscrivez-vous à la liste SVN correspondant à la branche que vous suivez. Par exemple, si vous suivez la branche 7-STABLE, inscrivez-vous à la liste svn-src-stable-7. Cela vous permettra de lire les courriers de trace des soumissions de toutes les modifications dès qu'elles sont faites et des informations pertinentes sur les éventuels effets de bord.

   Pour vous inscrire à ces listes, ou à une autre, rendez vous à https://lists.freebsd.org et cliquez sur la liste à laquelle vous désirez vous inscrire. Des instructions sur le reste de la procédure sont alors données. Si vous êtes intéressé par le suivi des modifications appliquées à l'ensemble de l'arborescence des sources, nous vous recommandons de vous inscrire à messages SVN de modification concernant l'intégrélité de l'arbre src (en dehors des arbres "user" et "projects").

2. Si vous installez un nouveau système et vous voulez qu'il utilise le dernier instantané publié tous les mois à partir de la branche FreeBSD-STABLE, consultez la page sur les instantanés pour plus d'information. D'autre part, vous pouvez installer la version FreeBSD-STABLE la plus récente à partir des sites miroirs et suivre les instructions ci-dessous pour mettre à jour votre système avec les sources FreeBSDstable; les plus récentes.

   Si vous faites tourner une version précédente de FreeBSD et que vous désirez mettre à jour via les sources vous pouvez aisément le faire à partir d'un site miroir FreeBSD. Cela peut être fait de deux manières: .. Utilisez le programme cvsup avec le fichier supfile nommé stable-supfile disponible dans le répertoire /usr/shared/examples/cvsup. C'est la méthode recommandée, puisqu'elle permet de récupérer la totalité des sources la première fois et par la suite

uniquement ce qui a été modifié. De nombreuses personnes exécutent `cvsup` depuis `cron` et maintiennent ainsi automatiquement à jour leurs sources. Vous devez personnaliser l'exemple de supfile précédent, et configurer cvsup pour votre environnement. .. Utilisez CTM. Si vous ne disposez pas d'une connexion Internet rapide et peu coûteuse, c'est la méthode que vous devriez penser à utiliser.

3. Avant tout, si vous avez besoin d'un accès rapide à la demande aux sources et que la bande passante n'est pas un problème, utilisez `cvsup` ou `ftp`. Sinon, utilisez CTM.
4. Avant de compiler FreeBSD-STABLE, lisez attentivement le Makefile dans /usr/src. Vous devriez au moins la première fois installer un nouveau noyau et recompiler le système, comme étape nécessaire à votre processus de mise à jour. La lecture de la liste de diffusion à propos de la branche FreeBSD-STABLE; et du fichier /usr/src/UPDATING vous tiendra au courant des autres procédures de transition qui sont parfois nécessaires lorsque nous préparons la prochaine version.

26.6. Synchroniser vos sources

Il existe différentes façons d'utiliser une connexion Internet (ou le courrier électronique) pour garder à jour les sources de n'importe quelle partie, ou de l'ensemble, du projet FreeBSD, selon ce qui vous intéresse. Les principaux services que nous fournissons sont le CVS anonyme, CVSup, et CTM.

Alors qu'il est possible de mettre à jour seulement certaines parties de l'arbre des sources, la seule procédure de mise à jour supportée est celle consistant à mettre à jour l'intégralité de l'arborescence et de recompiler les sources des applicatifs de base-"userland" (i.e., tous les programmes qui tournent dans l'espace utilisateur, comme ceux des répertoires /bin et /sbin) et du noyau. Ne mettre à jour qu'une partie des sources, uniquement le noyau, ou seul le "userland" mènera souvent à des problèmes. Ces problèmes pourront aller d'erreurs de compilation à des paniques du noyau ou même des corruptions de données.

CVS anonyme et CVSup utilisent une méthode de mise à jour pilotée par le client-*pull*. Dans le cas de CVSup, l'utilisateur (ou une procédure `cron`) appelle le programme `cvsup`, qui interagit avec un serveur `cvsupd` distant, pour mettre à jour vos fichiers. Les mises à jour que vous recevez sont les plus récentes, et vous ne les recevez seulement lorsque vous le désirez. Vous pouvez aisément restreindre vos mises à jour aux fichiers ou répertoires particuliers qui vous intéressent. Les mises à jour sont générées à la volée par le serveur, en fonction de ce que vous avez déjà et de ce que vous voulez. CVS anonyme est plus simpliste que CVSup, car ce n'est qu'une extension de CVS qui permet de récupérer des modifications directement d'une archive CVS distante. Pour cela, CVSup est bien plus efficace mais CVS anonyme est plus facile à utiliser.

CTM, à l'inverse, ne compare pas interactivement les sources dont vous disposez avec celles qui sont sur l'archive de référence. Au lieu de cela, une procédure qui identifie les modifications intervenues depuis qu'elle a été exécutée pour la dernière fois, est lancée plusieurs fois par jour sur la machine CTM de référence (maître), les modifications détectées sont compressées, affectées d'un numéro de séquence et encodées pour pouvoir être envoyées par courrier électronique (en ASCII imprimable uniquement). Une fois reçus, ces "deltas CTM" peuvent être passés à l'utilitaire

ctm_rmail(1) qui décodera, contrôlera et appliquera automatiquement les modifications à l'exemplaire des sources de l'utilisateur. Cette méthode est beaucoup plus efficace que CVSup et consomme beaucoup moins de ressources sur notre serveur, parce que c'est un modèle piloté par le serveur-*push* plutôt que par l'utilisateur-*pull*.

Il y a, bien sûr, quelques contreparties. Si vous effacez par inadvertance des parties de votre archive, CVSup s'en apercevra et vous reconstruira les parties endommagées. CTM ne le fera pas, et si vous effacez des parties de votre l'arborescence des sources (et que vous n'avez pas fait de sauvegarde) alors vous devrez repartir de zéro (à partir du plus récent "delta de base" CVS) et tout reconstituer avec CTM ou CVS anonyme, effacer les parties endommagées et resynchroniser.

26.7. Recompiler le système

Une fois que vous avez synchronisé votre arborescence des sources avec une version donnée de FreeBSD (FreeBSD-STABLE, FreeBSD-CURRENT, et ainsi de suite) vous pouvez alors utiliser cette arborescence des sources pour recompiler le système.

Faites une sauvegarde

On n'insistera jamais assez sur l'importance de faire une sauvegarde de votre système *avant* tout autre chose. Bien qu'il soit facile de "refaire le monde" (recompiler FreeBSD), si vous suivez ces instructions, vous ferez inévitablement des erreurs à un moment ou un autre, ou d'autres feront des erreurs au niveau de l'arborescence des sources qui empêcheraient votre système de redémarrer.

Assurez-vous que vous avez bien fait une sauvegarde. Ayez une disquette de maintenance, ou un CD démarrable à portée de la main. Vous ne l'utiliserez probablement pas, mais prudence est mère de sûreté!

S'abonner à la bonne liste de diffusion

Les branches FreeBSD-STABLE et FreeBSD-CURRENT sont, par nature, *en développement*. Les personnes qui participent à FreeBSD sont des humains, et des erreurs se produisent occasionnellement.

Ces erreurs sont parfois bénignes, provocant simplement l'affichage d'un nouveau message d'avertissement par votre système. Elles peuvent aussi être catastrophiques, et empêcher votre système de redémarrer ou détruire vos systèmes de fichiers (ou pire).

Quand de tels problèmes se produisent, un avertissement "heads up" est posté sur la liste de diffusion appropriée, décrivant la nature du problème et quels systèmes sont concernés. Un message "all clear" est posté quand le problème est résolu.

Si vous tentez de suivre FreeBSD-STABLE ou FreeBSD-CURRENT et que vous ne lisez pas la liste de diffusion à propos de la branche FreeBSD-STABLE; ou la liste de diffusion à propos de la branche FreeBSD-CURRENT, vous allez au devant d'ennuis.

N'utilisez pas la commande `make world`

> De nombreuses anciennes documentations préconisent d'utiliser la commande `make world`. Cette commande n'effectue pas un certain nombre d'étapes importantes et ne devrait être utilisée que si vous êtes sûr de ce que vous faites. Dans presque tout les cas `make world` n'est pas une bonne chose à faire, et la procédure décrite dans la suite de ce document devrait être utilisée à la place.

26.7.1. La méthode générique de mise à jour du système

Pour mettre à jour votre système, vous devriez consulter /usr/src/UPDATING pour toute opération préliminaire nécessaire en fonction de la version de vos sources et ensuite utiliser la procédure suivante:

```
# cd /usr/src
# make buildworld
# make buildkernel
# make installkernel
# shutdown -r now
```

Dans quelques rares cas, il est nécessaire de lancer un `mergemaster -p` avant l'étape `buildworld`. Ces cas sont décrits dans le fichier UPDATING. Généralement, vous pouvez omettre cette opération si vous ne mettez pas à jour d'une version majeure de FreeBSD à une autre.

Une fois l'opération `installkernel` terminée avec succès, vous devrez démarrer en mode mono-utilisateur (en utilisant par exemple la commande `boot -s` à l'invite du chargeur). Exécutez ensuite:

```
# mount -a -t ufs
# mergemaster -p
# cd /usr/src
# make installworld
# mergemaster
# reboot
```

Lisez les explications supplémentaires

La séquence décrite ci-dessus n'est qu'un court résumé pour vous aider à démarrer. Vous devriez cependant lire les sections suivantes afin de comprendre clairement chaque étape, tout particulièrement si vous désirez utiliser une configuration du noyau personnalisée.

26.7.2. Lire /usr/src/UPDATING

Avant tout autre chose, lisez /usr/src/UPDATING (ou le fichier équivalent en fonction de l'endroit où se trouve vos sources). Ce fichier devrait contenir les informations importantes au sujet des problèmes que vous pourriez rencontrer, ou indique l'ordre dans lequel vous devriez exécuter certaines commandes. Si le fichier UPDATING contredit quelque chose d'écrit ici, UPDATING prime

sur tout le reste.

La lecture du fichier UPDATING n'est pas un substitut à l'abonnement à la liste de diffusion correcte, comme décrit précédemment. Ces deux prérequis sont complémentaires, et non pas exclusifs.

26.7.3. Contrôler /etc/make.conf

Contrôlez les fichiers /usr/shared/examples/etc/make.conf et /etc/make.conf. Le premier contient des paramètres par défaut - la plupart étant placés en commentaires. Pour les utiliser quand vous recompilez votre système à partir des sources, rajoutés-les au fichier /etc/make.conf. Gardez à l'esprit que tout ce que vous ajoutez au fichier /etc/make.conf est utilisé chaque fois que vous invoquez la commande `make`, il est donc bon de s'assurer que les valeurs par défaut sont appropriées à votre système.

Un utilisateur typique voudra probablement copier les lignes `CFLAGS` et `NO_PROFILE` se trouvant dans /usr/shared/examples/etc/make.conf vers /etc/make.conf et les décommenter.

Examinez les autres définitions (`COPTFLAGS`, `NOPORTDOCS` et ainsi de suite) et décidez si elles vous conviennent.

26.7.4. Mettre à jour les fichiers dans /etc

Le répertoire /etc contient la plupart des informations de configuration de votre système, ainsi que les procédures de démarrage. Certaines de ces procédures changent d'une version à l'autre de FreeBSD.

Certains fichiers de configuration sont également utilisés en permanence par le système. En particulier /etc/group.

Il est arrivé que la phase d'installation `make installworld` ait besoin que certains utilisateurs et groupes existent. Il y a de fortes chances qu'ils n'aient pas été définis avant la mise à jour. C'est une source de problèmes. Dans certains cas `make buildworld` contrôlera si ces utilisateurs ou groupes existent.

Un exemple de cela fut l'addition de l'utilisateur `smmsp`. Le processus d'installation échouait quand `mtree` tentait de créer /var/spool/clientmqueue.

La solution est d'exécuter mergemaster(8) dans le mode pré-"buildworld" en ajoutant l'option `-p`. Cela effectuera la comparaison uniquement des fichiers essentiels pour le succès de la procédure `buildworld` ou `installworld`. Si votre vieille version de `mergemaster` ne supporte pas l'option `-p`, utilisez la nouvelle version présente dans l'arborescence des sources quand vous l'exécutez pour la première fois:

```
# cd /usr/src/usr.sbin/mergemaster
# ./mergemaster.sh -p
```

Si vous êtes particulièrement paranoïaque, vous pouvez contrôler votre système

afin de voir quels fichiers appartiennent au groupe que vous renommez ou effacez:

```
# find / -group GID -print
```

affichera les fichiers appartenant au groupe *GID* (qui peut être soit un nom de groupe ou un identifiant numérique de groupe).

26.7.5. Passer en mode mono-utilisateur

Il vaut mieux recompiler le système en mode mono-utilisateur. En dehors du fait que cela sera légèrement plus rapide, la réinstallation va modifier un grand nombre de fichiers systèmes importants, tous les binaires de base du système, les bibliothèques, les fichiers d'include et ainsi de suite. Les modifier sur un système en fonctionnement (en particulier s'il y a des utilisateurs connectés à ce moment là), c'est aller au devant de problèmes.

Une autre méthode consiste à compiler le système en mode multi-utilisateurs, et passer dans le mode mono-utilisateur pour l'installation. Si vous désirez utiliser cette méthode, conservez les étapes suivantes pour le moment où la compilation sera terminée. Vous pouvez reporter le passage en mode mono-utilisateur jusqu'à l'exécution de `installkernel` ou `installworld`.

En tant que super-utilisateur, vous pouvez exécuter la commande:

```
# shutdown now
```

sur un système en fonctionnement, pour passer en mode mono-utilisateur.

Ou bien, redémarrer le système, et à l'invite de démarrage, sélectionnez l'option "single user". Le système démarrera alors en mode mono-utilisateur. A l'invite de l'interpréteur de commandes, exécutez alors:

```
# fsck -p
# mount -u /
# mount -a -t ufs
# swapon -a
```

Cela effectue une vérification des systèmes de fichiers, remonte / en mode lecture/écriture, et monte tous les autres systèmes de fichiers UFS listés dans le fichier /etc/fstab, puis active la pagination.

Si votre horloge CMOS est réglée sur l'heure locale et non pas sur le fuseau GMT (cela est vrai si la sortie de la commande `date` ne donne pas l'heure et le fuseau correct), vous aurez également peut-être besoin d'exécuter la commande suivante:

```
# adjkerntz -i
```

> Cela permettra de s'assurer que vos paramètres de fuseaux horaires sont correctement configurés - sans cela, vous risquez de faire face, plus tard, à des problèmes.

26.7.6. Effacer /usr/obj

Au fur et à mesure que les différentes parties du système sont recompilées, elles sont placées dans des répertoires qui (par défaut) sont sous /usr/obj. Les répertoires sont agencés comme sous /usr/src.

Vous pouvez accélérer le processus `make buildworld`, et également vous éviter d'éventuels problèmes de dépendances en effaçant ce répertoire.

Certains fichiers dans /usr/obj peuvent avoir l'indicateur immuable positionné (consultez la page de manuel chflags(1) pour plus d'informations) qui doit être retiré en premier.

```
# cd /usr/obj
# chflags -R noschg *
# rm -rf *
```

26.7.7. Recompiler le système de base

26.7.7.1. Enregistrer la sortie

C'est une bonne idée d'enregistrer la sortie de make(1) dans un fichier. Si quelque chose se passe mal, vous aurez une trace des messages d'erreur. Même si cela ne vous aide pas à diagnostiquer ce qui n'a pas fonctionné, cela peut aider les autres si vous postez votre problème sur une des listes de diffusion de FreeBSD.

La méthode la plus aisée pour faire cela est d'utiliser la commande script(1), avec en paramètre le nom du fichier où enregistrer les résultats. Vous devez faire cela immédiatement juste avant de recompiler le système, et taper `exit` une fois que c'est terminé.

```
# script /var/tmp/mw.out
Script started, output file is /var/tmp/mw.out
# make TARGET
… compile, compile, compile …
# exit
Script done, …
```

Si vous le faites, *n'enregistrez pas* le résultat dans /tmp. Ce répertoire peut être vidé au prochain redémarrage du système. Un meilleur endroit de sauvegarde est /var/tmp (comme dans l'exemple précédent) ou dans le répertoire utilisateur de `root`.

26.7.7.2. Compiler le nouveau système

Vous devez être dans le répertoire /usr/src:

```
# cd /usr/src
```

(à moins, bien sûr, que votre code source ne soit ailleurs, auquel cas vous devrez aller dans le répertoire correspondant).

Pour recompiler le système, on utilise la commande make(1). Cette commande lit ses instructions dans le fichier Makefile, qui décrit comment devraient être reconstruits les programmes qui constituent FreeBSD, dans quel ordre, et ainsi de suite.

Le format général de la ligne de commande que vous taperez sera la suivante:

```
# make -x -DVARIABLE cible
```

Dans cet exemple, `-x` est une option que vous passez à make(1). Reportez-vous à la page de manuel pour un exemple d'options que vous pouvez passer.

`-D_VARIABLE_` transmet un variable au fichier Makefile. Le comportement du Makefile est défini par ces variables. Ce sont les mêmes variables que l'on trouve dans /etc/make.conf, et c'est un autre moyen de les positionner.

```
# make -DNO_PROFILE cible
```

est une autre manière de dire qu'il ne faut pas compiler les bibliothèques profilées et correspond à la ligne:

```
NO_PROFILE=    true #    Avoid compiling profiled libraries
```

dans /etc/make.conf.

cible indique à make(1) ce que vous voulez faire. Chaque Makefile définit un certain nombre de "cibles", et votre choix de cible détermine ce qui se passe.

Certaines cibles listées dans le fichier Makefile, ne doivent pas être employées. Ce sont des étapes intermédiaires utilisées par le processus de recompilation pour décomposer les étapes importantes de la recompilation du système en sous-étapes.

La plupart du temps, vous n'aurez pas besoin de passer de paramètres à make(1), et votre commande ressemblera à ceci:

```
# make cible
```

Où *cible* sera une des nombreuses options de compilation. La première cible devrait toujours être `buildworld`.

Comme leurs noms l'indiquent, `buildworld` reconstruit la nouvelle arborescence dans /usr/obj, et

`installworld`, une autre cible, l'installe sur la machine.

Disposer d'options séparées est très utile pour deux raisons. Tout d'abord cela vous permet de recompiler en toute sûreté en sachant qu'aucun composant du système actuel ne sera affecté. La compilation est "autonome". En raison de cela vous pouvez exécuter `buildworld` sur une machine en mode multi-utilisateurs sans redouter d'effets fâcheux. Il est néanmoins recommandé de toujours exécuter l'étape `installworld` en mode mono-utilisateur.

En second lieu, cela vous permet d'utiliser des systèmes montés par NFS pour mettre à jour plusieurs machines de votre réseau. Si vous avez trois machines `A`, `B` et `C` que vous voulez mettre à jour, exécutez `make buildworld` et `make installworld` sur `A`. `B` et `C` doivent ensuite monter par NFS /usr/src et /usr/obj depuis `A`, et vous pouvez alors exécuter `make installworld` pour installer le système recompilé sur `B` et `C`.

Bien que la cible `world` existe toujours, vous êtes fortement encouragé à ne pas l'utiliser.

Exécutez:

```
# make buildworld
```

Il est possible de passer l'option `-j` à make(1) ce qui lui permettra d'exécuter plusieurs processus simultanément. C'est particulièrement utile sur une machine avec plusieurs processeurs. Cependant, comme la compilation est plus gourmande en E/S plutôt qu'en CPU, c'est également utile sur des machines mono-processeur.

Typiquement sur une machine mono-processeur, vous exécuteriez:

```
# make -j4 buildworld
```

make(1) pourra exécuter jusqu'à 4 processus simultanément. Des constatations empiriques postées sur les listes de diffusion montrent que c'est en général ce qui apporte le plus de gain en performances.

Si vous avez une machine multi-processeurs et que vous avez configuré un noyau SMP, essayez des valeurs entre 6 et 19 et voyez quel bénéfice vous en tirez.

26.7.7.3. Durée

De nombreux facteurs influencent la durée de compilation, mais les machines récentes devraient mettrent seulement de une à deux heures pour compiler l'arborescence FreeBSD-STABLE, sans modification ni raccourcis durant le processus. Une arborescence FreeBSD-CURRENT nécessitera un peu plus de temps.

26.7.8. Compiler et installer un nouveau noyau

Pour tirer pleinement parti de votre nouveau système, vous devrez recompiler le noyau. C'est pratiquement indispensable, parce que certaines structures mémoires peuvent avoir changées, et des programmes comme ps(1) et top(1) ne fonctionneront pas tant que le système et le noyau

n'utilisent pas les mêmes versions de code source.

La manière la plus simple et la plus sûre est de compiler et installer un noyau basé sur le noyau GENERIC. Alors que le noyau GENERIC peut ne pas comporter les pilotes de périphériques nécessaires pour votre système, il devrait contenir tout ce qui est nécessaire pour faire démarrer votre système en mode mono-utilisateur. C'est une bonne façon de tester le fonctionnement de votre nouveau système. Après avoir démarré à partir du noyau GENERIC et vérifié que votre système fonctionne vous pouvez alors compiler un nouveau noyau basé sur votre fichier de configuration normal du noyau.

Sur FreeBSD, il est important de recompiler le système avant de compiler un nouveau noyau.

Si vous désirez compiler un noyau personnalisé, et que vous avez déjà un fichier de configuration, utilisez juste `KERNCONF=MONNOYAU` comme suit:

```
# cd /usr/src
# make buildkernel KERNCONF=MONNOYAU
# make installkernel KERNCONF=MONNOYAU
```

Notez que si vous avez augmenté la variable `kern.securelevel` à une valeur supérieure à 1 *et* que vous avez positionné l'indicateur `noschg` ou similaire sur votre noyau, il sera intéressant de passer en mode mono-utilisateur pour utiliser `installkernel`. Sinon vous devriez être en mesure d'exécuter ces commandes à partir du mode multi-utilisateur sans problèmes. Voir la page de manuel de init(8) pour plus de détails à propos de `kern.securelevel` et la page chflags(1) pour des informations sur les différents indicateurs de fichiers.

26.7.9. Redémarrer en mode mono-utilisateur

Vous devriez redémarrer en mode mono-utilisateur pour tester le fonctionnement du nouveau noyau. Pour cela suivez les instructions de Passer en mode mono-utilisateur.

26.7.10. Installer les nouveaux binaires système

Si vous avez compilé une version de FreeBSD assez récente pour avoir utilisé `make buildworld` alors vous devriez utiliser maintenant `installworld` pour installer les nouveaux binaires système.

Lancez:

```
# cd /usr/src
# make installworld
```

Si vous spécifiez des variables sur la ligne de commande de `make buildworld`, vous devez utiliser les mêmes variables avec la commande `make installworld`. Cela ne reste pas forcément vrai pour d'autres options; par exemple, `-j` ne doit jamais être utilisée avec `installworld`.

Par exemple, si vous exécutez:

```
# make -DNO_PROFILE buildworld
```

vous devrez ensuite installer les résultats avec:

```
# make -DNO_PROFILE installworld
```

sinon il essayera d'installer les bibliothèques profilées qui n'ont pas été recompilées à l'étape `make buildworld`.

26.7.11. Mettre à jour les fichiers non modifiés par `make installworld`

La recompilation du système ne mettra pas à jour certains répertoires (en particulier, /etc, /var et /usr) avec les fichiers nouveaux ou modifiés.

La manière la plus simple de mettre à jour ces fichiers est d'utiliser mergemaster(8), bien qu'il soit possible de le faire manuellement si vous le désirez. Indépendamment de la manière que vous choisissez, assurez-vous de faire une sauvegarde du répertoire /etc au cas où quelque chose se passerait mal.

26.7.11.1. `mergemaster`

L'utilitaire mergemaster(8) est une procédure Bourne qui vous aidera à déterminer les différences entre vos fichiers de configuration dans le répertoire /etc, et les fichiers de configuration dans l'arborescence des sources /usr/src/etc. C'est la solution recommandée pour maintenir à jour les fichiers de configuration du système avec ceux situés dans l'arborescence des sources.

Pour commencer, tapez simplement `mergemaster` à l'invite, et observez-le travailler. `mergemaster` commencera à constituer une arborescence temporaire, à partir de /, et la remplira avec divers fichiers de configuration. Ces fichiers sont alors comparés avec ceux actuellement installés sur votre système. A ce point, les fichiers qui diffèrent seront affichés dans le format diff(1), avec le signe `+` représentant les lignes modifiées ou ajoutées, et le `-` représentant les lignes qui seront soit complètement supprimées, soit remplacées avec une nouvelle ligne. Voir la page de manuel diff(1) pour plus d'informations au sujet de la syntaxe diff(1) et comment sont affichées les différences.

mergemaster(8) vous affichera ensuite chaque fichier présentant des différences, et vous aurez à ce moment-là le choix de soit supprimer le nouveau fichier (le fichier temporaire), soit d'installer le fichier temporaire non modifié, soit de fusionner le fichier temporaire et le fichier actuellement installé, soit enfin de revoir les résultats de l'opération diff(1).

Choisir de supprimer le fichier temporaire indiquera à mergemaster(8) que nous désirons conserver notre fichier actuel intacte, et effacera la nouvelle version. Cette option n'est pas recommandée, à moins que vous ne voyez aucune raison de modifier le fichier actuel. Vous pouvez obtenir de l'aide à n'importe quel moment en tapant `?` à l'invite de mergemaster(8). Si l'utilisateur choisit de passer un fichier, il sera présenté à nouveau une fois que tous les autres fichiers auront été traités.

Choisir d'installer un fichier temporaire intact remplacera le fichier actuel avec le nouveau. Pour la

plupart des fichiers non modifiées, c'est la meilleure option.

Choisir de fusionner le fichier, vous affichera un éditeur de texte, et le contenu des deux fichiers. Vous pouvez maintenant les fusionner en les visionnant côte à côte sur l'écran, et en sélectionnant des parties des deux fichiers pour créer un fichier final. Quand les fichiers sont comparés côte à côte, la touche `l` sélectionnera le contenu de gauche et la touche `r` sélectionnera celui de droite. Le résultat final sera un fichier constitué des deux parties, qui peut alors être installé. Cette option est habituellement utilisée pour les fichiers où les des paramètres ont été modifiés par l'utilisateur.

Choisir de revoir les résultats de l'opération diff(1) vous affichera les différences entre fichiers tout comme la fait mergemaster(8) avant de vous demander un choix.

Après que mergemaster(8) en ait terminé avec les fichiers système, il vous proposera de nouvelles opérations. mergemaster(8) vous demandera si vous désirez reconstruire le fichier des mots de passe et terminera en vous proposant de supprimer les fichiers temporaires restants.

26.7.11.2. Mise à jour manuelle

Si vous désirez faire la mise à jour manuellement, vous ne pouvez cependant pas vous contenter de copier les fichiers de /usr/src/etc dans /etc pour que cela fonctionne. Certains de ces fichiers doivent d'abord être "installés". En effet le répertoire /usr/src/etc "n'est pas" une copie de ce que devrait contenir votre répertoire /etc. De plus, il a des fichiers qui doivent être dans /etc et qui ne sont pas dans /usr/src/etc.

Si vous utilisez mergemaster(8) (comme recommandé), vous pouvez passer cette section et aller directement à la section suivante.

La façon la plus simple de procéder est d'installer les fichiers dans un nouveau répertoire, puis de passer en revue les différences.

Sauvegardez votre répertoire /etc actuel

Bien qu'en principe rien ne sera modifié automatiquement dans ce répertoire, prudence est mère de sûreté. Copiez donc votre répertoire /etc dans un endroit sûr. Quelque chose du genre:

```
# cp -Rp /etc /etc.old
```

conviendra; l'option `-R` fait une copie récursive, `-p` préserve la date, les autorisations des fichiers et ainsi de suite.

Vous devez créer un ensemble de répertoires provisoires pour y installer les fichiers du répertoire /etc et autres. /var/tmp/root est un bon choix, il y a un certain nombre de sous-répertoires à créer également:

```
# mkdir /var/tmp/root
# cd /usr/src/etc
# make DESTDIR=/var/tmp/root distrib-dirs distribution
```

Cela va créer l'arborescence nécessaire et y installera les fichiers. Un grand nombre des sous-répertoires créés dans /var/tmp/root sont vides et devront être supprimés. La façon la plus simple de le faire est:

```
# cd /var/tmp/root
# find -d . -type d | xargs rmdir 2>/dev/null
```

Ceci supprimera tous les répertoires vides (la sortie d'erreur standard est redirigée vers /dev/null pour empêcher les avertissements à propos des répertoires non vides).

/var/tmp/root contient maintenant tous les fichiers à installer à l'endroit requis sous /. Vous devez maintenant examiner chacun de ces fichiers pour déterminer en quoi ils diffèrent de vos propres fichiers.

Notez que certains des fichiers qui seront installés dans /var/tmp/root commencent par un ".". Au moment où sont écrites ces lignes, les seuls fichiers concernés sont les fichiers d'initialisation des interpréteurs de commandes dans /var/tmp/root/ et /var/tmp/root/root/, mais il pourrait y en avoir d'autres (cela dépend de quand vous lirez ces lignes). Assurez-vous d'utiliser la commande `ls -a` pour ne pas les oublier.

La manière la plus simple de procéder est d'utiliser la commande diff(1) pour comparer les deux fichiers:

```
# diff /etc/shells /var/tmp/root/etc/shells
```

Cela vous indiquera les différences entre votre fichier /etc/shells et le nouveau fichier /var/tmp/root//etc/shells. A partir de là, décidez si vous aller reporter les modifications que vous y avez apportée ou si vous allez simplement recopier le nouveau fichier.

Donnez au nouveau répertoire racine (/var/tmp/root) un nom qui inclue une date, pour pouvoir facilement comparer les différentes versions

Si vous recompilez fréquemment votre système, cela signifie que vous devez également souvent mettre à jour le répertoire /etc, ce qui peut rapidement devenir une corvée.

Vous pouvez accélérer le processus en conservant une copie du dernier ensemble de fichiers modifiés que vous avez reportés dans /etc. La procédure suivante présente une façon de faire.

1. Recompilez le système comme à l'accoutumé. Au moment de mettre à jour /etc et les autre répertoires, donnez au répertoire cible un nom basé sur la date du jour. Si vous faisiez cela le 14 février 1998, vous pourriez procéder comme suit:

   ```
   # mkdir /var/tmp/root-19980214
   # cd /usr/src/etc
   ```

```
# make DESTDIR=/var/tmp/root-19980214 \
    distrib-dirs distribution
```

2. Reporter les modifications depuis ce répertoire comme décrit plus haut.

   Ne supprimez pas le répertoire /var/tmp/root-19980214 quand vous aurez terminé.

3. Quand vous récupérez la dernière version des sources et la recompilerez, suivez l'étape 1. Vous aurez alors un nouveau répertoire, qui pourrait s'appeler /var/tmp/root-19980221 (si vous faites une mise à jour chaque semaine).

4. Vous pouvez maintenant voir les modifications intervenues d'une semaine à l'autre en utilisant diff(1) pour afficher les différences entre tous les fichiers deux répertoires:

   ```
   # cd /var/tmp
   # diff -r root-19980214 root-19980221
   ```

   Généralement, il y aura beaucoup moins de différences qu'entre /var/tmp/root-19980221/etc et /etc. Comme il y a beaucoup moins de différences, il est beaucoup plus facile de les reporter dans le répertoire /etc.

5. Vous pouvez maintenant supprimer le plus ancien des deux répertoires /var/tmp/root-*:

   ```
   # rm -rf /var/tmp/root-19980214
   ```

6. Répétez l'opération chaque fois que vous devez reporter des modifications dans /etc.

Vous pouvez utiliser date(1) pour automatiser la génération des noms de répertoires:

```
# mkdir /var/tmp/root-`date "+%Y%m%d"`
```

26.7.12. Redémarrer

Vous en avez terminé. Après avoir vérifié que tout semble être en place, vous pouvez alors redémarrez votre système. Un simple shutdown(8) devrait suffire:

```
# shutdown -r now
```

26.7.13. C'est fini

Vous devriez maintenant avoir mis à jour avec succès votre système FreeBSD. Félicitations.

Si les choses se sont légèrement mal passées, il est facile de recompiler un élément particulier du système. Par exemple, si vous avez accidentellement effacé /etc/magic lors de la mise à jour de /etc, la commande file(1) ne fonctionnerait plus. Dans ce cas, la solution serait d'exécuter:

```
# cd /usr/src/usr.bin/file
# make all install
```

26.7.14. Questions

26.7.15. Dois-je refaire le monde à chaque évolution?

Il n'y a pas de réponse toute faite à cette question, tout dépend de la nature des évolutions. Par exemple, si vous venez juste d'exécuter CVSup, et que les fichiers suivants on été mis à jour:

```
src/games/cribbage/instr.c
src/games/sail/pl_main.c
src/release/sysinstall/config.c
src/release/sysinstall/media.c
src/shared/mk/bsd.port.mk
```

cela ne vaut probablement pas la peine de recompiler tout le système. Vous pouvez tout simplement aller dans les sous-répertoires appropriés, exécuter `make all install`, et c'est à peu près tout. Mais s'il y a des évolutions importantes, par exemple sur src/lib/libc/stdlib alors vous devrez soit refaire le monde, ou recompiler au moins toutes les parties du système qui sont liées statiquement (de même que tout ce vous pourriez avoir ajouté qui y serait lié statiquement).

C'est à vous de voir. Vous préférerez peut-être recompiler votre système tous les quinze jours, et laisser les modifications s'empiler pendant quinze jours. Ou bien vous préférerez ne recompiler que ce qui a changé et vous faire confiance pour tout ce qui en dépend.

Et, bien sûr, cela dépend de la fréquence avec laquelle vous voulez faire vos mises à jour, et de si vous suivez la branche FreeBSD-STABLE ou FreeBSD-CURRENT.

26.7.16. Ma compilation échoue avec de nombreuses erreurs "signal 11" signal 11 (ou tout autre numéro de signal). Que s'est-il passé?

Cela indique généralement un problème matériel. (Re)compiler le système est un bon moyen de mettre votre matériel sous pression, et mettra souvent en évidence des défaillances de la mémoire vive. Elles se manifestent normalement d'elles-mêmes, la compilation échouant lors de la réception de mystérieux signaux.

Un bon indicateur de cet état de fait, est que vous pouvez relancer la compilation et qu'elle échouera en un endroit différent.

Dans ce cas, vous ne pouvez guère faire autre chose que d'intervertir les différents composants de votre matériel pour déterminer lequel est en cause.

26.7.17. Puis-je effacer /usr/obj après avoir fini?

Une réponse courte est oui.

/usr/obj contient tous les fichiers objets générés à la compilation. Normalement, une des premières étapes de `make buildworld` est de supprimer ce répertoire et de repartir à zéro. Dans ce cas, conserver le répertoire /usr/obj après avoir terminé ne sert pas à grand chose, alors que vous économiseriez pas mal d'espace disque (actuellement environ 340 MO).

Cependant, si vous savez ce que vous faites, vous pouvez faire en sorte que `make buildworld` saute cette étape. Cela rendra les compilations ultérieures plus rapides, puisque la plupart des sources n'auront pas besoin d'être recompilées. Le revers de la médaille est que des problèmes subtils de dépendance peuvent se manifester, provoquant l'échec de votre compilation de manière étrange. Cela génère fréquemment du bruit sur les listes de diffusion de FreeBSD, quand quelqu'un se plaint que sa mise à jour a échoué, sans réaliser que c'est parce qu'il a tenté de brûler les étapes.

26.7.18. Une recompilation interrompue peut-elle être reprise?

Tout dépend de jusqu'où vous êtes aller avant de rencontrer un problème.

En général (et ceci n'est pas une règle absolue) `make buildworld` crée de nouveaux exemplaires des outils indispensables (comme gcc(1) et make(1)) et des bibliothèques système. Ces outils et bibliothèques sont ensuite installés. Puis ils sont utilisés pour se reconstruire eux-mêmes, et installés de nouveau. L'intégralité du système (y compris maintenant les programmes utilisateurs classiques, comme ls(1) ou grep(1)) est alors recompilé avec les nouveaux fichiers système.

Si vous êtes à cette dernière étape, et que vous le savez (parce que vous avez consulté les résultats que vous avez enregistrés) alors vous pouvez (sans trop de risque) faire:

```
… fix the problem …
# cd /usr/src
# make -DNO_CLEAN all
```

Cela ne détruira pas les résultats du travail qu'à déjà effectué `make buildworld`.

Si vous voyez le message:

```
--------------------------------------------------------------
Building everything..
--------------------------------------------------------------
```

dans les comptes-rendus de `make buildworld` alors cette façon de procéder est probablement bonne.

Si vous ne voyez pas ce message, ou que vous doutez de vous, alors prudence est mère de sûreté, et il vaut mieux tout reprendre depuis le début.

26.7.19. Comment puis-je accélérer la compilation du système?

- Passez en mode mono-utilisateur.
- Mettez les répertoires /usr/src et /usr/obj sur des systèmes de fichiers et des disques différents. Si possible, installez ces disques sur des contrôleurs différents.
- Encore mieux, mettez ces systèmes de fichiers sur plusieurs disques utilisant le système ccd(4) (pilote de disques concaténés).
- Ne compilez pas les bibliothèques profilées (mettez "NO_PROFILE=true" dans le fichier /etc/make.conf). Vous n'en avez certainement pas besoin.
- Egalement dans /etc/make.conf, positionnez `CFLAGS` à quelque chose comme `-O -pipe`. L'optimisation `-O2` est bien plus lente, et la différence d'optimisation entre `-O` et `-O2` est en général négligeable. `-pipe` demande au compilateur d'utiliser des tuyaux à la place de fichiers temporaires, ce qui économise des accès disque (mais utilise plus de mémoire).
- Passez l'option `-jn` à make(1) pour permettre l'exécution de plusieurs processus en parallèle. Cela améliore généralement les choses, que vous ayez une machine mono- ou multi-processeurs.
- Le système de fichiers qui contient /usr/src peut être monté (ou remonté) avec l'option `noatime`. Cela empêche l'enregistrement des dates d'accès aux fichiers par le système de fichiers. Vous n'avez de toute façon probablement pas besoin de cette information.

```
# mount -u -o noatime /usr/src
```

Cet exemple suppose que /usr/src constitue à lui seul un système de fichiers. Si ce n'est pas le cas (s'il fait partie de /usr par exemple) vous devez alors indiquer le point de montage de ce système de fichiers, et non /usr/src.

- Le système de fichiers où se trouve /usr/obj peut être monté (ou remonté) avec l'option `async`. Les écritures sur le disque se feront alors de façon asynchrone. En d'autres termes, le programme reprend immédiatement la main, et l'écriture des données sur le disque se fait quelques secondes plus tard. Cela permet le groupement des écritures sur le disque, et le gain en performance peut être spectaculaire.

Gardez à l'esprit que cette option rend votre système de fichiers plus fragile. Avec cette option, les risques ne sont accrus qu'en cas de coupure d'alimentation, le système de fichiers soit irrécupérable quand la machine redémarrera.

S'il n'y a que /usr/obj sur ce système de fichiers, ce n'est alors pas un problème. Si vous avez d'autres données importantes sur ce système de fichiers, assurez-vous que vos sauvegardes soient à jour avant d'activer cette option.

```
# mount -u -o async /usr/obj
```

Comme auparavant, si /usr/obj ne constitue pas un système de fichiers en soit, remplacez-le dans l'exemple par le nom du point de montage approprié.

26.7.20. Que faire si quelque chose se passe mal?

Soyez absolument sûr que votre environnement ne contient pas des restes de compilation précédentes. Cela est plutôt simple:

```
# chflags -R noschg /usr/obj/usr
# rm -rf /usr/obj/usr
# cd /usr/src
# make cleandir
# make cleandir
```

En effet, `make cleandir` doit vraiment être exécutée deux fois.

Ensuite relancez l'ensemble du processus, en commençant avec `make buildworld`.

Si vous avez toujours des problèmes, envoyez l'erreur et le résultat de la commande `uname -a` à la liste de diffusion pour les questions d'ordre général à propos de FreeBSD. Tenez-vous prêt à répondre à d'autres concernant votre configuration!

26.8. Suivre les mises à jour pour plusieurs machines

Si vous avez plusieurs machines dont vous voulez maintenir à jour l'arborescence des sources, alors faire télécharger et recompiler à chacune d'entre elles les sources semble un gaspillage de ressources: espace disque, bande passante réseau, et cycles CPU. C'est en effet bien le cas, et la solution est d'avoir une machine qui fait la majeure partie du travail, pendant que le reste des machines montent ce travail par NFS. Cette section décrit une façon de le faire.

26.8.1. Préliminaires

Premièrement, identifiez un ensemble de machines qui va utiliser le même ensemble de binaires, que nous appellerons un *ensemble de compilation*. Chaque machine peut avoir un noyau personnalisé, mais elles exécuteront les mêmes binaires utilisateur du système de base. Dans cet ensemble de machine, choisissez une machine qui sera la *machine de compilation*. Cela sera la machine sur laquelle le monde et le noyau seront compilés. Idéalement, cela devrait être une machine rapide avec un CPU suffisamment disponible pour exécuter la commande `make buildworld` et `make buildkernel`. Vous voudrez également utiliser une *machine de test*, qui testera les mises à jour logicielles avant d'être utilisées en production. Cela *doit* être une machine que vous pouvez vous permettre d'avoir hors service pour une longue période. Cela peut être la machine de compilation, mais cela n'est pas obligatoire.

Toutes les machines de cet ensemble de compilation doivent monter /usr/obj et /usr/src à partir de la même machine, et du même point de montage. Idéalement, ces derniers sont sur deux disques différents sur la machine de compilation, mais peuvent également être montés par NFS sur cette machine. Si vous avez plusieurs ensembles de compilation, /usr/src devrait être sur une machine de

compilation, et monté par NFS sur les autres.

Finalement assurez-vous que /etc/make.conf et /etc/src.conf sur toutes les machines de l'ensemble de compilation sont en accord avec la machine de compilation. Cela signifie que la machine de compilation doit compiler toutes les parties du système de base que toute machine de l'ensemble de compilation va installer. De plus, chaque machine de compilation devra avoir son nom de noyau défini avec `KERNCONF` dans /etc/make.conf, et la machine de compilation devrait tous les lister dans `KERNCONF`, en listant son noyau en premier. La machine de compilation doit avoir les fichiers de configuration des noyaux de chaque machine dans /usr/src/sys/arch/conf si elle va compiler leur noyau.

26.8.2. Le système de base

Maintenant que tout est configuré, vous êtes fin prêt pour tout compiler. Compilez le noyau et le monde sur la machine de compilation comme décrit dans la Compiler le nouveau système, mais n'installez rien. La compilation une fois terminée, allez sur la machine de test, et installez le noyau que vous venez juste de compiler. Si la machine monte /usr/src et /usr/obj via NFS, quand vous redémarrez en mode mono-utilisateur vous devrez activer le réseau et monter ces répertoires. La méthode la plus simple est de démarrer en mode multi-utilisateur, puis exécutez `shutdown now` pour passer en mode mono-utilisateur. Une fois à ce niveau, vous pouvez installer le nouveau noyau et monde puis exécuter `mergemaster` comme vous le feriez habituellement. Une fois cela effectué, redémarrez pour retourner en mode multi-utilisateur pour cette machine.

Après que vous soyez certain que tout fonctionne correctement sur la machine de test, utilisez la même procédure pour installer le nouvel ensemble logiciel sur chacune des autres machines de l'ensemble de compilation.

26.8.3. Les logiciels portés

La même idée peut être utilisée pour le catalogue des logiciels portés. La première étape critique est de monter /usr/ports depuis la même machine vers toutes les machines de l'ensemble de compilation. Vous pouvez alors configurer correctement /etc/make.conf pour partager les archives. Vous devrez faire pointer `DISTDIR` sur un répertoire de partage commun dans lequel peut écrire n'importe quel utilisateur utilisé pour correspondance de l'utilisateur `root` par vos montages NFS. Chaque machine devrait faire pointer `WRKDIRPREFIX` sur une répertoire de compilation local. Et enfin, si vous projetez de compiler et distribuer des logiciels précompilés, vous devriez fixer `PACKAGES` sur un répertoire similaire à `DISTDIR`.

Chapitre 27. DTrace

27.1. Synopsis

DTrace, également désigné sous le nom de système de trace dynamique, a été développé par Sun™ comme outil de localisation de problèmes de performance sur des systèmes de production et d'avant-production. Ce n'est, en aucune manière, un outil de débogage, mais un outil pour l'analyse système en temps réel pour localiser les problèmes de performance et autres.

DTrace est un outil de profilage remarquable, avec une impressionnante multitude de fonctions pour diagnostiquer des problèmes système. Il peut également être utilisé avec des scripts pré-écrits pour pouvoir profiter de ses capacités. Les utilisateurs peuvent écrire leurs propres utilitaires en employant le langage de DTrace, D, leur permettant ainsi de personnaliser leur profilage en fonction de leurs besoins.

Après la lecture de ce chapitre, vous connaîtrez:

- Ce qu'est DTrace et quelles fonctionnalités il offre.
- Les différences entre la version DTrace de Solaris™ et celle fournie par FreeBSD.
- Comment activer et utiliser DTrace sur FreeBSD.

Avant de lire ce chapitre, vous devrez:

- Comprendre les fondements d'UNIX® et de FreeBSD (Quelques bases d'UNIX).
- Etre familier avec la configuration/compilation du noyau (Configurer le noyau de FreeBSD).
- Avoir une certaine connaissance concernant la sécurité et ses liens avec FreeBSD (Sécurité).
- Comprendre comment obtenir et recompiler les sources de FreeBSD (Mise à jour de FreeBSD).

Cette fonction est considérée comme expérimentale. Quelques options peuvent être absentes et d'autres ne fonctionneront peut-être pas du tout. A terme, cette fonction sera prête pour une utilisation en production, et cette documentation sera modifiée pour en tenir compte.

27.2. Des différences de mise en oeuvre

Bien que DTrace sous FreeBSD soit très semblable à DTrace sous Solaris™, des différences existent et devraient être expliquées avant de continuer. La différence principale que les utilisateurs remarqueront est que sur FreeBSD, DTrace doit être spécialement activé. Il y a des options de noyau et des modules qui doivent être activés pour que DTrace fonctionne correctement. Ces options seront expliquées plus tard.

Il existe une option de noyau, `DDB_CTF`, qui est employée pour activer la prise en charge du chargement des données CTF depuis les modules de noyau et du noyau lui-même. CTF est le format Compact C de Solaris™, qui encapsule une forme réduite d'information de débogage, semblable à DWARF et ses vénérables tables de symboles. Ces données CTF sont ajoutées aux fichiers binaires

par les outils de compilation `ctfconvert` et `ctfmerge`. L'utilitaire `ctfconvert` analyse les sections de débogage ELFDWARF crées par le compilateur et `ctfmerge` fusionne les sections ELFCTF qui sont sous forme objet vers soit des fichiers executables, soit des bibliothèques partagées. Plus d'informations sur comment activer cela pour le noyau et FreeBSD est à venir.

Quelques fournisseurs différents existent pour FreeBSD par rapport à Solaris™. Le plus notable est le fournisseur `dtmalloc`, qui permet le traçage de la fonction `malloc()` par type dans le noyau FreeBSD.

Seul l'utilisateur `root` peut utiliser DTrace sur FreeBSD. Ceci est lié aux différences de sécurité, Solaris™ dispose de quelques contrôles de sécurité de bas niveau qui n'existent pas encore sur FreeBSD. Ainsi /dev/dtrace/dtrace est strictement limité uniquement à l'utilisateur `root`.

Pour terminer, le logiciel DTrace est sous la licence de Sun™, CDDL. La `Common Development and Distribution License` est disponibles sous FreeBSD, voir le fichier /usr/src/cddl/contrib/opensolaris/OPENSOLARIS.LICENSE ou vous pouvez le consulter sur Internet à http://www.opensolaris.org/os/licensing.

Cette licence signifie qu'un noyau avec les options DTrace est toujours sous licence BSD; cependant, la licence CDDL est appliquée lorsque les modules sont distribués sous format binaire, ou quand les fichiers binaires sont chargés.

27.3. Activer la prise en charge de DTrace

Pour activer DTrace, il faut ajouter les lignes suivantes au fichier de configuration du noyau:

```
options         KDTRACE_HOOKS
options         DDB_CTF
```

Les utilisateurs de l'architecture AMD64 devraient ajouter la ligne suivante à leur fichier de configuration de noyau:

```
options         KDTRACE_FRAME
```

Cette option active la fonction FBT. DTrace fonctionnera sans cette option, mais il y aura des restrictions sur le traçage des limites des fonctions.

Les sources doivent être recompilées et installées avec les options CTF. Pour faire cela, recompiler les sources de FreeBSD en utilisant:

```
# cd /usr/src

# make WITH_CTF=1 kernel
```

Le système aura besoin d'être redémarré.

Après avoir redémarré et avoir laissé charger en mémoire le noyau, le support de l'interpréteur de commandes Korn devra être ajouté. Ceci est necessaire car la boîte à outils DTrace possède quelques utilitaires écrits en `ksh`. Il faut installer shells/ksh93. Il est également possible de faire fonctionner ces outils avec shells/pdksh ou shells/mksh.

Finalement, récupérer la boîte à outils DTrace la plus récente. La version actuelle est disponible à l'adresse http://www.opensolaris.org/os/community/dtrace/. Un système d'installation est inclu dans l'archive; cependant, cette installation n'est pas obligatoire pour utiliser les outils fournis.

27.4. Utiliser DTrace

Avant d'utiliser DTrace, il faut que le périphérique DTrace existe. Pour charger le périphérique, exécutez la commande suivante:

```
# kldload dtraceall
```

Le système devrait maintenant supporter DTrace. Pour afficher toutes les sondes, l'administrateur peut maintenant executer la commande:

```
# dtrace -l | more
```

Toutes les données sortantes de cette commande sont passées à l'utilitaire `more`, pour empêcher qu'elles saturent l'écran. A ce niveau, DTrace peut être considéré comme fonctionnel. On est maintenant prêt à passer en revue l'ensemble des outils disponibles.

La boîte à outils est une collection de scripts prêts à fonctionner avec DTrace pour rassembler des informations systèmes. Il y a des scripts pour vérifier les fichiers ouvertes, la mémoire, l'usage du CPU et beaucoup plus. Il faut extraire les scripts avec la commande suivante:

```
# gunzip -c DTracetoolkit* | tar xvf -
```

Aller dans ce répértoire en utilisant `cd` et changer les permissions de tous les fichiers, les fichiers avec les noms en miniscules, à `755`.

Chacun de ces scripts devra avoir son contenu modifié. Ceux qui font référence à /usr/bin/ksh devront pointer sur /usr/local/bin/ksh, les autres qui utilisent /usr/bin/sh devront être modifiés pour qu'ils utilisent /bin/sh, et finalement ceux qui utilisent /usr/bin/perl, devront pointer sur /usr/local/bin/perl.

A ce point il est prudent de rappeler au lecteur que le support de DTrace sous FreeBSD *n'est pas complet* et est encore *expérimental*. Un bon nombre de ces scripts ne fonctionneront pas, soit parce qu'ils sont trop spécifiques à Solaris™, soit parce qu'ils utilisent des sondes qui ne sont pas encore supportées.

Au moment de l'écriture de ces lignes, seuls deux des scripts de la boîte à outils DTrace sont

totalement supportés sous FreeBSD: les outils hotkernel et procsystime. Ce sont ces deux outils que nous détaillerons dans la suite de cette section.

L'outil hotkernel est censé identifier quel fonction utilise le plus de temps noyau. Fonctionnant normalement, il affichera une liste comparable à la suivante:

```
# ./hotkernel
Sampling... Hit Ctrl-C to end.
```

L'administrateur système doit utiliser la combinaison de touches `Ctrl` + `C` pour arrêter le processus. Le script affichera une liste de fonctions du noyau et des informations de temps, et les triera dans l'ordre croissant du temps consommé:

```
kernel`_thread_lock_flags                             2   0.0%
0xc1097063                                            2   0.0%
kernel`sched_userret                                  2   0.0%
kernel`kern_select                                    2   0.0%
kernel`generic_copyin                                 3   0.0%
kernel`_mtx_assert                                    3   0.0%
kernel`vm_fault                                       3   0.0%
kernel`sopoll_generic                                 3   0.0%
kernel`fixup_filename                                 4   0.0%
kernel`_isitmyx                                       4   0.0%
kernel`find_instance                                  4   0.0%
kernel`_mtx_unlock_flags                              5   0.0%
kernel`syscall                                        5   0.0%
kernel`DELAY                                          5   0.0%
0xc108a253                                            6   0.0%
kernel`witness_lock                                   7   0.0%
kernel`read_aux_data_no_wait                          7   0.0%
kernel`Xint0x80_syscall                               7   0.0%
kernel`witness_checkorder                             7   0.0%
kernel`sse2_pagezero                                  8   0.0%
kernel`strncmp                                        9   0.0%
kernel`spinlock_exit                                 10   0.0%
kernel`_mtx_lock_flags                               11   0.0%
kernel`witness_unlock                                15   0.0%
kernel`sched_idletd                                 137   0.3%
0xc10981a5                                        42139  99.3%
```

Ce script fonctionnera aussi avec des modules de noyau. Pour utiliser ce fonction, exécutez le script avec l'option `-m`:

```
# ./hotkernel -m
Sampling... Hit Ctrl-C to end.
^C
MODULE                                              COUNT   PCNT
0xc107882e                                              1   0.0%
```

```
0xc10e6aa4                                                1   0.0%
0xc1076983                                                1   0.0%
0xc109708a                                                1   0.0%
0xc1075a5d                                                1   0.0%
0xc1077325                                                1   0.0%
0xc108a245                                                1   0.0%
0xc107730d                                                1   0.0%
0xc1097063                                                2   0.0%
0xc108a253                                               73   0.0%
kernel                                                  874   0.4%
0xc10981a5                                           213781  99.6%
```

Le script procsystime capture et affiche le temps consommé en appels système pour un PID ou un processus donné. Dans l'exemple suivant, un nouvel exemplaire de /bin/csh a été lancé. L'outil procsystime a été exécuté et laissé en attente pendant que quelques commandes été tapées sur les autres incarnations de `csh`. Voici le résultat de ce test:

```
# ./procsystime -n csh
Tracing... Hit Ctrl-C to end...
^C

Elapsed Times for processes csh,

         SYSCALL          TIME (ns)
          getpid               6131
       sigreturn               8121
           close              19127
           fcntl              19959
             dup              26955
         setpgid              28070
            stat              31899
       setitimer              40938
           wait4              62717
       sigaction              67372
     sigprocmask             119091
    gettimeofday             183710
           write             263242
          execve             492547
           ioctl             770073
           vfork            3258923
      sigsuspend            6985124
            read         3988049784
```

Comme indiqué, l'appel système `read()` semble prendre le plus de temps en nanosecondes, alors que l'appel système `getpid()` prend très peu de temps.

27.5. Le langage D

La boîte à outils DTrace comprend plusieurs scripts écrits dans le langage spécifique de DTrace. Ce langage est appelé le "langage D" dans la documentation de Sun™, et est très proche du C++. Une étude en profondeur de ce langage sort du cadre de ce document. Il est abordé de manière très détaillée à l'adresse http://wikis.sun.com/display/DTrace/Documentation.

Partie IV: Réseau

FreeBSD est un des systèmes d'exploitation les plus utilisé pour les serveurs réseau à hautes performances. Les chapitres de cette partie abordent:

- les communications série
- PPP et PPP sur Ethernet
- le courrier électronique
- l'exécution de serveurs réseau
- les coupe-feux
- d'autres sujets réseau avancés

Ces chapitres sont destinés à être lus quand une information est nécessaire. Il n'est pas utile de les lire suivant un ordre particulier, ni de tous les lire avant de pouvoir utiliser FreeBSD dans un environnement réseau.

Chapitre 28. Serial Communications Traduction en Cours

28.1. Synopsis

28.2. Introduction

28.2.1. Terminology

28.2.2. Cables and Ports

28.2.2.1. Cables

28.2.2.1.1. Null-modem Cables

28.3. Terminals

28.3.1. Uses and Types of Terminals

28.3.2. Configuration

28.3.2.1. Adding an Entry to /etc/ttys

28.3.2.2. Force `init` to Reread /etc/ttys

28.3.3. Troubleshooting Your Connection

28.4. Dial-in Service

28.5. Dial-out Service

28.6. Setting Up the Serial Console

28.6.1. Tips for the Serial Console

28.6.1.1. Entering the DDB Debugger from the Serial Line

Chapitre 29. PPP et SLIP

29.1. Synopsis

FreeBSD dispose de nombreuses façons pour relier un ordinateur à un autre. Pour mettre en place un réseau ou établir une connexion Internet par l'intermédiaire d'un modem, ou pour autoriser d'autres à le faire par votre intermédiaire, il est nécessaire d'utiliser PPP ou SLIP. Ce chapitre décrit la configuration en détail de ces services de communication par modem.

Après la lecture de ce chapitre, vous saurez:

- Comment configurer PPP en mode utilisateur.
- Comment configurer PPP intégré au noyau.
- Comment configurer PPPoE (PPP sur Ethernet).
- Comment configurer PPPoA (PPP sur ATM).
- Comment configurer et utiliser un client et un serveur SLIP.

Avant de lire ce chapitre, vous devrez:

- Etre familier avec la terminologie réseau de base.
- Comprendre les bases, le but d'une connexion entrante par modem, et PPP et/ou SLIP.

Vous pouvez vous demander quelle est la principale différence entre PPP en mode utilisateur et PPP intégré au noyau. La réponse est simple: PPP en mode utilisateur traite les données entrantes et sortantes en dehors du noyau. C'est coûteux en terme de copie de donnée entre le noyau et l'espace utilisateur mais permet l'implémentation de plus de fonctionnalités PPP. PPP en mode utilisateur utilise le périphérique tun pour communiquer avec le monde extérieur alors que PPP intégré au noyau utilise le périphérique ppp.

Dans ce chapitre, le programme utilisateur PPP sera simplement appelé ppp, à moins qu'il faille explicitement faire la distinction entre lui et d'autres logiciels PPP comme pppd. Sauf indications contraires, toutes les commandes mentionnées dans ce chapitre doivent être exécutées par le super-utilisateur `root`.

29.2. Using User PPP Traduction en Cours

29.3. Utiliser PPP intégré au noyau

29.3.1. Configurer PPP intégré au noyau

Avant de configurer PPP sur votre machine, vérifiez que `pppd` est bien dans le répertoire /usr/sbin et que le répertoire /etc/ppp existe.

La commande `pppd` peut fonctionner selon deux modes:

1. Comme "client" - si vous désirez connecter votre machine au monde extérieur via une liaison PPP série ou un modem.
2. Comme "serveur" - si votre machine est sur le réseau, et sert à y connecter d'autres ordinateurs avec PPP.

Dans les deux cas, vous devrez renseigner un fichier d'options (/etc/ppp/options ou ~/.ppprc si vous avez plus d'un utilisateur sur votre machine utilisant PPP).

Vous aurez également besoin d'un logiciel "modem/série" (de préférence comms/kermit), pour appeler et établir la connexion avec la machine distante.

29.3.2. Utiliser pppd comme client

Le fichier /etc/ppp/options suivant pourrait être utilisé pour se connecter à la liaison PPP d'un concentrateur Cisco:

```
crtscts         # contrôle de flux matériel
modem           # liaison par modem
noipdefault     # adresse IP affectée par le serveur PPP distant
                # si la machine distante ne vous donne pas d'adresse
                # IP lors de la négociation IPCP, retirez cette option
passive         # attendre les paquets LCP
domain ppp.foo.com      # mettre ici votre nom de domaine

:remote_ip    # mettre ici l'adresse IP de la machine PPP distante
                # elle servira à router des paquets via la liaison PPP
                # si vous n'avez pas précisé l'option noipdefault
                # changez cette ligne en ip_locale:ip_distante

defaultroute    # mettre cette ligne si vous voulez que le serveur PPP soit
                # votre routeur par défaut
```

Pour se connecter:

1. Appelez la machine distante en utilisant kermit (ou un autre programme pour modem), puis entrez votre nom d'utilisateur et mot de passe (ou ce qu'il faut pour activer PPP sur la machine distante).
2. Quittez kermit (sans raccrocher la ligne).
3. Entrez la commande suivante:

   ```
   # /usr/src/usr.sbin/pppd.new/pppd /dev/tty01 19200
   ```

   Assurez-vous d'utiliser la vitesse et le nom de périphérique adéquats.

Votre ordinateur est maintenant connecté via PPP. Si la connexion échoue, vous pouvez ajouter

l'option debug au fichier /etc/ppp/options, et consulter les messages sur la console pour tracer le problème.

La procédure /etc/ppp/pppup ci-dessous effectuera automatiquement ces trois étapes:

```
#!/bin/sh
ps ax |grep pppd |grep -v grep
pid=`ps ax |grep pppd |grep -v grep|awk '{print $1;}'`
if [ "X${pid}" != "X" ] ; then
        echo 'arrêt de pppd, PID=' ${pid}
        kill ${pid}
fi
ps ax |grep kermit |grep -v grep
pid=`ps ax |grep kermit |grep -v grep|awk '{print $1;}'`
if [ "X${pid}" != "X" ] ; then
        echo 'arrêt de kermit, PID=' ${pid}
        kill -9 ${pid}
fi

ifconfig ppp0 down
ifconfig ppp0 delete

kermit -y /etc/ppp/kermit.dial
pppd /dev/tty01 19200
```

/etc/ppp/kermit.dial est une procédure kermit qui appelle et fournit toutes les informations d'authentification nécessaires à la machine distante (un exemple d'une telle procédure est donné à la fin de ce document).

Utilisez la procédure /etc/ppp/pppdown suivante pour terminer la session PPP et vous déconnecter:

```
#!/bin/sh
pid=`ps ax |grep pppd |grep -v grep|awk '{print $1;}'`
if [ X${pid} != "X" ] ; then
        echo 'arrêt de pppd, PID=' ${pid}
        kill -TERM ${pid}
fi

ps ax |grep kermit |grep -v grep
pid=`ps ax |grep kermit |grep -v grep|awk '{print $1;}'`
if [ "X${pid}" != "X" ] ; then
        echo 'arrêt de kermit, PID=' ${pid}
        kill -9 ${pid}
fi

/sbin/ifconfig ppp0 down
/sbin/ifconfig ppp0 delete
kermit -y /etc/ppp/kermit.hup
```

```
/etc/ppp/ppptest
```

Vérifiez si pppd tourne toujours en lançant la procédure /usr/etc/ppp/ppptest, qui devrait ressembler à ceci:

```
#!/bin/sh
pid=`ps ax| grep pppd |grep -v grep|awk '{print $1;}'`
if [ X${pid} != "X" ] ; then
        echo 'pppd actif: PID=' ${pid-NONE}
else
        echo 'Pas de pppd en cours d'exécution.'
fi
set -x
netstat -n -I ppp0
ifconfig ppp0
```

Pour raccrocher la ligne, exécutez /etc/ppp/kermit.hup, qui devrait contenir:

```
set line /dev/tty01 ; mettre ici le périphérique pour votre modem
set speed 19200
set file type binary
set file names literal
set win 8
set rec pack 1024
set send pack 1024
set block 3
set term bytesize 8
set command bytesize 8
set flow none

pau 1
out +++
inp 5 OK
out ATH0\13
echo \13
exit
```

Voici une autre méthode qui utilise chat au lieu de kermit.

Les deux fichiers suivants suffisent à établir une connexion avec pppd.

/etc/ppp/options:

```
/dev/cuaa1 115200

crtscts     # contrôle de flux matériel
modem       # liaison par modem
connect "/usr/bin/chat -f /etc/ppp/login.chat.script"
```

```
noipdefault # adresse IP affectée par le serveur PPP distant
            # si la machine distante ne vous donne pas d'adresse
            # IP lors de la négociation IPCP, retirer cette option
passive         # attendre les paquets LCP
domain your.domain  # mettre ici votre nom de domaine

:           # mettre ici l'adresse IP de la machine PPP distante
            # elle servira à router des paquets via la liaison PPP
            # si vous n'avez pas précisé l'option noipdefault
            # modifier cette ligne en ip_locale:ip_distante

defaultroute    # mettre cette ligne si vous voulez que le serveur PPP soit
            # votre routeur par défaut
```

/etc/ppp/login.chat.script:

Ce qui suit doit être tapé sur une seule ligne.

```
ABORT BUSY ABORT 'NO CARRIER' "" AT OK ATDTnuméro_de_téléphone
  CONNECT "" TIMEOUT 10 ogin:-\\r-ogin: nom_d_utilisateur
  TIMEOUT 5 sword: mot_de_passe
```

Une fois que ces fichiers sont installés et correctement modifiés, tout ce dont vous avez besoin de faire est de lancer pppd, comme suit:

```
# pppd
```

29.3.3. Utiliser pppd comme serveur

Le contenu du fichier /etc/ppp/options devrait être semblable à ce qui suit:

```
crtscts                         # contrôle de flux matériel
netmask 255.255.255.0           # masque de sous-réseau (facultatif)
192.114.208.20:192.114.208.165  # adresses IP des machines locales et distantes
                                # l'adresse locale ne doit pas être la même que
                                # celle que vous avez assignée à l'interface
                                # Ethernet (ou autre) de la machine.
                                # l'adresse IP de la machine distante est
                                # l'adresse IP qui lui sera affectée
domain ppp.foo.com              # votre nom de domaine
passive                         # attendre LCP
modem                           # liaison modem
```

La procédure /etc/ppp/pppserv ci-dessous demandera à pppd de se comporter comme un serveur:

```
#!/bin/sh
ps ax |grep pppd |grep -v grep
pid=`ps ax |grep pppd |grep -v grep|awk '{print $1;}'`
if [ "X${pid}" != "X" ] ; then
        echo 'arrêt de pppd, PID=' ${pid}
        kill ${pid}
fi
ps ax |grep kermit |grep -v grep
pid=`ps ax |grep kermit |grep -v grep|awk '{print $1;}'`
if [ "X${pid}" != "X" ] ; then
        echo 'arrêt de kermit, PID=' ${pid}
        kill -9 ${pid}
fi

# réinitialiser l'interface ppp
ifconfig ppp0 down
ifconfig ppp0 delete

# activer le mode réponse automatique
kermit -y /etc/ppp/kermit.ans

# lancer ppp
pppd /dev/tty01 19200
```

Utilisez cette procédure /etc/ppp/pppservdown pour arrêter le serveur:

```
#!/bin/sh
ps ax |grep pppd |grep -v grep
pid=`ps ax |grep pppd |grep -v grep|awk '{print $1;}'`
if [ "X${pid}" != "X" ] ; then
        echo 'arrêt de pppd, PID=' ${pid}
        kill ${pid}
fi
ps ax |grep kermit |grep -v grep
pid=`ps ax |grep kermit |grep -v grep|awk '{print $1;}'`
if [ "X${pid}" != "X" ] ; then
        echo 'arrêt de kermit, PID=' ${pid}
        kill -9 ${pid}
fi
ifconfig ppp0 down
ifconfig ppp0 delete

kermit -y /etc/ppp/kermit.noans
```

La procédure kermit ci-dessous (/etc/ppp/kermit.ans) activera ou désactivera le mode réponse automatique de votre modem:

```
set line /dev/tty01
```

```
set speed 19200
set file type binary
set file names literal
set win 8
set rec pack 1024
set send pack 1024
set block 3
set term bytesize 8
set command bytesize 8
set flow none

pau 1
out +++
inp 5 OK
out ATH0\13
inp 5 OK
echo \13
out ATS0=1\13   ; remplacer cela par ATS0=0\13 si vous voulez désactiver
                ; le mode réponse automatique
inp 5 OK
echo \13
exit
```

Une procédure nommée /etc/ppp/kermit.dial est utilisée pour appeler et s'authentifier sur la machine distante. Vous devrez l'adapter à vos besoins. Mettez-y votre nom d'utilisateur et votre mot de passe; vous devrez également modifier les entrées en fonctions des réponses que vous envoient votre modem et la machine distante.

```
;
; mettre ici la liaison série à laquelle est raccordé le modem:
;
set line /dev/tty01
;
; mettre ici la vitesse du modem:
;
set speed 19200
set file type binary            ; transfert 8 bits
set file names literal
set win 8
set rec pack 1024
set send pack 1024
set block 3
set term bytesize 8
set command bytesize 8
set flow none
set modem hayes
set dial hangup off
set carrier auto                ; puis SET CARRIER si nécessaire,
set dial display on             ; puis SET DIAL si nécessaire,
set input echo on
```

```
set input timeout proceed
set input case ignore
def \%x 0                       ; compteur d'ouverture de session
goto slhup

:slcmd                          ; mettre le modem en mode commande
echo Put the modem in command mode.
clear                           ; vider le tampon d'entrée
pause 1
output +++                      ; séquence d'échappement Hayes
input 1 OK\13\10                ; attendre OK
if success goto slhup
output \13
pause 1
output at\13
input 1 OK\13\10
if fail goto slcmd              ; si le modem ne répond pas OK, réessayer

:slhup                          ; raccrocher la ligne
clear                           ; vider le tampon d'entrée
pause 1
echo Hanging up the phone.
output ath0\13                  ; commande Hayes pour raccrocher
input 2 OK\13\10
if fail goto slcmd              ; si pas de réponse OK, passer le modem en mode
commande

:sldial                         ; composer le numéro
pause 1
echo Dialing.
output atdt9,550311\13\10       ; mettre ici le numéro de téléphone
assign \%x 0                    ; mettre le compteur à zéro

:look
clear                           ; vider le tampon d'entrée
increment \%x                   ; compter les secondes
input 1 {CONNECT }
if success goto sllogin
reinput 1 {NO CARRIER\13\10}
if success goto sldial
reinput 1 {NO DIALTONE\13\10}
if success goto slnodial
reinput 1 {\255}
if success goto slhup
reinput 1 {\127}
if success goto slhup
if  \%x 60 goto look
else goto slhup

:sllogin                        ; ouverture de session
assign \%x 0                    ; mettre le compteur à zéro
```

```
pause 1
echo Looking for login prompt.

:slloop
increment \%x                   ; compter les secondes
clear                           ; vider le tampon d'entrée
output \13
;
; put your expected login prompt here:
;
input 1 {Username: }
if success goto sluid
reinput 1 {\255}
if success goto slhup
reinput 1 {\127}
if success goto slhup
if  \%x 10 goto slloop         ; essayer 10 fois d'obtenir une invite de session
else goto slhup                 ; raccrocher et recommencer après 10 échecs

:sluid
;
; mettre ici votre nom d'utilisateur:
;
output nom-d-utilisateur-ppp\13
input 1 {Password: }
;
; mettre ici votre mot de passe:
;
output mot-de-passe-ppp\13
input 1 {Entering SLIP mode.}
echo
quit

:slnodial
echo \7Pas de tonalité.  Vérifiez votre ligne téléphonique!\7
exit 1

; local variables:
; mode: csh
; comment-start: "; "
; comment-start-skip: "; "
; end:
```

29.4. Utiliser PPP sur Ethernet (PPPoE)

Cette section décrit comment configurer PPP sur Ethernet (PPPoE).

29.4.1. Configuration du noyau

Il n'est plus du tout nécessaire de configurer le noyau pour utiliser PPPoE. Si le support netgraph nécessaire n'est pas compilé dans le noyau, il sera chargé dynamiquement par ppp.

29.4.2. Renseigner ppp.conf

Voici un exemple de fichier ppp.conf opérationnel:

```
default:
  set log Phase tun command # vous pouvez détailler plus les traces si vous le désirez
  set ifaddr 10.0.0.1/0 10.0.0.2/0

nom_du_fournisseur_d'accès:
  set device PPPoE:xl1 # remplacez xl1 par votre périphérique Ethernet
  set authname VOTRENOMDUTILISATEUR
  set authkey VOTREMOTDEPASSE
  set dial
  set login
  add default HISADDR
```

29.4.3. Exécuter ppp

En tant que `root`, vous pouvez lancer:

```
# ppp -ddial nom_du_fournisseur_d'accès
```

29.4.4. Lancer ppp au démarrage

Ajoutez ce qui suit à votre fichier /etc/rc.conf:

```
ppp_enable="YES"
ppp_mode="ddial"
ppp_nat="YES"   # si vous voulez activer NAT pour votre réseau local, sinon NO
ppp_profile="nom_du_fournisseur_d'accès"
```

29.4.5. Utilisation d'une étiquette de service PPPoE

Parfois il sera nécessaire d'utiliser une étiquette de service pour établir votre connexion. Les étiquettes de service sont employées pour faire la distinction entre différents serveurs PPPoE attachés à un réseau donné.

Vous devez avoir l'information concernant l'étiquette de service dans la documentation fournie par votre fournisseur d'accès. Si vous ne pouvez la trouver, contactez le support technique de votre fournisseur d'accès Internet.

En dernier ressort, vous pourrez essayer la méthode suggérée par le programme Roaring Penguin PPPoE qui peut-être trouvé dans le catalogue des logiciels portés. Gardez cependant à l'esprit, que cela peut déprogrammer votre modem et le rendre inutilisable, aussi réfléchissez à deux fois avant de le faire. Installez simplement le logiciel fourni avec le modem par votre fournisseur d'accès. Ensuite accédez au menu **Système** du programme. Le nom de votre profil devrait y figurer. C'est habituellement le nom du *FAI*.

Le nom du profil (étiquette de service) sera utilisé dans l'entrée de configuration PPPoE dans le fichier ppp.conf dans la partie fournisseur d'accès de la commande `set device` (voir la page de manuel ppp(8) pour plus de détails). Cela devrait ressembler à ceci:

```
set device PPPoE:xl1:FAI
```

N'oubliez pas de changer *xl1* pour le périphérique correct correspondant à votre carte Ethernet.

N'oubliez pas de changer *FAI* par le profil que vous avez déterminé ci-dessus.

Pour une information supplémentaire, consultez:

- Cheaper Broadband with FreeBSD on DSL par Renaud Waldura.
- Nutzung von T-DSL und T-Online mit FreeBSD par Udo Erdelhoff (en allemand).

29.4.6. PPPoE avec un modem ADSL 3Com® HomeConnect™ Dual Link

Ce modem ne respecte pas la RFC 2516 (*A Method for transmitting PPP over Ethernet (PPPoE)*, rédigée par L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, et R. Wheeler). Au lieu de cela des codes différents pour les types de paquets sont utilisés pour les frames Ethernet. Veuillez vous plaindre auprès de 3Com si vous pensez que le modem devrait respecter la spécification PPPoE.

Afin de permettre à FreeBSD de communiquer avec ce périphérique, un paramètre sysctl doit être configuré. Cela peut être effectué de manière automatique au démarrage en renseignant le fichier /etc/sysctl.conf:

```
net.graph.nonstandard_pppoe=1
```

ou peut être paramétré pour prendre immédiatement effet avec la commande:

```
# sysctl net.graph.nonstandard_pppoe=1
```

Malheureusement, parce que c'est un paramétrage concernant l'intégralité du système, il n'est pas possible de communiquer en même temps avec un client ou un serveur PPPoE normal et un modem ADSL 3Com® HomeConnect™.

29.5. Utiliser PPP sur ATM (PPPoA)

Ce qui suit décrit comment configurer PPP sur ATM (PPPoA). PPPoA est très populaire parmi les fournisseurs d'accès DSL européens.

29.5.1. Utiliser PPPoA avec le modem Alcatel SpeedTouch™ USB

Le support PPPoA pour ce périphérique est fourni sous la forme d'un logiciel porté sous FreeBSD car le "firmware" est distribué sous l'accord de licence d'Alcatel et ne peut être redistribué librement avec le système de base de FreeBSD.

Pour installer le logiciel, utilisez simplement le catalogue des logiciels portés. Installez le logiciel porté net/pppoa et suivez les instructions fournies avec.

Comme de nombreux périphériques, le modem USB Alcatel SpeedTouch™ a besoin de charger un "firmware" à partir de l'ordinateur hôte pour opérer correctement. Il est possible d'automatiser ce processus sous FreeBSD de manière à ce que ce transfert ait lieu dès que le périphérique est branché dans un port USB. L'information suivante peut être ajoutée au fichier /etc/usbd.conf pour autoriser ce transfert automatique de "firmware". Ce fichier doit être édité en tant que super-utilisateur.

```
device "Alcatel SpeedTouch USB"
    devname "ugen[0-9]+"
    vendor 0x06b9
    product 0x4061
    attach "/usr/local/sbin/modem_run -f /usr/local/libdata/mgmt.o"
```

Pour activer le "daemon" USB, usbd, ajoutez la ligne suivante dans le fichier /etc/rc.conf:

```
usbd_enable="YES"
```

Il est également possible de paramétrer ppp pour se connecter au démarrage. Pour cela ajoutez les lignes suivantes au fichier /etc/rc.conf. Encore une fois, vous devrez être attaché sous l'utilisateur `root` pour effectuer ces ajouts.

```
ppp_enable="YES"
ppp_mode="ddial"
ppp_profile="adsl"
```

Pour que cela fonctionne correctement, vous devrez utiliser le fichier d'exemple ppp.conf qui est fourni avec le logiciel porté net/pppoa.

29.5.2. Utiliser mpd

Vous pouvez utiliser mpd pour vous connecter à différents services, en particulier aux services PPTP. Vous trouverez mpd dans le catalogue des logiciels portés, net/mpd. De nombreux modems

ADSL demandent à ce qu'un tunnel PPTP soit créé entre le modem et l'ordinateur, le SpeedTouch™ Home d'Alcatel en fait partie.

Vous devez tout d'abord installer le logiciel porté, ensuite vous pouvez configurer mpd selon vos besoins et les paramètres propres au fournisseur d'accès. Le logiciel porté place un ensemble de fichiers de configuration très bien commentés dans le répertoire PREFIX/etc/mpd/. Notez qu'ici *PREFIX* représente le répertoire dans lequel les logiciels portés sont installés, par défaut le répertoire /usr/local/. Un guide complet pour la configuration de mpd est disponible dans le format HTML, une fois que le logiciel a été installé. Il se trouve dans le répertoire PREFIX/shared/doc/mpd/. Voici un exemple de configuration pour se connecter à un service ADSL à l'aide de mpd. La configuration est séparée en deux fichiers, le premier est mpd.conf:

```
default:
    load adsl

adsl:
    new -i ng0 adsl adsl
    set bundle authname username ①
    set bundle password password ②
    set bundle disable multilink

    set link no pap acfcomp protocomp
    set link disable chap
    set link accept chap
    set link keep-alive 30 10

    set ipcp no vjcomp
    set ipcp ranges 0.0.0.0/0 0.0.0.0/0

    set iface route default
    set iface disable on-demand
    set iface enable proxy-arp
    set iface idle 0

    open
```

① Le nom d'utilisateur utilisé pour vous identifier auprès de votre FAI.

② Le mot de passe utilisé pour vous identifier auprès de votre FAI.

Le fichier mpd.links contient les informations concernant la liaison, ou les liaisons, que vous souhaitez établir. En exemple de fichier mpd.links accompagnant l'exemple précédent est donné ci-dessous:

```
adsl:
    set link type pptp
    set pptp mode active
    set pptp enable originate outcall
    set pptp self 10.0.0.1 ①
```

```
    set pptp peer 10.0.0.138 ②
```

① L'adresse IP de la machine FreeBSD à partir de laquelle vous utiliserez mpd.

② L'adresse IP de votre modem ADSL. Pour le SpeedTouch™ Home d'Alcatel cette adresse est par défaut `10.0.0.138`.

Il est possible d'initialiser aisément une connexion en tapant la commande suivante en tant que `root`:

```
# mpd -b adsl
```

Vous pouvez voir quel est l'état de votre connexion à l'aide de la commande suivante:

```
% ifconfig ng0
ng0: flags=88d1<UP,POINTOPOINT,RUNNING,NOARP,SIMPLEX,MULTICAST> mtu 1500
     inet 216.136.204.117 --> 204.152.186.171 netmask 0xffffffff
```

L'utilisation de mpd est la méthode recommandée de connexion à un service ADSL sous FreeBSD.

29.5.3. Utiliser pptpclient

Il est également possible d'utiliser FreeBSD pour se connecter à d'autres service PPPoA en utilisant net/pptpclient.

