AFTERBOOT(8) Manuel de l'administrateur système OpenBSD AFTERBOOT(8)

NOM

afterboot - les choses à vérifier après le premier démarrage complet

DESCRIPTION

Avant toute chose

Ce document tente de dresser la liste des choses que l'administrateur système doit vérifier et configurer après l'installation et le premier démarrage complet du système. L'idée est de créer une liste de choses pouvant être vérifiées de façon à ce que vous puissiez être à peu près certain de ne rien avoir oublié d'évident. On suppose une connaissance basique d'UNIX, si ce n'est pas le cas, tapez :

```
# help
```

On ne fournit pas les instructions complètes pour corriger et régler les problèmes. Il y a pour cela des pages de manuel et d'autres méthodes qui sont disponibles. Par exemple, pour voir la page de manuel de la commande ls(1), tapez :

```
# man 1 ls
```

Les administrateurs se familiariseront rapidement avec OpenBSD s'ils s'habituent à utiliser les excellentes pages de manuel.

Les erratas

Au moment où vous aurez installé votre système, il est plus que probable que des bugs auront été trouvés dans cette version. Tous les problèmes importants et facilement réglables auront été rapportés sur http://www.openbsd.org/errata.html. Cette page web indique si un problème a des répercutions en terme de sécurité. Il vous est recommandé d'aller régulièrement consulter cette page.

Login

Connectez-vous en tant qu'utilisateur `root`. Vous pouvez pour cela utiliser soit la console, soit le réseau en passant par ssh(1). Si vous souhaitez interdire les connexions root par le réseau, éditez le fichier */etc/ssh/sshd_config* et fixez **PermitRootLogin** à no (voir sshd_config(5)).

Pour des raisons de sécurité, mieux vaut ne jamais se connecter en tant que root quand le système tourne, que ce soit pendant son fonctionnement normal ou au cours d'une maintenance. Les administrateurs sont plutôt encouragés à ajouter un utilisateur “normal”, d'ajouter ensuite cet utilisateur au groupe `wheel`, et d'utiliser les commandes su(1) et sudo(8) lorsque les privilèges root

sont requis. La procédure est décrite plus en détails un peu plus loin.

Mot de passe root

Modifiez le mot de passe de l'utilisateur root. (Remarquez que tout au long de la documentation, le terme “superutilisateur” est synonyme de l'utilisateur root.) Choisissez un mot de passe comportant des caractères alphanumériques et des caractères spéciaux (sauf l'espace), ainsi que des majuscules et des minuscules. Ne choisissez aucun mot d'aucun langage. Les intrus utilisent souvent des attaques par dictionnaire. Lancez la commande **/usr/bin/passwd** pour le modifier.

Mieux vaut systématiquement spécifier le chemin complet des commandes passwd(1) et su(1), car cela empêche, pour la plupart des shells, la possibilité d'exécuter des fichiers placés dans votre PATH. De plus, le PATH du superutilisateur ne devrait jamais contenir le répertoire courant (“.”).

Date du système

Vérifiez la date du système au moyen de la commande date(1). Si besoin, modifiez la date, et/ou modifiez le lien symbolique */etc/localtime* en le faisant pointer vers le bon fuseau horaire du répertoire */usr/share/zoneinfo*.

Exemples :

Régler la date actuelle au 27 Janvier 1999, 03:04 de l'après midi :

```
# date 199901271504
```

Régler le fuseau horaire à l'heure standard de l'Atlantique :

```
# ln -fs /usr/share/zoneinfo/Canada/Atlantic /etc/localtime
```

Vérifier le nom de l'hôte

Utilisez la commande **hostname** pour vérifier que le nom de votre machine soit correct. Voir la page de manuel de hostname(1) s'il a besoin d'être modifié. Vous devrez également éditer le fichier */etc/myname* afin qu'il survive au prochain redémarrage.

