Administration Système et Réseaux, Sécurité

Gestion surveillance et optimisation du système

Philippe Harrand

[1]Departement Informatique
Pôle Sciences et Technologie

[2]Direction Territoriale Sud Ouest
France Télécom

22 septembre 2007

Disques et systèmes de fichiers

Noyau

- Noyaux génériques
  - Souvent compilés pour i386
  - Volumineux
- Noyau personnalisé
  - Adapté au processeur
  - Limité au nécessaire

Version noyau

- Le premier nombre est la version majeure du noyau (actuellement 2 au 22/09/2007).
- Le second nombre est le numéro de version
- Le troisiéme nombre indique une évolution mineure
- Enfin le dernier nombre indique le numéro. . .

La dernière version stable (22/09/2007) est la **2.6.22.7**

Installation des sources

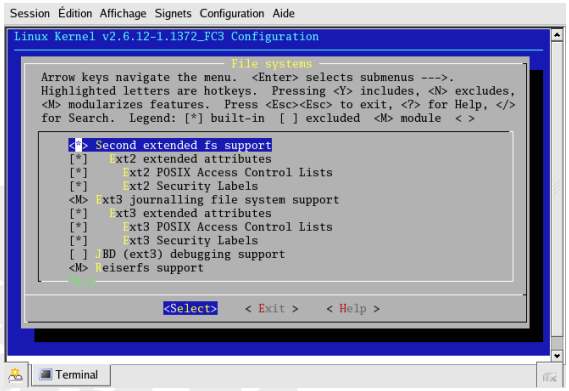
- Les sources officielles du noyau **Linux** sont disponible à www.kernel.org
- Les sources du noyau s'installent dans */usr/src/linux-<version>*
- Un lien symbolique vers le noyau en cours d'exécution est en principe */usr/src/linux*
- Votre distribution préférée propose des paquetages des sources et/ou des fichiers d'entête mais pas forcément la version la plus récente. . .

Configuration

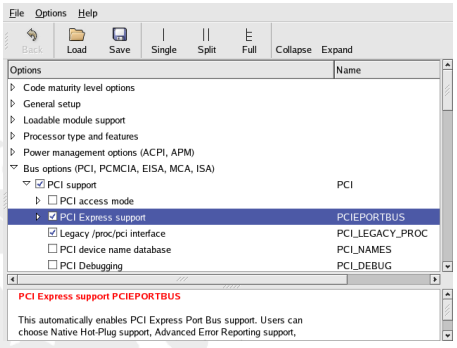
- *make config* : l'outil le plus basique, en mode texte
- *make menuconfig* : toujours en mode texte mais avec *ncurses*. UTILISABLE
- *make xconfig* : sous X, menu graphique, avec QT
- *make gconfig* : le même mais avec GTK.

En principe, votre distribution comporte les sources du noyau installé avec le fichier de configuration utilisé pour sa compilation

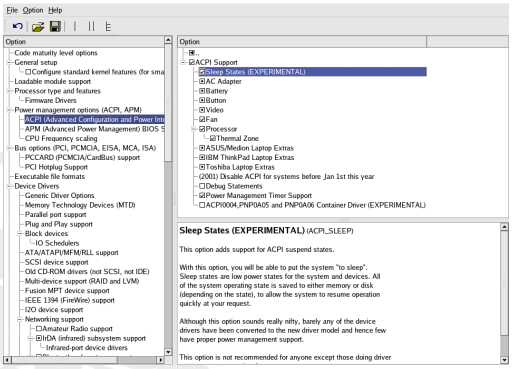
Make menuconfig



Make gconfig



Make xconfig



Compilation

- make bzImage
- allez boire un café
- make modules
- encore un café ?
- su
  - make modules_install
  - vérifiez/modifiez lilo.conf ou grub.conf

Ou tapez simplement make bzlilo et remettez votre ancien noyau dans la liste des options

PS

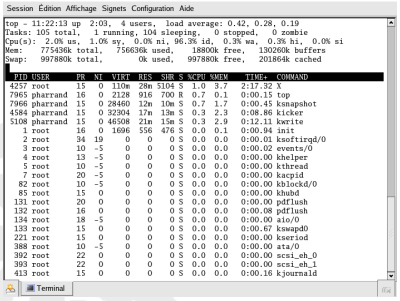
processus du terminal en cours. Options

- a affiche tous les processus
- u indique l'utilisateur
- x les processus n'ayant pas de terminal de contrôle

Taper ps aux donne donc un instantané des processus en cours d'exécution. Renvoyer la sortie vers *grep* avec un pipe "|" pour filtrer.