Pour utiliser net/pptpclient pour vous connecter à un service DSL, installez le logiciel porté ou le paquetage correspondant et éditez votre fichier /etc/ppp/ppp.conf. Vous aurez besoin des droits de super-utilisateur pour effectuer ces deux opérations. Un exemple de fichier ppp.conf est donné plus bas. Pour plus d'information sur les options du fichier ppp.conf, consultez la page de manuel de ppp, ppp(8).

```
adsl:
 set log phase chat lcp ipcp ccp tun command
 set timeout 0
 enable dns
 set authname username ①
 set authkey password ②
 set ifaddr 0 0
 add default HISADDR
```

① Le nom d'utilisateur de votre compte chez le fournisseur d'accès DSL.

② Le mot de passe de votre compte.

Etant donné que vous devez mettre le mot de passe de votre compte en clair dans le fichier ppp.conf, vous devez vous assurer que personne d'autre ne puisse lire le contenu de ce fichier. La série de commandes suivante s'assurera que ce fichier n'est lisible que par `root`. Référez-vous aux pages de manuel de chmod(1) et

chown(8) pour plus d'informations.

```
# chown root:wheel /etc/ppp/ppp.conf
# chmod 600 /etc/ppp/ppp.conf
```

Cela créera un tunnel pour une session PPP vers votre routeur DSL. Les modems DSL Ethernet ont une adresse IP pour le réseau local pré-configurée à laquelle vous vous connectez. Dans le cas du modem SpeedTouch™ Home d'Alcatel cette adresse est 10.0.0.138. La documentation de votre routeur devrait mentionner quelle adresse utilise votre périphérique. Pour créer le tunnel et démarrer une session PPP exécutez la commande suivante:

```
# pptp address adsl
```

Vous pourrez ajouter un "et commercial" ("") à la fin de la commande précédente car sinon pptp ne vous rendra pas la main.

Un périphérique virtuel de tunnel (tun) sera créé pour la communication entre les processus pptp et ppp. Une fois retourné à l'invite, ou que le processus pptp a confirmé la connexion, vous pouvez examiner le tunnel de cette manière:

```
% ifconfig tun0
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
        inet 216.136.204.21 --> 204.152.186.171 netmask 0xffffff00
        Opened by PID 918
```

Si vous n'êtes pas en mesure de vous connecter, vérifiez la configuration de votre routeur qui est généralement accessible par telnet ou avec un navigateur web. Si le problème persiste, vous devrez examiner la sortie de la commande pptp et le contenu du fichier de trace de ppp, /var/log/ppp.log à la recherche d'indices.

29.6. Utiliser SLIP

29.6.1. Configurer un client SLIP

Ce qui suit décrit une manière de configurer une machine FreeBSD pour utiliser SLIP sur un réseau où les noms de machine sont statiques. Si le nom de machine est affecté dynamiquement (votre adresse change à chaque connexion), vous devrez probablement utiliser une méthode plus sophistiquée.

Tout d'abord, déterminez sur quel port série votre modem est connecté. De nombreuses personnes utilisent un lien symbolique, comme /dev/modem, pour pointer vers le nom réel du périphérique, /dev/cuaaN (ou /dev/cuadN sous FreeBSD 6.X). Ceci vous permet de faire abstraction du véritable nom du périphérique même si vous déplacez le modem vers un autre port. Cela évite le côté pénible de devoir modifier un certain nombre de fichiers dans le répertoire /etc et les fichiers .kermrc pour l'ensemble du système!

/dev/cuaa0 (ou /dev/cuad0 sous FreeBSD 6.X) représente COM1, cuaa1 (ou /dev/cuad1) COM2, etc.

Assurez-vous d'avoir dans votre fichier de configuration du noyau ce qui suit:

```
device   sl
```

Sous FreeBSD 4.X, utilisez à la place la ligne suivante:

```
pseudo-device   sl      1
```

Cette configuration fait partie du noyau GENERIC, aussi cela ne devrait pas être un problème à moins que vous ne l'ayez effacée.

29.6.1.1. Ce que vous n'aurez à faire qu'une seule fois

1. Ajoutez votre machine, la passerelle et les serveurs de noms de domaines à votre fichier /etc/hosts. Le notre ressemble à ceci:

   ```
   127.0.0.1               localhost loghost
   136.152.64.181          water.CS.Example.EDU water.CS water
   136.152.64.1            inr-3.CS.Example.EDU inr-3 slip-gateway
   128.32.136.9            ns1.Example.EDU ns1
   128.32.136.12           ns2.Example.EDU ns2
   ```

2. Assurez-vous que `hosts` apparaît avant `bind` dans votre fichier /etc/host.conf sous les versions de FreeBSD antérieures à 5.0. Depuis FreeBSD 5.0, le système utilise à la place le fichier /etc/nsswitch.conf, vérifiez que `files` est avant `dns` dans la ligne `hosts` de ce fichier. Sans ces paramètres, il peut se passer des choses bizarres.
3. Editez le fichier /etc/rc.conf.
   a. Définissez votre nom de machine en éditant la ligne:

      ```
      hostname="myname.my.domain"
      ```

      Le nom Internet complet de la machine doit être utilisé ici.

   b. Ajoutez sl0 à la liste des interfaces réseau en modifiant la ligne:

      ```
      network_interfaces="lo0"
      ```

      en:

```
network_interfaces="lo0 sl0"
```

c. Définissez les paramètres de configuration de sl0 en ajoutant une ligne:

```
ifconfig_sl0="inet ${hostname} slip-gateway netmask 0xffffff00 up"
```

d. Indiquez la passerelle par défaut en modifiant la ligne:

```
defaultrouter="NO"
```

en:

```
defaultrouter="slip-gateway"
```

4. Créez un fichier /etc/resolv.conf qui contient:

```
domain CS.Example.EDU
nameserver 128.32.136.9
nameserver 128.32.136.12
```

Comme vous pouvez le voir, ceci définit les serveurs de noms de domaines. Bien entendu, les noms de domaines et les adresses dépendront de votre environnement.

5. Donnez des mots de passe pour les utilisateurs `root` et `toor` (et à tous les autres comptes qui n'auraient pas de mot de passe).
6. Redémarrez votre machine et vérifiez qu'elle a bien le nom voulu.

29.6.1.2. Etablir une connexion SLIP

1. Téléphonez, tapez `slip` à l'invite, puis entrez votre nom de machine et votre mot de passe. Ce que vous devez entrer dépend de votre environnement. Si vous utilisez Kermit, vous pouvez essayer une procédure comme celle-ci:

```
# configuration kermit
set modem hayes
set line /dev/modem
set speed 115200
set parity none
set flow rts/cts
set terminal bytesize 8
set file type binary
# The next macro will dial up and login
```

```
define slip dial 643-9600, input 10 =, if failure stop, -
output slip\x0d, input 10 Username:, if failure stop, -
output silvia\x0d, input 10 Password:, if failure stop, -
output ***\x0d, echo \x0aCONNECTED\x0a
```

Vous devez, bien évidemment, remplacer le nom d'utilisateur et le mot de passe par les votre. Après cela vous pouvez alors entrer simplement `slip` à l'invite de Kermit pour vous connecter.

Conserver votre mot de passe en clair dans un fichier quelconque est en général une *mauvaise* idée. Faites-le à vos risques et périls.

2. Laissez ensuite Kermit tel quel (vous pouvez le mettre en arrière-plan avec `Ctrl` + `z`) et en tant que `root`, tapez:

```
# slattach -h -c -s 115200 /dev/modem
```

Si vous êtes en mesure d'envoyer un `ping` vers des machines situées de l'autre côté du routeur, c'est que vous êtes connecté! Si cela ne fonctionne pas, vous pouvez essayer l'option `-a` au lieu de `-c` en argument de `slattach`.

29.6.1.3. Comment couper la connexion

Effectuez ceci:

```
# kill -INT `cat /var/run/slattach.modem.pid`
```

pour tuer `slattach`. Gardez à l'esprit que vous devez avoir les droits du super-utilisateur pour faire cela. Revenez ensuite sous `kermit` (en tapant `fg` si l'avez mis en tâche de fond) et quittez-le (`q`).

La page de manuel de slattach(8) dit que vous devez employer la commande `ifconfig sl0 down` pour indiquer que l'interface n'est plus active, mais cela ne change apparemment rien (les diagnostics donnés par la commande `ifconfig sl0` restent identiques).

Il arrive que parfois que votre modem refuse de raccrocher. Dans ce cas, relancez `kermit` et quittez-le de nouveau. Cela fonctionne en général à la seconde tentative.

29.6.1.4. Dépannage

Si cela ne fonctionne pas, n'hésitez pas à contacter la liste de diffusion freebsd-net. Voici les problèmes que certains ont rencontré jusqu'ici:

- Ne pas utiliser l'option `-c` ou `-a` avec `slattach` (Cela ne devrait pas poser de problème, mais des utilisateurs ont signalé que l'utilisation de cet indicateur a résolu leur problème).
- Utiliser `s10` au lieu de `sl0` (avec certaines polices de caractères, il est parfois difficile de faire la différence).

- Essayez `ifconfig sl0` pour connaître la configuration de votre interface. Vous obtiendrez, par exemple:

```
# ifconfig sl0
sl0: flags=10<POINTOPOINT>
        inet 136.152.64.181 --> 136.152.64.1 netmask ffffff00
```

- Si vous obtenez le message d'erreur `no route to host` lors de l'utilisation de ping(8), il se peut qu'il y ait un problème avec votre table de routage. Vous pouvez utiliser la commande `netstat -r` pour afficher les routes actives:

```
# netstat -r
Routing tables
Destination      Gateway            Flags     Refs     Use  IfaceMTU    Rtt
Netmasks:

(root node)
(root node)

Route Tree for Protocol Family inet:
(root node) =>
default          inr-3.Example.EDU  UG          8   224515  sl0 -      -
localhost.Exampl localhost.Example. UH          5    42127  lo0 -       0.438
inr-3.Example.ED water.CS.Example.E UH          1        0  sl0 -      -
water.CS.Example localhost.Example. UGH        34 47641234  lo0 -       0.438
(root node)
```

  Les exemples précédents proviennent d'un système relativement chargé. La valeurs sur votre système varieront en fonction de l'activité réseau.

29.6.2. Configurer un serveur SLIP

Ce document donne des indications pour la mise en oeuvre d'un serveur SLIP sur un système FreeBSD, ce qui signifie généralement configurer votre système pour ouvrir automatiquement une connexion à l'ouverture d'une session depuis un client SLIP distant.

29.6.2.1. Prérequis

Cette section est très technique, il vous faut donc quelques connaissances de base. On supposera que vous connaissez le protocole réseau TCP/IP et, en particulier, l'adressage des réseaux et des noeuds, les masques de sous-réseau, les sous-réseaux, le routage et les protocoles de routage tels que RIP. Ce sont les concepts que vous devez maîtriser pour configurer les services SLIP sur un serveur de connexions, et si ce n'est pas le cas, veuillez lire *TCP/IP Network Administration* de Craig Hunt chez O'Reilly Associates, Inc. (ISBN 0-937175-82-X), ou les ouvrages de Douglas Comer sur le protocole TCP/IP.

On suppose également que vous avez déjà installé vos modems et configuré les fichiers systèmes appropriés pour permettre l'ouverture de session via vos modems. Si vous ne l'avez pas encore fait

reportez-vous à la Dial-in Service pour des informations sur la configuration des connexions entrantes. Vous pouvez aussi consulter les pages de manuel de sio(4) pour plus d'information sur le pilote du port série et ttys(5), gettytab(5), getty(8), et init(8) en ce qui concerne la configuration du système pour qu'il autorise les connexions en provenance de modems, et peut-être la page de manuel stty(1) pour des informations sur le paramétrage des ports série (comme `clocal` pour les interfaces série directement connectées).

29.6.2.2. Rapide vue d'ensemble

Une configuration typique d'utilisation de FreeBSD comme serveur SLIP fonctionne de la manière suivante: un utilisateur SLIP appelle votre serveur SLIP FreeBSD et ouvre une session sous un identifiant utilisateur SLIP particulier qui lance /usr/sbin/sliplogin comme interpréteur de commandes. Le programme `sliplogin` consulte le fichier /etc/sliphome/slip.hosts à la recherche d'une ligne correspondant à cet utilisateur particulier, et s'il la trouve, connecte la ligne série à une interface SLIP disponible et lance ensuite la procédure /etc/sliphome/slip.login pour configurer cette interface SLIP.

29.6.2.2.1. Un exemple d'ouverture de session sur un serveur SLIP

Par exemple, si `Shelmerg` était un identifiant utilisateur SLIP, l'entrée pour `Shelmerg` ressemblerait à ceci:

```
Shelmerg:password:1964:89::0:0:Guy Helmer -
SLIP:/usr/users/Shelmerg:/usr/sbin/sliplogin
```

Quand `Shelmerg` ouvre une session, `sliplogin` consulte /etc/sliphome/slip.hosts à la recherche d'une ligne correspondant à l'identifiant de l'utilisateur correspondant; par exemple, il peut y avoir dans le fichier /etc/sliphome/slip.hosts la ligne:

```
Shelmerg        dc-slip sl-helmer       0xfffffc00        autocomp
```

`sliplogin` trouvera alors cette ligne, affectera la ligne série à l'interface SLIP suivante,et ensuite exécutera /etc/sliphome/slip.login avec les arguments suivants:

```
/etc/sliphome/slip.login 0 19200 Shelmerg dc-slip sl-helmer 0xfffffc00 autocomp
```

Si tous se passe bien, /etc/sliphome/slip.login exécutera un `ifconfig` sur l'interface SLIP que s'est attribué `sliplogin` (l'interface SLIP 0, dans l'exemple ci-dessus, qui est le premier paramètre passé à slip.login) pour définir l'adresse IP locale (`dc-slip`), l'adresse IP de la machine distante (`sl-helmer`), le masque de sous-réseau de l'interface SLIP (`0xfffffc00`), et tout autre indicateur supplémentaire (`autocomp`). Si quelque chose se passe mal, `sliplogin` fournit en général des messages d'information via la fonctionnalité de trace du "démon"syslogd, qui les enregistre habituellement dans le fichier /var/log/messages (reportez-vous au pages de manuel de syslogd(8) et syslog.conf(5) et consultez peut-être aussi le fichier /etc/syslog.conf pour voir ce que trace syslogd et où il enregistre ces messages.).

29.6.2.3. Configuration du noyau

Le noyau par défaut de FreeBSD (GENERIC) fourni le support SLIP (sl(4)); dans le cas d'un noyau personnalisé, vous devez ajouter la ligne suivante à votre fichier de configuration du noyau:

```
device   sl
```

Sous FreeBSD 4.X, utilisez la ligne suivante:

```
pseudo-device   sl      2
```

Le chiffre en fin de ligne représente le nombre maximum de connexions SLIP qui peuvent cohexister. Depuis FreeBSD 5.0, le pilote sl(4) est capable d'"auto-clonage".

Par défaut, votre machine FreeBSD ne transmettra pas les paquets. Si vous désirez que votre serveur SLIP FreeBSD agisse en routeur, vous devez éditer le fichier /etc/rc.conf et positionner la variable `gateway_enable` à `YES`.

Vous devrez ensuite redémarrer pour que les nouveaux paramètres prennent effet.

Veuillez vous référer à la Configurer le noyau de FreeBSD sur la configuration du noyau pour de l'aide sur ce sujet.

29.6.2.4. Configuration de sliplogin

Comme indiqué plus haut, il y a trois fichiers dans le répertoire /etc/sliphome qui servent à la configuration de /usr/sbin/sliplogin (voyez sliplogin(8) pour avoir la page de manuel de `sliplogin`): slip.hosts, définit les utilisateurs SLIP et les adresses IP qui leur sont associées, slip.login, qui ne fait en général que configurer l'interface SLIP, et (facultatif) slip.logout, qui effectue le travail inverse de slip.login quand la connexion série est terminée.

29.6.2.4.1. Configuration de slip.hosts

/etc/sliphome/slip.hosts contient des lignes avec au moins quatre champs séparés par des espaces:

- L'identifiant (ID) d'utilisateur SLIP;
- L'adresse locale (locale au serveur SLIP) de la liaison SLIP;
- L'adresse de l'autre extrémité de la liaison SLIP;
- Le masque de sous-réseau.

Les adresses locales et distantes peuvent être des noms de machines (qui seront convertis en adresses IP via /etc/hosts ou par le service de noms de domaines, en fonction de ce que contient le fichier /etc/nsswitch.conf, ou /etc/host.conf si vous utilisez FreeBSD 4.X), et le masque de sous-réseau peut être un nom qui sera converti en consultant le fichier /etc/networks. Par exemple, /etc/sliphome/slip.hosts contiendra:

```
#
# login local-addr      remote-addr     mask            opt1    opt2
#                                                (normal,compress,noicmp)
#
Shelmerg  dc-slip       sl-helmerg      0xfffffc00      autocomp
```

La ligne se termine par une ou plusieurs options:

- `normal` - pas de compression des en-têtes;
- `compress` - compression des en-têtes;
- `autocomp` - compression des en-têtes si la machine distante l'autorise;
- `noicmp` - interdit les paquets ICMP (de sorte que les paquets "ping" seront ignorés au lieu de consommer votre bande passante).

Le choix des adresses pour les deux extrémités des liaisons SLIP dépend du fait que vous leur dédiez un sous-réseau TCP/IP ou que vous comptiez utiliser un "proxy ARP" sur votre serveur SLIP (ce n'est pas un "vrai" proxy ARP, mais c'est la terminologie que nous utiliserons dans ce document pour le désigner). Si vous n'êtes pas sûr de la méthode à choisir ou de la façon d'assigner les adresses IP, référez-vous aux ouvrages sur le TCP/IP mentionnés à section sur les prérequis (Prérequis) et/ou consultez l'administrateur de votre réseau IP.

Si vous comptez utiliser un sous-réseau IP séparé pour vos clients SLIP, vous devrez définir l'adresse de sous-réseau à partir de votre réseau IP et attribuer à chacun de vos clients SLIP une adresse IP sur ce sous-réseau. Ensuite, vous devrez probablement configurer sur votre routeur IP le plus proche une route statique vers votre sous-réseau SLIP via votre serveur SLIP.

Sinon, si vous avez l'intention d'utiliser la méthode du "proxy ARP", vous devrez assigner à vos clients SLIP des adresses IP en provenance du sous-réseau Ethernet de votre serveur SLIP, et vous devrez également adapter vos procédures /etc/sliphome/slip.login et /etc/sliphome/slip.logout pour qu'elles utilisent arp(8) pour gérer les entrées proxy ARP dans la table ARP de votre serveur SLIP.

29.6.2.4.2. Configuration de slip.login

Le fichier /etc/sliphome/slip.login ressemble généralement à ceci:

```
#!/bin/sh -
#
#       @(#)slip.login  5.1 (Berkeley) 7/1/90

#
# procédure générique d'ouverture de session pour
# une liaison SLIP.  sliplogin l'appelle avec les paramètres:
#      1        2         3        4          5         6     7-n
# interface vitesse nom adresse-locale adresse-distante masque arg-optionnels
#
/sbin/ifconfig sl$1 inet $4 $5 netmask $6
```

Ce fichier slip.login ne fait qu'exécuter `ifconfig` sur l'interface SLIP appropriée avec comme paramètres les adresses locales et distantes et le masque de sous-réseau de l'interface SLIP.

Si vous avez choisi d'utiliser la méthode du "proxy ARP" (au lieu d'affecter un sous-réseau distinct à vos clients SLIP), votre fichier /etc/sliphome/slip.login devra ressembler à ceci:

```
#!/bin/sh -
#
#       @(#)slip.login  5.1 (Berkeley) 7/1/90

#
# procédure générique d'ouverture de session pour
# une liaison SLIP.  sliplogin l'appelle avec les paramètres:
#     1         2    3         4              5           6     7-n
# interface vitesse nom adresse-locale adresse-distante masque arg-optionnels
#
/sbin/ifconfig sl$1 inet $4 $5 netmask $6
# répondre aux requêtes ARP concernant le client SLIP avec notre
# adresse Ethernet
/usr/sbin/arp -s $5 00:11:22:33:44:55 pub
```

La ligne supplémentaire dans ce fichier slip.login, `arp -s $5 00:11:22:33:44:55 pub`, crée une entrée ARP dans la table ARP du serveur SLIP. Cette entrée ARP fait que le serveur SLIP répond avec sa propre adresse MAC lorsqu'un autre noeud IP du réseau Ethernet demande à dialoguer avec le client SLIP qui possède cette adresse IP.

Dans l'exemple donné ci-dessus, remplacez l'adresse MAC Ethernet (`00:11:22:33:44:55`) avec l'adresse MAC de la carte Ethernet de votre système, ou sinon votre "proxy ARP" ne fonctionnera jamais! Vous pouvez déterminer l'adresse MAC de votre serveur SLIP en examinant le résultat de la commande `netstat -i`; la seconde ligne doit ressembler à ce qui suit:

```
ed0   1500  Link0.2.c1.28.5f.4a         191923  0   129457     0   116
```

Cela indique que l'adresse MAC Ethernet de ce système est `00:02:c1:28:5f:4a` - les points dans les adresses MAC que donne `netstat -i` doivent être remplacés par des ":" et il faut ajouter un zéro devant chaque valeur hexadécimale donnée sur un seul digit pour obtenir des adresses dans le format requis par arp(8); consultez la page de manuel d'arp(8) pour avoir des informations complètes sur ces conventions.

Quand vous créez les fichiers /etc/sliphome/slip.login et /etc/sliphome/slip.logout, le bit "exécutable" (i.e., `chmod 755 /etc/sliphome/slip.login /etc/sliphome/slip.logout`) doit être positionné, ou sinon `sliplogin` sera incapable d'exécuter la procédure.

29.6.2.4.3. Configuration de slip.logout

/etc/sliphome/slip.logout n'est pas strictement indispensable (à moins que vous n'implémentiez un

"proxy ARP"), mais si vous décidez de la créer, voici un exemple de procédure slip.logout élémentaire:

```
#!/bin/sh -
#
#       slip.logout

#
# procédure générique de fermeture de session pour
# une liaison SLIP.  sliplogin l'appelle avec les paramètres:
#     1         2    3         4              5           6     7-n
# interface vitesse nom adresse-locale adresse-distante masque arg-optionnels
#
/sbin/ifconfig sl$1 down
```

Si vous utilisez la méthode "proxy ARP", vous voudrez que /etc/sliphome/slip.logout supprime l'entrée ARP pour le client SLIP:

```
#!/bin/sh -
#
#       @(#)slip.logout

#
# procédure générique de fermeture de session pour
# une liaison SLIP.  sliplogin l'appelle avec les paramètres:
#     1         2    3         4              5           6     7-n
# interface vitesse nom adresse-locale adresse-distante masque arg-optionnels
#
/sbin/ifconfig sl$1 down
# Cesser de répondre aux requêtes ARP concernant le client SLIP
/usr/sbin/arp -d $5
```

La commande `arp -d $5` supprime l'entrée ARP que la procédure slip.login pour le "proxy ARP" a ajouté quand le client SLIP a ouvert la session.

Il n'est pas inutile de répéter: assurez-vous que le bit "exécutable" de la procédure /etc/sliphome/slip.logout a été positionné après que vous l'ayez créée (i.e., `chmod 755 /etc/sliphome/slip.logout`).

29.6.2.5. A propos du routage

Si vous n'utilisez pas "proxy ARP" pour router les paquets entre vos clients SLIP et le reste de votre réseau (et peut-être l'Internet), vous devrez probablement ajouter des routes statiques vers le(s) routeur(s) par défaut le(s) plus proche(s) pour router le sous-réseau de vos clients SLIP via votre serveur SLIP.

29.6.2.5.1. Routes statiques

Ajouter des routes statiques vers vos routeurs les plus proches peut être problématique (voire impossible si vous n'avez pas les autorisations pour...). Si vous avez un réseau avec plusieurs routeurs, certains d'entre eux, tels que les Cisco et les Proteon, devront non seulement être configurés pour la route statique vers le sous-réseau SLIP, mais devront aussi savoir quelles routes statiques ils doivent annoncer aux autres routeurs, donc quelques compétences, un peu de dépannage ou de "bidouille" pourront être nécessaire pour que vos routes statiques fonctionnent.

29.6.2.5.2. Utiliser GateD®

GateD® est désormais un logiciel propriétaire et les sources ne seront donc plus disponibles (plus d'information sur le site Web de GateD®). Cette section existe uniquement pour des raisons de compatibilité pour ceux qui utilisent encore une ancienne version.

Une alternative aux maux de tête que provoquent les routes statiques est d'installer GateD® sur votre serveur SLIP FreeBSD et de le configurer pour qu'il utilise les protocoles de routage appropriés (RIP/OSPF/BGP/EGP) pour annoncer aux autres routeurs votre sous-réseau SLIP. Vous aurez besoin de créer un fichier /etc/gated.conf pour configurer GateD®; voici un exemple, semblable à celui que l'auteur a utilisé sur un serveur SLIP FreeBSD:

```
#
# fichier de configuration de gated dc.dsu.edu; pour la version
# 3.5alpha5
# diffusion des informations RIP pour xxx.xxx.yy via l'interface
# Ethernet "ed"
#
#
# options de trace
#
traceoptions "/var/tmp/gated.output" replace size 100k files 2 general ;

rip yes {
  interface sl noripout noripin ;
  interface ed ripin ripout version 1 ;
  traceoptions route ;
} ;

#
# Activer un certain nombre d'informations de trace sur l'interface
# au noyau:
kernel {
  traceoptions remnants request routes info interface ;
} ;

#
# Propager la route vers xxx.xxx.yy via l'Ethernet interface et RIP
#
```

```
export proto rip interface ed {
  proto direct {
      xxx.xxx.yy mask 255.255.252.0 metric 1; # SLIP connections
  } ;
} ;

#
# Accepter les routes de RIP via les interfaces Ethernet "ed"

import proto rip interface ed {
  all ;
} ;
```

L'exemple de fichier gated.conf ci-dessus diffuse l'information de routage concernant le sous-réseau SLIP *xxx.xxx.yy* via RIP sur l'interface Ethernet; si vous utilisez un pilote de périphérique Ethernet différent du pilote ed, vous devrez modifier en conséquence les références à l'interface ed. Ce fichier d'exemple active également les journaux sur /var/tmp/gated.output pour pouvoir déboguer le fonctionnement de GateD®; vous pouvez désactiver ces options de trace si GateD® fonctionne correctement pour vous. Vous devrez remplacer *xxx.xxx.yy* par l'adresse réseau de votre propre sous-réseau SLIP (assurez-vous de remplacer également le masque de sous-réseau dans la clause `proto direct`).

Une fois que vous avez installé et configuré GateD® sur votre système, vous devrez indiquer aux procédures de démarrage de FreeBSD de lancer GateD® à la place de routed. La manière la plus simple de faire cela est de positionner les variables `router` et `router_flags` dans le fichier /etc/rc.conf. Veuillez consulter la page de manuel de GateD® pour des informations sur les paramètres en ligne de commande.

Chapitre 30. Courrier électronique

30.1. Synopsis

Le "courrier électronique", plus connu sous le nom d'email, est une des formes de communication les plus utilisées aujourd'hui. Ce chapitre fournit une introduction sur comment faire fonctionner un serveur de courrier électronique sous FreeBSD, et comment envoyer et recevoir du courrier électronique sous FreeBSD. Cependant, cela n'est pas un document de référence, en fait de nombreux éléments importants ont été omis. Pour une couverture plus complète du sujet, le lecteur doit se référer aux nombreux ouvrages excellents listés dans l'Bibliographie.

Après la lecture de ce chapitre, vous connaîtrez:

- Quels composants logiciel sont impliqués dans l'envoi et la réception du courrier électronique.
- Où se trouvent sous FreeBSD les fichiers de configuration de base de sendmail.
- La différence entre boîtes aux lettres distantes et boîtes aux lettres locale.
- Comment empêcher les personnes à l'origine de courriers non sollicités (spam) d'utiliser votre serveur de courrier comme relais.
- Comment installer et configurer un agent de transfert de courrier alternatif sur votre système, en remplacement de sendmail.
- Comment dépanner les problèmes courants des serveurs de courrier électronique.
- Comment utiliser le protocole SMTP avec UUCP.
- Comment utiliser le courrier électronique avec une connexion temporaire.
- Comment configurer l'authentification SMTP pour une sécurité accrue.
- Comment installer et utiliser un client de messagerie, comme mutt pour envoyer et lire du courrier électronique.
- Comme récupérer votre courrier électronique à partir d'un serveur POP ou IMAP distant.
- Comment appliquer automatiquement des règles de filtrage au courrier entrant.

Avant de lire ce chapitre, vous devrez:

- Configurer correctement votre connexion réseau (Administration réseau avancée).
- Configurer correctement les informations DNS pour votre serveur de courrier (Administration réseau avancée).
- Savoir comment installer des logiciels tiers (Installer des applications. les logiciels pré-compilés et les logiciels portés).

30.2. Utilisation du courrier électronique

Il y a cinq éléments majeurs impliqués dans un échange de courrier. Ce sont: le programme utilisateur, le "daemon" serveur de courrier, le serveur DNS, une boîte aux lettres distante ou locale, et bien sûr le le serveur de courrier lui-même .

30.2.1. Le programme utilisateur

Cela inclut des programmes en ligne de commande comme mutt, pine, elm, et mail, et des programmes graphiques comme balsa, xfmail pour juste en nommer quelques-uns, ou quelque chose de plus "sophisticated" comme un navigateur WWW. Ces programmes transmettent simplement toutes les transactions concernant le courrier électronique au serveur de courrier local, soit en invoquant un des "daemons" serveurs (Agents de transfert de courrier) disponibles, soit via TCP.

30.2.2. Le "daemon" serveur de courrier

FreeBSD est fourni par défaut avec sendmail, mais supporte également de nombreux autres "daemons" serveurs de courrier, parmi lesquels:

- exim;
- postfix;
- qmail.

Le serveur a généralement deux fonctions-il est responsable de la réception du courrier comme celle de son envoi. Il n'est cependant *pas* responsable de la récupération du courrier électronique en utilisant des protocoles comme POP ou IMAP pour lire votre courrier, il ne vous permet pas non plus la connexion à des boîtes aux lettres locales de type mbox ou maildir. Vous avez besoin d'un "daemon" supplémentaire pour cela.

Les anciennes version de sendmail ont de sérieux problèmes de sécurité qui peuvent avoir pour conséquence l'obtention d'un accès local et/ou à distance à votre machine pour une personne malveillante. Vérifiez que vous utilisez une version à jour pour éviter de tels problèmes. Vous avez cependant toujours la possibilité d'installer un autre MTA à partir du catalogue des logiciels portés de FreeBSD.

30.2.3. Courrier électronique et DNS

Le système de noms de domaines (DNS) et son "daemon" `named` jouent un rôle important dans la transmission du courrier électronique. Afin de délivrer du courrier de votre site à un autre, le serveur recherchera le site distant dans la base de données DNS pour déterminer la machine qui recevra le courrier électronique pour le destinataire. Ce processus intervient également quand un courrier électronique est envoyé à partir d'une machine distante vers votre serveur de courrier.

Le DNS gère la correspondance entre nom de machine et adresse IP, et le stockage des informations spécifiques à la distribution du courrier électronique, connues sous le nom d'enregistrements MX. L'enregistrement MX ("Mail eXchanger") définit la machine, ou les machines, qui recevra le courrier pour un domaine particulier. Si vous n'avez pas d'enregistrement MX pour votre machine ou votre domaine, le courrier sera directement envoyé à votre machine à condition que vous ayez un enregistrement A faisant correspondre à votre nom de machine votre adresse IP.

Vous pouvez obtenir les enregistrements MX pour n'importe quel domaine en utilisant la commande host(1) est présentée ci-dessous:

```
% host -t mx FreeBSD.org
FreeBSD.org mail is handled (pri=10) by mx1.FreeBSD.org
```

30.2.4. Réception de courrier

La réception du courrier pour votre domaine se fait par le serveur de courrier. Il collectera le courrier qui est envoyé à destination de votre domaine et le stockera soit sous le format mbox (la méthode par défaut de stockage du courrier électronique) ou le format Maildir, en fonction de votre configuration. Une fois le courrier stocké, il peut être lu localement en utilisant des applications comme mail(1) ou mutt, ou lu à distance et récupéré en utilisant des protocoles tels que POP ou IMAP. Cela signifie que si vous désirez uniquement lire votre courrier électroniquement en local, vous n'avez pas besoin d'installer un serveur POP ou IMAP.

30.2.4.1. Accès aux boîtes aux lettres distantes en utilisant POP et IMAP

Pour accéder à des boîtes aux lettres distantes, vous devez avoir un accès à un serveur POP ou IMAP. Ces protocoles permettent aux utilisateurs de se connecter aisément à leurs boîtes aux lettres à partir de machines distantes. Bien que POP et IMAP permettent, tous les deux, l'accès aux boîtes aux lettres pour les utilisateurs, IMAP offre de nombreux avantages, parmi lesquels:

- IMAP peut stocker les messages sur un serveur distant et les récupérer.
- IMAP supporte les mises à jour concourantes.
- IMAP peut être extrêmement utile pour les connexions lentes car il permet aux utilisateurs de récupérer la structure des messages sans les télécharger. Il peut également effectuer des tâches comme la recherche sur le serveur pour réduire les transferts de données entre clients et serveurs.

Pour installer un serveur POP ou IMAP, les étapes suivantes doivent être suivies:

1. Choisissez un serveur IMAP ou POP correspondant à vos besoins. Les serveurs POP et IMAP suivants sont connus et sont de bons exemples:
   - qpopper;
   - teapop;
   - imap-uw;
   - courier-imap;
2. Installez le "daemon" POP ou IMAP de votre choix à partir du catalogue des logiciels portés.
3. Si cela est nécessaire, modifiez le fichier /etc/inetd.conf pour charger le serveur POP ou IMAP.

Il doit être noté que POP et IMAP transmettent les données, y compris les noms d'utilisateurs et mot de passe d'authentification en clair. Cela signifie que si vous désirez sécuriser la transmission des données avec ces protocoles, vous devriez considérer l'utilisation de de tunnels ssh(1). L'utilisation de tels tunnels est décrite

> dans la Tunnels SSH.

30.2.4.2. Accès aux boîtes aux lettres locales

Les boîtes aux lettres peuvent être accessibles localement en utilisant un client de messagerie sur le serveur où se trouve la boîte. Cela peut être fait en employant des applications telles que mutt ou mail(1).

30.2.5. Le serveur de courrier

Le serveur de courrier est le nom donné au serveur qui est responsable de la transmission et la réception du courrier pour votre machine, et probablement votre réseau.

30.3. Configuration de sendmail

sendmail(8) est l'agent de transfert de courrier (Mail Transfert Agent-MTA) par défaut sous FreeBSD. Le rôle de sendmail est d'accepter le courrier en provenance des agents de courrier utilisateur (Mail User Agents-MUA) et de délivrer le courrier aux programmes de gestion du courrier définis dans son fichier de configuration. sendmail peut également accepter les connexions réseau et délivrer le courrier dans des boîtes aux lettres locales ou le transmettre à un autre programme.

sendmail utilise les fichiers de configuration suivants:

Fichier	Fonction
/etc/mail/access	Fichier de la base de données d'accès de sendmail
/etc/mail/aliases	Alias de boîte aux lettres
/etc/mail/local-host-names	Liste des machines pour lesquelles sendmail accepte du courrier
/etc/mail/mailer.conf	Configuration du programme de gestion du courrier
/etc/mail/mailertable	Table de livraison du courrier
/etc/mail/sendmail.cf	Fichier de configuration principal de sendmail
/etc/mail/virtusertable	Table des domaines et utilisateurs virtuels

30.3.1. /etc/mail/access

La base de données d'accès définit quelle(s) machine(s) ou adresses IP ont accès au serveur de courrier local et quel type d'accès ils ont. Les machines peuvent être listées avec `OK`, `REJECT`, `RELAY` ou simplement transférées à la routine de gestion des erreurs sendmail avec une erreur donnée. Les machines qui sont listées avec `OK`, qui est le comportement par défaut, sont autorisées à envoyer du courrier à cette machine dès que la destination finale du courrier est la machine locale. Les machines listées avec `REJECT` se verront rejeter pour toute connexion au serveur. Les machines présentes avec l'option `RELAY` sont autorisées à envoyer du courrier à n'importe quelle destination

par l'intermédiaire de ce serveur de courrier.

Exemple 37. Configuration de la base de données d'accès de sendmail

```
cyberspammer.com                550 We don't accept mail from spammers
FREE.STEALTH.MAILER@            550 We don't accept mail from spammers
another.source.of.spam          REJECT
okay.cyberspammer.com           OK
128.32                          RELAY
```

Dans cet exemple nous avons cinq entrées. Les émetteurs de courrier qui correspondent à la partie gauche de la table sont affectés par l'action donnée sur la partie droite de la table. Les deux premiers exemples donnent un code d'erreur à la routine de gestion d'erreur de sendmail. Le message est affiché sur la machine distante quand un courrier électronique correspond à la partie gauche de la table. L'entrée suivante rejette le courrier en provenance d'une machine précise de l'Internet, `another.source.of.spam`. L'entrée suivante accepte les connexions à partir de la machine `okay.cyberspammer.com`, qui est plus précis que le `cyberspammer.com` de la ligne précédente. Les correspondances plus spécifiques priment sur les moins précises. La dernière entrée autorise le relais du courrier électronique en provenance de machines avec une adresse IP qui commence par `128.32`. Ces machines seront en mesure d'envoyer du courrier destiné à d'autres serveurs de courrier par l'intermédiaire de ce serveur de courrier.

Quand ce fichier est mis à jour, vous devez exécuter la commande `make` dans /etc/mail/ pour mettre à jour la base de données.

30.3.2. /etc/mail/aliases

La base de données d'alias contient une liste de boîtes aux lettres virtuelles dont le contenu sera transmis à d'autres utilisateurs, fichiers, programmes ou d'autres alias. Voici quelques exemples qui peuvent être utilisés dans /etc/mail/aliases:

Exemple 38. Exemple de base de données d'alias

```
root: localuser
ftp-bugs: joe,eric,paul
bit.bucket:  /dev/null
procmail: "|/usr/local/bin/procmail"
```

Le format du fichier est simple; le nom de la boîte aux lettres à gauche et la cible sur la droite. Le premier exemple transfère la boîte aux lettres `root` vers la boîte aux lettres `localuser`, qui est ensuite recherchée dans la base de données d'alias. Si aucune correspondance n'est trouvée alors le message est délivré à l'utilisateur locale `localuser`. L'exemple suivant montre une liste de correspondance. Un courrier envoyé à la boîte aux lettres `ftp-bugs` sera délivré aux trois boites locales `joe`, `eric`, et `paul`. Notez qu'une boîte aux lettres distante comme `user@exemple.com`/procmail pourra être spécifiée. L'exemple suivant montre comment transférer le courrier dans un fichier,

dans notre cas /dev/null. Le dernier exemple montre l'envoi du courrier à un programme, dans le cas présent le message est écrit sur l'entrée standard de /usr/local/bin/procmail par l'intermédiaire d'un tube UNIX®.

Quand ce fichier est mis à jour, vous devez exécuter la commande `make` dans /etc/mail/ pour mettre à jour la base de données.

30.3.3. /etc/mail/local-host-names

C'est la liste des machines pour lesquelles sendmail(8) accepte du courrier comme s'il était destiné à la machine locale. Placez-y tous les domaines ou machines pour lesquels sendmail doit recevoir du courrier. Par exemple, si le serveur de courrier devait accepter du courrier pour le domaine `exemple.com` et la machine `mail.exemple.com`, sont local-host-names ressemblera à quelque chose comme ceci:

```
exemple.com
mail.exemple.com
```

Quand ce fichier est mis à jour, sendmail(8) doit être relancé pour lire les changements.

30.3.4. /etc/mail/sendmail.cf

Fichier principal de configuration de sendmail, sendmail.cf contrôle le comportement général de sendmail, y compris tout depuis la réécriture des adresses de courrier jusqu'à l'envoi de message de rejet aux serveurs de courrier distants. Naturellement, avec tant de différentes activités, ce fichier de configuration est relativement complexe et son étude détaillée n'est pas le but de cette section. Heureusement, ce fichier a rarement besoin d'être modifié pour les serveurs de courrier standards.

Le fichier de configuration principal de sendmail peut être créé à partir de macros m4(1) qui définissent les fonctions et le comportement de sendmail. Veuillez consulter /usr/src/contrib/sendmail/cf/README pour plus de détails.

Quand des modifications à ce fichier sont apportées, sendmail doit être redémarré pour que les changements prennent effet.

30.3.5. /etc/mail/virtusertable

La table virtusertable fait correspondre les adresses de courrier électronique pour des domaines virtuels et les boîtes aux lettres avec des boîtes aux lettres réelles. Ces boîtes aux lettres peuvent être locales, distantes, des alias définis dans /etc/mail/aliases ou des fichiers.

Exemple 39. Exemple de correspondance de domaine virtuel de courrier

```
root@exemple.com                root
postmaster@exemple.com          postmaster@noc.exemple.net
@exemple.com                    joe
```

Dans l'exemple ci-dessus, nous avons une correspondance pour un domaine `exemple.com`. Ce fichier est traité jusqu'à trouver la première correspondance. Le premier élément fait correspondre `root@exemple.com` à la boîte aux lettres root locale. L'entrée suivante fait correspondre `postmaster@exemple.com` à la boîte aux lettres postmaster sur la machine `noc.exemple.net`. Et enfin, si un courrier en provenance de `exemple.com` n'a pas trouvé de correspondance, il correspondra à la dernière ligne, qui régira tous les autres messages adressés à quelqu'un du domaine `exemple.com`. La correspondance sera la boîte aux lettres locale `joe`.

30.4. Changer votre agent de transfert de courrier

Comme mentionné précédemment, FreeBSD est fournit avec sendmail comme agent de transfert du courrier (MTA - Mail Transfert Agent). Il est donc par défaut en charge de votre courrier sortant et entrant.

Cependant, pour une variété de raison, certains administrateurs système désirent changer le MTA de leur système. Ces raisons vont de la simple envie d'essayer un autre agent au besoin d'une fonction ou ensemble spécifique qui dépend d'un autre gestionnaire de courrier. Heureusement, quelle qu'en soit la raison, FreeBSD rend le changement aisé.

30.4.1. Installer un nouveau MTA

Vous avez un vaste choix d'agent disponible. Un bon point de départ est le catalogue des logiciels portés de FreeBSD où vous pourrez en trouver un grand nombre. Bien évidemment vous êtes libres d'utiliser n'importe quel agent de n'importe quelle origine, dès que vous pouvez le faire fonctionner sous FreeBSD.

Commencez par installer votre nouvel agent. Une fois ce dernier installé, il vous donne une chance de décider s'il remplit vraiment vos besoins, et vous donne l'opportunité de configurer votre nouveau logiciel avant de remplacer sendmail. Quand vous faites cela, vous devez être sûr que l'installation du nouveau logiciel ne tentera pas de remplacer des binaires du système comme /usr/bin/sendmail. Sinon, votre nouveau logiciel sera mis en service avant d'avoir pu le configurer.

Veuillez vous référer à la documentation de l'agent choisi pour de l'information sur comment configurer le logiciel que vous avez choisi.

30.4.2. Désactiver sendmail

La procédure utilisée pour lancer sendmail a changé de façon significative entre la 4.5-RELEASE et la 4.6-RELEASE. Par conséquent, la procédure utilisée pour la désactiver est légèrement différente.

30.4.2.1. FreeBSD 4.5-STABLE d'avant le 2002/4/4 et plus ancienne (y compris 4.5-RELEASE et précédentes)

Ajoutez:

```
sendmail_enable="NO"
```

dans /etc/rc.conf. Cela désactivera le service de courrier entrant de sendmail mais si

/etc/mail/mailer.conf (voir plus bas) n'est pas modifié, sendmail sera toujours utilisé pour envoyer du courrier électronique.

30.4.2.2. FreeBSD 4.5-STABLE d'après le 2002/4/4 (y compris 4.6-RELEASE et suivantes)

Afin de complètement désactiver sendmail vous devez utiliser

```
sendmail_enable="NONE"
```

dans /etc/rc.conf.

Si vous désactivez le service d'envoi de courrier de sendmail de cette manière, il est important que vous le remplaciez par un système de courrier alternatif fonctionnant parfaitement. Si vous choisissez de ne pas le faire, des fonctions du système comme periodic(8) ne seront pas en mesure de délivrer leur résultat par courrier électronique comme elles s'attendent normalement à le faire. De nombreux composants de votre système s'attendent à avoir un système compatible à sendmail en fonctionnement. Si des applications continuent à utiliser les binaires de sendmail pour essayer d'envoyer du courrier électronique après la désactivation, le courrier pourra aller dans une file d'attente inactive, et pourra n'être jamais livré.

Si vous voulez uniquement désactiver le service de réception de courrier de sendmail vous devriez fixer

```
sendmail_enable="NO"
```

dans /etc/rc.conf. Plus d'information sur les options de démarrage de sendmail est disponible à partir de la page de manuel de rc.sendmail(8).

30.4.3. Lancement de votre nouvel agent au démarrage

Vous pourrez avoir le choix entre deux méthodes pour lancer votre nouvel agent au démarrage, encore une fois en fonction de la version de FreeBSD dont vous disposez.

30.4.3.1. FreeBSD 4.5-STABLE d'avant le 2002/4/11 (y compris 4.5-RELEASE et précédentes)

Ajouter une procédure dans /usr/local/etc/rc.d/ qui se termine en .sh et qui est exécutable par `root`. La procédure devrait accepter les paramètres `start` et `stop`. Au moment du démarrage les procédures système exécuteront la commande

```
/usr/local/etc/rc.d/supermailer.sh start
```

que vous pouvez également utiliser pour démarrer le serveur. Au moment de l'arrêt du système, les procédures système utiliseront l'option `stop` en exécutant la commande

```
/usr/local/etc/rc.d/supermailer.sh stop
```

que vous pouvez également utiliser manuellement pour arrêter le serveur quand le système est en fonctionnement.

30.4.3.2. FreeBSD 4.5-STABLE d'après le 2002/4/11 (y compris 4.6-RELEASE et suivantes)

Avec les versions suivantes de FreeBSD, vous pouvez utiliser la méthode ci-dessus ou fixer

```
mta_start_script="nomfichier"
```

dans /etc/rc.conf, où *nomfichier* est le nom d'une procédure que vous voulez exécuter au démarrage pour lancer votre agent.

30.4.4. Remplacer sendmail comme gestionnaire du courrier du système par défaut

Le programme sendmail est tellement omniprésent comme logiciel standard sur les systèmes UNIX® que certains programmes supposent qu'il est tout simplement déjà installé et configuré. Pour cette raison, de nombreux agents alternatifs fournissent leur propre implémentation compatible avec l'interface en ligne de commande de sendmail; cela facilite leur utilisation comme remplaçant pour sendmail.

Donc, si vous utilisez un programme alternatif, vous devrez vérifier que le logiciel essayant d'exécuter les binaires standards de sendmail comme /usr/bin/sendmail exécute réellement l'agent que vous avez choisi à la place. Heureusement, FreeBSD fournit un système appelé mailwrapper(8) qui remplit ce travail pour vous.

Quand sendmail fonctionne tel qu'il a été installé, vous trouverez quelque chose comme ce qui suit dans /etc/mail/mailer.conf:

```
sendmail     /usr/libexec/sendmail/sendmail
send-mail   /usr/libexec/sendmail/sendmail
mailq       /usr/libexec/sendmail/sendmail
newaliases  /usr/libexec/sendmail/sendmail
hoststat    /usr/libexec/sendmail/sendmail
purgestat   /usr/libexec/sendmail/sendmail
```

Cela signifie que lorsque l'une des commandes courantes (comme sendmail lui-même) est lancée, le système invoque en fait une copie de "mailwrapper" appelée sendmail, qui lit mailer.conf et exécute /usr/libexec/sendmail/sendmail à la place. Ce système rend aisé le changement des binaires qui sont réellement exécutés quand les fonctions de sendmail par défaut sont invoquées.

Donc si vous avez voulu que /usr/local/supermailer/bin/sendmail-compat soit lancé en place de sendmail, vous pourrez modifier /etc/mail/mailer.conf de cette façon:

```
sendmail     /usr/local/supermailer/bin/sendmail-compat
send-mail   /usr/local/supermailer/bin/sendmail-compat
mailq       /usr/local/supermailer/bin/mailq-compat
newaliases  /usr/local/supermailer/bin/newaliases-compat
hoststat    /usr/local/supermailer/bin/hoststat-compat
purgestat   /usr/local/supermailer/bin/purgestat-compat
```

30.4.5. Pour en terminer

Une fois que vous avez tout configuré de la façon dont vous le désirez, vous devriez soit tuer les processus de sendmail dont vous n'avez plus besoin et lancer les processus appartenant à votre nouveau logiciel, ou tout simplement redémarrer. Le redémarrage vous donnera l'opportunité de vous assurer que vous avez correctement configuré votre système pour le lancement automatique de votre nouvel agent au démarrage.

30.5. Dépannage

30.5.1. Pourquoi faut-il que j'utilise le FQDN ("Fully Qualified Domain Name" - nom complet de machine) pour les machines de mon site?

Vous vous rendrez probablement compte que la machine est en fait dans un domaine différent; par exemple, si vous êtes dans le domaine `foo.bar.edu` et que vous voulez atteindre la machine `mumble` du domaine `bar.edu`, vous devrez utiliser son nom de machine complet, `mumble.bar.edu`, au lieu de juste `mumble`.

C'était traditionnellement autorisé par les résolveurs BIND BSD. Néanmoins, la version de BIND qui est maintenant livrée avec FreeBSD ne sait pas compléter les noms de machines abrégés autrement qu'avec le nom de votre domaine. Donc le nom non qualifié `mumble` doit correspondre à `mumble.foo.bar.edu`, sans quoi il sera recherché dans le domaine racine.

Cela diffère du comportement précédent, où la recherche se prolongeait à `mumble.bar.edu`, puis `mumble.edu`. Consultez la RFC 1535 pour savoir pourquoi cela était considéré comme une mauvaise pratique, voire même un trou de sécurité.

Comme solution, vous pouvez mettre la ligne:

```
search foo.bar.edu bar.edu
```

à la place de:

```
domain foo.bar.edu
```

dans votre fichier /etc/resolv.conf. Cependant, assurez-vous que la recherche ne franchit pas la "limite entre l'administration locale et publique", selon l'expression de la RFC 1535.

30.5.2. sendmail affiche le message mail loops back to myself

La réponse donnée dans la FAQ de sendmail est la suivante:

```
J'obtiens les messages d'erreur suivant:

553 MX list for domain.net points back to relay.domain.net
554 user@domain.net... Local configuration error

Comment puis-je résoudre ce problème?

Vous avez demandé que le courrier pour un domaine (e.g., domain.net)
soit transmis à une machine donnée (dans ce cas précis, relay.domain.net)
en utilisant un enregistrement MXMX record
, mais la machine relais ne se
connaît pas elle-même comme domain.net.  Ajoutez domain.net à
/etc/mail/local-host-names [connu sous le nom /etc/sendmail.cw dans les
versionsantérieure à 8.10] (si vous utilisez FEATURE(use_cw_file))
ou ajoutez "Cw domain.net" à
/etc/mail/sendmail.cf.
```

La FAQ de sendmail peut être trouvée à l'adresse http://www.sendmail.org/faq/ et sa lecture est recommandée si vous voulez "bidouiller" votre configuration du courrier électronique.

30.5.3. Comment puis-je faire tourner un serveur de courrier électronique avec une connexion téléphonique PPP PPP

Vous voulez connecter une machine FreeBSD du réseau local à l'Internet. Cette machine servira de passerelle de courrier électronique pour le réseau local. La connexion PPP n'est pas dédiée.

Il y a au moins deux façons de faire. L'une d'elle est d'utiliser UUCP.

L'autre méthode étant d'obtenir un serveur Internet constamment connecté pour qu'il vous fournisse les services MX pour votre domaine. Par exemple, si le domaine de votre compagnie est `exemple.com` et votre fournisseur d'accès a configuré `exemple.net` pour fournir un MX secondaire pour votre domaine:

```
exemple.com.            MX        10      exemple.com.
                       MX        20      exemple.net.
```

Une seule machine devrait être spécifiée comme destinataire final (ajoutez `Cw exemple.com` au fichier /etc/mail/sendmail.cf de `exemple.com`).

Quand le `sendmail` expéditeur tente de vous délivrer du courrier, il essaiera de se connecter à votre serveur (`exemple.com`) via votre liaison par modem. Ce qui échouera très probablement par dépassement de délai puisque vous n'êtes pas en ligne. Le programme sendmail enverra automatiquement le courrier au site MX secondaire, i.e. votre fournisseur d'accès (`exemple.net`). Le site MX secondaire essayera périodiquement de se connecter à votre machine pour expédier le

courrier au site MX primaire (`exemple.com`).

Vous pourrez vouloir utiliser quelque chose comme ceci comme procédure de connexion:

```
#!/bin/sh
# Mettez-moi dans /usr/local/bin/pppmyisp
( sleep 60 ; /usr/sbin/sendmail -q )
/usr/sbin/ppp -direct pppmyisp
```

Si vous avez l'intention de définir une procédure de connexion particulière pour un utilisateur, vous pourrez utiliser `sendmail -qRexemple.com` à la place de la procédure ci-dessus. Cela forcera le traitement immédiat de tout le courrier dans votre file d'attente pour `exemple.com`.

On peut encore affiner la configuration comme suit:

Message emprunté à la liste de diffusion pour les fournisseurs d'accès Internet utilisant FreeBSD.

```
 Nous fournissons un MX secondaire à un
client.  Le client se connecte
 à notre service automatiquement plusieurs fois par jour pour acheminer
 le courrier sur son MX primaire (nous n'appelons pas son site lorsque
 du courrier pour ses domaines arrive).  Notre sendmail envoie le courrier de la
 file d'attente toutes les demi-heures.  Pour l'instant, il doit rester
 une demi-heure en ligne pour être sûr que tout le courrier soit
 arrivé au MX primaire.

 Y-a-t-il une commande qui permette de dire à sendmail d'envoyer
 sur-le-champ tout le courrier? L'utilisateur n'a évidemment pas
 les droits super-utilisateur sur la machine.

Dans la section "privacy flags" (indicateurs de
confidentialité) de sendmail.cf, il y a la définition Opgoaway,restrictqrun

Supprimer restrictqrun permet à d'autres utilisateurs que le
super-utilisateur de lancer le traitement de la file d'attente.  Vous
pouvez aussi redéfinir les MXs.  Nous sommes le premier MX pour les
utilisateurs de ce type, et nous avons défini:

# Si nous sommes le meilleur MX pour une machine, essayer directement
# au lieu d'émettre des messages d'erreur de configuration locale.
OwTrue

De cette façon, un site distant vous enverra directement le courrier,
sans essayer de se connecter chez votre client.  Vous le lui
transmettez ensuite.  Cela ne marche qu'avec les "machines",
votre client doit nommer son serveur de courrier
"client.com" aussi bien que
"machine.client.com" dans le DNS.  Mettez seulement un
enregistrement A pour "client.com".
```

30.5.4. Pourquoi j'obtiens le message d'erreur Relaying Denied à chaque fois que j'envoie du courrier à partir d'autres machines?

Dans l'installation par défaut de FreeBSD, sendmail est configuré pour envoyer du courrier uniquement à partir de la machine sur laquelle il tourne. Par exemple, si un serveur POP est disponible, alors les utilisateurs pourront retirer leur courrier depuis l'école, le travail, ou toute autre machine distante mais ils ne seront toujours pas en mesure d'envoyer du courrier électronique à partir de machines extérieures. Généralement, quelques instants après une tentative, un courrier électronique sera envoyé par le MAILER-DAEMON avec un message `5.7 Relaying Denied`.

Il y a plusieurs façons d'y remédier. La solution la plus directe est de mettre l'adresse de votre fournisseur d'accès dans un fichier de domaine à relayer /etc/mail/relay-domains. Une façon rapide de le faire serait:

```
# echo "votre.fai.exemple.com" > /etc/mail/relay-domains
```

Après avoir créé ou édité ce fichier vous devez redémarrer sendmail. Cela fonctionne parfaitement si vous êtes l'administrateur d'un serveur et vous ne désirez pas envoyer de courrier localement, ou que vous désiriez utiliser un système ou un client "clic-bouton" sur une autre machine ou un autre FAI. C'est également très utile si vous avez uniquement qu'un ou deux comptes de courrier électronique configurés. S'il y a un grand nombre d'adresses à ajouter, vous pouvez tout simplement ouvrir ce fichier dans votre éditeur de texte favori et ensuite ajouter les domaines, un par ligne:

```
votre.fai.exemple.com
autre.fai.exemple.net
utilisateurs-fai.exemple.org
www.exemple.org
```

Désormais tout courrier envoyé vers votre système, par n'importe quelle machine de cette liste (en supposant que l'utilisateur possède un compte sur votre système), sera accepté. C'est un bon moyen d'autoriser aux utilisateurs d'envoyer du courrier électronique à distance depuis votre système sans autoriser l'utilisation de votre système pour l'envoi de courrier électronique non sollicité (SPAM).

30.6. Sujets avancés

LA fonction suivante couvre des sujets plus avancés comme la configuration du courrier électronique pour l'intégralité de votre domaine.

30.6.1. Basic Configuration

Sans aucune configuration, vous devrez être en mesure d'envoyer du courrier électronique à des machines extérieures à partir du moment où vous avez configuré /etc/resolv.conf ou que vous avez votre propre serveur de noms. Si vous désirez que le courrier pour votre machine soit délivré au

serveur de courrier (e.g., sendmail) sur votre propre machine FreeBSD, il y a deux méthodes:

- Faites tourner votre propre serveur de noms et possédez votre propre domaine. Par exemple FreeBSD.org
- Faire délivrer le courrier directement sur votre machine. Cela est possible en délivrant directement le courrier à la machine sur lequel pointe le DNS pour le courrier qui vous est destiné. Par exemple exemple.FreeBSD.org.

Indépendamment de la méthode que vous choisissez, afin d'avoir le courrier délivré directement à votre machine, elle doit avoir une adresse IP statique permanente (et non pas une adresse dynamique, comme avec la plupart des connexions PPP par modem). Si vous êtes derrière un coupe-feu, il doit autoriser le trafic SMTP en votre direction. Si vous voulez recevoir directement le courrier sur votre machine, vous devez être sûrs de l'une de ces deux choses:

- Assurez-vous que l'enregistrement MX (le nombre le plus bas) de votre DNS pointe sur l'adresse IP de votre machine.
- Assurez-vous qu'il n'y a pas d'entrée MX pour votre machine dans votre DNS.

Une des deux conditions précédentes vous permettra de recevoir directement le courrier pour votre machine.

Essayez:

```
# hostname
exemple.FreeBSD.org
# host exemple.FreeBSD.org
exemple.FreeBSD.org has address 204.216.27.XX
```

Si c'est la réponse que vous obtenez, le courrier adressé à votreindentifiant@exemple.FreeBSD.org arrivera sans problème (en supposant que sendmail fonctionne correctement sur exemple.FreeBSD.org).

Si au lieu de cela vous obtenez quelque chose de similaire à ceci:

```
# host exemple.FreeBSD.org
exemple.FreeBSD.org has address 204.216.27.XX
exemple.FreeBSD.org mail is handled (pri=10) by hub.FreeBSD.org
```

Tout le courrier adressé à votre machine (exemple.FreeBSD.org) arrivera sur hub adressé au même utilisateur au lieu d'être directement envoyé à votre machine.

L'information précédente est gérée par votre serveur DNS. L'enregistrement du DNS qui contient l'information de routage de courrier est l'entrée MX (_M_ail e_X_change). S'il n'y pas d'enregistrement MX, le courrier sera directement envoyé à la machine en utilisant son adresse IP.

Voici ce que fut à un moment donné l'entrée MX pour freefall.FreeBSD.org:

```
freefall        MX  30  mail.crl.net
freefall        MX  40  agora.rdrop.com
freefall        MX  10  freefall.FreeBSD.org
freefall        MX  20  who.cdrom.com
```

Comme vous pouvez le voir, `freefall` avait plusieurs entrées MX. L'entrée MX dont le numéro est le plus bas est la machine qui reçoit directement le courrier si elle est disponible; si elle n'est pas accessible pour diverses raisons, les autres (parfois appelées "MX de secours") acceptent temporairement les messages, et les transmettent à une machine de numéro plus faible quand elle devient disponible, et par la suite à la machine de numéro le plus bas.

Les sites MX alternatifs devraient avoir une connexion Internet séparée de la votre afin d'être les plus utiles. Votre fournisseur d'accès ou tout autre site amical ne devrait pas avoir de problème pour vous fournir ce service.

30.6.2. Courrier pour votre domaine

Pour configurer un serveur de courrier vous devez faire en sorte que tout le courrier à destination des diverses stations de travail lui soit envoyé. Concrètement, vous voulez "revendiquer" tout courrier pour n'importe quelle machine de votre domaine (dans ce cas `*.FreeBSD.org`) et le détourner vers votre serveur de courrier de sorte que vos utilisateurs puissent recevoir leur courrier sur le serveur de courrier principal.

Pour rendre les choses plus aisées, un compte utilisateur avec le même *nom d'utilisateur* devrait exister sur les deux machines. Utilisez adduser(8) pour ce faire.

Le serveur de courrier que vous utiliserez sera défini comme "mail exchanger" pour chaque station de travail du réseau. Cela est fait dans votre configuration de DNS de cette manière:

```
exemple.FreeBSD.org A   204.216.27.XX       ; Station de travail
            MX  10 hub.FreeBSD.org  ; Serveur de courrier
```

Cela redirigera le courrier pour votre station de travail au serveur de courrier quelque soit la machine sur laquelle pointe l'enregistrement A. Le courrier est envoyé sur la machine MX.

Vous ne pouvez le faire vous-même que si vous gérez un serveur de noms. Si ce n'est pas le cas, ou que vous ne pouvez avoir votre propre serveur DNS, parlez-en à votre fournisseur d'accès ou à celui qui fournit votre DNS.

Si vous faites de l'hébergement virtuel du courrier électronique, l'information suivante sera utile. Pour cet exemple, nous supposerons que vous avez un client qui possède son propre domaine, dans notre cas `client1.org`, et vous voulez que tout le courrier pour `client1.org` arrive sur votre serveur de courrier, `mail.mamachine.com`. L'entrée dans votre DNS devrait ressembler à ceci:

```
client1.org     MX  10  mail.mamachine.com
```

Vous n'avez *pas* besoin d'un enregistrement A pour `client1.org` si vous ne voulez gérer que le courrier pour ce domaine.

Soyez conscient que "pinger" `client1.org` ne fonctionnera pas à moins qu'un enregistrement A existe pour cette machine.

La dernière chose que vous devez faire est d'indiquer à sendmail sur le serveur de courrier quels sont les domaines et/ou machines pour lesquels il devrait accepter du courrier. Il y a peu de façons différentes de le faire. L'une des deux méthodes suivantes devrait fonctionner:

- Ajoutez les machines à votre fichier /etc/mail/local-host-names si vous utilisez la fonction `FEATURE(use_cw_file)`. Si vous utilisez une version de sendmail antérieure à la version 8.10, le fichier sera /etc/sendmail.cw.
- Ajoutez une ligne `Cwyour.host.com` à votre fichier /etc/sendmail.cf ou /etc/mail/sendmail.cf si vous utilisez sendmail 8.10 ou supérieur.

30.7. SMTP avec UUCP

La configuration de sendmail fournie avec FreeBSD est conçue pour les sites directement connectés à l'Internet. Les sites désirant échanger leur courrier électronique par l'intermédiaire d'UUCP doivent installer un autre fichier de configuration pour sendmail.

Modifier manuellement le fichier /etc/mail/sendmail.cf est un sujet réservé aux spécialistes. Dans version 8 de sendmail la génération des fichiers de configuration se fait par l'intermédiaire du processeur m4(1), où la configuration se fait à un haut niveau d'abstraction. Les fichiers de configuration m4(1) se trouvent dans le répertoire /usr/src/usr.sbin/sendmail/cf.

Si vous n'avez pas installé toutes les sources du système, l'ensemble des fichiers de configuration de sendmail a été regroupé dans une archive séparée des autres sources. En supposant que vous avez monté votre CDROM FreeBSD contenant les sources, faites:

```
# cd /cdrom/src
# cat scontrib.?? | tar xzf - -C /usr/src/contrib/sendmail
```

Cette extraction ne donne lieu qu'à une centaine de kilo-octets. Le fichier README dans le répertoire cf pourra faire office d'une introduction à la configuration m4(1).

La meilleure façon d'ajouter le support UUCP est d'utiliser la fonctionnalité `mailertable`. Cela créé une base de données que sendmail utilise pour décider de la manière dont il va router le courrier électronique.

Tout d'abord, vous devez créer votre fichier .mc. Le répertoire /usr/src/usr.sbin/sendmail/cf/cf contient quelques exemples. En supposant que vous avez appelé votre fichier foo.mc, tout ce dont vous avez besoin de faire pour le convertir en un fichier sendmail.cf valide est:

```
# cd /usr/src/usr.sbin/sendmail/cf/cf
# make foo.cf
```

```
# cp foo.cf /etc/mail/sendmail.cf
```

Un fichier .mc classique devrait ressembler à ceci:

```
VERSIONID(`Votre numéro de version') OSTYPE(bsd4.4)

FEATURE(accept_unresolvable_domains)
FEATURE(nocanonify)
FEATURE(mailertable, `hash -o /etc/mail/mailertable')

define(`UUCP_RELAY', votre.relai.uucp)
define(`UUCP_MAX_SIZE', 200000)
define(`confDONT_PROBE_INTERFACES')

MAILER(local)
MAILER(smtp)
MAILER(uucp)

Cw    alias.de.votre.nom.de.machine
Cw    votrenomdenoeuduucp.UUCP
```

Les lignes contenant les directives `accept_unresolvable_domains`, `nocanonify`, et `confDONT_PROBE_INTERFACES` empêcheront l'utilisation du DNS lors de l'envoi du courrier électronique. La directive `UUCP_RELAY` est nécessaire pour le support de l'UUCP. Mettez juste un nom de machine Internet capable de gérer des adresses d'un pseudo-domaine .UUCP; la plupart du temps, vous mettrez le nom du serveur de messagerie de votre fournisseur d'accès.

Après avoir défini tout ceci, vous avez besoin d'un fichier /etc/mail/mailertable. Si vous n'avez qu'un seul lien avec l'extérieur qui est utilisé pour votre courrier électronique, le fichier suivant devrait suffire:

```
#
# makemap hash /etc/mail/mailertable.db  /etc/mail/mailertable
.                           uucp-dom:your.uucp.relay
```

Un exemple plus complexe ressemblerait à ceci:

```
#
# makemap hash /etc/mail/mailertable.db  /etc/mail/mailertable
#
horus.interface-business.de   uucp-dom:horus
.interface-business.de        uucp-dom:if-bus
interface-business.de         uucp-dom:if-bus
.heep.sax.de                  smtp8:%1
horus.UUCP                    uucp-dom:horus
if-bus.UUCP                   uucp-dom:if-bus
```

```
.                               uucp-dom:
```

Les trois premières lignes gèrent les cas spécifiques où les courriers électroniques pour l'extérieur ne devraient pas être envoyés au serveur par défaut, mais plutôt à des serveurs UUCP voisins afin de "raccourcir" le chemin à parcourir. La ligne suivante gère le courrier électronique destiné au domaine Ethernet local et qui peut être distribué en utilisant le protocole SMTP. Et enfin, les voisins UUCP sont mentionnés dans la notation de pseudo-domaine UUCP, pour permettre à un courrier du type `voisin-uucp !destinataire` de passer outre les règles par défaut. La dernière ligne doit toujours être un point, ce qui correspond à tout le reste, avec la distribution UUCP vers un voisin UUCP qui sert de passerelle universelle de courrier électronique vers le reste du monde. Tous les noms de noeuds placés après le mot clé `uucp-dom:` doivent être des noms valides de voisins UUCP, que vous pouvez vérifier en utilisant la commande `uuname`.

Pour vous rappeler que ce fichier doit être converti en un fichier de base de données DBM avant d'être utilisable. La ligne de commande pour accomplir cette conversion est rappelée dans les commentaires au début du fichier mailertable. Vous devez lancer cette commande à chaque fois que vous modifiez votre fichier mailertable.

Pour finir: si vous n'êtes pas certain du bon fonctionnement de certaines configurations de routage du courrier électronique, rappelez-vous de l'option `-bt` de sendmail. Cela lance sendmail dans le *mode test d'adresse*; entrez simplement `3,0`, suivi de l'adresse que vous désirez tester. La dernière ligne vous indiquera le type d'agent utilisé pour l'envoi, la machine de destination à laquelle l'agent doit envoyer le message, et l'adresse (peut-être traduite) à laquelle il l'enverra. Pour quitter ce mode tapez `Ctrl` + `D`.

```
% sendmail -bt
ADDRESS TEST MODE (ruleset 3 NOT automatically invoked)
Enter <ruleset> <address>
> 3,0 foo@example.com
canonify           input: foo @ example . com
...
parse            returns: $# uucp-dom $@ your.uucp.relay $: foo < @ example . com . >
> ^D
```

30.8. Configuration pour l'envoi seul

Il existe de nombreux cas où vous désirez être capable d'uniquement envoyer du courrier électronique par l'intermédiaire d'un relais. Quelques exemples:

- Votre ordinateur est une machine de bureau, mais vous voulez utilisez des programmes comme send-pr(1). Pour cela vous devez utiliser le relais de courrier électronique de votre FAI.
- L'ordinateur est un serveur qui ne gère pas le courrier électronique localement, mais a besoin de soumettre tout le courrier à un relais pour qu'il soit transmis.

N'importe quel MTA est capable d'assurer cette fonction. Malheureusement, il peut être très compliqué de configurer correctement un MTA complet pour juste gérer le courrier sortant. Des logiciels comme sendmail et postfix sont largement surdimensionnés pour cette utilisation.

De plus, si vous utilisez un accès Internet classique, votre contrat peut vous interdire de faire tourner un "serveur de courrier électronique".

La manière la plus simple pour répondre à ce besoin est d'installer le logiciel porté mail/ssmtp. Exécutez les commandes suivantes en tant que `root`:

```
# cd /usr/ports/mail/ssmtp
# make install replace clean
```

Une fois installé, mail/ssmtp peut être configuré avec un fichier de quatre lignes, /usr/local/etc/ssmtp/ssmtp.conf:

```
root=yourrealemail@example.com
mailhub=mail.example.com
rewriteDomain=example.com
hostname=_HOSTNAME_
```

Assurez-vous d'employer votre adresse électronique réelle pour l'utilisateur `root`. Utilisez le relais de courrier électronique sortant de votre FAI à la place de `mail.example.com` (certains FAIs appellent cela le "serveur de courrier sortant" ou le "serveur SMTP").

Assurez-vous également d'avoir désactivé sendmail en fixant `sendmail_enable="NONE"` dans le fichier /etc/rc.conf.

mail/ssmtp dispose d'autres options. Consultez le fichier de configuration d'exemple dans le répertoire /usr/local/etc/ssmtp ou la page de manuel de ssmtp pour quelques exemples et plus d'informations.

Configurer ssmtp de cette manière permettra à toute application tournant sur votre ordinateur et ayant besoin d'envoyer un courrier électronique de fonctionner correctement, tout en n'outrepassant pas la politique de votre FAI ou en ne permettant pas l'utilisation de votre ordinateur comme base arrière pour "spammers".

30.9. Utiliser le courrier électronique avec une connexion temporaire

Si vous disposez d'une adresse IP statique, vous ne devez rien changer du paramétrage par défaut. Définissez votre nom de machine pour qu'il corresponde à celui qui vous a été assigné pour l'Internet et sendmail s'occupera du reste.

Si votre adresse IP vous est attribuée dynamiquement et que vous utilisez une connexion PPP par modem pour accèder à l'Internet, vous disposez probablement d'une boite aux lettres chez votre fournisseur d'accès. Supposons que le domaine de votre fournisseur d'accès soit `example.net`, que votre nom d'utilisateur soit `user`, que vous avez appelé votre machine `bsd.home`, et que votre fournisseur vous ait demandé d'utiliser la machine `relay.example.net` comme serveur relai de messagerie électronique.

Pour pouvoir rapatrier votre courrier depuis votre boite aux lettres, vous devez installer un agent de rapatriement. L'utilitaire fetchmail est un bon choix car il supporte la plupart des protocoles de messagerie. Ce programme est disponible sous forme de paquetage ou à partir du catalogue des logiciels portés (mail/fetchmail). La plupart du temps, votre fournisseur d'accès fournit l'accès aux boites aux lettre à l'aide du protocole POP. Si vous utilisez PPP en mode utilisateur, vous pouvez automatiquement récupérer votre courrier quand une connexion Internet est établie avec l'entrée suivante dans le fichier /etc/ppp/ppp.linkup:

```
MYADDR:
!bg su user -c fetchmail
```

Si vous utilisez sendmail (comme montré ci-dessous) pour distribuer le courrier aux comptes non-locaux, vous voudrez probablement que sendmail s'occupe de transmettre les messages en attente dès que votre connexion Internet est établie. Pour cela, ajoutez la commande suivante après la commande `fetchmail` dans le fichier /etc/ppp/ppp.linkup:

```
!bg su user -c "sendmail -q"
```

En supposant que vous avez un compte `user` sur `bsd.home`. Dans le répertoire de l'utilisateur `user` sur `bsd.home`, créez un fichier .fetchmailrc contenant:

```
poll example.net protocol pop3 fetchall pass MySecret
```

Ce fichier ne devrait être lisible que par l'utilisateur `user` car il contient le mot de passe `MySecret`.

Afin de pouvoir envoyer du courrier avec l'entête `from:` correcte, vous devez configurer sendmail pour utiliser l'adresse `user@example.net` plutôt que `user@bsd.home`. Vous pouvez également dire à sendmail d'envoyer le courrier via le serveur `relay.example.net`, permettant une transmission du courrier plus rapide.

Le fichier .mc suivant devrait suffire:

```
VERSIONID(`bsd.home.mc version 1.0')
OSTYPE(bsd4.4)dnl
FEATURE(nouucp)dnl
MAILER(local)dnl
MAILER(smtp)dnl
Cwlocalhost
Cwbsd.home
MASQUERADE_AS(`example.net')dnl
FEATURE(allmasquerade)dnl
FEATURE(masquerade_envelope)dnl
FEATURE(nocanonify)dnl
FEATURE(nodns)dnl
define(`SMART_HOST', `relay.example.net')
Dmbsd.home
```

```
define(`confDOMAIN_NAME',`bsd.home')dnl
define(`confDELIVERY_MODE',`deferred')dnl
```

Référez-vous à la section précédente pour des détails sur la conversion de ce fichier .mc en un fichier sendmail.cf. N'oubliez pas également de redémarrer sendmail après la mise à jour du fichier sendmail.cf.

30.10. Authentification SMTP

Disposer de l'authentification SMTP sur votre serveur de courrier présente un certain nombre d'avantages. L'authentification SMTP peut ajouter une autre couche de sécurité à sendmail, et a l'avantage de donner aux utilisateurs mobiles la possibilité d'utiliser le même serveur de courrier sans avoir besoin de reconfigurer les paramètres de leur client courrier à chaque déplacement.

1. Installez security/cyrus-sasl à partir du catalogue des logiciels portés. Vous pouvez trouver ce logiciel porté dans security/cyrus-sasl. security/cyrus-sasl dispose de nombreuses options de compilation possibles, pour la méthode que nous allons utiliser ici, assurez-vous de sélectionner l'option `pwcheck`.
2. Après avoir installé security/cyrus-sasl, éditez /usr/local/lib/sasl/Sendmail.conf (ou créez-le s'il n'existe pas) et ajoutez la ligne suivante:

   ```
   pwcheck_method: passwd
   ```

   Cette méthode activera au niveau de sendmail l'authentification par l'intermédiaire de votre base de données FreeBSD passwd. Cela nous épargne le problème de la création d'un nouvel ensemble de nom d'utilisateur et de mot de passe pour chaque utilisateur ayant besoin de recourir à l'authentification SMTP, et conserve le même nom d'utilisateur et mot de passe pour le courrier.

3. Maintenant éditez /etc/make.conf et ajoutez les lignes suivantes:

   ```
   SENDMAIL_CFLAGS=-I/usr/local/include/sasl1 -DSASL
   SENDMAIL_LDFLAGS=-L/usr/local/lib
   SENDMAIL_LDADD=-lsasl
   ```

   Ces lignes passeront à sendmail les bonnes options de configuration au moment de la compilation pour lier cyrus-sasl. Assurez-vous que cyrus-sasl a été installé avant de recompiler sendmail.

4. Recompilez sendmail en lançant les commandes suivantes:

   ```
   # cd /usr/src/usr.sbin/sendmail
   # make cleandir
   # make obj
   # make
   ```

```
# make install
```

La compilation de sendmail ne devrait pas présenter de problèmes si le répertoire /usr/src n'a pas subi d'énormes changements et si les bibliothèques partagés nécessaires sont disponibles.

5. Une fois que sendmail a été compilé et réinstallé, éditez votre fichier /etc/mail/freebsd.mc (ou tout autre fichier que vous utilisez comme fichier .mc. De nombreux administrateurs utilisent la sortie de hostname(1) comme nom de fichier .mc par unicité). Ajoutez-y les lignes qui suivents:

```
dnl set SASL options
TRUST_AUTH_MECH(`GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN')dnl
define(`confAUTH_MECHANISMS', `GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN')dnl
define(`confDEF_AUTH_INFO', `/etc/mail/auth-info')dnl
```

Ces options configurent les différentes méthodes disponibles pour sendmail pour l'authentification des utilisateurs. Si vous désirez utiliser une méthode autre que pwcheck, veuillez consulter la documentation fournie.

6. Enfin, exécutez make(1) quand vous êtes dans /etc/mail. Cela prendra votre nouveau fichier .mc et créera un fichier .cf appelé freebsd.cf (ou selon tout autre nom que vous avez utilisé pour votre fichier .mc). Ensuite utilisez la commande `make install restart`, qui copiera le fichier en sendmail.cf, et redémarrera proprement sendmail. Pour plus d'informations sur ce processus, vous devriez vous référrer au fichier /etc/mail/Makefile.

Si tout s'est bien passé, vous devriez être en mesure d'entrer votre identifiant dans votre programme de courrier et d'envoyer un message de test. Pour plus d'investigation, fixez le `LogLevel` de sendmail à 13 et scrutez /var/log/maillog à la recherche d'une erreur.

Vous pourrez rajouter les lignes suivantes au fichier /etc/rc.conf afin de rendre ce service disponible après chaque démarrage du système:

```
sasl_pwcheck_enable="YES"
sasl_pwcheck_program="/usr/local/sbin/pwcheck"
```

Cela assurera l'initialisation de SMTP_AUTH, l'authentification SMTP, au démarrage du système.

Pour plus d'informations, veuillez consulter la page de la documentation de sendmail concernant l'authentification SMTP.

30.11. Clients de messagerie

Un client de messagerie ("Mail User Agent"-MUA) est une application qui est utilisée pour envoyer et recevoir du courrier électronique. En outre, au fur et à mesure que le système du courrier électronique "évolue" et devient plus complexe, les MUA deviennent de plus en plus puissants,

offrant aux utilisateurs plus de fonctionnalités et de flexibilité. FreeBSD offre le support pour de nombreux clients de messagerie, ils peuvent tous être aisément installés à partir du catalogue des logiciels portés de FreeBSD. Les utilisateurs pourront choisir entre des clients de messagerie graphiques comme evolution ou balsa, des clients en mode console tels que mutt, pine ou `mail`, ou encore les interfaces Web utilisées par certaines organisations importantes.

30.11.1. mail

mail(1) est le client de messagerie ("Mail User Agent"-MUA) par défaut de FreeBSD. C'est un MUA en mode console qui offre toutes les fonctionnalités de base nécessaires pour envoyer et lire son courrier électronique en mode texte, cependant il est limité en ce qui concerne les possibilités de pièces jointes et ne supporte que les boîtes aux lettres locales.

Bien que `mail` ne supporte pas l'intéraction avec les serveurs POP ou IMAP, ces boîtes aux lettres peuvent être téléchargées vers un fichier mbox local en utilisant une application telle que fetchmail, qui sera abordée plus tard dans ce chapitre (Utiliser fetchmail).