Vérifier la configuration des interfaces réseau

La première chose à faire est un **ifconfig -a**, qui permet de voir si les interfaces réseau sont correctement configurées. Corrigez en éditant */etc/hostname.interface* (où *interface* est le nom de l'interface, par exemple “le0”), puis en utilisant ensuite ifconfig(8) pour la configurer manuellement si vous ne voulez pas redémarrer. Lisez la page de manuel hostname.if(5) pour plus d'informations sur le format des fichiers */etc/hostname.interface*. L'interface de bouclage (*loopback*) ressemblera à quelque chose comme :

```
lo0: flags=8009<UP,LOOPBACK,MULTICAST> mtu 32972
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
        inet6 ::1 prefixlen 128
        inet 127.0.0.1 netmask 0xff000000
```

une interface Ethernet à quelque chose comme :

```
le0: flags=9863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST>
        inet 192.168.4.52 netmask 0xffffff00 broadcast 192.168.4.255
        inet6 fe80::5ef0:f0f0%le0 prefixlen 64 scopeid 0x1
```

et une interface PPP à quelque chose comme :

```
ppp0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST>
        inet 203.3.131.108 --> 198.181.0.253 netmask 0xffff0000
```

Voir netstart(8) pour des instructions sur la configuration du routage multicast.

Voir dhcp(8) pour des instructions sur la configuration des interfaces par DHCP.

Vérifier les tables de routage

Lancez une commande **netstat -rn**. La sortie ressemblera à quelque chose comme :

```
Routing tables

Internet:
Destination    Gateway           Flags  Refs     Use  Mtu  Interface
default        192.168.4.254     UGS       0 11098028    -  le0
127            127.0.0.1         UGRS      0        0    -  lo0
127.0.0.1      127.0.0.1         UH        3       24    -  lo0
192.168.4      link#1            UC        0        0    -  le0
192.168.4.52   8:0:20:73:b8:4a   UHL       1     6707    -  le0
192.168.4.254  0:60:3e:99:67:ea  UHL       1        0    -  le0

Internet6:
Destination        Gateway       Flags  Refs  Use     Mtu  Interface
::/96              ::1           UGRS     0     0   32972  lo0 =>
::1                ::1           UH       4     0   32972  lo0
::ffff:0.0.0.0/96  ::1           UGRS     0     0   32972  lo0
fc80::/10          ::1           UGRS     0     0   32972  lo0
fe80::/10          ::1           UGRS     0     0   32972  lo0
fe80::%le0/64      link#1        UC       0     0    1500  le0
fe80::%lo0/64      fe80::1%lo0   U        0     0   32972  lo0
ff01::/32          ::1           U        0     0   32972  lo0
ff02::%le0/32      link#1        UC       0     0    1500  le0
ff02::%lo0/32      fe80::1%lo0   UC       0     0   32972  lo0
```

L'adresse de la passerelle par défaut est stockée dans le fichier */etc/mygate*. Si vous avez besoin

d'éditer ce fichier, un moyen simple et sans douleur de reconfigurer le réseau après-coup est de lancer les commandes **route flush** puis **sh -x /etc/netstart**. Vous préférerez peut-être configurer tout cela manuellement en utilisant des suites de commandes **route add** et **route delete** (voir route(8)). Si vous faites tourner dhclient(8), alors vous devrez le tuer en lançant **kill `cat /var/run/dhclient.pid`** après avoir détruit les routes.

Si vous désirez router les paquets entre des interfaces, ajoutez les deux directives suivantes (ou seulement l'une des deux, selon le besoin ou non de routage IPv4 et IPv6) au fichier */etc/sysctl.conf* :

```
net.inet.ip.forwarding=1
net.inet6.ip6.forwarding=1
```

Par défaut, les paquets ne sont pas transférés, conformément aux exigences des RFC.

