-1-0

Administration Unix

—

Cas de GNU/Linux/Debian

—

Volume 4

Ronan Keryell

rk@enstb.org

Novembre 2005

Version 1.2

Copyright (c)

- Copyright (c) 1986–2037 by `Ronan.Keryell@enstb.org`.

  This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, v1.0 or later (the latest version is presently available at `http://www.opencontent.org/openpub/`).
- Si vous améliorez ces cours, merci de m'envoyer vos modifications ! ☺
- Transparents 100 % à base de logiciels libres (LaTeX,...)

- Connexions à distance (ssh, ftp...)
- Système d'impression (BSD, CUPS...)
- Systèmes de nommage
  - Service DNS pour la résolution des noms
  - Système de nommage NIS
- Partage de fichiers en réseau avec NFS
- Auto-montage
- Archivage des données
  - tar, cpio, pax, mt...
  - Archivage en réseau avec rsync, partimage
  - AMANDA

- Administrer un domaine : faire des actions à distance
- `telnet`
  - Commande canal historique : portabilité sur tous systèmes
    - ∃ Mode émulation IBM 3270
  - Pas sécurisé ☹
  - ∃ version avec Kerberos, TLS & certificats X.509 ☺
- `rlogin` *`machine`* permet de se connecter sur une machine distante. Aucun mot de passe demandé si autorisé par fichier (distant...) `$HOME/.rhost` ou `/etc/hosts.equiv`
- `rsh` *`machine commande`* exécute une commande à distance dans son `$HOME`. Autorisation par les mêmes fichiers que `rlogin`

- `rcp [-rp] [`*machine-src* `:]fichiers [machine-dst :]`*rep* utilise le protocole `rsh` pour faire un `cp` de fichiers. Méta-caractères acceptés mais les protéger pour action à distance
- Ne pas laisser des `/etc/hosts.equiv` ou `.rhost` trop permissifs. Vérifier leur contenu
- Récupérer une copie d'écran à distance (`xwd -root` si X11)
- Interagir avec une machine Windows via SAMBA `smbclient`
- Toutes ces commandes sont peu sécurisées ☹ ⇝ utiliser plutôt `ssh` et `scp` ou utiliser Kerberos, IPsec, VPN...

- `ping` *`machine`* teste si les paquets réseau font bien l'aller-retour
- `rusers [-l]` demande et affiche la liste des utilisateurs connectés aux machines du réseau
- `rup` demande et affiche la charge des machines du réseau
- Ouvrir plein de `perfmeter` graphiques

- *File Transfer Protocol* : canal historique
- `ftp [-i]` *`machine`* ouvre une connexion
- Le nom de login `anonymous` signifie une connexion anonyme (on donne son adresse de mail comme mot de passe par convention) si un compte anonyme existe
- Commandes classiques `ls`, `cd`, `mkdir`
- `lcd` change de répertoire localement
- `get`/`put` pour transférer un fichier
- `mget`/`mput` pour transférer une liste de fichier (sans demander confirmation si `ftp -i`)
- `bin` demande) des transferts en binaire (pas de traduction de format de fin de ligne dans fichiers textuels, etc)

- `quit` ou `bye` pour arrêter
- Emballé maintenant dans les URL `ftp ://`*machine*`/` (anonymous)
- Protocole vieux et compliqué (ports dynamiques transfert de données différent port de commande, pas terrible pour les pare-feu, modes passif/actif...) ☹
- Toutes ces commandes sont peu sécurisées ⇝ utiliser plutôt `sftp` ou `SCP` d'OpenSSH
- ∃ Extensions FTPS au-dessus de TLS

  `http://www.ford-hutchinson.com/~fh-1-pfh/ftps-ext.html`

Serveur FTP

- Sert et accepte fichiers
- ∃ Nombreux serveurs avec différentes possibilités
- En fonction de charge, lancer autonome (tourne en attente de connexion) ou depuis super-démon `inetd` ou `xinetd` (lancé à chaque connexion)
- Exemple de ProFTPD `http://www.proftpd.org`
  - Modules & fichiers de configuration à la Apache
  - Nombreuses extensions
    - Chiffrement des transferts via TLS
    - Fichiers `.ftpaccess` à la `.htaccess`
    - Filtrage à la TCPwrapper

- Modes d'authentification (fichiers, Radius, LDAP, SQL...)
- Limitation de débit
- Hôtes virtuels (VirtualHost) sur même adresse IP
- Exécution dans `chroot` configurable

▶ Exemple de configuration `/etc/proftpd.conf`

```
#
# /etc/proftpd.conf -- This is a basic ProFTPD configuration file.
# To really apply changes reload proftpd after modifications.
#

ServerName "Debian"
ServerType inetd
DeferWelcome off
```

```
MultilineRFC2228 on
DefaultServer on
ShowSymlinks on

TimeoutNoTransfer 600
TimeoutStalled 600
TimeoutIdle 1200

DisplayLogin                    welcome.msg
DisplayFirstChdir               .message
ListOptions                 "-l"

DenyFilter \*.*/

# Uncomment this if you are using NIS or LDAP to retrieve passwords:
#PersistentPasswd off
```

```
# Uncomment this if you would use TLS module:
#TLSEngine  on

# Uncomment this if you would use quota module:
#Quotas on

# Port 21 is the standard FTP port.
Port 21

# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances 30
```

```
# Set the user and group that the server normally runs at.
User nobody
Group nogroup

# Umask 022 is a good standard umask to prevent new files and dirs
# (second parm) from being group and world writable.
Umask 022  022
# Normally, we want files to be overwriteable.
AllowOverwrite on

# Delay engine reduces impact of the so-called Timing Attack described in
# http://security.lss.hr/index.php?page=details&ID=LSS-2004-10-02
# It is on by default.
#DelayEngine  off

# A basic anonymous configuration, no upload directories.
```

```
# <Anonymous ~ftp>
#   User ftp
#   Group nogroup
#   # We want clients to be able to login with "anonymous" as well as "ftp"
#   UserAlias anonymous ftp
#   # Cosmetic changes, all files belongs to ftp user
#   DirFakeUser on ftp
#   DirFakeGroup on ftp
#
#   RequireValidShell off
#
#   # Limit the maximum number of anonymous logins
#   MaxClients 10
#
#   # We want 'welcome.msg' displayed at login, and '.message' displayed
#   # in each newly chdired directory.
#   DisplayLogin welcome.msg
```

```
#   DisplayFirstChdir .message
#
#   # Limit WRITE everywhere in the anonymous chroot
#   <Directory *>
#     <Limit WRITE>
#       DenyAll
#     </Limit>
#   </Directory>
#
#   # Uncomment this if you're brave.
#   # <Directory incoming>
#   #   # Umask 022 is a good standard umask to prevent new files and dirs
#   #   # (second parm) from being group and world writable.
#   #   Umask 022  022
#   #             <Limit READ WRITE>
#   #             DenyAll
#   #             </Limit>
```

```
#    #              <Limit STOR>
#    #              AllowAll
#    #              </Limit>
#    # </Directory>
#
# </Anonymous>
```

- Problème des protocoles comme `telnet` ou `rlogin` :
  - Font confiance aux traductions IP ↔ noms ou font passer les mots de passe en clair sur le réseau... ☹
  - Une connexion peut être détournée en cours de route (interception/injection, changement des tables de routage,...) : l'authentification sécurisée (OTP) ne suffit pas
- ⇝ Besoin logiciel sécurisé par chiffrement fort pour
  - Connexion à distance (style `rlogin`) : `ssh`
  - Exécution de commande à distance (style `rsh`) : `ssh`
  - Copie de fichier entre machines style `rcp` : `scp` ou style `ftp` : `sftp`

- Généalogie
  - Entreprise finlandaise : version 1. Protocole peu sécurisé (taille des paquets non chiffrée, somme de vérification non chiffrée,...). Utilisation non commerciable libre
  - Version 2 plus sécurisée. Utilisation non commerciable libre
  - OpenSSH sous produit libre d'OpenBSD ; version 1 et 2 du protocole
- Authentification forte
  - RSA ou autres. Clés publiques des autres dans son `~/.ssh/authorized_keys`

- Serveur génère un nombre aléatoire de 256 bits
- Chiffré par serveur avec la clé publique du client demandant la connexion
- Client déchiffre le nombre aléatoire avec sa clé secrète et renvoie son hachage MD5 (pour éviter une attaque de RSA à texte connu)
- Serveur calcule aussi le hachage MD5 et le compare à celui reçu

► `.rhosts` et `/etc/hosts.equiv` basée sur adresses IP (comme `rlogin`,...) mais avec protection par clé RSA par machine (`/etc/ssh_known_host` et `~/.ssh/known_hosts`) pour éviter les attaques IP et reroutage et une partie des mensonges de DNS

- Mélange des 2

- Confidentialité : toutes communications chiffrées automatiquement
  - Utilisation de RSA pour échanger les clés de l'algorithme symétrique
  - Algorithmes symétriques disponibles : IDEA, Blowfish,Triple-DES
  - Authentification démarrée après le chiffrement : pas de mots de passe en clair sur le réseau même si pas d'authentification forte
  - Possibilité de protéger clé secrète par une phrase secrète hachée par MD5 pour déchiffrer la clé via