Afin d'envoyer et de recevoir du courrier électronique, invoquez simplement la commande `mail` comme le montre l'exemple suivant:

```
% mail
```

Le contenu de la boîte aux lettres de l'utilisateur dans /var/mail est automatiquement lu par l'utilitaire `mail`. Si la boîte est vide, l'utilitaire rend la main avec un message indiquant qu'aucun courrier électronique ne peut être trouvé. Une fois que la boîte aux lettres a été lue, l'interface de l'application est lancée, et une liste de messages sera affichée. Les messages sont automatiquement numérotés, comme on peut le voir dans l'exemple suivant:

```
Mail version 8.1 6/6/93.  Type ? for help.
"/var/mail/marcs": 3 messages 3 new
>N  1 root@localhost        Mon Mar  8 14:05  14/510   "test"
 N  2 root@localhost        Mon Mar  8 14:05  14/509   "user account"
 N  3 root@localhost        Mon Mar  8 14:05  14/509   "sample"
```

Les messages peuvent désormais être lus en utilisant la commande `t` de `mail`, suivie du numéro du message qui devra être affiché. Dans cet exemple, nous lirons le premier courrier électronique:

```
% t 1
Message 1:
From root@localhost  Mon Mar  8 14:05:52 2004
X-Original-To: marcs@localhost
Delivered-To: marcs@localhost
To: marcs@localhost
Subject: test
Date: Mon,  8 Mar 2004 14:05:52 +0200 (SAST)
From: root@localhost (Charlie Root)
```

```
This is a test message, please reply if you receive it.
```

Comme nous pouvons le constater dans l'exemple ci-dessus, l'appuie sur la touche `t` fera afficher le message avec les entêtes complètes. Pour afficher à nouveau la liste des messages, la touche `h` doit être utilisée.

Si le message nécessite une réponse, vous pouvez utiliser `mail` pour cela, en entrant soit la touche `R`, soit la touche `r`. La touche `R` demande à `mail` de ne répondre qu'à l'expéditeur du message, alors que `r` répond à l'expéditeur mais également aux autres destinataires du message. Vous pouvez ajouter à la suite de ces commandes le numéro du courrier auquel vous désirez répondre. Une fois cela effectué, la réponse doit être tapée, et la fin du message doit être indiquée par un `.` sur une nouvelle ligne. Ci-dessous est présenté un exemple:

```
% R 1
To: root@localhost
Subject: Re: test

Thank you, I did get your email.
.
EOT
```

Afin d'envoyer un nouveau courrier électronique, la touche `m` doit être utilisée, suivie de l'adresse électronique du destinataire. Plusieurs destinataires peuvent également être spécifiés en séparant chaque adresse par une `,`. Le sujet du message peut alors être entré, suivi du corps du message. La fin d'un message doit être indiquée en mettant un `.` seul sur une nouvelle ligne.

```
% mail root@localhost
Subject: I mastered mail

Now I can send and receive email using mail ... :)
.
EOT
```

Bien qu'à partir de l'utilitaire `mail`, la commande `?` puisse être utilisée à tout instant pour afficher l'aide, la page de manuel mail(1) devrait être consultée pour plus d'aide sur `mail`.

Comme indiqué précédemment, la commande mail(1) à l'origine n'a pas été conçue pour gérer les pièces jointes, et par conséquent ne s'en sort pas très bien à ce niveau. Les MUAs plus récents comme mutt gérent les pièces jointes de manière plus intelligente. Mais si vous souhaitez toujours utiliser `mail`, le logiciel porté converters/mpack vous sera d'une grande aide.

30.11.2. mutt

mutt est un client de messagerie léger mais très puissant, avec de nombreuses fonctionnalités, parmi lesquelles:

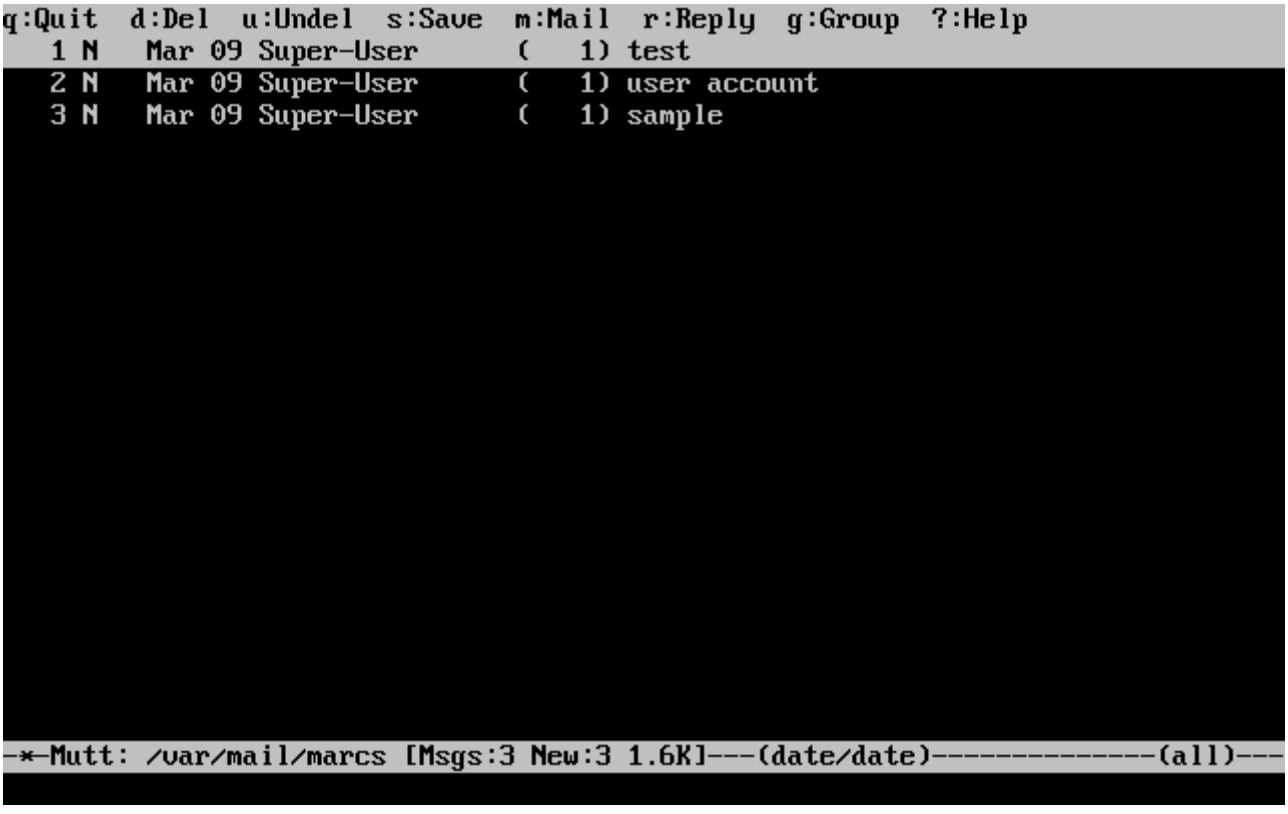
- la possibilité de gérer les fils ("threads") de discussions;
- le support PGP pour la signature électronique et le chiffrage de courriers électroniques;
- le support MIME;
- le support du format maildir;
- application hautement configurable et personnalisable.

Toutes ces caractéristiques font de mutt un des clients de messagerie les plus avancés. Consultez http://www.mutt.org pour plus d'informations sur mutt.

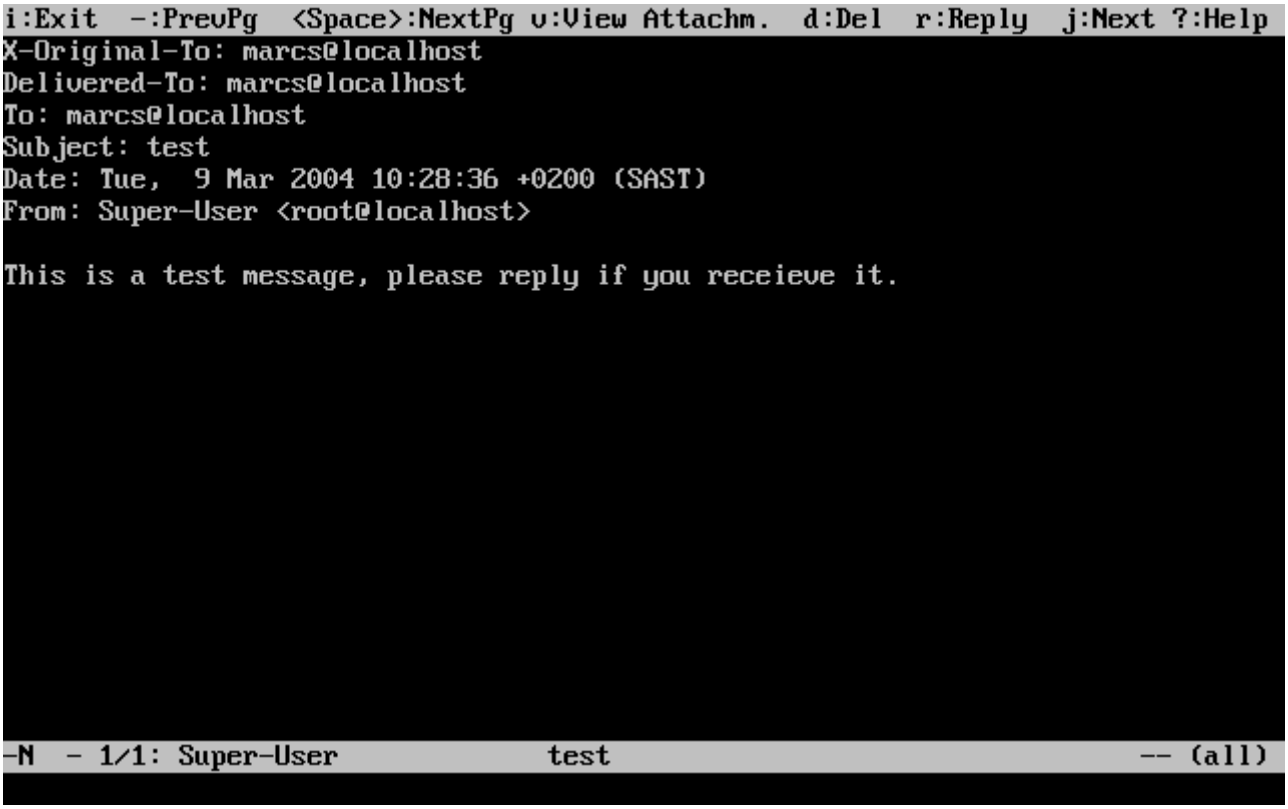
La version stable de mutt peut être installée en utilisant le logiciel porté mail/mutt, tandis que la version actuellement en développement peut être installée par l'intermédiaire du logiciel porté mail/mutt-devel. Une fois installé, mutt peut être lancé en tapant la commande suivante:

```
% mutt
```

mutt lira automatiquement le contenu de la boîte aux lettres de l'utilisateur dans /var/mail et en affiche le contenu le cas échéant. Si aucun message n'est trouvé dans cette boîte, alors mutt attendra une commande de l'utilisateur. L'exemple ci-dessous montre mutt affichant une liste de messages:



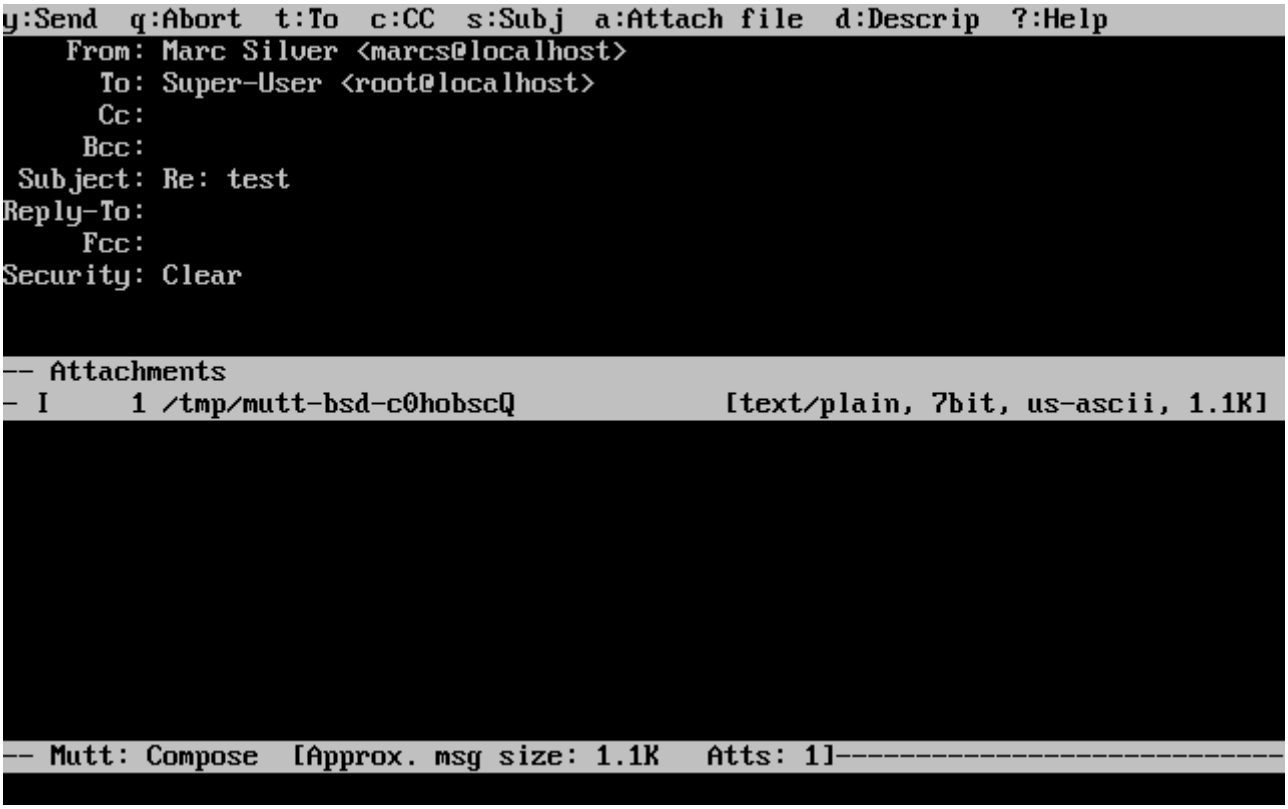
Afin de lire un message, sélectionnez-le en utilisant les touches fléchées, et appuyez sur `Entrée`. Un exemple montrant mutt affichant le contenu d'un message est donné ci-dessous:



Comme avec la commande mail(1), mutt permet aux utilisateurs de répondre uniquement à l'expéditeur du message comme également à l'ensemble de ses destinataires. Pour répondre uniquement à l'expéditeur du courrier électronique, utilisez le raccourci clavier `r`. Pour faire une réponse groupée, qui sera envoyée à l'expéditeur comme à tous les destinataires du message, utilisez la touche `g`.

mutt emploie vi(1) comme éditeur pour la création et la réponse aux courriers électronique. Cela peut être modifié par l'utilisateur en créant son propre fichier .muttrc dans leur répertoire personnel et en positionnant la variable `editor`.

Pour rédiger un nouveau message, appuyez sur la touche `m`. Après avoir donné un sujet valide, mutt lancera vi(1) et l'intégralité du message pourra être écrite. Une fois le courrier électronique rédigé, sauvegardez et quittez `vi` et mutt réapparaîtra affichant un écran résumant le courrier devant être envoyé. Pour envoyer le message, appuyez sur `y`. Un exemple de résumé peut être vu ci-dessous:



mutt propose également une aide complète, qui peut être consultée à partir de la plupart des menus en appuyant sur la touche `?`. La ligne située en haut de l'écran affiche également les raccourcis clavier appropriés.

30.11.3. pine

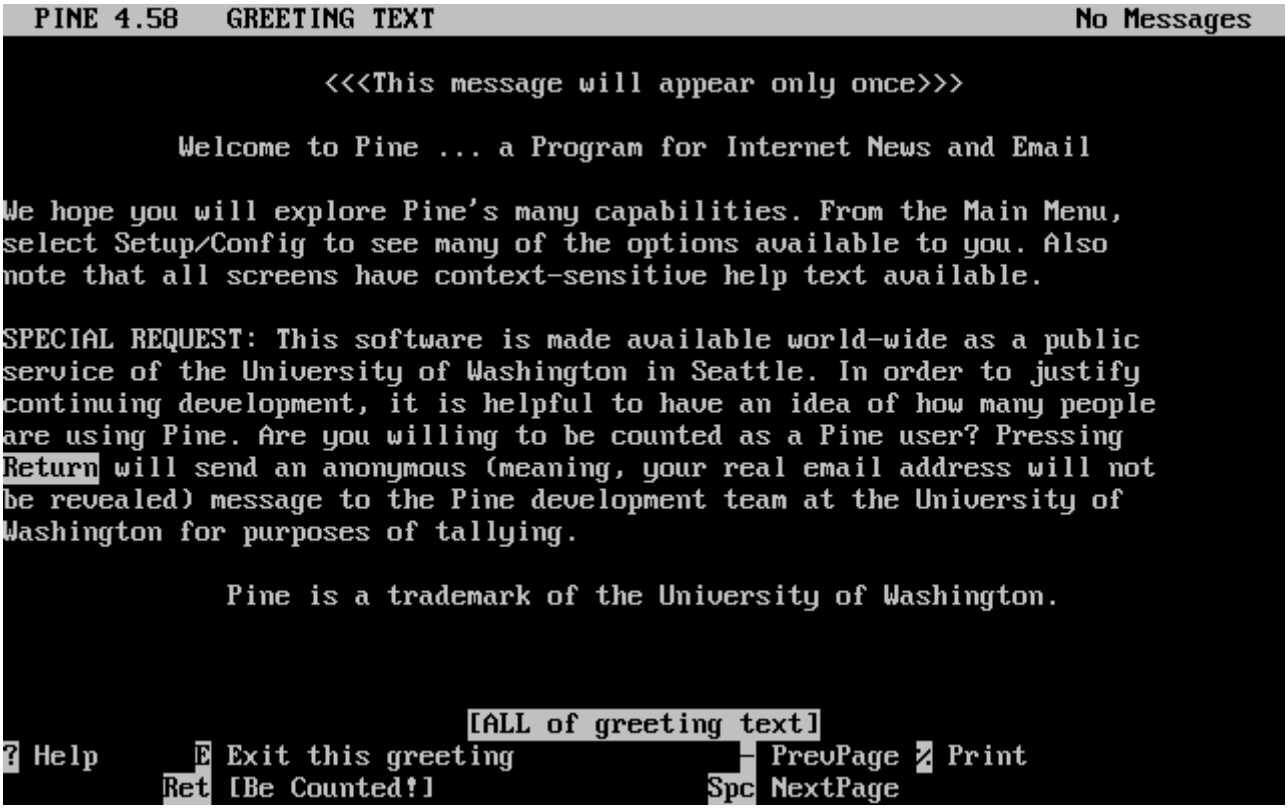
pine est destiné aux débutants, mais il dispose également de fonctions avancées.

Plusieurs vulnérabilités exploitables à distance ont été découvertes dans le logiciel pine par le passé, autorisant à un agresseur distant d'exécuter un programme arbitraire en tant qu'utilisateur local du système, en envoyant un courrier électronique particulier. Tous les problèmes *connus* ont été corrigés, mais le code source de pine est écrit d'une manière assez peu sécurisée et l'officier de sécurité de FreeBSD pense qu'il existe d'autres failles qui ne sont pas encore découvertes. Vous installez donc pine à vos propres risques.

La version actuelle de pine peut être installée en utilisant le logiciel porté mail/pine4. Une fois installé, pine peut être lancé en tapant la commande suivante:

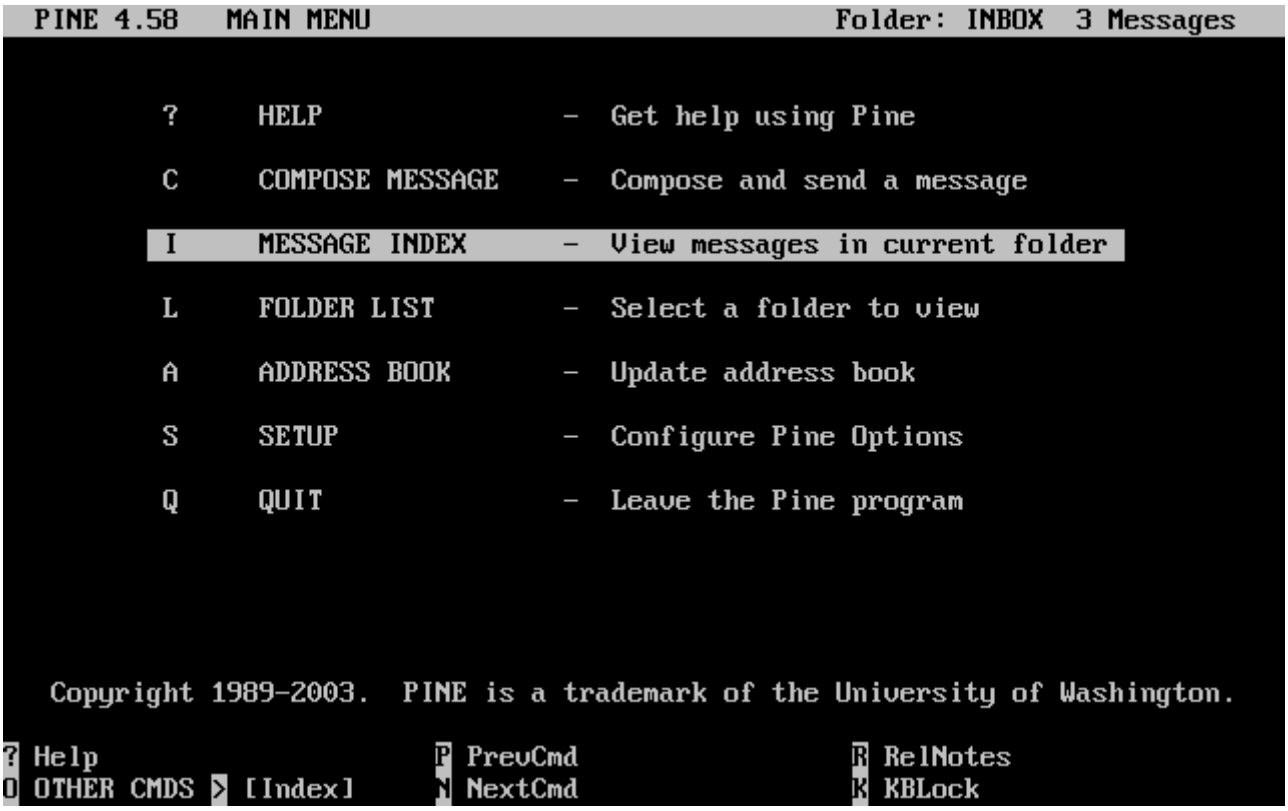
```
% pine
```

Lors du premier lancement de pine, ce dernier affiche une page de présentation avec une brève introduction, ainsi qu'un message de la part de l'équipe de développement de pine demandant l'envoi d'un courrier électronique anonyme pour leur permettre d'évaluer le nombre d'utilisateurs de leur client de messagerie. Pour envoyer ce courrier anonyme, appuyez sur `Entrée`, ou sinon appuyez sur `E` pour quitter la présentation sans envoyer de message anonyme. Un exemple de page de présentation peut être vu ci-dessous:

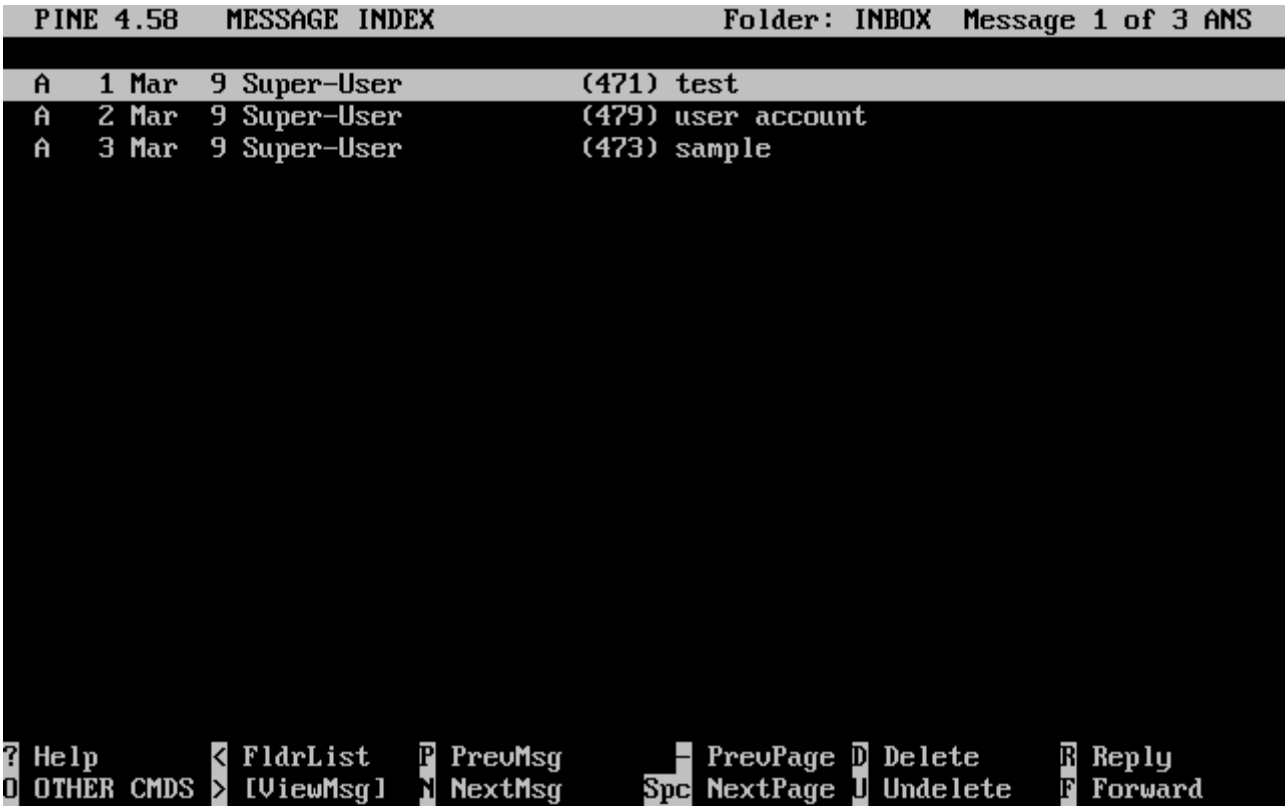


Le menu principal est ensuite affiché, menu dans lequel il est aisé de naviguer avec les touches fléchées. Ce menu principal fournit les raccourcis pour la rédaction de nouveaux messages, la navigation dans les répertoires de messages, et même la gestion des entrées du carnet d'adresses. Sous le menu principal, les raccourcis clavier correspondants pour effectuer les différentes tâches sont donnés.

Le répertoire ouvert par défaut par pine est inbox. Pour afficher l'index des messages, appuyez sur `I`, ou sélectionnez l'option MESSAGE INDEX comme montré ci-dessous:

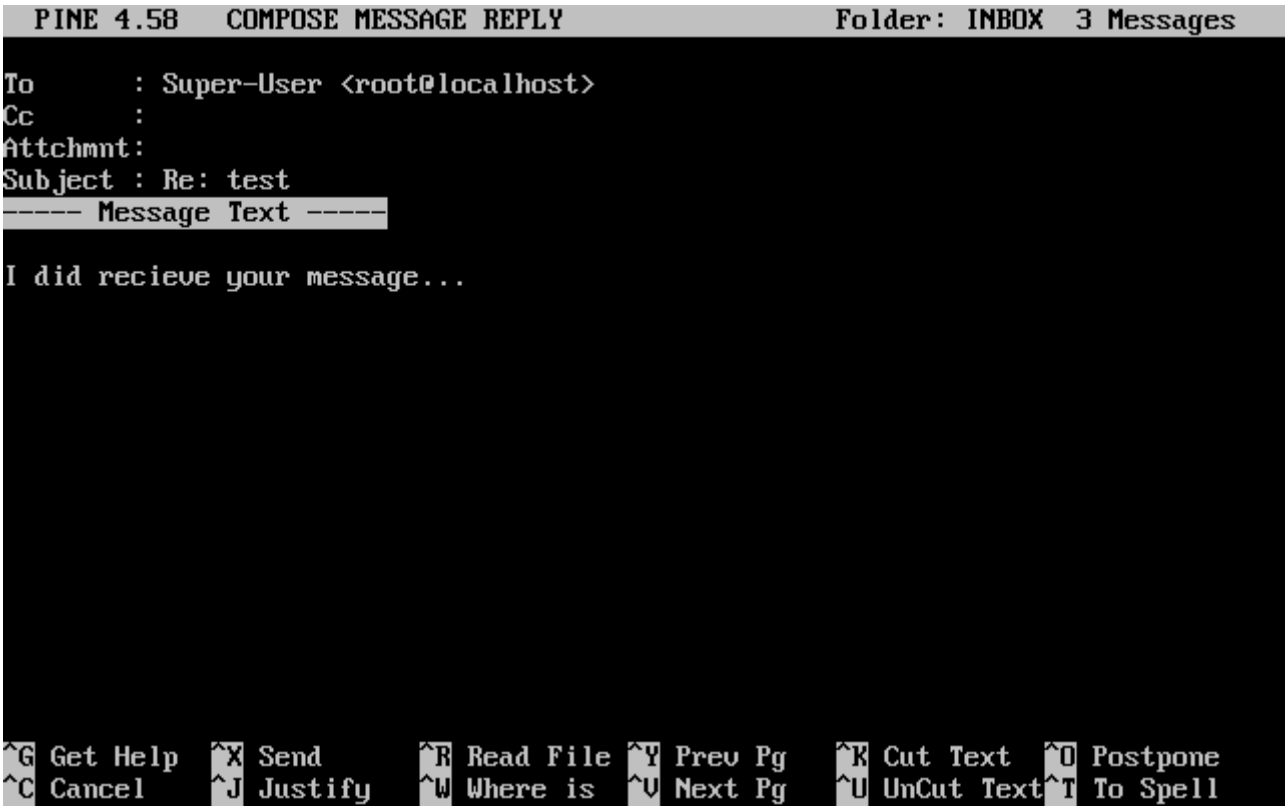


L'index des messages montre les messages dans le répertoire courant, on peut se déplacer dans l'index en utilisant les touches fléchées. Les messages en surbrillance peuvent être lus en appuyant sur la touche `Enter`.



Dans la capture d'écran ci-dessous, un message d'exemple est affiché par pine. Les raccourcis clavier sont affichés au bas de l'écran. Un exemple de raccourci est la touche `r`, qui demande au programme de répondre au message actuellement à l'écran.

La rédaction d'une réponse à un courrier électronique avec pine se fait en utilisant l'éditeur pico, qui est installé par défaut avec pine. L'utilitaire pico rend aisé les déplacements dans le message et est plus indulgent avec les novices que vi(1) ou mail(1). Une fois la réponse rédigée, le message peut être envoyé en appuyant sur `Ctrl` + `X`. pine vous demandera de confirmer votre action.



Le programme pine peut être personnalisé en utilisant l'option SETUP du menu principal. Consultez http://www.washington.edu/pine/ pour plus d'information.

30.12. Utiliser fetchmail

fetchmail est un client IMAP et POP complet qui offre aux utilisateurs le téléchargement automatiquement de leur courrier électronique à partir de serveurs IMAP et POP distants et sa sauvegarde dans des boîtes aux lettres locales; ainsi, le courrier électronique pourra être consulté plus facilement. fetchmail peut être installé en utilisant le logiciel porté mail/fetchmail, et offre diverses fonctionnalités, dont:

- le support des protocoles POP3, APOP, KPOP, IMAP, ETRN et ODMR;
- la capacité de faire suivre le courrier électronique en utilisant SMTP, ce qui autorise le filtrage, le transfert, et la gestion des alias de fonctionner correctement;
- la possibilité de fonctionner en mode "daemon" pour contrôler périodiquement si il y a de nouveaux messages;
- la possibilité de récupérer le courrier de plusieurs boîtes aux lettres et de le transférer en fonction d'une configuration bien précise aux différents utilisateurs locaux.

Bien qu'expliquer l'intégralité des fonctions de fetchmail dépasse le cadre de ce document, certaines fonctions de base seront abordées. L'utilitaire fetchmail nécessite un fichier de configuration nommé .fetchmailrc, afin de fonctionner correctement. Ce fichier comprend les

informations concernant les serveurs ainsi que les accréditations d'accès. En raison du caractère sensible du contenu de ce fichier, il est recommandé de ne le rendre lisible que par l'utilisateur, avec la commande suivante:

```
% chmod 600 .fetchmailrc
```

Le fichier .fetchmailrc suivant sert d'exemple pour récupérer le courrier électronique pour un seul utilisateur à partir d'une boîte aux lettres utilisant le protocole POP. Il demande à fetchmail de se connecter à `example.com` en utilisant le nom d'utilisateur `joesoap` et le mot de passe `XXX`. Dans cet exemple on suppose que l'utilisateur `joesoap` est également un utilisateur sur le système local.

```
poll example.com protocol pop3 username "joesoap" password "XXX"
```

L'exemple suivant présente la connexion à plusieurs serveurs POP et IMAP et la redirection vers différents utilisateurs locaux quand c'est nécessaire:

```
poll example.com proto pop3:
user "joesoap", with password "XXX", is "jsoap" here;
user "andrea", with password "XXXX";
poll example2.net proto imap:
user "john", with password "XXXXX", is "myth" here;
```

L'utilitaire fetchmail peut être exécuté en mode "daemon" en le lançant avec le paramètre `-d`, suivi par l'intervalle de temps (en secondes) que fetchmail doit respecter entre chaque consultation des serveurs listés dans le fichier .fetchmailrc. L'exemple suivant demandera à fetchmail de récupérer le courrier toutes les 60 secondes:

```
% fetchmail -d 60
```

Plus d'informations concernant fetchmail peuvent être trouvées sur http://www.catb.org/~esr/fetchmail/.

30.13. Utiliser procmail

L'utilitaire procmail est une application extrêmement puissante utilisée pour filtrer le courrier électronique entrant. Il permet aux utilisateurs de définir des "règles" qui seront utilisées sur le courrier entrant pour effectuer des opérations particulières ou pour transférer le courrier vers d'autres boîtes aux lettres et/ou adresses électroniques. procmail peut être installé en utilisant le logiciel porté mail/procmail. Une fois installé, il peut être intégré dans la plupart des MTAs, consultez la documentation de votre MTA pour plus d'information. Alternativement, procmail peut être intégré en ajoutant la ligne suivante à un fichier .forward dans le répertoire personnel de l'utilisateur employant les fonctionnalités de procmail:

```
"|exec /usr/local/bin/procmail || exit 75"
```

La suite de cette section présentera quelques règles de base pour procmail, avec une brève description de ce qu'elles font. Ces règles, ainsi que d'autres, doivent être ajoutées dans le fichier .procmailrc, qui doit résider dans le répertoire personnel de l'utilisateur.

La majorité de ces règles peut également être trouvée dans la page de manuel de procmailex(5).

Transférer tout courrier en provenance de `user@example.com` vers l'adresse externe `goodmail@example2.com`:

```
:0
* ^From.*user@example.com
! goodmail@example2.com
```

Transférer tous les courriers d'une taille inférieure à 1000 octets vers l'adresse externe `goodmail@example2.com`:

```
:0
*  1000
! goodmail@example2.com
```

Mettre tout le courrier à destination de `alternate@example.com` dans une boîte aux lettres appelée alternate:

```
:0
* ^TOalternate@example.com
alternate
```

Envoyer tous les courriers avec pour sujet "Spam" vers /dev/null:

```
:0
^Subject:.*Spam
/dev/null
```

Une recette utile pour trier les courriers en provenance des listes de diffusion `FreeBSD.org` et placer chaque liste dans sa propre boîte aux lettres:

```
:0
* ^Sender:.owner-freebsd-\/[^@]+@FreeBSD.ORG
{
    LISTNAME=${MATCH}
    :0
    * LISTNAME??^\/[^@]+
```

```
    FreeBSD-${MATCH}
}
```

Chapitre 31. Serveurs réseau

31.1. Synopsis

Ce chapitre abordera certains des services réseaux les plus fréquemment utilisés sur les systèmes UNIX®. Nous verrons comment installer, configurer, tester et maintenir plusieurs types différents de services réseaux. De plus, des exemples de fichier de configuration ont été inclus tout au long de ce chapitre pour que vous puissiez en bénéficier.

Après la lecture de ce chapitre, vous connaîtrez:

- Comment gérer le "daemon" inetd.
- Comment configurer un système de fichiers réseau.
- Comment mettre en place un serveur d'information sur le réseau pour partager les comptes utilisateurs.
- Comment configurer le paramétrage réseau automatique en utilisant DHCP.
- Comment configurer un serveur de noms de domaine.
- Comment configurer le serveur HTTP Apache.
- Comment configurer un serveur de transfert de fichier (FTP).
- Comment configurer un serveur de fichiers et d'impression pour des clients Windows® en utilisant Samba.
- Comment synchroniser l'heure et la date, et mettre en place en serveur de temps, avec le protocole NTP.

Avant de lire ce chapitre, vous devrez:

- Comprendre les bases des procédures /etc/rc.
- Etre familier avec la terminologie réseau de base.
- Savoir comment installer des applications tierce-partie (Installer des applications. les logiciels pré-compilés et les logiciels portés).

31.2. Le "super-serveur" inetd

31.2.1. Généralités

On fait parfois référence à inetd(8) comme étant le "super-serveur Internet" parce qu'il gère les connexions pour plusieurs services. Quand une connexion est reçue par inetd, ce dernier détermine à quel programme la connexion est destinée, invoque le processus en question et lui délègue la "socket" (le programme est invoqué avec la "socket" service comme entrée standard, sortie et descripteurs d'erreur). Exécuter inetd pour les serveurs qui ne sont pas utilisés intensément peut réduire la charge système globale quand on compare avec l'exécution de chaque "daemon" individuellement en mode autonome.

inetd est utilisé pour invoquer d'autres "daemon"s, mais plusieurs protocoles triviaux sont gérés directement, comme chargen, auth, et daytime.

Cette section abordera la configuration de base d'inetd à travers ses options en ligne de commande et son fichier de configuration /etc/inetd.conf.

31.2.2. Configuration

inetd est initialisé par l'intermédiaire du système rc(8). L'option `inetd_enable` est positionnée à la valeur `NO` par défaut, mais peut être activée par sysinstall lors de l'installation en fonction de la configuration choisie par l'utilisateur. Placer

```
inetd_enable="YES"
```

ou

```
inetd_enable="NO"
```

dans /etc/rc.conf activera ou désactivera le lancement d'inetd à la mise en route du système. La commande:

```
# /etc/rc.d/inetd rcvar
```

peut être lancée pour afficher le paramétrage en vigueur.

De plus, différentes options de ligne de commande peuvent être passées à inetd par l'intermédiaire de l'option `inetd_flags`.

31.2.3. Options en ligne de commande

Comme la plupart des "daemons", inetd possède de nombreuses options que l'on peut passer à son lancement afin de modifier son comportement. La liste complète des options se présente sous la forme:

```
inetd [-d] [-l] [-w] [-W] [-c maximum] [-C taux] [-a adresse | nom de machine] [-p fichier] [-R taux] [fichier de configuration]
```

Les options peuvent être passées à inetd en utilisant le paramètre `inetd_flags` dans /etc/rc.conf. Par défaut, `inetd_flags` contient `-wW -C 60`, qui active le "TCP wrapping" pour les services inetd, et empêche l'invocation d'un service plus de 60 fois par minute à partir d'une unique adresse IP.

Les novices seront heureux d'apprendre que ce paramétrage n'a en général pas besoin d'être modifié, cependant nous présentons ci-dessous les options de limitation du taux d'invocation étant donné que cela peut être utile si vous recevez une quantité excessive de connexions. Une liste complète d'options peut être trouvée dans la page de manuel de inetd(8).

-c maximum

Spécifie le nombre maximal par défaut d'invocations simultanées pour chaque service; il n'y a pas de limite par défaut. Cette option peut être surchargée pour chaque service à l'aide du paramètre `nb-max-enfants`.

-C taux

Précise le nombre maximal de fois qu'un service peut être invoqué à partir d'une unique adresse IP et cela sur une minute. Ce paramètre peut être configuré différemment pour chaque service avec le paramètre `nb-max-connexions-par-ip-par-minute`.

-R taux

Précise le nombre maximal de fois qu'un service peut être invoqué par minute; la valeur par défaut est 256. Un taux de 0 autorise un nombre illimité d'invocations.

-s maximum

Précise le nombre maximal de fois qu'un service peut être invoqué simultanément à partir d'une adresse IP unique; il n'y a pas de limite par défaut. Cette option peut-être surchargée pour chaque service individuellement avec le paramètre `max-child-per-ip`.

31.2.4. inetd.conf

La configuration d'inetd se fait par l'intermédiaire du fichier /etc/inetd.conf.

Quand le fichier /etc/inetd.conf est modifié, inetd peut être forcé de relire son fichier de configuration en utilisant la commande:

Exemple 40. Recharger le fichier de configuration d'inetd

```
# /etc/rc.d/inetd reload
```

Chaque ligne du fichier de configuration ne mentionne qu'un seul "daemon". Les commentaires dans le fichier sont précédés par un "#". Le format de chaque entrée du fichier /etc/inetd.conf est le suivant:

```
nom-du-service
type-de-socket
protocole
{wait|nowait}[/nb-max-enfants[/nb-connexions-max-par-minute]]
{wait|nowait}[/nb-max-enfants[/nb-connexions-max-par-minute[/nb-max-enfants-par-ip]]]
utilisateur[:groupe][/classe-session]
programme-serveur
arguments-du-programme-serveur
```

Un exemple d'entrée pour le "daemon" ftpd(8) utilisant l'IPv4 ressemblerait:

```
ftp     stream  tcp     nowait  root    /usr/libexec/ftpd       ftpd -l
```

nom-du-service

C'est le nom de service du "daemon" en question. Il doit correspondre à un des services listés dans le fichier /etc/services. Cela détermine quel port inetd doit écouter. Si un nouveau service est créé, il doit être ajouté en premier lieu dans /etc/services.

type-de-socket

Soit `stream`, soit `dgram`, soit `raw`, ou `seqpacket`. `stream` doit être utilisé pour les "daemon"s TCP, alors que `dgram` est utilisé pour les "daemon"s utilisant le protocole UDP.

protocole

Un des suivants:

Protocole	Explication
tcp, tcp4	TCP IPv4
udp, udp4	UDP IPv4
tcp6	TCP IPv6
udp6	UDP IPv6
tcp46	TCP IPv4 et v6
udp46	UDP IPv4 et v6

{wait|nowait}[/nb-max-enfants[/nb-max-connexions-par-ip-par-minute[/nb-max-enfants-par-ip]]]

`wait|nowait` indique si le "daemon" invoqué par inetd est capable ou non de gérer sa propre "socket". Les "socket"s de type `dgram` doivent utiliser l'option `wait`, alors que les "daemons à socket stream", qui sont généralement multi-threadés, devraient utiliser `nowait`. L'option `wait` a généralement pour conséquence de fournir plusieurs "socket"s à un "daemon", tandis que l'option `nowait` invoquera un "daemon" enfant pour chaque nouvelle "socket".

Le nombre maximal de "daemon"s qu'inetd peut invoquer peut être fixé en utilisant l'option `nb-max-enfants`. Si une limite de dix instances pour un "daemon" est nécessaire, `/10` devra être placé après `nowait`. Spécifier `/0` autorise un nombre illimité d'enfant.

En plus de `nb-max-enfants`, deux autres options limitant le nombre maximal de connexions à partir d'un emplacement vers un "daemon" particulier peuvent être activéees. L'option `nb-max-connexions-par-ip-par-minute` limite le nombre de connexions par minutes à partir d'une adresse IP donnée, par exemple, une valeur de dix limiterait à dix le nombre de tentatives de connexions par minute pour une adresse IP particulière. L'option `max-child-per-ip` limite le nombre d'enfants qui peuvent être lancés pour une adresse IP unique à un instant donné. Ces options sont utiles pour empêcher l'abus excessif intentionnel ou par inadvertance des ressources d'une machine et les attaques par déni de service ("Denial of Service-DOS").

Dans ce champ, `wait` ou `nowait` est obligatoire. `nb-max-enfants`, `nb-max-connexions-par-ip-par-minute` et `max-child-per-ip` sont optionnelles.

Un "daemon" utilisant un flux de type multi-threadé sans limites `nb-max-enfants`, `nb-max-connexions-par-ip-par-minute` ou `max-child-per-ip` sera tout simplement affecté de l'option `nowait`.

Le même "daemon" avec une limite maximale de dix "daemon" serait: `nowait/10`.

La même configuration avec une limite de vingt connexions par adresse IP par minute et une limite maximale de dix "daemon"s enfant serait: `nowait/10/20`.

Ces options sont utilisées comme valeurs par défaut par le "daemon" fingerd(8), comme le montre ce qui suit:

```
finger stream  tcp     nowait/3/10 nobody /usr/libexec/fingerd fingerd -s
```

Et enfin, un exemple de champ avec un maximum de 100 enfants en tout, avec un maximum de 5 adresses IP distinctes serait: `nowait/100/0/5`.

utilisateur

C'est l'utilisateur sous lequel le "daemon" en question est exécuté. En général les "daemon"s tournent sous l'utilisateur `root`. Pour des questions de sécurité, il est courant de rencontrer des serveurs tournant sous l'utilisateur `daemon`, ou sous l'utilisateur avec le moins de privilèges: `nobody`.

programme-serveur

Le chemin complet du "daemon" qui doit être exécuté quand une requête est reçue. Si le "daemon" est un service fourni en interne par inetd, alors l'option `internal` devrait être utilisée.

arguments-programme-serveur

Cette option va de pair avec `programme-serveur` en précisant les arguments, en commençant avec `argv[0]`, passés au "daemon" lors de son invocation. Si `mydaemon -d` est la ligne de commande, `mydaemon -d` sera la valeur de l'option `arguments-programme-serveur`. Ici également, si le "daemon" est un service interne, utilisez `internal`.

31.2.5. Sécurité

En fonction des choix effectués à l'installation, plusieurs services peuvent être activés par défaut. S'il n'y a pas de raison particulière à l'utilisation d'un "daemon", envisagez de le désactiver. Ajoutez un caractère "#" devant le "daemon" en question dans le fichier /etc/inetd.conf, et ensuite rechargez la configuration d'inetd. Certains "daemon"s comme fingerd, devraient être évités parce qu'ils peuvent fournir des informations utiles aux personnes malveillantes.

Certains "daemon"s n'ont aucune conscience des problèmes de sécurité, et ont un long délai limite, ou pas du tout, d'expiration pour les tentatives de connexions. Cela permet à une personne malveillante d'envoyer régulièrement et de manière espacée des demandes de connexions à un "daemon" particulier, avec pour conséquence de saturer les ressources disponibles. Cela peut être une bonne idée de placer des limitations `nb-max-connexions-par-ip-par-minute`, `max-child` ou `nb-max-enfants` sur certains "daemon"s si vous trouvez que vous avez trop de connexions.

Par défaut, le "TCP wrapping" est activé. Consultez la page de manuel hosts_access(5) pour plus d'information sur le placement de restrictions TCP pour divers "daemon"s invoqués par inetd.

31.2.6. Divers

daytime, time, echo, discard, chargen, et auth sont des services fournis en interne par inetd.

Le service auth fournit les services réseau d'identification, et est configurable à un certain degré, alors que les autres services ne peuvent être que stoppés ou en fonctionnement.

Consultez la page de manuel de inetd(8) pour plus d'informations.

31.3. Système de fichiers réseau (NFS)

Parmi les différents systèmes de fichiers que FreeBSD supporte se trouve le système de fichiers réseau, connu sous le nom de NFS. NFS permet à un système de partager des répertoires et des fichiers avec d'autres systèmes par l'intermédiaire d'un réseau. En utilisant NFS, les utilisateurs et les programmes peuvent accéder aux fichiers sur des systèmes distants comme s'ils étaient des fichiers locaux.

Certains des avantages les plus remarquables offerts par NFS sont:

- Les stations de travail utilisent moins d'espace disque en local parce que les données utilisées en commun peuvent être stockées sur une seule machine tout en restant accessibles aux autres machines sur le réseau.
- Les utilisateurs n'ont pas besoin d'avoir un répertoire personnel sur chaque machine du réseau. Les répertoires personnels pourront se trouver sur le serveur NFS et seront disponibles par l'intermédiaire du réseau.
- Les périphériques de stockage comme les lecteurs de disquettes, de CDROM, de disquettes Zip® peuvent être utilisés par d'autres machines sur le réseau. Cela pourra réduire le nombre de lecteurs de medias amovibles sur le réseau.

31.3.1. Comment NFS fonctionne

NFS consiste en deux éléments principaux: un serveur et un ou plusieurs clients. Le client accède à distance aux données stockées sur la machine serveur. Afin que tout cela fonctionne correctement quelques processus doivent être configurés et en fonctionnement.

Sur le serveur, les "daemons" suivants doivent tourner:

Daemon	Description
nfsd	Le "daemon" NFS qui répond aux requêtes des clients NFS.
mountd	Le "daemon" de montage NFS qui traite les requêtes que lui passe nfsd(8).
rpcbind	Ce "daemon" permet aux clients NFS de trouver le port que le serveur NFS utilise.

Le client peut également faire tourner un "daemon" connu sous le nom de nfsiod. Le "daemon" nfsiod traite les requêtes en provenance du serveur NFS. Ceci est optionnel, et améliore les performances, mais n'est pas indispensable pour une utilisation normale et correcte. Consultez la page de manuel nfsiod(8) pour plus d'informations.

31.3.2. Configurer NFS

La configuration de NFS est une opération relativement directe. Les processus qui doivent tourner peuvent tous être lancés au démarrage en modifiant légèrement votre fichier /etc/rc.conf.

Sur le serveur NFS, assurez-vous que les options suivantes sont configurées dans le fichier /etc/rc.conf:

```
rpcbind_enable="YES"
nfs_server_enable="YES"
mountd_flags="-r"
```

mountd est automatiquement exécuté dès que le serveur NFS est activé.

Sur le client, assurez-vous que cette option est présente dans le fichier /etc/rc.conf:

```
nfs_client_enable="YES"
```

Le fichier /etc/exports indique quels systèmes de fichiers NFS devraient être exportés (parfois on utilise le terme de "partagés"). Chaque ligne dans /etc/exports précise un système de fichiers à exporter et quelles machines auront accès à ce système de fichiers. En plus des machines qui auront accès, des options d'accès peuvent également être présentes. Ces options sont nombreuses mais seules quelques unes seront abordées ici. Vous pouvez aisément découvrir d'autres options en lisant la page de manuel exports(5).

Voici quelques exemples d'entrées du fichier /etc/exports:

Les exemples suivants donnent une idée de comment exporter des systèmes de fichiers bien que certains paramètres peuvent être différents en fonction de votre environnement et votre configuration réseau. Par exemple, pour exporter le répertoire /cdrom pour les trois machines d'exemple qui appartiennent au même domaine que le serveur (d'où l'absence du nom de domaine pour chacune d'entre elles) ou qui ont une entrée dans votre fichier /etc/hosts. Le paramètre `-ro` limite l'accès en lecture seule au système de fichiers exporté. Avec ce paramètre, le système distant ne pourra pas écrire sur le système de fichiers exporté.

```
/cdrom -ro host1 host2 host3
```

La ligne suivante exporte /home pour les trois machines en utilisant les adresses IP. C'est une configuration utile si vous disposez d'un réseau privé sans serveur DNS configuré. Le fichier /etc/hosts pourrait éventuellement être configuré pour les noms de machines internes, consultez la page de manuel hosts(5) pour plus d'information. Le paramètre `-alldirs` autorise l'utilisation des

sous-répertoires en tant que point de montage. En d'autres termes, il ne montera pas les sous-répertoires mais autorisera le client à ne monter que les répertoires qui sont nécessaires ou désirés.

```
/home  -alldirs  10.0.0.2 10.0.0.3 10.0.0.4
```

La ligne suivante exporte /a pour que deux clients d'un domaine différent puissent y accéder. Le paramètre `-maproot=root` autorise l'utilisateur `root` du système distant à écrire des données sur le système de fichiers exporté en tant que `root`. Si le paramètre `-maproot=root` n'est pas précisé, même si un utilisateur dispose d'un accès `root` sur le système distant, il ne pourra pas modifier de fichiers sur le système de fichiers exporté.

```
/a  -maproot=root  host.example.com box.example.org
```

Afin de pouvoir accéder à un système de fichiers exporté, le client doit avoir les permissions de le faire. Assurez-vous que le client est mentionné dans votre fichier /etc/exports.

Dans /etc/exports, chaque ligne représente l'information d'exportation d'un système de fichiers vers une machine. Une machine distante ne peut être spécifiée qu'une fois par système de fichiers, et ne devrait avoir qu'une seule entrée par défaut. Par exemple, supposons que /usr soit un seul système de fichiers. Le fichier /etc/exports suivant serait invalide:

```
# Invalide quand /usr est un système de fichiers
/usr/src   client
/usr/ports client
```

Un système de fichiers, /usr, a deux lignes précisant des exportations vers la même machine, `client`. Le format correct pour une telle situation est:

```
/usr/src /usr/ports  client
```

Les propriétés d'un système de fichiers exporté vers une machine donnée devraient apparaître sur une ligne. Les lignes sans client sont traitées comme destinée à une seule machine. Cela limite la manière dont vous pouvez exporter les systèmes de fichiers, mais pour la plupart des gens cela n'est pas un problème.

Ce qui suit est un exemple de liste d'exportation valide, où les répertoires /usr et /exports sont des systèmes de fichiers locaux:

```
# Exporte src et ports vers client01 et client02, mais seul
# client01 dispose des privilèges root dessus
/usr/src /usr/ports -maproot=root    client01
/usr/src /usr/ports               client02
# Les machines clientes ont les privilèges root et peuvent monter tout
# de /exports.  N'importe qui peut monter en lecture seule
# /exports/obj
```

```
/exports -alldirs -maproot=root      client01 client02
/exports/obj -ro
```

Le "daemon"mountd doit être forcé de relire le fichier /etc/exports à chacune de ses modifications, afin que les changements puissent prendre effet. Cela peut être effectué soit en envoyant un signal HUP au "daemon":

```
# kill -HUP `cat /var/run/mountd.pid`
```

soit en invoquant la procédure rc(8) de `mountd` avec le paramètre approprié:

```
# /etc/rc.d/mountd onereload
```

Veuillez consulter la Utilisation du système rc sous FreeBSD pour plus d'information sur l'utilisation des procédures rc.

De plus, un redémarrage permettra à FreeBSD de tout configurer proprement. Un redémarrage n'est cependant pas nécessaire. Exécuter les commandes suivantes en tant que `root` devrait mettre en place ce qui est nécessaire.

Sur le serveur NFS:

```
# rpcbind
# nfsd -u -t -n 4
# mountd -r
```

Sur le client NFS:

```
# nfsiod -n 4
```

Maintenant il devrait être possible de monter un système de fichiers distant. Dans nos exemples le nom du serveur sera `serveur` et le nom du client `client`. Si vous voulez monter temporairement un système de fichiers distant ou vous voulez simplement tester la configuration, exécutez juste une commande comme celle-ci en tant que `root` sur le client:

```
# mount serveur:/home /mnt
```

Cela montera le répertoire /home situé sur le serveur au point /mnt sur le client. Si tout est correctement configuré vous devriez être en mesure d'entrer dans le répertoire /mnt sur le client et de voir tous les fichiers qui sont sur le serveur.

Si vous désirez monter automatiquement un système de fichiers distant à chaque démarrage de l'ordinateur, ajoutez le système de fichiers au fichier /etc/fstab. Voici un exemple:

```
server:/home    /mnt    nfs rw  0   0
```

La page de manuel fstab(5) liste toutes les options disponibles.

31.3.3. Verrouillage

Certaines applications (par exemple mutt) ont besoin du verrouillage des fichiers pour fonctionner correctement. Dans le cas du NFS, rpc.lockd peut être utilisé pour assurer le verrouillage des fichiers. Pour l'activer, ajouter ce qui suit au fichier /etc/rc.conf sur les machines clientes et serveur (on suppose que les clients et le serveur NFS sont déjà configurés):

```
rpc_lockd_enable="YES"
rpc_statd_enable="YES"
```

Lancez l'application en utilisant:

```
# /etc/rc.d/nfslocking start
```

Si un verrouillage réel n'est pas nécessaire entre les clients et le serveur NFS, il est possible de laisser le client NFS effectuer le verrouillage localement en passant l'option `-L` à mount_nfs(8). Veuillez vous référer à la page de manuel mount_nfs(8) pour de plus amples détails.

31.3.4. Exemples pratiques d'utilisation

Il existe de nombreuses applications pratiques de NFS. Les plus communes sont présentés ci-dessous:

- Configurer plusieurs machines pour partager un CDROM ou un autre médium. C'est moins cher et souvent une méthode plus pratique pour installer des logiciels sur de multiples machines.
- Sur les réseaux importants, il peut être plus pratique de configurer un serveur NFS central sur lequel tous les répertoires utilisateurs sont stockés. Ces répertoires utilisateurs peuvent alors être exportés vers le réseau, les utilisateurs devraient alors toujours avoir le même répertoire utilisateur indépendamment de la station de travail sur laquelle ils ouvrent une session.
- Plusieurs machines pourront avoir un répertoire /usr/ports/distfiles commun. De cette manière, quand vous avez besoin d'installer un logiciel porté sur plusieurs machines, vous pouvez accéder rapidement aux sources sans les télécharger sur chaque machine.

31.3.5. Montages automatiques avec amd

amd(8) ("automatic mounter daemon"-"daemon" de montage automatique) monte automatiquement un système de fichiers distant dès que l'on accède à un fichier ou un répertoire contenu par ce système de fichiers. Les systèmes de fichiers qui sont inactifs pendant une certaine période seront automatiquement démontés par amd. L'utilisation d'amd offre une alternative simple aux montages permanents qui sont généralement listés dans /etc/fstab.

amd opère en s'attachant comme un serveur NFS aux répertoires /host et /net. Quand on accède à un fichier à l'intérieur de ces répertoires, amd recherche le montage distant correspondant et le monte automatiquement. /net est utilisé pour monter un système de fichiers exporté à partir d'une adresse IP, alors que /host est utilisé pour monter un système de fichiers exporté à partir d'un nom de machine distant.

Un accès à un fichier dans /host/foobar/usr demandera à amd de tenter de monter l'export /usr sur la machine `foobar`.

Exemple 41. Monter un systèmes de fichiers exporté avec amd

Vous pouvez voir les systèmes de fichiers exportés par une machine distante avec la commande `showmount`. Par exemple, pour voir les répertoires exportés par une machine appelée `foobar`, vous pouvez utiliser:

```
% showmount -e foobar
Exports list on foobar:
/usr                               10.10.10.0
/a                                 10.10.10.0
% cd /host/foobar/usr
```

Comme on le voit dans l'exemple, `showmount` liste /usr comme une exportation. Quand on change de répertoire pour /host/foobar/usr, amd tente de résoudre le nom de machine `foobar` et de monter automatiquement le système exporté désiré.

amd peut être lancé par les procédures de démarrage en ajoutant les lignes suivantes dans le fichier /etc/rc.conf:

```
amd_enable="YES"
```

De plus, des paramètres peuvent être passés à amd à l'aide de l'option `amd_flags`. Par défaut, l'option `amd_flags` est possitionnée à:

```
amd_flags="-a /.amd_mnt -l syslog /host /etc/amd.map /net /etc/amd.map"
```

Le fichier /etc/amd.map définit les options par défaut avec lesquelles les systèmes exportés sont montés. Le fichier /etc/amd.conf définit certaines des fonctionnalités les plus avancées de amd.

Consultez les pages de manuel de amd(8) et amd.conf(8) pour plus d'informations.

31.3.6. Problèmes d'intégration avec d'autres systèmes

Certaines cartes Ethernet ISA présentent des limitations qui peuvent poser de sérieux problèmes sur un réseau, en particulier avec NFS. Ce n'est pas une particularité de FreeBSD, mais FreeBSD en est également affecté.

Ce problème se produit pratiquement à chaque fois que des systèmes (FreeBSD) PC sont sur le même réseau que des stations de travail très performantes, comme celles de Silicon Graphics, Inc. et Sun Microsystems, Inc. Les montages NFS se feront sans difficulté, et certaines opérations pourront réussir, puis soudain le serveur semblera ne plus répondre au client, bien que les requêtes vers ou en provenance d'autres systèmes continueront à être traitées normalement. Cela se manifeste sur la machine cliente, que ce soit le système FreeBSD ou la station de travail. Sur de nombreux systèmes, il n'est pas possible d'arrêter le client proprement une fois que ce problème apparaît. La seule solution est souvent de réinitialiser le client parce que le problème NFS ne peut être résolu.

Bien que la solution "correcte" est d'installer une carte Ethernet plus performante et de plus grande capacité sur le système FreeBSD, il existe une solution simple qui donnera satisfaction. Si le système FreeBSD est le *serveur*, ajoutez l'option `-w=1024` lors du montage sur le client. Si le système FreeBSD est le *client*, alors montez le système de fichiers NFS avec l'option `-r=1024`. Ces options peuvent être spécifiées dans le quatrième champ de l'entrée fstab sur le client pour les montages automatiques, ou en utilisant le paramètre `-o` de la commande mount(8) pour les montages manuels.

Il faut noter qu'il existe un problème différent, que l'on confond parfois avec le précédent, qui peut se produire lorsque les serveurs et les clients NFS sont sur des réseaux différents. Si c'est le cas, *assurez-vous* que vos routeurs transmettent bien les informations UDP nécessaires, ou vous n'irez nulle part, quoi que vous fassiez par ailleurs.

Dans les exemples suivants, `fastws` est le nom de la station de travail (interface) performante, et `freebox` celui d'une machine (interface) FreeBSD avec une carte Ethernet moins performante. /sharedfs est le système de fichiers NFS qui sera exporté (consulter la page de manuel exports(5)), et /project sera le point de montage sur le client pour le système de fichiers exporté. Dans tous les cas, des options supplémentaires, telles que `hard soft` et `bg` seront peut-être nécessaires pour vos applications.

Exemple d'extrait du fichier /etc/fstab sur `freebox` quand le système FreeBSD (`freebox`) est le client:

```
fastws:/sharedfs /project nfs rw,-r=1024 0 0
```

Commande de montage manuelle sur `freebox`:

```
# mount -t nfs -o -r=1024 fastws:/sharedfs /project
```

Exemple d'extrait du fichier /etc/fstab sur `fastws` quand le système FreeBSD est le serveur:

```
freebox:/sharedfs /project nfs rw,-w=1024 0 0
```

Commande de montage manuelle sur `fastws`:

```
# mount -t nfs -o -w=1024 freebox:/sharedfs /project
```

Presque n'importe quelle carte Ethernet 16 bits permettra d'opérer sans l'utilisation des paramètres restrictifs précédents sur les tailles des tampons de lecture et d'écriture.

Pour ceux que cela intéresse, voici ce qui se passe quand le problème survient, ce qui explique également pourquoi ce n'est pas récupérable. NFS travaille généralement avec une taille de "bloc" de 8 k (bien qu'il arrive qu'il les fragmente en de plus petits morceaux). Comme la taille maximale d'un paquet Ethernet est de 1500 octets, le "bloc" NFS est divisé en plusieurs paquets Ethernet, bien qu'il soit toujours vu comme quelque chose d'unitaire par les couches supérieures du code, et doit être réceptionné, assemblé, et *acquitté* comme tel. Les stations de travail performantes peuvent traiter les paquets qui composent le bloc NFS les uns après les autres, pratiquement aussi rapidement que le standard le permet. Sur les cartes les plus petites, de moindre capacité, les derniers paquets d'un même bloc écrasent les paquets précédents avant qu'ils aient pu être transmis à la machine et le bloc ne peut être réassemblé ou acquitté. Avec pour conséquence, le dépassement du délai d'attente sur la station de travail qui recommence alors la transmission, mais en renvoyant l'intégralité des 8 K, et ce processus se répète à l'infini.

En définissant la taille de bloc inférieure à la taille d'un paquet Ethernet, nous nous assurons que chaque paquet Ethernet complet sera acquitté individuellement, évitant ainsi la situation de blocage.

Des écrasements peuvent toujours survenir quand des stations de travail performantes surchargent un système PC de données, mais avec de meilleures cartes, de tels écrasements ne sont pas systématiques pour les "blocs" NFS. Quand un écrasement apparaît, les blocs affectés sont retransmis, et ils y a de fortes chances pour qu'ils soient reçus, assemblés et acquittés.

31.4. Services d'information réseau (NIS/YP)

31.4.1. Qu'est-ce que c'est?

NIS, qui signifie "Network Information Services" (services d'information réseau), fut développé par Sun Microsystems pour centraliser l'administration de systèmes UNIX® (à l'origine SunOS™). C'est devenu aujourd'hui un standard industriel; tous les systèmes importants de type UNIX® (Solaris™, HP-UX, AIX®, Linux, NetBSD, OpenBSD, FreeBSD, etc.) supportent NIS.

NIS était appelé au départ "Yellow Pages" (page jaunes), mais étant donné que c'était marque déposée, Sun changea le nom. L'ancienne appelation (et yp) est toujours rencontrée et utilisée.

C'est un système client/serveur basé sur les RPCs qui permet à un groupe de machines d'un domaine NIS de partager un ensemble de fichiers de configuration communs. Cela permet à un administrateur système de mettre en place des clients NIS avec un minimum de configuration et d'ajouter, modifier ou supprimer les informations de configuration à partir d'un unique emplacement.

C'est similaire au système de domaine Windows NT®; bien que l'implémentation interne des deux n'est pas du tout identique, les fonctionnalités de base sont comparables.

31.4.2. Termes/processus à connaître

Il existe plusieurs termes et processus utilisateurs que vous rencontrerez lors de la configuration de

NIS sous FreeBSD, que vous vouliez mettre en place un serveur NIS ou un client NIS:

Terme	Description
Nom de domaine NIS	Un serveur maître NIS et tous ses clients (y compris ses serveurs esclaves) ont un domaine NIS. Similaire au nom de domaine Windows NT®, le nom de domaine NIS n'a rien à voir avec le système DNS.
rpcbind	Doit tourner afin d'activer les RPC (Remote Procedure Call, appel de procédures distantes, un protocole réseau utilisé par NIS). Si rpcbind ne tourne pas, il sera impossible de faire fonctionner un serveur NIS, ou jouer le rôle d'un client NIS.
ypbind	Fait pointer un client NIS vers son serveur NIS. Il récupérera le nom de domaine NIS auprès du système, et en utilisant les RPC, se connectera au serveur. ypbind est le coeur de la communication client-serveur dans un environnement NIS; si ypbind meurt sur une machine cliente, elle ne sera pas en mesure d'accéder au serveur NIS.
ypserv	Ne devrait tourner que sur les serveurs NIS, c'est le processus serveur en lui-même. Si ypserv(8) meurt, alors le serveur ne pourra plus répondre aux requêtes NIS (avec un peu de chance, un serveur esclave prendra la relève). Il existe des implémentations de NIS (mais ce n'est pas le cas de celle de FreeBSD), qui n'essayent pas de se reconnecter à un autre serveur si le serveur utilisé précédemment meurt. Souvent, la seule solution dans ce cas est de relancer le processus serveur (ou même redémarrer le serveur) ou le processus ypbind sur le client.
rpc.yppasswdd	Un autre processus qui ne devrait tourner que sur les serveurs maître NIS; c'est un "daemon" qui permettra aux clients de modifier leur mot de passe NIS. Si ce "daemon" ne tourne pas, les utilisateurs devront ouvrir une session sur le serveur maître NIS et y changer à cet endroit leur mot de passe.

31.4.3. Comment cela fonctionne-t-il?

Dans un environnement NIS il y a trois types de machines: les serveurs maîtres, les serveurs esclaves et les clients. Les serveurs centralisent les informations de configuration des machines. Les

serveurs maîtres détiennent l'exemplaire de référence de ces informations, tandis que les serveurs esclaves en ont un double pour assurer la redondance. Les clients attendent des serveurs qu'ils leur fournissent ces informations.

Le contenu de nombreux fichiers peut être partagé de cette manière. Les fichiers master.passwd, group, et hosts sont fréquemment partagés par l'intermédiaire de NIS. A chaque fois qu'un processus d'une machine cliente a besoin d'une information qu'il trouverait normalement localement dans un de ces fichiers, il émet une requête au serveur NIS auquel il est rattaché pour obtenir cette information.

31.4.3.1. Type de machine

- Un *serveur NIS maître*. Ce serveur, analogue à un contrôleur de domaine Windows NT® primaire, gère les fichiers utilisés par tous les clients NIS. Les fichiers passwd, group, et les autres fichiers utilisés par les clients NIS résident sur le serveur maître.

Il est possible pour une machine d'être un serveur NIS maître pour plus qu'un domaine NIS. Cependant, ce cas ne sera pas abordé dans cette introduction, qui suppose un environnement NIS relativement petit.

- *Serveurs NIS esclaves*. Similaire aux contrôleurs de domaine Windows NT® de secours, les serveurs NIS esclaves possèdent une copie des fichiers du serveur NIS maître. Les serveurs NIS esclaves fournissent la redondance nécessaire dans les environnements importants. Ils aident également à à la répartition de la charge du serveur maître: les clients NIS s'attachent toujours au serveur NIS dont ils reçoivent la réponse en premier, y compris si c'est la réponse d'un serveur esclave.
- *Clients NIS*. Les clients NIS, comme la plupart des stations de travail Windows NT®, s'identifient auprès du serveur NIS (ou le contrôleur de domaine Windows NT® dans le cas de stations de travail Windows NT®) pour l'ouverture de sessions.

31.4.4. Utiliser NIS/YP

Cette section traitera de la configuration d'un exemple d'environnement NIS.

31.4.4.1. Planification

Supposons que vous êtes l'administrateur d'un petit laboratoire universitaire. Ce laboratoire dispose de 15 machines FreeBSD, et ne possède pas actuellement de point central d'administration; chaque machine a ses propres fichiers /etc/passwd et /etc/master.passwd. Ces fichiers sont maintenus à jour entre eux grâce à des interventions manuelles; actuellement quand vous ajoutez un utilisateur pour le laboratoire, vous devez exécuter `adduser` sur les 15 machines. Cela doit changer, vous avez donc décidé de convertir le laboratoire à l'utilisation de NIS en utilisant deux machines comme serveurs.

La configuration du laboratoire ressemble à quelque chose comme:

Nom de machine	Adresse IP	Rôle de la machine
`ellington`	`10.0.0.2`	Maître NIS

Nom de machine	Adresse IP	Rôle de la machine
coltrane	10.0.0.3	Esclave NIS
basie	10.0.0.4	Station de travail
bird	10.0.0.5	Machine cliente
cli[1-11]	10.0.0.[6-17]	Autres machines clientes

Si vous mettez en place un système NIS pour la première fois, c'est une bonne idée de penser à ce que vous voulez en faire. Peu importe la taille de votre réseau, il y a quelques décisions à prendre.

31.4.4.1.1. Choisir un nom de domaine NIS

Ce n'est pas le "nom de domaine" dont vous avez l'habitude. Il est plus exactement appelé "nom de domaine NIS". Quand un client diffuse des requêtes pour obtenir des informations, il y inclut le nom de domaine NIS auquel il appartient. C'est ainsi que plusieurs serveurs d'un même réseau peuvent savoir lequel d'entre eux doit répondre aux différentes requêtes. Pensez au nom de domaine NIS comme le nom d'un groupe de machines qui sont reliées entre elles.

Certains choisissent d'utiliser leur nom de domaine Internet pour nom de domaine NIS. Ce n'est pas conseillé parce que c'est une source de confusion quand il faut résoudre un problème réseau. Le nom de domaine NIS devrait être unique sur votre réseau et est utile s'il décrit le groupe de machines qu'il représente. Par exemple, le département artistique de Acme Inc. pourrait avoir "acme-art" comme nom de domaine NIS. Pour notre exemple, nous supposerons que vous avez choisi le nom *test-domain*.

Cependant, certains systèmes d'exploitation (notamment SunOS™) utilisent leur nom de domaine NIS pour nom de domaine Internet. Si une ou plusieurs machines sur votre réseau présentent cette restriction, vous *devez* utiliser votre nom de domaine Internet pour nom de domaine NIS.

31.4.4.1.2. Contraintes au niveau du serveur

Il y a plusieurs choses à garder à l'esprit quand on choisit une machine destinée à être un serveur NIS. Un des problèmes du NIS est le degré de dépendance des clients vis à vis du serveur. Si un client ne peut contacter le serveur de son domaine NIS, la plupart du temps la machine n'est plus utilisable. L'absence d'information sur les utilisateurs et les groupes bloque la plupart des systèmes. Vous devez donc vous assurer de choisir une machine qui ne sera pas redémarré fréquemment, ni utilisée pour du développement. Idéalement, le serveur NIS devrait être une machine dont l'unique utilisation serait d'être un serveur NIS. Si vous avez un réseau qui n'est pas très chargé, il peut être envisagé de mettre le serveur NIS sur une machine fournissant d'autres services, gardez juste à l'esprit que si le serveur NIS n'est pas disponible à un instant donné, cela affectera *tous* vos clients NIS.

31.4.4.2. Serveurs NIS

La copie de référence de toutes les informations NIS est stockée sur une seule machine appelée serveur NIS maître. Les bases de données utilisées pour le stockage de ces informations sont appelées tables NIS ("NIS maps"). Sous FreeBSD ces tables se trouvent dans /var/yp/[domainname] où [domainname] est le nom du domaine NIS concerné. Un seul serveur NIS peut gérer plusieurs domaines à la fois, il peut donc y avoir plusieurs de ces répertoires, un pour chaque domaine.

Chaque domaine aura son propre jeu de tables.

Les serveurs NIS maîtres et esclaves traitent toutes les requêtes NIS à l'aide du "daemon" ypserv. ypserv reçoit les requêtes des clients NIS, traduit le nom de domaine et le nom de table demandés en chemin d'accès à la base de données correspondante et transmet l'information de la base de données au client.

31.4.4.2.1. Configurer un serveur NIS maître

Selon vos besoins, la configuration d'un serveur NIS maître peut être relativement simple. FreeBSD offre par défaut un support direct du NIS. Tout ce dont vous avez besoin est d'ajouter les lignes qui suivent au fichier /etc/rc.conf, et FreeBSD s'occupera du reste pour vous.

```
nisdomainname="test-domain"
```

1. Cette ligne définie le nom de domaine NIS, `test-domain`, à la configuration du réseau (e.g. au démarrage).

   ```
   nis_server_enable="YES"
   ```

2. Demandera à FreeBSD de lancer les processus du serveur NIS dès que le réseau est en fonctionnement.

   ```
   nis_yppasswdd_enable="YES"
   ```

3. Ceci activera le "daemon" rpc.yppasswdd, qui, comme mentionné précedement, permettra aux utilisateurs de modifier leur mot de passe à partir d'une machine cliente.

Selon votre configuration NIS, vous aurez peut-être à ajouter des entrées supplémentaires. Consultez la section sur les serveurs NIS qui sont également des clients NIS, plus bas, pour plus de détails.

Maintenant, tout ce que vous devez faire est d'exécuter la commande `/etc/netstart` en tant que super-utilisateur. Elle configurera tout en utilisant les valeurs que vous avez définies dans /etc/rc.conf.

31.4.4.2.2. Initialisation des tables NIS

Les *tables NIS* sont des fichiers de base de données, qui sont conservés dans le répertoire /var/yp. Elles sont générées à partir des fichiers de configuration du répertoire /etc du serveur NIS maître, avec une exception: le fichier /etc/master.passwd. Et cela pour une bonne raison, vous ne voulez pas divulguer les mots de passe pour l'utilisateur `root` et autres comptes d'administration aux autres serveurs du domaine NIS. Par conséquent, avant d'initialiser les tables NIS, vous devrez faire:

```
# cp /etc/master.passwd /var/yp/master.passwd
  # cd /var/yp
  # vi master.passwd
```

Vous devrez effacer toutes les entrées concernant les comptes système (`bin`, `tty`, `kmem`, `games`, etc.), tout comme les comptes que vous ne désirez pas propager aux clients NIS (par exemple `root` et tout autre compte avec un UID 0 (super-utilisateur)).

Assurez-vous que le fichier /var/yp/master.passwd n'est pas lisible par son groupe ou le reste du monde (mode 600)! Utilisez la commande `chmod` si nécessaire.

Cela achevé, il est temps d'initialiser les tables NIS! FreeBSD dispose d'une procédure appelée `ypinit` pour le faire à votre place (consultez sa page de manuel pour plus d'informations). Notez que cette procédure est disponible sur la plupart des systèmes d'exploitation du type UNIX®, mais pas tous. Sur Digital UNIX/Compaq Tru64 UNIX, elle est appelée `ypsetup`. Comme nous voulons générer les tables pour un maître NIS, nous passons l'option `-m` à `ypinit`. Pour générer les tables NIS, en supposant que vous avez effectué les étapes précédentes, lancez:

```
ellington# ypinit -m test-domain
Server Type: MASTER Domain: test-domain
Creating an YP server will require that you answer a few questions.
Questions will all be asked at the beginning of the procedure.
Do you want this procedure to quit on non-fatal errors? [y/n: n] n
Ok, please remember to go back and redo manually whatever fails.
If you don't, something might not work.
At this point, we have to construct a list of this domains YP servers.
rod.darktech.org is already known as master server.
Please continue to add any slave servers, one per line. When you are
done with the list, type a <control D>.
master server   :  ellington
next host to add:  coltrane
next host to add:  ^D
The current list of NIS servers looks like this:
ellington
coltrane
Is this correct?  [y/n: y] y

[..output from map generation..]

NIS Map update completed.
ellington has been setup as an YP master server without any errors.
```

`ypinit` devrait avoir créé /var/yp/Makefile à partir de /var/yp/Makefile.dist. Une fois créé, ce fichier suppose que vous être dans un environnement composé uniquement de machines FreeBSD et avec un seul serveur. Comme `test-domain` dispose également d'un serveur esclave, vous devez éditer /var/yp/Makefile:

```
ellington# vi /var/yp/Makefile
```

Vous devez commenter la ligne

```
NOPUSH = "True"
```

(si elle n'est pas déjà commentée).