Vérifier les montages des disques

Vérifiez que les disques sont correctement montés en comparant le fichier */etc/fstab* à la sortie des commandes mount(8) et df(1). Exemple :

```
# cat /etc/fstab
/dev/sd0a / ffs rw 1 1
/dev/sd0d /usr ffs rw,nodev 1 2
/dev/sd0e /var ffs rw,nodev,nosuid 1 3
/dev/sd0g /tmp ffs rw,nodev,nosuid 1 4
/dev/sd0h /home ffs rw,nodev,nosuid 1 5

# mount
/dev/sd0a on / type ffs (local)
/dev/sd0d on /usr type ffs (local, nodev)
/dev/sd0e on /var type ffs (local, nodev, nosuid)
/dev/sd0g on /tmp type ffs (local, nodev, nosuid)
/dev/sd0h on /home type ffs (local, nodev, nosuid)

# df
Filesystem  1024-blocks     Used    Avail Capacity  Mounted on
/dev/sd0a         22311    14589     6606    69%    /
/dev/sd0d        203399   150221    43008    78%    /usr
/dev/sd0e         10447      682     9242     7%    /var
/dev/sd0g         18823        2    17879     0%    /tmp
/dev/sd0h          7519     5255     1888    74%    /home

# pstat -s
Device      512-blocks     Used    Avail Capacity  Priority
swap_device     131072    84656    46416    65%    0
```

Éditez */etc/fstab* et utilisez comme il se doit les commandes mount(8) et umount(8) Référez-vous à l'exemple ci-dessus et à fstab(5) pour des informations sur le format de ce fichier.

Vous voudrez peut-être aussi faire vos partitions NFS dès maintenant, ou vous en occuper plus tard.

Vérifier le bon fonctionnement du système

Vous pouvez utiliser ps(1), netstat(1) et fstat(1) pour vérifier respectivement les processus en cours de fonctionnement, les connexions réseau, et les fichiers ouverts.

MODIFICATIONS PLUS AVANCÉES

Le système devrait désormais être utilisable, mais il se peut que vous souhaitiez procéder à quelques personnalisations supplémentaires, comme ajouter des utilisateurs, etc.. Beaucoup des sections suivantes peuvent être passées si vous n'utilisez pas le paquetage concerné. Nous vous suggérons de faire un **cd /etc** et d'éditer tous les fichiers devant l'être dans ce répertoire.

Remarquez que le fichier */etc/motd* est modifié par */etc/rc* à chaque démarrage du système. Pour conserver un message personnalisé, assurez-vous de laisser deux lignes vides en haut du fichier, sans quoi votre message sera écrasé.

Ajouter de nouveaux utilisateurs

Ajoutez des utilisateurs. Il existe un script adduser(8). Vous voudrez peut-être utiliser vipw(8) pour ajouter des utilisateurs au fichier */etc/passwd*, puis éditer */etc/group* à la main pour ajouter de nouveaux groupes. Vous voudrez peut-être également éditer */etc/login.conf* et retoucher certaines des limites documentées dans login.conf(5). La page de manuel de su(1) vous dit de vous assurer de placer vos utilisateurs dans le groupe “wheel” s'ils ont besoin d'un accès root (seulement dans le cas où vous n'utilisez pas Kerberos). Par exemple :

```
wheel:*:0:root,myself
```

Suivez les instructions de login_krb5(8) si vous utilisez Kerberos pour l'authentification.

Les scripts de commande système

Les scripts */etc/rc.** sont invoqués au démarrage, après la fin du mode mono-utilisateur (*single user*), et à l'extinction. Tout le processus est plus ou moins contrôlé par le script maître */etc/rc*. Ce script ne devrait pas être modifié par les administrateurs.

/etc/rc est quant à lui influencé par les variables se trouvant dans */etc/rc.conf*. Celui-ci non plus ne devrait pas être modifié par les administrateurs : les modifications spécifiques à un site devraient être apportées au fichier */etc/rc.conf.local* (à créer si nécessaire).