3DES. Sinon : `root` local peut voler trivialement la clé d'un utilisateur local pour connexion à distance

- Encapsulation chiffrée du protocole X11 et gestion automatique Xauthority & `$DISPLAY`
- Redirection de n'importe quel port TCP/IP (transaction commerciale et monétaire, accès Intranet, serveur de mail, de News,...)
- Pas de confiance *a priori* au réseau
- Remplace les commandes `rlogin`, `rsh` (`ssh`), `rcp` (`scp`) et `ftp` (`sftp`)
- Éventuelle compression des données (marche mieux *avant* le chiffrement ☺)

- Couplage possible avec des calculettes d'authentification et S/Key
- Compatibilité avec l'authentification pare-feu TIS
- Ne pas oublier de supprimer l'usage de `rlogin`, `rsh`,...
- Essaye d'être facile à utiliser pour ne pas dégoûter de la sécurité !
- Distributions
  - L'original : `http://www.ssh.fi`, `ftp://ftp.cs.hut.fi/pub/ssh`
  - `ssh2` gratuit en utilisation non commerciale
  - `lsh` aussi v2 GNU en cours de développement

- Version libre OpenSSH basée sur `ssh1.27` mais aussi v2 `www.openssh.org`
- Introduction :

  `http://www-lns.mit.edu/compfac/ssh.html`

- PuTTY sous Windows

  `http://www.chiark.greenend.org.uk/~sgtatham/putty`

- `winscp` graphique sous Windows

  `http://winscp.sourceforge.net`

- `/`*`user`*`@`*`machine`*` :`... sous Emacs (le mode TRAMP gère aussi la gestion des versions à distance)

- FileZilla sous Windows accepte entre autre protocole SFTP `http://filezilla.sourceforge.net`

- URL `fish:` sous KDE

- De manière générale `lufs` permet de faire apparaître des fichiers distants comme un système de fichiers local sous Linux `http://lufs.sourceforge.net`

- ...

La sécurité n'a plus l'excuse de la complexité ☺

- `ssh`, `slogin`, `scp` : commandes de base. Peuvent être installées sous les noms de `rsh`, `rlogin` et `rcp`
  - Utilise les clés publiques DSA des machines distantes de `/etc/ssh_known_hosts` ou `~/.ssh/known_hosts` pour vérifier que la machine cible est bien la bonne
  - `~/.ssh/id_dsa` contient sa clé secrète DSA et `~/.ssh/id_dsa.pub` la clé publique correspondante
  - `~/.ssh/id_dsa.pub` doit être présent dans le `/.ssh/authorized_keys` distant pour autorisation
- `sshd` serveur à lancer en attente de connexion
  - `/etc/ssh_host_key` contient la clé secrète du serveur créée à l'installation

- `/etc/ssh_host_key.pub` contient la clé publique du serveur créée à l'installation. Récupérée par `make-ssh-known-hosts` pour permettre une authentification à la connexion
- `/etc/ssh_known_hosts` et `~/.ssh/known_hosts` permettent l'autorisation par machine via mécanisme `rhosts`
- `/.ssh/authorized_keys` contient les clés publiques RSA pour se connecter chez un utilisateur

- `ssh-keygen` crée sa double clé RSA personnelle protégée (chiffrée) par phrase secrète. Stockage d'un commentaire pour aider la mémoire ☺
- `make-ssh-known-hosts` interroge le DNS d'un domaine

pour construire la liste des machines. Interroge ensuite tous les serveurs `ssh` pour récupérer leur clé publique et construit le fichier `/etc/ssh_known_host`

- ⚠ ⚠ : comme la confiance est basée aussi sur les clés publiques, être sûr qu'on a les bonnes clés publiques. Problème de démarrage du processus...

- Interactions avec machines distantes
  - Administration système : connexions sans arrêt à machines distantes
  - Développeur : connexions à serveurs CVS ou SVN via `ssh` incessantes

  ⇝ Pénible de retaper sans arrêt phrases secrètes ☹
- Création entité authentification `ssh-agent`
  - Fournit clés secrètes aux `ssh`
  - Lancé au démarrage typiquement par gestionnaire de fenêtres
  - S'annonce via variables d'environnement `SSH_AUTH_SOCK` et `SSH_AGENT_PID`

- Alimentation et contrôle de l'agent via `ssh-add`
  - Sans option : rajoute identité(s) par défaut après saisie phrase(s) secrète(s)
  - `-L` affiche clés publiques servies
  - `-e` et `-s` pour gérer lecteurs de cartes d'authentification
  - `-x` verrouille agent avec mot de passe (temps du repas...) et `-X` déverrouille

  `man ssh-add`

- ∃ extensions de `ssh` qui utilisent PKI et X.509

Utilisation de ssh

`man ssh` : remplace `telnet`, `rsh` et `rlogin`

- Typiquement

  `ssh [`*`options`*`] [`*`nom`*`@]`*`machine`*

- Quelques options parmi nombreuses disponibles
  - `-X` autorise téléportation protocole affichage X11 via `ssh` de manière sécurisée : commande graphique lancée à distance affiche en local ☺
    Si machine distante corrompue, possibilité pirate de prendre contrôle écran local... ☹
  - `-C` comprime les communications
  - `-p` *`port`* utilise autre chose que le port TCP 22 (tunnels sécurisés...)

- `-L` [*bind_address*/]*port*/*host*/*hostport* téléporte de manière sécurisée une connexion TCP sur machine *locale* *port* vers *host* et port *hostport* *depuis* la machine *distante*
  Spécifier * ou plus précis (`localhost`...) dans *bind_address* pour restreindre connexions côté local
- `-R` [*bind_address*/]*port*/*host*/*hostport* téléporte de manière sécurisée une connexion TCP sur machine *distante* *port* *localement* vers *host* et port *hostport*
  Pour raisons de sécurité, écoute que sur interface locale sur machine distante. Spécifier * ou plus précis dans *bind_address* sinon
- `-A` téléporte service d'authentification de `ssh-agent`

- Pratique : permet d'enchaîner des `ssh` sans avoir à retaper des phrases secrètes ☺
- Si machine distante sous contrôle ennemis, utilisation du service d'authentification par ennemis ☹

  - `-4` force à utiliser IPv4
  - `-6` force à utiliser IPv6

Mettre options préférées dans `.ssh/config` :

```
Compression        yes
KeepAlive        no
ForwardX11        yes
# Pratique mais dangereux si la machine distante est piratée...
#ForwardAgent        yes
GatewayPorts        yes
```

Commandes interactives de ssh

- Interaction hors ligne avec système avec commandes en retour-chariot/newline + `~` (hérité de `telnet`)
- Quelques commandes
  - `~.` : déconnexion
  - `~^Z` : passe en tâche de fond
  - `~#` : affiche connexions téléportées
  - `~&` : passe en tâche de fond et déconnecte une fois connexions téléportées terminées
  - `~C` : rajoute/annule des téléportations de ports

Utilisation de scp et sftp

- `man scp` : remplace `rcp` pour copier fichiers entre machines/utilisateurs
  - Utilise `ssh` à distance
  - `scp [`*options*`] [[`*user*`@]`*host1*`:]`*file1* `[...] [[`*user*`@]`*host2*`:]`*file2*
- Quelques options
  - `-p` préserve dates d'accès, de modification, modes et utilisateurs si possible
  - `-r` copie récursive des répertoires
  - `-P` *port* utilise autre chose que port TCP 22
  - `-l` *bande-passante* limite le débit
- `man sftp` : remplace `ftp`

Utilisation de scp et sftp

- Pour nostalgiques de syntaxe `ftp` interactive...
- Utilise `ssh` qui lance un `sftp-server` à distance
- `sftp` *host*
- `sftp [[`*user*`@]`*host*`[:`*file* `[`*local-file*`]]]`
- `-b` *batchfile* exécute liste de commandes

Accès intranet ENSMP et ENST Bretagne depuis monde extérieur :

- ~/.ssh/config :

```
# Se connecter à ENSTBr via "ssh info"
Host info
        HostName enstb.org
        # Connexion via ssh vers machine réseau ENST Bretagne
        LocalForward 10022 gavotte.enst-bretagne.fr:22

# Se connecter indirectement à réseau interne via "ssh inte
Host interne
        HostName localhost
        Port 10022
        # All ports as 2xyzt
```

```
        # Accès aux News de l'ENST Bretagne
        LocalForward 20119 news.enst-bretagne.fr/119
        # Accès machine Windows via rdesktop localhost
        LocalForward 3389 taureau-tse.enst-bretagne.fr/3389
        # Pour envoyer des mails directement de l'intérieur
        LocalForward 20025 localhost/25
        # Proxy WWW pour accéder intranets ENST Bretagne
        LocalForward 28080 proxy.enst-bretagne.fr/8080

# Se connecter aux Mines via "ssh cri"
Host cri
        HostName ssh-cri.ensmp.fr
        # Intranet des Mines :
        # All ports as 3xyzt
```

```
# Accès aux News des Mines
LocalForward 30119 "news.ensmp.fr:119"
# Pour envoyer des mails directement de l'intérieur
LocalForward 30025 localhost/25
# Proxy WWW pour accéder intranets ENST Bretagne
LocalForward 38080 "www.ccf.ensmp.fr:80"
LocalForward 30389 "ldap.trad.fr:389"
LocalForward 32389 "ldap2.trad.fr:389"
```