31.4.4.2.3. Configurer un serveur NIS esclave

Configurer un serveur NIS esclave est encore plus simple que de configurer un serveur maître. Ouvrez une session sur le serveur esclave et éditez le fichier /etc/rc.conf comme précédemment. La seule différence est que nous devons maintenant utiliser l'option `-s` avec `ypinit`. L'option `-s` a besoin du nom du serveur NIS maître, donc notre ligne de commande ressemblera à:

```
coltrane# ypinit -s ellington test-domain

Server Type: SLAVE Domain: test-domain Master: ellington

Creating an YP server will require that you answer a few questions.
Questions will all be asked at the beginning of the procedure.

Do you want this procedure to quit on non-fatal errors? [y/n: n]  n

Ok, please remember to go back and redo manually whatever fails.
If you don't, something might not work.
There will be no further questions. The remainder of the procedure
should take a few minutes, to copy the databases from ellington.
Transferring netgroup...
ypxfr: Exiting: Map successfully transferred
Transferring netgroup.byuser...
ypxfr: Exiting: Map successfully transferred
Transferring netgroup.byhost...
ypxfr: Exiting: Map successfully transferred
Transferring master.passwd.byuid...
ypxfr: Exiting: Map successfully transferred
Transferring passwd.byuid...
ypxfr: Exiting: Map successfully transferred
Transferring passwd.byname...
ypxfr: Exiting: Map successfully transferred
Transferring group.bygid...
ypxfr: Exiting: Map successfully transferred
Transferring group.byname...
ypxfr: Exiting: Map successfully transferred
Transferring services.byname...
ypxfr: Exiting: Map successfully transferred
Transferring rpc.bynumber...
ypxfr: Exiting: Map successfully transferred
```

```
Transferring rpc.byname...
ypxfr: Exiting: Map successfully transferred
Transferring protocols.byname...
ypxfr: Exiting: Map successfully transferred
Transferring master.passwd.byname...
ypxfr: Exiting: Map successfully transferred
Transferring networks.byname...
ypxfr: Exiting: Map successfully transferred
Transferring networks.byaddr...
ypxfr: Exiting: Map successfully transferred
Transferring netid.byname...
ypxfr: Exiting: Map successfully transferred
Transferring hosts.byaddr...
ypxfr: Exiting: Map successfully transferred
Transferring protocols.bynumber...
ypxfr: Exiting: Map successfully transferred
Transferring ypservers...
ypxfr: Exiting: Map successfully transferred
Transferring hosts.byname...
ypxfr: Exiting: Map successfully transferred

coltrane has been setup as an YP slave server without any errors.
Don't forget to update map ypservers on ellington.
```

Vous devriez avoir un répertoire appelé /var/yp/test-domain. Des copies des tables du serveur NIS maître devraient se trouver dans ce répertoire. Vous devrez vous assurer que ces tables restent à jour. Les entrées suivantes dans /etc/crontab sur vos serveurs esclaves s'en chargeront:

```
20      *       *       *       *       root    /usr/libexec/ypxfr passwd.byname
21      *       *       *       *       root    /usr/libexec/ypxfr passwd.byuid
```

Ces deux lignes obligent le serveur esclave à synchroniser ses tables avec celles du serveur maître. Bien que ces entrées ne soient pas indispensables puisque le serveur maître essaye de s'assurer que toute modification de ses tables NIS soit répercutée à ses serveurs esclaves et comme l'information sur les mots de passe est vitale pour les systèmes qui dépendent du serveur, il est bon de forcer les mises à jour. C'est d'autant plus important sur les réseaux chargés où il n'est pas certain que les mises à jour soient intégrales.

Maintenant, exécutez la commande `/etc/netstart` sur le serveur esclave, ce qui lancera le serveur NIS.

31.4.4.3. Clients NIS

Un client NIS établit une connexion avec un serveur NIS donné par l'intermédiaire du "daemon" ypbind. ypbind consulte le nom de domaine par défaut du système (défini par la commande `domainname`), et commence à diffuser des requêtes RPC sur le réseau local. Ces requêtes précisent le nom de domaine auquel ypbind essaye de se rattacher. Si un serveur configuré pour ce domaine reçoit une des requêtes diffusées, il répond à ypbind, qui enregistrera l'adresse du serveur. S'il y a

plusieurs serveurs disponibles (un maître et plusieurs esclaves par example), ypbind utilisera l'adresse du premier à répondre. Dès lors, le système client dirigera toutes ses requêtes NIS vers ce serveur. ypbind enverra de temps en temps des requêtes "ping" au serveur pour s'assurer qu'il fonctionne toujours. S'il ne reçoit pas de réponse dans un laps de temps raisonnable, ypbind considérera ne plus être attaché au domaine et recommencera à diffuser des requêtes dans l'espoir de trouver un autre serveur.

31.4.4.3.1. Configurer un client NIS

Configurer une machine FreeBSD en client NIS est assez simple.

1. Editez le fichier /etc/rc.conf et ajoutez les lignes suivantes afin de définir le nom de domaine NIS et lancez ypbind au démarrage du réseau:

```
nisdomainname="test-domain"
nis_client_enable="YES"
```

2. Pour importer tous les mots de passe disponibles du serveur NIS, effacez tous les comptes utilisateur de votre fichier /etc/master.passwd et utilisez `vipw` pour ajouter la ligne suivante à la fin du fichier:

```
+::::::::::
```

Cette ligne permet à chaque utilisateur ayant un compte valide dans les tables de mots de passe du serveur d'avoir un compte sur le client. Il y a plusieurs façons de configurer votre client NIS en modifiant cette ligne. Consultez la section groupes réseau plus bas pour plus d'informations. Pour en savoir plus, reportez-vous à l'ouvrage `Managing NFS and NIS` de chez O'Reilly.

Vous devriez conservez au moins un compte local (i.e. non-importé via NIS) dans votre fichier /etc/master.passwd et ce compte devrait également être membre du groupe `wheel`. Si quelque chose se passe mal avec NIS, ce compte peut être utilisé pour ouvrir une session à distance, devenir `root`, et effectuer les corrections nécessaires.

3. Pour importer tous les groupes disponibles du serveur NIS, ajoutez cette ligne à votre fichier /etc/group:

```
+:*::
```

Une fois que c'est fait, vous devriez être en mesure d'exécuter `ypcat passwd` et voir la table des mots de passe du serveur NIS.

31.4.5. Sécurité du NIS

De façon générale, n'importe quel utilisateur distant peut émettre une requête RPC à destination de ypserv(8) et récupérer le contenu de vos tables NIS, en supposant que l'utilisateur distant connaisse votre nom de domaine. Pour éviter ces transactions non autorisées, ypserv(8) dispose d'une fonctionnalité appelée "securenets" qui peut être utilisée pour restreindre l'accès à un ensemble donné de machines. Au démarrage, ypserv(8) tentera de charger les informations sur les "securenets" à partir d'un fichier nommé /var/yp/securenets.

Ce chemin d'accès peut varier en fonction du chemin d'accès défini par l'option `-p`. Ce fichier contient des entrées sous la forme de définitions de réseau et d'un masque de sous-réseau séparé par une espace. Les lignes commençant par un "#" sont considérées comme des commentaires. Un exemple de fichier securenets peut ressembler à ceci:

```
# autorise les connexions depuis la machine locale -- obligatoire
127.0.0.1     255.255.255.255
# autorise les connexions de n'importe quelle machine
# du réseau 192.168.128.0
192.168.128.0 255.255.255.0
# autorise les connexions de n'importe quelle machine
# entre 10.0.0.0 et 10.0.15.255
# y compris les machines du laboratoire de test
10.0.0.0      255.255.240.0
```

Si ypserv(8) reçoit une requête d'une adresse qui satisfait à ces règles, il la traite normalement. Si une adresse ne correspond pas aux règles, la requête sera ignorée et un message d'avertissement sera enregistré. Si le fichier /var/yp/securenets n'existe pas, `ypserv` autorisera les connexions à partir de n'importe quelle machine.

Le programme `ypserv` supporte également l'outil TCP Wrapper de Wietse Venema. Cela permet à l'administrateur d'utiliser les fichiers de configuration de TCP Wrapper pour contrôler les accès à la place de /var/yp/securenets.

Bien que ces deux mécanismes de contrôle d'accès offrent une certaine sécurité, il sont, de même que le test du port privilégié, vulnérables aux attaques par "usurpation" d'adresses. Tout le trafic relatif à NIS devrait être bloqué par votre coupe-feu.

Les serveurs utilisant /var/yp/securenets pourront échouer à traiter les requêtes de clients NIS légitimes avec des implémentation TCP/IP archaïques. Certaines de ces implémentations positionnent à zéro les bits de la partie machine de l'adresse IP lors de diffusions et/ou sont incapables respecter le masque de sous-réseau lors du calcul de l'adresse de diffusion. Alors que certains de ces problèmes peuvent être corrigés en modifiant la configuration du client, d'autres problèmes peuvent forcer le retrait des systèmes clients fautifs ou l'abandon de /var/yp/securenets.

Utiliser /var/yp/securenets sur un serveur avec une implémentation TCP/IP

> archaïque est une mauvaise idée et sera à l'origine de pertes de la fonctionnalité NIS pour une grande partie de votre réseau.
>
> L'utilisation du système TCP Wrapper augmente les temps de latence de votre serveur NIS. Le délai supplémentaire peut être suffisamment long pour dépasser le délai d'attente des programmes clients, tout particulièrement sur des réseaux chargés ou avec des serveurs NIS lents. Si un ou plusieurs de vos systèmes clients souffrent de ces symptômes, vous devrez convertir les systèmes clients en question en serveurs esclaves NIS et les forcer à se rattacher à eux-mêmes.

31.4.6. Interdire l'accès à certains utilisateurs

Dans notre laboratoire, il y a une machine `basie` qui est supposée être une station de travail de la faculté. Nous ne voulons pas retirer cette machine du domaine NIS, le fichier passwd sur le serveur maître NIS contient les comptes pour la faculté et les étudiants. Que pouvons-nous faire?

Il existe une méthode pour interdire à certains utilisateurs d'ouvrir une session sur une machine, même s'ils sont présents dans la base de données NIS. Pour cela, tout ce dont vous avez besoin de faire est d'ajouter *-nom_utilisateur* à la fin du fichier /etc/master.passwd sur la machine cliente, où *nom_utilisateur* est le nom de l'utilisateur auquel vous désirez refuser l'accès. Ceci doit être fait de préférence avec `vipw`, puisque `vipw` contrôlera vos changements au fichier /etc/master.passwd, et régénérera automatiquement la base de données à la fin de l'édition. Par exemple, si nous voulions interdire l'ouverture de session à l'utilisateur `bill` sur la machine `basie` nous ferions:

```
basie# vipw
[add -bill to the end, exit]
vipw: rebuilding the database...
vipw: done

basie# cat /etc/master.passwd

root:[password]:0:0::0:0:The super-user:/root:/bin/csh
toor:[password]:0:0::0:0:The other super-user:/root:/bin/sh
daemon:*:1:1::0:0:Owner of many system processes:/root:/sbin/nologin
operator:*:2:5::0:0:System &:/:/sbin/nologin
bin:*:3:7::0:0:Binaries Commands and Source,,,:/:/sbin/nologin
tty:*:4:65533::0:0:Tty Sandbox:/:/sbin/nologin
kmem:*:5:65533::0:0:KMem Sandbox:/:/sbin/nologin
games:*:7:13::0:0:Games pseudo-user:/usr/games:/sbin/nologin
news:*:8:8::0:0:News Subsystem:/:/sbin/nologin
man:*:9:9::0:0:Mister Man Pages:/usr/shared/man:/sbin/nologin
bind:*:53:53::0:0:Bind Sandbox:/:/sbin/nologin
uucp:*:66:66::0:0:UUCP pseudo-user:/var/spool/uucppublic:/usr/libexec/uucp/uucico
xten:*:67:67::0:0:X-10 daemon:/usr/local/xten:/sbin/nologin
pop:*:68:6::0:0:Post Office Owner:/nonexistent:/sbin/nologin
nobody:*:65534:65534::0:0:Unprivileged user:/nonexistent:/sbin/nologin
+:::::::::
-bill
```

```
basie#
```

31.4.7. Utiliser les groupes réseau ("netgroups")

La méthode présentée dans la section précédente fonctionne relativement bien si vous avez besoin de règles spécifiques pour un petit nombre d'utilisateurs et/ou de machines. Sur les réseaux plus important, vous *oublierez* d'interdire l'accès aux machines sensibles à certains utilisateurs, ou vous devrez même modifier chaque machine séparément, perdant par là même les avantages du NIS: l'administration *centralisée*.

La solution des développeurs du NIS pour ce problème est appelé *groupes réseau* ("netgroups"). Leur objet et définition peuvent être comparés aux groupes utilisés par les systèmes UNIX®. La principale différence étant l'absence d'identifiants (ID) numériques et la capacité de définir un groupe réseau à l'aide de comptes utilisateur et d'autres groupes réseau.

Les groupes réseau furent développés pour gérer des réseaux importants et complexes avec des centaines de machines et d'utilisateurs. C'est une bonne option si vous êtes forcés de faire avec une telle situation. Cependant leur complexité rend impossible une explication avec des exemples simples. L'exemple utilisé dans le reste de cette section met en évidence ce problème.

Supposons que l'introduction avec succès de NIS dans votre laboratoire a retenu l'attention de vos supérieurs. Votre mission suivante est d'étendre la couverture de votre domaine NIS à d'autres machines sur le campus. Les deux tables contiennent les noms des nouveaux utilisateurs et des nouvelles machines ainsi qu'une courte description de chacun.

Nom(s) d'utilisateurs	Description
`alpha`, `beta`	Les employés du département IT ("Information Technology")
`charlie`, `delta`	Les nouveaux apprentis du département IT
`echo`, `foxtrott`, `golf`, ...	Les employés ordinaires
`able`, `baker`, ...	Les internes actuels

Nom(s) de machines	Description
`war`, `death`, `famine`, `pollution`	Vos serveurs les plus importants. Seuls les employés du département IT sont autorisés à ouvrir des sessions sur ces machines.
`pride`, `greed`, `envy`, `wrath`, `lust`, `sloth`	Serveurs moins importants. Tous les membres du laboratoire IT sont autorisés à ouvrir des sessions sur ces machines.
`one`, `two`, `three`, `four`, ...	Stations de travail ordinaires. Seuls les employés *réels* sont autorisés à utiliser ces machines.
`trashcan`	Une très vielle machine sans données sensibles. Même les internes peuvent utiliser cette machine.

Si vous avez essayé d'implémenter ces restrictions en bloquant séparément chaque utilisateur, vous avez dû ajouter une ligne `-utilisateur` à chaque fichier passwd de chaque système pour chaque utilisateur non-autorisé à ouvrir une session sur le système. Si vous omettez ne serait-ce qu'une entrée, vous aurez des problèmes. Il doit être possible de faire cela lors de la configuration initiale, cependant vous *finirez* par oublier d'ajouter les lignes pour de nouveaux utilisateurs lors d'opérations quotidiennes. Après tout, Murphy était quelqu'un d'optimiste.

Traiter cette situation avec les groupes réseau présente plusieurs avantages. Chaque utilisateur n'a pas besoin d'être traité séparément; vous assignez un utilisateur à un ou plusieurs groupes réseau et autorisez ou refusez l'ouverture de session à tous les membres du groupe réseau. Si vous ajoutez une nouvelle machine, vous n'aurez à définir les restrictions d'ouverture de session que pour les groupes réseau. Ces modifications sont indépendantes les unes des autres, plus de "pour chaque combinaison d'utilisateur et de machine faire..." Si votre configuration NIS est réfléchie, vous n'aurez à modifier qu'une configuration centrale pour autoriser ou refuser l'accès aux machines.

La première étape est l'initialisation de la table NIS du groupe réseau. La version FreeBSD d'ypinit(8) ne crée pas de table par défaut, mais son implémentation NIS la supportera une fois créée. Pour créer une table vide, tapez simplement

```
ellington# vi /var/yp/netgroup
```

et commencez à ajouter du contenu. Pour notre exemple, nous avons besoin de quatre groupes réseau: les employées du département IT, les apprentis du département IT, les employés normaux et les internes.

```
IT_EMP  (,alpha,test-domain)    (,beta,test-domain)
IT_APP  (,charlie,test-domain)  (,delta,test-domain)
USERS   (,echo,test-domain)     (,foxtrott,test-domain) \
        (,golf,test-domain)
INTERNS (,able,test-domain)     (,baker,test-domain)
```

`IT_EMP`, `IT_APP` etc. sont les noms des groupes réseau. Chaque groupement entre parenthèses ajoute un ou plusieurs comptes utilisateurs aux groupes. Les trois champs dans un groupement sont:

1. Le nom de la/les machine(s) où les éléments suivants sont valides. Si vous ne précisez pas un nom de machine, l'entrée est valide sur toutes les machines. Si vous précisez un nom de machine, vous pénétrerez dans un royaume obscure, d'horreur et de confusion totale.
2. Le nom du compte qui appartient au groupe réseau.
3. Le domaine NIS pour le compte. Vous pouvez importer les comptes d'autres domaines NIS dans votre groupe réseau si vous êtes une de ces personnes malchanceuses avec plus d'un domaine NIS.

Chacun de ces champs peut contenir des jokers. Consultez la page de manuel netgroup(5) pour plus de détails.

Les noms de groupes réseau plus long que 8 caractères ne devraient pas être

> utilisés, tout particulièrement si vous avez des machines utilisant d'autres systèmes d'exploitation dans votre domaine NIS. Les noms sont sensibles à la casse des caractères; utiliser des majuscules pour vos noms de groupes réseau est une méthode simple pour distinguer les utilisateurs, les machines et les noms de groupes réseau.
>
> Certains clients NIS (autres que FreeBSD) ne peuvent gérer les groupes réseau avec un grand nombre d'entrées. Par exemple, certaines anciennes versions de SunOS™ commencent à causer des problèmes si un groupe réseau contient plus de 15 *entrées*. Vous pouvez contourner cette limite en créant plusieurs sous-groupes réseau avec 15 utilisateurs ou moins et un véritable groupe réseau constitué des sous-groupes réseau:
>
> ```
> BIGGRP1  (,joe1,domain)  (,joe2,domain)  (,joe3,domain) [...]
> BIGGRP2  (,joe16,domain)  (,joe17,domain) [...]
> BIGGRP3  (,joe31,domain)  (,joe32,domain)
> BIGGROUP  BIGGRP1 BIGGRP2 BIGGRP3
> ```
>
> Vous pouvez répéter ce processus si vous avez besoin de plus de 255 utilisateurs dans un seul groupe réseau.

Activer et propager votre nouvelle table NIS est simple:

```
ellington# cd /var/yp
ellington# make
```

Ceci générera les trois tables NIS netgroup, netgroup.byhost et netgroup.byuser. Utilisez ypcat(1) pour contrôler si vos nouvelles tables NIs sont disponibles:

```
ellington% ypcat -k netgroup
ellington% ypcat -k netgroup.byhost
ellington% ypcat -k netgroup.byuser
```

La sortie devrait être semblable au contenu de /var/yp/netgroup. La deuxième commande ne produira pas de sortie si vous n'avez pas précisé les groupes réseau spécifiques à une machine. La troisième commande peut être utilisée pour obtenir les listes des groupes réseau pour un utilisateur.

La configuration du client est plutôt simple. Pour configurer le serveur `war`, vous devez lancer vipw(8) et remplacer la ligne

```
+:::::::::
```

par

```
+@IT_EMP:::::::::
```

Maintenant, seules les données pour les utilisateurs définis dans le groupe réseau `IT_EMP` sont importées dans la base de données de mots de passe de `war` et seuls ces utilisateurs sont autorisés à ouvrir une session.

Malheureusement, cette limitation s'applique également à la fonction `~` de l'interpréteur de commandes et toutes les routines de conversion entre nom d'utilisateur et identifiant numérique d'utilisateur. En d'autres termes, `cd ~utilisateur` ne fonctionnera pas, et `ls -l` affichera l'ID numérique à la place du nom d'utilisateur et `find . -user joe -print` échouera avec le message d'erreur `No such user`. Pour corriger cela, vous devrez importer toutes les entrées d'utilisateurs *sans leur autoriser l'ouverture de session sur vos serveurs*.

Cela peut être fait en ajoutant une autre ligne au fichier /etc/master.passwd. Cette ligne devrait contenir:

`+:::::::::/sbin/nologin`, signifiant "Importer toutes les entrées mais remplacer l'interpréteur de commandes avec /sbin/nologin dans les entrées importées". Vous pouvez remplacer n'importe quel champ dans l'entrée `passwd` en plaçant une valeur par défaut dans votre fichier /etc/master.passwd.

Assurez-vous que `:::::::::/sbin/nologin` est placée après `@IT_EMP:::::::::`. Sinon, tous les comptes utilisateur importés du NIS auront /sbin/nologin comme interpréteur de commandes.

Après cette modification, vous ne devrez uniquement que modifier une des tables NIS si un nouvel employé rejoint le département IT. Vous pourrez utiliser une approche similaire pour les serveurs moins importants en remplaçant l'ancienne ligne `+:::::::::` dans leur version locale de /etc/master.passwd avec quelque chose de semblable à ceci:

```
+@IT_EMP:::::::::
+@IT_APP:::::::::
+:::::::::/sbin/nologin
```

Les lignes correspondantes pour les stations de travail normales seraient:

```
+@IT_EMP:::::::::
+@USERS:::::::::
+:::::::::/sbin/nologin
```

Tout était parfait jusqu'au changement de politique quelques semaines plus tard: le département IT commença à engager des internes. Les internes du département IT sont autorisés à utiliser les stations de travail normales et les serveurs les moins importants; les apprentis du département IT sont autorisés à ouvrir des sessions sur les serveurs principaux. Vous ajoutez alors un nouveau groupe réseau `IT_INTERN`, ajoutez les nouveaux internes IT à ce groupe réseau et commencez à modifier la configuration sur chaque machine... Comme disait l'ancien: "Erreurs dans la planification centralisée mènent à un désordre général".

La capacité de NIS à créer des groupes réseau à partir d'autres groupes réseau peut être utilisée pour éviter de telles situations. Une possibilité est la création de groupes réseau basés sur le rôle du groupe. Par exemple vous pourriez créer un groupe réseau appelé `BIGSRV` pour définir les restrictions d'ouverture de session pour les serveurs importants, un autre groupe réseau appelé `SMALLSRV` pour les serveurs moins importants et un troisième groupe réseau nommé `USERBOX` pour les stations de travail normales. Chacun de ces groupes réseau contient les groupes réseau autorisés à ouvrir des sessions sur ces machines. Les nouvelles entrées pour la table NIS de groupes réseau devrait ressembler à ceci:

```
BIGSRV    IT_EMP  IT_APP
SMALLSRV  IT_EMP  IT_APP  ITINTERN
USERBOX   IT_EMP  ITINTERN USERS
```

Cette méthode qui consiste à définir des restrictions d'ouverture de session fonctionne relativement bien si vous pouvez définir des groupes de machines avec des restrictions identiques. Malheureusement, ceci est une exception et pas une généralité. La plupart du temps, vous aurez besoin de définir des restrictions d'ouverture de session par machine.

La définition de groupes réseau spécifiques aux machines est une autre possibilité pour traiter la modification de politique soulignée précédemment. Dans ce scénario, le fichier /etc/master.passwd de chaque machine contient deux lignes débutant par "+". La première ajoute un groupe réseau avec les comptes autorisés à ouvrir une session sur cette machine, la seconde ajoute tous les comptes avec l'interpréteur de commandes /sbin/nologin. C'est une bonne idée d'utiliser des majuscules pour le nom de la machine ainsi que celui du groupe réseau. Dans d'autres termes, les lignes en question devraient être semblables à:

```
+@NOMMACHINE:::::::::
+:::::::::/sbin/nologin
```

Une fois cette tâche achevée pour toutes vos machines, vous n'aurez plus jamais à modifier les versions locales du fichier /etc/master.passwd. Tous les changements futurs peuvent être gérés en modifiant la table NIS. Voici un exemple d'une table de groupes réseau possible pour ce scénario avec quelques petits plus:

```
# Définir tout d'abord les groupes d'utilisateurs
IT_EMP    (,alpha,test-domain)    (,beta,test-domain)
IT_APP    (,charlie,test-domain)  (,delta,test-domain)
DEPT1     (,echo,test-domain)     (,foxtrott,test-domain)
DEPT2     (,golf,test-domain)     (,hotel,test-domain)
DEPT3     (,india,test-domain)    (,juliet,test-domain)
ITINTERN  (,kilo,test-domain)     (,lima,test-domain)
D_INTERNS (,able,test-domain)     (,baker,test-domain)
#
# Définir, maintenant, des groupes basés sur les rôles
USERS     DEPT1   DEPT2     DEPT3
BIGSRV    IT_EMP  IT_APP
SMALLSRV  IT_EMP  IT_APP    ITINTERN
```

```
USERBOX   IT_EMP  ITINTERN  USERS
#
# Et un groupe pour les tâches spéciales
# Permettre à echo et golf d'accéder à notre machine anti-virus
SECURITY  IT_EMP  (,echo,test-domain)  (,golf,test-domain)
#
# les groupes réseau basés sur un ensemble de machines
# Nos principaux serveurs
WAR       BIGSRV
FAMINE    BIGSRV
# L'utilisateur india a besoin d'un accès à ce serveur
POLLUTION  BIGSRV  (,india,test-domain)
#
# Celle-ci est très importante et nécessite plus de restrictions d'accès
DEATH     IT_EMP
#
# La machine anti-virus mentionnée précédemment
ONE       SECURITY
#
# Restreindre l'accès à une machine à un seul utilisateur
TWO       (,hotel,test-domain)
# [...d'autres groupes suivent]
```

Si vous utilisez une sorte de base de données pour gérer vos comptes utilisateur, vous devriez pouvoir créer la première partie de la table avec les outils de votre base de données. De cette façon, les nouveaux utilisateurs auront automatiquement accès aux machines.

Dernier avertissement: il n'est pas toujours conseillé d'utiliser des groupes réseau basés sur les machines. Si vous déployez quelques douzaines ou même centaines de machines identiques pour des laboratoires pour étudiants, vous devriez utiliser des groupes basés sur les types d'utilisateurs plutôt que sur les machines pour conserver la taille de la table NIS dans des limites raisonnables.

31.4.8. Les choses importantes à ne pas oublier

Il y a un certain nombre de choses que vous devrez effectuer différemment maintenant que vous êtes dans un environnement NIS.

- A chaque fois que vous désirez ajouter un utilisateur au laboratoire, vous devez l'ajouter *uniquement* sur le serveur NIS et *vous devez ne pas oublier de reconstruire les tables NIS*. Si vous oubliez de le faire, le nouvel utilisateur ne pourra pas ouvrir de session en dehors du serveur maître NIS. Par exemple, si nous devons ajouter au laboratoire un nouvel utilisateur `jsmith`, nous ferions:

  ```
  # pw useradd jsmith
  # cd /var/yp
  # make test-domain
  ```

  Vous pouvez lancer `adduser jsmith` à la place de `pw useradd jsmith`.

- *Conservez les comptes d'administration en dehors des tables NIS*. Vous ne voulez pas propager les comptes et mots de passe d'administration sur les machines qui auront des utilisateurs qui ne devraient pas avoir accès à ces comptes.
- *Sécurisez les serveurs maître et esclave NIS, et réduisez leur temps d'arrêt*. Si quelqu'un tente soit d'attaquer soit de simplement arrêter ces machines, de nombreuses personnes ne pourront plus ouvrir de session dans le laboratoire.

  C'est la principale faiblesse d'un système d'administration centralisée. Si vous ne protégez pas vos serveurs NIS, vous aurez à faire face à de nombreux utilisateurs mécontents!

31.4.9. Compatibilité NIS version 1

ypserv sous FreeBSD offre un support des clients NIS version 1. L'implémentation NIS de FreeBSD utilise uniquement le protocole NIS version 2, cependant d'autres implémentations disposent du support pour le protocole version 1 pour des raisons de compatibilité avec d'anciens systèmes. Les "daemons" ypbind fournis avec ces systèmes tenteront de s'attacher à un serveur NIS version 1 même s'ils n'en ont pas besoin (et ils pourront continuer à diffuser des requêtes pour en trouver un même après avoir reçu une réponse d'un serveur NIS version 2). Notez que bien que les requêtes des clients normaux soient supportées, cette version d'ypserv ne supporte pas les requêtes de transfert de tables version 1; par conséquent il n'est pas possible de l'utiliser comme serveur maître ou esclave avec des serveurs NIS plus anciens qui ne supportent que la version 1 du protocole. Heureusement, il n'y a, aujourd'hui, presque plus de serveurs de ce type actifs.

31.4.10. Serveurs NIS qui sont aussi des clients NIS

Il faut faire attention quand on utilise ypserv dans un domaine avec plusieurs serveurs NIS qui sont également des clients NIS. Il est en général préférable de forcer les serveurs de se rattacher à eux-mêmes plutôt que de les laisser diffuser des requêtes de rattachement et éventuellement se rattacher réciproquement les uns aux autres. Il peut en résulter de curieux problèmes si l'un des serveurs tombe et que d'autres en dépendent. Tous les clients finiront par dépasser leur délai d'attente et se tenteront de se rattacher à d'autres serveurs, mais ce délai peut être considérable et le problème persistera puisque les serveurs peuvent à nouveau se rattacher les uns aux autres.

Vous pouvez obliger une machine à se rattacher à un serveur particulier en exécutant `ypbind` avec l'option `-S`. Si vous ne désirez pas faire cela à la main à chaque fois que vous redémarrez votre serveur NIS, vous pouvez ajouter les lignes suivantes à votre fichier /etc/rc.conf:

```
nis_client_enable="YES" # run client stuff as well
nis_client_flags="-S NIS domain,server"
```

Voir la page de manuel de ypbind(8) pour plus d'informations.

31.4.11. Formats des mots de passe

Un des problèmes les plus courants que l'on rencontre en mettant en oeuvre NIS est celui de la compatibilité des formats de mots de passe. Si votre serveur NIS utilise des mots de passe chiffrés avec l'algorithme DES, il ne supportera que les clients utilisant également DES. Par exemple, si vous

avez des client NIS Solaris™ sur votre réseau, alors vous aurez presque certainement besoin d'utiliser des mots de passe chiffrés avec le système DES.

Pour déterminer quel format vos serveurs et clients utilisent, consultez le fichier /etc/login.conf. Si la machine est configurée pour utiliser des mots de passe chiffrés avec DES, alors la classe `default` contiendra une entrée comme celle-ci:

```
default:\
    :passwd_format=des:\
    :copyright=/etc/COPYRIGHT:\
    [Entrées suivantes omises]
```

D'autres valeurs possibles pour la capacité `passwd_format` sont `blf` et `md5` (respectivement pour les chiffrages de mots de passe Blowfish et MD5).

Si vous avez modifié le fichier /etc/login.conf, vous devrez également regénérer la base de données des capacités de classes de session, ce qui est accompli en exécutant la commande suivante en tant que `root`:

```
# cap_mkdb /etc/login.conf
```

Le format des mots de passe utilisés dans /etc/master.passwd ne sera pas mis à jour avant qu'un utilisateur ne change son mot de passe pour la première fois *après* la régénération de la base de données des capacités de classes de session.

Ensuite, afin de s'assurer que les mots de passe sont chiffrés avec le format que vous avez choisi, vous devez vérifier que l'entrée `crypt_default` dans le fichier /etc/auth.conf donne la priorité au format de mots de passe choisi. Par exemple, quand les mots de passe DES sont utilisés, l'entrée serait:

```
crypt_default   =   des blf md5
```

En suivant les points précédents sur chaque serveur et client NIS sous FreeBSD, vous pouvez être sûr qu'ils seront tous d'accord sur le format de mot de passe utilisé dans le réseau. Si vous avez des problèmes d'authentification sur un client NIS, c'est probablement la première chose à vérifier. Rappelez-vous: si vous désirez mettre en place un serveur NIS pour un réseau hétérogène, vous devrez probablement utiliser DES sur tous les systèmes car c'est le standard le plus courant.

31.5. Configuration réseau automatique (DHCP)

31.5.1. Qu'est-ce que DHCP?

DHCP, le protocole d'attribution dynamique des adresses ("Dynamic Host Configuration Protocol"), décrit les moyens par lesquels un système peut se connecter à un réseau et obtenir les informations nécessaires pour dialoguer sur ce réseau. Les versions de FreeBSD antérieures à la version 6.0

utilisent l'implémentation du client DHCP (dhclient(8)) de l'ISC (Internet Software Consortium). Les versions suivantes utilisent le programme `dhclient` d'OpenBSD issu d'OpenBSD 3.7. Toutes les informations données ici au sujet de `dhclient` sont valables aussi bien pour le client DHCP d'ISC que pour celui d'OpenBSD. Le serveur DHCP est celui distribué par le consortium ISC.

31.5.2. Ce que traite cette section

Cette section décrit les composants côté client des clients DHCP d'ISC et d' OpenBSD et côté serveur du système DHCP ISC. Le programme client, `dhclient`, est intégré à FreeBSD, la partie serveur est disponible à partir du logiciel porté net/isc-dhcp3-server. Les pages de manuel dhclient(8), dhcp-options(5), et dhclient.conf(5), en plus des références données plus bas, sont des ressources utiles.

31.5.3. Comment cela fonctionne-t-il?

Quand `dhclient`, le client DHCP, est exécuté sur la machine cliente, il commence à diffuser des requêtes de demandes d'information de configuration. Par défaut, ces requêtes sont effectuées sur le port UDP 68. Le serveur répond sur le port UDP 67, fournissant au client une adresse IP et d'autres informations réseau importantes comme le masque de sous-réseau, les routeurs, et les serveurs DNS. Toutes ces informations viennent sous la forme d'un "bail" DHCP qui est uniquement valide pendant un certain temps (configuré par l'administrateur du serveur DHCP). De cette façon, les adresses IP expirées pour les clients qui ne sont plus connectés peuvent être automatiquement récupérées.

Les clients DHCP peuvent obtenir une grande quantité d'informations à partir du serveur. Une liste exhaustive est donnée dans la page de manuel dhcp-options(5).

31.5.4. Intégration dans FreeBSD

Le client DHCP ISC ou OpenBSD (en fonction de la version de FreeBSD que vous utilisez), `dhclient`, est complètement intégré à FreeBSD. Le support du client DHCP est fourni avec l'installeur et le système de base, rendant évident le besoin d'une connaissance détaillée des configurations réseaux pour n'importe quel réseau utilisant un serveur DHCP. `dhclient` fait partie de toutes les versions de FreeBSD depuis la version 3.2.

DHCP est supporté par sysinstall. Quand on configure une interface réseau sous sysinstall, la deuxième question posée est: "Voulez-vous tenter la configuration DHCP de l'interface?". Répondre par l'affirmative à cette question lancera `dhclient`, et en cas de succès, complétera automatiquement les informations de configuration réseau.

Vous devez faire deux choses pour que votre système utilise DHCP au démarrage:

- Assurez-vous que le périphérique bpf est compilé dans votre noyau. Pour cela, vous devez ajouter la ligne `device bpf` à votre fichier de configuration du noyau, et recompiler le noyau. Pour plus d'informations sur la compilation de noyaux, consultez le Configurer le noyau de FreeBSD.

  Le périphérique bpf est déjà présent dans le noyau GENERIC qui est fourni avec FreeBSD, vous ne devez donc pas créer de noyau spécifique pour faire fonctionner DHCP.

Ceux qui sont particulièrement conscients de l'aspect sécurité devraient noter que bpf est également le périphérique qui permet le fonctionnement de "renifleurs" de paquets (de tels programmes doivent être lancés sous l'utilisateur `root`). bpf*est* nécessaire pour utiliser DHCP, mais si vous êtes très sensible à la sécurité, vous ne devriez probablement pas ajouter bpf à votre noyau parce que vous projetez d'utiliser DHCP dans le futur.

- Editez votre fichier /etc/rc.conf pour y ajouter ce qui suit:

```
ifconfig_fxp0="DHCP"
```

Assurez-vous de bien remplacer `fxp0` par l'interface que vous voulez configurer de façon dynamique comme décrit dans la Configuration des cartes réseaux.

Si vous utilisez un emplacement différent pour `dhclient`, ou si vous désirez passer des arguments supplémentaires à `dhclient`, ajoutez ce qui suit (en effectuant des modifications si nécessaire):

```
dhcp_program="/sbin/dhclient"
dhcp_flags=""
```

Le serveur DHCP, dhcpd, fait partie du logiciel porté net/isc-dhcp3-server disponible dans le catalogue des logiciels portés. Ce logiciel porté contient le serveur DHCP ISC et sa documentation.

31.5.5. Fichiers

- /etc/dhclient.conf

  `dhclient` nécessite un fichier de configuration, /etc/dhclient.conf. Généralement le fichier ne contient que des commentaires, les valeurs par défaut étant suffisantes. Ce fichier de configuration est décrit par la page de manuel dhclient.conf(5).

- /sbin/dhclient

  `dhclient` est lié statiquement et réside dans le répertoire /sbin. La page de manuel dhclient(8) donne beaucoup plus d'informations au sujet de `dhclient`.

- /sbin/dhclient-script

  `dhclient-script` est la procédure de configuration du client DHCP spécifique à FreeBSD. Elle est décrite dans la page de manuel dhclient-script(8), mais ne devrait pas demander de modification de la part de l'utilisateur pour fonctionner correctement.

- /var/db/dhclient.leases

  Le client DHCP conserve une base de données des baux valides, qui est écrite comme un fichier

journal. La page de manuel dhclient.leases(5) en donne une description légèrement plus longue.

31.5.6. Lecture supplémentaire

Le protocole DHCP est intégralement décrit dans la RFC 2131. Des informations sont également disponibles à l'adresse http://www.dhcp.org/.

31.5.7. Installer et configurer un serveur DHCP

31.5.7.1. Ce que traite cette section

Cette section fournit les informations nécessaires à la configuration d'un système FreeBSD comme serveur DHCP en utilisant l'implémentation ISC (Internet Software Consortium) du serveur DHCP.

Le serveur n'est pas fourni dans le système de base de FreeBSD, et vous devrez installer le logiciel porté net/isc-dhcp3-server pour bénéficier de ce service. Lisez le Installer des applications. les logiciels pré-compilés et les logiciels portés pour plus d'information sur l'utilisation du catalogue des logiciels portés.

31.5.7.2. Installation d'un serveur DHCP

Afin de configurer votre système FreeBSD en serveur DHCP, vous devrez vous assurer que le support du périphérique bpf(4) est compilé dans votre noyau. Pour cela ajouter la ligne `device bpf` dans votre fichier de configuration du noyau. Pour plus d'information sur la compilation de noyaux, consultez le Configurer le noyau de FreeBSD.

Le périphérique bpf est déjà présent dans le noyau GENERIC qui est fourni avec FreeBSD, vous ne devez donc pas créer de noyau spécifique pour faire fonctionner DHCP.

Ceux qui sont particulièrement conscients de l'aspect sécurité devraient noter que bpf est également le périphérique qui permet le fonctionnement de "renifleurs" de paquets (de tels programmes nécessitent également un accès avec privilèges). bpf*est* nécessaire pour utiliser DHCP, mais si vous êtes très sensible à la sécurité, vous ne devriez probablement pas ajouter bpf à votre noyau parce que vous projetez d'utiliser DHCP dans le futur.

Il vous reste ensuite à éditer le fichier dhcpd.conf d'exemple qui a été installé par le logiciel porté net/isc-dhcp3-server. Par défaut, cela sera /usr/local/etc/dhcpd.conf.sample, et vous devriez le copier vers /usr/local/etc/dhcpd.conf avant de commencer vos modifications.

31.5.7.3. Configuration du serveur DHCP

dhcpd.conf est composé de déclarations concernant les masques de sous-réseaux et les machines, il est peut-être plus facile à expliquer à l'aide d'un exemple:

```
option domain-name "example.com"; ①
option domain-name-servers 192.168.4.100; ②
option subnet-mask 255.255.255.0; ③
```

```
default-lease-time 3600; ④
max-lease-time 86400; ⑤
ddns-update-style none; ⑥

subnet 192.168.4.0 netmask 255.255.255.0 {
  range 192.168.4.129 192.168.4.254; ⑦
  option routers 192.168.4.1; ⑧
}

host mailhost {
  hardware ethernet 02:03:04:05:06:07; ⑨
  fixed-address mailhost.example.com; ⑩
}
```

① Cette option spécifie le domaine qui sera donné aux clients comme domaine par défaut. Consultez la page de manuel de resolv.conf(5) pour plus d'information sur sa signification.

② Cette option donne une liste, séparée par des virgules, de serveurs DNS que le client devrait utiliser.

③ Le masque de sous-réseau qui sera fourni aux clients.

④ Un client peut demander un bail d'une durée bien précise. Sinon par défaut le serveur alloue un bail avec cette durée avant expiration (en secondes).

⑤ C'est la durée maximale d'allocation autorisée par le serveur. Si un client demande un bail plus long, le bail sera accordé mais il ne sera valide que durant `max-lease-time` secondes.

⑥ Cette option indique si le serveur DHCP doit tenter de mettre à jour le DNS quand un bail est accepté ou révoqué. Dans l'implémentation ISC, cette option est *obligatoire*.

⑦ Ceci indique quelles adresses IP devraient être utilisées dans l'ensemble des adresses réservées aux clients. Les adresses comprises dans l'intervalle spécifiée sont allouées aux clients.

⑧ Définit la passerelle par défaut fournie aux clients.

⑨ L'adresse matérielle MAC d'une machine (de manière à ce que le serveur DHCP puisse reconnaître une machine quand elle envoie une requête).

⑩ Indique que la machine devrait se voir attribuer toujours la même adresse IP. Notez que l'utilisation d'un nom de machine ici est correct, puisque le serveur DHCP effectuera une résolution de nom sur le nom de la machine avant de renvoyer l'information sur le bail.

Une fois l'écriture de votre fichier dhcpd.conf terminée, vous devez activer le serveur DHCP dans le fichier /etc/rc.conf, en ajoutant:

```
dhcpd_enable="YES"
dhcpd_ifaces="dc0"
```

Remplacez le nom de l'interface `dc0` avec celui de l'interface (ou des interfaces, séparées par un espace) sur laquelle votre serveur DHCP attendra les requêtes des clients DHCP.

Ensuite, vous pouvez lancer le serveur en tapant la commande suivante:

```
# /usr/local/etc/rc.d/isc-dhcpd.sh start
```

Si vous devez, dans le futur, effectuer des changements dans la configuration de votre serveur, il est important de savoir que l'envoi d'un signal `SIGHUP` à dhcpd ne provoque *pas* le rechargement de la configuration, contrairement à la plupart des "daemons". Vous devrez envoyer un signal `SIGTERM` pour arrêter le processus, puis le relancer en utilisant la commande ci-dessus.

31.5.7.4. Fichiers

- /usr/local/sbin/dhcpd

  dhcpd est lié statiquement et réside dans le répertoire /usr/local/sbin. La page de manuel dhcpd(8) installée avec le logiciel porté donne beaucoup plus d'informations au sujet de dhcpd.

- /usr/local/etc/dhcpd.conf

  dhcpd nécessite un fichier de configuration, /usr/local/etc/dhcpd.conf avant de pouvoir commencer à offrir ses services aux client. Ce fichier doit contenir toutes les informations à fournir aux clients qui seront traités, en plus des informations concernant le fonctionnement du serveur. Ce fichier de configuration est décrit par la page de manuel dhcpd.conf(5) installée par le logiciel porté.

- /var/db/dhcpd.leases

  Le serveur DHCP conserve une base de données des baux qu'il a délivré, qui est écrite comme un fichier journal. La page de manuel dhcpd.leases(5) installée par le logiciel porté en donne une description légèrement plus longue.

- /usr/local/sbin/dhcrelay

  dhcrelay est utilisé dans les environnements avancés où un serveur DHCP fait suivre la requête d'un client vers un autre serveur DHCP sur un réseau séparé. Si vous avez besoin de cette fonctionnalité, installez alors le logiciel porté net/isc-dhcp3-server. La page de manuel dhcrelay(8) fournie avec le logiciel porté contient plus de détails.

31.6. Serveurs de noms (DNS)

31.6.1. Généralités

FreeBSD utilise, par défaut, BIND (Berkeley Internet Name Domain), qui est l'implémentation la plus courante du protocole DNS. Le DNS est le protocole qui effectue la correspondance entre noms et adresses IP, et inversement. Par exemple une requête pour `www.FreeBSD.org` aura pour réponse l'adresse IP du serveur Web du projet FreeBSD, et une requête pour `ftp.FreeBSD.org` renverra l'adresse IP de la machine FTP correspondante. De même, l'opposé est possible. Une requête pour une adresse IP retourne son nom de machine. Il n'est pas nécessaire de faire tourner un serveur DNS pour effectuer des requêtes DNS sur un système.

FreeBSD est actuellement fourni par défaut avec le serveur DNSBIND9. Notre installation est dotée

de fonctionnalités étendues au niveau de la sécurité, d'une nouvelle organisation du système de fichiers et d'une configuration en environnement chroot(8) automatisée.

Le DNS est coordonné sur l'Internet à travers un système complexe de serveurs de noms racines faisant autorité, de domaines de premier niveau ("Top Level Domain", TLD), et d'autres serveurs de noms de plus petites tailles qui hébergent, directement ou font office de "cache", l'information pour des domaines individuels.

Actuellement, BIND est maintenu par l'Internet Software Consortium http://www.isc.org/.

31.6.2. Terminologie

Pour comprendre ce document, certains termes relatifs au DNS doivent être maîtrisés.

Terme	Definition
"Forward" DNS	Correspondance noms de machine vers adresses IP.
Origine	Fait référence au domaine couvert par un fichier de zone particulier.
named, BIND, serveur de noms	Noms courants pour le serveur de noms BIND de FreeBSD
Resolveur	Un processus système par l'intermédiaire duquel une machine contacte un serveur de noms pour obtenir des informations sur une zone.
DNS inverse	C'est l'inverse du DNS "classique" ("Forward" DNS). C'est la correspondance adresses IP vers noms de machine.
Zone racine	Début de la hiérarchie de la zone Internet. Toutes les zones sont rattachées à la zone racine, de la même manière qu'un système de fichier est rattaché au répertoire racine.
Zone	Un domaine individuel, un sous-domaine, ou une partie des noms administrés par un même serveur faisant autorité.

Exemples de zones:

- `.` est la zone racine
- `org.` est un domaine de premier niveau (TLD) sous la zone racine
- `example.org.` est une zone sous le TLD `org.`
- `1.168.192.in-addr.arpa` est une zone faisant référence à toutes les adresses IP qui appartiennent l'espace d'adresse `192.168.1.*`.

Comme on peut le remarquer, la partie la plus significative d'un nom de machine est à sa gauche.

Par exemple, `example.org.` est plus spécifique que `org.`, comme `org.` est à son tour plus spécifique que la zone racine. La constitution de chaque partie d'un nom de machine est proche de celle d'un système de fichiers: le répertoire /dev se trouve sous la racine, et ainsi de suite.

31.6.3. Les raisons de faire tourner un serveur de noms

Les serveurs de noms se présentent généralement sous deux formes: un serveur de noms faisant autorité, et un serveur de noms cache.

Un serveur de noms faisant autorité est nécessaire quand:

- on désire fournir des informations DNS au reste du monde, être le serveur faisant autorité lors des réponses aux requêtes.
- un domaine, comme par exemple `example.org`, est enregistré et des adresses IP doivent être assignées à des noms de machine appartenant à ce domaine.
- un bloc d'adresses IP nécessite des entrées DNS inverses (IP vers nom de machine).
- un second serveur de noms ou de secours, appelé esclave, qui répondra aux requêtes.

Un serveur de noms cache est nécessaire quand:

- un serveur de noms local peut faire office de cache et répondre plus rapidement que l'interrogation d'un serveur de noms extérieur.

Quand on émet des requêtes pour `www.FreeBSD.org`, le résolveur interroge généralement le serveur de noms du fournisseur d'accès, et récupère la réponse. Avec un serveur DNS cache local, la requête doit être effectuée qu'une seule fois vers le monde extérieur par le serveur DNS cache. Chaque interrogation suivante n'aura pas à être transmise en dehors du réseau local, puisque l'information est désormais disponible localement dans le cache.

31.6.4. Comment cela fonctionne-t-il?

Sous FreeBSD le "daemon" BIND est appelé named pour des raisons évidentes.

Fichier	Description
named(8)	le "daemon" BIND
rndc(8)	le programme de contrôle du serveur de noms
/etc/namedb	répertoire où se trouvent les informations sur les zones de BIND
/etc/namedb/named.conf	le fichier de configuration du "daemon"

En fonction de la manière dont est configurée sur le serveur une zone donnée, les fichiers relatifs à cette zone pourront être trouvés dans les sous-répertoires master, slave, ou dynamic du répertoire /etc/namedb. Ces fichiers contiennent les informations DNS qui seront données par le serveur de noms en réponse aux requêtes.

31.6.5. Lancer BIND

Puisque BIND est installé par défaut, sa configuration est relativement simple.

La configuration par défaut de named est un serveur de noms résolveur basique, tournant dans un environnement chroot(8). Pour lancer le serveur avec cette configuration, utilisez la commande suivante:

```
# /etc/rc.d/named forcestart
```

Pour s'assurer que le "daemon" named est lancé à chaque démarrage, ajoutez la ligne suivante dans /etc/rc.conf:

```
named_enable="YES"
```

Il existe, bien évidemment, de nombreuses options de configuration pour /etc/namedb/named.conf qui dépassent le cadre de ce document. Si vous êtes intéressé par les options de démarrage de named sous FreeBSD, jetez un oeil aux paramètres `named_*` dans /etc/defaults/rc.conf et consultez la page de manuel rc.conf(5). La section Utilisation du système rc(8) sous FreeBSD constitue également une bonne lecture.

31.6.6. Fichiers de configuration

Les fichiers de configuration pour named se trouvent dans le répertoire /etc/namedb et devront être adaptés avant toute utilisation, à moins que l'on ait besoin que d'un simple résolveur. C'est dans ce répertoire où la majeure partie de la configuration se fera.

31.6.6.1. Utilisation de `make-localhost`

Pour configurer une zone maître, il faut se rendre dans le répertoire /etc/namedb/ et exécuter la commande suivante:

```
# sh make-localhost
```

Si tout s'est bien passé, un nouveau fichier devrait apparaître dans le sous-répertoire master. Les noms de fichiers devraient être localhost.rev pour le nom de domaine local et localhost-v6.rev pour les configurations IPv6. Tout comme le fichier de configuration par défaut, les informations nécessaires seront présentes dans le fichier named.conf.

31.6.6.2. /etc/namedb/named.conf

```
// $FreeBSD$
//
// Reportez-vous aux pages de manuel named.conf(5) et named(8), et à
// la documentation se trouvant dans /usr/shared/doc/bind9 pour plus de
// détails.
```

```
//
// Si vous devez configurer un serveur primaire, assurez-vous d'avoir
// compris les détails épineux du fonctionnement du DNS.  Même avec de
// simples erreurs, vous pouvez rompre la connexion entre les parties
// affectées, ou causer un important et inutile trafic Internet.

options {
        directory "/etc/namedb";
    pid-file    "/var/run/named/pid";
    dump-file   "/var/dump/named_dump.db";
    statistics-file "/var/stats/named.stats";

// Si named est utilisé uniquement en tant que résolveur local, ceci
// est un bon réglage par défaut.  Pour un named qui doit être
// accessible à l'ensemble du réseau, commentez cette option, précisez
// l'adresse IP correcte, ou supprimez cette option.
    listen-on   { 127.0.0.1; };

// Si l'IPv6 est activé sur le système, décommentez cette option pour
// une utilisation en résolveur local.  Pour donner l'accès au réseau,
// précisez une adresse IPv6, ou le mot-clé "any".
//  listen-on-v6    { ::1; };

// En plus de la clause "forwarders", vous pouvez forcer votre serveur
// de noms à ne jamais être à l'origine de
// requêtes, mais plutôt faire suivre les demandes en
// activant la ligne suivante:
//
//      forward only;

// Si vous avez accès à un serveur de noms au niveau de
// votre fournisseur d'accès, ajoutez ici son adresse IP, et
// activez la ligne ci-dessous.  Cela vous permettra de
// bénéficier de son cache, réduisant ainsi le
// trafic Internet.
/*
        forwarders {
                127.0.0.1;
        };
*/
```

Comme les commentaires le précisent, pour bénéficier d'un cache en amont de votre connexion, le paramètre `forwarders` peut être activé. Dans des circonstances normales, un serveur de noms interrogera de façon récursive certains serveurs de noms jusqu'à obtenir la réponse à sa requête. Avec ce paramètre activé, votre serveur interrogera le serveur de noms en amont (ou le serveur de noms fourni) en premier, en bénéficiant alors de son cache. Si le serveur en question gère beaucoup de trafic, et est un serveur rapide, activer cette option peut en valoir la peine.

`127.0.0.1` ne fonctionnera *pas* ici. Remplacez cette adresse IP par un serveur de

noms en amont de votre connexion.

```
        /*
         * S'il y a un coupe-feu entre vous et les serveurs de noms
         * avec lesquels vous voulez communiquer, vous aurez
         * peut-être besoin de décommenter la directive
         * query-source ci-dessous.  Les versions
         * précédentes de BIND lançaient des
         * requêtes à partir du port 53, mais depuis la
         * version 8, BIND utilise
         * par défaut un port pseudo-aléatoire quelconque non
         * réservé.
         */
        // query-source address * port 53;
};

// Si vous activez un serveur de noms local, n'oubliez pas d'entrer
// 127.0.0.1 dans votre fichier /etc/resolv.conf de sorte que ce
// serveur soit interrogé le premier.  Assurez-vous
// également de l'activer dans /etc/rc.conf.

zone "." {
        type hint;
        file "named.root";
};

zone "0.0.127.IN-ADDR.ARPA" {
        type master;
    file "master/localhost.rev";
};

// RFC 3152
zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA" {
    type master;
    file "master/localhost-v6.rev";
};

// NB: N'utilisez pas les adresses IP ci-dessous, elles sont factices,
// et ne servent que pour des besoins de
// démonstration/documentation!
//
// Exemple d'entrées de configuration de zone esclave.
// Il peut être pratique de devenir serveur esclave pour la
// zone à laquelle appartient votre domaine.  Demandez à
// votre administrateur réseau l'adresse IP du serveur primaire
// responsable de la zone.
//
// N'oubliez jamais d'inclure la résolution de la zone inverse
// (IN-ADDR.ARPA)!
// (Ce sont les premiers octets de l'adresse IP, en ordre inverse,
```

```
// auxquels ont a ajouté ".IN-ADDR.ARPA".)
//
// Avant de commencer à configurer une zone primaire, il faut
// être sûr que vous avez parfaitement compris comment le
// DNS et BIND fonctionnent.  Il apparaît parfois des pièges
// peu évidents à saisir.  En comparaison, configurer une
// zone esclave est plus simple.
//
// NB: N'activez pas aveuglément les exemples ci-dessous. :-)
// Utilisez des noms et des adresses réelles.

/* Un exemple de zone maître
zone "example.net" {
    type master;
    file "master/example.net";
};
*/

/* Un exemple de zone dynamique
key "exampleorgkey" {
    algorithm hmac-md5;
    secret "sf87HJqjkqh8ac87a02lla==";
};
zone "example.org" {
    type master;
    allow-update {
        key "exampleorgkey";
    };
    file "dynamic/example.org";
};
*/

/* Exemple de zones esclaves directes et inverses
zone "example.com" {
    type slave;
    file "slave/example.com";
    masters {
        192.168.1.1;
    };
};
zone "1.168.192.in-addr.arpa" {
    type slave;
    file "slave/1.168.192.in-addr.arpa";
    masters {
        192.168.1.1;
    };
};
*/
```

Dans named.conf, ce sont des exemples d'entrées d'un serveur esclave.

Pour chaque nouvelle zone gérée, une nouvelle entrée de zone doit être ajoutée au fichier named.conf.

Par exemple, l'entrée de zone la plus simple possible pour `example.org` serait:

```
zone "example.org" {
    type master;
    file "master/example.org";
};
```

Ce sera un serveur maître pour la zone, comme indiqué par l'option `type`, concervant ses informations de zone dans le fichier /etc/namedb/master/example.org comme précisé par l'option `file`.

```
zone "example.org" {
    type slave;
    file "slave/example.org";
};
```

Dans le cas d'un esclave, les informations concernant la zone seront transférées à partir du serveur maître pour la zone en question, et sauvegardées dans le fichier indiqué. Si ou lorsque le serveur maître tombe ou est inaccessible, le serveur esclave disposera des informations de la zone transférée et sera capable de les diffuser.

31.6.6.3. Fichiers de zone

Un exemple de fichier de zone maître pour `example.org` (défini dans /etc/namedb/master/example.org) suit:

```
$TTL 3600        ; 1 hour
example.org.    IN      SOA      ns1.example.org. admin.example.org. (
                                2006051501      ; Serial
                                10800           ; Refresh
                                3600            ; Retry
                                604800          ; Expire
                                86400           ; Minimum TTL
                        )

; Serveurs DNS
                IN      NS      ns1.example.org.
                IN      NS      ns2.example.org.

; Enregistrements MX
                IN      MX 10   mx.example.org.
                IN      MX 20   mail.example.org.

                IN      A       192.168.1.1
```

```
; Noms de machine
localhost       IN      A       127.0.0.1
ns1             IN      A       192.168.1.2
ns2             IN      A       192.168.1.3
mx              IN      A       192.168.1.4
mail            IN      A       192.168.1.5

; Alias
www             IN      CNAME   @
```

Notez que chaque nom de machine se terminant par un "." est un nom de machine complet, alors que tout ce qui se termine pas par un "." est référencé par rapport à une origine. Par exemple, `www` sera traduit en `www.origine`. Dans notre fichier de zone fictif, notre origine est `example.org.`, donc `www` sera traduit en `www.example.org.`

Le format d'un fichier de zone est le suivant:

```
nom-enregistrement      IN type-enregistrement   valeur
```

Les enregistrements DNS les plus couramment utilisés:

SOA
: début des données de zone

NS
: serveur de noms faisant autorité

A
: adresse d'une machine

CNAME
: alias d'un nom de machine

MX
: serveur de messagerie recevant le courrier pour le domaine

PTR
: un pointeur sur un nom de domaine (utilisé dans le DNS inverse)

```
example.org. IN SOA ns1.example.org. admin.example.org. (
                        2006051501      ; Serial
                        10800           ; Refresh after 3 hours
                        3600            ; Retry after 1 hour
                        604800          ; Expire after 1 week
                        86400 )         ; Minimum TTL of 1 day
```

`example.org.`

le nom de domaine, également l'origine pour ce fichier de zone.

`ns1.example.org.`

le serveur de noms primaire/faisant autorité pour cette zone.

`admin.example.org.`

la personne responsable pour cette zone avec le caractère "@" remplacé. (admin@example.org devient `admin.example.org`)

`2006051501`

le numéro de série de ce fichier. Celui-ci doit être incrémenté à chaque modification du fichier de zone. De nos jours, de nombreux administrateurs préfèrent un format du type `aaaammjjrr` pour le numéro de série. `2006051501` signifierait dernière modification le 15/05/2006, le `01` indiquant que c'est la seconde fois que ce fichier a été révisé ce jour. Le numéro de série est important puisqu'il indique aux serveurs de noms esclaves pour la zone une modification de celle-ci.

```
       IN NS           ns1.example.org.
```

C'est une entrée de type NS. Tous les serveurs de noms qui doivent faire autorité pour la zone devront inclure une de ces entrées.

```
localhost       IN      A       127.0.0.1
ns1             IN      A       192.168.1.2
ns2             IN      A       192.168.1.3
mx              IN      A       192.168.1.4
mail            IN      A       192.168.1.5
```

Un enregistrement de type A indique des noms de machine. Comme présenté ci-dessus `ns1.example.org` sera résolu en `192.168.1.2`.

```
                IN      A       192.168.1.1
```

Cette ligne assigne l'adresse IP `192.168.1.1` à l'origine, dans cet exemple `example.org`.

```
www             IN CNAME        @
```

L'enregistrement de type CNAME est généralement utilisé pour créer des alias à une machine. Dans l'exemple, `www` est un alias de la machine connue sous le nom `localhost.example.org` (`127.0.0.1`). Les enregistrements CNAME peuvent être utilisés pour fournir des alias à des noms de machines, ou permettre la rotation ("round robin") d'un nom de machine entre plusieurs machines.

```
                IN MX   10      mail.example.org.
```

L'enregistrement MX indique quels serveurs de messagerie sont responsables de la gestion du courrier entrant pour la zone. `mail.example.org` est le nom de machine du serveur de messagerie, et 10 étant la priorité du serveur de messagerie.

On peut avoir plusieurs serveurs de messagerie, avec des priorités de 10, 20, etc. Un serveur de messagerie tentant de transmettre du courrier au domaine `example.org` essaiera en premier le MX avec la plus haute priorité (l'enregistrement avec le numéro de priorité le plus bas), puis celui venant en second, etc, jusqu'à ce que le courrier puisse être correctement délivré.

Pour les fichiers de zone in-addr.arpa (DNS inverse), le même format est utilisé, à l'exception du fait que des entrées PTR seront utilisées en place de A ou CNAME.

```
$TTL 3600

1.168.192.in-addr.arpa. IN SOA ns1.example.org. admin.example.org. (
                        2006051501      ; Serial
                        10800           ; Refresh
                        3600            ; Retry
                        604800          ; Expire
                        3600 )          ; Minimum

        IN      NS      ns1.example.org.
        IN      NS      ns2.example.org.

1       IN      PTR     example.org.
2       IN      PTR     ns1.example.org.
3       IN      PTR     ns2.example.org.
4       IN      PTR     mx.example.org.
5       IN      PTR     mail.example.org.
```

Ce fichier donne la correspondance entre adresses IP et noms de machines de notre domaine fictif.

31.6.7. Serveur de noms cache

Un serveur de noms cache est un serveur de noms qui ne fait autorité pour aucune zone. Il émet simplement des requêtes, et se souvient du résultat pour une utilisation ultérieure. Pour mettre en place un tel serveur, configurez le serveur de noms comme à l'accoutumé, en prenant bien soin de n'inclure aucune zone.

31.6.8. Sécurité

Bien que BIND soit l'implémentation la plus courante du DNS, le problème de la sécurité subsiste toujours. De possibles problèmes de sécurité exploitables sont parfois découvert.

Bien que FreeBSD enferme automatiquement named dans un environnement chroot(8), il existe plusieurs autres mécanismes de sécurité qui pourraient aider à se prémunir contre de possibles

attaques DNS.

C'est une bonne idée de lire les avis de sécurité du CERT et de s'inscrire à la liste de diffusion des avis de sécurité pour FreeBSD pour se maintenir au courant des problèmes de sécurité actuels de l'Internet et de FreeBSD.

Si un problème surgit, conserver les sources à jour et disposer d'une version compilée de named récente ne seront pas de trop.

31.6.9. Lectures supplémentaires

Les pages de manuel de BIND/named: rndc(8) named(8) named.conf(8).

- Page officielle ISC concernant BIND
- Forum officiel ISC concernant BIND
- FAQ BIND
- DNS et BIND 5ème Edition de chez O'Reilly
- RFC1034 - Domain Names - Concepts and Facilities
- RFC1035 - Domain Names - Implementation and Specification

31.7. Serveur HTTP Apache

31.7.1. Généralités

FreeBSD est utilisé pour faire tourner certains des sites les plus chargés au monde. La majorité des serveurs web sur l'Internet utilisent le serveur HTTP Apache. Les versions pré-compilées d'Apache devraient se trouver sur le support d'installation de FreeBSD que vous avez utilisé. Si vous n'avez pas installé Apache à l'installation de FreeBSD, alors vous pouvez installer le serveur à partir du logiciel porté www/apache13 ou www/apache20.

Une fois qu'Apache a été installé avec succès, il doit être configuré.

Cette section traite de la version 1.3.X du serveur HTTP Apache étant donné que c'est la version la plus largement utilisée sous FreeBSD. Apache 2.X introduit de nombreuses nouvelles technologies mais elles ne sont pas abordées ici. Pour plus d'informations concernant Apache 2.X veuillez consulter http://httpd.apache.org/.

31.7.2. Configuration

Le fichier principal de configuration du serveur HTTP Apache est, sous FreeBSD, le fichier /usr/local/etc/apache/httpd.conf. Ce fichier est un fichier texte de configuration UNIX® typique avec des lignes de commentaires débutant par un caractère #. Une description complète de toutes les options de configuration possibles dépasse le cadre de cet ouvrage, aussi seules les directives les plus fréquemment modifiées seront décrites ici.

`ServerRoot "/usr/local"`

Indique le répertoire d'installation par défaut pour l'arborescence Apache. Les binaires sont stockés dans les sous-répertoires bin et sbin de la racine du serveur, et les fichiers de configuration dans etc/apache.

`ServerAdmin you@your.address`

L'adresse électronique à laquelle tous les problèmes concernant le serveur doivent être rapportés. Cette adresse apparaît sur certaines pages générées par le serveur, comme des pages d'erreur.

`ServerName www.example.com`

La directive `ServerName` vous permet de fixer un nom de machine qui est renvoyé aux clients de votre serveur si le nom est différent de celui de la machine (i.e, utilisez `www` à la place du véritable nom de la machine).

`DocumentRoot "/usr/local/www/data"`

`DocumentRoot` est le répertoire où se trouvent les documents que votre serveur diffusera. Par défaut, toutes les requêtes sont prises en compte par rapport à ce répertoire, mais des liens symboliques et des alias peuvent être utilisés pour pointer vers d'autres emplacements.

C'est toujours une bonne idée de faire des copies de sauvegarde de votre fichier de configuration d'Apache avant de faire des modifications. Une fois que vous êtes satisfait avec votre configuration, vous êtes prêt à lancer Apache.

31.7.3. Exécuter Apache

Apache n'est pas lancé à partir du "super-serveur" inetd comme pour beaucoup d'autres serveurs réseau. Il est configuré pour tourner de façon autonome pour de meilleures performances à la réception des requêtes HTTP des navigateurs web. Une procédure est fournie pour rendre le démarrage, l'arrêt, et le redémarrage du serveur aussi simple que possible. Pour démarrer Apache pour la première fois, exécutez:

```
# /usr/local/sbin/apachectl start
```

Vous pouvez arrêter le serveur à tout moment en tapant:

```
# /usr/local/sbin/apachectl stop
```

Après avoir effectué des modifications dans le fichier de configuration, vous devez redémarrer le serveur:

```
# /usr/local/sbin/apachectl restart
```

Pour redémarrer Apache sans faire échouer les connexions en cours, exécutez:

```
# /usr/local/sbin/apachectl graceful
```

Des informations supplémentaires sont disponibles dans la page de manuel d'apachectl(8).

Pour lancer Apache au démarrage du système, ajoutez la ligne suivante au fichier /etc/rc.conf:

```
apache_enable="YES"
```

Si vous désirez passer des options en ligne de commande supplémentaires au programme `httpd` d'Apache lancé au démarrage du système, vous pouvez les spécifier à l'aide d'une ligne dans rc.conf:

```
apache_flags=""
```

Maintenant que le serveur web tourne, vous pouvez voir votre site web en pointant votre navigateur sur `http://localhost/`. La page web affichée par défaut est /usr/local/www/data/index.html.

31.7.4. Serveurs virtuels

Apache supporte deux types différents de serveurs virtuels. Le premier type est celui des serveurs virtuels basés sur les noms. Ce type de serveurs virtuels utilise les entêtes HTTP/1.1 pour déterminer le nom de la machine. Cela autorise le partage de la même adresse IP entre plusieurs domaines différents.

Pour configurer Apache à l'utilisation de serveurs virtuels basés sur les noms, ajoutez une entrée comme la suivante à votre fichier httpd.conf:

```
NameVirtualHost *
```

Si votre serveur web est appelé `www.domain.tld` et que vous voulez mettre en place un domain virtuel pour `www.someotherdomain.tld` alors vous ajouterez les entrées suivantes au fichier httpd.conf:

```
<VirtualHost *>
ServerName www.domain.tld
DocumentRoot /www/domain.tld
</VirtualHost>

<VirtualHost *>
ServerName www.someotherdomain.tld
DocumentRoot /www/someotherdomain.tld
</VirtualHost>
```

Remplacez les addresses avec celles que vous désirez utiliser et le chemin d'accès des documents avec celui que vous utilisez.

Pour plus d'informations sur la mise en place de serveurs virtuels, veuillez consulter la documentation officielle d'Apache à l'adresse http://httpd.apache.org/docs/vhosts/.

31.7.5. Modules Apache

Il existe de nombreux modules Apache disponibles en vue d'ajouter des fonctionnalités au serveur de base. Le catalogue des logiciels portés offre une méthode simple d'installation d'Apache avec certains des modules les plus populaires.

31.7.5.1. mod_ssl

Le module mod_ssl utilise la bibliothèque OpenSSL pour offrir un chiffrement solide à l'aide des protocoles "Secure Sockets Layer" (SSL v2/v3) et "Transport Layer Security". Ce module fourni tout ce qui est nécessaire à la demande de certificats signés auprès d'une autorité de certification connue de façon à pouvoir faire tourner un serveur web sécurisé sous FreeBSD.

Si vous n'avez pas déjà installé Apache, alors une version d'Apache 1.3.X comprenant mod_ssl peut être installée à l'aide du logiciel porté www/apache13-modssl. Le support SSL est également disponible pour Apache 2.X avec le logiciel porté www/apache20, où il est activé par défaut.

31.7.5.2. Sites Web dynamiques avec Perl PHP

Ces dernières années, de plus en plus d'entreprises se sont tournées vers l'Internet pour augmenter leurs revenus et renforcer leur exposition. Cela a eu pour conséquence d'accroître le besoin de contenus Web interactifs. Quand certaines entreprises, comme Microsoft®, ont introduit dans leurs produits propriétaires des solutions à ces besoins, la communauté des logiciels libres a également répondu à l'appel. Deux options pour obtenir du contenu Web dynamique sont mod_perl et mod_php.

31.7.5.2.1. mod_perl

Le projet d'intégration Apache/Perl réuni la puissance du langage de programmation Perl et le serveur HTTP Apache. Avec le module mod_perl il est alors possible d'écrire des modules Apache entièrement en Perl. De plus, la présence d'un interpréteur intégré au serveur évite la surcharge due au lancement d'un interpréteur externe et le délai pénalisant du démarrage de Perl.

Le module mod_perl est peut être obtenu de diverses manières. Pour l'utilisation du module mod_perl souvenez-vous que mod_perl 1.0 ne fonctionne qu'avec Apache 1.3 et mod_perl 2.0 ne fonctionne qu'avec Apache 2. Le module mod_perl 1.0 est disponible sous www/mod_perl et une version compilée en statique sous www/apache13-modperl. Le module mod_perl 2.0 est disponible sous www/mod_perl2.

31.7.5.2.2. mod_php

PHP, aussi connu sous le nom de "PHP: Hypertext Preprocessor" est un langage de script tout particulièrement adapté au développement Web. Pouvant être intégré à du HTML, sa syntaxe est dérivée du C, Java™, et du Perl avec pour objectif de permettre aux développeurs Web d'écrire

rapidement des pages Web au contenu généré dynamiquement.

Pour ajouter le support de PHP5 au serveur Web Apache, commencez par installer le logiciel porté lang/php5.

Si c'est la première installation du logiciel lang/php5, les OPTIONS disponibles seront affichées automatiquement. Si aucun menu n'est affiché, parce que le logiciel porté lang/php5 a été installé par le passé, il est toujours possible de forcer l'affichage du menu des options de compilation en utilisant la commande:

```
# make config
```

dans le répertoire du logiciel porté.

Dans le menu des options de compilation, sélectionnez l'option APACHE pour compiler mod_php5 sous forme de module chargeable pour le serveur Web Apache.

De nombreux sites utilisent toujours PHP4 pour diverses raisons (des problèmes de compatibilité ou des applications Web déjà déployées). Si mod_php4 est requis à la place de mod_php5, utilisez alors le logiciel porté lang/php4. Le logiciel porté lang/php4 supporte plusieurs des options de configuration et de compilation du logiciel porté lang/php5.

Cela installera et configurera les modules requis au support des applications dynamiques PHP. Assurez-vous que les sections suivantes ont été ajoutées au fichier /usr/local/etc/apache/httpd.conf:

```
LoadModule php5_module        libexec/apache/libphp5.so
```

```
AddModule mod_php5.c
    IfModule mod_php5.c
        DirectoryIndex index.php index.html
    /IfModule
    IfModule mod_php5.c
        AddType application/x-httpd-php .php
        AddType application/x-httpd-php-source .phps
    /IfModule
```

Ensuite, un simple appel à la commande apachectl pour un redémarrage élégant est requis pour charger le module PHP:

```
# apachectl graceful
```

Lors des futures mises à jour de PHP, la commande make config ne sera pas nécessaire; les OPTIONS précédemment sélectionnées sont automatiquement sauvegardées par le système des logiciels portés de FreeBSD.

Le support de PHP sous FreeBSD est extrêmement modulaire ce qui donne lieu à une installation de base limitée. Il est très simple d'ajouter une fonctionnalité en utilisant le logiciel porté lang/php5-extensions. Ce logiciel porté fournit un menu pour l'installation des extensions PHP. Alternativement, il est possible d'installer les extensions individuellement en utilisant les logiciels portés correspondants.

Par exemple, pour ajouter à PHP5 le support pour le serveur de bases de données MySQL, installez simplement le logiciel porté databases/php5-mysql.

Après l'installation d'une extension, le serveur Apache doit être redémarré pour prendre en compte les changements de configuration:

```
# apachectl graceful
```

31.8. Protocole de transfert de fichiers (FTP)

31.8.1. Généralités

Le protocol de transfert de fichiers (FTP) offre aux utilisateurs une méthode simple pour transférer des fichiers vers ou à partir d'un serveur FTP. FreeBSD comprend un serveur FTP, ftpd, dans le système de base. Cela rend la configuration et l'administration d'un serveur FTP sous FreeBSD très simple.

31.8.2. Configuration

L'étape de configuration la plus important est de décider quels comptes seront autorisés à accéder au serveur FTP. Un système FreeBSD classique possède de nombreux comptes système utilisés par divers "daemon"s, mais les utilisateurs inconnus ne devraient pas être autorisés à ouvrir de session sous ces comptes. Le fichier /etc/ftpusers est une liste d'utilisateurs interdits d'accès au serveur FTP. Par défaut, il inclut les comptes systèmes précédemment mentionnés, mais il est possible d'ajouter des utilisateurs précis qui ne devraient pas avoir accès au serveur FTP.

Vous pouvez vouloir restreindre l'accès à certains utilisateurs sans leur refuser complètement l'utilisation du serveur FTP. Cela peut être réalisé à l'aide du fichier /etc/ftpchroot. Ce fichier liste les utilisateurs et les groupes sujet à des restrictions d'accès FTP. La page de manuel ftpchroot(5) fournit tous les détails, cela ne sera donc pas décrit ici.

Si vous désirez activer l'accès FTP anonyme sur votre serveur, vous devez alors créer un utilisateur appelé `ftp` sur votre serveur FreeBSD. Les utilisateurs seront donc en mesure d'ouvrir une session FTP sur votre serveur sous le nom d'utilisateur `ftp` ou `anonymous` et sans aucun mot de passe (par convention l'adresse électronique de l'utilisateur devrait être utilisée comme mot de passe). Le serveur FTP appellera chroot(2) quand un utilisateur anonyme ouvrira une session, pour restreindre l'accès juste au répertoire personnel de l'utilisateur `ftp`.

Il existe deux fichiers texte qui spécifient les messages de bienvenue à afficher aux clients FTP. Le contenu du fichier /etc/ftpwelcome sera affiché aux utilisateurs avant qu'ils atteignent l'invite de session. Après une ouverture de session, le contenu du fichier /etc/ftpmotd sera affiché. Notez que

le chemin d'accès à ce fichier est relatif à l'environnement de la session, aussi le fichier ~ftp/etc/ftpmotd sera affiché aux utilisateurs anonymes.

Une fois que le serveur FTP a été configuré correctement, il doit être activé dans le fichier /etc/inetd.conf. Ici il faut juste retirer le symbole de commentaire "#" en face de la ligne ftpd:

```
ftp stream  tcp nowait  root    /usr/libexec/ftpd   ftpd -l
```

Comme expliqué dans la Recharger le fichier de configuration d'inetd, la configuration d'inetd doit être rechargée après que le fichier de configuration ait été modifié.

Vous pouvez maintenant ouvrir une session FTP sur votre serveur en tapant:

```
% ftp localhost
```

31.8.3. Maintenance

Le "daemon" ftpd utilise syslog(3) pour l'enregistrement des messages. Par défaut, le "daemon" de gestion des journaux du système enverra les messages relatifs au FTP dans le fichier /var/log/xferlog. L'emplacement des journaux FTP peut être modifié en changeant la ligne suivante dans le fichier /etc/syslog.conf:

```
ftp.info      /var/log/xferlog
```

Soyez conscient des éventuels problèmes impliqués par l'utilisation d'un serveur FTP acceptant les connexions anonymes. Vous devriez, tout particulièrement, penser à deux fois avant d'autoriser les utilisateurs anonyme à déposer des fichiers sur le serveur. Votre site FTP pourrait devenir un forum d'échange de logiciels commerciaux sans les licences ou pire. Si vous devez autoriser le dépôt de fichiers de façon anonyme sur le serveur FTP, alors vous devriez fixer les permissions sur ces fichiers de telle sorte qu'ils ne puissent être lus par d'autres utilisateurs anonymes avant qu'ils n'aient pu être contrôlés.

31.9. Serveur de fichiers et d'impression pour clients Microsoft® Windows® (Samba)

31.9.1. Généralités

Samba est un logiciel libre très populaire qui offre des services de partage de fichiers et d'imprimantes pour les clients Microsoft® Windows®. De tels clients peuvent se connecter et utiliser l'espace de fichiers d'une machine FreeBSD comme si c'était un disque local, ou utiliser des imprimantes FreeBSD comme si elles étaient des imprimantes locales.

Samba devrait se trouver sur votre support d'installation. Si vous n'avez pas installé Samba à l'installation de FreeBSD, vous pouvez alors l'installer à partir de la version pré-compilée ou portée net/samba3.

31.9.2. Configuration

Le fichier de configuration par défaut de Samba est installé sous le nom /usr/local/etc/smb.conf.default. Ce fichier doit être copié vers /usr/local/etc/smb.conf et personnalisé avant que Samba ne puisse être utilisé.

Le fichier smb.conf contient la configuration nécessaire à l'exécution de Samba, comme la définition des imprimantes et des "systèmes de fichiers partagés" que vous désirez partager avec les clients Windows®. Le logiciel Samba comprend une interface Web appelé swat qui offre une méthode simple de configuration du fichier smb.conf.

31.9.2.1. Utilisation de l'interface web d'administration de Samba (SWAT)

L'interface web d'administration de Samba (SWAT) est exécutée sous la forme d'un "daemon" à partir d'inetd. Par conséquent, la ligne suivante dans le fichier /etc/inetd.conf doit être décommentée avant que swat ne puisse être utilisé pour configurer Samba:

```
swat   stream  tcp     nowait/400      root    /usr/local/sbin/swat    swat
```

Comme expliqué dans la Recharger le fichier de configuration d'inetd, la configuration d'inetd doit être rechargée après modification de ce fichier de configuration.

Une fois que swat a été activé dans inetd.conf, vous pouvez utiliser un navigateur pour vous connecter à l'adresse http://localhost:901. Vous devez ouvrir tout d'abord une session sous le compte système `root`.

Une fois que vous avez ouvert une session sur la page principale de configuration de Samba, vous pouvez naviguer dans la documentation du système, ou commencer par cliquer sur l'onglet **Globals**. Le menu **Globals** correspond aux variables situées dans la section `[global]` du fichier /usr/local/etc/smb.conf.

31.9.2.2. Paramétrages généraux

Que vous utilisiez swat ou éditiez directement le fichier /usr/local/etc/smb.conf, les premières directives que vous allez sûrement rencontrer en configurant Samba seront:

`workgroup`

Le nom de domaine NT ou le groupe de travail pour les ordinateurs qui accéderont à ce serveur.

`netbios name`

Fixe le nom NetBIOS sous lequel est connu le serveur Samba. Par défaut c'est le même que la première composante du nom de la machine pour le DNS.

`server string`

Cette directive définie la chaîne de caractères qui sera affichée lors de l'utilisation de la commande `net view` et par d'autres outils réseau recherchant à afficher une description du serveur.

31.9.2.3. Paramètres de sécurité

Deux des plus importants paramétrages de /usr/local/etc/smb.conf sont le mode de sécurité choisi, et le format de mot de passe pour les utilisateurs. Les directives suivantes contrôlent ces options:

`security`

Les deux options les plus courantes sont `security = share` et `security = user`. Si vos clients utilisent des noms d'utilisateur identiques à ceux sur votre machine FreeBSD, alors vous voudrez utiliser un niveau de sécurité utilisateur. C'est le mode de sécurité par défaut et qui demande aux clients de d'ouvrir une session avant de pouvoir accéder aux ressources partagées.

Dans le niveau de sécurité partage ("share"), le client n'a pas besoin d'ouvrir de session avant de pouvoir se connecter à une ressource partagée. C'était le mode de sécurité par défaut d'anciennes versions de Samba.

`passdb backend`

Samba possède plusieurs modèles de support d'authentification. Vous pouvez authentifier des clients avec LDAP, NIS+, une base de données SQL ou un fichier de mot de passe modifié. La méthode d'authentification par défaut est appelée `smbpasswd`, et c'est celle qui sera présentée ici.