Toute commande qui devrait être lancée avant que le système ne fixe son niveau de sécurité devrait être invoquée depuis */etc/rc.securelevel*, et les commandes à lancer après que le système ait fixé son niveau de sécurité devrait être invoquées depuis */etc/rc.local*. Les commandes à lancer avant que le système ne s'éteigne devraient être ajoutées à */etc/rc.shutdown*.

Pour plus d'informations concernant les fichiers de démarrage et/ou d'extinction, voir rc(8), rc.conf(8), securelevel(7) et rc.shutdown(8).

Si vous avez installé X, vous voudrez peut-être activer xdm(1), le Gestionnaire d'Affichage de X (*X Display Manager*). Pour ce faire modifiez la valeur de *xdm_flags* dans */etc/rc.conf.local*.

Régler le type de clavier

Certaines architectures permettent de contrôler le type de clavier. Utilisez la commande kbd(8) pour changer le codage du clavier. **kbd -l** donnera la liste de tous les codages disponibles. **kbd xxx** sélectionnera le codage *xxx*. Stockez le codage dans */etc/kbdtype* pour vous assurer qu'il sera automatiquement réglé au démarrage.

Imprimantes

Éditez */etc/printcap* et */etc/hosts.lpd* pour mettre en place n'importe quelle imprimante. Consultez lpd(8) et printcap(5) au besoin.

Alias d'adresse e-mail

Éditez */etc/mail/aliases* et faites pointer les trois alias standards vers une liste de diffusion ou l'administrateur du système.

```
# Well-known aliases -- these should be filled in!
root:           sysadm
manager:        root
dumper:         root
```

Lancez newaliases(8) après modification.

Sendmail

L'agent de messagerie par défaut d'OpenBSD est sendmail(8). Les détails sur la configuration d'un mailer alternatif sont documentés dans mailer.conf(5).

OpenBSD est livré avec un fichier */etc/mail/localhost.cf* par défaut qui fonctionnera pour des installations simples ; il a été généré à partir du fichier *openbsd-localhost.mc* du dossier */usr/share/sendmail/cf*. Voyez s'il-vous-plaît */usr/share/sendmail/README* et */usr/share/doc/smm/08.sendmailop/op.me* pour plus d'information sur la génération de vos propres fichiers de configuration de sendmail. Pour l'installation par défaut, sendmail est configuré pour n'accepter des connexions qu'en provenance de l'hôte local et ne pas accepter de connexions sur l'une ou l'autre des interfaces externes. Cela permet d'envoyer des messages localement, mais empêche de recevoir des messages provenant de serveurs distants, ce qui est l'idéal si vous avez une unique machine dédiée aux messages entrants et plusieurs clients. Pour faire en sorte que sendmail

accepte les connexions réseau externes, modifiez la variable *sendmail_flags* dans */etc/rc.conf.local* pour utiliser le fichier */etc/mail/sendmail.cf*, de la manière indiquée dans les commentaires que vous y trouverez. Ce fichier a été généré à partir de *openbsd-proto.mc*.

Remarquez que sendmail écoute désormais par défaut sur le port 587. C'est pour implémenter le protocole de soumission de messages de la RFC 2476. Vous voudrez peut-être désactiver cela via l'option **no_default_msa** du fichier .mc de votre sendmail. Voir */usr/share/sendmail/README* pour de plus amples informations.

Les scripts daily, weekly et monthly

Jetez un œil aux scripts */etc/daily*, */etc/weekly* et */etc/monthly*, et modifiez-les éventuellement selon vos besoins. Les choses spécifiques à votre site devraient être placées dans */etc/daily.local*, */etc/weekly.local* et */etc/monthly.local*.

Ces scripts ont été limités de manière à ce que le système continue de tourner sans prendre l'espace disque des processus normaux et des mises à jour des bases de données. (Vous n'avez probablement pas besoin de les comprendre.)

Le script */etc/daily* fournit un moyen de procéder à une sauvegarde quotidienne du système de fichiers racine. Voir daily(8) pour plus d'informations.