- Accéder aux News, Mail et Forum sous Emacs/GNUS :
  ~/.gnus.el

```
(defun mail-method-enst-bretagne () "Post as enst-bretagne.fr"
  (interactive)
  (setq message-send-mail-function 'smtpmail-send-it
;; Assume a ssh tunnel from localhost:20025 to gavotte.enst-bretagne.fr
smtpmail-smtp-service 20025
```

```
;; For the enveloppe From:
user-mail-address "Ronan.Keryell@enst-bretagne.fr"
))
(defun mail-method-ensmp () "Post as cri.ensmp.fr"
  (interactive)
  (setq message-send-mail-function 'smtpmail-send-it
;; Assume a ssh tunnel from localhost:30025 to ssh-cri.ensmp.fr:25:
smtpmail-smtp-service 30025
;; For the enveloppe From:
user-mail-address "Ronan.Keryell@cri.ensmp.fr"
))
(setq
 ;; First the default SMTP host:
 smtpmail-default-smtp-server "localhost"

 ;; Plus de connexion directe aux Mines :
 gnus-nntp-server nil
```

```
;; Mes serveurs
rk-serveur-news-enstbr '(nntp
 "news.enst-bretagne.fr"
 ;; Assume a ssh tunnel from localhost:20119 to news.enst-bretagne.fr:
 (nntp-address "localhost")
 (nntp-port-number 20119))
rk-serveur-news-mines '(nntp
"Mines"
;; Assume a ssh tunnel from localhost:30119 to news.ensmp.fr:119:
(nntp-address "localhost")
(nntp-mail-method-enstbport-number 30119)
)
rk-serveur-forum-enstb '(nntp
 "Forum ENST Bretagne"
 (nntp-address "melimelo.enst-bretagne.fr")
 (nntp-port-number 7777)
 )
```

```
;; Où lis-je :
gnus-select-method  rk-serveur-news-enstbr
gnus-secondary-select-methods (list
                                rk-serveur-news-mines
                                rk-serveur-forum-enstb)
;; Différents serveurs pour poster les News :
gnus-post-method (list
                  rk-serveur-news-enstbr
                  rk-serveur-news-mines
                  rk-serveur-forum-enstb
                  )
)
```

Plan

- Connexions à distance (ssh, ftp...)
- Système d'impression (BSD, CUPS...)
- Systèmes de nommage
  - Service DNS pour la résolution des noms
  - Système de nommage NIS
- Partage de fichiers en réseau avec NFS
- Auto-montage
- Archivage des données
  - tar, cpio, pax, mt...
  - Archivage en réseau avec rsync, partimage
  - AMANDA

- *spool* : *Simultaneous Peripheral Operation On Line* : empile requêtes d'impression pour faire autre chose ⇝ impressions en différé
- ∃ Nombreux systèmes de gestion imprimante
  - BSD (`lpr`, `lpq`,...)
  - System V (`lp`, `lpstat`,...)
  - Windows & SMB
  - CUPS
  - ...
- Imprimantes locales : impressions sont mises en attente de libération de l'imprimante dans une zone de spool `/var/spool/lp`, `/var/spool/lpd`, `/var/spool/cups`...

- Imprimantes distantes : mise en attente dans `/var/spool/...` et envoi par protocole BSD, TCP *pass-through*, IPP... sur le serveur de l'imprimante distante, voire l'imprimante elle-même (mais implémentation parfois fantaisiste des protocoles réseau...)
- ⇝ Penser à avoir de gros `/var/spool/`...
- Installation par outils graphiques ou textuels (`lpadmin`)
- ∃ Alternative plus moderne libre : CUPS

Base de donnée dans

- `$HOME/.printers`
- `/etc/printers.conf`
- Système « canal historique » inspiré des `termcap` et autres `terminfo`...

```
# The default printer:
_default:\
  :use=lw-d3-etage

# All the printers:
_all:\
  :all=copieur-d3-rdc,lw-d109,lw-d3-etage,lw-rdc,lw-rdc-hall,DJ1

lw-d3-etage:\
```

```
:bsdaddr=lw-d3-etage.priv.enst-bretagne.fr,lp:\
:description=Imprimante HP double face de l'étage:
```

modifiable aussi par outils graphiques et `lpdadmin`)

- Ressource NIS `printers.conf.byname` pour distribuer liste imprimante
- Ressource NIS+ et FNS
- Accès direct via

  `lpr -P` *`serveur:imprimante fichier`*

Choix de l'imprimante par défaut

- Variables environnement `PRINTER` et `LPDEST`
- Recherche d'une imprimante `_default` dans les fichiers précédents

Contrôle imprimante à la System V

- `lpstat -p` *`imprimante`* donne des informations sur l'*`imprimante`*
- `accept` *`imprimante`* accepte les demandes d'impression
- `reject -r` *`une-raison imprimante`* n'accepte plus les demandes d'impression
- `enable` *`imprimante`* permet l'impression
- `disable -r` *`une-raison imprimante`* arrête l'impression
- `cancel -u` *`user`* `|` *`request-id-list`* `|` *`imprimante`* annule des travaux d'impression
- `lpmove` *`impr-src impr-dst`* transfère les impressions depuis une imprimante vers une autre en faisant un `reject` *`impr-src`*

Contrôle imprimante à la System V

- `lpadmin -A` contrôle la marche à suivre en cas d'alerte
- `lpadmin -u allow:`*`user-list`* autorise des utilisateurs
- `lpadmin -u deny:`*`user-list`* interdit à des utilisateurs
- `lpshut` arrête le système d'impression
- `lpsched` démarre le système d'impression
- ⇝ Méthodes « canal historique »...

- Puis arriva CUPS...
- Base produit commercial d'Easy Software Products (ESP Print Pro)
- Gestion de files d'attente
- Utilise Internet Printing Protocol (IPP) TCP port 631
- Multiprotocole : IPP, LPD, LP, SMB, HP JetDirect...
- Gère imprimantes PostScript
- Exploite description fine imprimante PostScript au format PPD (PostScript Printer Description) ⇝ choix des paramètres imprimante (couleur, définition, double face, agrafage...) et menus
- Gère classes d'imprimantes (tolérance aux pannes, répartition de charge...)

- Gère quotas, droits, statistiques
- Mode commande à la System V
- Repris dans MacOS X
- Paquets Debian utiles : `printconf`, `cupsys`, `cupsys-bsd`, `cupsys-client`, `gnome-cups-manager`, `kdeprint` (`kprinter`), `cups-pdf`...

`http://www.cups.org`

- `kprinter` avec KDE
- `gnome-cups-manager`, `gnome-cups-add` avec GNOME
- `xpp` avec X11 de base

CUPS et BSD

- Permet d'utiliser protocole BSD
- Paquet Debian `cupsys-bsd` pour avoir commandes BSD canal historique
  - `lpr [-P` *`imprimante`*`]` : imprime
    - `-o` *`option`* permet de changer comportement imprimante

      `-o PrintoutMode=Photo -o Duplex=DuplexNoTumble`
  - `lpq` : affiche travaux en attente
  - `lprm` : supprime travaux
  - `lpc` : contrôle files d'impression

Interface WWW CUPS

- IPP protocole basé sur HTTP mais port TCP 631
- ⇝ Utilisation aussi comme interface de configuration ! ☺

  `http://localhost:631`
- Gestion
  - Travaux
  - Files d'attentes
  - Imprimantes (installation, contrôle...)
  - ... Documentation ! ☺

Le plus d'expressivité !

- `lp [-d destination] [-o option]` : imprime
- `cancel` annule impression
- `lpstat` affiche états imprimantes, travaux & classes
  - `-t` affiche informations sur tout
  - `-d` indique quelle est imprimante par défaut
  - `-p [imprimantes]` affiche état imprimante
- `lpoptions` affiche et définit options et paramètres par défaut imprimante *pour soi*
  - `-l` affiche options
  - `-d destination [-o option=valeur]` en tant qu'imprimante par défaut

- `-p` *`destination`* `[-o` *`option=valeur`*`]` rajoute options par défaut
- `-r` *`option`* supprime options
- `-x` supprime toutes options
- Stocké dans `~/.lpoptions`
- `/etc/cups/lpoptions` pour toute une machine

- `lpadmin` administre imprimantes et classes
  - `-d` *`destination`* choisi imprimante par défaut (si pas de `lpoptions`)
  - `-p` *`imprimante`* configure imprimante
    - `-c` *`classe`* dans une classe

- `-m` *`modèle`* modèle PPD d'imprimante (fichier déjà disponible dans `/usr/share/cups/model`)
- `-P` *`fichier-PPD`*
- `-o` *`option`* choisit une option globale

▶ `-x` *`destination`* supprime des

Mise à jour fichier `/etc/cups/printers.conf` et répertoire `/etc/cups/ppd`

- `lppasswd` gère mots de passe associés à imprimantes, classes...