En supposant que le modèle `smbpasswd` par défaut est utilisé, le fichier /usr/local/private/smbpasswd doit être créé pour permettre à Samba d'identifier les clients. Si vous désirez donner accès à vos comptes utilisateur UNIX® à partir de clients Windows®, utilisez la commande suivante:

```
# smbpasswd -a username
```

Veuillez consulter le tutorial officiel de Samba pour des informations supplémentaires sur les options de configuration. Avec les bases présentées ici, vous devriez disposer de tous les éléments nécessaires au démarrage de Samba.

31.9.3. Démarrage de Samba

Le logiciel porté net/samba3 amène une nouvelle procédure de démarrage qui peut être employée pour contrôler Samba. Pour activer cette procédure de manière à ce qu'elle soit utilisée pour par exemple lancer, arrêter ou relancer Samba, ajoutez la ligne suivante au fichier /etc/rc.conf:

```
samba_enable="YES"
```

Ou, pour un contrôle plus fin:

```
nmbd_enable="YES"
    smbd_enable="YES"
```

Avec cela, Samba sera automatiquement lancé au démarrage.

Il est alors possible de démarrer Samba à n'importe quel moment en tapant:

```
# /usr/local/etc/rc.d/samba start
Starting SAMBA: removing stale tdbs :
Starting nmbd.
Starting smbd.
```

Veuillez consulter la Utilisation du système rc(8) sous FreeBSD pour plus d'information sur les procédures rc.

Samba consiste essentiellement en trois "daemon"s séparés. Vous devriez vous rendre compte que les "daemon"s nmbd et smbd sont lancés par la procédure samba. Si vous avez activé la résolution de noms winbind dans le fichier smb.conf, alors le "daemon" winbindd sera également lancé.

Vous pouvez arrêter Samba à tout moment en tapant:

```
# /usr/local/etc/rc.d/samba stop
```

Samba est une suite logiciels complexes avec des fonctionnalités permettant une large intégration avec les réseaux Microsoft® Windows®. Pour plus d'information sur les fonctionnalités non-abordées dans ce document, veuillez consulter http://www.samba.org.

31.10. Synchronisation de l'horloge avec NTP

31.10.1. Généralités

Avec le temps, l'horloge d'un ordinateur tend à dériver. Le protocole NTP ("Network Time Protocol") est une des manières pour s'assurer que votre horloge reste précise.

De nombreux services Internet ont besoin, ou tirent partie, de la précision des horloges des ordinateurs. Par exemple, un serveur web, peut recevoir des requêtes pour n'envoyer un fichier que s'il a été modifié depuis un certain temps. Sur un réseau local, il est essentiel que les ordinateurs partageant des fichiers à partir du même serveur de fichiers aient des horloges synchronisées de manière à ce que les dates de création ou de dernière modification d'un fichier ("timestamp") soient cohérentes. Des services comme cron(8) reposent sur une horloge système précise pour exécuter des commandes à des moments précis.

FreeBSD est fourni avec le serveur NTP ntpd(8) qui peut être utilisé pour contacter d'autres serveurs NTP pour régler l'horloge de votre machine ou pour jouer le rôle de serveur de temps pour d'autres.

31.10.2. Choisir les serveurs NTP appropriés

Afin de synchroniser votre horloge, vous devrez trouver un ou plusieurs serveurs NTP. Votre administrateur réseau ou votre FAI peuvent avoir mis en place un serveur NTP dans cet objectif-consultez leur documentation pour voir si c'est le cas. Il existe une liste en ligne de serveurs NTP accessibles par le public que vous pouvez utiliser pour trouver un serveur NTP proche de vous. Assurez-vous d'avoir pris connaissance de la politique d'utilisation des serveurs que vous choisissez, et demandez la permission si nécessaire.

Choisir plusieurs serveurs NTP non-connectés entre eux est une bonne idée au cas où un des serveurs que vous utilisez devient inaccessible ou que son horloge n'est plus fiable. ntpd(8) utilise intelligemment les réponses qu'il reçoit d'autres serveurs-il favorisera les plus fiables par rapport aux moins fiables.

31.10.3. Configuration de votre machine

31.10.3.1. Configuration de base

Si vous désirez synchroniser votre horloge uniquement lors du démarrage de la machine, vous pouvez alors employer ntpdate(8). Cela peut être approprié pour certaines machines de bureau qui sont fréquemment redémarrées et qui ne nécessites qu'une synchronisation épisodique, cependant la plupart des machines devraient utiliser ntpd(8).

Utiliser ntpdate(8) au moment du démarrage est également une bonne idée pour les machines qui exécutent ntpd(8). Le programme ntpd(8) modifie l'horloge graduellement, alors que ntpdate(8) change directement l'horloge, peu importe la différence entre l'heure actuelle de la machine et l'heure correcte.

Pour activer ntpdate(8) au démarrage, ajoutez la ligne `ntpdate_enable="YES"` au fichier /etc/rc.conf. Vous devrez également préciser tous les serveurs avec lesquels vous désirez vous synchroniser et tous les indicateurs devant être passés à ntpdate(8) avec `ntpdate_flags`.

31.10.3.2. Configuration générale

NTP est configuré par l'intermédiaire du fichier /etc/ntp.conf suivant le format décrit dans la page de manuel ntp.conf(5). Voici un exemple simple:

```
server ntplocal.example.com prefer
server timeserver.example.org
server ntp2a.example.net

driftfile /var/db/ntp.drift
```

L'option `server` précise quels serveurs doivent être utilisés, avec un serveur listé par ligne. Si un serveur est spécifié avec l'argument `prefer`, comme c'est le cas pour `ntplocal.example.com`, ce serveur est préféré par rapport aux autres serveurs. Une réponse en provenance d'un serveur *préféré* sera ignorée si elle diffère de façon significative des réponses des autres serveurs, sinon elle sera utilisée sans considérer les autres réponses. L'argument `prefer` est normalement employé pour les serveurs NTP qui sont connus pour leur grande précision, comme ceux avec des systèmes spéciaux de contrôle du matériel.

L'option `driftfile` précise quel fichier est utilisé pour stocker le décalage de fréquence de l'horloge. Le programme ntpd(8) l'utilise pour compenser automatiquement la dérive naturelle de l'horloge, permettant de maintenir un réglage raisonnablement correct même s'il est coupé d'autres sources extérieures de temps pendant une certaine période.

L'option `driftfile` précise également quel fichier est utilisé pour stocker l'information concernant les réponses précédentes des serveurs NTP que vous utilisez. Il ne devrait pas être modifié par un

autre processus.

31.10.3.3. Contrôler l'accès à votre serveur

Par défaut, votre serveur NTP sera accessible par toutes les machines sur l'Internet. L'option `restrict` du fichier /etc/ntp.conf vous permet de contrôler quelles machines peuvent accéder à votre serveur.

Si vous voulez refuser à tout le monde l'accès à votre serveur NTP, ajoutez la ligne suivante au fichier /etc/ntp.conf:

```
restrict default ignore
```

Cela empêchera également à votre serveur d'accéder à tout serveur listé dans votre configuration locale. Si vous avez besoin de synchroniser votre serveur NTP avec un serveur NTP externe, vous devez alors autoriser le serveur en question. Consultez la page de manuel de ntp.conf(5) pour plus d'information.

Si vous désirez autoriser uniquement l'accès aux machines de votre réseau pour qu'elles puissent synchroniser leur horloge, tout en vous assurant qu'elles ne peuvent configurer le serveur ou être utilisées comme point de de synchronisation, ajoutez:

```
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
```

à la place, où `192.168.1.0` est une adresse IP de votre réseau et `255.255.255.0` est votre masque de sous-réseau.

Le fichier /etc/ntp.conf peut contenir plusieurs options `restrict`. Pour plus de détails, lisez la section `Access Control Support` de la page de manuel ntp.conf(5).

31.10.4. Exécuter le serveur NTP

Pour s'assurer que le serveur NTP est lancé au démarrage, ajoutez la ligne `ntpd_enable="YES"` dans le fichier /etc/rc.conf. Si vous désirez passer des indicateurs supplémentaires à ntpd(8), éditez les paramètres de l'option `ntpd_flags` dans /etc/rc.conf.

Pour lancer le serveur sans redémarrer votre machine, exécutez `ntpd` en étant sûr de préciser tout paramètre supplémentaire de `ntpd_flags` dans /etc/rc.conf. Par exemple:

```
# ntpd -p /var/run/ntpd.pid
```

31.10.5. Utiliser ntpd avec une connexion Internet temporaire

Le programme ntpd(8) n'a pas besoin d'une connexion permanente à l'Internet pour fonctionner correctement. Cependant, si vous disposez d'une connexion temporaire qui est configurée de telle sorte qu'il y ait établissement de la connexion à la demande, c'est une bonne idée d'empêcher le

trafic NTP de déclencher la numérotation ou de maintenir constamment établie la connexion. Si vous utilisez PPP en mode utilisateur, vous pouvez employer les directives `filter` dans le fichier /etc/ppp/ppp.conf. Par exemple:

```
set filter dial 0 deny udp src eq 123
# Empêche le trafic NTP de lancer une connexion
set filter dial 1 permit 0 0
set filter alive 0 deny udp src eq 123
# Empêche le trafic NTP entrant de garder la connexion établie
set filter alive 1 deny udp dst eq 123
# Empêche le trafic NTP sortant de garder la connexion établie
set filter alive 2 permit 0/0 0/0
```

Pour plus de détails lisez la section `PACKET FILTERING` de la page de manuel ppp(8) et les exemples du répertoire /usr/shared/examples/ppp/.

Certains fournisseurs d'accès Internet bloquent les ports dont le numéro est faible, empêchant NTP de fonctionner puisque les réponses n'atteignent jamais votre machine.

31.10.6. Information supplémentaire

La documentation pour le serveur NTP peut être trouvée dans le répertoire /usr/shared/doc/ntp/ sous le format HTML.

Chapitre 32. Firewalls Traduction en Cours

32.1. Introduction

32.2. Firewall Concepts

32.3. Firewall Packages

32.4. The OpenBSD Packet Filter (PF) and ALTQ

32.5. The IPFILTER (IPF) Firewall

32.6. IPFW

Chapitre 33. Administration réseau avancée

33.1. Synopsis

Ce chapitre abordera certains nombre de sujets réseau avancés.

Après la lecture de ce chapitre, vous connaîtrez:

- Les bases sur les passerelles et les routes.
- Comment configurer les périphériques IEEE 802.11 et Bluetooth®.
- Comment utiliser FreeBSD en tant que pont ("bridge").
- Comment configurer le démarrage via le réseau pour une machine sans disque dur.
- Comment configurer la translation d'adresse réseau.
- Comment connecter deux ordinateurs via PLIP.
- Comment configurer l'IPv6 sur une machine FreeBSD.
- Comment configurer ATM.

Avant de lire ce chapitre, vous devrez:

- Comprendre les bases des procédures /etc/rc.
- Etre familier avec la terminologie réseau de base.
- Savoir comment configurer et installer un nouveau noyau FreeBSD (Configurer le noyau de FreeBSD).
- Savoir comment installer des logiciels tierce-partie (Installer des applications. les logiciels pré-compilés et les logiciels portés).

33.2. Passerelles et routes

Pour qu'une machine soit en mesure d'en contacter une autre, il faut que soit mis en place un mécanisme qui décrive comment aller de l'une à l'autre. C'est ce que l'on appelle le *routage*. Une "route" est définie par une paire d'adresses: une "destination" et une "passerelle". Cette paire signifie que pour atteindre cette *destination*, vous devez passer par cette *passerelle*. Il y a trois sortes de destination: les machines individuelles, les sous-réseaux, et "default"-la destination par défaut. La route par défaut ("default route") est utilisée lorsqu'aucune autre route n'est applicable. Nous parlerons un peu plus des routes par défaut par la suite. Il existe également trois sortes de passerelles: les machines individuelles, les interfaces (aussi appelées "liens"), et les adresses Ethernet matérielles (adresses MAC).

33.2.1. Un exemple

Pour illustrer différents aspects du routage, nous utiliserons l'exemple suivant, qui est produit par la commande `netstat`:

```
% netstat -r
Routing tables

Destination      Gateway            Flags     Refs     Use     Netif Expire

default          outside-gw         UGSc       37      418      ppp0
localhost        localhost          UH          0      181       lo0
test0            0:e0:b5:36:cf:4f   UHLW        5    63288       ed0     77
10.20.30.255     link#1             UHLW        1     2421
example.com      link#1             UC          0        0
host1            0:e0:a8:37:8:1e    UHLW        3     4601       lo0
host2            0:e0:a8:37:8:1e    UHLW        0        5       lo0 =>
host2.example.com link#1             UC          0        0
224              link#1             UC          0        0
```

Les deux premières lignes définissent la route par défaut (dont nous parlerons dans la section suivante) et la route `localhost`.

L'interface (colonne `Netif`) qu'il est indiqué d'utiliser pour `localhost` est lo0, aussi appelée interface "loopback"-en boucle. Ce qui veut dire que tout le trafic vers cette destination doit rester interne, au lieu d'être envoyé sur le réseau local, puisqu'il reviendra de toute façon à son point de départ.

Ce qui se remarque ensuite, ce sont les adresses commençant par `0:e0:`. Ce sont les adresses Ethernet matérielles, qui sont également connues sous le nom d'adresses MAC. FreeBSD reconnaîtra automatiquement toute machine (`test0` dans l'exemple) sur le réseau local Ethernet et ajoutera une route vers cette machine, directement via l'interface Ethernet ed0. Il y a aussi un délai (colonne `Expire`) associé à ce type de route, qui est utilisé si l'on entend plus parler de cette machine pendant un laps de temps précis. Quand cela arrive, la route vers cette machine est automatiquement supprimée. Ces machines sont identifiées par un mécanisme appelé RIP ("Routing Information Protocol"-protocole d'information de routage), qui met en place des routes vers les machines locales en déterminant le chemin le plus court.

FreeBSD ajoutera également des routes de sous-réseau pour le sous-réseau local (`10.20.30.255` est l'adresse de diffusion pour le sous-réseau `10.20.30`, et `example.com` est le nom de domaine associé à ce sous-réseau). La dénomination `link#1` fait référence à la première carte Ethernet de la machine. Vous constaterez qu'il n'y a pas d'autre interface associée à ces routes.

Ces deux types de routes (vers les machines du réseau local et les sous-réseaux locaux) sont automatiquement configurés par un "daemon" appelé routed. S'il ne tourne pas, alors seules les routes définies comme statiques (i.e. explicitement définies) existeront.

La ligne `host1` fait référence à votre machine, qui est identifiée par l'adresse Ethernet. Puisque nous sommes l'émetteur, FreeBSD sait qu'il faut utiliser l'interface en "boucle" (lo0) plutôt que d'envoyer les données sur l'interface Ethernet.

Les deux lignes `host2` montrent ce qui se passe quand on utilise un alias avec ifconfig(8) (lisez la section sur l'Ethernet pour savoir pour quelles raisons on peut vouloir cela). Le symbole `=` qui suit l'interface lo0 indique que non seulement nous utilisons l'interface en "boucle" (puisque cette adresse correspond également à la machine locale), mais que c'est plus spécifiquement un alias. Ce

type de route n'apparaît que sur la machine pour laquelle est défini l'alias; sur toutes les autres machines du réseau local il n'y aura q'une ligne `link#1` pour cette machine.

La dernière ligne (le sous-réseau destinataire `224`) concerne le multicasting (diffusion pour plusieurs destinataires), qui sera abordé dans une autre section.

Et enfin, diverses caractéristiques de chaque route sont indiquées dans la colonne `Flags` (indicateurs). Ci-dessous, une courte table présente certains de ces indicateurs et leur signification:

U	Active ("Up"): la route est active.
H	Machine ("Host"): la destination de la route est une machine.
G	Passerelle ("Gateway"): envoyer tout ce qui concerne cette destination sur la machine distante indiquée, qui déterminera à qui transmettre ensuite.
S	Statique ("Static"): cette route a été configurée manuellement et non pas générée automatiquement par le système.
C	Clone: génère une nouvelle route sur la base de celle-ci pour les machines auxquelles nous nous connectons. Ce type de route est normalement utilisé pour les réseaux locaux.
W	Clonée ("WasCloned"): cette route a été auto-configurée (Clone) à partir d'une route pour le réseau local.
L	Lien ("Link"): la route fait référence à une adresse matérielle Ethernet.

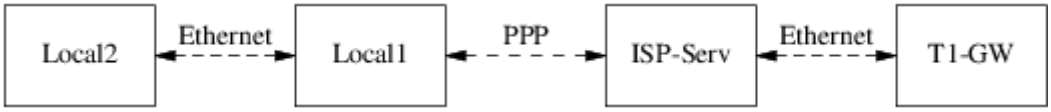
33.2.2. Routes par défaut

Quand le système local doit établir une connexion avec une machine distante, il consulte la table de routage pour voir s'il existe déjà une route connue. Si la machine distante appartient à un sous-réseau auquel le système sait se connecter (routes clonées), alors le système vérifie s'il peut se connecter via cette interface.

Si toutes les routes connues échouent, il reste alors au système une dernière option: la route par "défaut". Cette route est un type particulier de route passerelle (c'est généralement la seule du système), et est toujours marquée avec un `c` dans le champ des indicateurs. Pour les machines du réseau local, cette passerelle est définie avec la machine qui est directement connectée au monde extérieur (que ce soit par une liaison PPP, DSL, cable, T1, ou toute autre interface réseau).

Si vous configurez la route par défaut sur une machine qui fonctionne comme passerelle vers le monde extérieur, alors la route par défaut sera la passerelle de votre Fournisseur d'Accès à Internet (FAI).

Examinons un exemple de route par défaut. Voici une configuration classique:



Les machines `Local1` et `Local2` sont sur votre site. `Local1` est connectée au serveur du FAI via une liaison PPP par modem. Ce serveur PPP est connecté par l'intermédiaire d'un réseau local à un autre ordinateur passerelle relié au point d'entrée Internet du FAI.

Les routes par défaut sur chacune de vos machines seront:

Machine	Passerelle par défaut	Interface
Local2	Local1	Ethernet
Local1	T1-GW	PPP

Une question qui revient souvent est "Pourquoi (ou comment) définir `T1-GW` comme passerelle par défaut pour `Local1`, plutôt que le serveur du FAI auquel elle est connectée?".

Rappelez-vous, puisque l'interface PPP utilise, de votre côté de la connexion, une adresse IP du réseau local du FAI, les routes vers toute autre machine du réseau local du FAI seront automatiquement générées. Par conséquent vous savez déjà comment atteindre la machine `T1-GW`, il n'y a donc pas besoin d'étape intermédiaire qui passe par le serveur du FAI.

Il est habituel d'attribuer l'adresse `X.X.X.1` à la passerelle sur votre réseau local. Donc (dans notre exemple), si votre espace d'adresse de classe C local était `10.20.30` et que votre FAI utilisait l'espace `10.9.9`, alors les routes par défaut seraient:

Machine	Route par défaut
Local2 (10.20.30.2)	Local1 (10.20.30.1)
Local1 (10.20.30.1, 10.9.9.30)	T1-GW (10.9.9.1)

Vous pouvez aisément définir la route par défaut via le fichier /etc/rc.conf. Dans notre exemple, sur la machine `Local2`, nous avons ajouté la ligne suivante dans /etc/rc.conf:

```
defaultrouter="10.20.30.1"
```

Il est également possible de faire directement cela à partir de la ligne de commande avec la commande route(8):

```
# route add default 10.20.30.1
```

Pour plus d'informations sur la manipulation à la main des tables de routage réseau, consultez la page de manuel route(8).

33.2.3. Machines sur deux réseaux

Il y a un autre type de configuration dont il faut parler, c'est celle d'une machine qui est connectée à deux réseaux différents. Techniquement, toute machine servant de passerelle (comme dans l'exemple ci-dessus, en utilisant une connexion PPP) est une machine sur deux réseaux. Mais ce terme n'est normalement utilisé que pour faire référence à une machine qui est sur deux réseaux locaux différents.

Selon le cas, la machine dispose de deux cartes Ethernet, ayant chacune une adresse sur des sous-réseaux séparés. Alternativement, la machine peut ne disposer que d'une seule carte Ethernet, et utiliser des alias avec ifconfig(8). Le premier cas correspond à l'utilisation de deux réseaux Ethernet physiquement séparés, le deuxième cas est employé s'il n'y a qu'un seul réseau physique mais deux sous-réseaux logiquement distincts.

Dans les deux cas, les tables de routage sont définies de telle sorte que chaque sous-réseau sache que cette machine est la passerelle (route entrante) vers l'autre sous-réseau. Cette configuration, où la machine sert de routeur entre les deux sous-réseaux, est souvent utilisée quand il faut mettre en place un dispositif de sécurité: filtrage de paquets ou coupe-feu, dans l'une ou dans les deux directions.

Si vous voulez que cette machine transmette réellement les paquets entre les deux interfaces, vous devez demander à FreeBSD d'activer cette fonctionnalité. Lisez la section suivante pour plus de détails sur comment faire cela.

33.2.4. Mettre en place un routeur

Un routeur est un système qui transmet les paquets d'une interface à une autre. Les standards de l'Internet et de bons principes d'ingénierie empêchent le projet FreeBSD d'activer cette fonction par défaut sous FreeBSD. Vous pouvez l'activer en positionnant à `YES` la variable suivante du fichier rc.conf(5):

```
gateway_enable=YES          # Set to YES if this host will be a gateway
```

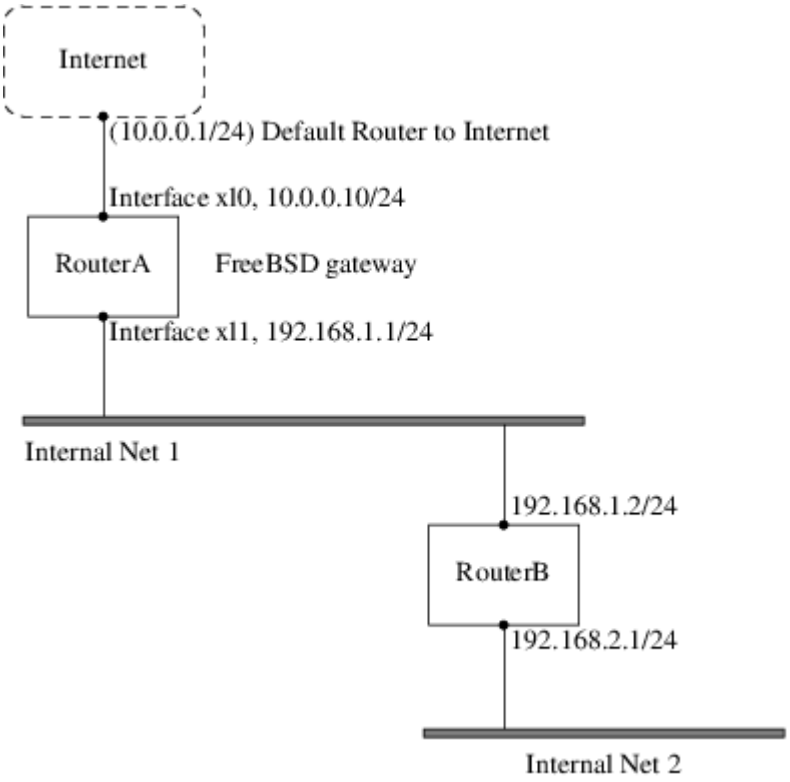
Cette option fixera la variable sysctl(8) `net.inet.ip.forwarding` à la valeur `1`. Si vous devez arrêter temporairement le routage, vous pouvez positionner la variable momentanément à `0`.

Votre nouveau routeur aura besoin de route pour savoir où envoyer le trafic. Si votre réseau est suffisamment simple vous pouvez utiliser des routes statiques. FreeBSD est également fourni avec le "daemon" de routage BSD standard routed(8), qui comprend et utilise les protocoles RIP (version 1 est 2) et IRDP. Le support de BGP v4, OSPF v2, et d'autres protocoles de routage sophistiqué est disponible avec le logiciel net/zebra. Des produits commerciaux comme GateD® sont également disponibles comme solutions avancées de routage.

33.2.5. Configurarion des routes statiques

33.2.5.1. Configuration manuelle

Supposons que nous avons un réseau comme celui-ci:



Dans ce scénario, `RouteurA` est notre machine FreeBSD qui joue le rôle de routeur pour l'Internet. Elle a une route par défaut vers `10.0.0.1` qui permet de se connecter au reste du monde extérieur. Nous supposerons que la machine `RouteurB` est correctement configurée et sait comment transmettre vers n'importe quelle destination (D'après notre schéma c'est relativement simple. Ajoutez juste une route par défaut sur `RouteurB` en utilisant `192.168.1.1` comme passerelle).

Si nous regardons la table de routage de `RouteurA` nous verrions quelque chose comme:

```
% netstat -nr
Routing tables

Internet:
Destination        Gateway            Flags    Refs      Use  Netif  Expire
default            10.0.0.1           UGS         0    49378    xl0
127.0.0.1          127.0.0.1          UH          0        6    lo0
10.0.0/24          link#1             UC          0        0    xl0
192.168.1/24       link#2             UC          0        0    xl1
```

Avec la table de routage actuelle, `RouteurA` ne sera pas en mesure d'atteindre notre réseau interne 2. Elle ne dispose pas de route pour `192.168.2.0/24`. Une manière de résoudre cela est d'ajouter manuellement la route. La commande suivante ajouterait le réseau interne 2 à la table de routage de `RouteurA` en utilisant `192.168.1.2` comme point intermédiaire:

```
# route add -net 192.168.2.0/24 192.168.1.2
```

Maintenant `RouteurA` peut joindre n'importe quelle machine du réseau `192.168.2.0/24`.

33.2.5.2. Configuration persistante

L'exemple précédent est parfait pour configurer une route statique sur un système en fonctionnement. Cependant, le problème est que l'information de routage ne sera pas conservée si vous redémarrez votre machine FreeBSD. L'addition d'une route statique doit se faire dans votre fichier /etc/rc.conf:

```
# Add Internal Net 2 as a static route
static_routes="internalnet2"
route_internalnet2="-net 192.168.2.0/24 192.168.1.2"
```

La variable `static_routes` est une liste de chaîne de caractères séparées par une espace. Chaque chaîne fait référence à un nom de route. Dans notre exemple nous avons qu'une seule chaîne dans `static_routes`. Cette chaîne est *internalnet2*. Nous ajoutons ensuite une variable de configuration appelée `route_internalnet2` dans laquelle nous mettons tous les paramètres de configuration que nous passerions à la commande route(8). Pour nous exemple précédent nous aurions utilisé la commande:

```
# route add -net 192.168.2.0/24 192.168.1.2
```

nous avons donc besoin de `"-net 192.168.2.0/24 192.168.1.2"`.

Comme cela a été précisé, nous pouvons avoir plus d'une chaîne dans la variable `static_routes`. Cela nous permet de créer plusieurs routes statiques. Les lignes suivantes donnent un exemple d'ajout de routes statiques pour les réseaux `192.168.0.0/24` et `192.168.1.0/24` sur un routeur imaginaire:

```
static_routes="net1 net2"
route_net1="-net 192.168.0.0/24 192.168.0.1"
route_net2="-net 192.168.1.0/24 192.168.1.1"
```

33.2.6. Propagation de route

Nous avons déjà expliqué comment définir nos routes vers le monde extérieur, mais pas comment le monde extérieur apprend à nous localiser.

Nous savons déjà que les tables de routages peuvent être renseignées pour que tout le trafic pour un espace d'adresses donné (dans nos exemples, un sous-réseau de classe C) soit envoyé à une machine précise de ce réseau, qui transmettra les paquets entrants.

Lorsqu'il attribue un espace d'adresses à votre site, votre fournisseur d'accès définira ses tables de routage de sorte que tout le trafic destiné à votre sous-réseau vous soit envoyé sur votre liaison PPP. Mais comment les sites à l'autre bout du pays savent-ils qu'ils doivent passer par votre fournisseur d'accès?

Il existe un mécanisme (assez semblable au système d'information distribué du DNS) qui conserve un enregistrement de tous les espaces d'adresses affectés, et définit leur point de connexion à la

dorsale Internet ("backbone"). La "dorsale" comprend les liaisons principales qui véhiculent le trafic Internet à travers le pays et le monde entier. Chaque machine de la dorsale dispose d'une copie de l'ensemble des tables maîtresses qui aiguillent le trafic pour un réseau donné vers le transporteur correspondant de la dorsale, et de là par l'intermédiaire de fournisseurs d'accès successifs, jusqu'à atteindre votre réseau.

C'est le rôle de votre fournisseur d'accès d'annoncer aux sites de la dorsale qu'il est le point de connexion (et par conséquent la route entrante) pour votre site. C'est ce que l'on appelle la propagation de route.

33.2.7. En cas de problème

Il se peut qu'il y ait parfois un problème avec la propagation de route et que certains sites ne puissent vous atteindre. La commande probablement la plus utile pour déterminer où une route est défaillante est la commande traceroute(8). Elle est également utile si vous n'arrivez pas à vous connecter à une machine distante (i.e. lorsque ping(8) échoue).

La commande traceroute(8) prend comme paramètre le nom de la machine distante avec laquelle vous essayez d'établir une connexion. Elle vous donnera la liste de passerelles intermédiaires jusqu'à la machine cible, ou jusqu'à ce qu'il n'y ait plus de connexion.

Pour plus d'informations, consultez la page de manuel de traceroute(8).

33.2.8. Routage multicast

FreeBSD supporte nativement les applications et le routage multicast (diffusion pour plusieurs destinataires). Les applications multicast ne nécessitent pas de configuration spécifique de FreeBSD, généralement, elles fonctionneront directement. Le routage multicast demande à ce que le support soit compilé dans le noyau:

```
options MROUTING
```

De plus, le "daemon" de routage multicast, mrouted(8) doit être configuré par l'intermédiaire du fichier /etc/mrouted.conf pour mettre en place des tunnels et le protocole DVMRP. Plus de détails sur la configuration du routage multicast peuvent être trouvés dans la page de manuel de mrouted(8).

33.3. Réseau sans fil

33.3.1. Introduction

Il peut être très utile de pouvoir utiliser un micro-ordinateur sans le désagrément d'être constamment relié à un câble réseau. FreeBSD peut être utilisé comme client sans fil, et même comme "point d'accès" sans fil.

33.3.2. Modes de fonctionnement des systèmes sans fils

Il existe deux manières différentes de configurer les périphériques sans fil 802.11: les modes BSS et IBSS.

33.3.2.1. Mode BSS

Le mode BSS est le mode généralement utilisé. Le mode BSS est également appelé mode infrastructure. Dans ce mode, plusieurs points d'accès sans fils sont connectés à un réseau câblé. Chaque réseau sans fil possède son propre nom. Ce nom est ce que l'on appelle le "SSID" du réseau.

Les clients sans fils se connectent à ces points d'accès sans fils. La norme IEEE 802.11 définie le protocole que les réseaux sans fils utilisent pour les connexions. Un client sans fil peut être attaché à un réseau particulier quand un SSID est fixé. Un client peut s'attacher à n'importe quel réseau en ne définissant pas explicitement de SSID.

33.3.2.2. Mode IBSS

Le mode IBSS, également appelé mode "ad-hoc", est conçu pour les connexions point à point. Il existe en fait deux types de mode ad-hoc. Le premier est le mode IBSS, également appelé mode ad-hoc ou IEEE ad-hoc. Ce mode est défini par les normes IEEE 802.11. Le deuxième mode est appelé ad-hoc démo ou encore mode ad-hoc Lucent (et parfois, ce qui prête à confusion, mode ad-hoc). C'est l'ancien mode ad-hoc pré-standard 802.11 et ne devrait être utilisé qu'avec d'anciennes installations. Nous ne parlerons pas des modes ad-hoc dans ce qui suit.

33.3.3. Mode infrastructure

33.3.3.1. Points d'accès

Un point d'accès est un périphérique sans fil qui permet à un ou plusieurs clients sans fils d'utiliser ce périphérique comme un hub. Quand ils utilisent un point d'accès, tous les clients communiquent par l'intermédiaire de ce point d'accès. Plusieurs points d'accès sont souvent utilisés pour couvrir l'intégralité d'une zone géographique comme une maison, une entreprise, ou un parc avec un réseau sans fil.

Les points d'accès ont généralement plusieurs connexions réseaux: la carte réseaux sans fil, et une ou plusieurs cartes réseaux Ethernet pour les connexions avec le reste du réseau.

Les points d'accès peuvent être achetés tout fait, ou vous pouvez construire le votre avec FreeBSD et une carte réseau sans fil supportée. De nombreux constructeurs proposent des points d'accès et des cartes réseaux sans fils avec diverses fonctionnalités.

33.3.3.2. Construire un point d'accès avec FreeBSD

33.3.3.2.1. Pré-requis

En vue de mettre en place un point d'accès sans fil sous FreeBSD, vous avez besoin d'une carte réseau sans fil compatible. Actuellement seule les cartes basées sur le circuit Prism sont supportées. Vous aurez également besoin d'une carte réseau câblée supportée par FreeBSD (cela ne devrait pas être difficile à trouver, FreeBSD supporte de nombreuses cartes). Dans le cadre de cette section,

nous supposerons que le trafic passera par un pont entre la carte sans fil et le réseau relié à la carte réseau classique.

Le mode point d'accès implémenté par FreeBSD fonctionne mieux avec certaines versions de firmware. Les cartes utilisant un circuit Prism 2 devraient utiliser un firmware 1.3.4 ou plus récent. Les cartes Prism 2.5 et Prism 3 devraient utiliser la version 1.4.9. Des versions de firmware plus anciennes pourront ne pas fonctionner correctement. Actuellement, la seule manière de mettre à jour vos cartes est d'utiliser les outils de mise à jour du firmware pour Windows® disponibles auprès du constructeur de votre carte.

33.3.3.2.2. Configuration

Assurez-vous tout d'abord que votre système voit la carte réseau sans fil:

```
# ifconfig -a
wi0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet6 fe80::202:2dff:fe2d:c938%wi0 prefixlen 64 scopeid 0x7
    inet 0.0.0.0 netmask 0xff000000 broadcast 255.255.255.255
    ether 00:09:2d:2d:c9:50
    media: IEEE 802.11 Wireless Ethernet autoselect (DS/2Mbps)
    status: no carrier
    ssid ""
    stationname "FreeBSD Wireless node"
    channel 10 authmode OPEN powersavemode OFF powersavesleep 100
    wepmode OFF weptxkey 1
```

Ne vous préoccupez pas des détails, verifiez juste que s'affiche quelque chose qui vous indique qu'une carte réseau sans fil est installée. Si vous avez des problèmes à voir l'interface réseau sans fil correspondante, et que vous utilisez une carte de type PC Card, vous devriez consultez les pages de manuel pccardc(8) et pccardd(8) pour plus d'information.

Ensuite, vous devrez charger un module afin de mettre en place la partie de FreeBSD faisant office de pont pour le point d'accès. Pour charger le module bridge(4), exécutez la commande suivante:

```
# kldload bridge
```

Vous ne devriez pas voir apparaître de message d'erreur lors du chargement du module. Si ce n'est pas le cas, vous devrez peut-être compiler le support bridge(4) dans votre noyau. La section sur le Bridging de ce manuel devrait pouvoir vous aider dans cette tâche.

Maintenant que cette partie est assurée, nous devons dire à FreeBSD entre quelles interface le pont doit être installé. Nous effectuons cette configuration en utilisant sysctl(8):

```
# sysctl net.link.ether.bridge.enable=1
# sysctl net.link.ether.bridge.config="wi0 xl0"
# sysctl net.inet.ip.forwarding=1
```

Sous les versions antérieures à la 5.2, vous devez utiliser à la place les options suivantes:

```
# sysctl net.link.ether.bridge=1
# sysctl net.link.ether.bridge_cfg="wi0,xl0"
# sysctl net.inet.ip.forwarding=1
```

Il est maintenant possible de configurer la carte. La commande suivante positionnera la carte en mode point d'accès:

```
# ifconfig wi0 ssid my_net channel 11 media DS/11Mbps mediaopt hostap up stationname
"FreeBSD AP"
```

La ligne ifconfig(8) active l'interface wi0, fixe son paramètre SSID à la valeur *my_net*, et fixe le nom de station à *FreeBSD AP*. L'option `media DS/11Mbps` positionne la carte dans le mode 11Mbps et est nécessaire pour que le paramètre `mediaopt` soit pris en compte. L'option `mediaopt hostap` place l'interface dans le mode point d'accès. L'option `channel 11` fixe le canal 802.11b à employer. La page de manuel wicontrol(8) donne les options de canaux valides en fonction de votre zone géographique.

Vous devez maintenant disposer d'un point d'accès opérationnel et en fonctionnement. Vous êtes encouragés à lire les pages de manuel wicontrol(8), ifconfig(8), et wi(4) pour plus d'amples informations.

Il est également conseillé de lire la section qui suit sur le chiffrage.

33.3.3.2.3. Information d'état

Une fois que le point d'accès est configuré et opérationnel, les opérateurs voudront voir quels clients sont associés avec le point d'accès. A n'importe quel instant, l'opérateur pourra taper:

```
# wicontrol -l
1 station:
00:09:b7:7b:9d:16  asid=04c0, flags=3<ASSOC,AUTH>, caps=1<ESS>, rates
=f<1M,2M,5.5M,11M>, sig=38/15
```

Ceci nous montre qu'une station est associée, ainsi que son paramétrage. Les informations indiquées concernant le signal devraient être utilisées uniquement comme une indication relative sur sa puissance. Sa conversion en dBm ou tout autre unité varie en fonction des différentes versions de firmware.

33.3.3.3. Clients

Un client sans fil est un système qui se connecte à un point d'accès ou un autre client directement.

Typiquement, les clients sans fils disposent d'une seule interface réseau, la carte réseau sans fil.

Il existe quelques manières différentes de configurer un client sans fil. Elles sont basées sur les

différents modes sans fils, généralement les modes BSS (mode infrastructure, qui nécessite un point d'accès), et IBSS (mode ad-hoc, ou mode point à point). Dans notre exemple, nous utiliserons le plus populaire des deux, le mode BSS, pour discuter avec un point d'accès.

33.3.3.3.1. Pré-requis

Il n'y a qu'un seul pré-requis pour configurer FreeBSD comme client sans fil. Vous aurez besoin d'une carte sans fil supportée par FreeBSD.

33.3.3.3.2. Configurer un client sans fil FreeBSD

Avant de commencer, vous aurez besoin de connaître certaines choses concernant le réseau sans fil auquel vous désirez vous connecter. Dans cet exemple, nous rejoignons un réseau ayant pour nom *my_net*, et avec le chiffrage des liaisons désactivé.

Dans cet exemple, nous n'utilisons pas le chiffrage des liaisons, ce qui est une situation dangereuse. Dans la section suivante, nous verrons comment activer le chiffrage, pourquoi il est important de le faire, et pourquoi certaines technologies de chiffrage ne vous protégerons pas complètement.

Assurez-vous que votre carte est reconnue par FreeBSD:

```
# ifconfig -a
wi0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet6 fe80::202:2dff:fe2d:c938%wi0 prefixlen 64 scopeid 0x7
    inet 0.0.0.0 netmask 0xff000000 broadcast 255.255.255.255
    ether 00:09:2d:2d:c9:50
    media: IEEE 802.11 Wireless Ethernet autoselect (DS/2Mbps)
    status: no carrier
    ssid ""
    stationname "FreeBSD Wireless node"
    channel 10 authmode OPEN powersavemode OFF powersavesleep 100
    wepmode OFF weptxkey 1
```

Maintenant, nous pouvons configurer la carte suivant les paramètres de notre réseau:

```
# ifconfig wi0 inet 192.168.0.20 netmask 255.255.255.0 ssid my_net
```

Remplacez `192.168.0.20` et `255.255.255.0` avec une adresse IP ainsi qu'un masque de sous-réseau valides de votre réseau câblé. Rappelez-vous, notre point d'accès joue le rôle de pont entre le réseau sans fil et le réseau câblé, il apparaîtra aux autres cartes sur votre réseau que vous êtes sur le même réseau câblé.

Une fois cela effectué, vous devriez être en mesure d'utiliser ping(8) pour atteindre les machines sur le réseau câblé de la même façon que si vous étiez connecté en utilisant un câble réseau standard.

Si vous rencontrez des problèmes avec votre connexion sans fil, vérifiez que vous êtes associé-

"associated" (connecté) avec le point d'accès:

```
# ifconfig wi0
```

devrait retourner un certain nombre d'information; et vous devriez voir s'afficher:

```
status: associated
```

Si `associated` n'est pas affiché, alors il se peut que vous soyez hors de portée du point d'accès, que vous ayez le chiffrage activé, ou peut-être que vous ayez un problème de configuration.

33.3.3.4. Chiffrement

L'utilisation du chiffrement sur un réseau sans fil est important parce que vous n'avez plus la possibilité de conserver le réseau dans une zone protégée. Vos données sans fil seront diffusées dans tout le voisinage, et toute personne désirant y accéder pourra le faire. C'est ici que le chiffrement entre en jeu. En chiffrant les données qui sont envoyées par les ondes, vous rendez plus difficile l'interception de celles-ci par quiconque d'intéressé.

Les deux méthodes les plus courantes de chiffrage des données entre un client et un point d'accès sont le protocol WEP et ipsec(4).

33.3.3.4.1. WEP

WEP est l'abbrévation de "Wired Equivalency Protocol". Le protocole de chiffrage WEP est une tentative de rendre les réseaux sans fils aussi sûrs et sécurisés qu'un réseau filaire. Malheureusement, il a été craqué, et est relativement simple à déjouer. Cela signifie que l'on ne doit pas lui faire confiance quand il est nécessaire de chiffrer des données sensibles.

Cela reste mieux que rien du tout, utilisez ce qui suit pour activer WEP sur votre nouveau point d'accès FreeBSD:

```
# ifconfig wi0 inet up ssid my_net wepmode on wepkey 0x1234567890 media DS/11Mbps
mediaopt hostap
```

Et vous pouvez activer WEP sur un client avec la commande:

```
# ifconfig wi0 inet 192.168.0.20 netmask 255.255.255.0 ssid my_net wepmode on wepkey
0x1234567890
```

Notez que vous devriez remplacer *0x1234567890* par une clé plus personnelle.

33.3.3.4.2. IPsec

ipsec(4) est un outil bien plus puissant et robuste pour chiffrer des données sur un réseau. C'est la méthode à préférer pour chiffrer les données sur un réseau sans fil. Vous pouvez obtenir plus de

détails concernant ipsec(4) et comment l'implémenter dans la section IPsec de ce manuel.

33.3.3.5. Outils

Il existe un petit nombre d'outils disponibles pour le débogage et la configuration d'un réseau sans fil, et nous tenterons ici d'en décrire certains ainsi que leurs fonctionnalités.

33.3.3.5.1. La suite bsd-airtools

La suite bsd-airtools est une trousse à outils complète qui comprend des outils d'audit sans fil pour le craquage du système WEP, la détection de points d'accès, etc.

Les utilitaires bsd-airtools peuvent être installés à partir du logiciel porté net-mgmt/bsd-airtools. Des instructions sur l'installation des logiciels portés peuvent être trouvées dans le Installer des applications. les logiciels pré-compilés et les logiciels portés de ce manuel.

Le programme `dstumbler` est l'outil qui permet la recherche de points d'accès et la mesure du rapport signal sur bruit. Si vous avez des difficultés à mettre en place et à faire fonctionner votre point d'accès, `dstumbler` pourra vous aider dans ce sens.

Pour tester la sécurité de votre réseau sans fil, vous pouvez choisir d'employer les outils "dweputils" (`dwepcrack`, `dwepdump` et `dwepkeygen`) pour vous aider à déterminer si WEP répond à vos besoins en matière de sécurité au niveau de votre réseau sans fil.

33.3.3.5.2. Les utilitaires `wicontrol`, `ancontrol` et `raycontrol`

Il existe des outils que vous pouvez utiliser pour contrôler le comportement de votre carte réseau sans fil sur le réseau sans fil. Dans les exemples précédents, nous avons choisi d'employer wicontrol(8) puisque notre carte sans fil utilise l'interface wi0. Si vous avez une carte sans fil Cisco, elle apparaîtrait comme an0, et vous utiliseriez alors le programme ancontrol(8).

33.3.3.5.3. La commande `ifconfig`

La commande ifconfig(8) propose plusieurs options identiques à celles de wicontrol(8), cependant il manque quelques options. Consultez la page de manuel d'ifconfig(8) pour les différents paramètres et options en ligne de commande.

33.3.3.6. Cartes supportées

33.3.3.6.1. Points d'accès

Les seules cartes actuellement supportées pour le mode BSS (points d'accès) sont celles basées sur les circuits Prism 2, 2.5, ou 3. Pour une liste complète, consultez la page de manuel de wi(4).

33.3.3.6.2. Clients 802.11b

Presque toutes les cartes réseaux sans fil 802.11b sont supportées sous FreeBSD. La plupart des cartes basées sur les circuits Prism, Spectrum24, Hermes, Aironet, et Raylink fonctionneront dans le mode IBSS (ad-hoc, point à point, et BSS).

33.3.3.6.3. Clients 802.11a 802.11g

Le pilote de périphérique ath(4) supporte les normes 802.11a et 802.11g. Si votre carte est basée sur un circuit Atheros, vous devriez être en mesure d'utiliser ce pilote.

Malheureusement il y a toujours de nombreux fabricants qui ne fournissent pas à la communauté des logiciels libres les informations concernant les pilotes pour leurs cartes considérant de telles informations comme des secrets industriels. Par conséquent, il ne reste aux développeurs de FreeBSD et d'autres systèmes d'exploitation libres que deux choix: développer les pilotes en passant par un long et pénible processus de "reverse engineering" ou utiliser les pilotes binaires existants disponibles pour la plateforme Microsoft® Windows®. La plupart des développeurs, y compris ceux impliqués dans FreeBSD, ont choisi cette dernière approche.

Grâce aux contributions de Bill Paul (wpaul), depuis FreeBSD 5.3-RELEASE, il existe un support "natif" pour la spécification d'interface des pilotes de périphérique réseau (Network Driver Interface Specification-NDIS). Le NDISulator FreeBSD (connu également sous le nom de Project Evil) prend un pilote binaire réseau Windows® et lui fait penser qu'il est en train de tourner sous Windows®. Cette fonctionnalité est relativement nouvelle, mais semble fonctionner correctement dans la plupart des tests.

Pour utiliser le NDISulator, vous avez besoin de trois choses:

1. les sources du noyau;
2. le pilote binaire Windows® XP (extension .SYS);
3. le fichier de configuration du pilote Windows® XP (extension .INF).

Vous aurez besoin de compiler le module d'interface du mini-pilote ndis(4). En tant que `root`:

```
# cd /usr/src/sys/modules/ndis
# make  make install
```

Recherchez les fichiers spécifiques à votre carte. Généralement, ils peuvent être trouvés sur les CDs livrés avec la carte ou sur le site du fabricant. Dans les exemples qui suivent nous utiliseront les fichiers W32DRIVER.SYS et W32DRIVER.INF.

L'étape suivante est de compiler le pilote binaire dans un module chargeable du noyau. Pour effectuer cela, en tant que `root`, rendez vous dans le répertoire du module if_ndis et copiez-y les fichiers du pilote Windows®:

```
# cd /usr/src/sys/modules/if_ndis
# cp /path/to/driver/W32DRIVER.SYS ./
# cp /path/to/driver/W32DRIVER.INF ./
```

Nous utiliserons maintenant l'utilitaire `ndiscvt` pour générer le fichier d'entête ndis_driver_data.h du pilote pour la compilation du module:

```
# ndiscvt -i W32DRIVER.INF -s W32DRIVER.SYS -o ndis_driver_data.h
```

Les options `-i` et `-s` précisent respectivement le fichier de configuration et le fichier binaire. Nous utilisons l'option `-o ndis_driver_data.h` car le Makefile recherchera ce fichier lors de la compilation du module.

Certains pilotes Windows® nécessitent des fichiers supplémentaires pour fonctionner. Vous pouvez les ajouter avec `ndiscvt` en utilisant l'option `-f`. Consultez la page de manuel ndiscvt(8) pour plus d'information.

Nous pouvons enfin compiler et installer le module du pilote:

```
# make  make install
```

Pour utiliser le pilote, vous devez charger les modules appropriés:

```
# kldload ndis
# kldload if_ndis
```

La première commande charge le pilote d'interface NDIS, la seconde charge l'interface réseau. Contrôlez la sortie de dmesg(8) à la recherche d'une quelconque erreur au chargement. Si tout s'est bien passé, vous devriez obtenir une sortie ressemblant à ce qui suit:

```
ndis0: <Wireless-G PCI Adapter> mem 0xf4100000-0xf4101fff irq 3 at device 8.0 on pci1
      ndis0: NDIS API version: 5.0
      ndis0: Ethernet address: 0a:b1:2c:d3:4e:f5
      ndis0: 11b rates: 1Mbps 2Mbps 5.5Mbps 11Mbps
      ndis0: 11g rates: 6Mbps 9Mbps 12Mbps 18Mbps 36Mbps 48Mbps 54Mbps
```

A partir de là, vous pouvez traiter le périphérique ndis0 comme n'importe quel périphérique sans fil (e.g. wi0) et consulter les premières sections de ce chapitre.

33.4. Bluetooth

33.4.1. Introduction

Bluetooth® est une technologie sans fil pour créer des réseaux personnels sans fils fonctionnant dans la bande 2.4 GHz ne nécessitant pas d'autorisation, avec une portée de 10 mètres. Les réseaux étant généralement composés de périphériques nomades comme les téléphones portables, les assistants personnels et les ordinateurs portables. Contrairement à l'autre technologie sans fil, Wi-Fi, Bluetooth® offre un niveau plus élevé de profils de service, par exemple des serveurs de fichiers semblables à FTP, "file pushing", transport de la voix, émulation de lignes séries, et bien plus.

La pile Bluetooth® sous FreeBSD utilise le système Netgraph (voir netgraph(4)). Une large gamme

d'adaptateurs USB Bluetooth® sont supportés par le pilote ng_ubt(4). Les périphériques Bluetooth® basés sur le circuit Broadcom BCM2033 sont supportés par les pilotes ubtbcmfw(4) et ng_ubt(4). La carte 3Com Bluetooth® PC Card 3CRWB60-A demande le pilote ng_bt3c(4). Les périphériques Bluetooth® de type série et UART sont supportés via les pilotes sio(4), ng_h4(4) et hcseriald(8). Cette section décrit l'utilisation d'un adaptateur USB Bluetooth®. Le support Bluetooth® est disponible sur les systèmes 5.0 et suivants.

33.4.2. Branchement du périphérique

Par défaut les pilotes de périphériques Bluetooth® sont disponibles sous la forme de modules du noyau. Avant de brancher le périphérique, vous devrez charger le pilote dans le noyau:

```
# kldload ng_ubt
```

Si le périphérique Bluetooth® est présent au démarrage du système, chargez le module à partir de /boot/loader.conf:

```
ng_ubt_load="YES"
```

Branchez votre clé USB. Une sortie semblable à celle-ci devrait s'afficher sur la console (ou dans les journaux du système):

```
ubt0: vendor 0x0a12 product 0x0001, rev 1.10/5.25, addr 2
ubt0: Interface 0 endpoints: interrupt=0x81, bulk-in=0x82, bulk-out=0x2
ubt0: Interface 1 (alt.config 5) endpoints: isoc-in=0x83, isoc-out=0x3,
      wMaxPacketSize=49, nframes=6, buffer size=294
```

La pile Bluetooth doit être lancée manuellement sous FreeBSD 6.0, et sous les versions 5.0 antérieures à la 5.5. Ce lancement est automatique à partir de devd(8) sous FreeBSD 5.5, 6.1 et versions suivantes.

Copiez /usr/shared/examples/netgraph/bluetooth/rc.bluetooth à un emplacement adapté, comme /etc/rc.bluetooth. Cette procédure est utilisée pour démarrer et arrêter la pile Bluetooth®. C'est une bonne idée d'arrêter la pile avant de débrancher le périphérique, mais ce n'est pas (généralement) fatal. Quand la pile démarre, vous devriez avoir des messages similaires aux suivants:

```
# /etc/rc.bluetooth start ubt0
BD_ADDR: 00:02:72:00:d4:1a
Features: 0xff 0xff 0xf 00 00 00 00 00
<3-Slot> <5-Slot> <Encryption> <Slot offset>
<Timing accuracy> <Switch> <Hold mode> <Sniff mode>
<Park mode> <RSSI> <Channel quality> <SCO link>
<HV2 packets> <HV3 packets> <u-law log> <A-law log> <CVSD>
<Paging scheme> <Power control> <Transparent SCO data>
Max. ACL packet size: 192 bytes
```

```
Number of ACL packets: 8
Max. SCO packet size: 64 bytes
Number of SCO packets: 8
```

33.4.3. Interface de contrôle de l'hôte (HCI)

L'interface de contrôle de l'hôte (HCI) fournit une interface de commande pour le contrôleur de la bande de base et le gestionnaire de liaisons, et l'accès à l'état du matériel et aux registres de contrôle. Cette interface offre une méthode uniforme d'accès aux fonctions de la bande de base Bluetooth®. La couche HCI de l'hôte échange des données et des commandes avec le firmware HCI du matériel Bluetooth®. Le pilote de la couche de transport du contrôleur d'hôte (i.e. le bus physique) fournit aux deux couches HCI la possibilité d'échanger des informations entre elles.

Un seul noeud Netgraph de type *hci* est créé pour un périphérique Bluetooth®. Le noeud HCI est normalement connecté au noeud du pilote Bluetooth® (flux descendant) et au noeud L2CAP (flux montant). Toutes les opérations HCI doivent être effectuées sur le noeud HCI et non pas sur le noeud du pilote de périphérique. Le nom par défaut pour le noeud HCI est "devicehci". Pour plus de détails consultez la page de manuel ng_hci(4).

Une des tâches les plus courantes est la recherche de périphériques Bluetooth® dans le voisinage hertzien. Cette opération est appelée *inquiry* (enquête, recherche). Cette recherche et les autres opérations relatives à HCI sont effectuées par l'utilitaire hccontrol(8). L'exemple ci-dessous montre comment déterminer quels périphériques Bluetooth® sont dans le voisinage. Vous devriez obtenir une listes de périphériques au bout de quelques secondes. Notez qu'un périphérique distant ne répondra à la recherche que s'il est placé dans le mode *discoverable*.

```
% hccontrol -n ubt0hci inquiry
Inquiry result, num_responses=1
Inquiry result #0
       BD_ADDR: 00:80:37:29:19:a4
       Page Scan Rep. Mode: 0x1
       Page Scan Period Mode: 00
       Page Scan Mode: 00
       Class: 52:02:04
       Clock offset: 0x78ef
Inquiry complete. Status: No error [00]
```

BD_ADDR est l'adresse unique d'un périphérique Bluetooth®, similaire à l'adresse MAC d'une carte réseau. Cette adresse est nécessaire pour communiquer avec un périphérique. Il est possible d'assigner un nom humainement compréhensible à l'adresse BD_ADDR. Le fichier /etc/bluetooth/hosts contient des informations concernant les hôtes Bluetooth® connus. L'exemple suivant montre comment obtenir le nom qui a été assigné au périphérique distant:

```
% hccontrol -n ubt0hci remote_name_request 00:80:37:29:19:a4
BD_ADDR: 00:80:37:29:19:a4
Name: Pav's T39
```

Si vous effectuez une recherche sur un périphérique Bluetooth® distant, vous devriez trouver votre ordinateur en tant que "votre.machine.nom (ubt0)". Le nom affecté au périphérique local peut être modifié à tout moment.

Le système Bluetooth® fournit une connexion point à point (seules deux matériels Bluetooth® sont concernés), ou une connexion point à multipoints. Dans le cas d'une connexion point à multipoints, la connexion est partagés entre plusieurs périphériques Bluetooth®. L'exemple suivant montre comment obtenir la liste des connexions en bande de base actives pour le périphérique local:

```
% hccontrol -n ubt0hci read_connection_list
Remote BD_ADDR    Handle Type Mode Role Encrypt Pending Queue State
00:80:37:29:19:a4     41  ACL    0 MAST    NONE       0     0 OPEN
```

Une *manipulation de la connexion* est utile quand la fin d'une connexion en bande de base est nécessaire. Notez qu'il n'est normalement pas nécessaire de le faire à la main. La pile mettra fin automatiquement aux connexions en bande de base inactives.

```
# hccontrol -n ubt0hci disconnect 41
Connection handle: 41
Reason: Connection terminated by local host [0x16]
```

Référez-vous à la commande `hccontrol help` pour une liste complète des commandes HCI disponibles. La plupart des commandes HCI ne nécessitent pas les privilèges du super-utilisateur.

33.4.4. Protocole d'adaptation et de contrôle de lien logique (L2CAP)

Le protocole d'adaptation et de contrôle de lien logique (L2CAP) fournit des services orientés connexion ou non aux protocoles de niveaux supérieurs, et cela avec des possibilités de multiplexage de protocoles, de segmentation et de réassemblage. L2CAP permet aux applications et aux protocoles de niveaux supérieurs de transmettre et recevoir des paquets L2CAP d'une taille allant jusqu'à 64 Ko.

L2CAP est basé sur le concept de *canaux*. Un canal est une connexion logique au sommet de la connexion en bande de base. Chaque canal est attaché à un protocole suivant le schéma plusieurs-vers-un. Plusieurs canaux peuvent être attachés au même protocole, mais un canal ne peut être attachés à plusieurs protocoles. Chaque paquet L2CAP reçu sur un canal est dirigé vers le protocole de niveau supérieur approprié. Plusieurs canaux peuvent partager la même connexion en bande de base.

Un seul noeud Netgraph de type *l2cap* est créé pour un périphérique Bluetooth®. Le noeud L2CAP est normalement connecté au noeud HCI Bluetooth® (flux descendant) et aux noeuds des "sockets" Bluetooth® (flux montant). Le nom par défaut pour le noeud L2CAP est "device2cap". Pour plus de détails consultez la page de manuel ng_l2cap(4).

Une commande utile est l2ping(8), qui peut être utilisée pour "pinguer" les autres périphériques. Certaines implémentations de Bluetooth® peuvent ne pas renvoyer toutes les données qui leur sont envoyées, aussi `0 bytes` dans ce qui suit est normal.

```
# l2ping -a 00:80:37:29:19:a4
0 bytes from 0:80:37:29:19:a4 seq_no=0 time=48.633 ms result=0
0 bytes from 0:80:37:29:19:a4 seq_no=1 time=37.551 ms result=0
0 bytes from 0:80:37:29:19:a4 seq_no=2 time=28.324 ms result=0
0 bytes from 0:80:37:29:19:a4 seq_no=3 time=46.150 ms result=0
```

L'utilitaire l2control(8) est employé pour effectuer diverses opérations sur les noeuds L2CAP. Cet exemple montre comment obtenir la liste des connexions logiques (canaux) et la liste des connexions en bande de base pour le périphérique local:

```
% l2control -a 00:02:72:00:d4:1a read_channel_list
L2CAP channels:
Remote BD_ADDR     SCID/ DCID   PSM  IMTU/ OMTU State
00:07:e0:00:0b:ca    66/   64     3   132/  672 OPEN
% l2control -a 00:02:72:00:d4:1a read_connection_list
L2CAP connections:
Remote BD_ADDR    Handle Flags Pending State
00:07:e0:00:0b:ca     41 O           0 OPEN
```

Un autre outil de diagnostic est btsockstat(1). Il effectue un travail similaire à celui de netstat(1), mais relatif aux structures de données réseau Bluetooth®. L'exemple ci-dessous montre la même connexion logique que l2control(8) ci-dessus.

```
% btsockstat
Active L2CAP sockets
PCB      Recv-Q Send-Q Local address/PSM       Foreign address   CID   State
c2afe900      0      0 00:02:72:00:d4:1a/3     00:07:e0:00:0b:ca 66    OPEN
Active RFCOMM sessions
L2PCB    PCB      Flag MTU   Out-Q DLCs State
c2afe900 c2b53380 1    127   0     Yes  OPEN
Active RFCOMM sockets
PCB      Recv-Q Send-Q Local address     Foreign address   Chan DLCI State
c2e8bc80      0    250 00:02:72:00:d4:1a 00:07:e0:00:0b:ca 3    6    OPEN
```

33.4.5. Protocole RFCOMM

Le protocole RFCOMM permet l'émulation du port série au-dessus du protocole L2CAP. Le protocole est basé sur la norme ETSI TS 07.10. RFCOMM est un protocole de transport simple, avec les dispositions supplémentaires pour émuler les 9 circuits (signaux) d'un port série RS232 (EIATIA-232-E). Le protocole RFCOMM supporte jusqu'à 60 connexions simultanées (canaux RFCOMM) entre deux périphériques Bluetooth®.

Dans le cas de RFCOMM, l'établissement d'une communication implique deux applications tournant sur des périphériques différents (les extrémités de la communication) avec un segment de communication entre eux. RFCOMM est prévu pour couvrir les applications faisant usage des ports séries des périphériques sur lesquels elles résident. Le segment de communication est une liaison

Bluetooth® d'un périphérique vers un autre (connexion directe).

RFCOMM est seulement concerné par la connexion entre périphériques dans le cas d'un raccordement direct, ou entre le périphérique et un modem dans le cas d'un réseau. RFCOMM peut supporter d'autres configurations, comme les modules qui communiquent par l'intermédiaire de la technologie sans fil Bluetooth® d'un côté et utilise une interface câblée de l'autre côté.

Sous FreeBSD, le protocole RFCOMM est implémenté au niveau de la couche des "sockets" Bluetooth®.

33.4.6. Couplage des périphériques

Par défaut, une communication Bluetooth® n'est pas authentifiée, et n'importe quel périphérique peut parler avec n'importe quel autre périphérique. Un périphérique Bluetooth® (par exemple un téléphone portable) peut choisir de demander une authentification pour fournir un service particulier (par exemple un service de connexion téléphonique). L'authentification Bluetooth® est généralement effectuée avec des *codes PIN*. Un code PIN est une chaîne ASCII d'une longueur de 16 caractères. L'utilisateur doit entrer le même code PIN sur les deux périphériques. Une fois que l'utilisateur a entré le code PIN, les deux périphériques génèrent une *clé de liaison* (link key). Ensuite la clé peut être enregistrée soit dans les périphériques eux-mêmes ou sur un moyen de stockage non-volatile. La fois suivante les deux périphériques utiliseront la clé précédemment générée. La procédure décrite est appelée *couplage*. Si la clé de liaison est perdue par un des périphériques alors l'opération de couplage doit être répétée.

Le "daemon" hcsecd(8) est responsable de la gestion de toutes les requêtes d'authentification Bluetooth®. Le fichier de configuration par défaut est /etc/bluetooth/hcsecd.conf. Un exemple de section pour un téléphone portable avec un code PIN arbitraire de "1234" est donné ci-dessous:

```
device {
        bdaddr  00:80:37:29:19:a4;
        name    "Pav's T39";
        key     nokey;
        pin     "1234";
      }
```

Il n'y pas de limitation sur les codes PIN (en dehors de la longueur). Certains périphériques (comme les casques-micro Bluetooth®) peuvent avoir un code PIN définitivement fixé. Le paramètre `-d` force le "daemon" hcsecd(8) à rester en tâche de fond, il est donc aisé de voir ce qu'il se passe. Configurez le périphérique distant pour recevoir le couplage et initier la connexion Bluetooth® vers le périphérique distant. Le périphérique distant devrait annoncer que le couplage a été accepté, et demander le code PIN. Entrez le même code PIN que celui que vous avez dans le fichier hcsecd.conf. Maintenant votre PC et le périphérique distant sont couplés. Alternativement, vous pouvez initier le couplage sur le périphérique distant.

Sous FreeBSD 5.5, 6.1 et versions suivantes, la ligne suivante peut être ajoutée au fichier /etc/rc.conf pour obtenir un lancement automatique de hcsecd au démarrage du système:

```
hcsecd_enable="YES"
```

Ce qui suit est une partie de la sortie du "daemon" hcsecd:

```
hcsecd[16484]: Got Link_Key_Request event from 'ubt0hci', remote bdaddr
0:80:37:29:19:a4
hcsecd[16484]: Found matching entry, remote bdaddr 0:80:37:29:19:a4, name 'Pav's T39',
link key doesn't exist
hcsecd[16484]: Sending Link_Key_Negative_Reply to 'ubt0hci' for remote bdaddr
0:80:37:29:19:a4
hcsecd[16484]: Got PIN_Code_Request event from 'ubt0hci', remote bdaddr
0:80:37:29:19:a4
hcsecd[16484]: Found matching entry, remote bdaddr 0:80:37:29:19:a4, name 'Pav's T39',
PIN code exists
hcsecd[16484]: Sending PIN_Code_Reply to 'ubt0hci' for remote bdaddr 0:80:37:29:19:a4
```

33.4.7. Le protocole de découverte de service (SDP)

Le protocole de découverte de service (SDP) offre aux applications clientes les moyens de découvrir l'existence des services fournis par les applications serveurs ainsi que les propriétés (attributs) de ces services. Les attributs d'un service comprennent le type ou la classe du service offert et le mécanisme ou l'information sur le protocole nécessaire pour utiliser le service.

Le SDP implique la communication entre un serveur SDP et un client SDP. Le serveur maintient une liste d'enregistrements de services qui décrit les caractéristiques des services associés avec le serveur. Chaque enregistrement de service contient l'information sur un seul serveur. Un client peut récupérer l'information à partir d'un enregistrement de service maintenu par le serveur SDP en émettant une requête SDP. Si le client, ou une application associée avec le client, décide d'utiliser un service, il doit ouvrir une connexion séparée avec le fournisseur du service afin d'utiliser ce service. Le SDP fournit un mécanisme pour découvrir les services et leur attributs, mais n'offre pas de mécanisme pour utiliser ces services.

Généralement, un client SDP recherche les services sur la base de caractéristiques de services désirées. Cependant, il est parfois désirable de découvrir quel type de services sont décrits par les enregistrements de services d'un serveur SDP sans aucune information préalable sur les services. Ce processus de recherche des services offerts est appelé *navigation* ("browsing").

Le serveur SDP Bluetooth® sdpd(8) et le client en ligne de commande sdpcontrol(8) font partie de l'installation FreeBSD standard. L'exemple suivant montre comment effectuer un requête de navigation ("browse") SDP:

```
% sdpcontrol -a 00:01:03:fc:6e:ec browse
Record Handle: 00000000
Service Class ID List:
        Service Discovery Server (0x1000)
Protocol Descriptor List:
        L2CAP (0x0100)
```

```
                Protocol specific parameter #1: u/int/uuid16 1
                Protocol specific parameter #2: u/int/uuid16 1

Record Handle: 0x00000001
Service Class ID List:
        Browse Group Descriptor (0x1001)

Record Handle: 0x00000002
Service Class ID List:
        LAN Access Using PPP (0x1102)
Protocol Descriptor List:
        L2CAP (0x0100)
        RFCOMM (0x0003)
                Protocol specific parameter #1: u/int8/bool 1
Bluetooth Profile Descriptor List:
        LAN Access Using PPP (0x1102) ver. 1.0
```

i. et ainsi de suite. Remarquez que chaque service a une liste d'attributs (canal RFCOMM par exemple). En fonction du service vous pourrez avoir besoin de prendre note de certains de ces attributs. Certaines implémentations Bluetooth® ne supportent pas les requêtes de navigation et peuvent renvoyer une liste vide. Dans ce cas il est possible de chercher un service spécifique. L'exemple ci-dessous montre comment chercher le service OBEX Object Push (OPUSH):

```
% sdpcontrol -a 00:01:03:fc:6e:ec search OPUSH
```

Offrir des services sous FreeBSD aux clients Bluetooth® se fait à l'aide du serveur sdpd(8). Sous les versions de FreeBSD 5.5, 6.1 et plus récentes, la ligne suivante peut être ajoutée au fichier /etc/rc.conf:

```
sdpd_enable="YES"
```

Ensuite, le "démon"sdpd peut être démarré avec:

```
# /etc/rc.d/sdpd start
```

Sous FreeBSD 6.0, et sous les versions FreeBSD 5.X antérieures à 5.5, sdpd n'est pas intégré aux procédures de démarrage du système. Il doit être lancé manuellement:

```
# sdpd
```

L'application serveur locale qui désire offrir un service Bluetooth® à des clients distants enregistrera le service auprès du "daemon" SDP local. Un exemple d'une telle application est rfcomm_pppd(8). Une fois démarré, il enregistrera un service de réseau local Bluetooth® auprès du serveur SDP local.

La liste des services enregistrés auprès du serveur SDP local peut être obtenue en émettant une requête de navigation ("browse") SDP par l'intermédiaire du canal de contrôle:

```
# sdpcontrol -l browse
```

33.4.8. Les profils Dial-Up Networking (DUN) et accès au réseau local avec PPP (LAN)

Le profil Dial-Up Networking (DUN) est principalement utilisé avec les modems et les téléphones portables. Les cas de figure couverts par ce profil sont les suivants:

- Utilisation d'un téléphone portable ou d'un modem par un ordinateur comme modem sans fil pour se connecter à un serveur d'accès Internet, ou pour l'utilisation de services accessibles par téléphone;
- Utilisation d'un téléphone portable ou d'un modem par un ordinateur pour recevoir des appels avec transmission de données.

Le profil d'accès au réseau local avec PPP (LAN) peut être utilisé dans les situations suivantes:

- Accès au réseau local pour un périphérique Bluetooth®;
- Accès au réseau local pour plusieurs périphériques Bluetooth®;
- Liaison PC à PC (en utilisant le protocole PPP sur une émulation de câble série).

Sous FreeBSD les deux profils sont implémentés par ppp(8) et rfcomm_pppd(8)-un "wrapper" convertit la connexion Bluetooth® RFCOMM en quelque chose d'utilisable par PPP. Avant qu'un profil ne soit utilisable, un nouveau label doit être créé dans le fichier /etc/ppp/ppp.conf. Consultez la page de manuel rfcomm_pppd(8) pour des exemples.

Dans l'exemple suivant rfcomm_pppd(8) sera employé pour ouvrir un connexion RFCOMM avec le périphérique distant avec une adresse BD_ADDR 00:80:37:29:19:a4 sur un canal DUN RFCOMM. Le numéro de canal RFCOMM réel sera obtenu du périphérique distant par l'intermédiaire de SDP. Il est possible de préciser le canal RFCOMM à la main, dans ce cas rfcomm_pppd(8) n'émettra pas de requête SDP. Utilisez sdpcontrol(8) pour trouver le canal RFCOMM sur le périphérique distant.

```
# rfcomm_pppd -a 00:80:37:29:19:a4 -c -C dun -l rfcomm-dialup
```

Afin de fournir un service d'accès au réseau local avec PPP, le serveur sdpd(8) doit être en fonctionnement. Une nouvelle entrée pour les clients du réseau local doit être créée dans le fichier /etc/ppp/ppp.conf. Consultez la page de manuel rfcomm_pppd(8) pour des exemples. Enfin, lancez le serveur RFCOMM PPP sur un numéro de canal RFCOMM valide. Le serveur RFCOMM PPP enregistrera automatiquement un service Bluetooth® LAN auprès du "daemon" SDP local. L'exemple ci-dessous montre comment démarrer le serveur RFCOMM PPP:

```
# rfcomm_pppd -s -C 7 -l rfcomm-server
```

33.4.9. Le profil OBEX Object Push (OPUSH)

OBEX (échange d'objets) est un protocole très largement utilisé pour les transferts de fichiers entre périphériques mobiles. Son utilisation principale se trouve dans les communications par infrarouge, où il est utilisé pour le transfert des fichiers entre ordinateurs portables ou PDAs, et pour envoyer des cartes de visite électronique ou des éléments d'agenda entre téléphones portables et d'autres périphériques disposant d'applications de gestion d'informations personnelles (PIM).

Le serveur et le client OBEX sont implémentés dans le logiciel tierce-partie obexapp, qui est disponible sous la forme du logiciel porté comms/obexapp.

Le client OBEX est employé pour "pousser" et/ou "tirer" des objets du serveur OBEX. Un objet peut être, par exemple, une carte de visite ou un rendez-vous. Le client OBEX peut obtenir un numéro de canal RFCOMM d'un périphérique distant par l'intermédiaire de SDP. Cela peut être fait en spécifiant le nom du service plutôt que le numéro du canal RFCOMM. Les noms de service supportés sont: IrMC, FTRN et OPUSH. Il est possible de préciser le canal RFCOMM par un nombre. Un exemple de session OBEX est présenté ci-dessous, où l'objet information du périphérique d'un téléphone portable est récupéré, et un nouvel objet (carte de visite) est envoyé dans le répertoire du téléphone.

```
% obexapp -a 00:80:37:29:19:a4 -C IrMC
obex> get telecom/devinfo.txt devinfo-t39.txt
Success, response: OK, Success (0x20)
obex> put new.vcf
Success, response: OK, Success (0x20)
obex> di
Success, response: OK, Success (0x20)
```

Afin de fournir le service OBEX Object Push, le serveur sdpd(8) doit tourner. Un dossier racine où tous les objets entrant seront stockés doit être créé. Le chemin d'accès par défaut du répertoire racine est /var/spool/obex. Le serveur OBEX enregistrera automatiquement le service OBEX Object Push auprès du "daemon" SDP local. L'exemple ci-dessous montre comment démarrer le serveur OBEX:

```
# obexapp -s -C 10
```

33.4.10. Le profil port série (SPP)

Le profil port série (SPP) permet aux périphériques Bluetooth® d'émuler un câble série RS232 (ou similaire). Ce profil traite avec les applications classiques en utilisant Bluetooth® comme un câble de remplacement, à travers une abstraction de port série virtuel.

L'utilitaire rfcomm_sppd(1) implémente le profil port série. Un pseudo terminal est utilisé comme abstraction de port série virtuel. L'exemple ci-dessous montre comment se connecter à un service port série d'un périphérique distant. Notez que vous n'avez pas besoin d'indiquer un canal RFCOMM - rfcomm_sppd(1) peut l'obtenir auprès du périphérique distant via SDP. Si vous désirez forcer cela, spécifiez un canal RFCOMM sur la ligne de commande.

```
# rfcomm_sppd -a 00:07:E0:00:0B:CA -t /dev/ttyp6
rfcomm_sppd[94692]: Starting on /dev/ttyp6...
```

Une fois connecté, le pseudo-terminal peut être utilisé comme un port série:

```
# cu -l ttyp6
```

33.4.11. Dépannage

33.4.11.1. Un périphérique distant ne peut pas se connecter

Certains anciens périphériques Bluetooth® ne supportent pas de changement de rôle. Par défaut, quand FreeBSD accepte une nouvelle connexion, il tente d'effectuer un changement de rôle et de devenir maître. Les périphériques qui ne supportent pas cela ne seront pas en mesure de se connecter. Notez qu'un changement de rôle est effectué quand une nouvelle connexion est établie, il n'est donc pas possible de demander au périphérique distant s'il supporte le changement de rôle. Il existe une option HCI pour désactiver le changement de rôle au niveau local:

```
# hccontrol -n ubt0hci write_node_role_switch 0
```

33.4.11.2. Quelque chose ne va pas, puis-je voir ce qui se passe exactement?

Bien sûr. Utilisez le logiciel tierce-partie hcidump qui est disponible sous comms/hcidump dans le catalogue des logiciels portés. L'utilitaire hcidump est similaire à tcpdump(1). Il peut être utilisé pour afficher le contenu des paquets Bluetooth® à l'écran et les sauvegarder dans un fichier.

33.5. Bridging

33.5.1. Introduction

Il est parfois utile de diviser un réseau physique (comme un réseau Ethernet) en deux réseaux séparés sans avoir à créer de sous-réseaux IPs et à utiliser un routeur pour connecter ces réseaux entre eux. Le périphérique qui connecte ensemble deux réseaux de cette manière est appelé "bridge"-pont. Un système FreeBSD avec deux cartes réseaux peut faire fonction de pont.

Le pont apprend les adresses MAC (adresses Ethernet) des périphériques branchés sur chacune de ses interfaces réseaux. Il transmet le trafic entre deux réseaux uniquement quand la source et la destination sont sur des réseaux différents.

Sous de nombreux aspects, un pont ressemble à un switch (commutateur) Ethernet avec très peu de ports.

33.5.2. Situations où l'utilisation d'un pont est appropriée

Il existe deux situations dans lesquelles un pont est de nos jours utilisé.

33.5.2.1. Trafic important sur un segment

La première situation apparaît quand un segment physique d'un réseau est submergé par le trafic, mais vous ne voulez pas, pour différentes raisons, subdiviser le réseau et interconnecter les sous-réseaux à l'aide d'un routeur.

Prenons comme exemple un journal où les bureaux de la rédaction et de la production sont sur le même sous-réseau. Les utilisateurs de la rédaction utilisent tous le serveur de fichiers `A`, et les utilisateurs de la production le serveur `B`. Un réseau Ethernet est utilisé pour connecter ensemble les utilisateurs, et des surcharges du réseau ralentissent les échanges.

Si les utilisateurs de la rédaction peuvent être cantonné sur un segment, et les utilisateurs de la production sur un autre, les deux réseaux pourront être connectés par un pont. Seul le trafic réseau destiné aux interfaces réseaux situées de l'"autre" côté du pont sera transmis à l'autre réseau, réduisant ainsi les congestions sur chaque segment.

33.5.2.2. Coupe-feu filtrant/régulant le trafic

La deuxième situation est quand un coupe-feu est nécessaire mais sans translation d'adresses (NAT).

Un exemple est une compagnie qui est connectée à son fournisseur d'accès internet par l'intermédiaire d'une connexion ISDN ou DSL. Elle dispose de 13 adresses IP routables fournies par le fournisseur d'accès et dispose de 10 PCs sur son réseau. Dans cette situation, utiliser un coupe-feu/routeur est complexe en raison des problèmes de sous-réseaux.

Un coupe-feu basé sur un pont peut être configuré et positionné dans le flux juste en aval de leur routeur DSL/ISDN sans aucun problème d'adressage IP.

33.5.3. Configuration d'un pont

33.5.3.1. Choix des cartes réseaux

Un pont nécessite au moins deux cartes réseaux pour fonctionner. Malheureusement toutes les cartes réseaux ne supportent pas le mode bridging. Lisez la page de manuel bridge(4) pour des détails sur les cartes supportées.

Installez et testez les deux cartes réseaux avant de poursuivre.

33.5.3.2. Modification de la configuration du noyau

Pour activer le support nécessaire pour mettre en place un pont ajouter la ligne suivante:

```
options BRIDGE
```

à votre fichier de configuration du noyau, et recompilez votre noyau.

33.5.3.3. Support du coupe-feu

Si vous projetez d'utiliser un pont en tant que coupe-feu, vous devrez également ajouter l'option `IPFIREWALL`. Lisez la Firewalls pour des informations générales sur la configuration d'un pont en tant que coupe-feu.

Si vous avez besoin de permettre le passage à travers le pont des paquets non-IP (comme ARP), il existe une option du coupe-feu qui doit être activée. Cette option est `IPFIREWALL_DEFAULT_TO_ACCEPT`. Prennez note que cela modifie le fonctionnement par défaut du coupe-feu, ce dernier acceptera alors tous les paquets. Assurez-vous de savoir ce que ce changement signifie pour votre ensemble de règles de filtrage avant de l'effectuer.

33.5.3.4. Support de la régulation du trafic

Si vous désirez utiliser le pont comme régulateur de trafic, vous devrez ajouter l'option `DUMMYNET` à votre fichier de configuration du noyau. Consultez la page de manuel dummynet(4) pour plus d'information.

33.5.4. Activer le pont

Ajoutez la ligne:

```
net.link.ether.bridge.enable=1
```

au fichier /etc/sysctl.conf pour activer le pont au démarrage, et la ligne:

```
net.link.ether.bridge.config=if1,if2
```

pour activer le mode bridging sur les interfaces spécifiées (remplacez *if1* et *if2* par les noms de vos interfaces réseaux). Si vous désirez que les paquets traversant le pont soient filtrés par ipfw(8), vous devrez ajouter également la ligne:

```
net.link.ether.bridge.ipfw=1
```

Pour les versions antérieures à FreeBSD 5.2-RELEASE, utilisez les lignes suivantes:

```
net.link.ether.bridge=1
net.link.ether.bridge_cfg=if1,if2
net.link.ether.bridge_ipfw=1
```

33.5.5. Informations supplémentaires

Si vous désirez être en mesure de vous connecter au pont par l'intermédiaire de ssh(1), il est correct d'ajouter à l'une des cartes réseaux une adresse IP. Il existe un consensus sur le fait qu'assigner une adresse aux deux cartes est une mauvaise idée.