TOP

top affiche les processus en cours d'exécution en temps réel

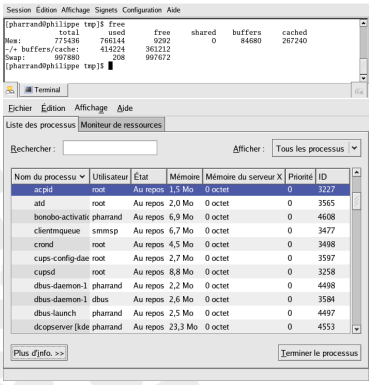


Pour quitter top, appuyez sur la touche [q]

Commandes de top

Commande	***Description***
[Espace]	Réactualise immédiatement l'affichage des données
[h]	Affiche un écran d'aide
[k]	Arrête un processus. Indiquer l'ID du processus et le signal à envoyer
[n]	Change le nombre de processus affichés
[u]	Trie les processus par utilisateurs
[M]	Trie les processus par utilisation de la mémoire
[P]	Trie les processus par utilisation de l'unité centrale
[H]	Commute l'affichage des processus fils

Free / gnome-system-monitor



Journaux

- syslogd journaux système
- klogd journal du noyau
- les journaux sont dans */var/log*
- configuration de syslog dans */etc/syslog.conf*

Syslog

Les fichiers de log standards sont les suivants :

- */var/log/messages* est le fichier système qui récupère tout
- */var/log/boot.log* . . .
- */var/log/secure* informations de connexions
- */var/log/maillog* courrier entrant et sortant
- */var/log/spooler* messages d'erreur des daemons uucp et innd (news)
- plus les journaux des différents serveurs

Classement des types de messages

<service>.<niveau> ;<service>.<niveau> ;. . .[-]<fichier>

Services

auth ou security	Messages de sécurité et d'authentification
authpriv	La même chose mais logs plus privés
cron	Messages de crontab et de at
daemon	Messages systèmes générés par le daemon
ftp	Messages du serveur ftp
kern	Messages du noyau
lpr	Messages du serveur d'impression
mail	Messages du serveur de messagerie
news	Messages du serveur de news
syslog	Messages de syslog lui-même
user	Messages des programmes utilisateurs
uucp	Messages UUCP

Criticité

7	debug	Messages de débogage
6	info	Messages d'information
5	notice	Plus importants que les messages info
4	warning ou warn	Messages d'avertissement
3	err	Messages d'erreur
2	crit	Situation critique
1	alert	Intervention immédiate
0	emerg ou panic	Système inutilisable

Syslog.conf

```
kern.*                                          /var/log/kernel
# Log anything (except mail) of level info or higher
# Don't log private authentication messages !
*.info ;mail.none ;authpriv.none ;cron.none     /var/log/messages
# The authpriv file has restricted access.
authpriv.*                                      /var/log/secure
# Log all the mail messages in one place.
mail.*                                          /var/log/maillog
# Log cron stuff
cron.*                                          /var/log/cron
# Everybody gets emergency messages
*.emerg                                         *
```

Conseils

- syslog ne crée pas de fichiers. Faites un *touch /var/log/monFichier*
- isolez les messages importants des messages normaux
- utilisez une partition spéciale pour placer vos fichiers de log
- vérifiez que vos fichiers ne deviennent pas trop volumineux. Faites les tourner (logrotate) régulièrement
- Lisez souvent vos logs. Il existe des outils pour en extraire les messages importants, voire se faire envoyer les messages importants, à savoir autobuse, logcheck, swatch, system-logviewer (redhat)...