- Besoin pour imprimante donnée du bon PPD (PPD précis ⇝ contrôle fin imprimante)
- Base dans `http://www.linuxprinting.org`
- Si pas imprimante PostScript, utilise GhostScript pour faire *rasterisation*
- Exemple d'installation Laser PostScript couleur
  - Recherche de `.ppd` dans CD-ROM installation... Windows ! ☺

```
cp /cdrom/English/Drivers/Win2000_XP/PS/HP5500_6.ppd /usr/share/cups/model/HP/
/usr/sbin/lpadmin -p couleur -L "D3-126 1er étage sud Couleur" \
   -D "Imprimante HP LaserJet 5500dn couleur double face de l'étage" \
   -E -v socket://lw-d3-126-couleur.priv.enst-bretagne.fr -m HP/HP5500_6.ppd
lpoptions -p couleur -o Duplex=DuplexNoTumble -o Duplexer=True
lpoptions -p couleur/duplex -o Duplex=DuplexNoTumble -o Duplexer=True
lpoptions -p couleur/duplex_landscape -o Duplex=DuplexTumble -o Duplexer=True
lpoptions -p couleur/simplex -o Duplex=None -o Duplexer=True
```

- Exemple d'installation imprimante jet d'encre non PostScript couleur
  - Récupération du PPD de

    `http://www.linuxprinting.org/show_printer.cgi?recnum=HP-Offic`

    et mis dans

    `/usr/share/cups/model/HP-OfficeJet_7130-hpijs.ppd`
  - Installation

```
/usr/sbin/lpadmin -p maison -L "Bureau Keropars" \
    -D "HP OfficeJet 7310 serial=MY49MG91V60407 double face" \
    -E -v usb:/dev/usb/lp0 -m HP-OfficeJet_7130-hpijs.ppd
```

  - Via

    `http://localhost:631/admin/?op=config-printer&printer_name=ma`

    passage en mode double face par défaut pour tout le monde (modification du fichier `/etc/cups/ppd/maison.ppd`)

Détection imprimantes dans CUPS

- Par défaut chaque serveur fait broadcast IPP

```
BrowseProtocols all
BrowseAddress @LOCAL
BrowseAllow .enstb.org
BrowseAllow keryell.pck.nerim.net
```

- Clients écoutent
- Possibilité de restreindre accès

```
<Location />
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
Allow From .enstb.org
Allow From .enst-bretagne.fr
```

```
Allow keryell.pck.nerim.net
</Location>
<Location /admin>
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
</Location>
```

- Contacter en plus serveurs spécifiques

  `BrowsePoll ipp.enstb.org`

- Chaque serveur peut faire proxy (cas routeur du RIRE/enstb.org)

Configuration globale dans `/etc/cups/cupsd.conf`

- Connexions à distance (ssh, ftp...)
- Système d'impression (BSD, CUPS...)
- Systèmes de nommage
  - Service DNS pour la résolution des noms
  - Système de nommage NIS
- Partage de fichiers en réseau avec NFS
- Auto-montage
- Archivage des données
  - tar, cpio, pax, mt...
  - Archivage en réseau avec rsync, partimage
  - AMANDA

- Trop d'informations spécifiques à 1 site pour être dupliquées sur chaque machine
- Besoin de pouvoir remettre à jour les informations instantanément sur toutes les machines
- Paramétrage de la source des information pour les `get`*X*`by`*Y*`()` (`gethostbyname()`, `getpwnam()`,...)
- Différents systèmes possibles sélectionnés par type de ressources selon `/etc/nsswitch.conf`
  - Fichiers
  - NIS
  - NIS+
  - DNS : système de nommage des machines sur Internet. Plutôt réservé à la ressource `hosts`

- LDAP (sur TLS de préférence pour raisons de sécurité) : annuaire hiérarchique, version allégée de X.500
- Federated Naming Service (FNS) : méthode de nommage fédérant NIS+, NIS, fichiers, DNS, et X.500/LDAP. API XFN dépassant les `getX by Y()`

⇝ `man nsswitch.conf`

- Pas un système de nommage réseau
- À dupliquer sur toutes les machines... mais robuste
- Nommage en réseau « à la main » : mettre en place un système de synchronisation des fichiers depuis une base centrale
- `/etc/nsswitch.conf` typique :

```
passwd:      files
group:       files
hosts:      dns files
ipnodes:     files
networks:    files
protocols:   files
rpc:         files
ethers:      files
netmasks:    files
bootparams:  files
```

```
publickey:   files
netgroup:    files
automount:   files
aliases:     files
services:    files
```

```
sendmailvars:   files
printers:       user files
auth_attr:   files
prof_attr:   files
project:     files
```

- Distribue des tableaux associatifs
- Pas très sécurisé en local car les mots de passe chiffrés sont accessibles pour essais de craquage
- Système très répandu
- Choisir un nom de domaine NIS unique sur son réseau. Par exemple nom de domaine Internet
- Vérifier que `/etc/nodename` contient bien le nom de la machine
- Mettre dans `/etc/defaultdomain` le nom du domaine
  - Est utilisé par le système pour la commande `domainname`
  - `domainname` permet de connaître ou modifier le nom de domaine NIS

- Choisir le serveur NIS maître et les serveurs esclaves
- Faire `/usr/lib/yp/ypinit -m` sur le serveur maître qui demande la liste de tous les serveurs
- Si `/etc/resolv.conf` existe sur le serveur les NIS font suivre les requêtes `hosts` au DNS
- Faire `/usr/lib/yp/ypinit -s` *maître* sur serveur esclave
- Sur les clients, installation paquet Debian `nis` fait le travail
- Remplacer les `/etc/nsswitch.conf` avec contenu plus spécifique

```
passwd:   compat
group:    compat
shadow:   compat
netgroup: nis
```

`compat` permet astuces du style

```
+miquels::::::
+ed::::::
+dth::::::
+@labo::::::
-@eleves::::::
+:*::::::/etc/NoShell
```

où `@...` sont des `netgroup`

- `/var/yp/Makefile` contrôle les tables NIS exportées. Éditer pour rajouter ses propres ressources. Faire `make` dans `/var/yp` pour propager les ressources lorsque les fichiers de référence sont modifiés
- `/etc/ypserv.securenets` restreint l'accès des NIS

- `ypcat [-k]` *`table`* permet d'afficher le contenu d'une table NIS
- `ypcat -k ypservers` affiche liste des serveurs NIS
- `ypwhich` donne le serveur actuellement utilisé
- `ypwhich -m` *`table`* indique le serveur maître d'une table
- `ypwhich -x` donne la liste des alias

- Organisation hiérarchique de l'espace de nommage
- Distribue tout type d'information (binaires...)
- Serveurs secondaires pour répartition de la charge et secours
- Mécanisme d'authentification et d'autorisation tables par tables
- Mots de passes chiffrés pas lisibles par les utilisateurs
- Système plutôt Sun
- Supplanté par LDAP

- Adresses IP de 32 bits pour numéroter les machines sur Internet $\equiv$ 10 chiffres décimaux
- Utilisation intensive pour le courrier, WWW, news, `telnet`, `ftp`,...
- IPv6 sur 128 bits $\equiv \rightsquigarrow$ 39 chiffres décimaux à retenir...
- Nécessité de noms mnémotechniques et plus commerciaux
- Conversion entre numéros IP et noms de machines et autres
- Nécessite un visibilité mondiale
- Offrir une distribution spatiale
- Gérer la cohérence temporelle

- Besoin d'une bonne tolérance aux pannes

Domain Name System (DNS)

Données cruciales...

- Importance stratégique
- DNS en panne : perte de services importants
- DNS corrompu : système délirant
- DNS piraté : pages WWW pointant vers la concurrence
- Bien choisir ses noms (marques, lisibilité...)
- Bien payer à temps ses enregistrements (si payants)
- Monde où la carte banquaire est reine... Attention aux retards administratifs ! Sinon ☹
- ∃ boîtes internationales de cyber-racket qui rachètent un domaine dès qu'il devient libre (si on a oublié le loyer), font pointer vers des sites pornographiques et veulent le revendre cher ☹

- ARPAnet : quelques machines au début
- Toutes les informations sur les nœuds du réseau étaient dans LE fichier `HOST.TXT`, RFC 952

```
NET : 198.49.236.0 : PENSACOLANET2 :
GATEWAY : 26.10.0.14, 147.36.15.1 : PIRMASENS-GW1.ARMY.MIL : CIS
HOST : 134.229.2.2 : PENS-EMH1.NAVY.MIL : ATT-3B2 : UNIX : X.25,
HOST : 134.124.40.5 : WHALENS.UMSL.EDU :: AIX : TCP/TELNET,TCP/F
HOST : 137.194.160.1 : ULYSSE.ENST.FR : SUN : UNIX ::
```

- Maintenu par le `Network Information Center` au SRI
- Récupéré périodiquement par les nœuds du réseau
- Problème avec $\nearrow$ nombre machines
  - Chaque modification/ajout de machine $\rightsquigarrow$ mail au SRI

- Mise à jour ⇝ transfert du fichier vers nombreuses machines ↘ performance du réseau
- Conflits de noms globaux
- Problèmes de cohérence entre les copies existantes

- Toujours dans UNIX !
  - `gettable` : récupère `HOST.TXT`
  - `htable` : `HOST.TXT` ⇝ `/etc/hosts` et autres

⇝ Trouver autre chose...