Si vous avez plusieurs ponts sur votre réseau, il ne peut y en avoir plus d'un sur le chemin qui sera emprunté par le trafic entre deux stations de travail. Techniquement, cela signifie qu'il n'y a pas de support pour la gestion du "spanning tree".

Un pont peut ajouter des temps de latence lors de l'utilisation de ping(8), et tout particulièrement dans le cas du trafic d'un segment vers un autre.

33.6. Système sans disque dur

Une machine FreeBSD peut démarrer via le réseau et fonctionner sans disque dur local, en utilisant des systèmes de fichiers montés à partir d'un serveur NFS. Aucune modification du système n'est nécessaire en dehors des fichiers de configuration standards. Un tel système est facile à mettre en oeuvre comme tous les éléments sont directement disponibles:

- Il y a au moins deux méthodes possibles pour charger un noyau via le réseau:
  - PXE: l'environnement d'exécution préalable au démarrage d'Intel® (Preboot eXecution Environment) est une sorte de ROM intelligente présente sur certaines cartes réseau ou cartes mère. Consultez la page de manuel pxeboot(8) pour plus de détails.
  - Le logiciel porté Etherboot (net/etherboot) produit un code stockable dans une ROM pour démarrer des noyaux via le réseau. Le code peut être soit implanté dans une PROM de démarrage sur une carte réseau, soit chargé à partir d'une disquette (ou d'un disque dur local), ou à partir d'un système MS-DOS® en fonctionnement. De nombreuses cartes réseau sont supportées.
- Une procédure d'exemple (/usr/shared/examples/diskless/clone_root) facilite la création et la maintenance du système de fichiers racine de la station de travail sur le serveur. La procédure demandera sûrement quelques modifications mais vous permettra de démarrer rapidement.
- Des fichiers de démarrage du système existent dans le répertoire /etc pour détecter et supporter le démarrage d'un système sans disque dur.
- La pagination, si nécessaire, peut être faite par l'intermédiaire d'un fichier NFS ou sur un disque local.

Il existe plusieurs façons de configurer des stations de travail sans disque dur. Plusieurs éléments entrent en oeuvre, et la plupart peuvent être ajustés en fonction des besoins locaux. Ce qui suit décrit des variations sur la configuration d'un système complet, mettant en avant le simplicité et la compatibilité avec les procédures standards de démarrage de FreeBSD. Le système décrit présente les caractéristiques suivantes:

- Les stations de travail sans disque dur utilisent des systèmes de fichiers / et /usr partagés et en lecture seule.

  Le système de fichiers racine est une copie d'une racine FreeBSD standard (généralement celle du serveur), avec certains fichiers de configuration remplacés par des versions spécifiques à un fonctionnement sans disque dur, et parfois à la station de travail auxquels ils appartiennent.

  Les parties de la racine qui doivent être inscriptibles sont remplacées par des systèmes de fichiers mfs(8) (FreeBSD 4.X) ou md(4) (FreeBSD 5.X). Toute modification sera perdue au redémarrage du système.

- Le noyau est transféré et chargé soit à l'aide d'Etherboot soit de PXE comme certaines situations peuvent exiger l'utilisation de l'une ou l'autre méthode.

Ainsi décrit, le système n'est pas sécurisé. Il devrait se trouver dans une partie protégée du réseau, et les autres machines ne devraient pas lui faire confiance aveuglément.

Toutes les instructions de cette section ont été testées sous FreeBSD 4.9-RELEASE et 5.2.1-RELEASE. Le texte est destiné à l'origine pour une utilisation sous 4.X. Des notes on été insérées aux endroits nécessaires pour indiquer les modifications concernant la branche 5.X.

33.6.1. Information de fond

Mettre en place des stations de travail sans disque dur est à la fois relativement simple et enclin aux erreurs. Ces dernières sont parfois difficiles à diagnostiquer pour de nombreuses raisons. Par exemple:

- Des options de compilation peuvent donner lieu à des comportements différents à l'exécution.
- Les messages d'erreurs sont souvent cachés ou totalement absents.

Dans ce contexte, avoir quelques connaissances des mécanismes sous-jacents impliqués est très utile pour résoudre les problèmes qui peuvent surgir.

Plusieurs opérations doivent être effectuées pour un amorçage réussi:

- La machine doit obtenir des paramètres de base comme son adresse IP, le nom du fichier exécutable, le nom du serveur, l'emplacement de la racine. Ceci est fait en utilisant le protocole DHCP ou le protocole BOOTP. DHCP est une extension compatible de BOOTP, et utilise les mêmes numéros de ports et son format de paquets basic.

  Il est possible de configurer un système pour n'utiliser que BOOTP. Le programme serveur bootpd(8) fait partie du système de base de FreeBSD.

  Cependant, DHCP présente plusieurs avantage sur BOOTP (des fichiers de configuration plus lisibles, la possibilité d'utiliser PXE, plus de nombreux autres avantages n'ayant pas de relation directe avec les systèmes sans disque dur), et nous décrirons principalement une configuration DHCP, avec des exemples équivalent utilisant bootpd(8) quand cela est possible. L'exemple de configuration utilisera le logiciel ISC DHCP (la version 3.0.1.r12 était installée sur le serveur de test).

- La machine a besoin de transférer un ou plusieurs programmes en mémoire locale. TFTP ou NFS sont utilisés. Le choix entre TFTP et NFS est à de nombreux endroits une option sélectionnée lors de la compilation. Une source d'erreur courante est d'indiquer des noms de fichiers pour le mauvais protocole: TFTP transfère généralement tous les fichiers à partir d'un seul répertoire sur le serveur, et attendra des noms de fichiers relatifs à ce répertoire. NFS a besoin de chemins d'accès absolus.
- Les éventuels programmes d'amorce intermédiaires et le noyau doivent être initialisés et exécutés. Il existe plusieurs variations à ce niveau:

- PXE chargera pxeboot(8), qui est une version modifiée du chargeur. Le chargeur (loader(8)) récupérera la plupart des paramètres nécessaires au démarrage du système, et les transmettra au noyau avant de lui abandonner le contrôle du système. Dans ce cas il est possible d'utiliser un noyau GENERIC.
- Etherboot, chargera directement le noyau avec moins de préparation. Vous devrez compiler un noyau avec des options particulières.

  PXE et Etherboot fonctionnent aussi bien l'un que l'autre avec des systèmes 4.X. Comme le noyau des systèmes 5.X laisse au chargeur (loader(8)) un peu plus de travail à effectuer, PXE est préféré pour les systèmes 5.X.

  Si votre BIOS et vos cartes réseau supportent PXE, vous devriez probablement l'utiliser. Cependant, il est toujours possible de démarrer un système 5.X à l'aide d'Etherboot.

- Et enfin, la machine a besoin d'accéder à ses systèmes de fichiers. NFS est utilisé dans tous les cas.

Consultez également la page de manuel diskless(8).

33.6.2. Configuration

33.6.2.1. Configuration utilisant ISC DHCP

Le serveur ISC DHCP peut répondre aux requêtes BOOTP et DHCP.

Avec la version 4.9, ISC DHCP 3.0 ne fait pas partie du système de base. Vous devrez installer le logiciel porté net/isc-dhcp3-server ou la version pré-compilée correspondante.

Une fois ISC DHCP installé, il nécessite un fichier de configuration pour fonctionner (normalement appelé /usr/local/etc/dhcpd.conf). Voici un exemple commenté, où la machine `margaux` utilise Etherboot et où la machine `corbieres` emploie PXE:

```
default-lease-time 600;
max-lease-time 7200;
authoritative;

option domain-name "example.com";
option domain-name-servers 192.168.4.1;
option routers 192.168.4.1;

subnet 192.168.4.0 netmask 255.255.255.0 {
  use-host-decl-names on; ①
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.4.255;

  host margaux {
    hardware ethernet 01:23:45:67:89:ab;
    fixed-address margaux.example.com;
    next-server 192.168.4.4; ②
    filename "/data/misc/kernel.diskless"; ③
```

```
    option root-path "192.168.4.4:/data/misc/diskless"; ④
  }
  host corbieres {
    hardware ethernet 00:02:b3:27:62:df;
    fixed-address corbieres.example.com;
    next-server 192.168.4.4;
    filename "pxeboot";
    option root-path "192.168.4.4:/data/misc/diskless";
  }
}
```

① Cette option dit à dhcpd d'envoyer le paramètre des déclarations `host` comme nom de machine pour la machine sans disque dur. Une autre méthode aurait été d'ajouter `option host-name margaux` à l'intérieur des déclarations `host`.

② La directive `next-server` désigne le serveur TFTP ou NFS à utiliser pour télécharger le chargeur ou le noyau (le comportement par défaut étant d'utiliser la même machine que le serveur DHCP).

③ La directive `filename` précise le fichier que chargera Etherboot ou PXE à la prochaine étape. Il doit être défini en fonction de la méthode de transfert utilisée. Etherboot peut être compilé pour utiliser NFS ou TFTP. Le logiciel porté pour FreeBSD utilisera NFS par défaut. PXE emploie TFTP, c'est pourquoi un chemin d'accès relatif est utilisé ici (cela peut dépendre de la configuration du serveur TFTP, mais devrait être plutôt classique). De plus, PXE charge pxeboot, et non pas le noyau. Il existe d'autres possibilités intéressantes, comme le chargement de pxeboot à partir du répertoire /boot d'un CD-ROM FreeBSD (comme pxeboot(8) peut charger un noyau GENERIC cela rend possible l'utilisation de PXE pour démarrer à partir d'un lecteur de CD-ROM distant).

④ L'option `root-path` définie le chemin d'accès au système de fichiers racine, suivant la notation classique de NFS. En utilisant PXE, il est possible de ne pas préciser l'adresse IP de la machine dès lors que vous n'activez pas l'option BOOTP du noyau. Le serveur NFS sera alors le même que le serveur TFTP.

33.6.2.2. Configuration utilisant BOOTP

Ce qui suit présente une configuration bootpd équivalente (réduite à un seul client). Elle se trouverait sous /etc/bootptab.

Veuillez noter qu'Etherboot doit être compilé avec l'option `NO_DHCP_SUPPORT` (qui n'est pas activée par défaut) afin d'utiliser BOOTP et que PXE *nécessite* DHCP. The seul avantage évident de bootpd est qu'il est disponible dans le système de base.

```
.def100:\
  :hn:ht=1:sa=192.168.4.4:vm=rfc1048:\
  :sm=255.255.255.0:\
  :ds=192.168.4.1:\
  :gw=192.168.4.1:\
  :hd="/tftpboot":\
  :bf="/kernel.diskless":\
  :rp="192.168.4.4:/data/misc/diskless":
```

```
margaux:ha=0123456789ab:tc=.def100
```

33.6.2.3. Préparation d'un programme de démarrage avec Etherboot

Le site Web d'Etherboot propose une documentation importante principalement destinée aux systèmes Linux, mais contenant néamoins des informations utiles. Ce qui suit présente comment vous utiliseriez Etherboot sur un système FreeBSD.

Vous devez tout d'abord installer le logiciel porté net/etherboot ou sa version pré-compilée.

Vous pouvez modifier la configuration d'Etherboot (i.e. pour utiliser TFTP au lieu de NFS) en éditant le fichier Config dans le répertoire des sources d'Etherboot.

Pour notre configuration nous utiliserons une disquette de démarrage. Pour d'autres méthodes (PROM, ou un programme MS-DOS®), consultez la documentation d'Etherboot.

Pour créer une disquette de démarrage, insérez une disquette dans le lecteur de la machine où vous avez installé Etherboot, puis rendez-vous dans le répertoire src de l'arborescence Etherboot et tapez:

```
# gmake bin32/devicetype.fd0
```

devicetype dépend du type de carte Ethernet se trouvant dans la station de travail sans disque dur. Référez-vous au fichier NIC dans le même répertoire pour déterminer la valeur *devicetype* correcte.

33.6.2.4. Démarrer avec PXE

Par défaut le chargeur pxeboot(8) charge le noyau via NFS. Il peut être compilé pour utiliser TFTP à la place en spécifiant l'option `LOADER_TFTP_SUPPORT` dans le fichier /etc/make.conf. Lisez les commentaires dans le fichier /etc/defaults/make.conf (ou /usr/shared/examples/etc/make.conf pour les systèmes 5.X) pour plus de détails.

Il existe deux autres options de make.conf non-documentées qui peuvent être utiles pour la configuration d'une machine faisant fonction de console série sans disque dur: `BOOT_PXELDR_PROBE_KEYBOARD`, et `BOOT_PXELDR_ALWAYS_SERIAL` (cette dernière n'existe que sous FreeBSD 5.X).

Pour utiliser PXE quand la machine démarre, vous aurez normalement besoin de sélectionner l'option `Boot from network` dans votre BIOS, ou d'appuyer sur une touche de fonction lors de l'initialisation du PC.

33.6.2.5. Configuration des serveurs TFTP et NFS

Si vous utilisez PXE ou Etherboot configurés pour employer TFTP, vous devez activer tftpd sur le serveur de fichier:

1. Créez un répertoire à partir duquel tftpd proposera les fichiers, e.g. /tftpboot.
2. Ajoutez la ligne suivante à votre fichier /etc/inetd.conf:

```
tftp    dgram   udp wait    root    /usr/libexec/tftpd  tftpd -l -s /tftpboot
```

Il apparaît que certaines versions de PXE veulent la version TCP de TFTP. Dans ce cas, ajoutez une seconde ligne, en remplaçant `dgram udp` par `stream tcp`.

3. Demandez à inetd de relire son fichier de configuration:

```
# kill -HUP `cat /var/run/inetd.pid`
```

Le répertoire tftpboot peut être placé n'importe où sur le serveur. Assurez-vous que son emplacement est défini dans les fichiers inetd.conf et dhcpd.conf.

Dans tous les cas, vous devez également activer NFS et exporter le système de fichiers approprié sur le serveur NFS.

1. Ajoutez ce qui suit au fichier /etc/rc.conf:

```
nfs_server_enable="YES"
```

2. Exportez le système de fichiers contenant le répertoire racine du système sans disque dur en ajoutant ce qui suit au fichier /etc/exports (ajustez le point de montage et remplacez *margaux corbieres* avec les noms des stations de travail sans disque dur):

```
/data/misc -alldirs -ro margaux corbieres
```

3. Demandez à mountd de relire son fichier de configuration. Si vous avez eu besoin d'activer NFS dans /etc/rc.conf lors du premier point, vous voudrez probablement plutot redémarrer la machine.

```
# kill -HUP `cat /var/run/mountd.pid`
```

33.6.2.6. Compilation d'un noyau pour système sans disque dur

Si vous utilisez Etherboot, vous devez créer un fichier de configuration du noyau pour le client sans disque dur avec les options suivantes (en plus des options habituelles):

```
options     BOOTP          # Use BOOTP to obtain IP address/hostname
options     BOOTP_NFSROOT  # NFS mount root filesystem using BOOTP info
```

Vous pouvez vouloir également employer les options `BOOTP_NFSV3`, `BOOT_COMPAT` et `BOOTP_WIRED_TO` (référez-vous au fichier LINT sous 4.X ou NOTES sous 5.X).

Les noms de ces options sont historiques et légèrement trompeur comme elles activent indifféremment l'utilisation de DHCP et BOOTP dans le noyau (il est également possible de forcer une utilisation stricte de BOOTP ou DHCP).

Compilez le noyau (voir Configurer le noyau de FreeBSD), et copiez-le à l'emplacement indiqué dans dhcpd.conf.

Quand on utilise PXE, la compilation d'un noyau avec les options précédentes n'est pas strictement nécessaire (bien que conseillé). Les activer causera un plus grand nombre de requêtes DHCP générées lors du démarrage du noyau, avec un petit risque d'inconsistance entre les nouvelles valeurs et celles récupérées par pxeboot(8) dans certains cas particuliers. L'avantage de leur utilisation est que le nom de la machine sera forcément défini. Sinon vous devrez définir le nom de la machine par une autre méthode, par exemple dans un fichier rc.conf particulier au client.

Afin d'être chargeable par Etherboot, un noyau 5.X doit être compilé avec les "device hints". Vous définirez normalement l'option suivante dans le fichier de configuration (voir le fichier de commentaires sur la configuration: NOTES):

```
hints       "GENERIC.hints"
```

33.6.2.7. Préparer le système de fichiers racine

Vous devez créer un système de fichiers racine pour les stations de travail sans disque dur, à l'emplacement défini par `root-path` dans le fichier dhcpd.conf. Les sections suivantes décrivent deux manières de le faire.

33.6.2.7.1. Utilisation de la procédure clone_root

C'est la méthode la plus rapide pour créer un système de fichiers racine, mais elle est, pour le moment, uniquement supportée sous FreeBSD 4.X.. Cette procédure est située à l'emplacement /usr/shared/examples/diskless/clone_root et demande quelques modifications, pour au moins ajuster l'emplacement du système de fichiers à créer (la variable `DEST`).

Référez-vous aux commentaires situés en début de la procédure pour information. Ils expliquent comment le système de fichiers de base est construit, et comment les fichiers peuvent être remplacés de façon sélective par des versions spécifiques à un fonctionnement sans disque dur, ou à un sous-réseau, ou encore à une station de travail particulière. Ils donnent également des exemples de fichiers /etc/fstab et /etc/rc.conf pour un fonctionnement sans disque dur.

Les fichiers README dans le répertoire /usr/shared/examples/diskless contiennent beaucoup d'information de fond, mais, avec les autres exemples du répertoire diskless, ils documentent une méthode de configuration qui est distincte de celle utilisée par clone_root et les procédures de démarrage du système de /etc, ce qui est un peu à l'origine de confusions. Utilisez-les comme

référence uniquement, à moins que vous préfériez la méthode qu'ils décrivent, dans quel cas vous devrez modifier les procédures rc.

33.6.2.7.2. Utilisation de la procédure `make world` standard

Cette méthode s'applique aussi bien à FreeBSD 4.X qu'à FreeBSD 5.X et installera un système complet (et non pas uniquement le système de fichiers racine) dans le répertoire défini par `DESTDIR`. Tout ce dont vous avez besoin de faire est d'exécuter la procédure suivante:

```
#!/bin/sh
export DESTDIR=/data/misc/diskless
mkdir -p ${DESTDIR}
cd /usr/src; make world  make kernel
cd /usr/src/etc; make distribution
```

Une fois cela terminé, vous devrez personaliser vos fichiers /etc/rc.conf et /etc/fstab situés dans `DESTDIR` en fonction de vos besoins.

33.6.2.8. Configuration de l'espace de pagination

Si nécessaire, un fichier de pagination situé sur le serveur peut être utilisé via NFS. Une des méthodes couramment utilisées pour cela n'est plus supportée sous 5.X.

33.6.2.8.1. Pagination via NFS sous FreeBSD 4.X

L'emplacement et la taille du fichier de pagination peuvent être spécifiés avec les options BOOTP/DHCP 128 et 129 spécifiques à FreeBSD. Des exemples de fichiers de configuration pour ISC DHCP 3.0 ou bootpd suivent:

1. Ajoutez les lignes suivantes au fichier dhcpd.conf:

   ```
   # Global section
   option swap-path code 128 = string;
   option swap-size code 129 = integer 32;

   host margaux {
     ... # Standard lines, see above
     option swap-path "192.168.4.4:/netswapvolume/netswap";
     option swap-size 64000;
   }
   ```

   `swap-path` est le chemin d'accès vers un répertoire où les fichiers de pagination sont situés. Chaque fichier sera nommé swap.ip-client.

   Les anciennes version de dhcpd utilisaient une syntaxe du type `option option-128 "…`, qui n'est plus supportée.

   /etc/bootptab utiliserait la syntaxe suivante à la place:

```
T128="192.168.4.4:/netswapvolume/netswap":T129=0000fa00
```

Dans le fichier /etc/bootptab, la taille de l'espace de pagination doit être exprimée en hexadécimal.

2. Sur le serveur du fichier de pagination par NFS, créez le(s) fichier(s) de pagination:

```
# mkdir /netswapvolume/netswap
# cd /netswapvolume/netswap
# dd if=/dev/zero bs=1024 count=64000 of=swap.192.168.4.6
# chmod 0600 swap.192.168.4.6
```

192.168.4.6 est l'adresse IP du client sans disque dur.

3. Sur le serveur du fichier de pagination par NFS, ajoutez la ligne suivante au fichier /etc/exports:

```
/netswapvolume  -maproot=0:10 -alldirs margaux corbieres
```

Ensuite demandez à mountd à relire le fichier exports, comme plus haut.

33.6.2.8.2. Pagination via NFS sous FreeBSD 5.X

Le noyau ne supporte pas l'activation de la pagination par NFS au démarrage. L'espace de pagination doit être activé par les procédures de démarrage, en montant un système de fichiers accessible en écriture et en créant et en activant un fichier de pagination. Pour créer un fichier de pagination de la taille appropriée, vous pouvez effectuer ce qui suit:

```
# dd if=/dev/zero of=/path/to/swapfile bs=1k count=1 oseek=100000
```

Pour ensuite l'activer, vous devez ajouter la ligne suivante à votre fichier rc.conf:

```
swapfile=/path/to/swapfile
```

33.6.2.9. Problèmes divers

33.6.2.9.1. Utilisation d'un /usr en lecture seule

Si la station de travail sans disque dur est configurée pour exécuter X, you devrez ajuster le fichier de configuration de XDM, qui envoie le journal d'erreurs sur /usr par défaut.

33.6.2.9.2. Utilisation d'un serveur non-FreeBSD

Quand le serveur pour le système de fichiers racine ne fait pas tourner FreeBSD, vous devrez créer

le système de fichiers racine sur une machine FreeBSD, puis le copier vers sa destination en utilisant `tar` ou `cpio`.

Dans cette situation, il y a parfois des problèmes avec les fichiers spéciaux de périphériques dans /dev, en raison de différences de taille sur les entiers. Une solution à ce problème est d'exporter un répertoire à partir du serveur non-FreeBSD, de monter ce répertoire sur une machine FreeBSD, et exécuter `MAKEDEV` sur la machine FreeBSD pour créer les entrées de périphériques correctes (FreeBSD 5.X et les versions suivantes utilisent devfs(5) pour l'allocation des fichiers spéciaux de périphériques de manière transparente pour l'utilisateur, exécuter `MAKEDEV` sur ces versions est inutile).

33.7. ISDN

Une bonne source d'information sur la technologie et le matériel ISDN (RNIS) est la page ISDN de Dan Kegel.

Voici un rapide aperçu à propos de l'ISDN:

- Si vous résidez en Europe, vous devriez étudier la section sur les cartes ISDN.
- Si vous envisagez d'utiliser l'ISDN avant tout pour vous connecter à l'Internet par l'intermédiaire d'un fournisseur d'accès Internet et d'une ligne téléphonique non dédiée, vous devriez vous intéresser aux Adaptateurs Terminaux. C'est la solution la plus souple, qui vous posera le moins de problèmes si vous changez de fournisseur d'accès.
- Si vous interconnectez deux réseaux locaux, ou si vous vous connectez à l'Internet avec une liaison ISDN dédiée, vous devriez envisager un pont/routeur autonome.

Le coût est un facteur déterminant de la solution que vous choisirez. Les options suivantes sont listées de la moins chère à la plus chère.

33.7.1. Cartes ISDN

L'implémentation ISDN de FreeBSD ne supporte que la norme DSS1/Q.931 (ou Euro-ISDN) utilisant des cartes passives. Depuis FreeBSD 4.4, quelques cartes actives sont supportées où le firmware supporte également d'autres protocoles au niveau des signaux, cela inclut les premières cartes supportées du type "Primary Rate ISDN" (PRI).

Le logiciel isdn4bsd vous permet de vous connecter à d'autres routeurs ISDN soit en utilisant l'IP sur de l'HDLC de base, soit en utilisant PPP synchrone: en employant PPP intégré au noyau avec `isppp`, une version modifiée du pilote de périphérique sppp(4), ou en employant ppp(8) en mode utilisateur. L'utilisation de ppp(8) en mode utilisateur rend possible l'agrégation de deux ou plus canaux ISDN de type B. Une application capable de répondre aux appels téléphoniques est également disponible, tout comme de nombreux utilitaires comme un modem logiciel 300 bauds.

Un nombre croissant de cartes ISDN pour PC sont supportées sous FreeBSD et les retours montrent qu'elles sont utilisées avec succès dans toute l'Europe et dans de nombreuses autres parties du monde.

Les cartes ISDN passives supportées sont principalement celles avec le circuit ISDN ISAC/HSCX/IPAC

d'Infineon (précédemment Siemens), mais également les cartes avec des circuits en provenance de Cologne Chip (cartes ISA uniquement), les cartes PCI avec les circuits Winbond W6692, quelques cartes avec les circuits Tiger300/320/ISAC et quelques cartes avec des circuits spécifiques comme l'AVM Fritz!Card PCI V.1.0 de l'AVM Fritz!Card PnP.

Actuellement les cartes ISDN actives supportées sont les cartes AVM B1 (ISA et PCI) BRI et les cartes PCI AVM T1 PRI.

Pour de la documentation sur isdn4bsd, consultez le répertoire /usr/shared/examples/isdn/ sur votre système FreeBSD ou sur la page web d'isdn4bsd qui propose également des astuces, des erratas et bien plus de documentation que le manuel d'isdn4bsd.

Au cas où vous seriez intéressé par l'ajout du support pour un protocole ISDN différent, d'une carte ISDN pour PC non encore supportée ou par l'amélioration d'isdn4bsd, veuillez contacter Hellmuth Michaelis <hm@FreeBSD.org>.

Pour les questions concernant l'installation, la configuration et le dépannage d'isdn4bsd, une liste de diffusion freebsd-isdn est disponible.

33.7.2. Adaptateurs terminaux ISDN

Les adaptateurs terminaux-"Terminal adapters (TA)"; sont l'équivalent ISDN des modems pour les lignes téléphoniques ordinaires.

La plupart des TA utilisent le jeu de commandes standard des modems Hayes, et peuvent être utilisés en remplacement d'un modem.

Un TA fonctionne essentiellement de la même manière qu'un modem à la différence que la vitesse de la connexion sera plus élevée qu'avec votre vieux modem. Vous devrez configurer PPP de façon exactement identique que pour un modem classique. Assurez-vous de fixer la vitesse de votre port série la plus haute possible.

Le principal avantage d'utiliser un TA pour vous connecter à votre fournisseur d'accès Internet est de pouvoir utiliser PPP en mode dynamic. Comme l'espace d'adressage IP disponible devient de plus en plus restreint, la plupart des fournisseurs d'accès ne désirent plus vous fournir d'adresse IP statique. La plupart des routeurs autonomes ne peuvent pas fonctionner avec une allocation dynamique d'adresse IP.

Les fonctionnalités et la stabilité de la connexion des adaptateurs terminaux reposent complètement sur le "daemon" PPP. Cela vous permet de passer facilement d'un modem classique à l'ISDN sur une machine FreeBSD, si vous avez déjà configuré PPP. Cependant, les problèmes que vous avez éventuellement rencontrés avec PPP persisteront.

Si vous désirez un maximum de stabilité, utilisez PPP intégré au noyau, à la place du PPP en mode utilisateur.

Les adaptateurs suivants sont connus pour fonctionner avec FreeBSD:

- Motorola BitSurfer et Bitsurfer Pro
- Adtran

La plupart des adaptateurs terminaux fonctionneront probablement également, les fabricants de TA font en sorte que leurs produits acceptent la plupart du jeu de commandes AT des modems.

Le vrai problème avec les adaptateurs terminaux est que comme pour les modems, il vous faudra une bonne interface série dans votre ordinateur.

Vous devriez lire le document sur les ports série sous FreeBSD pour comprendre en détail le fonctionnement des périphériques série et les différences entre les ports séries asynchrones et synchrones.

Un adaptateur terminal sur un port série PC standard (asynchrone) vous limite à 115.2 Kbs, même si vous disposez d'une connexion à 128 Kbs. Pour utiliser complètement les 128 Kbs offert par l'ISDN, vous devez brancher l'adaptateur sur une carte série synchrone.

Ne vous imaginez pas qu'il suffit d'acheter un adaptateur terminal interne pour s'affranchir du problème synchrone/asynchrone. Les adaptateurs internes disposent simplement d'un port série PC standard. Tout ce que vous y gagnerez sera d'économiser un câble série et de libérer une prise électrique.

Une carte synchrone avec un adaptateur terminal est au moins aussi rapide qu'un routeur autonome, piloté par une simple machine FreeBSD, et probablement plus souple.

Le choix entre carte synchrone/adaptateur ou routeur autonome est une question de goût. Ce sujet a été abordé dans les listes de diffusion. Nous vous suggérons de chercher dans les archives pour obtenir l'intégralité de la discussion.

33.7.3. Ponts/Routeurs ISDN autonomes

Les ponts ou routeurs ISDN ne sont pas spécifiques à FreeBSD ou à tout autre système d'exploitation. Pour une description complète de la technologie du routage et des ponts, veuillez vous reportez à un ouvrage de référence sur les réseaux.

Dans le contexte de cette section, les termes de routeur et de pont seront utilisés indifféremment.

Comme le prix des routeurs/ponts ISDN d'entrée de gamme baissent, il est probable qu'ils deviennent un choix de plus en plus populaire. Un routeur ISDN est une petite boîte qui se branche directement sur votre réseau Ethernet, et gère sa propre connexion aux autres ponts/routeurs. Il intègre le logiciel nécessaire au support du protocole PPP et d'autres protocoles.

Un routeur vous offrira un débit plus élevé qu'un adaptateur terminal standard, puisqu'il utilisera une connexion ISDN synchrone.

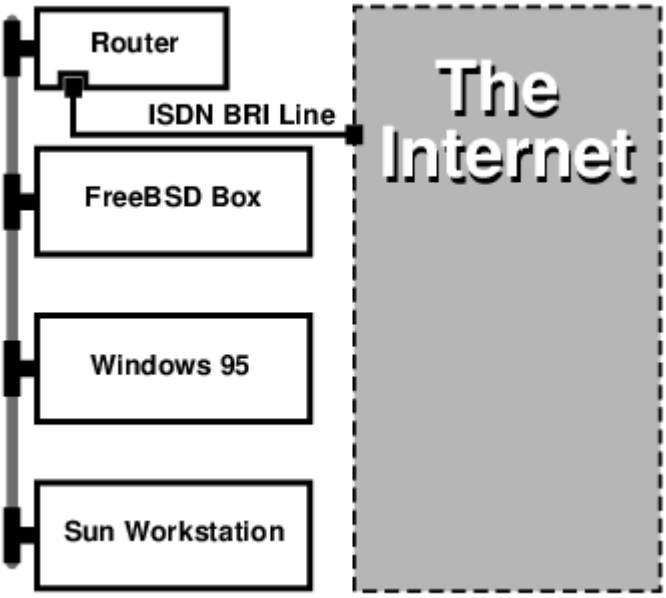
Le principal problème avec les routeurs et ponts ISDN est que l'intéropérabilité entre les matériels des différents constructeurs n'est pas toujours garantie. Si vous projetez de vous connecter à un fournisseur d'accès Internet, vous devriez discuter de vos besoins avec ce dernier.

Si vous envisagez de connecter ensemble deux réseaux locaux, comme le réseau de votre domicile et celui de votre bureau, c'est la solution la plus simple et celle qui demande le moins de maintenance. Etant donné que vous êtes la personne qui achète les équipements pour les deux extrémités, vous êtes sûr que cela fonctionnera.

Par exemple pour connecter un ordinateur personnel situé à son domicile ou le réseau d'une agence à celui du siège social, la configuration suivante pourra être utilisée:

Exemple 42. Réseau d'agence ou à domicile

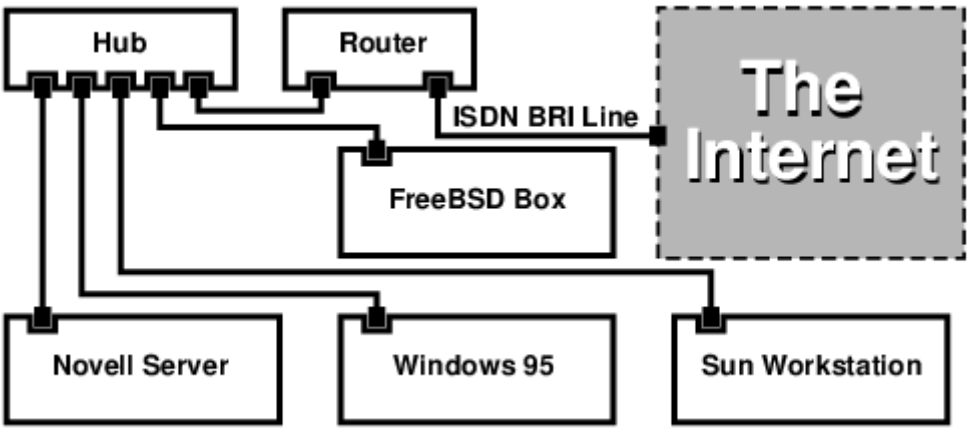
Le réseau utilise une topologie en bus avec une connectique Ethernet 10 base 2 ("thinnet"). Connectez le routeur au réseau à l'aide d'un émetteur/récepteur AUI/10BT si nécessaire.



Si votre réseau de domicile/d'agence n'est constitué que d'un seul ordinateur, vous pouvez utiliser une paire torsadée croisée pour le connecter directement au routeur autonome.

Exemple 43. Siège social ou autre réseau

Le réseau utilise une topologie en étoile avec une connectique Ethernet 10 base T ("paire torsadée").



Un des principaux avantages de la plupart des routeurs/ponts est le fait qu'ils permettent d'avoir deux connexions PPP *séparées et indépendantes* vers deux sites différents et cela en *même* temps. Ceci n'est pas supporté par la plupart des adaptateurs terminaux, en dehors de modèles spécifiques

(en général coûteux) qui disposent de deux ports série. Ne confondez pas cette possibilité avec l'agrégation de canaux, MPP, etc.

Ceci peut être une fonctionnalité très utile si, par exemple, vous disposez d'une connexion ISDN dédiée au bureau et vous voudriez en profiter mais vous ne voulez pas acquérir une nouvelle ligne ISDN. Un routeur au bureau peut gérer un canal B dédié (64 Kbps) vers l'Internet et utiliser l'autre canal B pour une autre connexion. Le deuxième canal B peut être utilisé pour les connexions entrantes, sortantes ou pour l'agrégation de canaux (MPP, etc.) avec le premier canal B pour augmenter la bande passante.

Un pont Ethernet vous permettra de transmettre autre chose que juste du trafic IP. Vous pouvez également faire passer de l'IPX/SPX ou tout autre protocole que vous utilisez.

33.8. Translation d'adresses

33.8.1. Généralités

Le "daemon" de translation d'adresses ("Network Address Translation"-NAT) de FreeBSD, généralement connu sous le nom de natd(8) est un "daemon" qui accepte les paquets IP entrants, change l'adresse de la source par celle de la machine locale et ré-injecte les paquets dans le flux sortant des paquets IP. Le programme natd(8) effectue cela en changeant l'adresse IP et le port source de sorte quand les données réponse arrivent il soit en mesure de déterminer la provenance des données d'origine et les transférer à l'émetteur original.

L'utilisation classique de NAT est le partage de connexion Internet.

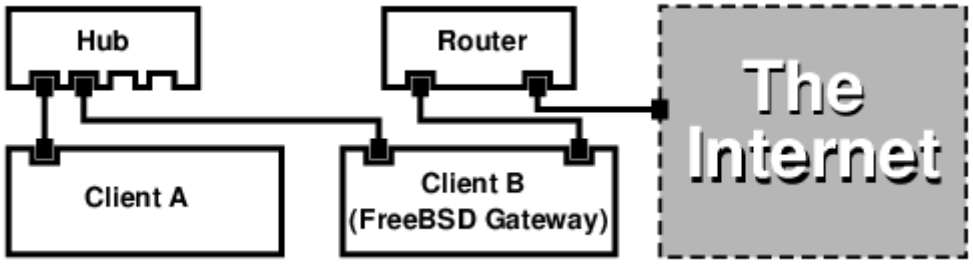
33.8.2. Architecture du réseau

En raison de la diminution du nombre d'adresses IP libres sous IPv4, et de l'augmentation du nombre d'utilisateurs de lignes haut-débit comme le câble ou l'ADSL, le besoin d'utiliser une solution de partage de connexion est donc en constante augmentation. La possibilité de connecter plusieurs ordinateurs par l'intermédiaire d'une connexion et d'une adresse IP fait de natd(8) une solution de choix.

Plus généralement, un utilisateur dispose d'une machine connecté sur la câble ou une ligne ADSL avec une adresse IP et désire utiliser cet ordinateur connecté pour fournir un accès Internet à d'autres machines du réseau local.

Pour cela, la machine FreeBSD sur Internet doit jouer le rôle de passerelle. Cette machine passerelle doit avoir deux cartes réseaux-l'une pour se connecter au routeur Internet, l'autre est connectée au réseau local. Toutes les machines du réseau local sont connectées par l'intermédiaire d'un hub ou d'un switch.

Il existe plusieurs manières pour connecter un réseau local à l'Internet à travers une passerelle FreeBSD. Cet exemple n'abordera que le cas d'une passerelle avec au moins deux cartes réseaux.



Une telle configuration est communément utilisée pour partager une connexion Internet. Une des machines du réseau local est connectée à Internet. Le reste des machines accède à Internet par l'intermédiaire de cette machine "passerelle".

33.8.3. Configuration

Les options suivantes doivent être présentes dans le fichier de configuration du noyau:

```
options IPFIREWALL
options IPDIVERT
```

De plus, les options suivantes peuvent également être utiles:

```
options IPFIREWALL_DEFAULT_TO_ACCEPT
options IPFIREWALL_VERBOSE
```

Ce qui suit doit figurer dans le fichier /etc/rc.conf:

```
gateway_enable="YES" ①
firewall_enable="YES" ②
firewall_type="OPEN" ③
natd_enable="YES"
natd_interface="fxp0" ④
natd_flags="" ⑤
```

① Configure la machine comme passerelle. Exécuter `sysctl net.inet.ip.forwarding=1` aurait le même effet.

② Active au démarrage les règles du coupe-feu se trouvant dans le fichier /etc/rc.firewall.

③ Cela spécifie un ensemble de règles prédéfinies pour le coupe-feu qui autorise tous les paquets entrant. Consultez le fichier /etc/rc.firewall pour d'autres ensembles de régles.

④ Indique à travers quelle interface transférer les paquets (l'interface connectée à l'Internet).

⑤ Toutes options de configuration supplémentaires passées à natd(8) au démarrage.

Le fait d'avoir les options précédentes définies dans le fichier /etc/rc.conf lancera la commande /etc/rc.conf au démarrage. Cette commande peut être également exécutée à la main.

Il est également possible d'utiliser un fichier de configuration pour natd(8) quand

il y a trop d'options à passer. Dans ce cas, le fichier de configuration doit être défini en ajoutant la ligne suivante au fichier /etc/rc.conf:

```
natd_flags="-f /etc/natd.conf"
```

Le fichier /etc/natd.conf contiendra une liste d'options de configuration, une par ligne. Par exemple le cas de figure de la section suivante utiliserait le fichier suivant:

```
redirect_port tcp 192.168.0.2:6667 6667
redirect_port tcp 192.168.0.3:80 80
```

Pour plus d'information concernant le fichier de configuration, consultez la page de manuel de natd(8) au sujet de l'option `-f`.

A chaque machine et interface derrière le réseau local doit être assigné une adresse IP de l'espace d'adresses privées comme défini par la RFC 1918 et doit disposer d'une passerelle par défaut qui est l'adresse IP interne de la machine natd(8).

Par exemple, les clients `A` et `B` du réseau local ont les adresses IP `192.168.0.2` et `192.168.0.3`, tandis que l'interface sur le réseau local de la machine natd a pour adresse IP `192.168.0.1`. La passerelle par défaut des clients `A` et `B` doit être l'adresse `192.168.0.1` de la machine natd. L'interface externe ou Internet de cette dernière ne demande aucune modification spécifique pour que natd(8) puisse fonctionner.

33.8.4. Redirection de ports

L'inconvénient avec natd(8) est que les clients du réseau local ne sont pas accessibles depuis l'Internet. Les clients sur le réseau local peuvent établir des connexions sortantes vers le monde extérieur mais ne peuvent recevoir de connexions entrantes. Cela présente un problème si l'on tente de faire tourner des services Internet sur une des machines du réseau local. Une solution simple à ce problème est de rediriger les ports Internet sélectionnés de la machine natd vers le client sur le réseau local.

Par exemple, un serveur IRC tourne sur le client `A`, et un serveur web sur le client `B`. Pour que cela fonctionne correctement, les connections reçues sur les ports 6667 (IRC) et 80 (web) doivent être redirigées vers les machines correspondantes.

L'option `-redirect_port` doit être passée à natd(8) avec les autres options adéquates. La syntaxe est la suivante:

```
-redirect_port proto targetIP:targetPORT[-targetPORT]
               [aliasIP:]aliasPORT[-aliasPORT]
               [remoteIP[:remotePORT[-remotePORT]]]
```

Dans l'exemple précédent, l'argument passé à la commande devrait être:

```
-redirect_port tcp 192.168.0.2:6667 6667
-redirect_port tcp 192.168.0.3:80 80
```

Cela va rediriger les ports *tcp* voulus vers les machines du réseau local.

L'option `-redirect_port` peut être utilisée pour indiquer une plage de ports plutôt que des ports individuels. Par exemple *tcp 192.168.0.2:2000-3000 2000-3000* redirigerait toutes les connexions reçues sur les ports 2000 à 3000 vers les ports 2000 à 3000 du client `A`.

Ces options peuvent être utilisées quand on exécute directement natd(8), placées dans l'option `natd_flags=""` du fichier /etc/rc.conf, ou passées par l'intermédiaire d'un fichier de configuration.

Pour plus d'éléments et d'options de configuration consultez la page de manuel natd(8)

33.8.5. Redirection d'adresses

La redirection d'adresses est utile si plusieurs adresses IP sont disponibles mais doivent se trouver sur une seule machine. Avec cela, natd(8) peut assigner à chaque client du réseau local sa propre adresse IP externe. Le programme natd(8) récrit alors les paquets sortant des clients du réseau local avec l'adresse IP externe correcte et redirige tout le trafic entrant sur une adresse IP particulière vers la machine du réseau local correspondante. Ce principe est également connu sous le nom de translation d'adresses statique. Par exemple, les adresses IP `128.1.1.1`, `128.1.1.2`, et `128.1.1.3` appartiennent à la passerelle natd. L'adresse `128.1.1.1` peut être utilisée comme adresse IP externe de la passerelle natd, tandis que `128.1.1.2` et `128.1.1.3` sont redirigées vers les machines `A` et `B` du réseau local.

La syntaxe de l'option `-redirect_address` est la suivante:

```
-redirect_address localIP publicIP
```

localIP	L'adresse IP interne du client sur le réseau local.
publicIP	L'adresse IP externe correspondant au client sur le réseau local.

Dans l'exemple, les arguments passés à la commande seraient:

```
-redirect_address 192.168.0.2 128.1.1.2
-redirect_address 192.168.0.3 128.1.1.3
```

Comme pour l'option `-redirect_port`, ces options peuvent être placées dans l'option `natd_flags=""` du fichier /etc/rc.conf, ou passées par l'intermédiaire d'un fichier de configuration. Avec la redirection d'adresse, il n'y a pas besoin de redirection de ports puisque toutes les données reçues sur une IP particulière sont redirigées.

Les adresses IP sur la machine natd doivent être active et pointer sur l'interface externe. Consultez la page de manuel rc.conf(5) pour cela.

33.9. IP sur liaison parallèle (PLIP)

PLIP nous permet d'utiliser le protocole TCP/IP entre ports parallèles. C'est utile sur des machines sans cartes réseaux, ou pour effectuer une installation sur ordinateur portable. Dans cette section nous aborderons:

- La fabrication d'un câble parallèle ("laplink").
- La connexion de deux ordinateurs via PLIP.

33.9.1. Fabriquer un câble parallèle

Vous pouvez acheter un câble parallèle auprès de la plupart des vendeurs de matériel informatique. Si ce n'est pas le cas, ou désirez savoir comment est fait un tel câble, le tableau suivant montre comment en faire un à partir d'un câble parallèle d'imprimante.

Tableau 8. Câblage d'un câble parallèle pour réseau

A-name	A-End	B-End	Descr.	Post/Bit
.... DATA0 -ERROR	.... 2 15	.... 15 2	Data	.... 0/0x01 1/0x08 ....
.... DATA1 +SLCT	.... 3 13	.... 13 3	Data	.... 0/0x02 1/0x10 ....
.... DATA2 +PE	.... 4 12	.... 12 4	Data	.... 0/0x04 1/0x20 ....
.... DATA3 -ACK	.... 5 10	.... 10 5	Strobe	.... 0/0x08 1/0x40 ....
.... DATA4 BUSY	.... 6 11	.... 11 6	Data	.... 0/0x10 1/0x80 ....
GND	18-25	18-25	GND	-

33.9.2. Configurer PLIP

Tout d'abord procurez-vous un câble "laplink". Vérifiez ensuite que les deux ordinateurs disposent d'un noyau avec le support pour le pilote de périphérique lpt(4).

```
# grep lp /var/run/dmesg.boot
lpt0: <Printer> on ppbus0
```

```
lpt0: Interrupt-driven port
```

Le port parallèle doit fonctionner sous interruption, sous FreeBSD 4.X vous devriez avoir une ligne semblable à la ligne suivante dans le fichier de configuration du noyau:

```
device ppc0 at isa? irq 7
```

Sous FreeBSD 5.X, le fichier /boot/device.hints devrait contenir les lignes suivantes:

```
hint.ppc.0.at="isa"
hint.ppc.0.irq="7"
```

Ensuite vérifiez si le fichier de configuration du noyau contient une ligne `device plip` ou si le module plip.ko est chargé. Dans les deux cas l'interface réseau parallèle devrait apparaître quand vous utilisez la commande ifconfig(8):

```
# ifconfig plip0
plip0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> mtu 1500
```

Branchez le câble "laplink" sur les interfaces parallèles des deux ordinateurs.

Configurez les paramètres de l'interface réseau des deux côtés en tant que `root`. Par exemple, si vous voulez connecter la machine `host1` avec la machine `host2`:

```
                host1 ----- host2
IP Address    10.0.0.1      10.0.0.2
```

Configurez l'interface sur `host1` en tapant:

```
# ifconfig plip0 10.0.0.1 10.0.0.2
```

Configurez l'interface sur `host2` en tapant:

```
# ifconfig plip0 10.0.0.2 10.0.0.1
```

Vous devriez avoir maintenant une connexion qui fonctionne. Veuillez consulter les pages de manuel lp(4) et lpt(4) pour plus de détails.

Vous devriez également ajouter les deux noms de machines dans le fichier /etc/hosts:

```
127.0.0.1               localhost.my.domain localhost
10.0.0.1                host1.my.domain host1
```

```
10.0.0.2                host2.my.domain
```

Pour vérifier le bon fonctionnement de la connexion, aller sur les deux machines et effectuez un "ping" vers l'autre machine. Par exemple, sur `host1`:

```
# ifconfig plip0
plip0: flags=8851<UP,POINTOPOINT,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet 10.0.0.1 --> 10.0.0.2 netmask 0xff000000
# netstat -r
Routing tables

Internet:
Destination        Gateway           Flags     Refs     Use      Netif Expire
host2              host1               UH          0       0       plip0
# ping -c 4 host2
PING host2 (10.0.0.2): 56 data bytes
64 bytes from 10.0.0.2: icmp_seq=0 ttl=255 time=2.774 ms
64 bytes from 10.0.0.2: icmp_seq=1 ttl=255 time=2.530 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=255 time=2.556 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=255 time=2.714 ms

--- host2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.530/2.643/2.774/0.103 ms
```

33.10. IPv6

L'IPv6 (également connu sous le nom de IPng "IP nouvelle génération") est la nouvelle version du très célèbre protocole IP (aussi connu sous le nom d'IPv4). Comme les autres systèmes BSD, FreeBSD utilise l'implémentation IPv6 KAME. Votre système FreeBSD est donc fourni avec tout ce dont vous aurez besoin pour tester l'IPv6. Cette section se concentre sur la configuration et l'utilisation d'IPv6.

Au début des années 90, on a pris conscience de la diminution rapide de l'espace d'adresses IPv4. Etant donné le taux d'expansion de l'Internet, deux problèmes majeurs apparaissaient:

- Le manque d'adresses. Aujourd'hui ce n'est plus vraiment un problème puisque les espaces d'adresses privées RFC1918 (`10.0.0.0/8`, `172.16.0.0/12`, et `192.168.0.0/16`) et la translation d'adresses (NAT) sont utilisés.
- Les tables des routeurs devenaient trop importantes. C'est toujours un problème actuellement.

L'IPv6 remédie à ces problèmes et à de nombreux autres:

- Espace d'adressage sur 128 bits. Ou plus précisément, il y a 340 282 366 920 938 463 463 374 607 431 768 211 456 adresses disponibles. Cela équivaut à approximativement 6.67 * 10^27 adresses IPv6 par kilomètre-carré de surface de notre planète.
- Les routeurs ne stockeront que des regroupements d'adresses dans leurs tables de routage

réduisant donc l'espace moyen d'une table de routage à 8192 entrées.

IPv6 présente également de nombreuses autres intéressantes fonctionnalités telles que:

- L'autoconfiguration des adresses (RFC2462)
- Adresses unicast ("une parmi plusieurs")
- Adresses multicast (multidestinataires) obligatoires
- IPsec (protocole de sécurité IP)
- Struture d'entête simplifiée
- IP mobile
- Mécanismes de transition IPv6-vers-IPv4

Pour plus d'informations consultez les références suivantes:

- Généralités sur l'IPv6 à playground.sun.com
- KAME.net
- 6bone.net

33.10.1. Les adresses IPv6

Il existe différent types d'adresses IPv6: unicast, anycast et multicast.

Les adresses unicast (mono-destinataire) sont les adresses classiques. Un paquet envoyé à une adresse unicast arrive à l'interface correspondant à l'adresse.

Les adresses anycast ne sont normalement pas distinguables des adresses unicast mais correspondent à un groupe d'interfaces. Un paquet destiné à une adresse anycast arrivera à l'interface la plus proche (en terme d'unité de distance du protocole de routage). Les adresses anycast devraient n'être utilisées que par les routeurs.

Les adresses multicast identifient un groupe d'interfaces. Un paquet destiné à une adresse multicast arrivera sur toutes les interfaces appartenant au groupe multicast.

L'adresse de diffusion IPv4 (généralement `xxx.xxx.xxx.255`) est exprimée par des adresses multicast en IPv6.

Tableau 9. Adresses IPv6 réservées

Adresse IPv6	Longueur du préfixe (bits)	Description	Notes
`::`	128 bits	non-spécifiée	similaire à `0.0.0.0` sous IPv4
`::1`	128 bits	adresse de boucle	similaire à `127.0.0.1` sous IPv4

Adresse IPv6	Longueur du préfixe (bits)	Description	Notes
`::00:xx:xx:xx:xx`	96 bits	IPv4 encapsulé	Les 32 bits de poids faible sont l'adresse IPv4. Egalement appelée "adresse IPv6 compatible IPv4".
`::ff:xx:xx:xx:xx`	96 bits	adresse IPv6 mappée IPv4	Les 32 bits de poids faible sont l'adresse IPv4. Destinées aux machines ne supportant pas l'IPv6.
`fe80::` - `feb::`	10 bits	lien-local	similaire à l'interface de boucle sous IPv4
`fec0::` - `fef::`	10 bits	site-local	
`ff::`	8 bits	multicast	
`001` (base 2)	3 bits	unicast globale	Toutes les adresses unicast globales sont assignées à partir de ce pool. Les trois premiers bits de l'adresse sont "001".

33.10.2. Lecture des adresses IPv6

La forme canonique est représentée suivant le schéma: `x:x:x:x:x:x:x:x`, où chaque "x" est une valeur héxadécimale sur 16 bits. Par exemple `FEBC:A574:382B:23C1:AA49:4592:4EFE:9982`

Souvent dans une adresse on aura de longues sous-parties constituées de zéros, une telle sous-partie peut être abrégée par "::". Les trois "0"s de poids fort de chaque quartet hexadécimal peuvent également être omis. Par exemple `fe80::1` correspond à la forme canonique `fe80:0000:0000:0000:0000:0000:0000:0001`.

Une troisième forme est d'écrire les derniers 32 bits dans le style IPv4 bien connu (décimal) avec des points "." comme séparateurs. Par exemple `2002::10.0.0.1` correspond à la représentation canonique (hexadécimale) `2002:0000:0000:0000:0000:0000:0a00:0001` qui est à son tour équivalente à l'écriture `2002::a00:1`.

Maintenant le lecteur devrait être en mesure de comprendre ce qui suit:

```
# ifconfig
```

```
rl0: flags=8943UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST mtu 1500
        inet 10.0.0.10 netmask 0xffffff00 broadcast 10.0.0.255
```

```
        inet6 fe80::200:21ff:fe03:8e1%rl0 prefixlen 64 scopeid 0x1
        ether 00:00:21:03:08:e1
        media: Ethernet autoselect (100baseTX )
        status: active
```

`fe80::200:21ff:fe03:8e1%rl0` est une adresse de lien local configurée automatiquement. Elle est générée à partir de l'adresse MAC dans le cas de l'autoconfiguration.

Pour plus d'informations sur la structure des adresses IPv6 consultez la RFC3513.

33.10.3. Se connecter

Actuellement, il y a quatre façons de se connecter à des machines et des réseaux utilisant l'IPv6:

- Rejoindre le réseau expérimental 6bone
- Obtenir un réseau IPv6 auprès de votre fournisseur d'accès. Contactez votre fournisseur d'accès Internet pour plus d'informations.
- Utilisation d'un tunnel 6-vers-4 (RFC3068)
- Utilisation du logiciel porté net/freenet6 si vous utilisez une connexion par modem.

Ici nous ne parlerons que de la manière de se connecter au réseau 6bone puisque cela semble être aujourd'hui la méthode de connexion la plus populaire.

Consultez tout d'abord le site 6bone et recherchez une connexion 6bone proche de vous. Contactez le responsable et avec un peu de chance on vous donnera les instructions à suivre pour configurer votre connexion. Généralement cela implique la mise en place d'un tunnel GRE (gif).

Voici un exemple typique de configuration d'un tunnel gif(4):

```
# ifconfig gif0 create
# ifconfig gif0
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
# ifconfig gif0 tunnel MON_ADR_IPv4 MON_ADR_IPv4_ASSIGNEE_A_LAUTRE_BOUT_DU_TUNNEL
# ifconfig gif0 inet6 alias MON_ADR_IPv6_ASSIGNEE_A_LEXTREMITE_DU_TUNNEL
MON_ADR_IPv6_ASSIGNEE_A_LAUTRE_BOUT_DU_TUNNEL
```

Remplacez les mots en majuscules par les informations que vous avez reçues du point d'accès 6bone.

Ceci établit le tunnel. Vérifiez si le tunnel fonctionne en utilisant ping6(8) sur l'adresse `ff02::1%gif0`. Vous devriez récevoir les réponses aux requêtes ping.

Au cas où vous seriez intrigué par l'adresse `ff02:1%gif0`, sachez que c'est une adresse multicast. `%gif0` précise que l'adresse multicast de l'interface gif0 doit être utilisée. Puisque nous utilisons `ping` sur une adresse multicast, l'autre bout du tunnel devrait également répondre.

Désormais, la mise en place d'une route vers votre lien 6bone devrait être relativement directe:

```
# route add -inet6 default -interface gif0
# ping6 -n MON_LIEN_MONTANT
```

```
# traceroute6 www.jp.FreeBSD.org
(3ffe:505:2008:1:2a0:24ff:fe57:e561) from 3ffe:8060:100::40:2, 30 hops max, 12 byte
packets
     1  atnet-meta6  14.147 ms  15.499 ms  24.319 ms
     2  6bone-gw2-ATNET-NT.ipv6.tilab.com  103.408 ms  95.072 ms *
     3  3ffe:1831:0:ffff::4  138.645 ms  134.437 ms  144.257 ms
     4  3ffe:1810:0:6:290:27ff:fe79:7677  282.975 ms  278.666 ms  292.811 ms
     5  3ffe:1800:0:ff00::4  400.131 ms  396.324 ms  394.769 ms
     6  3ffe:1800:0:3:290:27ff:fe14:cdee  394.712 ms  397.19 ms  394.102 ms
```

La sortie pourra être différente d'une machine à une autre. Maintenant vous devriez être en mesure d'atteindre le site IPv6 www.kame.net et de voir la tortue dansante - et cela si vous disposez d'un navigateur supportant l'IPv6 comme www/mozilla, Konqueror qui fait partie du logiciel x11/kdebase3, ou www/epiphany.

33.10.4. DNS dans le monde IPv6

A l'origine, il existait deux types d'enregistrement DNS pour l'IPv6. L'organisme IETF a déclaré obsolète l'enregistrement A6. Les enregistrements AAAA sont aujourd'hui le standard.

L'utilisation des enregistrements AAAA est assez direct. Assignez votre nom de machine à la nouvelle adresse IPv6 que vous venez d'obtenir en ajoutant:

```
MYHOSTNAME           AAAA    MYIPv6ADDR
```

à votre fichier de zone DNS primaire. Dans le cas où vous ne gérez pas vos propres zones DNS contactez le responsable de votre DNS. Les versions actuelles de bind (version 8.3 et 9) et dns/djbdns (avec le correctif IPv6) supportent les enregistrements AAAA.

33.10.5. Effectuer les changements nécessaires dans le fichier /etc/rc.conf

33.10.5.1. Paramétrage du client IPv6

Ces paramètres vous permettront de configurer une machine qui sera sur votre réseau local et sera un client, non pas un routeur. Pour que rtsol(8) configure automatiquement votre interface réseau au démarrage tout ce dont vous avez besoin d'ajouter est:

```
ipv6_enable="YES"
```

Pour assigner une adresse IP statique telle que `2001:471:1f11:251:290:27ff:fee0:2093`, à votre

interface fxp0, ajoutez:

```
ipv6_ifconfig_fxp0="2001:471:1f11:251:290:27ff:fee0:2093"
```

Pour assigner le routeur par défaut `2001:471:1f11:251::1`, ajoutez ce qui suit au fichier /etc/rc.conf:

```
ipv6_defaultrouter="2001:471:1f11:251::1"
```

33.10.5.2. Paramétrage d'un routeur/passerelle IPv6

Ceci vous aidera à mettre en oeuvre les instructions que votre fournisseur de tunnel, tel que 6bone, vous a donné et à les convertir en paramètres qui seront conservés à chaque démarrage. Pour rétablir votre tunnel au démarrage, utilisez quelque chose comme ce qui suit dans le fichier /etc/rc.conf:

Listez les interfaces génériques de tunnel qui seront configurées, par exemple gif0:

```
gif_interfaces="gif0"
```

Pour configurer l'interface avec une adresse (extrémité) locale *MY_IPv4_ADDR* vers une adresse (extrémité) distante *REMOTE_IPv4_ADDR*:

```
gifconfig_gif0="MY_IPv4_ADDR REMOTE_IPv4_ADDR"
```

Pour utiliser l'adresse IPv6 que l'on vous a assigné en vue d'être utilisée pour votre extrémité du tunnel IPv6, ajoutez:

```
ipv6_ifconfig_gif0="MY_ASSIGNED_IPv6_TUNNEL_ENDPOINT_ADDR"
```

Ensuite tout ce qu'il reste à faire est de définir la route par défaut pour l'IPv6. C'est l'autre extrémité du tunnel IPv6:

```
ipv6_defaultrouter="MY_IPv6_REMOTE_TUNNEL_ENDPOINT_ADDR"
```

33.10.5.3. Paramétrage d'un tunnel IPv6

Si le serveur doit router de l'IPv6 entre votre réseau et le reste du monde, le paramètre suivant sera également nécessaire dans votre fichier /etc/rc.conf:

```
ipv6_gateway_enable="YES"
```

33.10.6. Annonce du routeur et auto-configuration

Cette section vous aidera à configurer rtadvd(8) pour l'annonce de la route IPv6 par défaut.

Pour activer rtadvd(8), vous devrez ajouter ce qui suit à votre fichier /etc/rc.conf:

```
rtadvd_enable="YES"
```

Il est important que vous indiquiez l'interface sur laquelle le routeur IPv6 sera sollicité. Par exemple pour que rtadvd(8) utilise fxp0:

```
rtadvd_interfaces="fxp0"
```

Nous devons maintenant créer le fichier de configuration /etc/rtadvd.conf. Voici un exemple:

```
fxp0:\
    :addrs#1:addr="2001:471:1f11:246::":prefixlen#64:tc=ether:
```

Remplacez fxp0 avec l'interface que vous allez utiliser.

Ensuite remplacez `2001:471:1f11:246::` avec votre préfixe.

Si vous êtes un sous-réseau `/64` dédié, il ne sera pas nécessaire de modifier quelque chose d'autre. Sinon, vous devrez modifier `prefixlen#` avec la valeur correcte.

33.11. ATM ("Asynchronous Transfer Mode")

33.11.1. Configuration IP conventionnelle sur ATM (PVCs)

L'IP conventionnelle sur ATM ("Classical IP over ATM"-CLIP) est la méthode la plus simple pour utiliser ATM (Asynchronous Transfer Mode) avec l'IP. Elle peut être utilisée en mode non connecté ("Switched Virtual Connections"-SVCs) et en mode connecté ("Permanent Virtual Connections"-PVCs). Cette section décrit comment configurer un réseau basé sur les PVCs.

33.11.1.1. Configurations en réseau maillé

La première méthode de configuration CLIP avec des PVCs est de connecter entre elles chaque machine du réseau par l'intermédiaire d'une PVC dédiée. Bien que cela soit simple à configurer, cela tend à devenir impraticable avec un nombre important de machines. Notre exemple suppose que nous avons quatre machines sur le réseau, chacune connectée au réseau ATM à l'aide d'une carte réseau ATM. La première étape est d'établir le plan des adresses IP et des connexions ATM entre machines. Nous utilisons le plan suivant:

Machine	Adresse IP
hostA	192.168.173.1

Machine	Adresse IP
hostB	192.168.173.2
hostC	192.168.173.3
hostD	192.168.173.4

Pour réaliser un réseau maillé, nous avons besoin d'une connexion ATM entre chaque paire de machines:

Machines	Couple VPI.VCI
hostA - hostB	0.100
hostA - hostC	0.101
hostA - hostD	0.102
hostB - hostC	0.103
hostB - hostD	0.104
hostC - hostD	0.105

Les valeurs VPI et VCI à chaque extrémité de la connexion peuvent bien évidemment être différentes, mais par souci de simplicité nous supposerons quelles sont identiques. Ensuite nous devons configurer les interfaces ATM sur chaque machine:

```
hostA# ifconfig hatm0 192.168.173.1 up
hostB# ifconfig hatm0 192.168.173.2 up
hostC# ifconfig hatm0 192.168.173.3 up
hostD# ifconfig hatm0 192.168.173.4 up
```

en supposant que l'interface ATM est hatm0 sur toutes les machines. Maintenant les PVCs doivent être configurées sur hostA (nous supposons qu'elles sont déjà configurées sur les switches ATM, vous devez consulter le manuel du switch sur comment réaliser cette configuration).

```
hostA# atmconfig natm add 192.168.173.2 hatm0 0 100 llc/snap ubr
hostA# atmconfig natm add 192.168.173.3 hatm0 0 101 llc/snap ubr
hostA# atmconfig natm add 192.168.173.4 hatm0 0 102 llc/snap ubr

hostB# atmconfig natm add 192.168.173.1 hatm0 0 100 llc/snap ubr
hostB# atmconfig natm add 192.168.173.3 hatm0 0 103 llc/snap ubr
hostB# atmconfig natm add 192.168.173.4 hatm0 0 104 llc/snap ubr

hostC# atmconfig natm add 192.168.173.1 hatm0 0 101 llc/snap ubr
hostC# atmconfig natm add 192.168.173.2 hatm0 0 103 llc/snap ubr
hostC# atmconfig natm add 192.168.173.4 hatm0 0 105 llc/snap ubr

hostD# atmconfig natm add 192.168.173.1 hatm0 0 102 llc/snap ubr
hostD# atmconfig natm add 192.168.173.2 hatm0 0 104 llc/snap ubr
hostD# atmconfig natm add 192.168.173.3 hatm0 0 105 llc/snap ubr
```

Bien évidemment des contrats de trafic autres qu'UBR ("Unspecified Bit Rate") peuvent être utilisés dès que la carte ATM les supportent. Dans ce cas le nom du contrat de trafic est suivi par les paramètres du trafic. De l'aide concernant l'outil atmconfig(8) peut être obtenue avec:

```
# atmconfig help natm add
```

ou dans la page de manuel de atmconfig(8).

La même configuration peut être faite par l'intermédiaire de /etc/rc.conf. Pour la machine `hostA` cela ressemblerait à:

```
network_interfaces="lo0 hatm0"
ifconfig_hatm0="inet 192.168.173.1 up"
natm_static_routes="hostB hostC hostD"
route_hostB="192.168.173.2 hatm0 0 100 llc/snap ubr"
route_hostC="192.168.173.3 hatm0 0 101 llc/snap ubr"
route_hostD="192.168.173.4 hatm0 0 102 llc/snap ubr"
```

L'état de toutes les routes CLIP peut être obtenu avec:

```
hostA# atmconfig natm show
```

Partie V: Annexes

Annexe A: Se procurer FreeBSD

A.1. Editeurs de CD-ROMs et DVDs

A.1.1. Produits vendus en boîte

Des versions en boîte de FreeBSD sont disponibles (CDs de FreeBSD, logiciels supplémentaires, et documentation papier) auprès de plusieurs revendeurs:

- CompUSA
  WWW: http://www.compusa.com/
- Frys Electronics
  WWW: http://www.frys.com/

A.1.2. CDs et DVDs

Les CDs et DVDs de FreeBSD sont disponibles auprès de nombreux revendeurs en ligne:

- BSD Mall by Daemon News
  PO Box 161
  Nauvoo, IL 62354
  USA
  Phone: +1 866 273-6255
  Fax: +1 217 453-9956
  Email: <sales@bsdmall.com>
  WWW: http://www.bsdmall.com/
- BSD-Systems
  Email: <info@bsd-systems.co.uk>
  WWW: http://www.bsd-systems.co.uk
- FreeBSD Mall, Inc.
  3623 Sanford Street
  Concord, CA 94520-1405
  USA
  Phone: +1 925 240-6652
  Fax: +1 925 674-0821
  Email: <info@freebsdmall.com>
  WWW: http://www.freebsdmall.com/
- Dr. Hinner EDV
  St. Augustinus-Str. 10
  D-81825 München
  Allemagne
  Phone: (089) 428 419
  WWW: http://www.hinner.de/linux/freebsd.html
- Ikarios
  22-24 rue Voltaire

92000 Nanterre
France
WWW: http://ikarios.com/form/#freebsd

- JMC Software
  Ireland
  Phone: 353 1 6291282
  WWW: http://www.thelinuxmall.com

- Linux CD Mall
  Private Bag MBE N348
  Auckland 1030
  New Zealand
  Phone: +64 21 866529
  WWW: http://www.linuxcdmall.co.nz/

- The Linux Emporium
  Hilliard House, Lester Way
  Wallingford
  OX10 9TA
  Royaume-Uni
  Phone: +44 1491 837010
  Fax: +44 1491 837016
  WWW: http://www.linuxemporium.co.uk/products/freebsd/

- Linux+ DVD Magazine
  Lewartowskiego 6
  Warsaw
  00-190
  Poland
  Phone: +48 22 860 18 18
  Email: <editors@lpmagazine.org>
  WWW: http://www.lpmagazine.org/

- Linux System Labs Australie
  21 Ray Drive
  Balwyn North
  VIC - 3104
  Australie
  Phone: +61 3 9857 5918
  Fax: +61 3 9857 8974
  WWW: http://www.lsl.com.au

- LinuxCenter.Ru
  Galernaya Street, 55
  Saint-Petersburg
  190000
  Russia
  Phone: +7-812-3125208
  Email: <info@linuxcenter.ru>
  WWW: http://linuxcenter.ru/freebsd

A.1.3. Distributeurs

Si vous êtes un revendeur et désirez vendre des CDROMs de FreeBSD, veuillez contacter un distributeur:

- Cylogistics
  809B Cuesta Dr., #2149
  Mountain View, CA 94040
  USA
  Phone: +1 650 694-4949
  Fax: +1 650 694-4953
  Email: <sales@cylogistics.com>
  WWW: http://www.cylogistics.com/
- Ingram Micro
  1600 E. St. Andrew Place
  Santa Ana, CA 92705-4926
  USA
  Phone: 1 (800) 456-8000
  WWW: http://www.ingrammicro.com/
- Kudzu, LLC
  7375 Washington Ave. S.
  Edina, MN 55439
  USA
  Phone: +1 952 947-0822
  Fax: +1 952 947-0876
  Email: <sales@kudzuenterprises.com>
- Navarre Corp
  7400 49th Ave South
  New Hope, MN 55428
  USA
  Phone: +1 763 535-8333
  Fax: +1 763 535-0341
  WWW: http://www.navarre.com/

A.2. Sites FTP

Les sources officielles de FreeBSD sont disponibles via FTP anonyme à partir d'un ensemble de sites miroir. Le site ftp://ftp.FreeBSD.org/pub/FreeBSD/ dispose d'une bonne connectivité et autorise un grand nombre de connexions, mais vous avez intérêt à trouver plutôt un site miroir "plus proche" (tout particulièrement si vous décidez de mettre en place une sorte de miroir à votre tour).

La base de données des sites miroir FreeBSD est plus à jour que la liste de ce Manuel, parce qu'elle tire ses informations du DNS plutôt que se reposer sur une liste statique de machines.

De plus, FreeBSD est disponible via FTP anonyme à partir des sites miroir ci-dessous. Si vous décidez de vous procurer FreeBSD via FTP anonyme, essayez si possible d'utiliser un site proche de vous. Les sites miroir listés en tant que "sites miroir primaires" disposent généralement de

l'intégralité de l'archive FreeBSD (toutes les versions actuellement disponibles pour chacune des architectures) mais vous obtiendrez les temps de téléchargements les plus courts à partir d'un site situé dans votre pays ou votre région. Les sites régionaux proposent les versions les plus récentes des architectures les plus populaires mais pourraient ne pas proposer l'intégralité de l'archive de FreeBSD. Tous les sites proposent un accès FTP anonyme mais certains sites fournissent également un accès suivant d'autres méthodes. Les méthodes d'accès disponibles pour chaque site sont données entre parenthèses après le nom de la machine.

Central Servers, Primary Mirror Sites, Armenia, Australia, Austria, Brazil, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Ireland, Japan, Korea, Latvia, Lithuania, Netherlands, New Zealand, Norway, Poland, Russia, Saudi Arabia, Slovenia, South Africa, Spain, Sweden, Switzerland, Taiwan, Ukraine, United Kingdom, United States of America.

(as of UTC)

Central Servers

ftp://ftp.FreeBSD.org/pub/FreeBSD/ (ftp / ftpv6 / http://ftp.FreeBSD.org/pub/FreeBSD/ / http://ftp.FreeBSD.org/pub/FreeBSD/)

Primary Mirror Sites

In case of problems, please contact the hostmaster <mirror-admin@FreeBSD.org> for this domain.

- ftp://ftp1.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp3.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp4.FreeBSD.org/pub/FreeBSD/ (ftp / ftpv6 / http://ftp4.FreeBSD.org/pub/FreeBSD/ / http://ftp4.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp5.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp6.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp7.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp10.FreeBSD.org/pub/FreeBSD/ (ftp / ftpv6 / http://ftp10.FreeBSD.org/pub/FreeBSD/ / http://ftp10.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp11.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp13.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp14.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp14.FreeBSD.org/pub/FreeBSD/)

Armenia

In case of problems, please contact the hostmaster <hostmaster@am.FreeBSD.org> for this domain.

- ftp://ftp1.am.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp1.am.FreeBSD.org/pub/FreeBSD/ / rsync)

Australia

In case of problems, please contact the hostmaster <hostmaster@au.FreeBSD.org> for this domain.

- ftp://ftp.au.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.au.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp3.au.FreeBSD.org/pub/FreeBSD/ (ftp)

Austria

In case of problems, please contact the hostmaster <hostmaster@at.FreeBSD.org> for this domain.

- ftp://ftp.at.FreeBSD.org/pub/FreeBSD/ (ftp / ftpv6 / http://ftp.at.FreeBSD.org/pub/FreeBSD/ / http://ftp.at.FreeBSD.org/pub/FreeBSD/)

Brazil

In case of problems, please contact the hostmaster <hostmaster@br.FreeBSD.org> for this domain.

- ftp://ftp2.br.FreeBSD.org/FreeBSD/ (ftp / http://ftp2.br.FreeBSD.org/)
- ftp://ftp3.br.FreeBSD.org/pub/FreeBSD/ (ftp / rsync)
- ftp://ftp4.br.FreeBSD.org/pub/FreeBSD/ (ftp)

Czech Republic

In case of problems, please contact the hostmaster <hostmaster@cz.FreeBSD.org> for this domain.

- ftp://ftp.cz.FreeBSD.org/pub/FreeBSD/ (ftp / ftp://ftp.cz.FreeBSD.org/pub/FreeBSD/ / http://ftp.cz.FreeBSD.org/pub/FreeBSD/ / http://ftp.cz.FreeBSD.org/pub/FreeBSD/ / rsync / rsyncv6)
- ftp://ftp2.cz.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp2.cz.FreeBSD.org/pub/FreeBSD/)

Denmark

In case of problems, please contact the hostmaster <staff@dotsrc.org> for this domain.

- ftp://ftp.dk.FreeBSD.org/pub/FreeBSD/ (ftp / ftpv6 / http://ftp.dk.FreeBSD.org/pub/FreeBSD/ / http://ftp.dk.FreeBSD.org/pub/FreeBSD/)

Estonia

In case of problems, please contact the hostmaster <hostmaster@ee.FreeBSD.org> for this domain.

- ftp://ftp.ee.FreeBSD.org/pub/FreeBSD/ (ftp)

Finland

In case of problems, please contact the hostmaster <hostmaster@fi.FreeBSD.org> for this domain.

- ftp://ftp.fi.FreeBSD.org/pub/FreeBSD/ (ftp)

France

In case of problems, please contact the hostmaster <hostmaster@fr.FreeBSD.org> for this domain.

- ftp://ftp.fr.FreeBSD.org/pub/FreeBSD/ (ftp)

- ftp://ftp1.fr.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp1.fr.FreeBSD.org/pub/FreeBSD/ / rsync)
- ftp://ftp3.fr.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp6.fr.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp6.fr.FreeBSD.org/pub/FreeBSD/ (ftp / rsync)
- ftp://ftp7.fr.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp8.fr.FreeBSD.org/pub/FreeBSD/ (ftp)

Germany

In case of problems, please contact the hostmaster <de-bsd-hubs@de.FreeBSD.org> for this domain.

- ftp://ftp.de.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp1.de.FreeBSD.org/freebsd/ (ftp / http://www1.de.FreeBSD.org/freebsd/ / rsync://rsync3.de.FreeBSD.org/freebsd/)
- ftp://ftp2.de.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp2.de.FreeBSD.org/pub/FreeBSD/ / rsync)
- ftp://ftp4.de.FreeBSD.org/FreeBSD/ (ftp / http://ftp4.de.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp5.de.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp7.de.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp7.de.FreeBSD.org/pub/FreeBSD/)

Greece

In case of problems, please contact the hostmaster <hostmaster@gr.FreeBSD.org> for this domain.

- ftp://ftp.gr.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.gr.FreeBSD.org/pub/FreeBSD/ (ftp)

Hong Kong

ftp://ftp.hk.FreeBSD.org/pub/FreeBSD/ (ftp)

Ireland

In case of problems, please contact the hostmaster <hostmaster@ie.FreeBSD.org> for this domain.

- ftp://ftp3.ie.FreeBSD.org/pub/FreeBSD/ (ftp / rsync)

Japan

In case of problems, please contact the hostmaster <hostmaster@jp.FreeBSD.org> for this domain.

- ftp://ftp.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp3.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp4.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp5.jp.FreeBSD.org/pub/FreeBSD/ (ftp)

- ftp://ftp6.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp7.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp8.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp9.jp.FreeBSD.org/pub/FreeBSD/ (ftp)

Korea

In case of problems, please contact the hostmaster <hostmaster@kr.FreeBSD.org> for this domain.

- ftp://ftp.kr.FreeBSD.org/pub/FreeBSD/ (ftp / rsync)
- ftp://ftp2.kr.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp2.kr.FreeBSD.org/pub/FreeBSD/)

Latvia

In case of problems, please contact the hostmaster <hostmaster@lv.FreeBSD.org> for this domain.

- ftp://ftp.lv.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.lv.FreeBSD.org/pub/FreeBSD/)

Lithuania

In case of problems, please contact the hostmaster <hostmaster@lt.FreeBSD.org> for this domain.

- ftp://ftp.lt.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.lt.FreeBSD.org/pub/FreeBSD/)

Netherlands

In case of problems, please contact the hostmaster <hostmaster@nl.FreeBSD.org> for this domain.

- ftp://ftp.nl.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.nl.FreeBSD.org/os/FreeBSD/ / rsync)
- ftp://ftp2.nl.FreeBSD.org/pub/FreeBSD/ (ftp)

New Zealand

- ftp://ftp.nz.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.nz.FreeBSD.org/pub/FreeBSD/)

Norway

In case of problems, please contact the hostmaster <hostmaster@no.FreeBSD.org> for this domain.

- ftp://ftp.no.FreeBSD.org/pub/FreeBSD/ (ftp / rsync)

Poland

In case of problems, please contact the hostmaster <hostmaster@pl.FreeBSD.org> for this domain.

- ftp://ftp.pl.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp2.pl.FreeBSD.org

Russia

In case of problems, please contact the hostmaster <hostmaster@ru.FreeBSD.org> for this domain.

- ftp://ftp.ru.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.ru.FreeBSD.org/FreeBSD/ / rsync)
- ftp://ftp2.ru.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp2.ru.FreeBSD.org/pub/FreeBSD/ / rsync)
- ftp://ftp5.ru.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp5.ru.FreeBSD.org/pub/FreeBSD/ / rsync)
- ftp://ftp6.ru.FreeBSD.org/pub/FreeBSD/ (ftp)

Saudi Arabia

In case of problems, please contact the hostmaster <ftpadmin@isu.net.sa> for this domain.

- ftp://ftp.isu.net.sa/pub/ftp.freebsd.org (ftp)

Slovenia

In case of problems, please contact the hostmaster <hostmaster@si.FreeBSD.org> for this domain.

- ftp://ftp.si.FreeBSD.org/pub/FreeBSD/ (ftp)

South Africa

In case of problems, please contact the hostmaster <hostmaster@za.FreeBSD.org> for this domain.

- ftp://ftp.za.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.za.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp4.za.FreeBSD.org/pub/FreeBSD/ (ftp)

Spain

In case of problems, please contact the hostmaster <hostmaster@es.FreeBSD.org> for this domain.

- ftp://ftp.es.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.es.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp3.es.FreeBSD.org/pub/FreeBSD/ (ftp)

Sweden

In case of problems, please contact the hostmaster <hostmaster@se.FreeBSD.org> for this domain.

- ftp://ftp.se.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.se.FreeBSD.org/pub/FreeBSD/ (ftp / rsync://ftp2.se.FreeBSD.org/)
- ftp://ftp3.se.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp4.se.FreeBSD.org/pub/FreeBSD/ (ftp / ftp://ftp4.se.FreeBSD.org/pub/FreeBSD/ / http://ftp4.se.FreeBSD.org/pub/FreeBSD/ / http://ftp4.se.FreeBSD.org/pub/FreeBSD/ / rsync://ftp4.se.FreeBSD.org/pub/FreeBSD/ / rsync://ftp4.se.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp6.se.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp6.se.FreeBSD.org/pub/FreeBSD/)

Switzerland

In case of problems, please contact the hostmaster <hostmaster@ch.FreeBSD.org> for this domain.