Tests

Tester avec la commande *logger* qui envoie des messages directement à syslog. *logger -p ftp.info "Message pour voir"*

- L'option -p permet d'indiquer le niveau de priorité. Par défaut user.notice
- L'option -f permet d'indiquer un fichier
- L'option -t permet d'indiquer un tag

Exporter vos logs

- envoyer des logs vers un utilisateur connecté : *kern.crit root, toto, moi*
- Centraliser tous les messages de vos serveurs linux sur une seule machine.
  - ajouter dans */etc/rc.d/init.d/syslog* de la machine qui reçoit l'option -r derrière syslogd (514 UDP)
  - sur la machine qui doit envoyer les messages, indiquer dans le fichier /etc/syslog.conf "*kern.crit @l'autre_machine*"

Logrotate

Logrotate

- périodiquement (chaque jour, semaine, mois) logrotate fait une copie des fichiers de log
- efface les fichiers de log
- seuls les plus récents sont conservés.
- configuration de logrotate dans */etc/logrotate.conf* et */etc/logrotate.d*

Cron

- Le démon cron est chargé d'exécuter les tâches périodiques
- exécute pour *root* les commandes des fichiers contenus dans les répertoires */etc/cron.hourly*, */etc/cron.daily*, */etc/cron.weekly* et */etc/cron.monthly*
- Les utilisateurs se servent de la commande crontab pour gérer les tâches périodiques qui leur sont propres.

anacron

- cron asynchrone
- exécute les tâches programmées dès le retour sous tension de la machine
- sans intérêt pour une machine sous tension en permanence sauf. . .

At

- exécute les tâches programmées à une heure précise
- n'exécute les tâches programmées qu'une seule fois
- permet d'indiquer l'heure de lancement de manière précise

Optimisation

- arrêter les démons inutiles */sbin/service –status-all*
- ne PAS utiliser un fichier mais une partition
- mettre la partition d'échange sur un autre disque que la racine
- ou mieux, deux partitions sur des disques distincts
- utilisez des systèmes de fichiers rapides pour le type d'utilisation de votre machine et faites des sauvegardes. . .
- monter ses partitions avec l'option noatime
- limiter le nombre de processus par utilisateurs *ulimit -u<nombre>* dans */etc/.profile*

Partage de charge

- Une machine distribue le traffic vers des serveurs redondants
- Selon différentes méthodes
  - *Round-Robin*
  - *Weighted Round-Robin*
  - *Least Connexion*
  - *Weighted Least Connexion*
  - En fonction des adresses source ou destination

xenfr.org

Haute Disponibilité

- Le "distributeur" est redondant
- Le "distributeur" passif prend l'adresse IP de l'actif quand il détecte une défaillance
- Et retourne dans sa configuration originelle quand le défaillant refonctionne

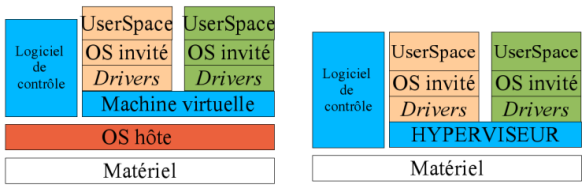
Virtualisation

- Une machine physique émule plusieurs machines virtuelles
- Qui font tourner chacune un système d'exploitation
- ⇒ Limiter les dégats en cas de crash ou de prise de contrôle
- ⇒ Allouer dynamiquement la puissance de calcul
- ⇒ Economiser sur le matériel, la maintenance, la consommation et le volume

Types de virtualisation

- Machine virtuelle
  - Emulation
  - Les systèmes invités ne voient rien
  - Possibilité d'émuler différents types de processeurs
  - Gourmand à très gourmand
  - *VmWare*, *Qemu*, etc
- Para-virtualisation ou hyperviseur
  - Les noyaux invités doivent être modifiés
  - sauf pour *Xen V3*
  - Très performant
  - *Xen*, *ESX Server* de *VmWare*, *Microsoft Longhorn serveur*

Serveurs Virtuels



- VMWARE GSX / Server / Workstation
- VirtualPC
- Les émulateurs
- XEN
- VMWARE ESX
- HypervisorIBM

Image xenfr.org