Naissance du DNS

- Trouver un nouveau système
- Extensible
- Sans goulet d'étranglement
- Distribué
- Administration locale décentralisée
- ⇝ RFC 882 et RFC 883 en 1984
- Réalisation de JEEVES
- Réalisation de BIND sur UNIX 4.3BSD

Principe du DNS

- Hiérarchiser les espaces de nommage
- Contrôle local sur son propre morceau
- Robustesse par réplication
- Performances par cache des données
- Communication par mécanisme client/serveur : resolver/serveur de nom

Hiérarchie de nommage

Système de fichiers UNIX

Hiérarchie du DNS

- Nommage unique du chemin même si un sous-chemin ou une feuille sont identiques
- Mécanisme similaire aux liens : les alias (liens symboliques) ou les réplications (liens *hard*)

Hiérarchie de nommage

- Montage d'un disque ou d'un système de fichier sur un serveur distant : reléguer un sous-domaine à un autre serveur DNS
- Montage possible d'un disque depuis plusieurs machines pour résister aux pannes : plusieurs serveurs DNS peuvent servir un sous-domaine

Hiérarchie de nommage

Système de fichiers UNIX

Hiérarchie du DNS

- Chaque feuille contient l'information de traduction telles que
  - Numéro IP

- Type de matériel
- Comment envoyer le mail
- ...

- Un nœud non feuille représente un domaine mais peut aussi être un nom de domaine de machine
- Hiérarchie logique : pas de relation physique (géographique...) a priori

- « . » : *top-level domain*, domaine racine
- Domaine de premier niveau
  - `com` commerciaux
  - `edu` organismes d'éducation américains (universités)
  - `gov` organismes gouvernementaux USA
  - `mil` organismes militaires USA
  - `net` organismes de gestion de réseaux
  - `org` organismes non-commerciaux
  - `int` organismes internationaux
  - `arpa` transition ARPAnet⟶Internet + traduction inverse
  - Tendance au flou et au débordement dans les domaines `com`, `net` et `org`...

- Très américain : historiquement ARPAnet...
- Nouveau : `.biz`, `.info`,... : Cf. `http://www.icann.org`
- Domaines par pays quasi-ISO 3166
  - `fr`
  - `de`
  - `uk` (et non `gb`)

- Domaine de second niveau
  - `com.au`, `edu.au` comme « . »
  - `ensmp.fr` : à plat dans `.fr`
  - Hiérarchisé dans `.fr` :
    - `gouv.fr` gouvernement français

- `tm.fr` marques déposées en France
- `asso.fr` associations loi 1901
- ...

- 3ème niveau, etc.

RFC 1035

- Noms séparés par des « . ». Taille du tout ≤ 255
- Taille de chaque nom $\leq$ 63 caractères ASCII (lettres, chiffres et « - » (pas en première ni dernière position), premier caractère forcément une lettre)
- Égalité entre minuscule et majuscule
- Concaténation d'au plus 127 noms
- Nom absolu (non ambigu...) si terminé par « . » : FQDN
  Fully Qualified Domain Name
  Supposons l'existence de `cs.ensmp.fr` (Computer Science)
  Qui est `cs` ?

- `cs.` (Tchécoslovaquie) ?
- `cs.ensmp.fr.` (si on est dans le domaine `ensmp.fr`) ?
  Dernier par défaut

- Domaine ≡ sous-arbre de l'espace de nommage
  - `···.ensmp.fr`
  - `···.org`
  - `···.enstb.org`
  - `···.rire.enstb.org`

Délégation

- Réalise la hiérarchisation administrative
- Sous-domaines gérés par d'autres organismes responsables de leur propres données et de leurs propres délégations
- Le domaine parent n'a que des pointeurs vers les DNS gérant les sous-domaines
- `fr.` a un pointeur `ensmp` vers les DNS de l'École des Mines de Paris
- Limite implicite dans le nombre (127) mais pas dans l'enchaînement des délégations

Zones

Point de délégation dans la hiérarchie DNS

- **Zone** ≡ **portion du domaine** gérée effectivement par un serveur
- Un serveur contient les données de son/ses domaine(s) : la/les *zone*(s) : il fait **autorité** en la matière (*authoritative*)
- Un domaine est divisé en plusieurs zone s'il y a **délégation**
- Un serveur **maître primaire** charge les données depuis un fichier local (« base de données »)
- Un serveur (**esclave** ou **maître secondaire**) transfère au démarrage la zone depuis un serveur de référence (serveur maître) qui fait autorité
- Un serveur peut faire autorité sur plusieurs zones

Système de résolution

- Programme client ou bibliothèque de résolution (*resolver*)
- Interroge *un* (son) serveur de nom
- Interprète les réponses (numéro IP, erreur,...)
- Renvoie l'information au client (`ssh`, navigateur, `ftp`,...)
- Un serveur de nom est *aussi* capable de résoudre les noms en se promenant dans la hiérarchie de serveur pour les domaines dont il n'a pas autorité
- Problème : où commencer la recherche ?
  Dans une liste de serveurs racine (*hint*) !

- Demande de résoudre *récursivement* `www.amanda.org` qui demande au serveur de nom local

Question du serveur de nom local	*Serveur de*	*Répon*
`www.amanda.org` ?	« . »	Aller voir serveur de `or`
`www.amanda.org` ?	« `org.` »	Aller voir serveur de `amanda.or`
`www.amanda.org` ?	« `amanda.org.` »	nom canonique `spiderman.amanda.or`
`spiderman.amanda.org` ?	« `amanda.org.` »	`208.213.83`

- Si le système de résolution ne demandait pas la récursion, il devrait *itérer* lui-même...
- Économie :
  - le serveur contacte le serveur *connu* le plus proche

dans la hiérarchie au lieu d'un serveur racine

- exemple
  - `deauville.ensmp.fr` demande qui est `www.enst.fr`
  - Demande au serveur de `fr.` plutôt qu'à un serveur racine (dénis de service ☹)

- Seul le serveur de nom local (ou celui attaché au resolver) fait de la récursion
- Les serveurs racines ne font *plus* de récursion pour des raisons de performances... En plus cela permet de ne pas cacher de l'information et donc d'économiser de la mémoire !
- Si plusieurs serveurs de noms possibles : choix par BIND en fonction du temps d'aller-retour des paquets DNS

- Besoins
  - Autorisation d'une connexion `rlogin` à partir d'un nom dans son `.rhosts`
  - Messages de debug plus humains
  - ...
- Comment avoir la traduction inverse des mécanismes précédents ?
- Traduction nom vers adresse implémentée et efficace dans le DNS
- Comment adapter le système existant ?

Traduction numéro IP vers nom de domaine

- Idée : découper une adresse IP de 32 bits 4 paquets de 8 bits codés en décimal $x.y.z.t$
- Créer un domaine spécifique `in-addr.arpa.` pour la traduction inverse
- Faire une recherche $x.y.z.t$`.in-addr.arpa.` ?
  - `deauville.ensmp.fr` $\equiv$ `192.54.172.242`
  - `192.54.172.242.in-addr.arpa.` ?
  - Réseaux : hiérarchisé par le poids fort (sous-réseaux...) : 1 réseau des Mines : `192.54.172.*`
  - Tous les noms de machines seraient dans `192.54.172.*.in-addr.arpa.` ?
  - Mauvais ! Il faudrait être responsable du haut de la hiérarchie... ☹

Traduction numéro IP vers nom de domaine

- Idée : inverser les nombres de l'adresse
  - Recherche de t.z.y.x.`in-addr.arpa.`
  - `242.172.54.192.in-addr.arpa.` ?
  - Mines responsable de `*.172.54.192.in-addr.arpa.` bas de la hiérarchie
- `http://www.ipindex.net/`
  `http://blues.eurovia.es/mirrors/www.ipindex.net` donne une idée de l'usage des adresses IP
- Services de géoréférence : `http://www.maxmind.com`
- Comment faire du CIDR alors que tout est fait pour des classes A, B ou C ? Cf. plus loin...