- ftp://ftp.ch.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.ch.FreeBSD.org/pub/FreeBSD/)

Taiwan

In case of problems, please contact the hostmaster <hostmaster@tw.FreeBSD.org> for this domain.

- ftp://ftp.ch.FreeBSD.org/pub/FreeBSD/ (ftp / ftp://ftp.tw.FreeBSD.org/pub/FreeBSD/ / rsync / rsyncv6)
- ftp://ftp2.tw.FreeBSD.org/pub/FreeBSD/ (ftp / ftp://ftp2.tw.FreeBSD.org/pub/FreeBSD/ / http://ftp2.tw.FreeBSD.org/pub/FreeBSD/ / http://ftp2.tw.FreeBSD.org/pub/FreeBSD/ / rsync / rsyncv6)
- ftp://ftp4.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp5.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp6.tw.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp6.tw.FreeBSD.org/ / rsync)
- ftp://ftp7.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp8.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp11.tw.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp11.tw.FreeBSD.org/FreeBSD/)
- ftp://ftp12.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp13.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp14.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp15.tw.FreeBSD.org/pub/FreeBSD/ (ftp)

Ukraine

- ftp://ftp.ua.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.ua.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp6.ua.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp6.ua.FreeBSD.org/pub/FreeBSD / rsync://ftp6.ua.FreeBSD.org/FreeBSD/)
- ftp://ftp7.ua.FreeBSD.org/pub/FreeBSD/ (ftp)

United Kingdom

In case of problems, please contact the hostmaster <hostmaster@uk.FreeBSD.org> for this domain.

- ftp://ftp.uk.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.uk.FreeBSD.org/pub/FreeBSD/ (ftp / rsync://ftp2.uk.FreeBSD.org/ftp.freebsd.org/pub/FreeBSD/)
- ftp://ftp3.uk.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp4.uk.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp5.uk.FreeBSD.org/pub/FreeBSD/ (ftp)

United States of America

In case of problems, please contact the hostmaster <hostmaster@us.FreeBSD.org> for this domain.

- ftp://ftp1.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp3.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp4.us.FreeBSD.org/pub/FreeBSD/ (ftp / ftpv6 / http://ftp4.us.FreeBSD.org/pub/FreeBSD/ / http://ftp4.us.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp5.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp6.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp8.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp10.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp11.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp13.us.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp13.us.FreeBSD.org/pub/FreeBSD/ / rsync)
- ftp://ftp14.us.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp14.us.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp15.us.FreeBSD.org/pub/FreeBSD/ (ftp)

A.3. CVS anonyme

A.3.1. Introduction

CVS anonyme (ou comme on l'appelle également, *anoncvs*) est une de fonctionnalité des utilitaires CVS livrés avec FreeBSD qui permet la synchronisation avec un référentiel CVS sur une machine distante. Elle permet, entre autres, aux utilisateurs de FreeBSD, de lire, sans autorisation particulière, les archives disponibles sur l'un des serveurs anoncvs officiels du projet FreeBSD. Pour l'utiliser, il suffit simplement de définir la variable d'environnement `CVSROOT` pour qu'elle pointe sur le serveur anoncvs approprié, fournir le fameux mot de passe "anoncvs" avec la commande `cvs login`, puis ensuite utiliser la commande cvs(1) pour y accéder de la même manière qu'à un référentiel local.

La commande `cvs login`, stocke les mots de passe utilisés pour authentification sur le serveur CVS dans un fichier appelé .cvspass dans votre répertoire `HOME`. Si ce fichier n'existe pas, vous pourrez obtenir une erreur quand vous essaierez d'utiliser `cvs login` pour la première fois. Créez juste un fichier .cvspass vide, et relancez la commande.

Bien que l'on puisse aussi dire que CVSup et anoncvs assurent globalement la même fonction, il y a diverses nuances qui peuvent influencer l'utilisateur dans son choix d'une méthode de synchronisation. En résumé, CVSup utilise plus efficacement les ressources réseau et est de loin la méthode la plus sophistiquée des deux, mais cela a un prix. Pour employer CVSup, il faut d'abord installer et configurer un programme client spécialisé avant de pouvoir récupérer quoi que ce soit, et il faut ensuite travailler par sous-ensemble relativement importants, que CVSup appelle *catalogues*.

anoncvs, au contraire, peut être utilisé pour examiner n'importe quoi, d'un seul fichier à un programme particulier (tel que `ls` ou `grep`) en faisant référence au nom du module CVS. Bien sûr,

anoncvs n'est bon qu'à lire un référentiel CVS, si vous avez donc l'intention de développer localement sur un référentiel partagé avec le projet FreeBSD, alors vous n'avez d'autre choix que d'utiliser CVSup.

A.3.2. Utiliser CVS anonyme

Configurer cvs(1) pour utiliser un référentiel CVS anonyme consiste simplement à définir la variable d'environnement `CVSROOT` pour qu'elle pointe sur l'un des serveurs anoncvs du projet FreeBSD. A la date de rédaction de ce document, les serveurs suivants sont disponibles:

- *Autriche*: :pserver:anoncvs@anoncvs.at.FreeBSD.org:/home/ncvs (Utilisez `cvs login` et entrez le mot de passe "anoncvs" quand on vous le demandera.)
- *France*: :pserver:anoncvs@anoncvs.fr.FreeBSD.org:/home/ncvs (pserver (mot de passe "anoncvs"), ssh (aucun mot de passe))
- *Allemagne*: :pserver:anoncvs@anoncvs.de.FreeBSD.org:/home/ncvs (rsh, pserver, ssh, ssh/2022)
- *Japon*: :pserver:anoncvs@anoncvs.jp.FreeBSD.org:/home/ncvs (Utilisez `cvs login` et entrez le mot de passe "anoncvs" quand on vous le demandera.)
- *Taiwan*: :pserver:anoncvs@anoncvs.tw.FreeBSD.org:/home/ncvs (pserver (utilisez `cvs login` and entrez n'importe quel mot de passe quand on vous le demandera), ssh (pas de mot de passe))

```
SSH2 HostKey: 1024 e8:3b:29:7b:ca:9f:ac:e9:45:cb:c8:17:ae:9b:eb:55
/etc/ssh/ssh_host_dsa_key.pub
```

- *USA*: freebsdanoncvs@anoncvs.FreeBSD.org:/home/ncvs (ssh uniquement - pas de mot de passe)

```
SSH HostKey: 1024 a1:e7:46:de:fb:56:ef:05:bc:73:aa:91:09:da:f7:f4
root@sanmateo.ecn.purdue.edu
SSH2 HostKey: 1024 52:02:38:1a:2f:a8:71:d3:f5:83:93:8d:aa:00:6f:65
ssh_host_dsa_key.pub
```

- *USA*: anoncvs@anoncvs1.FreeBSD.org:/home/ncvs (ssh2 uniquement - pas de mot de passe)

```
SSH2 HostKey: 2048 53:1f:15:a3:72:5c:43:f6:44:0e:6a:e9:bb:f8:01:62
/etc/ssh/ssh_host_dsa_key.pub
```

Comme CVS vous permet de récupérer ("check out") pratiquement n'importe quelle version des sources de FreeBSD ayant existé (ou, dans certains cas, à venir), vous devez maîtriser l'indicateur de révision (`-r`) de cvs(1) et connaître les valeurs qu'il peut prendre dans le référentiel du projet FreeBSD.

Il y a deux sortes d'étiquettes, les étiquettes de révision et les étiquettes de branches. Les étiquettes de révision s'appliquent à une révision particulière. Leur signification ne varie pas d'un jour à l'autre. Les étiquettes de branche, à l'inverse, se rapportent à la dernière révision sur une branche particulière à un moment donné. Comme les étiquettes de branche ne se rapportent pas à une

révision particulière, elles peuvent désigner demain quelque chose de différent de ce qu'elles référencent aujourd'hui.

Etiquettes CVS présente les étiquettes de révision qui peuvent intéresser l'utilisateur. Encore une fois, aucune ne s'applique au catalogue des logiciels portés puisque ce dernier ne présente pas de multiples branches de développement.

Quand vous précisez une étiquette de branche, vous obtenez normalement la dernière version des fichiers de cette branche de développement. Si vous voulez une version antérieure, vous pouvez l'obtenir en précisant une date avec l'indicateur `-D date`. Reportez-vous aux pages de manuel cvs(1) pour plus de détails.

A.3.3. Exemples

Bien qu'il soit vraiment recommandé de lire attentivement les pages de manuel de cvs(1) avant de faire quoi que ce soit, voici quelques exemples rapides qui vous montrent essentiellement comment utiliser CVS anonyme:

Exemple 44. Récupérer quelque chose de -CURRENT (ls(1)):

```
% setenv CVSROOT :pserver:anoncvs@anoncvs.tw.FreeBSD.org:/home/ncvs
% cvs login
At the prompt, enter any word for « password ».
% cvs co ls
```

Exemple 45. Utiliser SSH pour récupérer l'arborescence src/:

```
% cvs -d freebsdanoncvs@anoncvs.FreeBSD.org:/home/ncvs co src
The authenticity of host 'anoncvs.freebsd.org (128.46.156.46)' can't be
established.
DSA key fingerprint is 52:02:38:1a:2f:a8:71:d3:f5:83:93:8d:aa:00:6f:65.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'anoncvs.freebsd.org' (DSA) to the list of known hosts.
```

Exemple 46. Récupérer la version 6-STABLE de ls(1):

```
% setenv CVSROOT :pserver:anoncvs@anoncvs.tw.FreeBSD.org:/home/ncvs
% cvs login
At the prompt, enter any word for « password ».
% cvs co -rRELENG_6 ls
```

Exemple 47. Générer la liste des différences concernant ls(1) (sous forme de "diffs unifiés") entre différentes versions de FreeBSD

```
% setenv CVSROOT :pserver:anoncvs@anoncvs.tw.FreeBSD.org:/home/ncvs
% cvs login
At the prompt, enter any word for « password ».
% cvs rdiff -u -rRELENG_5_3_0_RELEASE -rRELENG_5_4_0_RELEASE ls
```

Exemple 48. Savoir quels autres noms de modules peuvent être utilisés:

```
% setenv CVSROOT :pserver:anoncvs@anoncvs.tw.FreeBSD.org:/home/ncvs
% cvs login
At the prompt, enter any word for « password ».
% cvs co modules
% more modules/modules
```

A.3.4. Autres ressources

Les ressources supplémentaires suivantes peuvent être utiles pour apprendre à se servir de CVS:

- Guide CVS de Cal Poly.
- CVS Home, la communauté de développement et de support de CVS.
- CVSweb est l'interface Web pour CVS du projet FreeBSD.

A.4. Utiliser CTM

CTM est une méthode pour synchroniser une arborescence de répertoires distants avec une arborescence centrale. Elle a été développée pour être utilisée avec l'arborescence des sources de FreeBSD, bien que d'autres puissent avec le temps la trouver utile pour d'autres besoins. Il existe actuellement très peu, sinon aucune, documentation sur la façon de créer les deltas, contactez-donc la liste de diffusion ctm-users-desc pour obtenir plus d'informations et si vous souhaitez utiliser CTM pour autre chose.

A.4.1. Pourquoi utiliser CTM?

CTM vous procurera un exemplaire local de l'arborescence des sources de FreeBSD. Il y a plusieurs "moutures" de l'arborescence disponibles. Que vous désiriez suivre toute l'arborescence CVS ou seulement une de ses branches, CTM peut vous fournir ce dont vous avez besoin. Si vous développez activement sous FreeBSD, mais ne disposez que d'une connectivité TCP/IP peu fiable ou n'en avez pas du tout, ou voulez tout simplement que les modifications vous soient automatiquement envoyées, CTM est ce qu'il vous faut. Il vous faudra jusqu'à trois deltas par jour sur les branches les plus actives. Cependant, vous devriez envisager de vous les faire envoyer automatiquement par courrier électronique. La taille des mises à jour est toujours aussi petite que possible. Typiquement moins de 5KO, occasionnellement (une fois sur 10), entre 10 et 50KO, et de

temps à autre, une grosse modification de 100KO ou plus.

Vous devrez aussi vous tenir au courant des différentes contre-parties liées au fait de travailler directement avec les sources en cours de développement plutôt qu'avec les versions publiées. C'est particulièrement vrai si vous choisissez les sources de la branche "-CURRENT". Il est recommandé de lire Se synchroniser avec la version -CURRENT de FreeBSD.

A.4.2. Que vous faut-il pour utiliser CTM?

Vous aurez besoin de deux choses: le programme CTM, et les deltas initiaux à lui fournir (pour mettre à jour avec la version "courante").

Le programme CTM fait partie de FreeBSD depuis la publication de la version 2.0, et se trouve dans /usr/src/usr.sbin/ctm si vous avez un exemplaire des sources en ligne.

Vous pouvez obtenir les "deltas" à fournir à CTM de deux façons, par FTP ou par courrier électronique. Si vous avez un accès FTP à l'Internet, les sites suivants supportent l'accès à CTM:

ftp://ftp.FreeBSD.org/pub/FreeBSD/CTM/

ou reportez-vous à la section Sites miroirs.

Allez dans le répertoire vous concernant et commencez par télécharger le fichier README.

Si vous souhaitez récupérer vos deltas par courrier électronique:

Abonnez-vous à l'une des listes de distribution CTM. ctm-cvs-cur-desc comprend toute l'arborescence -CURRENT. liste de diffusion des sources de la branche 4-STABLE via CTM concerne la branche 4.X, etc... (Si vous ne savez pas comment vous abonner à une liste, cliquez sur le nom de la liste ci-dessus ou sur https://lists.freebsd.org puis cliquez sur la liste à laquelle vous désirez vous abonner. La page devrait contenir toutes les instructions nécessaires à l'abonnement.)

Dès que vous commencez à recevoir vos mises à jour CTM par courrier électronique, vous pouvez utiliser le programme `ctm_rmail` pour les décompacter et les appliquer. Vous pouvez en fait utiliser directement le programme `ctm_rmail` à partir d'une entrée dans /etc/aliases si vous voulez automatiser complètement le processus. Consultez les pages de manuel de `ctm_rmail` pour plus de détails.

Quelle que soit la méthode que vous utilisez pour récupérer les deltas CTM, vous devriez vous abonner à la liste de diffusion ctm-announce-desc. Ce sera, dans l'avenir, le seul endroit où les annonces concernant le fonctionnement du système CTM seront faites. Cliquez sur le nom de la liste et suivez les instructions pour s'inscrire à la liste.

A.4.3. Utiliser CTM pour la première fois

Avant de pouvoir utiliser les deltas CTM, il vous faut un point de départ pour appliquer les deltas générés à partir de là.

Tout d'abord vous devez déterminer ce que vous avez déjà. Tout le monde peut partir d'un

répertoire "vide". Vous devez utiliser un delta "Empty" (vide) au départ pour débuter votre arborescence supportée par CTM. Il fut question que l'un de ces deltas de départ soit distribué sur le CD, cependant ce n'est actuellement pas le cas.

Puisque les arborescences représentent plusieurs dizaines de mégaoctets, vous préférerez commencer avec ce que vous avez déjà sous la main. Si vous disposez d'une version de FreeBSD sur CD, vous pouvez copier ou extraire les sources initiales qui s'y trouvent. Cela évitera un transfert de données conséquent.

Vous pouvez reconnaître ces deltas de transition au `X` qui suit leur numéro de séquence (src-cur.3210XEmpty.gz par exemple). La dénomination après le `X` correspond à l'origine de votre "racine" initiale. Empty est un répertoire vide. La règle est qu'une transition de base à partir de Empty est générée tous les 100 deltas. Au passage, elles sont volumineuses! De 70 à 80 mégaoctets de données compressées avec `gzip` est une taille habituelle pour les deltas XEmpty.

Une fois que vous avez sélectionné un delta initial à partir duquel commencer, il vous faudra également tous les deltas de numéro supérieur qui le suivent.

A.4.4. Utiliser CTM au quotidien

Pour appliquer les deltas, tapez simplement:

```
# cd /où/vous/voulez/mettre/les/fichiers
# ctm -v -v /où/vous/mettez/vos/deltas/src-xxx.*
```

CTM reconnaît les deltas qui ont été compressés avec `gzip`, vous n'avez donc pas besoin de les décompresser avant, ce qui économise de l'espace disque.

A moins d'être absolument sûr du résultat, CTM ne touchera pas à votre arborescence. Pour contrôler la validité d'un delta, vous pouvez également utiliser l'indicateur `-c` et CTM ne modifiera alors pas votre arborescence; il vérifiera simplement l'intégrité du delta et regardera s'il peut s'appliquer proprement à votre arborescence en l'état.

Il y a aussi d'autres option pour CTM, voyez les pages de manuel ou lisez les sources pour plus d'informations.

C'est à peu près tout. Chaque fois que vous recevez un delta, passez-le à CTM pour tenir à jour votre arborescence des sources.

N'effacez pas les deltas s'il vous est difficile de les télécharger de nouveau. Vous pouvez en avoir besoin si quelque chose mauvais se produit. Même si vous n'avez que des disquettes, envisagez d'utiliser fdwrite(1) pour en faire une copie.

A.4.5. Conserver vos modifications locales

Si vous êtes développeur vous voudrez expérimenter et modifier des fichiers de l'arborescence des sources. CTM supporte de façon limitée les modifications locales: avant de contrôler l'existence d'un fichier foo, il regarde tout d'abord s'il y a un fichier foo.ctm. Si ce fichier existe, CTM l'utilisera au lieu de foo.

Ce comportement vous permet de conserver de façon simple des modifications locales: copiez simplement les fichiers que vous envisagez de modifier dans des fichiers de même nom, mais avec le suffixe .ctm. Vous pouvez ensuite bidouiller tranquillement le code, pendant que CTM maintient à jour le fichier .ctm.

A.4.6. D'autres options intéressantes de CTM

A.4.6.1. Savoir avec précision ce que va modifier une mise à jour

Vous pouvez connaître la liste des modifications que CTM appliquera à votre archive des sources en utilisant CTM avec l'option `-l`.

C'est utile si vous voulez conserver la trace des modifications, pré- ou post- modifier les fichiers concernés, ou vous vous sentez un tantinet paranoïaque.

A.4.6.2. Faire des sauvegardes avant la mise à jour

Parfois vous voudrez sauvegarder tous les fichiers qui seraient toucher par une mise à jour CTM.

Avec l'option `-B fichier_de_sauvegarde`, CTM sauvegarde tous les fichiers que seraient modifiés par delta CTM donné dans fichier_de_sauvegarde.

A.4.6.3. Restreindre la liste des fichiers touchés par une mise à jour

Parfois vous voudrez restreindre le champ d'application d'une mise à jour CTM, ou serez intéressé à n'extraire que quelques fichiers d'une séquence de deltas.

Vous pouvez contrôler la liste de fichiers sur laquelle travaillera CTM en donnant comme filtre une expression régulière avec les options `-e` et `-x`.

Par exemple, pour extraire une version à jour de lib/libc/Makefile de la série de deltas CTM que vous avez sauvegardé, lancez les commandes:

```
# cd /where/ever/you/want/to/extract/it/
# ctm -e '^lib/libc/Makefile' ~ctm/src-xxx.*
```

Pour chaque fichier d'un delta CTM, les options `-e` et `-x` sont appliquées dans l'ordre donné sur la ligne de commande. Le fichier est traité par CTM uniquement s'il est sélectionné après application des options `-e` et `-x`.

A.4.7. Perspectives pour CTM

Il y en a des tonnes:

- Utiliser une méthode d'authentification au système CTM pour détecter la substitution de mises à jour.
- Faire le ménage dans les options de CTM, elles commencent à engendrer de la confusion et à contredire l'intuition.

A.4.8. Divers

Il existe aussi une séquence de deltas pour le catalogue des logiciels portés, mais elle n'a pas reçue beaucoup d'écho jusqu'ici.

A.4.9. Miroirs CTM

CTM/FreeBSD est disponible via FTP anonyme sur les miroirs suivants. Si vous faites le choix de vous procurer CTM via FTP anonyme, utilisez s'il vous plaît un site proche de vous.

En cas de problème, contactez la liste de diffusion ctm-users-desc.

Californie, Bay Area, source officielle

- ftp://ftp.FreeBSD.org/pub/FreeBSD/development/CTM/

Afrique du Sud, serveur de sauvegarde pour les anciens deltas

- ftp://ftp.za.FreeBSD.org/pub/FreeBSD/CTM/

Taïwan/R.O.C.

- ftp://ctm.tw.FreeBSD.org/pub/FreeBSD/development/CTM/
- ftp://ctm2.tw.FreeBSD.org/pub/FreeBSD/development/CTM/
- ftp://ctm3.tw.FreeBSD.org/pub/FreeBSD/development/CTM/

Si vous n'avez pas trouvé de miroir proche de vous, où si le miroir est incomplet, essayez d'utiliser un moteur de recherche comme alltheweb.

A.5. Utiliser CVSup

A.5.1. Introduction

CVSup est un ensemble de logiciels pour la distribution et la mise à jour d'arborescences de sources à partir d'un référentiel CVS principal sur une machine serveur distante. Les sources de FreeBSD sont archivées sous un référentiel CVS sur une machine centrale de développement en Californie. Grâce à CVSup, les utilisateurs de FreeBSD peuvent facilement tenir à jour leur propre arborescence de sources.

CVSup utilise le modèle *pull* de mise à jour. Dans ce schéma, chaque client réclame les mises à jour au serveur, si et quand il le souhaite. Le serveur attend passivement les demandes de mises à jour de ses clients. Toutes les mises à jour sont donc faites à la demande du client. Le serveur n'envoie jamais de mise à jour non sollicitée. Les utilisateurs doivent soit exécuter le client CVSup à la main pour obtenir une mise à jour, soit mettre en oeuvre une tâche `cron` pour l'exécuter automatiquement et à intervalles réguliers.

Le terme CVSup, avec les majuscules, désigne l'ensemble du logiciel. Ses principales composantes sont le client `cvsup` qui s'exécute sur les machines de chaque utilisateur, et le serveur `cvsupd`, qui tourne sur tous les sites miroir de FreeBSD.

En lisant la documentation et les listes de diffusion de FreeBSD, vous trouverez des références à sup. sup était le prédécesseur de CVSup, et remplissait la même fonction. CVSup est utilisé de la

même façon que sup et, emploie de fait des fichiers de configuration qui sont compatibles avec ceux de sup. sup n'est plus utilisé pour le projet FreeBSD, parce que CVSup est à la fois plus rapide et plus souple.

L'utilitaire csup est une réécriture en C du logiciel CVSup. Son plus grand avantage est d'être plus rapide et de ne pas dépendre du langage Modula-3, vous n'avez donc pas besoin de l'installer. De plus si vous utilisez FreeBSD 6.2 ou une version suivante, vous pouvez directement utiliser cet utilitaire puisqu'il fait partie du système de base. Les anciennes versions de FreeBSD ne disposent pas de csup(1) dans leur système de base, mais vous pouvez facilement installer le logiciel porté net/csup, ou le paquetage pré-compilé correspondant. L'utilitaire csup ne supporte pas, cependant, le mode CVS. Si vous désirez dupliquer l'intégralité de dépôts, vous aurez toujours besoin de CVSup. Si vous avez décidé d'utiliser csup, passez les étapes concernant l'installation de CVSup et remplacez les références à CVSup par csup dans le reste de cette section.

A.5.2. Installation

La méthode la plus simple pour installer CVSup est d'utiliser la version pré-compilée net/cvsup du catalogue des logiciels portés de FreeBSD. Si vous préférez compiler CVSup à partir des sources, vous pouvez directement utiliser le logiciel porté net/cvsup. Cependant soyez averti: le logiciel porté net/cvsup est écrit en Modula-3, qui demande un temps et un espace disque non négligeables pour le télécharger et le compiler.

Si vous avez l'intention d'utiliser CVSup sur une machine qui ne disposera pas de XFree86™ ou Xorg, comme un serveur, assurez-vous que le logiciel porté de n'incluera pas l'interface graphique ("GUI") de CVSup, net/cvsup-without-gui.

Si vous voulez installer csup sous FreeBSD 6.1 et version précédentes, vous pouvez utiliser le paquetage pré-compilé net/csup du catalogue des logiciels portés. Si vous préférez compiler csup à partir des sources, vous pouvez directement utiliser le logiciel porté net/csup.

A.5.3. Configuration de CVSup

Le fonctionnement de CVSup est contrôlé par un fichier de configuration appelé supfile. Il y a des exemples de fichiers supfile dans le répertoire /usr/shared/examples/cvsup/.

Les informations du fichier supfile répondent pour CVSup aux question suivantes:

- Quels fichiers voulez-vous télécharger?
- Quelles versions de ces fichiers voulez-vous?
- D'où voulez-vous les télécharger?
- Où voulez-vous les mettre sur votre machine?
- Où voulez-vous mettre les fichiers d'état de votre machine?

Dans les sections suivantes, nous allons renseigner un fichier supfile typique en répondant une à une à chacune de ces questions. Commençons par décrire la structure d'ensemble d'un fichier

supfile.

Un fichier supfile est un fichier texte. Les commentaires débutent par un `#` et se prolongent jusqu'à la fin de la ligne. Les lignes vides ou qui ne contiennent que des commentaires sont ignorées.

Les autres lignes décrivent les ensembles de fichiers que l'utilisateur souhaite recevoir. Ces lignes commencent par le nom d'un "catalogue" - *collection*, un regroupement logique de fichiers défini par le serveur. Le nom du catalogue dit au serveur quels fichiers vous voulez. Ce nom est éventuellement suivi d'un ou plusieurs champs, séparés par un espace. Ces champs répondent aux questions listées ci-dessus. Il y deux types de champs: des indicateurs et des valeurs. Un indicateur est un mot-clé autonome, e.g., `delete` ou `compress`. Une valeur commence aussi par un mot-clé, mais il est impérativement suivi sans espace par un `=` et un deuxième mot. Par exemple, `release=cvs` est un champ définissant une valeur.

Un fichier supfile spécifie en général plus d'un catalogue à télécharger. Une façon de construire un fichier supfile consiste à préciser explicitement tous les champs nécessaires pour chaque catalogue. Cependant, cela tend à donner des fichiers supfile avec des lignes assez longues, et ce n'est pas très pratique parce que la plupart des champs sont les mêmes pour tous les catalogues du fichier supfile. CVSup fournit un mécanisme pour s'affranchir de ce problème. Les lignes qui commencent par le nom du pseudo-catalogue spécial `*default` servent à définir les indicateurs et les valeurs qui seront pris par défaut pour les catalogues listés ensuite dans le fichier supfile. Une valeur par défaut peut-être surchargée pour un catalogue particulier, en associant au catalogue lui-même une valeur différente. Les valeurs par défaut peuvent également être redéfinies, ou bien on peut en définir de nouvelles, en cours de fichier supfile, par de nouvelles lignes `*default`.

Sachant cela, nous allons maintenant mettre au point un fichier supfile pour télécharger et mettre à jour l'arborescence principale de FreeBSD-CURRENT.

- Quels fichiers voulez-vous télécharger?

  Les fichiers disponibles via CVSup sont regroupés par "catalogues" - *collections*. Les catalogues disponibles sont décrits dans la section suivante. Dans notre exemple, nous souhaitons recevoir toute l'arborescence principale du système FreeBSD. Il existe un unique gros catalogue `src-all` qui correspond à tout cela. Pour commencer à renseigner notre fichier supfile, nous listons simplement les catalogues, un par ligne (dans notre cas, une seule ligne):

  ```
  src-all
  ```

- Quelle(s) version(s) voulez-vous télécharger?

  Avec CVSup, vous pouvez obtenir pratiquement n'importe quelle version qui ait existé des sources. C'est possible parce que le serveur cvsupd travaille directement à partir du référentiel CVS, qui contient toutes les versions. Vous indiquez quelle version vous voulez en utilisant les valeurs `tag=` et `date=`.

  Faites très attention à définir correctement la valeur `tag=`. Certaines étiquettes ne s'appliquent qu'à certains catalogues. Si l'étiquette que vous donnez n'est pas valable ou mal orthographiée, CVSup effacera des fichiers que vous ne

> vouliez probablement pas supprimer. En particulier, n'utilisez *que* `tag=.` pour les catalogues `ports-*`.

Les valeurs données avec `tag=` sont des étiquettes symboliques définies dans le référentiel. Il y a deux sortes d'étiquettes, les étiquettes de révision et les étiquettes de branches. Les étiquettes de révision s'appliquent à une révision particulière. Leur signification ne varie pas d'un jour à l'autre. Les étiquettes de branches, à l'inverse, se rapportent à la dernière révision sur une branche particulière à un moment donné. Comme les étiquettes de branches ne se rapportent pas à une révision particulière, elles peuvent désigner demain quelque chose de différent de ce qu'elles référencent aujourd'hui.

Etiquettes CVS contient les étiquettes de branches qui peuvent intéresser les utilisateurs. Quand on spécifie une étiquette dans le fichier de configuration de CVSup, elle doit être précédée du champ `tag=` (`RELENG_4` deviendra `tag=RELENG_4`). Gardez à l'esprit que seule l'étiquette `tag=.` n'a de signification pour le catalogue des logiciels portés.

> Faites très attention à mentionner précisément l'étiquette exacte. CVSup ne sait différencier une étiquette valide d'une étiquette qui ne l'est pas. Si vous orthographiez mal l'étiquette, CVSup se comportera comme si vous aviez donné une étiquette valide qui ne se réfère à aucun fichier. Dans ce cas il supprimera toutes les sources que vous avez déjà.

Lorsque vous indiquez une étiquette de branche, vous recevez normalement les dernières versions des fichiers sur cette branche de développement. Si vous voulez récupérer des version antérieures, vous pouvez le faire en donnant une date avec le champ `date=`. La page de manuel de cvsup(1) vous expliquent comment le faire.

Dans notre exemple, nous désirons obtenir FreeBSD-CURRENT. Nous ajoutons alors la ligne suivante au début de notre fichier supfile:

```
*default tag=.
```

Il existe un cas particulier important qui se produit lorsque que l'on ne spécifie ni le champ `tag=` ni le champ `date=`. Dans ce cas, vous obtenez alors les fichiers RCS directement du référentiel CVS du serveur, plutôt que de recevoir une version donnée. Les développeurs préfèrent généralement cette façon de travailler. En maintenant une version du référentiel lui-même sur leur système, ils ont la possibilité de consulter l'historique des révisions et d'accéder aux versions antérieures des fichiers. Cet avantage ne s'obtient cependant qu'au prix d'une consommation importante d'espace disque.

- D'où voulez-vous les télécharger?

  Nous employons le champ `host=` pour dire à `cvsup` où récupérer ses mises à jour. N'importe quel des sites miroir CVSup fera l'affaire, bien que vous devriez essayer de choisir un site proche de vous. Dans cet exemple, nous utiliserons un site fictif de distribution de FreeBSD `cvsup99.FreeBSD.org`:

```
*default host=cvsup99.FreeBSD.org
```

Vous devrez changer le site pour un qui existe réellement avant d'exécuter CVSup. Lors de l'exécution de `cvsup`, vous pouvez surcharger cette définition sur la ligne de commande avec l'option `-h nom_de_machine`.

- Où voulez-vous les mettre sur votre machine?

  Le champ `prefix=` dit à `cvsup` où mettre les fichiers qu'il obtient. Dans l'exemple, nous mettrons les fichiers source directement dans notre arborescence des sources, /usr/src. Le répertoire src est déjà implicitement défini dans les catalogues que nous avons choisis de télécharger, voici donc la définition correcte:

  ```
  *default prefix=/usr
  ```

- Où `cvsup` doit-il mettre les fichiers d'état?

  Le client CVSup tient à jour des fichiers d'état dans ce qui est appelé le répertoire de "base". Ces fichiers permettent à CVSup de travailler plus efficacement en gardant la trace des modifications que vous avez déjà reçues. Nous utiliserons le répertoire de base standard, /var/db:

  ```
  *default base=/var/db
  ```

  Si votre répertoire de base n'existe pas encore, c'est le moment de le créer. Le client `cvsup` refusera de s'exécuter si le répertoire de base n'existe pas.

- Diverses autres options de configuration dans le fichier supfile:

  Il y a une autre ligne d'instruction qui doit normalement figurer dans le fichier supfile:

  ```
  *default release=cvs delete use-rel-suffix compress
  ```

  `release=cvs` dit au serveur d'obtenir les informations du référentiel principal de FreeBSD. C'est quasiment toujours le cas, mais il existe d'autres possibilités qui sortent du cadre du présent document.

  `delete` donne à CVSup l'autorisation de supprimer des fichiers. Vous devriez toujours utiliser cette possibilité, de sorte que CVSup puisse vraiment maintenir à jour votre arborescence des sources. CVSup veille à ne supprimer que les fichiers qu'il maintient. Les fichiers supplémentaires que vous pourriez avoir ne seront pas touchés.

  `use-rel-suffix` est... ésotérique. Si vous voulez vraiment savoir de quoi il retourne, lisez la page de manuel de cvsup(1). Sinon, mettez cet indicateur et ne vous en souciez pas plus.

  `compress` permet d'utiliser un algorithme de compression de type gzip(1) sur la ligne de

communication. Si votre connexion a la vitesse d'une ligne T1 ou plus, vous ne devriez probablement pas utiliser la compression. Sinon, cela facilite substantiellement les choses.

- Assembler les morceaux:

  Voici le fichier supfile de notre exemple en entier:

```
*default tag=.
*default host=cvsup99.FreeBSD.org
*default prefix=/usr
*default base=/var/db
*default release=cvs delete use-rel-suffix compress

src-all
```

A.5.3.1. Le fichier refuse

Comme mentionné ci-dessus, CVSup utilise une méthode de type *pull*. Fondamentalement, cela signifie que vous vous connectez au serveur CVSup, ce dernier dit, "Voici ce que vous pouvez télécharger...", puis votre client répond "Ok, je prendrai ceci, ceci, ceci et cela". Dans la configuration par défaut, le client CVSup téléchargera chaque fichier associé avec le catalogue et l'étiquette que vous avez choisi dans le fichier de configuration. Cependant cela ne correspond pas toujours à ce que vous désirez, tout particulièrement si vous mettez à jour les arborescences doc, ports, ou www - la plupart des personnes sont incapables de lire quatre ou cinq langues différentes, et donc elles n'ont pas besoin de télécharger les fichiers spécifiques à certaines langues. Si vous mettez à jour le catalogue des logiciels portés, vous pouvez remédier à cela en spécifiant chaque catalogue individuellement (e.g., *ports-astrology*, *ports-biology*, etc au lieu de spécifier simplement *ports-all*). Cependant puisque les arborescences doc et www ne disposent pas de catalogues spécifiques à chaque langue, vous devez utiliser une des nombreuses fonctions de CVSup: le fichier refuse.

Le fichier refuse indique essentiellement à CVSup qu'il ne doit pas télécharger chaque fichier d'un catalogue; en d'autre termes, il dit au client de *refuser* certains fichiers du serveur. Le fichier refuse peut être trouvé (ou, si vous n'en disposez pas encore d'un, doit être placé) dans base/sup/. *base* est défini dans votre supfile; notre répertoire *base* est défini en tant que /var/db ce qui signifie que le fichier refuse est par défaut /var/db/sup/refuse.

Le fichier refuse a un format très simple; il contient tout simplement les noms des fichiers ou des répertoires que vous ne désirez pas rapatrier. Par exemple, si vous ne pouvez parler d'autres langues que l'anglais ou un peu d'allemand, et vous ne ressentez pas le besoin de lire la traduction en allemand de la documentation, vous pouvez mettre ce qui suit dans le fichier refuse:

```
doc/bn_*
doc/da_*
doc/de_*
doc/el_*
doc/es_*
doc/fr_*
```

```
doc/it_*
doc/ja_*
doc/nl_*
doc/no_*
doc/pl_*
doc/pt_*
doc/ru_*
doc/sr_*
doc/tr_*
doc/zh_*
```

et ainsi de suite pour les autres langues (vous pouvez en trouver une liste complète en parcourant le référentiel CVS de FreeBSD).

Avec cette fonction très utile, les utilisateurs disposant d'une connexion lente ou payant le temps de connexion à la minute seront en mesure d'économiser de précieuses minutes comme ils n'auront plus du tout besoin de télécharger des fichiers qu'ils n'utiliseront jamais. Pour plus d'information sur les fichiers refuse et d'autres caractéristiques intéressantes de CVSup, consultez sa page de manuel.

A.5.4. Exécuter CVSup

Vous êtes maintenant prêt à essayer de faire une mise à jour. La ligne de commande à utiliser est très simple:

```
# cvsup supfile
```

où supfile est bien sûr le nom du fichier supfile que vous venez de créer. Si vous êtes sous X11, `cvsup` affichera une interface graphique avec des boutons pour les opérations courantes. Appuyez sur le bouton btn[go] et suivez le déroulement des opérations.

Comme, dans cet l'exemple, vous mettez directement à jour votre arborescence /usr/src, vous devrez exécuter le programme en tant que `root` de façon à ce que `cvsup` ait le droit de mettre à jour vos fichiers. Comme vous venez juste de créer votre fichier de configuration et n'avez encore jamais utilisé le programme, il est compréhensible que cela vous rende nerveux. Il est facile de faire un essai sans toucher à vos précieux fichiers. Créez juste un nouveau répertoire quelque part et donnez-le en argument supplémentaire sur la ligne de commande:

```
# mkdir /var/tmp/dest
# cvsup supfile /var/tmp/dest
```

Le répertoire indiqué sera pris comme destination pour tous les fichiers modifiés. CVSup examinera les fichiers habituels dans /usr/src, mais ne les modifiera pas et n'en supprimera aucun. Les modifications atterriront dans /var/tmp/dest/usr/src. CVSup ne touchera pas non plus à ses fichiers d'état dans le répertoire de base, lorsqu'il est invoqué de cette manière. Les nouvelles versions de ces fichiers iront dans le répertoire indiqué. A partir du moment où vous avez les les droits en lecture sur /usr/src, vous n'avez pas besoin d'être `root` pour faire ce genre d'essai.

Si vous n'êtes pas sous X11, ou si vous n'aimez tout simplement pas les interfaces graphiques, vous devrez ajouter quelques options supplémentaires sur la ligne de commande de `cvsup`:

```
# cvsup -g -L 2 supfile
```

L'option `-g` dit à CVSup de ne pas utiliser son interface graphique. C'est automatique si vous n'êtes pas sous X11, sinon vous devez le préciser.

L'option`-L 2` dit à CVSup d'afficher le détail de ce qu'il est en train de faire. Il y a trois niveaux de trace, de `-L 0` à `-L 2`. La valeur par défaut est de 0, ce qui équivaut à n'émettre que les messages d'erreur.

Il y a de nombreuses autres option disponibles. Pour en obtenir un résumé, tapez `cvsup -H`. Pour une description plus détaillée, reportez-vous aux pages de manuel.

Une fois que vous êtes satisfait de la façon dont se passent les mises à jour, vous pouvez mettre en place une exécution de CVSup à intervalles réguliers en utilisant cron(8). Bien évidemment, vous ne devez pas laisser CVSup utiliser don interface graphique quand vous le lancez depuis cron(8).

A.5.5. Catalogue de fichiers CVSup

Les catalogues de fichiers disponibles via CVSup sont organisés hiérarchiquement. Il y a quelques gros catalogues, qui sont divisés en plus petits sous-catalogues. Recevoir un gros catalogue équivaut à recevoir chacun de ces sous-catalogues. Les relations hiérarchiques entre les sous-catalogues sont décrites par les indentations dans la liste ci-dessous.

Les catalogues habituellement les plus employés sont `src-all`, et `ports-all`. Les autres catalogues ne sont utilisés que par de petits groupes de personnes pour des besoins particuliers, et certains sites miroir ne les mettent pas à disposition.

`cvs-all release=cvs`
: Le référentiel CVS principal de FreeBSD, incluant les logiciels de chiffrement.

`distrib release=cvs`
: Les fichiers ayant trait à la distribution et à la mise en place de sites miroir FreeBSD.

`doc-all release=cvs`
: Les sources du manuel FreeBSD et d'autres documentations. Cela de comprend pas les fichiers pour le site Web de FreeBSD.

`ports-all release=cvs`
: Le catalogue des logiciels portés de FreeBSD.

Si vous ne voulez pas mettre à jour l'intégralité du catalogue `ports-all` (l'intégralité du catalogue des logiciels portés), mais utiliser un des sous-catalogues listés ci-dessous, assurez-vous de *toujours* mettre à jour le sous-catalogue `ports-base`! Dès qu'il y a un changement dans l'infrastructure de compilation des logiciels portés représentée par `ports-base`, il est certain que

ces changements seront utilisés par un logiciel porté très rapidement. Donc, si vous ne mettez à jour que les logiciels portés en tant que tel et qu'ils utilisent certains des changements, il y a de grandes chances pour que leur compilation échoue avec de mystérieux messages d'erreur. La *première* chose à faire dans ce cas est de vérifier que votre sous-catalogue `ports-base` est à jour.

Si vous voulez construire votre propre version locale du fichier ports/INDEX, vous *devez* accepter le catalogue `ports-all` (l'intégralité du catalogue des logiciels portés). La construction de ports/INDEX avec une arborescence partielle n'est pas supportée. Consultez la FAQ.

`ports-accessibility release=cvs`

Logiciels pour utilisateurs handicapées.

`ports-arabic release=cvs`

Support pour l'arabe.

`ports-archivers release=cvs`

Outils d'archivage.

`ports-astro release=cvs`

Logiciels d'astronomie.

`ports-audio release=cvs`

Support du son.

`ports-base release=cvs`

L'infrastructure de compilation du catalogue des logiciels portés - divers fichiers situés dans les répertoires Mk/ et Tools/ sous-répertoires de la hiérarchie /usr/ports.

Lisez l'important avertissement ci-dessus: vous devriez *toujours* mettre à jour ce sous-catalogue, dès que vous mettez à jour une partie du catalogue des logiciels portés de FreeBSD!

`ports-benchmarks release=cvs`

Evaluation de performances.

`ports-biology release=cvs`

Biologie.

`ports-cad release=cvs`

Outils de conception assistée par ordinateur.

`ports-chinese release=cvs`

Support pour le chinois.

`ports-comms release=cvs`
: Logiciels de communication.

`ports-converters release=cvs`
: Conversion entre codages de caratères.

`ports-databases release=cvs`
: Bases de données.

`ports-deskutils release=cvs`
: Les choses que l'on trouvait sur un bureau avant l'invention des ordinateurs.

`ports-devel release=cvs`
: Outils de développement.

`ports-dns release=cvs`
: Logiciels relatifs au DNS.

`ports-editors release=cvs`
: Editeurs.

`ports-emulators release=cvs`
: Emulateurs d'autres systèmes d'exploitation.

`ports-finance release=cvs`
: Applications concernant les finances et l'argent.

`ports-ftp release=cvs`
: Clients et serveurs FTP.

`ports-games release=cvs`
: Jeux.

`ports-german release=cvs`
: Support pour l'allemand.

`ports-graphics release=cvs`
: Outils graphiques.

`ports-hebrew release=cvs`
: Support de l'hébreu.

`ports-hungarian release=cvs`
: Support du hongrois.

`ports-irc release=cvs`
: Outils pour l'IRC.

`ports-japanese release=cvs`
: Support pour le japonais.

`ports-java release=cvs`
: Outils Java™.

`ports-korean release=cvs`
: Support pour le coréen.

`ports-lang release=cvs`
: Langages de programmation.

`ports-mail release=cvs`
: Logiciels de courrier électronique.

`ports-math release=cvs`
: Logiciels de calcul numérique.

`ports-mbone release=cvs`
: Applications MBone.

`ports-misc release=cvs`
: Utilitaires divers.

`ports-multimedia release=cvs`
: Logiciels pour le multimedia.

`ports-net release=cvs`
: Logiciels réseau.

`ports-net-im release=cvs`
: Logiciels de messagerie instantanée.

`ports-net-mgmt release=cvs`
: Logiciels de gestion des réseaux.

`ports-net-p2p release=cvs`
: Logiciels pour le "peer to peer".

`ports-news release=cvs`
: Logiciels pour les forums de discussion USENET.

`ports-palm release=cvs`
: Logiciels de support des machines Palm™.

`ports-polish release=cvs`
: Support pour le polonais.

`ports-ports-mgmt release=cvs`

Utilitaires pour la gestion des logiciels portés et des paquetages.

`ports-portuguese release=cvs`

Support pour le portugais.

`ports-print release=cvs`

Logiciels d'impression.

`ports-russian release=cvs`

Support pour le russe.

`ports-science release=cvs`

Science.

`ports-security release=cvs`

Outils de sécurité.

`ports-shells release=cvs`

Interpréteurs de commandes.

`ports-sysutils release=cvs`

Utilitaires système.

`ports-textproc release=cvs`

Outils de traitement de texte (sauf les logiciels de publication assistée par ordinateur).

`ports-ukrainian release=cvs`

Support de l'ukrainien.

`ports-vietnamese release=cvs`

Support du vietnamien.

`ports-www release=cvs`

Logiciels concernant le World Wide Web.

`ports-x11 release=cvs`

Logiciel pour le système X window.

`ports-x11-clocks release=cvs`

Horloges pour X11.

`ports-x11-drivers release=cvs`

pilotes de périphérique X11.

`ports-x11-fm release=cvs`

Gestionnaires de fichiers pour X11.

`ports-x11-fonts release=cvs`
: Polices de caractères et outils associés pour X11.

`ports-x11-toolkits release=cvs`
: "Toolkits" X11.

`ports-x11-servers release=cvs`
: Serveurs X11.

`ports-x11-themes release=cvs`
: Thèmes X11.

`ports-x11-wm release=cvs`
: Gestionnaires de fenêtres pour X11.

`projects-all release=cvs`
: Les sources présentes dans le dépots des projets FreeBSD.

`src-all release=cvs`
: Les sources du système FreeBSD, comprenant les logiciels de chiffrement.

`src-base release=cvs`
: Divers fichiers en haut de la hiérarchie /usr/src.

`src-bin release=cvs`
: Programmes utilisateurs qui peuvent être utiles en mode mono-utilisateur (/usr/src/bin).

`src-cddl release=cvs`
: Utilitaires et bibliothèques sous licence CDDL (/usr/src/cddl).

`src-contrib release=cvs`
: Utilitaires et bibliothèques d'origine indépendante du projet FreeBSD, employés à peu près tels quels (/usr/src/contrib).

`src-crypto release=cvs`
: Utilitaires et bibliothèques pour le chiffrement d'origine indépendante du projet FreeBSD, employés à peu près tels quels (/usr/src/crypto).

`src-eBones release=cvs`
: Kerberos et DES (/usr/src/eBones). Non utilisés dans les versions de FreeBSD actuellement publiées.

`src-etc release=cvs`
: Fichiers de configuration du système (/usr/src/etc).

`src-games release=cvs`
: Jeux (/usr/src/games).

`src-gnu release=cvs`

Utilitaires soumis à la licence publique GNU (/usr/src/gnu).

`src-include release=cvs`

Fichiers d'entête (/usr/src/include).

`src-kerberos5 release=cvs`

Logiciel de sécurité Kerberos5 (/usr/src/kerberos5).

`src-kerberosIV release=cvs`

Logiciel de sécurité KerberosIV (/usr/src/kerberosIV).

`src-lib release=cvs`

Bibliothèques (/usr/src/lib).

`src-libexec release=cvs`

Programmes système normalement exécutés par d'autres programmes (/usr/src/libexec).

`src-release release=cvs`

Fichiers nécessaires à la génération d'une version publiable de FreeBSD (/usr/src/release).

`src-rescue release=cvs`

Programmes liés en statique pour les dépannages d'urgence; consultez la page de manuel rescue(8) (/usr/src/rescue).

`src-sbin release=cvs`

Utilitaires système pour le mode mono-utilisateur (/usr/src/sbin).

`src-secure release=cvs`

Commandes et bibliothèques pour le chiffrage (/usr/src/secure).

`src-share release=cvs`

Fichiers qui peuvent être partagés par plusieurs systèmes (/usr/src/share).

`src-sys release=cvs`

Le noyau (/usr/src/sys).

`src-sys-crypto release=cvs`

Code du noyau destiné au chiffrement (/usr/src/sys/crypto).

`src-tools release=cvs`

Divers outils pour la maintenance de FreeBSD (/usr/src/tools).

`src-usrbin release=cvs`

Outils utilisateur (/usr/src/usr.bin).

`src-usrsbin release=cvs`

Utilitaires système (/usr/src/usr.sbin).

`www release=cvs`
: Les sources du site WWW de FreeBSD.

`distrib release=self`
: Fichiers de configuration du serveur CVSup. Utilisés par les sites miroir CVSup.

`gnats release=current`
: Base de données GNATS d'historique des bogues.

`mail-archive release=current`
: Archives des listes de diffusion FreeBSD.

`www release=current`
: Les fichiers/données WWW publiés (pas les fichiers source). Utilisés par les sites miroir WWW.

A.5.6. Pour plus d'informations

Pour la FAQ de CVSup et d'autres informations concernant CVSup, consultez la page Web de CVSup.

La plupart des discussions relatives à l'utilisation de CVSup sous FreeBSD ont lieu sur la liste de diffusion pour les discussions techniques sur FreeBSD. Les nouvelles versions du logiciel y sont annoncés ainsi que sur la liste de diffusion pour les annonces relatives à FreeBSD.

Pour toutes les questions et rapports de bogues concernant CVSup, consultez la FAQ CVSup.

A.5.7. Sites CVSup

Des serveurs CVSup pour FreeBSD fonctionnent aux sites suivants:

A.6. Utiliser Portsnap

A.6.1. Introduction

Portsnap est un système de distribution sécurisée du catalogue des logiciels portés de FreeBSD. Approximativement chaque heure, un "instantané" du catalogue des logiciels portés est généré, rassemblé et signé de manière chiffrée. Les fichiers résultants sont alors distribués par l'intermédiaire du protocole HTTP.

Tout comme CVSup, Portsnap utilise un modèle de mise à jour de type *pull*: le catalogue des logiciels portés packagé et signé est placé sur un serveur Web qui attend les requêtes des clients. Les utilisateurs doivent soit exécuter manuellement portsnap(8) pour télécharger les mises à jour, soit configurer cron(8) pour un téléchargement régulier et automatique des mises à jour.

Pour des raisons techniques, Portsnap ne met pas à jour le catalogue des logiciels portés directement dans le répertoire /usr/ports; le logiciel travaille plutôt par défaut sur une version compressée de l'arborescence des logiciels portés dans le répertoire /var/db/portsnap. Cette copie compressée est ensuite utilisée pour mettre à jour le catalogue des logiciels portés.

Si Portsnap est installé à partir du catalogue des logiciels portés de FreeBSD, alors l'emplacement par défaut pour son instantané compressé sera /usr/local/portsnap au lieu de /var/db/portsnap.

A.6.2. Installation

Sous FreeBSD 6.0 et les versions plus récentes, Portsnap fait partie du système de base de FreeBSD. Sous des versions plus anciennes de FreeBSD, il peut être installé à partir du logiciel porté ports-mgmt/portsnap.

A.6.3. Configuration de Portsnap

L'exécution de Portsnap est contrôlée par le fichier de configuration /etc/portsnap.conf. Pour la plupart des utilisateurs, le fichier de configuration par défaut sera suffisant; pour plus de détails, consultez la page de manuel portsnap.conf(5).

Si Portsnap est installé à partir du catalogue des logiciels portés, il utilisera /usr/local/etc/portsnap.conf comme fichier de configuration au lieu de /etc/portsnap.conf. Ce fichier n'est pas créé lors de l'installation du logiciel, mais un fichier d'exemple est fourni; pour le copier à son emplacement correct, utilisez la commande suivante:

```
# cd /usr/local/etc  cp portsnap.conf.sample portsnap.conf
```

A.6.4. Exécuter Portsnap pour la première fois

Au premier lancement de la commande portsnap(8), il sera nécessaire de télécharger un instantané compressé de l'intégralité de l'arborescence des logiciels portés dans /var/db/portsnap (ou /usr/local/portsnap si Portsnap a été installé à partir du catalogue des logiciels portés). Au début de l'année 2006, cela représentait un téléchargement d'environ 41 Mo.

```
# portsnap fetch
```

Une fois que l'instantané compressé a été récupéré, une copie utilisable de l'arborescence des logiciels portés peut être extraite dans le répertoire /usr/ports. Cela est nécessaire même si une arborescence a déjà été créée dans ce répertoire (par exemple en utilisant CVSup), puisque cela met en place une version de référence à partir de laquelle `portsnap` peut déterminer plus tard quelles parties du catalogue des logiciels portés a besoin d'une mise à jour.

```
# portsnap extract
```

Dans l'installation par défaut de FreeBSD /usr/ports n'est pas créé. Si vous utilisez FreeBSD 6.0-RELEASE, ce répertoire doit être créé avant d'utiliser la commande `portsnap`. Sur les versions de FreeBSD plus récentes ou de Portsnap, cette création

est effectuée automatiquement à la premiere utilisation de la commande `portsnap`.

A.6.5. Mettre à jour l'arborescence des logiciels portés

Après qu'un instantané initial du catalogue des logiciels portés ait été récupéré puis décompressé dans le répertoire /usr/ports, la mise à jour du catalogue se divise en deux étapes: la récupération (*fetch*) des mises à jour de l'instantané, et leur utilisation pour mettre à jour (*update*) le catalogue des logiciels portés en tant que tel. Ces deux étapes peuvent être effectuées par l'intermédiaire d'une seule commande `portsnap`:

```
# portsnap fetch update
```

Des versions anciennes de `portsnap` ne supporte pas cette syntaxe; en cas d'échec, utilisez à la place ceci:

```
# portsnap fetch
# portsnap update
```

A.6.6. Exécuter Portsnap à partir de cron

Afin d'éviter tout problème "d'embouteillage" lors de l'accès aux serveurs Portsnap, `portsnap fetch` ne fonctionnera pas à partir d'une tâche cron(8). Il existe, à la place, une commande `portsnap cron` spécifique, qui patiente durant un délai aléatoire pouvant aller jusqu'à 3600 secondes avant de récupérer les mises à jour.

De plus, il est fortement recommandé de ne pas exécuter `portsnap update` à partir d'une tâche `cron`, puisque cela peut être à l'origine de graves problèmes si la commande a lieu au même moment qu'un logiciel porté est en train d'être compilé ou installé. Cependant, les fichiers INDEX peuvent être mis à jour sans risque, et cela peut être fait en passant l'indicateur `-I` à la commande `portsnap` (bien entendu si `portsnap -I update` est exécuté à par `cron`, il sera alors nécessaire de lancer `portsnap update` sans l'option `-I` ultérieurement pour mettre à jour le reste de l'arborescence).

L'ajout de la ligne suivante dans le fichier /etc/crontab demandera à `portsnap` de mettre à jour son instantané compressé et les fichiers INDEX du répertoire /usr/ports, et enverra un courrier électronique si un logiciel porté installé n'est pas à jour:

```
0 3 * * * root portsnap -I cron update  pkg_version -vIL=
```

Si l'horloge système n'est pas positionnée sur le fuseau horaire local, remplacez `3` par une valeur quelconque comprise entre 0 et 23, afin de répartir de manière plus équilibrée la charge sur les serveurs Portsnap.

Des versions anciennes de `portsnap` ne supportent pas l'utilisation de commandes multiples (par exemple `cron update`) lors de la même invocation de `portsnap`. Si la

ligne précédente échoue, essayez de remplacer `portsnap -I cron update` par `portsnap cron portsnap -I update`.

A.7. Etiquettes CVS

Quand on récupère ou l'on met à jour les sources en utilisant cvs ou CVSup, une étiquette de révision doit être spécifiée. Une étiquette de révision fait référence soit à une branche particulière de développement de FreeBSD, soit à un moment particulier dans le temps. Le premier type d'étiquette est nommé "étiquette de branche", le second type "étiquette de publication" - *release tags*.

A.7.1. Etiquettes de branche

Toutes ces étiquettes, à l'exception de l'étiquette `HEAD` (qui est une étiquette toujours valide), ne s'appliquent qu'à l'arborescence src/. Il n'y a pas de branche pour les arborescences ports/, doc/, et www/.

HEAD

Nom symbolique pour la branche principale de développement, ou FreeBSD-CURRENT. C'est aussi la valeur par défaut lorsque la révision n'est pas précisée.

Sous CVSup, cette étiquette est représentée par un `.` (ce n'est pas une ponctuation, mais bien le caractère `.`).

Sous CVS, c'est la valeur par défaut quand aucune étiquette de révision n'est précisée. Ce n'est généralement *pas* une bonne idée de récupérer ou mettre à jour vers les sources CURRENT sur une machine STABLE, à moins que cela ne soit vraiment votre intention.

RELENG_6

Branche de développement pour FreeBSD-6.X, également connue sous le nom de FreeBSD 6-STABLE.

RELENG_6_2

Branche de publication de la version FreeBSD-6.2, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_6_1

Branche de publication de la version FreeBSD-6.1, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_6_0

Branche de publication de la version FreeBSD-6.0, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_5

Branche de développement pour FreeBSD-5.X, également connue sous le nom de FreeBSD 5-

STABLE.

RELENG_5_5

Branche de publication de la version FreeBSD-5.5, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_5_4

Branche de publication de la version FreeBSD-5.4, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_5_3

Branche de publication de la version FreeBSD-5.3, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_5_2

Branche de publication des versions FreeBSD-5.2 et FreeBSD-5.2.1, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_5_1

Branche de publication de la version FreeBSD-5.1, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_5_0

Branche de publication de la version FreeBSD-5.0, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_4

Branche de développement de FreeBSD-4.X, aussi connue sous le nom de FreeBSD 4-STABLE.

RELENG_4_11

Branche de publication de la version FreeBSD-4.11, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_4_10

Branche de publication de la version FreeBSD-4.10, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_4_9

Branche de publication de la version FreeBSD-4.9, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_4_8

Branche de publication de la version FreeBSD-4.8, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_4_7

Branche de publication de la version FreeBSD-4.7, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_4_6

Branche de publication des versions FreeBSD-4.6 et FreeBSD-4.6.2, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_4_5

Branche de publication de la version FreeBSD-4.5, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_4_4

Branche de publication de la version FreeBSD-4.4, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_4_3

Branche de publication de la version FreeBSD-4.3, utilisée uniquement pour les avis de sécurité et autres correctifs de problèmes critiques.

RELENG_3

Branche de développement de FreeBSD-3.X, aussi connue sous le nom de 3.X-STABLE.

RELENG_2_2

Branche de développement de FreeBSD-2.2.X, aussi connue sous le nom de 2.2-STABLE. Cette branche est en grande partie obsolète.

A.7.2. Etiquettes de publication

Ces étiquettes font référence à un moment bien précis dans le temps quand une version particulière de FreeBSD a été publiée. Le processus d'ingénierie des publications est documenté en détails dans les documents Information sur la publication des versions et Processus de publication. L'arborescence src utilise des étiquettes commençant par `RELENG_`. Les arborescences ports et doc utilisent des étiquettes dont les noms commencent par `RELEASE`. Enfin, l'arborescence www ne bénéficie pas d'étiquette particulière pour les publications.

RELENG_6_2_0_RELEASE

FreeBSD 6.2

RELENG_6_1_0_RELEASE

FreeBSD 6.1

RELENG_6_0_0_RELEASE

FreeBSD 6.0

RELENG_5_5_0_RELEASE

FreeBSD 5.5

RELENG_5_4_0_RELEASE

FreeBSD 5.4

RELENG_4_11_0_RELEASE
: FreeBSD 4.11

RELENG_5_3_0_RELEASE
: FreeBSD 5.3

RELENG_4_10_0_RELEASE
: FreeBSD 4.10

RELENG_5_2_1_RELEASE
: FreeBSD 5.2.1

RELENG_5_2_0_RELEASE
: FreeBSD 5.2

RELENG_4_9_0_RELEASE
: FreeBSD 4.9

RELENG_5_1_0_RELEASE
: FreeBSD 5.1

RELENG_4_8_0_RELEASE
: FreeBSD 4.8

RELENG_5_0_0_RELEASE
: FreeBSD 5.0

RELENG_4_7_0_RELEASE
: FreeBSD 4.7

RELENG_4_6_2_RELEASE
: FreeBSD 4.6.2

RELENG_4_6_1_RELEASE
: FreeBSD 4.6.1

RELENG_4_6_0_RELEASE
: FreeBSD 4.6

RELENG_4_5_0_RELEASE
: FreeBSD 4.5

RELENG_4_4_0_RELEASE
: FreeBSD 4.4

RELENG_4_3_0_RELEASE
: FreeBSD 4.3

RELENG_4_2_0_RELEASE
: FreeBSD 4.2

RELENG_4_1_1_RELEASE
: FreeBSD 4.1.1

RELENG_4_1_0_RELEASE
: FreeBSD 4.1

RELENG_4_0_0_RELEASE
: FreeBSD 4.0

RELENG_3_5_0_RELEASE
: FreeBSD-3.5

RELENG_3_4_0_RELEASE
: FreeBSD-3.4

RELENG_3_3_0_RELEASE
: FreeBSD-3.3

RELENG_3_2_0_RELEASE
: FreeBSD-3.2

RELENG_3_1_0_RELEASE
: FreeBSD-3.1

RELENG_3_0_0_RELEASE
: FreeBSD-3.0

RELENG_2_2_8_RELEASE
: FreeBSD-2.2.8

RELENG_2_2_7_RELEASE
: FreeBSD-2.2.7

RELENG_2_2_6_RELEASE
: FreeBSD-2.2.6

RELENG_2_2_5_RELEASE
: FreeBSD-2.2.5

RELENG_2_2_2_RELEASE
: FreeBSD-2.2.2

RELENG_2_2_1_RELEASE
: FreeBSD-2.2.1

RELENG_2_2_0_RELEASE

FreeBSD-2.2.0

A.8. Sites AFS

Il y a des serveurs AFS pour FreeBSD sur les sites suivants:

Suède

Le chemin d'accès au fichiers est /afs/stacken.kth.se/ftp/pub/FreeBSD/

```
stacken.kth.se          # Stacken Computer Club, KTH, Suède
130.237.234.43          #hot.stacken.kth.se
130.237.237.230         #fishburger.stacken.kth.se
130.237.234.3           #milko.stacken.kth.se
```

Responsable ftp@stacken.kth.se

A.9. Sites rsync

Les sites suivants fournissent FreeBSD en utilisant le protocole rsync. L'utilitaire rsync fonctionne globalement de la même manière que la commande rcp(1), mais il dispose de plus d'options et utilise le protocole de mise à jour à distance rsync qui ne transfert que les différences entre deux ensembles de fichiers, ce qui accélère énormément la synchronisation par le réseau. C'est surtout utile si vous disposez d'un miroir du serveur FTP de FreeBSD, ou du référentiel CVS. La suite rsync est disponible sur de nombreux systèmes d'exploitation, et sous FreeBSD, voir le logiciel porté net/rsync ou utilisez la version pré-compilée.

République Tchèque

rsync://ftp.cz.FreeBSD.org/

Collections disponibles:

- ftp: un miroir partiel du serveur FTP FreeBSD.
- FreeBSD: un miroir complet du serveur FTP FreeBSD.

Allemagne

rsync://grappa.unix-ag.uni-kl.de/

Collections disponibles:

- freebsd-cvs: référentiel CVS FreeBSD complet.

Cette machine est également miroir des référentiels CVS des projets NetBSD et OpenBSD, parmi d'autres.

Hollande

rsync://ftp.nl.FreeBSD.org/

Collections disponibles:

- vol/4/freebsd-core: un miroir complet du serveur FTP FreeBSD.

Thailande

rsync://ftp.tw.FreeBSD.org/

rsync://ftp2.tw.FreeBSD.org/

rsync://ftp6.tw.FreeBSD.org/

Collections disponibles:

- FreeBSD: Un miroir complet du serveur FTP FreeBSD.

Royaume-Uni

rsync://rsync.mirror.ac.uk/

Collections disponibles:

- ftp.freebsd.org: Un miroir complet du serveur FTP FreeBSD.

Etats Unis d'Amérique

rsync://ftp-master.FreeBSD.org/

Ce serveur ne pourra être utilisé que par les sites miroirs primaires FreeBSD.

Collections disponibles:

- FreeBSD: l'archive principale du serveur FTP FreeBSD.
- acl: la liste principale ACL de FreeBSD.

  rsync://ftp13.FreeBSD.org/

  Collections disponibles:

- FreeBSD: Un miroir complet du serveur FTP FreeBSD.

Annexe B: Bibliographie

Bien que les pages de manuel soient la documentation de référence pour chaque facette du système d'exploitation FreeBSD, il est de notoriété publique qu'elles n'expliquent pas comment assembler les morceaux pour avoir un système d'exploitation qui tourne sans encombre. Il n'y a pour cela pas d'autre alternative qu'un bon livre sur l'administration UNIX® et un bon manuel utilisateur.

B.1. Livres magazines consacrés à FreeBSD

Livres revues internationaux:

- Utiliser FreeBSD (en chinois traditionnel), publié par Drmaster., 1997. ISBN 9-578-39435-7.
- FreeBSD Unleashed (traduction en chinois simplifié), publié par China Machine Press. ISBN 7-111-10201-0.
- FreeBSD From Scratch First Edition (en chinois simplifié), publié par China Machine Press. ISBN 7-111-07482-3.
- FreeBSD From Scratch Second Edition (en chinois simplifié), publié par China Machine Press. ISBN 7-111-10286-X.
- Manuel FreeBSD (traduction en chinois simplifié), publié par Posts Telecom Press. ISBN 7-115-10541-3.
- FreeBSD 3.x Internet (en chinois simplifié), publié par Tsinghua University Press. ISBN 7-900625-66-6.
- FreeBSD Windows (en chinois simplifié), ISBN 7-113-03845-X
- FreeBSD Internet Services HOWTO (en chinois simplifié), ISBN 7-113-03423-3
- FreeBSD pour les utilisateurs de PC 98 (en Japonais), publié par SHUWA System Co, LTD. ISBN 4-87966-468-5 C3055 P2900E.
- FreeBSD (en Japonais), publié par CUTT. ISBN 4-906391-22-2 C3055 P2400E.
- Introduction complète à FreeBSD (en Japonais), publié par Shoeisha Co., Ltd. ISBN 4-88135-473-6 P3600E.
- Kit de démarrage pour Unix personnel FreeBSD (en Japonais), publié par ASCII. ISBN 4-7561-1733-3 P3000E.
- Manuel de référence FreeBSD (traduction en Japonais), publié par ASCII. ISBN 4-7561-1580-2 P3800E.
- FreeBSD avec méthode (en Allemand), publié par Computer und Literatur Verlag/Vertrieb Hanser, 1998. ISBN 3-932311-31-0.
- FreeBSD 4 - Installieren, Konfigurieren, Administrieren (en Allemand), publié par Computer und Literatur Verlag, 2001. ISBN 3-932311-88-4.
- FreeBSD 5 - Installieren, Konfigurieren, Administrieren (en Allemand), publié par Computer und Literatur Verlag, 2003. ISBN 3-936546-06-1.
- FreeBSD de Luxe (en Allemand), publié par Verlag Modere Industrie, 2003. ISBN 3-8266-1343-0.

- Manuel d'installation et d'utilisation de FreeBSD (en Japonais), publié par Mainichi Communications Inc., 1998. ISBN 4-8399-0112-0.
- Onno W Purbo, Dodi Maryanto, Syahrial Hubbany, Widjil Widodo *Construire un serveur Internet avec FreeBSD* (en Indonésien), publié par Elex Media Komputindo.
- Absolute BSD: The Ultimate Guide to FreeBSD (traduction en chinois traditionnel), publié par GrandTech Press, 2003. ISBN 986-7944-92-5.
- The FreeBSD 6.0 Book (en chinois traditionnel), publié par Drmaster, 2006. ISBN 9-575-27878-X.

Livres revues en langue anglaise:

- Absolute BSD: The Ultimate Guide to FreeBSD, publié par No Starch Press, 2002. ISBN: 1886411743
- The Complete FreeBSD, publié par O'Reilly, 2003. ISBN: 0596005164
- The FreeBSD Corporate Networker's Guide, publié par Addison-Wesley, 2000. ISBN: 0201704811
- FreeBSD: An Open-Source Operating System for Your Personal Computer, publié par The Bit Tree Press, 2001. ISBN: 0971204500
- Teach Yourself FreeBSD in 24 Hours, publié par Sams, 2002. ISBN: 0672324245
- FreeBSD unleashed, publié par Sams, 2006. ISBN: 0672328755
- FreeBSD: The Complete Reference, publié McGrawHill, 2003. ISBN: 0072224096

B.2. Manuels d'utilisation

- Computer Systems Research Group, UC Berkeley. *4.4BSD User's Reference Manual*. O'Reilly Associates, Inc., 1994. ISBN 1-56592-075-9
- Computer Systems Research Group, UC Berkeley. *4.4BSD User's Supplementary Documents*. O'Reilly Associates, Inc., 1994. ISBN 1-56592-076-7
- *UNIX in a Nutshell*. O'Reilly Associates, Inc., 1990. ISBN 093717520X
- Mui, Linda. *What You Need To Know When You Can't Find Your UNIX System Administrator*. O'Reilly Associates, Inc., 1995. ISBN 1-56592-104-6
- L'Université de l'Etat d'Ohio a écrit un Cours d'introduction à Unix qui est disponible en ligne aux formats HTML et PostScript.

  Une version en Italien de ce document fait partie du projet de documentation FreeBSD Italien.

- Jpman Project, Groupe d'utilisateurs japonais de FreeBSD. Manuel de référence utilisateur de FreeBSD (traduction en Japonais). Mainichi Communications Inc., 1998. ISBN4-8399-0088-4 P3800E.
- L'Université d'Edinburgh a écrit un Guide en ligne pour les nouveaux venus à l'environnement Unix.

B.3. Manuels d'administration

- Albitz, Paul and Liu, Cricket. *DNS and BIND*, 4th Ed. O'Reilly Associates, Inc., 2001. ISBN 1-59600-158-4
- Computer Systems Research Group, UC Berkeley. *4.4BSD System Manager's Manual*. O'Reilly Associates, Inc., 1994. ISBN 1-56592-080-5
- Costales, Brian, et al. *Sendmail*, 2nd Ed. O'Reilly Associates, Inc., 1997. ISBN 1-56592-222-0
- Frisch, Æleen. *Essential System Administration*, 2nd Ed. O'Reilly Associates, Inc., 1995. ISBN 1-56592-127-5
- Hunt, Craig. *TCP/IP Network Administration*, 2nd Ed. O'Reilly Associates, Inc., 1997. ISBN 1-56592-322-7
- Nemeth, Evi. *UNIX System Administration Handbook*. 3rd Ed. Prentice Hall, 2000. ISBN 0-13-020601-6
- Stern, Hal *Managing NFS and NIS* O'Reilly Associates, Inc., 1991. ISBN 0-937175-75-7
- Jpman Project, Groupe d'utilisateurs japonais de FreeBSD. Manuel de l'administrateur système FreeBSD (traduction en Japonais). Mainichi Communications Inc., 1998. ISBN4-8399-0109-0 P3300E.
- Dreyfus, Emmanuel. Cahiers de l'Admin: BSD 2nde Ed. (en Français), Eyrolles, 2004. ISBN 2-212-11463-X

B.4. Manuels de programmation

- Asente, Paul, Converse, Diana, and Swick, Ralph. *X Window System Toolkit*. Digital Press, 1998. ISBN 1-55558-178-1
- Computer Systems Research Group, UC Berkeley. *4.4BSD Programmer's Reference Manual*. O'Reilly Associates, Inc., 1994. ISBN 1-56592-078-3
- Computer Systems Research Group, UC Berkeley. *4.4BSD Programmer's Supplementary Documents*. O'Reilly Associates, Inc., 1994. ISBN 1-56592-079-1
- Harbison, Samuel P. and Steele, Guy L. Jr. *C: A Reference Manual*. 4th ed. Prentice Hall, 1995. ISBN 0-13-326224-3
- Kernighan, Brian and Dennis M. Ritchie. *The C Programming Language*. 2nd Ed. PTR Prentice Hall, 1988. ISBN 0-13-110362-8
- Lehey, Greg. *Porting UNIX Software*. O'Reilly Associates, Inc., 1995. ISBN 1-56592-126-7
- Plauger, P. J. *The Standard C Library*. Prentice Hall, 1992. ISBN 0-13-131509-9
- Spinellis, Diomidis. Code Reading: The Open Source Perspective. Addison-Wesley, 2003. ISBN 0-201-79940-5
- Spinellis, Diomidis. Code Quality: The Open Source Perspective. Addison-Wesley, 2006. ISBN 0-321-16607-8
- Stevens, W. Richard and Stephen A. Rago. *Advanced Programming in the UNIX Environment*. 2nd Ed. Reading, Mass. : Addison-Wesley, 2005. ISBN 0-201-43307-9

- Stevens, W. Richard. *UNIX Network Programming*. 2nd Ed, PTR Prentice Hall, 1998. ISBN 0-13-490012-X
- Wells, Bill. "Writing Serial Drivers for UNIX". *Dr. Dobb's Journal*. 19(15), December 1994. pp68-71, 97-99.

B.5. "Internes" du système d'exploitation

- Andleigh, Prabhat K. *UNIX System Architecture*. Prentice-Hall, Inc., 1990. ISBN 0-13-949843-5
- Jolitz, William. "Porting UNIX to the 386". *Dr. Dobb's Journal*. January 1991-July 1992.
- Leffler, Samuel J., Marshall Kirk McKusick, Michael J Karels and John Quarterman *The Design and Implementation of the 4.3BSD UNIX Operating System*. Reading, Mass. : Addison-Wesley, 1989. ISBN 0-201-06196-1
- Leffler, Samuel J., Marshall Kirk McKusick, *The Design and Implementation of the 4.3BSD UNIX Operating System: Answer Book*. Reading, Mass. : Addison-Wesley, 1991. ISBN 0-201-54629-9
- McKusick, Marshall Kirk, Keith Bostic, Michael J Karels, and John Quarterman. *The Design and Implementation of the 4.4BSD Operating System*. Reading, Mass. : Addison-Wesley, 1996. ISBN 0-201-54979-4

  (Le chapitre 2 de ce livre est disponible en ligne en tant que partie du Projet de Documentation de FreeBSD, et le chapitre 9 ici.)

- Marshall Kirk McKusick, George V. Neville-Neil *The Design and Implementation of the FreeBSD Operating System*. Boston, Mass. : Addison-Wesley, 2004. ISBN 0-201-70245-2
- Stevens, W. Richard. *TCP/IP Illustrated, Volume 1: The Protocols*. Reading, Mass. : Addison-Wesley, 1996. ISBN 0-201-63346-9
- Schimmel, Curt. *Unix Systems for Modern Architectures*. Reading, Mass. : Addison-Wesley, 1994. ISBN 0-201-63338-8
- Stevens, W. Richard. *TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP and the UNIX Domain Protocols*. Reading, Mass. : Addison-Wesley, 1996. ISBN 0-201-63495-3
- Vahalia, Uresh. *UNIX Internals — The New Frontiers*. Prentice Hall, 1996. ISBN 0-13-101908-2
- Wright, Gary R. and W. Richard Stevens. *TCP/IP Illustrated, Volume 2: The Implementation*. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-63354-X

B.6. Ouvrages de référence en matière de sécurité

- Cheswick, William R. and Steven M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-63357-4
- Garfinkel, Simson and Gene Spafford. *Practical UNIX Internet Security*. 2nd Ed. O'Reilly Associates, Inc., 1996. ISBN 1-56592-148-8
- Garfinkel, Simson. *PGP Pretty Good Privacy* O'Reilly Associates, Inc., 1995. ISBN 1-56592-098-8

B.7. Ouvrages de référence sur le matériel

- Anderson, Don and Tom Shanley. *Pentium Processor System Architecture*. 2nd Ed. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-40992-5
- Ferraro, Richard F. *Programmer's Guide to the EGA, VGA, and Super VGA Cards*. 3rd ed. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-62490-7
- Intel Corporation publie la documentation sur ses processeurs, circuits et standards sur son site web développeur, généralement sous forme de fichiers PDF.
- Shanley, Tom. *80486 System Architecture*. 3rd ed. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-40994-1
- Shanley, Tom. *ISA System Architecture*. 3rd ed. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-40996-8
- Shanley, Tom. *PCI System Architecture*. 4th ed. Reading, Mass. : Addison-Wesley, 1999. ISBN 0-201-30974-2
- Van Gilluwe, Frank. *The Undocumented PC*, 2nd Ed. Reading, Mass: Addison-Wesley Pub. Co., 1996. ISBN 0-201-47950-8
- Messmer, Hans-Peter. *The Indispensable PC Hardware Book*, 4th Ed. Reading, Mass: Addison-Wesley Pub. Co., 2002. ISBN 0-201-59616-4

B.8. Histoire d'UNIX®

- Lion, John *Lion's Commentary on UNIX, 6th Ed. With Source Code*. ITP Media Group, 1996. ISBN 1573980137
- Raymond, Eric S. *The New Hacker's Dictionary, 3rd edition*. MIT Press, 1996. ISBN 0-262-68092-0. Aussi connu sous le nom de Jargon File
- Salus, Peter H. *A quarter century of UNIX*. Addison-Wesley Publishing Company, Inc., 1994. ISBN 0-201-54777-5
- Simon Garfinkel, Daniel Weise, Steven Strassmann. *The UNIX-HATERS Handbook*. IDG Books Worldwide, Inc., 1994. ISBN 1-56884-203-1. Epuisé, mais disponible en ligne.
- Don Libes, Sandy Ressler *Life with UNIX* - special edition. Prentice-Hall, Inc., 1989. ISBN 0-13-536657-7
- *The BSD family tree*. http://www.FreeBSD.org/cgi/cvsweb.cgi/src/shared/misc/bsd-family-tree ou local sur une machine FreeBSD.
- *The BSD Release Announcements collection*. 1997. http://www.de.FreeBSD.org/de/ftp/releases/
- *Networked Computer Science Technical Reports Library*. http://www.ncstrl.org/
- *Anciennes version de BSD du Computer Systems Research group (CSRG)*. http://www.mckusick.com/csrg/: Ces 4 CDROMs incluent toutes les versions de BSD de 1BSD à 4.4BSD et 4.4BSD-Lite2 (mais malheureusement pas 2.11BSD). De plus le dernier CDROM contient les dernières sources et les fichiers SCCS.

B.9. Revues et journaux

- *The C/C++ Users Journal*. RD Publications Inc. ISSN 1075-2838
- *Sys Admin - The Journal for UNIX System Administrators* Miller Freeman, Inc., ISSN 1061-2688
- *freeX - Das Magazin für Linux - BSD - UNIX* (in German) Computer- und Literaturverlag GmbH, ISSN 1436-7033

Annexe C: Ressources sur Internet

L'évolution rapide de FreeBSD rend peu pratique le suivi des développements via des supports imprimés. Les supports électroniques sont le meilleur, sinon la plupart du temps le seul, moyen de se tenir au courant des dernières avancées. Comme FreeBSD est un effort basé sur le volontariat, la communauté des utilisateurs sert généralement de "service de support technique", le courrier électronique et les forums de discussion étant le meilleur moyen de contacter cette communauté.

Les points de contact les plus importants avec la communauté des utilisateurs de FreeBSD sont listés ci-dessous. Si vous connaissez d'autres ressources qui n'y figurent pas, communiquez-les s'il vous plaît à la liste de diffusion du groupe de documentation de FreeBSD de façon à ce qu'elles soient aussi mentionnées.

C.1. Listes de diffusion

Bien qu'un grand de nombre de développeurs de FreeBSD lisent les forums de discussion, nous ne pouvons vous garantir de réponse en temps et en heure à vos questions (ni même de réponse tout court) si vous ne les postez que sur un des forums `comp.unix.bsd.freebsd.*`. En adressant vos questions sur la liste de diffusion appropriée vous nous contacterez en même temps qu'un auditoire FreeBSD concentré, ce qui vous garantit invariablement une meilleure (ou tout au moins une plus rapide) réponse.

Les chartes d'utilisation pour les différentes listes sont données à la fin de ce document. *Lisez-les s'il vous plaît avant de vous inscrire ou d'envoyer du courrier à une liste*. La plupart des inscrits à nos listes reçoivent maintenant des centaines de messages en rapport à FreeBSD chaque jour, et en définissant des chartes et des règles d'utilisation, nous essayons de garder assez élevé le rapport signal/bruit sur les listes. Ne pas le faire verrait l'échec des listes de diffusion comme moyen efficace de communication pour le projet.