Renforcer la sécurité

Vous voudrez peut-être renforcer un peu plus la sécurité en éditant */etc/fbtab* au moment d'installer X. Dans */etc/inetd.conf*, commentez toutes les entrées dont vous ne vous servez pas, et n'ajoutez que ce dont vous avez réellement besoin.

Les autres fichiers de /etc

Jetez un œil aux autres fichiers de */etc* et éditez-les selon vos besoins. (N'éditez pas les fichiers se terminant par *.db*, comme *pwd.db* ou *spwd.db*. N'éditez pas non plus ni *localtime* ni *rmt*, et n'éditez aucun répertoire.)

Crontab (les processus tournant en tâche de fond)

Jetez un œil à ce qui tourne en tapant **crontab -l** en tant qu'utilisateur root, et voyez si vous trouvez quoi que ce soit d'inattendu. Avez-vous besoin de quoi que ce soit d'autre ? Souhaiteriez-vous modifier quelque chose ? Par exemple, si vous n'aimez pas que root récupère la sortie des scripts *daily*, et que vous vouliez que seuls les scripts de sécurité soient envoyés en interne, vous pouvez taper **crontab -e** et modifier certaines lignes de façon à y avoir :

```
30  1  *  *  *   /bin/sh /etc/daily 2>&1 > /var/log/daily.out
30  3  *  *  6   /bin/sh /etc/weekly 2>&1 > /var/log/weekly.out
30  5  1  *  *   /bin/sh /etc/monthly 2>&1 > /var/log/monthly.out
```

Voir crontab(5).

Le nettoyage du lendemain

Après que le processus de sécurité de nuit se soit lancé pour la première fois, modifiez les propriétaires et les permissions des fichiers, répertoires, et périphériques incriminés ; root devrait avoir reçu un message ayant pour sujet “<nom d'hôte> daily insecurity output.”. Ce message contient un ensemble de recommandations de sécurité, présenté sous la forme d'une liste comme celle-ci :

```
var/mail:
        permissions (0755, 0775)
etc/daily:
        user (0, 3)
```

Mieux vaut suivre les conseils présentés dans cette liste. Le réglage recommandé apparaît en premier dans les parenthèses, tandis que le réglage actuel arrive en second. Cette liste est générée par mtree(8) en utilisant */etc/mtree/special*. Utilisez chmod(1), chgrp(1) et chown(8) de la manière appropriée.

Les démons

Activez et/ou désactivez les processus démon selon vos besoins. intro(8) contient un guide d'utilisation des différents démons disponibles dans le système OpenBSD.

Les paquetages

Installez vos propres paquetages. La collection des ports d'OpenBSD comprend un grand ensemble de logiciels tiers. Beaucoup d'entre eux sont disponibles sous la forme de paquetages binaires que vous pouvez télécharger depuis ftp://ftp.openbsd.org ou un miroir, et installer grâce à pkg_add(1). Voir ports(7) et packages(7) pour plus de détails.

Copiez les binaires commerciaux que l'on vous a fourni. Vous devrez alors installer toutes les bibliothèques partagées nécessaires, etc. Lisez les pages de manuel compat_* pour comprendre comment installer et utiliser le mode de compatibilité.

Il y a également d'autres logiciels tiers disponibles uniquement sous forme de code source, soit parce qu'il n'a pas encore été porté pour OpenBSD, soit parce qu'une licence restrictive rend impossible la redistribution sous forme binaire. Pensez à jeter un œil aux listes de diffusion, car il arrive de temps en temps qu'on y trouve des solutions à des problèmes déjà rencontrés par d'autres.

Compiler un noyau

Les informations sur la construction et la modification d'un noyau se trouvent dans config(8).

VOIR AUSSI

ksh(1), man(1), pkg_add(1), ps(1), vi(1), hier(7), config(8), dmesg(8), ifconfig(8), intro(8), sudo(8), sysctl(8)

HISTORIQUE

Ce document est apparu pour la première fois dans OpenBSD 2.2.

OpenBSD 4.3 30 Novembre 2007 6