Mécanisme de cache

- Problème : goulet d'étranglement aux serveurs racines à chaque requête ☹
- Idée : mécanisme de cache ☺
- Retenir dans une mémoire les traductions les plus souvent demandées
- Retenir aussi le fait que certaines traductions n'existent pas (erreurs répétitives...) : cachage négatif
- Retenir toutes les informations aperçues lors des recherches récursives : cela peut servir plus tard (liste de serveurs faisant autorité, leurs numéros IP,...)

  ⇝ Attaques par pollution si on accepte *toute* information sans vérification si serveur fait autorité ☹

Mécanisme de cache

- Permet de survivre un peu mieux à une coupure réseau ou à des pannes de DNS distants...
- Comment propager les mises à jour des données aux caches des serveurs ? Trop de caches de serveurs et pas de mécanisme hiérarchique de diffusion
- Rajout d'une durée de vie (TTL *Time To Live*) associé à une zone choisie par l'administrateur
- Si la durée de vie d'une donnée est dépassée, la donnée est effacée du cache
- Compromis à trouver sur le TTL
  - Bonnes performances $\rightsquigarrow$ TTL $\nearrow$
  - Propagation des mises à jour rapides $\rightsquigarrow$ TTL $\searrow$

Mécanisme de cache

- TTL pour les réponses négatives fixé à 10 minutes par défaut
- Même avec les caches les serveurs racines reçoivent des milliers de requêtes par seconde... mais on y survit !

RFC 1035

- Définit une représentation textuelle aux paquets binaires du protocole (requête dans outils, réponses, fichiers de données,...)
- `CLASS` définit la classe d'utilisation de l'enregistrement (DNS plus large qu'Internet)
  - `IN` Internet
  - `CS` CSNET (obsolète)
  - `CH` CHAOS (MIT)
  - `HS` Hesiod
- `RR` (`Resource Record`) contient un enregistrement d'information de différents types avec une durée de vie optionnelle en seconde (32 bits) :

Types de ressources du DNS

- `A` adresse de machine

  `www IN A 192.54.172.231` Une machine avec plusieurs adresse a plusieurs `A RR`

- `NS` nom d'un serveur de nom faisant autorité pour délégation

  `trad IN NS chailly.ensmp.fr.`

- `CNAME` définit un alias qui a pour *nom canonique*...

  `www.kazimodal CNAME kazimodal`

  Un alias ne doit pas être utilisé en partie droite d'un RR afin de limiter les récursions

- `SOA` *start of a zone of authority*
  - *`MNAME`* nom du serveur de référence (maître)

- *RNAME* nom de domaine encodant l'adresse mail en `destinataire.un.domaine` interprété en `destinataire@un.domaine` pour Internet
- *SERIAL* numéro de série sur 32 bits monotone croissant modulo 32 bits utilisé pour avertir des mises à jour. Ne pas oublier d'augmenter ce nombre sur un maître après chaque modification si on veut que les modifications soient propagées...
  Valeur 0 spéciale de resynchronisation : propage systématiquement aux serveurs secondaires
- *REFRESH* temps en seconde (32 bits) avant un rafraîchissement de zone
- *RETRY* temps en seconde (32 bits) avant un autre

essai de rafraîchissement de zone qui a échoué

- *EXPIRE* temps en seconde (32 bits) avant que la zone ne soit plus considérée comme faisant autorité
- *MINIMUM* durée de vie (TTL) (32 bits) en seconde des données cachées négativement

```
@ IN SOA chailly.ensmp.fr. keryell.chailly.ensmp.fr. (
        98120200          ; Serial
        21600    ; Refresh 6 hour (nic.fr said...)
        3600     ; Retry   1 hour
        3600000  ; Expire  1000 hours
        600  )   ; Cachage négatif 10 minutes
```

- `WKS` déclare les *well known service* fournis

- `PTR` pointeur dans nom de domaine, typiquement pour la traduction adresse vers nom dans `in-addr.arpa`
  `1 IN PTR routeur-10.4.0.ensmp.fr.`
- `HINFO` informations sur le CPU et l'OS de la machine
- `MX` définit la machine vers qui doit être envoyé le courrier avec un ordre de priorité décroissant (0 $\equiv$ en premier)
- `TXT` de l'information textuelle quelconque

Extensions expérimentales dans

- RFC 1183 : DCE, nom du responsable, X25, ISDN (Numéris)
- RFC 1664 : X400

RFC 1035 section 5

- Utile pour lire le contenu des caches
- Sert à définir une zone dans BIND
- Orienté ligne
- mais `(···)` permet d'écrire un enregistrement sur plusieurs lignes
- `;` commentaire
- `@` représente l'origine courante de la zone. Utilisée dans les noms relatifs (ne terminant pas par « . ») ≈ répertoire courant (« . ») dans un système de fichiers
- `$ORIGIN` *domain-name* `[`*comment*`]` change l'origine courante de la zone ≈ `cd` sous Unix

- `$INCLUDE` *file-name* [*domain-name*] [*comment*] inclut un fichier et définit son (et seulement son) origine courante

- Un enregistrement a la forme
  - *domain-name rr* [*comment*]
  - <blank> *rr* [*comment*] pour ajouter l'enregistrement au nom de domaine précédent
  - *rr* ont la forme
    - [*TTL*] [*class*] *type RDATA*
    - [*class*] [*TTL*] *type RDATA*

    Les *TTL* et *class* manquants prennent les mêmes valeurs que celles des enregistrements précédents

    - Certains enregistrements peuvent avoir plusieurs valeurs

- Exemple de routeurs ou de répartition de charge : plusieurs RR A paramétrable en :
  - Réponse tourniquet (répartit la charge sur plusieurs serveurs)
  - Réponse la plus proche en terme de réseau (diminue la pression réseau)

▶ `$TTL` *TTL* fixe le TTL par défaut pour les enregistrements suivants

- Pour le cache (accessible par `rndc dumpdb`) il faut aussi noter la non existence

```
SPOOL.MU.EDU.          8284    AAAA   ;-$NXRRSET
; authauthority
                       8284    A6     ;-$NXRRSET
```

```
; authanswer
```

Fichier /etc/resolv.conf

- Fichier de configuration du resolver : explique à sa machine comment faire les traductions
- `man resolv.conf` (resolver de Sun) ou `man -s 5 resolver` (resolver BIND)
- Options
  - `nameserver` *`adresse`* précise le serveur de nom à utiliser
  - `domain` *`name`* définit le nom de domaine local rajouté aux noms relatifs
  - `search` *`searchlist`* définit une liste de domaines (séparés par des espaces) essayés lors d'une résolution de nom relatifs

- ▶ `sortlist` *`addresslist`* trie les réponses dans l'ordre de préférence des numéros de réseaux donnés
- ▶ `options` *`optionlist`* précise certaines options fines `options ndots :2` : recherche des noms sans les considérer comme locaux s'ils ont 2 « . » ou plus

- Si un nom complet local est défini avec la commande `hostname`, le domaine peut ne pas être précisé dans `/etc/resolv.conf`
- Vérifier que la syntaxe est correctement comprise avec un `set all` dans `nslookup`

```
nameserver 192.44.75.10
nameserver 192.108.115.2
nameserver 192.44.77.1
```

```
search enst-bretagne.fr enstb.org ensmp.fr trad.org
domain enst-bretagne.fr
```

On peut prendre en compte un fichier d'alias de noms en initialisant la variable d'environnement `HOSTALIASES` à ce nom de fichier

Fichier /etc/nsswitch.conf

- Précise l'utilisation des systèmes de nommage par ressource
- Ressources `aliases`, `automount`,...,*`hosts`*,...
- Systèmes de nommages : `files`, `nis`, `nisplus`, `dns`, `compat`, `xfn`
- Exemple

  ```
  hosts : xfn dns nis [NOTFOUND=return] files
  ```

- `man nsswitch.conf`

Vers un resolver indépendant

- Resolver standard :
  - Bibliothèque lié avec processus utilisateur
  - Nouveaux protocoles (chaînes de bits et DNAME IPv6, DNSSEC,...)
  - Devient trop complexe et trop lourd
- Idée avoir un processus indépendant qui factorise le travail de résolution
- Accessible par bibliothèque simplifiée (*light-weight resolver*) par UDP port 921 sur `localhost` (résout problèmes d'insécurité)
- Travail effectué par processus démon `lwresd` configuré via `/etc/lwresd.conf` ou BIND avec directive `lwres`

- Nécessité d'avoir des outils de mise au point
- Besoin d'interroger directement un DNS
- Court-circuite la résolution classique par le système d'exploitation (NIS, `/etc/hosts`, `/etc/resolv.conf`)
- Possibilité de demander toute une zone
- Permet de simuler des requêtes inter-DNS
- Peut passer outre les dépassements de temps de réponse

Programme maintenu par l'équipe de BIND... donc à préférer

- `man dig`
- Interroge par défaut les serveurs de nom de `/etc/resolv.conf` mais ignore `search` ou `domain`
- `dig [@server] [-f query-file] [-k key-file] [-y name :key] [-i] [[-x] domain [query-type] [+query-option] [-dig-option] ]*`
  - *query-type* : `any`, `a`, `sig`, `mx`, `axfr` (transfert de zone), `ixfr=N` (transfert de zone incrémentale depuis le n° de série *N*),... Peut aussi être précisé par `-t query-type`
  - `-x` devant une adresse demande automatiquement la requête inverse dans `in-addr.arpa` et PTR ou

`ip6.arpa`> Rajouter `-i` pour vieilles requêtes IPv6 dans `ip6.int`

- Plein d'options
  - `+[no]tcp` : utilise TCP au lieu d'UDP
  - `+domain=`*somename* : utilise un domaine par défaut
  - `+[no]search` : utilise la liste de domaines de `resolv.conf`
  - `+[no]cdflag` : positionne le bit CD (*checking disabled*) pour éviter les vérifications DNSSEC
  - `+[no]recurse` : positionne le bit RD (*recursion desired*) demandant au serveur la recherche récursive

- `+[no]nssearch` : affiche le SOA du domaine selon tous les serveurs DNS du domaine
- `+[no]trace` : trace récursivement la requête depuis les serveurs racines
- `+[no]short` : moins verbeux
- `+[no]dnssec` : demande à utiliser DNSSEC

▶ *key-file* contient une clé pour DNSSEC

▶ *name* :*key* idem en ligne de commande car `ps` peut l'afficher...