Si vous désirez tester votre capacité à envoyer du courrier aux listes FreeBSD, envoyez un message de test à la liste liste de diffusion de test. Veuillez ne pas envoyer de messages de test vers une autre liste.

En cas de doute sur la liste sur laquelle poser une question, lisez Comment obtenir les meilleurs résultats sur la liste de diffusion FreeBSD-questions.

Avant de poster sur une liste de diffusion, veuillez apprendre à utiliser au mieux les listes de diffusion, comme par exemple éviter de relancer des discussions qui reviennent régulièrement, en lisant le document (FAQ) sur les questions fréquemment posées au sujet des listes de diffusion.

Des archives de toutes les listes de diffusion sont conservées et on peut effectuer des recherches sur le serveur World Wide Web de FreeBSD. Les archives interrogeables par mots-clés offrent un excellent moyen de trouver des réponses aux questions fréquemment posées et devraient être consultées avant de poster une question.

C.1.1. Résumé des listes de diffusion

Listes générales: les listes suivantes sont des listes générales auxquelles chacun est libre (et

encouragé) de s'inscrire:

Liste	Objet
cvs-all	Toutes les modifications de l'arborescence des sources
freebsd-advocacy	Propagande FreeBSD
liste de diffusion pour les annonces relatives à FreeBSD	Evénements et étapes importantes du projet
freebsd-arch	Discussions sur l'architecture et l'implémentation de FreeBSD
freebsd-bugbusters	Discussions concernant la maintenance de la base des données des rapports de bogue de FreeBSD et des outils rattachés
freebsd-bugs	Rapports de bogue
freebsd-chat	Sujets non-techniques en rapport avec la communauté FreeBSD
liste de diffusion à propos de la branche FreeBSD-CURRENT	Discussions concernant l'utilisation de FreeBSD-CURRENT
freebsd-isp	Pour les fournisseurs d'accès utilisant FreeBSD
freebsd-jobs	Emplois et interventions de consultants en rapport avec FreeBSD
freebsd-policy	Décisions de la politique de l'équipe de base de FreeBSD. Volume faible, et accès en lecture uniquement
freebsd-questions	Questions des utilisateurs et support technique
liste de diffusion des avis de sécurité pour FreeBSD	Avis de sécurité
liste de diffusion à propos de la branche FreeBSD-STABLE;	Discussions concernant l'utilisation de FreeBSD-STABLE
liste de diffusion de test	Où envoyer vos messages de test au lieu que dans une des listes réelles

Listes techniques: les listes suivantes sont destinées aux discussions techniques. Vous devriez lire la charte d'utilisation pour chaque liste attentivement avant de s'y inscrire ou d'y envoyer du courrier parce qu'il y a des règles fermes quant à leur utilisation et leur contenu.

Liste	Objet
liste de diffusion concernant ACPI sous FreeBSD	Développement de l'ACPI et de la gestion d'energie
freebsd-afs	Portage d'AFS sous FreeBSD

Liste	Objet
freebsd-aic7xxx	Développement de pilotes pour les contrôleurs AIC 7xxx d'Adaptec®
alpha	Portage de FreeBSD sur les systèmes Alpha
freebsd-amd64	Portage de FreeBSD sur les systèmes AMD64
freebsd-apache	Discussion sur les logiciels portés relatifs à Apache
freebsd-arm	Portage de FreeBSD sur les processeurs ARM®
freebsd-atm	Utilisation de réseaux ATM avec FreeBSD
freebsd-audit	Projet d'audit du code source
freebsd-binup	Conception et développement du système de mise à jour binaire
freebsd-bluetooth	Utilisation de la technologie Bluetooth® sous FreeBSD
freebsd-cluster	Utilisation de FreeBSD dans un environnement en grappe
freebsd-cvsweb	Maintenance du système CVSweb
freebsd-database	Discussions à propos de l'utilisation de bases de données et de leur développement sous FreeBSD
freebsd-doc	Création de documents en rapport avec FreeBSD
freebsd-drivers	Ecrire des pilotes de périphériques pour FreeBSD
freebsd-eclipse	Pour les utilisateurs FreeBSD de l'EDI Eclipse, les outils, les applications clientes et les logiciels portés.
freebsd-embedded	Utilisation de FreeBSD dans les applications embarquées
freebsd-eol	Entre-aide sur les logiciels relatifs à FreeBSD et qui ne sont plus supportés par le projet FreeBSD.
freebsd-emulation	Emulation d'autres systèmes comme Linux/MS-DOS®/Windows®
freebsd-firewire	Discussion technique au sujet du FireWire® (iLink, IEEE 1394) sous FreeBSD
freebsd-fs	Systèmes de fichiers
freebsd-geom	Discussions spécifiques à GEOM et à ses implémentations
freebsd-gnome	Portage de GNOME et des applications GNOME
freebsd-hackers	Discussions techniques générales

Liste	Objet
freebsd-hardware	Discussion générale à propos du matériel fonctionnant sous FreeBSD
freebsd-i18n	Internationalisation de FreeBSD
freebsd-ia32	FreeBSD sur la plate-forme IA-32 (Intel® x86)
freebsd-ia64	Portage de FreeBSD sur les futurs système Intel® IA64
freebsd-ipfw	Discussion technique concernant le développement du nouveau code du coupe-feu
freebsd-isdn	Développeurs ISDN
freebsd-jail	Discussion au sujet des environnements jail(8)
freebsd-java	Développeurs Java™ et personnes portant et les JDKs sous FreeBSD
freebsd-kde	Portage de KDE et des applications pour KDE
freebsd-lfs	Portage de LFS sous FreeBSD
freebsd-libh	Le système d'installation et de logiciel pré-compilé de seconde génération
freebsd-mips	Portage de FreeBSD sur MIPS®
freebsd-mobile	Discussions à propos des ordinateurs portables
freebsd-mozilla	Portage de Mozilla sous FreeBSD
liste de diffusion pour les discussions concernant le multimédia sous FreeBSD	Applications multimédia
freebsd-new-bus	Discussions techniques au sujet de l'architecture de bus
freebsd-net	Discussion au sujet des réseaux et du code source TCP/IP
freebsd-openoffice	Portage d'OpenOffice.org et de StarOffice™ sous FreeBSD
freebsd-performance	Questions relatives à l'optimisation pour les installations à charge/performances élevées.
freebsd-perl	Maintenance des logiciels portés relatifs à perl
freebsd-pf	Discussions et questions concernant le système de coupe-feu packet filter
freebsd-platforms	Portages sur des plateformes à architecture non Intel®
freebsd-ports	Discussion sur le catalogue des logiciels portés
freebsd-ports-bugs	Discussion sur les bogues/PRs des logiciels portés
freebsd-ppc	Portage de FreeBSD pour le PowerPC®

Liste	Objet
freebsd-proliant	Discussion technique sur l'utilisation de FreeBSD sur les serveurs HP ProLiant
freebsd-python	Problèmes concernant l'utilisation de Python sous FreeBSD
qa	Discussion sur la qualité de FreeBSD, généralement entre deux versions
freebsd-rc	Discussion relative au système rc.d et à son développement
freebsd-realtime	Développement des extensions temps réel de FreeBSD
freebsd-scsi	Sous-système SCSI
liste de diffusion pour les questions concernant la sécurité	Questions concernant la sécurité
freebsd-small	Utilisation de FreeBSD dans les applications embarquées (obsolète, utilisez freebsd-embedded à la place)
smp	Discussions sur la conception du traitement symétrique multiprocesseurs
freebsd-sparc64	Portage de FreeBSD sur les systèmes SPARC®
freebsd-standards	Conformité de FreeBSD aux normes C99 et POSIX®
freebsd-sun4v	Portage de FreeBSD sur les systèmes basés sur UltraSPARC® T1
freebsd-threads	Threading sous FreeBSD
freebsd-testing	Tests de stabilité et de performance de FreeBSD
freebsd-tokenring	Support du Token Ring sous FreeBSD
freebsd-x11	Support et maintenance de X11 sous FreeBSD
freebsd-usb	Discussion sur le support USB sous FreeBSD
freebsd-vuxml	Discussion sur l'infrastructure VuXML
freebsd-x11	Maintenance and support of X11 on FreeBSD

Liste à accès restreint: les listes suivantes sont pour les assistances plus spécialisées (et exigeantes) et ne sont probablement pas d'intérêt général. C'est aussi une bonne idée d'être d'abord actif sur les listes techniques avant de vous inscrire à une de ces listes limités de sorte que vous compreniez l'étiquette impliquée dans ces communications.

Liste	Objet
freebsd-hubs	Pour ceux qui gèrent des sites miroir (questions d'infrastructure)

Liste	Objet
freebsd-user-groups	Coordination des groupes d'utilisateurs
freebsd-vendors	Coordination des fournisseurs des pré-versions
freebsd-www	Webmestres de www.FreeBSD.org

Résumé de liste: Toutes les listes ci-dessus sont également disponibles sous forme de résumé. Une fois inscrit à une liste, vous pouvez modifier vos options de résumé dans les options de votre compte.

Listes CVS lists: Les listes suivantes sont destinées aux personnes intéressées par la lecture des journaux des modifications effectuées sur les différentes partie de l'arborescence des sources. Ce sont des listes à *lecture seule* et on ne devrait pas y envoyer de messages.

Liste	Partie de l'arborescence des sources	Description de la partie (des sources concernées)
cvs-all	/usr/(CVSROOT|doc|ports|projects|src)	Toute modification de l'arborescence (agrégation de l'ensemble des listes CVS)
cvs-doc	/usr/(doc|www)	Toutes les modifications effectuées sur les arborescences doc et www
cvs-ports	/usr/ports	Toutes les modifications effectuées sur l'arborescence des logiciels portés
cvs-projects	/usr/projects	Toutes les modifications effectuées sur l'arborescence des projets
cvs-src	/usr/src	Toutes les modifications effectuées sur l'arborescence des sources

C.1.2. Comment s'inscrire

Pour s'inscrire à une liste, cliquez sur le nom d'une liste ci-dessus où sur https://lists.freebsd.org et cliquez ensuite sur la liste qui vous intéresse. La page de la liste devrait contenir toutes les instructions nécessaires à l'inscription.

Pour poster réellement sur une liste, envoyez simplement un courrier électronique à l'adresse nom-de-la-liste@FreeBSD.org. Ce courrier sera alors redistribué à l'ensemble des membres de la liste de par le monde.

Pour vous désabonner d'une liste, cliquez sur l'URL se trouvant à la fin de chaque message reçu de la liste. Il est également possible d'envoyer un message à nom-de-la-liste-unsubscribe@FreeBSD.org pour vous désabonner.

Encore une fois, nous voudrions vous demander de garder aux discussions sur les listes techniques leur caractère technique. Si vous n'êtes intéressés uniquement que par les annonces importantes alors nous vous suggérons de vous inscrire à la liste liste de diffusion pour les annonces relatives à FreeBSD, dont le trafic n'est qu'occasionnel.

C.1.3. Chartes d'utilisation des listes

Il y a pour *toutes* les listes de diffusion FreeBSD des règles de base auxquelles tous leurs utilisateurs doivent se conformer. En cas de non respect de ces règles, et après deux (2) avertissements écrits de la part du "Postmaster" de FreeBSD postmaster@FreeBSD.org, au troisième manquement, le contrevenant sera désabonné de toutes les listes de diffusion de FreeBSD, et ses messages ultérieurs filtrés. Nous regrettons de devoir prendre de telles mesures, mais l'Internet d'aujourd'hui est un milieu relativement hostile, et beaucoup ne se rendent pas compte de la fragilité de certains de ses mécanismes.

Règles générales:

- Le sujet de tout message doit correspondre au sujet traité par la liste à laquelle il est adressé, e.g., si c'est une liste concernant des problèmes techniques alors le contenu de votre message doit être technique. Le bavardage continu et les polémiques ne font que dégrader la qualité de la liste de diffusion pour tous les utilisateurs et ne seront pas tolérés. Pour des discussions libres sans sujet particulier, la liste de diffusion pour la discussion de sujets non-techniques en rapport avec FreeBSD est disponible et devrait être utilisée dans ce cas.
- Aucun message ne doit être adressé à plus de 2 listes de diffusion, et à 2 listes uniquement dans le cas où il y a une nécessité évidente de poster sur les deux listes. Pour la plupart des listes, il y a déjà beaucoup de souscripteurs communs, et mis à part les cas les plus ésotériques (par exemple "-stable -scsi"), il n'y a pas vraiment de raison de poster sur plus d'une liste à la fois. Si vous recevez un message où apparaissent sur la ligne `Cc` plusieurs listes de diffusion, vous devez purger cette ligne `Cc` avant d'y répondre. *Vous êtes toujours responsable de vos expéditions croisées, peu importe qui en a été à l'origine.*
- Les attaques personnelles et les insultes (dans le cadre d'une discussion) ne sont pas autorisés, et cela concerne tout autant les utilisateurs que les développeurs. Les manquements grossiers à la "nétiquette", citer ou reposter des courriers privés quand l'accord n'en a pas été donné et ne le sera pas, par exemple, sont désapprouvés, mais pas particulièrement réprimés. *Cependant* de tels contenus entrent rarement dans le cadre des règles d'utilisation d'une liste, et entraîneront donc probablement un avertissement (ou une exclusion) pour cette seule raison.
- La publicité pour des produits ou services sans rapport avec FreeBSD est rigoureusement interdite et entraînera l'exclusion immédiate s'il s'avère que le contrevenant adresse ses publicités par "courrier électronique non sollicité" - spam.

Chartes liste par liste:

liste de diffusion concernant ACPI sous FreeBSD

Développement de l'ACPI et de la gestion de l'énergie

freebsd-afs

Système de fichiers Andrew - Andrew File System

C’est une liste de discussion sur le portage et l’utilisation d’AFS de CMU/Transarc.

liste de diffusion pour les annonces relatives à FreeBSD

Evénements importants / étapes importantes pour le projet

C’est une liste pour les gens intéressés uniquement par les annonces occasionnelles d’évènements FreeBSD importants. Cela inclut les annonces d’instantanés et autres versions. Cela comprend également les annonces de nouvelles fonctionnalités de FreeBSD. Il peut y avoir aussi des appels à volontaires, etc… C’est une liste de faible volume et rigoureusement modérée.

freebsd-arch

Discussions concernant l’architecture et l’implémentation

C’est une liste pour discuter de l’architecture de FreeBSD. Les messages y seront habituellement de nature technique. Des exemples de sujets qui cadrent avec cette liste sont:

- Comment revoir le système de compilation pour que plusieurs compilations personnalisées puissent être effectuées en même temps.
- Que faut-il corriger dans VFS pour que les couches Heidemann fonctionnent.
- Comment modifier l’interface des pilotes de périphériques pour que la même interface fonctionne proprement sur différents bus et architectures.
- Comment écrire un pilote réseau.

freebsd-audit

Projet d’audit du code source

C’est la liste de discussion pour le projet d’audit du code source de FreeBSD. Bien que n’étant à l’origine destinée qu’aux modifications relatives à la sécurité, sa charte a été élargie pour l’examen de toute modification de code.

Cette liste est très chargée de correctif, et n’est probablement pas intéressant pour l’utilisateur moyen de FreeBSD. Les discussions sur la sécurité non relatives à une modification particulière du code ont lieu sur freebsd-security. Réciproquement, tous les développeurs sont encouragés à envoyer leur correctifs sur la liste pour examen, tout particulièrement s’ils touchent une partie du système où un bogue peut compromettre l’intégrité du système.

freebsd-binup

Projet de mise à jour binaire de FreeBSD

Cette liste existe pour discuter du système de mise à jour binaire, ou binup. Problèmes de conception, détails d’implémentation, correctifs, rapports de bogue, rapport d’état, demandes de fonctionnalités, traces des modifications du code, et tout ce qui peut avoir rapport avec binup sont à leur place ici.

freebsd-bluetooth

Bluetooth® sous FreeBSD

C’est un forum où se rassemble les utilisateurs de la technologie Bluetooth® sous FreeBSD. Problèmes de conception, détails de l’implémentation, rapports de bogues, état du support,

demande de fonctionnalités, et tous les sujets en rapport avec Bluetooth® sont les bienvenues.

freebsd-bugbusters

Coordination de la gestion des rapports de bogue

L'objet de cette liste est de servir de forum de coordination et de discussion entre le "Boguemestre", ses chasseurs de bogues et toute autre partie intéressée dans la base de données des PRs. Cette liste n'est pas destinée aux discussions sur des bogues spécifiques, correctifs ou PRs.

freebsd-bugs

Rapports de bogue

C'est la liste pour rapporter les bogues de FreeBSD. Chaque fois que c'est possible, les bogues devraient être soumis en utilisant la commande send-pr(1) ou son interface WEB.

freebsd-chat

Sujets non-techniques en rapport avec la communauté FreeBSD

Cette liste reçoit le résidu des discussions sur les autres listes: informations sociologiques, et non techniques. Cela va de savoir si Jordan ressemble ou non à un furet de bande dessinée, s'il faut tapez en majuscules, qui boit trop de café, quelle est la meilleure bière, qui brasse de la bière dans sa cave, et ainsi de suite. Les annonces occasionnelles d'événements importants (les prochaines fêtes, mariages, naissances, nouveaux emplois, etc...) peuvent être adressées aux listes techniques, mais doivent ensuite être redirigées sur cette liste.

Core Team

Equipe de base de FreeBSD

C'est une liste interne à l'usage des membres de l'équipe de base. Des messages peuvent y être adressés lorsqu'un sujet en rapport avec FreeBSD demande arbitrage ou examen à haut niveau.

liste de diffusion à propos de la branche FreeBSD-CURRENT

Discussions concernant l'utilisation de FreeBSD-CURRENT

C'est la liste de diffusion pour les utilisateurs de FreeBSD-CURRENT. Elle inclut avertissements au sujet de nouvelles fonctionnalités de -CURRENT qui affecteront les utilisateurs, et les instructions sur ce qu'il faut faire pour rester à jour avec -CURRENT. Tous les utilisateurs de "CURRENT" doivent s'inscrire à cette liste. C'est une liste de discussion technique sur laquelle le contenu doit être strictement technique.

freebsd-cvsweb

Project CVSweb de FreeBSD

Discussions techniques au sujet de l'utilisation, du développement et de la maintenance du FreeBSD-CVSweb.

freebsd-doc

Project de documentation

C’est la liste de discussion sur les questions et projets liés à la rédaction de documentation pour FreeBSD. Les membres de cette liste sont collectivement appelés "Le Projet de Documentation de FreeBSD" - The FreeBSD Documentation Project. C’est une liste ouverte; n’hésitez pas à vous inscrire et à participer!

freebsd-drivers

Ecrire des pilotes de périphériques pour FreeBSD

C’est une liste pour les discussions techniques au sujet des pilotes de périphériques sous FreeBSD. C’est principalement un lieu où les personnes écrivant les pilotes peuvent poser des questions sur l’écriture de pilotes utilisant les APIs du noyau FreeBSD.

freebsd-eclipse

Pour les utilisateurs FreeBSD de l’EDI Eclipse, les outils, les applications clientes et les logiciels portés.

L’objectif de cette liste est de fournir un support pour tout que qui concerne le choix, l’installation, l’utilisation, le développement et la maintenance de l’EDI Eclipse, des ses outils, de ses applications clients sous FreeBSD et l’aide au portage de l’EDI Eclipse et de ses greffons sous l’environnement FreeBSD.

Le but est également de faciliter les échanges d’information entre les communautés Eclipse et FreeBSD pour un bénéfice mutuel.

Bien que cette liste soit principalement destinée à répondre aux demandes des utilisateurs d’Eclipse, elle est également un forum pour ceux qui désirent développer des applications spécifiques à FreeBSD en utilisant le système Eclipse.

freebsd-embedded

Utilisation de FreeBSD dans les applications embarquées

Cette liste aborde les sujets relatifs à l’utilisation de FreeBSD dans les systèmes embarqués. C’est une liste de diffusion à caractère technique pour laquelle on attend un contenu strictement technique. Dans le cadre de cette liste, nous définissons le terme de système embarqué pour les appareils informatisés qui ne sont pas des stations de travail et qui sont destinés à une application bien particulière et limitée par opposition aux systèmes informatiques classiques. Des exemples de systèmes embarqués, parmi tant d’autres, sont les combinés téléphoniques, les équipements réseau comme les routeurs, les commutateurs et les PABXs, les équipements de mesure à distance, les PDAs, les systèmes de distributeurs, et ainsi de suite.

freebsd-emulation

Emulation d’autres systèmes comme Linux/MS-DOS®/Windows®

C’est une liste pour les discussions techniques relativent à l’exécution sous FreeBSD de programmes écris pour d’autres systèmes d’exploitation.

freebsd-eol

Entre-aide sur les logiciels relatifs à FreeBSD et qui ne sont plus supportés par le projet FreeBSD.

Cette liste est destinée aux personnes désirant proposer ou recherchant une aide pour les logiciels relatifs à FreeBSD pour lesquels le projet FreeBSD ne fournir officiellement plus de support (par exemple sous la forme d'avis de sécutité et de correctifs).

freebsd-firewire

FireWire® (iLink, IEEE 1394)

C'est une liste pour les discussions sur la conception et le développement d'un sous-système FireWire® (IEEE 1394, iLink) sous FreeBSD. Les sujets appropriés incluent spécifiquement les normes, les bus périphériques et leur protocole, l'ensemble d'adaptateurs/cartes/circuits, et l'architecture et l'implémentation de leur propre support.

freebsd-fs

Systèmes de fichiers

Discussions concernant les systèmes de fichiers FreeBSD. C'est une liste de discussion technique sur laquelle le contenu doit être strictement technique.

freebsd-geom

GEOM

Discussions spécifiques à GEOM et aux implémentations relatives. C'est une liste de diffusion technique sur laquelle le contenu doit être strictement technique.

freebsd-gnome

GNOME

Discussions concernant l'environnement de travail GNOME sous les systèmes FreeBSD. C'est une liste de discussion technique sur laquelle le contenu doit être strictement technique.

freebsd-ipfw

Coupe-feu IP

C'est le forum pour les discussions techniques concernant la nouvelle implémentation du code du coupe-feu IP sous FreeBSD. C'est une liste de discussion technique sur laquelle le contenu doit être strictement technique.

freebsd-ia64

Portage de FreeBSD sur IA64

C'est une liste de discussion technique pour les personnes travaillant sur le portage de FreeBSD sur la plate-forme IA-64 d'Intel®, pour soulever les problèmes ou discuter de solutions alternatives. Ceux qui sont intéressés à suivre les discussions techniques sont aussi bienvenus.

freebsd-isdn

Communications ISDN

C'est la liste pour les personnes discutant du développement du support ISDN de FreeBSD.

freebsd-java

Développement Java™

C'est la liste pour les personnes discutant du développement d'applications Java™ significatives sous FreeBSD et du portage et de la maintenance des JDK™s.

freebsd-jobs

Recherches et offres d'emplois

C'est un forum pour poster des offres d'emplois et des curriculum vitae relatifs à FreeBSD, c'est à dire si vous cherchez un emploi concernant FreeBSD ou que vous offrez un emploi impliquant FreeBSD, alors c'est le bon endroit. Ce n'est *pas* une liste de diffusion pour les problèmes généraux relatifs aux offres et à la recherche d'un emploi puisque des forums adéquats existent déjà par ailleurs.

Notez que cette liste, comme les autres listes de diffusion du domaine `FreeBSD.org`, est diffusée au niveau mondial. Par conséquent, vous devez être précis quant à l'emplacement, les possibilités de travail à distance ou de déplacement.

Les messages devraient utiliser uniquement des formats ouverts - de préférence du texte brut, mais le PDF, l'HTML, et quelques autres formats sont acceptables. Les formats propriétaires comme Microsoft® Word (.doc) seront rejetés par le serveur de la liste de diffusion.

freebsd-kde

KDE

Discussions concernant KDE sous les systèmes FreeBSD. C'est une liste de discussion technique sur laquelle le contenu doit rester strictement technique.

freebsd-hackers

Discussions techniques

C'est le forum pour les discussions techniques au sujet de FreeBSD. C'est la principale liste technique. Elle est destinée à ceux qui travaillent activement à FreeBSD, pour soulever des problèmes et discuter de solutions alternatives. Ceux qui sont intéressés à suivre les discussions techniques sont aussi bienvenus. C'est une liste de discussion technique sur laquelle le contenu doit être strictement technique.

freebsd-hardware

Discussions générales sur le matériel pour FreeBSD

Discussions générales sur les types de matériel sur lesquels tourne FreeBSD, les problèmes rencontrés et suggestions sur quoi acheter ou éviter.

freebsd-hubs

Sites miroir

Annonces et discussions pour les personnes qui font fonctionner les sites miroir FreeBSD.

freebsd-isp

Questions concernant les fournisseurs d'accès à Internet

C'est la liste pour discuter des sujets qui intéressent les fournisseurs d'accès Internet - Internet Service Providers (ISPs) - qui utilisent FreeBSD. C'est une liste de discussion technique sur laquelle le contenu doit être strictement technique.

freebsd-openoffice

OpenOffice.org

Discussions concernant le portage et la maintenance d'OpenOffice.org et StarOffice™.

freebsd-performance

Discussions au sujet de l'optimisation et l'accélération de la vitesse d'exécution de FreeBSD

Cette liste de diffusion existe pour offrir un endroit aux hackers, administrateurs, et/ou les parties concernées pour discuter de sujets ayant trait aux performances de FreeBSD. Les sujets acceptables comprennent les discussions concernant les installations de FreeBSD qui sont soit sous charge importante, soit présentant des problèmes de performance, ou encore qui repoussent les limites de FreeBSD. Les personnes désirant travailler sur l'amélioration des performances de FreeBSD sont grandement encouragées à s'inscrire à cette liste. C'est une liste hautement technique destinée aux utilisateurs expérimentés de FreeBSD, aux hackers, ou aux administrateurs intéressés par un FreeBSD rapide, robuste, et adaptable. Ce n'est pas une liste de questions-réponses qui remplace la lecture de la documentation, mais c'est un endroit où il est possible d'effectuer des contributions ou de se préoccuper de sujets non-résolus relatifs aux performances.

freebsd-pf

Discussions et questions concernant le système de coupe-feu packet filter

Discussions concernant le système de coupe-feu packet filter (pf) sous FreeBSD. Les discussions techniques ainsi que les questions des utilisateurs sont les bienvenues. Cette liste est également un endroit où discuter du système de qualité de service ALTQ.

freebsd-platforms

Portage sur les plate-formes non Intel®

Questions concernant le support d'autres plates-formes, discussions générales et propositions pour les portages sur des plates-formes non Intel®. C'est une liste de discussion technique sur laquelle le contenu doit être strictement technique.

freebsd-policy

Décisions de la politique de l'équipe de base

C'est une liste de discussion à faible trafic, et en lecture seule pour les décisions de la politique de l'équipe de base.

freebsd-ports

Discussion sur les "logiciels portés"

Discussions concernant le ``catalogue des logiciels portés'' de FreeBSD (/usr/ports), propositions de portages, modifications de l'infrastructure du catalogue des logiciels portés et coordination générale. C'est une liste de discussion technique sur laquelle le contenu doit être strictement technique.

freebsd-proliant

Discussion technique sur l'utilisation de FreeBSD sur les serveurs HP ProLiant

Cette liste de diffusion doit être utilisée pour les discussions techniques concernant l'utilisation de FreeBSD sur les serveurs HP ProLiant, y compris les discussions sur les pilotes spécifiques à ces machines, les logiciels de gestion, les outils de configuration, et les mises à jour du BIOS. C'est également le premier endroit où discuter des modules hpasmd, hpasmcli, et hpacucli.

freebsd-python

Python sous FreeBSD

C'est une liste pour les discussions relatives à l'amélioration du support de Python sous FreeBSD. C'est une liste de discussion technique. Elle est destinée aux personnes travaillant sur le portage de Python, de ses modules tiers partie et éléments relatifs à Zope sous FreeBSD. Les personnes intéressées par ces discussions techniques sont également les bienvenues.

freebsd-questions

Questions des utilisateurs

C'est la liste pour les questions à propos de FreeBSD. Vous ne devriez pas adresser de questions du type "comment faire" aux listes techniques à moins que vous n'estimiez que la question soit vraiment très technique.

freebsd-scsi

Sous-système SCSI

C'est la liste de diffusion pour ceux qui travaillent sur le sous-système SCSI de FreeBSD. C'est une liste de discussion technique sur laquelle le contenu doit être strictement technique.

liste de diffusion pour les questions concernant la sécurité

Questions relatives à la sécurité

Questions ayant trait à la sécurité des ordinateurs sous FreeBSD (DES, Kerberos, trous de sécurité connus et correctifs, etc...). C'est une liste de discussion technique sur laquelle le contenu doit être strictement technique. Notez que ce n'est pas une liste de question-réponse, mais ce type de contribution (la question ET la réponse) à la FAQ est le bienvenue.

liste de diffusion des avis de sécurité pour FreeBSD

Avis de sécurité

Notifications des problèmes de sécurité concernant FreeBSD et correctifs. Ce n'est pas une liste de discussion. La liste de discussion correspondante est FreeBSD-security.

freebsd-small

Utilisation de FreeBSD dans les applications embarquées

Cette liste discute de sujets relatifs aux installations inhabituellement petites et embarquées de FreeBSD. C'est une liste de discussion technique sur laquelle un contenu strictement technique est attendu.

Cette liste est obsolète depuis la création de freebsd-embedded.

liste de diffusion à propos de la branche FreeBSD-STABLE;

Discussions concernant l'utilisation de FreeBSD-STABLE

C'est la liste de diffusion pour les utilisateurs de FreeBSD-STABLE. Elle inclut avertissements au sujet de nouvelles fonctionnalités de -STABLE qui affecteront les utilisateurs, et des instructions sur ce qu'il faut faire pour rester à jour avec -STABLE. Tous les utilisateurs de la branche "STABLE" devraient s'inscrire à cette liste. C'est une liste de discussion technique sur laquelle le contenu doit être strictement technique.

freebsd-standards

Conformité aux normes C99 POSIX

C'est un forum pour les discussions techniques concernant la conformité de FreeBSD aux normes C99 et POSIX.

freebsd-usb

Discussion sur le support USB sous FreeBSD

C'est une liste de diffusion pour les discussions techniques relatives au support de l'USB sous FreeBSD

freebsd-user-groups

Coordination des groupes d'utilisateurs

C'est la liste pour les coordinateurs des différents groupes locaux d'utilisateurs, destinée à leurs discussions entre eux et avec un membre désigné de l'équipe de base. Cette liste doit se limiter aux comptes-rendus de réunions et à la coordination de projets entre plusieurs groupes d'utilisateurs.

freebsd-vendors

Fournisseurs

Coordination des discussions entre le projet FreeBSD et les fournisseurs de logiciel ou de matériel pour FreeBSD.

C.1.4. Filtrages en vigueur sur les listes de diffusion

Les listes de diffusion FreeBSD sont filtrées de plusieurs façons en vue d'éviter la distribution de SPAM, de virus, et tout autre message non-sollicité. Les opérations de filtrage décries dans cette section ne comprennent pas toutes celles utilisées pour protéger les listes re diffusion.

Seuls certains types de pièces jointes sont autorisés sur les listes de diffusion. Toutes les pièces jointes avec un format MIME qui ne figurent pas parmi la liste ci-dessous seront retirées avant que le message ne soit distribué sur les listes de diffusion.

- application/octet-stream
- application/pdf
- application/pgp-signature
- application/x-pkcs7-signature
- message/rfc822
- multipart/alternative
- multipart/related
- multipart/signed
- text/html
- text/plain
- text/x-diff
- text/x-patch

Certaines listes de diffusion pourront autoriser des pièces jointes sous d'autres formats MIME, mais la liste précédente devrait être applicable pour la plupart des listes de diffusion.

Si un message contient une version HTML et une version texte du contenu du message, la version HTML sera retirée. Si le corps d'un message est uniquement sous forme HTML, il sera converti sous forme texte brut.

C.2. Forums de discussion

En plus de deux forums de discussion spécifiques à FreeBSD, il y en a de nombreux autres où il est question de FreeBSD ou qui sont par ailleurs d'intérêt pour les utilisateurs de FreeBSD. Des archives interrogeables par mots-clés sont disponibles pour certains de ces forums, grâce à Warren Toomey wkt@cs.adfa.edu.au.

C.2.1. Forums spécifiques à BSD

- comp.unix.bsd.freebsd.announce
- comp.unix.bsd.freebsd.misc
- de.comp.os.unix.bsd (Allemand)
- fr.comp.os.bsd (Français)
- it.comp.os.freebsd (Italien)
- tw.bbs.comp.386bsd (Chinois)

C.2.2. Autres forums UNIX® intéressants

- comp.unix
- comp.unix.questions
- comp.unix.admin
- comp.unix.programmer
- comp.unix.shell
- comp.unix.user-friendly
- comp.security.unix
- comp.sources.unix
- comp.unix.advocacy
- comp.unix.misc
- comp.bugs.4bsd
- comp.bugs.4bsd.ucb-fixes
- comp.unix.bsd

C.2.3. Système X Window

- comp.windows.x.i386unix
- comp.windows.x
- comp.windows.x.apps
- comp.windows.x.announce
- comp.windows.x.intrinsics
- comp.windows.x.motif
- comp.windows.x.pex
- comp.emulators.ms-windows.wine

C.3. Serveurs World Wide Web

C.4. Adresses électroniques

Les groupes d'utilisateurs suivants fournissent à leurs membres des adresses électroniques liées à FreeBSD. Les administrateurs cités se réservent le droit de supprimer l'adresse si elle est à l'origine d'abus.

Domaine	Possibilités offertes	Groupe d'utilisateurs	Administrateur
ukug.uk.FreeBSD.org	Transmission de courrier uniquement	freebsd-users@uk.FreeBSD.org	Lee Johnston lee@uk.FreeBSD.org

C.5. Comptes

Les groupes d'utilisateurs suivants fournissent des comptes aux personnes supportant le projet FreeBSD. Les administrateurs cités se réservent le droit de supprimer le compte s'il est à l'origine d'abus.

Hôte	Accès	Possibilités offertes	Administrateur
dogma.freebsd-uk.eu.org	Telnet/FTP/SSH	Adresse électronique, espace Web, FTP anonyme	Lee Johnston lee@uk.FreeBSD.org

Annexe D: Clés OpenPGP

Les clés OpenPGP des officiers FreeBSD.org sont données ici. Ces clés peuvent être utilisées pour vérifier une signature ou pour envoyer un courrier électronique chiffré à un des officiers. Une liste complète des clés OpenPGP FreeBSD est disponible dans l'article Clés PGP. Le trouseau complet peut être télécharger depuis pgpkeyring.txt.

D.1. Officers

D.1.1. L'officier de sécurité <security-officer@FreeBSD.org>

```
pub   rsa4096/D9AD2A18057474CB 2022-12-11 [C] [expires: 2026-01-24]
      Key fingerprint = 0BE3 3275 D74C 953C 79F8  1107 D9AD 2A18 0574 74CB
uid                           FreeBSD Security Officer <security-officer@freebsd.org>
sub   rsa4096/6E58DE901F001AEF 2022-12-11 [S] [expires: 2026-01-15]
sub   rsa4096/46DB26D62F6039B7 2022-12-11 [E] [expires: 2026-01-15]
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGOVdeUBEADHF5VGg1iPbACB+7lomX6aDytUf0k2k2Yc/Kp6lfYv7JKU+1nr
TcNF7Gt1YkajPSeWRKNZw/X94g4w5TEOHbJ6QQWx9g+N7RjEq75actQ/r2N5zY4S
ujfFTepbvgR55mLTxlxGKFBmNrfNbpHRyh4GwFRgPlxf5Jy9SB+0m54yFS4QlSd0
pIzO0CLkjHUFy/8S93oSK2zUkgok5gLWruBXom+8VC3OtBElkWswPkE1pKZvMQCv
VyM+7BS+MCFXSdZczDZZoEzpQJGhUYFsdg0KqlLv6z1rP+HsgUYKTkRpcrumDQV0
MMuCE4ECU6nFDDTnbR8Wn3LF5oTt0GtwS0nWf+nZ1SFTDURcSPR4Lp/PKjuDAkOS
P8BaruCNx1ItHSwcnXw0gS4+h8FjtWNZpsawtzjjgApcl+m9KP6dkBcbN+i1DHm6
NG6YQVtVWyN8aOKmoC/FEm1CWh1bv+ri9XOkF2EqT/ktbjbT1hFoFGBkS9/35y1G
3KKyWtwKcyF4OXcArl6sQwGgiYnZEG3sUMaGrwQovRtMf7le3cAYsMkXyiAnEufa
deuabYLD8qp9L/eNo+9aZmhJqQg4EQb+ePH7bGPNDZ+M5oGUwReX857FoWaPhs4L
dAKQ1YwASxdKKh8wnaamjIeZSGP5TCjurH7pADAIaB3/D+ZNl2a7od+C1wARAQAB
tDdGcmVlQlNEIFNlY3VyaXR5IE9mZmljZXIgPHNlY3VyaXR5LW9mZmljZXJAZnJl
ZWJzZC5vcmc+iQJSBBMBCgA8AhsBBAsJCAcEFQoJCAUWAgMBAAIeBQIXgBYhBAvj
MnXXTJU8efgRB9mtKhgFdHTLBQJjlXeQBQkF3u+rAAoJENmtKhgFdHTLOVoQALS3
cj7rqYkHiV4zDYrgPEp9O1kAyGI8VdfGAMkDVTqr+wP4v/o7LIUrgwZl5qxesVFB
VknFr0Wp5g9h0iAjasoI5sDd6tH2SmumhBHXFVdftzDQhrugxH6fWRhHs0SaFYCk
Qt5nFbcpUfWgtQ35XTbsL8iENdYpjKXsSFQrJneGSwxIjWYTFn6ps/AI3gwR8+Bn
OffEFdYugJ049O6Vu6YBFJHrnMO7NbF4v95dVYuLtpMIaXWM+V9KITmhaBzFz5fM
Q7UOzcLlbxOYKNIWcp8QQk429mayKW5VUeUExUD1ZzBHn+P6ZG7QTMDu/RmBqiHo
ewCMVz4n9uXT5BiOngE4CvS0WQwHzK+k9MLpG2u/Bo9+LT0Ceh9Ou1rfU5+0tRwl
GyOFFjf3INS7I7gkcAwxQ7dzDItN/UQPZpg8y9mABU2x4enz0AvTnb61d/1dnTEr
tdNgU433he0ZnD1HurZCjBEWC656wv6iMdWcD8gjhMbmEpPmjvXcYlTO6zhEygSM
DiwdQCWK2W4++YJerA6ULBi3niNWBpofOFH8XylV56ruhjtHCo7+/3carcMoPOJv
lVZ1zCKxLro3TRBT15JTFBGqblRyTopFK3PuxW//GTnZOtpQEOV6yL4RAXcWeC1d
1hb5k/YxUmRF6XsDNEH4b08T8ZO8dV3dAV43Wh1oiQEzBBABCAAdFiEEuyjUCzYO
7pNq7RVv5fe8y6O93fgFAmObXVYACgkQ5fe8y6O93fiBlwf/W8y1XXJIx1ZA3n6u
f7aS70rbP9KFPr4U0dixwKE/gbtIQ9ckeNXrDDWz0v0NCz4qS+33IPiJg1WcY3vR
W90e7QgAueCo5TdZPImPbCs42vadpa5byMXS4Pw+xyT+d/yp2oLKYbj3En4bg1GM
```

```
w71DezIjvV+e01UR++u1t9yZ8LOWM5Kumz1zyQLZDZ8qIKt1bBfpa+E0cEqtNQWu
iGhQE3AHI8eWV+jBkg5y2zHRIevbWb1UPsj43lgkFtAGHk9rrM8Rmgr4AXr531iD
srBwauKZ/MElcF3MINuLH+gkPPaFHw/YIpLRLaZXZVsw3Xi1RNXI2n2ea29dvs/C
Lcf1vYkCMwQQAQgAHRYhBPwOh4rlr+eIAo1jVdOXkvSep+XCBQJjm14FAAoJENOX
kvSep+XC0DcP/1ZB7k9p1T+9QbbZZE1PJiHby3815ccH3XKexbNmmakHIn3L6Cet
F891Kqt9ssbhFRMNtyZ/k/8y8Hv5bKxVep5/HMyK+8aqfDFN0WMrqZh0/CiR6DJh
gnAmPNw/hAVHMHaYGII9kCrFfPFJ02FKoc81g9F08odb7TV+UlvRjkErhRxF+dGS
wQoO0RCbf0Z1cs7nd0Vb2z4IJh4XMxBjWc/uQ2Q9dH/0uRzwpAnR4YX+MG5YrX7Z
zBvDyR0r76iQwRSDKgioNgkr6R3rq1NZGdaj+8b0LzdOqtzKJ/eupDe3+H67e/EN
qymtreGjrubpiU9bKvYArisUqhE5KtguryvR6Qz9bj87nPg33DT3WWGVrwFRxBox
dbWzjQFv0wug8m4GAwVF7fPR5/eW7IHw8zvgn0vSPcZz7MZ4e6Y5jN4kA5/xWJYZ
Sps54qQWB+FA30unIXN68KqdIzONIbtaY3W4/JjJUCm4T+wEjKaH+wJX8w1DMjlg
mkTmGh/UrTyC1vXbPgk9Sy3cRTICR1T9z7W8UlmTtnKrUklrjlFR7SXzrEXzLGOX
Fm+NEHpHNXqzcm6c3QfzY/yQ9HSAQ/t7SUQ9caRePbDz3/msyPxtGFor9roQv6VN
wRXCyRgkH4Y5tPhJAQ8G/FxX+VXFb93QL0lfelb23/BBu6cUwW63SRn5iHUEExYI
AB0WIQQeB2Johg/5/ikUnJwDU9SVF1S13AUCZISO3wAKCRADU9SVF1S13NnqAP95
LA1Om9XSAKl76VtV+L3JPDdAwIdbNa0OsRT4Wm7U3wD/YoFrdHXVHHQFKwYeUUhj
XZcxnZLe9Ixo0/JP+RVFVw65Ag0EY5V2yQEQAOqjzPpMUCGu8eElXnAd2PruC6hi
+lc/yC90KqizxIuW6qLQBaAkTCWq7suYpDqoygn7YM3rL50S285WAECAXrcst/cV
Aqr0UH/e6p4iJCUIiXcfjd/wq20RnN/+VuvLhjpCFLY5czfVS31D7Uh9MbC+zUTz
8nVTiNCsAao0qSdfJDIzB4nSO+9xIsme/dLsI5QlU5PdxOBV6HdEhCUXOoratJCb
KAOlLxtPwyMKxmv4oZ7Mqlt10peKjhpBb97qcIzJhHxujQZD0OmzIA6xoQ2eSCGd
xCEDsZ09kr3Esw1AwKnQ51xmWpFWNFk6627M1bo8+hzOz81CrTZhYrgE+1JXv6V1
L2A9lMsimdE1BHNycDS+dBOpIB9qxXCwAab4ykfvNxox/ZPDUrTy7v7mDI5uDNTN
CYYsKCj1UidycOKzSziB9Oa2uvmMJ5XstgNBf7Z8Cky1dtVd4ol6bU9L5nos9tbY
eSXFi4bmcWB7AJiVCMq6N+LBbUKWGLglB4TU1qhttpqv31X9V6ges5gARY/RuRTK
sVyhwsn7SDcqmNKRy0im2AYakwEp7hT07ulahOSLxjP+5hCf+nSJlwbxJ8ozwjjb
zeN2yLlJSI00klkIFBNUDt3wzFRW/n6qlf+/lepgzekfNrYMtfPB8AT07Z2A3U4x
lgiV346dZymbY/EjABEBAAGJBHIEGAEKACYWIQQL4zJ110yVPHn4EQfZrSoYBXR0
ywUCY5V2yQIbAgUJAgIpAAJACRDZrSoYBXR0y8F0IAQZAQoAHRYhBLYVJ36BCH33
XIGDO25Y3pAfABrvBQJjlXbJAAoJEG5Y3pAfABrvuBsQAOlQFPXhx6whO4yw5Ziz
IS02YHhSVMVYKS2T9jPIKi1qxnEiEw9eKH0bW0Oj0TEhZPyM2NJID7DRWK5r8+Ks
Mu8jwm1fUmIrefAx6fCVfCWRECT1MlbL3jhh6AcX/nK2e3Bn8vgExhzczO3JlvD6
wPCc0FkpiY7yDB9ihu1+gbE5Hg6dvftttRXDrbEdAifbNp9KYxDigxdlOb0S14hj
CBysLWH5Su/khcIlkeuqZcI8TmDldnUb2OqTCVpFhaNwsPSrHBzmb0s2sXo4FL03
pLsOdwhi31W6kjk4KvW5FKrOpoEwUMKVNMf50DHdvonUoUHRSIc/cV5NqUWHwvc0
T5031qk0CCRRa/+/iij/p2RG7c1mx7ZECj+jZfmvjSqT+WHJ1BFlNJMWyK4fdVRZ
WyCaoAecdbukwzDwUCUqHJFIWeFtbut7SOPxcwg7sbnKNApAKdi491dvH75s/U/O
wRYO/2P+ymHlqtyix2jq0ReSVYcQPXswQ8i2ifX41F+xTSl4RWCBBeXB1Nxk3+Hs
V4Jnnp1zAJZ0KlKW/oJxbNFdI1TImkpr2p8ioFf+aiePLvDkgeaG8vABgjoihPXW
HVAMR8Z+GvBY/A6OdexpibkTvC/zDr0/Exs4lsylZKDwvvFbctcpHVXBeCBQLX5v
fLrsTkaCLWF/SV9OdMykvYKU7ZAP+gKEwhp+HPFuOHZbOBhqFUdkfeCkdzX/QGdz
Tuz349roRhgz2vRfN7MtbtuzA6NWWhEWt5DcUgX/Y5I3Q4Z2bt3JiXQ6WJMgMMOX
Ar+XxtxyRRykc1HV3DQ/cq8OWYubNnIbgebPNIFr2OIWKsR9yDaucZzpmLfzaMZU
Au5hWmU9fIw5SIKGnQABBnNMhilfD+CkETp6baTvjTK4rpaobjJdeCTrsWgfXRNC
8x3hDvcrjPD70MylOGVQdx8GYChWJnCKXsLTGX7KwdfxkjclTyzWvdcCemp0eLha
mLGb9y1dtWdNIDcVCvZJy0lipHVUdFYYxb4iLZJANL631tlPM6AA8sO1/L4mqEGn
AIHVrUQd+2QkSiOl9mKlpgaR/fJz683BR5Qen9ywX0JPtBupqPW3t9VbO/uNxUql
HCeAhPi9NLOpujpYLfgW5QAfS3u0nkp5nrbkCoQUua2q0Oj7J0mFmtWtcE1c9+TH
mFJVb8j2G9yQw3ADe3Qp9ALazP5nVDVri8NZBhHK1/KuBmRYZtcyfqXUnKoiiWAl
m5rHaRiztW7e3wqm2oJu/RkEAagybutEuBWh2Ej2+gDxjEKKtIKGu54lif4kqTww
```

```
jKTcN1ekGihwwgCMUkBSBeNXk1ClkzLFHwESJCcFwdEgpVYQTKFsu0emYISyco3I
pUajGzfUiQRyBBgBCgAmAhsCFiEEC+MydddMlTx5+BEH2a0qGAV0dMsFAmWFy28F
CQPyfaYCQMF0IAQZAQoAHRYhBLYVJ36BCH33XIGDO25Y3pAfABrvBQJjlXbJAAoJ
EG5Y3pAfABrvuBsQAOlQFPXhx6whO4yw5ZizIS02YHhSVMVYKS2T9jPIKi1qxnEi
Ew9eKH0bW0Oj0TEhZPyM2NJID7DRWK5r8+KsMu8jwm1fUmIrefAx6fCVfCWRECT1
MlbL3jhh6AcX/nK2e3Bn8vgExhzczO3JlvD6wPCc0FkpiY7yDB9ihu1+gbE5Hg6d
vftttRXDrbEdAifbNp9KYxDigxdlOb0S14hjCBysLWH5Su/khcIlkeuqZcI8TmDl
dnUb2OqTCVpFhaNwsPSrHBzmb0s2sXo4FL03pLsOdwhi31W6kjk4KvW5FKrOpoEw
UMKVNMf50DHdvonUoUHRSIc/cV5NqUWHwvc0T5031qk0CCRRa/+/iij/p2RG7c1m
x7ZECj+jZfmvjSqT+WHJ1BFlNJMWyK4fdVRZWyCaoAecdbukwzDwUCUqHJFIWeFt
but7SOPxcwg7sbnKNApAKdi491dvH75s/U/OwRYO/2P+ymHlqtyix2jq0ReSVYcQ
PXswQ8i2ifX41F+xTSl4RWCBBeXB1Nxk3+HsV4Jnnp1zAJZ0KlKW/oJxbNFdI1TI
mkpr2p8ioFf+aiePLvDkgeaG8vABgjoihPXWHVAMR8Z+GvBY/A6OdexpibkTvC/z
Dr0/Exs4lsylZKDwvvFbctcpHVXBeCBQLX5vfLrsTkaCLWF/SV9OdMykvYKUCRDZ
rSoYBXR0yyOqEACitDvbkbfjaton6izr4T8QU2yvhJHkf4B6KeVDbKY1J4784OxX
p2bJgPeF53SYBe8gm3YHjp8ULh4A/19U4hswyE8ymcm5nIs8OLyBdxkuBZJGEnzx
H3woiyYqWH7991kzhEjUkuMgKLuTI1HiO0oLMuPQNhUHOnWafSVPC0XO/tIL12Om
oUuc7ligY9Z9AceFjTZOuHamixHAAc6hpxdIW+yhC/qTpc2VK0niWeuQfq3453iR
Tf9MnR5Beztl3ZYRWcx7UiFuKGwZwBibNnNmUs6GyQcJ5UTa1oeJcLqHi0Lf/r0j
Xo3wgJq7EZjjVyU+GI2ZVoDOaS6c4/OvLm62XoeSlnn/dQxUcjUki+x8lb69IxSF
1xAgsC/oNtFZYd5rHdlnqIBUYK0lLtSCXBkzVeivSiQa0hL5on8LDu1nw2bXyW61
yt/YxVb4FanMxAqdYVBhOfU0RaPNifH01rbb4TwC9bTZN1LQ1KI/Swb/SruUE0Ry
T28fhYRtsReS2PnUODghJSFDJbwFbBZf6RKI16q1xqKRRvxIWPm+lMOi1NLOKR9P
+OKy9HmChMw0UJUcVl1cJ2xtRl3wi5t6AA6HoNv/TrLeYVgMR9wYmKlpvjTQ5jTd
rbHD1XP5jGsp8QsJMGja1m/7cryReCpcVxvImeReaOdgz+zDmQqq3O5zuIkEcgQY
AQoAJgIbAhYhBAvjMnXXTJU8efgRB9mtKhgFdHTLBQJnhEEJBQkF0/JAAkDBdCAE
GQEKAB0WIQS2FSd+gQh991yBgztuWN6QHwAa7wUCY5V2yQAKCRBuWN6QHwAa77gb
EADpUBT14cesITuMsOWYsyEtNmB4UlTFWCktk/YzyCotasZxIhMPXih9G1tDo9Ex
IWT8jNjSSA+w0Viua/PirDLvI8JtX1JiK3nwMenwlXwlkRAk9TJWy944YegHF/5y
tntwZ/L4BMYc3MztyZbw+sDwnNBZKYmO8gwfYobtfoGxOR4Onb37bbUVw62xHQIn
2zafSmMQ4oMXZTm9EteIYwgcrC1h+Urv5IXCJZHrqmXCPE5g5XZ1G9jqkwlaRYWj
cLD0qxwc5m9LNrF6OBS9N6S7DncIYt9VupI5OCr1uRSqzqaBMFDClTTH+dAx3b6J
1KFB0UiHP3FeTalFh8L3NE+dN9apNAgkUWv/v4oo/6dkRu3NZse2RAo/o2X5r40q
k/lhydQRZTSTFsiuH3VUWVsgmqAHnHW7pMMw8FAlKhyRSFnhbW7re0jj8XMIO7G5
yjQKQCnYuPdXbx++bP1PzsEWDv9j/sph5arcosdo6tEXklWHED17MEPIton1+NRf
sU0peEVggQXlwdTcZN/h7FeCZ56dcwCWdCpSlv6CcWzRXSNUyJpKa9qfIqBX/mon
jy7w5IHmhvLwAYI6IoT11h1QDEfGfhrwWPwOjnXsaYm5E7wv8w69PxMbOJbMpWSg
8L7xW3LXKR1VwXggUC1+b3y67E5Ggi1hf0lfTnTMpL2ClAkQ2a0qGAV0dMsNxRAA
suW1aLh+hgydW+iH6DmdQRMESsB1kE02kO1462TAQaziIAvNoxw5h48xvyEnrDA8
d+9IDMyxdrLmAbndUlSveMa9+EPiGHwr6VTyFL8nA5F7DcFi4mjEyGKe18JcaAlY
UtvHgWH6EjiX2iSXpsrJFEhtfFNolZ5sp9LFI6hOBihSJxZK4sbMR7Q6IkDuAVpT
FLiejBRlsXpFvTGL6040CtxbL5cqkVMYP38rFMTuc3pGGJA4wb5EC1dGjUi6XjbY
H7kuCAFyXqV9eQQP61x7K9W8qnXW+weCIMKfSX7AcCtH1jXBAM6lqpPrh6amc+/r
bg2eNA7DmgJnEY4apIcDB/b4khRMga2ozeGWWyIvOaVvR2R7ALQ+Rgut85cM+4+V
l2PHmOzW/yYdHVb5REQItFR5COb/mGUqYhkCtiV3nXo/K0uOQKu5SBbNzLuNvuwd
n+Eimxjl18VnrGG7sjtUa0MLmtr62GiEVrhrDqa/biHp8LdWkAQjLZ4aTRh2XZig
gaVFZHmkw3ILPyKKM21UXdM0YRk3TGVK8ODQy58ebPS4v9yYT9gUA9UDkDYeGcF2
qjoDPVNvcG6H8jCSsPRl1KZwtqqITCOSAIAPI4Nu97kO6nbOyQpYlwjd1MhvVXnP
66mHSvmqaxbNGX1mF9B/yERkBkooNZrKuJSvBTC2J1q5Ag0EY5V3BwEQAMpFVczZ
o9ZPNsgW791UW5o6wnrnd1nIO+S4rc37q2TEz8KGHCuxo5NwffZ2t6Ln04BI54pb
apg17b7a0hPka37HFkL28n4VyMdx0CsAm3QEfUsdK6xwKV2SucYeVcrV1upcN4Pd
```

```
XD7su1I7/A4CWXFJG047zJ0Z89lJZiQEiAq7ghvEoinC0sm+0a6ao/ocqCgWCKM1
yCPOyzJXleRrv29SRnYziMR+q2U0x9xg9Xl6GMwUmFwbJc9nORVvLH7fbU6/du8E
goAYrglFOFZG/TSolSGWRSMiavz0JSD/i+rEN4aIT4WfBe+L9Wy1AmrNxiAO+zKm
zHQu3JSxDncr+y+hcd+W0gqw10FoI9jWLcL7kR+6a0iOjuJSXSopq2l3DafiPxtC
Fmr4CGQhzBHM6e4/v/NNd3F0XpVbJ6RQph7lkfvfz8q2lvUlHhezJ0p1xXmhff9C
HjdVMhmAmz5+imBAXk2mottNfKb0pFEen1xY3K/UPA4g+oPsSj495MsvIg9eIMCc
C3/z0SEUMWH/styyJzPqfpyfGwZeTcIj9vg2o+RnGvmcLVYA/EGToPk905kv/cK7
3oy8bZyOB0zMg7T9PaWgLUO0sqjqo0Mw3knFySg3oRXlcilPQvfPdX0JvwLpc9DW
lr1+1GkCXJ08lWugJc96CJQupKRb1IbC0oUXABEBAAGJAjwEGAEKACYWIQQL4zJ1
10yVPHn4EQfZrSoYBXR0ywUCY5V3BwIbDAUJAgIpAAAKCRDZrSoYBXR0ywwtD/wI
DmEcHdFlyFRTomUBjbeK2uzcZIhkkgL58lc63UPle5iJ2FBvmYS+0rQS53sVEscc
n5KfkOwTryKllvWbl0IzuiqfawxALcfWpfZJHzTMSnDHfgXvOOyFMQruqRDAHAr7
PNC0CnbT0sEF2ZFzad8M9fLqtkXUx4mgECNGJ4CVqg75KY8uUzv/BmRwEf587FT5
/iAIed5MjFB2VFDX9GABcvTTbHxCZIxnxl3cs15SxT0lAofZ2ueU6kWYWZSXFeaE
M/4ymPJws2mmV0AkbJghLXCn9Mx3nX6NTZZ9Harbru+RzW3/Hg3DZd0J9vko8Paf
P0l1NWtgyX74CqvTgjzTxXTnqrRXzcczK7fhcC2u4i0prPtXXcyyi7SwpoLikaZC
LFFhUmOx+mS5TjtgFyFZBNxnO7iAwkzfcTcC9sPoWaFmiQf6q5EIYzG+WQpncj80
mxl3HWOP6oFj/hZJRYseKeMkvJzLTo87rFdM6CsMrLwETR6e+aWM0btPFil1rXVA
CNOjsy0bxTV8OJEfyxnYmyjvnBvB0kdiaVEDdVhxgSqzLAX4mgXa49/V6M/uzMr+
n3/A1Jdk4V6fVm8S5cFIXxoUat3cB4xGaT9OWD3o1NPr6eS9Vo0EsJlRl81SG68f
S+Qtk2fX27T68YG4Aa3zMfZxUsVuFLtTuQbRC+fJpIkCPAQYAQoAJgIbDBYhBAvj
MnXXTJU8efgRB9mtKhgFdHTLBQJlhcuqBQkD8n1oAAoJENmtKhgFdHTLoO0QAJsT
E9fkleb7YzPEuP9GJ3jx8PGdWm7n+8UNdr24kS6gOXVUfPZrWa5So21hcIwZb4PZ
DqHSVSQnRciKhSnG7gplYPNGZ4+FWbLr/mBRYarjkVFLUuCPexSIjxV1KSGJnWs9
YTVAKZAz75GpCML6jD6biCOQCQ86wqOdWvZIZR8YvurrxR64ABB0rjbsaG8cNOUX
1cwAfdLwthf64dS+2m3lqNGDHkP5eNL0RIxC5gXYEp0lvmlMH3ZuO5WrfH73PTDg
89bxXeuhrFmSEwf4xWm603oi8/2qQvR9/7jb0o+t71NQuWrWIFONZWWgZBUGso+u
yT3XgY4YqKGR3z2QzKHYnJ6M7SvSYpqS7RtcxcCXF0HGNfES8cAgtKVpFtbtSwXX
p8O8oLyjmVIO/NjUpbLOGdFIsarsezLFV9f2fqZ63J34hyUSg8LrYVV1fA5DJUpe
bbX4hLpdk0MMtgG43BwKIGlJTpL5RkQ/uQU3YW2kairy7o+1imDD0TRzQxtdjVOI
5vnlTNcfJZIIfLx4drABA12OvpX3dfPV62R+8BAlJFT430CG6AISJIBqJRFvuikm
nZGUvEHmOUs/FLbbaXTPkKc7tR2WIwljRvMV+Qk84cWcX6YchMslMuiDM1mtlQZi
g34WHGSE+zCWnXAslIHlSwox7qfdO0Kz2XncSbIAiQI8BBgBCgAmAhsMFiEEC+My
dddMlTx5+BEH2a0qGAV0dMsFAmeEQS4FCQXT8gIACgkQ2a0qGAV0dMsm1Q//V09x
OutSbWU44KRurdnGKsk56DFlqXtjGYJqDPrODpX3M8IDf2MuTIN2yfPMv984bAbO
A9RL7EaGVlQUW9QWPURMsZKEFQljhfxRJO9JoGDYI7uRDnSEi6WjVvgUk5OiIh0K
EI4jEcaLCzveIEcswrVDSAn+7nGvewP8Rrx7qMUNvLAltxiMyfGXneavRs3sfusz
db9LTTY8lCU0xrslaXrrvfCkaRbskFi3S31I+1ZB/ewuAhHqfc13eRBjPwQOanJF
epAzP4GF41fVQN9GtssATCD+dV6OFhYjfWJbOIcPv277wCvGIFucM9XRjbkCIYFQ
E5W+1O/act3Obj1sB90C+cVOgCng37YqfObYLF19RE4+a7NUAh/GxHj+8TxUyvvr
aWWyfNqTMDjHMShNDjG0qSzFX7vfyUpmfAfz+6ad78aks9LMf+86iGkvBhXFs7cz
Vv4PWWYV1+WShNU2Y9yMaH3zpWUaREdB07HKbLva4Y1icqWVx+z6xs3PvsqbTei/
moXiZk7ohpbBm0htJlki22ARYrGXSK6w5RQtCZoBW0DEj5JNBjkK6XbAW3VFuAA1
J5wLS2z0eIR5adP+/SxQUbTq+ZFiOGdBP1g/783e7zEdyA0YfA2KU9OdLzupUix/
x+JYcxmrZXndSMObd0IiWOhwXlgarbJJMReOORg=
=cYaK
-----END PGP PUBLIC KEY BLOCK-----
```

D.1.2. Le secrétaire de l'équipe de base <core-secretary@FreeBSD.org>

```
pub   rsa4096/4D632518C3546B05 2024-02-17 [SC] [expires: 2028-02-08]
      Key fingerprint = 1A23 6A92 528D 00DD 7965  76FE 4D63 2518 C354 6B05
uid                           FreeBSD Core Team Secretary <core-
secretary@FreeBSD.org>
sub   rsa4096/CABFDE12CA516ED2 2024-02-17 [E] [expires: 2028-02-08]
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGXQ1o8BEAC+Rcg8cmVxuP17Vu+q5KgCx/XiulQuqKXAqqBlYCH2jqk6DINP
yFrREGBhzd/qNmlAYEahQ4Zgl0bUZNTrZVDyzicOvPP0jH+KSTQwRs7NOawEdlVO
cyHrwDCPEqf5ZzD4NhfTriEOw+j0pEH/onitUGvoQRtx15xWyaJQxDEBMTYMLewE
86D1bltwnTNczE3UZb7oQLJXkAX5hcLtou70XJGgZITvJkK+kp/xot2eFjnqRz/u
WeXnKhYAmC07EKwZ1uw047eHKwMMRBYqzApLwoQtfE430Kxf2q8de64x8zDbi6YM
1J4r8OAxOtHVyfJ0j7Q23DEZz0VVb4b1Tx5OG2Re/KSNvqI0awJO4TcRmOR88OyY
dzyXgnX6Sa7GVQY1FXvn7vtFuDAt7egZOzeomSHL9bdX07LTQ4UtM88EV9wm3q4q
smoatV9jsvPQ1zxCU3aQD/5eWTJH2/kz1LIuBL/Qi5XQpJn91lBtUWJrCgkHWPGu
f//rnnXmsG7DAChW+yZ7cFO8lfNa8sFhPqSxCYphWmJTrvadyQtDngB8JakWdnmK
pfGS6y5lel+181vw38ZZKt04AKM+nDY8051lBM7Q9Q6kTLI33UZeImndx5xYukVD
kV6aQ31HYfEark15c7iEz+OAcwFnM2ntXMt7kKGd40CqzusiPcQkPqPbAQARAQAB
tDhGcmVlQlNEIENvcmUgVGVhbSBTZWNyZXRhcnkgPGNvcmUtc2VjcmV0YXJ5QEZy
ZWVCU0Qub3JnPokCVwQTAQoAQQIbAwgLCQ0IDAcLAwUVCgkICwUWAwIBAAIeBQIX
gBYhBBojapJSjQDdeWV2/k1jJRjDVGsFBQJnp8PiBQkHeofTAAoJEE1jJRjDVGsF
GMIQALhj+mNpH8OmTFeihQ6t9P8un3llz6Wmqe/Q+ULWeqJvV/uC1J5T9fnoGhwF
MgECuguXYJtoYQ16KXnsSOs1tcqMOK9GtEtFJTGe2DtfLiBednwUvu9j3HmTlwLN
M+7rqkiC0HCg2qSjcMjxbVbA5BSgNkgfyTSO2YdjfaZ+ceiHwo/qa5xWE6i2dMR1
PLGMMHTeELdtdSH6VR9/3h0qt3qzwdMBRCVAQHbim7CqwjUH9jg+IOySXl81jNoB
xuVZR3pKshyY4Oxo1dK+W86Uiff/+c4jCAxokGWIR7C4MkZZWUQqV7920gkZFC/5
qzpT1A1/sFUg8HfFTr0vCoPSVFWn2+Tto3vr78DICVaAf02aYAFlyKK18BMCoHkS
hDDO+/JQZmvHOIgEYK+T2WN1c9gm9IDJzGZuH0X2C/vkREnJKkccJfB4pXuN10wt
fqyP9fn8h6+/t+sv3qNLm4d8fkmLXofulG3WB4i/F+Hip2rjPvvBCF7zl4xy6cJ2
xVY5HUOBTqmIwVhYwUpXaqNoWa/qJBLTuot3z7ciKmKX6Lq+Dze5dzhrPNl/CalC
HBf3miHRK3TZbYLooG3bcEWgxU2BnBi3vl5NpCoUOKkPYRlALXi2TyHmPxO7oT4e
mIzS6BgnXOqO+AXvbKKfayuSePdBqkNMK/SMC4Dylkf6Xj25iQIzBBABCgAdFiEE
EBpxaxYrAOVb7eoFrbv4YQo3ibcFAmbu7x4ACgkQrbv4YQo3ibcr5A//TIcbD/EW
YJz0zrUQdc9xG3UNfU6uHmQzAuUy5ginevyqv0TSso5qvSkOHvdxbi41rfMiB2RJ
V3q0n0PSvHFld89fOTZUMZXaPvozCiBYWScrt+KA/2pq3K8mUumHS+IFtpHLL2Tu
+gI8XCHUFxO9HUThM/rFlIyEdzoctgmqQ7IG4uZG+o2J3w09llhDAUe0vraJK1On
p9yFACnRrhqvl41JeUWcv9MH9JcwHUqtUo9WLTCIb+hkByTOyRfHBYpYw//bdXdf
6rkCwKVWpyMDbk61zq2VsS1kqbP9IH/A8CsBnA6mg+zPq2i7HIFw8Swj4OGJcIvG
a9ubUYJRjDhX/vBpNrtncANZ88FQmA+Maq0vu0LS5IIGyIKkvd1fKIsyvBDDa9kE
nfCW0XMkJA0Gf+kxdB+elXQHBwKO2sr5BiKnJT5lJq3Yu9fxxGBnf93yiN4E9bmF
gG7cZxpyb1Bp76TJhLcANyybOTjCtiNRrgqeaSx9/6hSPfPigGXIne0H2lmJO6oq
jUrsYmFiWvU9sc7AcPVw/eHG8FgW35TuwKX71z8w994iaahUPNcSVyXOUD+QNROv
HhGUXrc81t613rivh22N0NZpNubVatq43KV7+/bnPyWBIi1Awh3vIFsNNSQSrYxF
lUuQaAHQXTeZMZ/7npE4t86seMt0T7BGn765Ag0EZdDWjwEQAL3VwFifpnRCYzQ4
VZ1dAjp8w542iRprqeA+C3tvNbk2OvKpN3DIc49l2bgNZ/VI7/T58lEKrFsgLK4w
AWtv18OV7xuh0AuOblmq5MvcPrUelkPj5HA7M6Ng/rAubuHfwdP/IjIrzzY6+XDh
```

```
fP9N5KIv9VRJYT23BbvLPeit4J4tQEB/NpxL3L6zI75qq4R3T/EkHP6Y9Buup9Lr
isJlcxkSK+CyORCgTpEz6fWsXiTDgS7cTaQ969XCygBpj4wRQzwkBdokxo1wsiFt
4zLt07/PrPYjeHltTDkrF9XDNhLNJ5GliHnd01oHg1j5/n+9Osvh1maoFwuBxXTN
nTZ2P+7RKLBaVQVSkUa5KJbXoM3v7bMbXM5aLs2XjglrAzrZOV+Y7zOu5UYQdpXd
7x8XAEtEozRJzt7dosQIhKx9h4LlltFFulDUpf5VCvcUEoAzMbiX0aju9n5Rwsql
DHatU9Mm3W8OdFXj1foIXZD+VX2Jp9DgxPLoAJ0CWhPXJ8f+WFSJZCjWoPJEJKWY
0EOxiXyAuvAyniAZAC/eKZkfGckXmu7edRgYbRTTwPmZ/axa/k9aHsHLwmbxuZo/
xxQXzqU70EleHZ31A3mOqsC1epjN6dn4AFKgvVesP/K/fbvSsfsfiABS2A/68ne4
zJG73Tnk4L6J79vrXc2iMJbmdg3ZABEBAAGJAjwEGAEKACYCGwwWIQQaI2qSUo0A
3Xlldv5NYyUYw1RrBQUCZ6fEFQUJB3qIBgAKCRBNYyUYw1RrBQd9EACMVckxzy4w
aUGlERguJ+kslS8MkMjNqnfDPLRDVxbUxNvbbhw7/u9blM65DCGCeNLc2n4oiu5C
E3I095AKmvq/0dOa81mEEdZkC1CVc64bXWbEyz5AtSHUpgdxRso6C+YopndSiz1T
WcIagQRXfWaw3FBWPooA87gmibmSmCegCtqx+uyc5QxX2eFI8mRK7vlfnGpYKHs0
D1/yUSGQOwoNRJ5FYm+ynfDE3FzHEQL7lv1vpv1k3xNKfBziMMg4IMEBKNHV4VKN
qJpa8UCodeTGSWQdNnCeCWPsxz5oQjCcVH9Z3e8sMpWLHhRcBZzSwXUOws2GbRMH
xHwrfrpHJcrBhe64pgfGOvZLUJ9BDs+8egTHsqRFacipbtTR+hhVhuJEHDaQQWuM
8IRHj9HIuTAczET8JTDHTMIoo8DZdOtiW/YgqCDwYghkI77d12oNQqYoeJ2HiqbK
cGzwCpsR0A+p/iOAxJG13tsxqZV8TQ8iTokWG6ACtZ7sfeWEhxqMbUKUMgogZn0I
3n1kV+tUZC6BQrIYI7TiKg95wLZsIydeoIsQoNZwvyKAXfVmQ62YjIX8njZwN+07
8/ipUPJxCYa8zL8BZyDmoFJqa3y9z+11+vtiZ9t+aTwGvjpHDwyeCJco7go9cU3m
GRFZYciqIoG4n3tl8Pob15vFlVqk47rRqg==
=8TzT
-----END PGP PUBLIC KEY BLOCK-----
```

D.1.3. Le secrétaire de l'équipe de gestion des logiciels portés <portmgr-secretary@FreeBSD.org>

```
pub   ed25519/E3C401F60D709D59 2023-03-06 [SC] [expires: 2027-03-05]
      Key fingerprint = BED4 A1D3 6555 B681 2E9F  ABDA E3C4 01F6 0D70 9D59
uid                           FreeBSD Ports Management Team Secretary <portmgr-
secretary@FreeBSD.org>
sub   cv25519/2C92B55E27A641C3 2023-03-06 [E] [expires: 2027-03-05]
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEZAXJvxYJKwYBBAHaRw8BAQdASFAC20WL3R1T6uNyGMZbfJCxDkcP4C5vi3Op
tcZ2fbq0R0ZyZWVCU0QgUG9ydHMgTWFuYWdlbWVudCBUZWFtIFNlY3JldGFyeSA8
cG9ydG1nci1zZWNyZXRhcnlARnJlZUJTRC5vcmc+iJYEExYKAD4WIQS+1KHTZVW2
gS6fq9rjxAH2DXCdWQUCZAXJvwIbAwUJB4TOAAULCQgHAwUVCgkICwUWAwIBAAIe
BQIXgAAKCRDjxAH2DXCdWYN1AP43TjyfZtZ3DLYT++g0+SuPsoO/3yWVybA+UmFL
zb8MngEA+LLNUfvEwCuXS/soh+ww5bpfmi3UUmeGiQEAXug3iA+JATMEEAEKAB0W
IQT7N0XIbxXo7ayBMvzYKU7Du8TX1QUCZAXLkwAKCRDYKU7Du8TX1XHMB/9R1MX4
6zMgpKqPPt76GOI+eGEdBK6bY8aJZjQGdqTh9f6VtXVoTGIG7cvhc9X8tDBoB0PT
2KZWheF51AV1+NHU4HwLAQ1BMebrFvWSfkw4xg4fBGwDhz9/GN85No+Js772V5ey
8lRiL6meRVWxMlLyWcxGd8JjcC5yX/iAUQ3SBGCLqW7unWjjg7CTd+AMBwcqPGrv
ax8q6eFVguJcHJAjMnKf6HAy4cpK3s+uMoUBCGnszSN12B3ysKfyC4pNO/pix5tA
Q5v8aRqTeFPh5zmNhWo0KGPzplTPqRQSHDl7GDQC8Ru3MhzFkeWzHsexjZVwS6W2
DPcYpuuAsA0XOZIZiQIzBBABCgAdFiEEEBpxaxYrAOVb7eoFrbv4YQo3ibcFAmQF
```

```
0u0ACgkQrbv4YQo3ibccwg/9F2Xuic3nhKxRbB3mJeDo6SYQETa/Gh1qQ34+8zlt
8UMazOx67gnYQfy+pXjro6eQ2up0a4eUYezcNOudqAQD21nRz3HA6EQVNcE/TzEA
xl5CJntTaLOt7S+EDXFW5BuQIvhhoMGgm8+WNVgA0EJ7tfL0OcYBSvr19fqwChEn
9c14cSk6mgHSsleP5NvskYN053pxHwy0LTSb8YBBv52th37t/CRFC1363rS5q+D7
JixFopd1O5pKpA5ipvE4gGgRjPtwjx0SjjepwK/3fuhEJQQyKzTIKlMfu2Dj/iR2
Li1Sfccau5LQXOj9fUITU3u1YG7yrm8VGzT7ao4d+KRwgMLjd2pLqiGIbbJwGBiP
FRmtilWQoeIlmSlFX4obAA517DOK0pW1mH8+eEn4EJd3SekT3yzFyKTASv0J48Z8
3F928xg+eZvHxVC0t1J+J5IG0gt3EEncuWKIPQGR7PiQbti6R3FQVTz6WfMWOebP
Qi0E9F/Aqakr6Vj2sKGrDq+ebpaF5G8Yw1YrUl2IDiPzkCegp3ZbI0wh11Xvzhi8
LXPQGK4jBQas4G8cegfitzmtdGRHYrbMv0R9I4mvaL+WlOuD2AvyVG28lguqVhnN
AZP+ohdquYyX2CNCVvbKWAtXo6Ur0vWG8BL8m6defAtEkIwVBALaOHQOSI3aNUz4
lwy4OARkBcm/EgorBgEEAZdVAQUBAQdAsefmSfxEOdOr02+K/6noYCuJ1FeAWVz6
jFYQ+9w6jggDAQgHiH4EGBYKACYWIQS+1KHTZVW2gS6fq9rjxAH2DXCdWQUCZAXJ
vwIbDAUJB4TOAAAKCRDjxAH2DXCdWRl4AP9h5ot212BK29S6ZcMBhHvmtF5PG1oD
c7LnZycSRmbFiwEAndCMpAGOhDW8iVgDd0wLQq/ZMPe+xccfG1b3zFH2EgE=
=iiAT
-----END PGP PUBLIC KEY BLOCK-----
```

D.1.4. <doceng-secretary@FreeBSD.org>

```
pub   rsa2048/E1C03580AEB45E58 2019-10-31 [SC] [expires: 2022-10-30]
      Key fingerprint = F24D 7B32 B864 625E 5541  A0E4 E1C0 3580 AEB4 5E58
uid                           FreeBSD Doceng Team Secretary <doceng-
secretary@freebsd.org>
sub   rsa2048/9EA8D713509472FC 2019-10-31 [E] [expires: 2022-10-30]
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBF27FFcBCADeoSsIgyQUY8vREwkTikwFFlNg31MVy5s/Nq1cNK1PRfRMnprS
yfB62KqbYuz16bmQKaA9zHN4FGfiTvR6tl66LVHm1s/5HPiLv8sP14GsruLro9zN
v72dO7a9i68bMw+jarPOnu9dGiDFEI0dACOkdCGEYKEUapQeNpmWRrQ46BeXyFwF
JcNx76bJJUkwk6fWC0W63D762e6lCEX6ndoaPjjLBnFvtx13heNGUc8RukBwe2mA
U5pSGHj47J05bdWiRSwZaXa8PcW+20zTWaP755w7zWe4h60GANY7OsT9nuOqsioJ
QonxTrJuZweKRV8fNQ1EfDws3HZr7/7iXvO3ABEBAAG0PEZyZWVCU0QgRG9jZW5n
IFRlYW0gU2VjcmV0YXJ5IDxkb2Nlbmctc2VjcmV0YXJ5QGZyZWVic2Qub3JnPokB
VAQTAQoAPhYhBPJNezK4ZGJeVUGg5OHANYCutF5YBQJduxRXAhsDBQkFo5qABQsJ
CAcDBRUKCQgLBRYDAgEAAh4BAheAAAoJEOHANYCutF5YB2IIALw+EPYmOz9qlqIn
oTFmk/5MrcdzC5iLEfxubbF6TopDWsWPiOh5mAuvfEmROSGf6ctvdYe9UtQV3VNY
KeeyskeFrIBOFo2KG/dFqKPAWef6IfhbW3HWDWo5uOBg01jHzQ/pB1n6SMKiXfsM
idL9wN+UQKxF3Y7S/bVrZTV0isRUolO9+8kQeSYT/NMojVM0H2fWrTP/TaNEW4fY
JBDAl5hsktzdl8sdbNqdC0GiX3xb4GvgVzGGQELagsxjfuXk6PfOyn6Wx2d+yRcI
FrKojmhihBp5VGFQkntBIXQkaW0xhW+WBGxwXdaAl0drQlZ3W+edgdOl705x73kf
Uw3Fh2a5AQ0EXbsUVwEIANEPAsltM4vFj2pi5xEuHEcZIrIX/ZJhoaBtZkqvkB+H
4pu3/eQHK5hg0Dw12ugffPMz8mi57iGNI9TXd8ZYMJxAdvEZSDHCKZTX9G+FcxWa
/AzKNiG25uSISzz7rMB/lV1gofCdGtpHFRFTiNxFcoacugTdlYDiscgJZMJSg/hC
GXBdEKXR5WRAgAGandcL8llCToOt1lZEOkd5vJM861w6evgDhAZ2HGhRuG8/NDxG
r4UtlnYGUCFof/Q4oPNbDJzmZXF+8OQyTNcEpVD3leEOWG1Uv5XWS2XKVHcHZZ++
ISo/B5Q6Oi3SJFCVV9f+g09YF+PgfP/mVMBgif2fT20AEQEAAYkBPAQYAQoAJhYh
```

```
BPJNezK4ZGJeVUGg5OHANYCutF5YBQJduxRXAhsMBQkFo5qAAAoJEOHANYCutF5Y
kecIAMTh2VHQqjXHTszQMsy3NjiTVVITI3z+pzY0u2EYmLytXQ2pZMzLHMcklmub
5po0X4EvL6bZiJcLMI2mSrOs0Gp8P3hyMI40IkqoLMp7VA2LFlPgIJ7K5W4oVwf8
khY6lw7qg2l69APm/MM3xAyiL4p6MU8tpvWg5AncZ6lxyy27rxVflzEtCrKQuG/a
oVaOlMjH3uxvOK6IIxlhvWD0nKs/e2h2HIAZ+ILE6ytS5ZEg2GXuigoQZdEnv71L
xyvE9JANwGZLkDxnS5pgN2ikfkQYlFpJEkrNTQleCOHIIIp8vgJngEaP51xOIbQM
CiG/y3cmKQ/ZfH7BBvlZVtZKQsI=
=MQKT
-----END PGP PUBLIC KEY BLOCK-----
```