- Plein d'autres options...
  `dig @dns.princeton.edu cri.ensmp.fr any +norecurse`
- Notation `-x 128.9.0.32` à la place de `32.0.9.128.in-addr.arpa`

Programme dig

- Pour avoir le contenu d'une zone :

  `dig @dns-cri.ensmp.fr enstb.org axfr`

  ...si autorisé !
- `dig --help` et `dig -h` plus complet
- Possible de mettre des options dans son `${HOME}/.digrc`

- BIND est le gestionnaire de DNS le plus connu et probablement un des plus complets
- Fonctionne sur Unix et Windows 2000
- DNS Dynamic Updates RFC 2136
- DNS Change Notification RFC 1996
- Nouvelle syntaxe des fichiers de configuration avec la version 8/9 par rapport à la version 4 et :
  - Système de log flexible par catégories
  - Listes d'accès par adresse IP sur les requêtes, transferts de zones et mises à jours pour chaque zone
  - Transferts de zones plus efficaces

- Meilleures performances pour les serveurs gérant des milliers de zones
- Sécurité
- Parallélisé pour multi-processeurs
- Plein de bugs corrigés...

- Possibilité de convertir un fichier de configuration version 4.9.x en version 8/9 via `contrib/named-bootconf/named-bootconf.sh`
- $\exists$ Nombreux outils d'aide à génération de fichiers de zone

- Connexions à distance (ssh, ftp...)
- Système d'impression (BSD, CUPS...)
- Systèmes de nommage
  - Service DNS pour la résolution des noms
  - Système de nommage NIS
- Partage de fichiers en réseau avec NFS
- Auto-montage
- Archivage des données
  - tar, cpio, pax, mt...
  - Archivage en réseau avec rsync, partimage
  - AMANDA

- Si pas déjà installé...
- Un extrait de ce qui est en rapport avec `bind` :
  `apt-cache search bind` donne entre autres :

```
autodns-dhcp - Automatic DNS updates for DHCP
bind9 - Internet Domain Name Server
bind9-doc - Documentation for BIND
bind9-host - Version of 'host' bundled with BIND 9.X
dhcp-dns - Dynamic DNS updates for DHCP
dlint - Checks dns zone information using nameserver lookups
dnsmasq - A caching DNS forwarder.
dnsutils - Clients provided with BIND
host - Utility for Querying DNS Servers
ldap2dns - LDAP based DNS management system.
libbind-confparser-perl - Parser class for BIND configuration fi
libbind-dev - Static Libraries and Headers used by BIND
```

```
liblwres1 - Lightweight Resolver Library used by BIND
lwresd - Lightweight Resolver Daemon
nslint - Lint for DNS files, checks integrity
```

- Une installation :

```
amd1:~/fai# apt-get install bind9 bind9-doc bind9-host dnsutils
Reading Package Lists... Done
Building Dependency Tree... Done
Sorry, bind9-host is already the newest version.
Sorry, dnsutils is already the newest version.
The following NEW packages will be installed:
  bind9 bind9-doc
0 packages upgraded, 2 newly installed, 0 to remove and 10  not
Need to get 0B/387kB of archives. After unpacking 943kB will be
Selecting previously deselected package bind9.
(Reading database ... 90425 files and directories currently inst
```

```
Unpacking bind9 (from .../b/bind9/bind9_9.2.1-4_i386.deb) ...
Selecting previously deselected package bind9-doc.
Unpacking bind9-doc (from .../bind9-doc_9.2.1-4_all.deb) ...
Setting up bind9 (9.2.1-4) ...
Starting domain name service: named.

Setting up bind9-doc (9.2.1-4) ...
amd1:~/fai# ps augxww|grep named
root     17192  0.0  0.4 10156 2132 ?        S    16:08   0:00 /
root     17193  0.0  0.4 10156 2132 ?        S    16:08   0:00 /
root     17194  0.0  0.4 10156 2132 ?        S    16:08   0:00 /
root     17195  0.0  0.4 10156 2132 ?        S    16:08   0:00 /
root     17196  0.0  0.4 10156 2132 ?        S    16:08   0:00 /
root     17202  0.0  0.0  1324  428 pts/0    R    16:08   0:00 g
```

- Une trace dans les messages systèmes

/var/log/syslog :

```
Dec  4 16:08:13 amd1 named[17192]: starting BIND 9.2.1
Dec  4 16:08:13 amd1 named[17192]: using 1 CPU
Dec  4 16:08:13 amd1 named[17194]: loading configuration from '/
Dec  4 16:08:13 amd1 named[17194]: listening on IPv4 interface l
Dec  4 16:08:13 amd1 named[17194]: listening on IPv4 interface e
Dec  4 16:08:13 amd1 named[17194]: listening on IPv4 interface e
Dec  4 16:08:13 amd1 named[17194]: command channel listening on
Dec  4 16:08:13 amd1 named[17194]: command channel listening on
Dec  4 16:08:13 amd1 named[17194]: zone 0.in-addr.arpa/IN: loade
Dec  4 16:08:13 amd1 named[17194]: zone 127.in-addr.arpa/IN: loa
Dec  4 16:08:13 amd1 named[17194]: zone 255.in-addr.arpa/IN: loa
Dec  4 16:08:13 amd1 named[17194]: zone localhost/IN: loaded ser
Dec  4 16:08:13 amd1 named[17194]: running
```

Ça marche !

Exemple de configuration

```
/*
 * A simple BIND configuration
 */

/* Commentaire */
// Comment taire ?
# Comme en terre
options {
        directory "/var/named";
};

logging {
        category lame-servers { null; };
        category cname { null; };
};

zone "isc.org" in {
```

Exemple de configuration

```
        type master;
        // Le fichier de référence :
        file "master/isc.org";
};

zone "vix.com" in {
        type slave;
        // Le fichier de sauvegarde :
        file "slave/vix.com";
        masters { 10.0.0.53; };
};

zone "." in {
        type hint;
        // Le fichier définissant les racines :
        file "named.cache";
};
```

Exemple de configuration

```
zone "0.0.127.in-addr.arpa" in {
        type master;
        file "master/127.0.0";
};
```

- Partage de fichiers en réseau par machines hétérogènes de fichiers ou de hiérarchies
- Aide à rendre les machines uniformes par centralisation de l'information
- Protocole portable (Unix, Windows, VMS,...)
- Devices non partageables
- Exportation contrôlée des ressources sur la base d'une hiérarchie et d'un groupe de machine
- Les hiérarchies exportées ne peuvent pas se recouvrir
- Sous Unix exportation d'un système de fichier ou d'une partie
- Version

- 2 : Version la plus commune
- 3 : À partir de Solaris 2.5, nécessite clients et serveurs V3
  - Autorise les écritures asynchrones sur disque (ne bloque pas le client)
  - Macro-requêtes pour diminuer le traffic
  - Vérification des droits améliorés
  - Dépasse 8 Ko/paquets
  - Support des ACL
  - NFS au dessus de TCP en plus d'UDP (pas spécifique version 3)
  - Gestion des gros fichiers (plus de 2 Go)

- Utilisation dynamique de plusieurs serveurs en cas de panne sur des systèmes de fichier en lecture seule (`/usr/local`,...)
- WebNFS RFC 2054. RFC 2225 : meilleur débit que HTTP, pas de sur-coût à la FTP
- Sécurité Kerberos V5 et RPCSEC_GSS (API)

Arrivé dans Linux récents

- NFS v4
  - Tolérance aux pannes
  - Modèle de sécurité orienté utilisateur et pas que machine

- À la main avec
  `exportfs [-o` *options*`]` *chemin*
  Quelques *options*
  - `nosuid` Empêche la création de programme `setuid` et `setgid`
  - `ro` Exporte en lecture seulement à une liste de machine ou à tout l'univers
  - `no_root_squash` Les machines spécifiées ont les droits de `root`
  - `root_squash` Les machines spécifiées auront les fichiers à `root` comme appartenant à utilisateur anonyme

- `all_squash` Tout les fichiers sont vu comme appartenant à 1 utilisateur
- `rw` Exporte en lecture et écriture à une liste de machine ou à tout l'univers
- *`liste-machines`* consiste en des noms de machine, des `netgroup`, des suffixe DNS (à condition d'avoir `dns` en tête de `hosts` dans `/etc/nsswitch.conf`, des (sous-)réseaux. « - » est utilisé comme privatif dans les accès

- Automatiquement au démarrage en mettant les lignes précédentes dans le fichier `/etc/exports`

```
/                    master(rw) trusty(rw,no_root_squash)
/projects            proj*.local.domain(rw)
```

```
/usr            *.local.domain(ro) @trusted(rw)
/home/joe       pc001(rw,all_squash,anonuid=150,anongid=100
/pub            (ro,all_squash)
```

Prise en compte des modifications avec `exportfs -a`

- Vérifier que le serveur NFS est lancé avec

  `/etc/init.d/nfs.server start`

  Normalement lancé au démarrage si existence de

  `/etc/exports`

- Avec `mount -t nfs`, `/etc/fstab` ou l'auto-monteur
- Syntaxe `mount [-t nfs] [options_génériques] [-o options_spécifiques] [-O ] ressource mount_point`
  - *ressource* à monter
    - *host :pathname*
    - Une liste de ressources séparées par des virgules : système de tolérance aux pannes (mais en lecture seulement)
  - Quelques options
    - `fg` Bloque jusqu'à ce que le montage soit fait (défaut)
    - `bg` Réessaye en tâche de fond si le montage échoue

- `hard` Réessaye l'entrée-sortie jusqu'à ce que le serveur réponde
- `soft` Renvoie un code d'erreur si le serveur ne répond pas. Si un programme ne teste pas les retours d'erreurs... ☹
- `intr` Accepte d'interrompre les un accès `hard` bloquant en tapant `^C` au clavier
- `nointr` Le contraire
- `ro` Monte en lecture seule
- `rw` Monte en lecture/écriture
- `suid` Autorise l'exécution de programmes en `setuid`. Comportement par défaut...

- `nosuid` L'inverse

- Montage automatique si dans `/etc/fstab`

  `server:/usr/local/pub  /pub  nfs  suid,tcp,rw,bg,hard,intr`

- `nfsstat` permet d'avoir diverses statistiques sur le fonctionnement de NFS en fonction des options

- `showmount` permet d'avoir à distance informations sur les clients ou les partitions exportées d'un serveur donné

Plan

- Connexions à distance (ssh, ftp...)
- Système d'impression (BSD, CUPS...)
- Systèmes de nommage
  - Service DNS pour la résolution des noms
  - Système de nommage NIS
- Partage de fichiers en réseau avec NFS
- Auto-montage
- Archivage des données
  - tar, cpio, pax, mt...
  - Archivage en réseau avec rsync, partimage
  - AMANDA

Auto-monteur

- Trop de montages saturent le système
- ⇝ Montage et démontage à la demande à partir de tables centralisées
- Tout ne peut pas être connu dès le départ
- Uniformisation des machines
- Éviter de devoir être `root` pour monter des répertoires (distants)
- Généralisation de l'espace de nommage `/net/`*machine*`/`*fichier*
- Permet facilement stockage distribué au plus près des utilisateurs en utilisant les To de disque sur chaque machine au lieu de SAN/NAS goulets d'étranglement et hors de prix

- Changement de tous les montages de toutes les machines de manière centralisée
- ⇝ AutoFS de Solaris : probablement l'automonteur d'Unix le plus avancé
- Sous Linux, `amd` de BSD et `autofs` imitation AutoFS Solaris

- Une *carte* peut être un fichier /etc/*carte* ou une *carte* NIS, NIS+... en fonction de /etc/nsswitch.conf
- Master map : /etc/auto_master associe des répertoires avec des cartes

```
keryell@voltaire ~: more /etc/auto_master
# Master map for automounter
#
+auto.master
keryell@voltaire ~: ypcat -k auto.master
/home auto.home -hard,bg,intr
/misc   /etc/auto.misc
/net -hosts             -nosuid,nobrowse
/- auto.direct
```

- `-hosts` signifie de monter les fichiers (exportés !) de n'importe quelle machine demandée dans le répertoire
- `/-` évite d'associer une carte avec un répertoire

- `/etc/auto.misc` :

```
cd      -fstype=iso9660,ro,nosuid,nodev :/dev/cdrom
linux   -ro,soft,intr           ftp.example.org:/pub/linux
boot    -fstype=ext2            :/dev/hda1
floppy  -fstype=auto            :/dev/fd0
usb     -fstype=auto            :/dev/uba1
sda     -fstype=auto,uid=keryell,users          :/dev/sda1
sdb     -fstype=auto,uid=keryell,users          :/dev/sdb1
sdc     -fstype=auto,uid=keryell,users          :/dev/sdc1
sdd     -fstype=auto,uid=keryell,users          :/dev/sdd1
```

- Direct map : dirige AutoFS directement vers des systèmes de fichiers à partir d'un nom de répertoire

```
keryell@voltaire ~: ypcat -k auto.direct
/var/mail -rw,hard,intr,actimeo=0 palo-alto:/export/verre2/
/users -rw,hard,intr    palo-alto:/export/verre1
```

  Cartes directes pas encore au point sous Linux...

- Indirect map : monte des systèmes de fichier à partir d'une clé (nom de répertoire dans répertoire surveillé)

```
keryell@voltaire ~: ypcat -k auto.home
palo-alto / &:/export   /verre1 &:/export/verre1 \
        /verre2 &:/export/verre2 /verre3 &:/export/verre3 \
        /verre4 &:/export/verre4
```

  - & rappelle le nom de la clé

- ► `*` accepte n'importe quelle clé

  `*  &:/export`

- Possibilité d'utiliser des variables pour changer localement des montages : `$ARCH`, `$CPU`, `$HOST`, `$OSNAME`, `$OSREL`, `$OSVERS`
- Possibilité de mettre des poids dans des montages redondants
- Ne pas mettre au même endroit exportation et montage local mais plutôt par exemple `/export/...` et `/home/...`
- `automount` contrôle le comportement d'`automountd` (relecture d'`auto_master`, changement du temps de raffraichissement)

- `/etc/init.d/autofs status` donne info sur montages en cours

- Connexions à distance (ssh, ftp...)
- Système d'impression (BSD, CUPS...)
- Systèmes de nommage
  - Service DNS pour la résolution des noms
  - Système de nommage NIS
- Partage de fichiers en réseau avec NFS
- Auto-montage
- Archivage des données
  - tar, cpio, pax, mt...
  - Archivage en réseau avec rsync, partimage
  - AMANDA

Nécessité des sauvegardes

- Les fichiers représentent la propriété intellectuelle. Toute la vie d'une entreprise sous forme de fichiers...
- Les pannes existent, les utilisateurs aussi ☺ (rm␣−rf␣toto.␣∗) et les bugs aussi...
- La majorité des entreprises ne survivent pas à moyen terme à la perte de leur informatique ☹
- Nécessité de faire des sauvegardes régulières (1 fois par jour)
- Et sur le long terme (années) pour retrouver des fichiers perdus par erreur et dont on ne s'aperçoit pas tout de suite ☹
- Cher car pas grand public ☹ ⇝ Confiance aveugle

~~informatique~~bureautique ☹

- Mais ∃ versions USB moins chères...
- Stocker les média de sauvegarde à différents endroits le plus loin possible du système de sauvegarde (autres bâtiments, villes)
- Penser à chiffrer les sauvegardes en milieu sensible
- Ne pas oublier que les média ne sont pas éternels (≈ 10 ans pour les bandes magnétiques)
- Faire des migrations (bonne nouvelle : croissance exponentielle capacités ☺)
- Que faire de média dont plus aucun lecteur n'existe ? Légende disant qu'il existe un service de l'État qui possède tous les types de lecteurs possibles au cas où...

- Choisir un système matériel : DAT (36 Go et 3 Mo/s), Exabyte 8mm, AIT-4 (200 Go, 24 Mo/s), SAIT-1 (500 Go, 30 Mo/s), SDLT600 (300 Go, 36 Mo/s), LTO Ultrium-3 (400 Go, 80 Mo/s)
- Publicités souvent faites avec compression en plus... ☹
- RAITs : RAIDs de bandes (↗ tolérance, ↗ débit, ↗ capacité), automates de plein de bandes
- Choisir une logiciel de sauvegarde

  `http://www.backupcentral.com`

  - Outils bruts par partition et par machine : `dump`/`restore`,...
  - Outils automatisant la sauvegarde d'un réseau et

utilisant des outils bruts

`http://www.backupcentral.com/free-backup-software2.html`

- Bacula `http://www.bacula.org` très client-serveur
- Amanda (`www.amanda.org`) client-serveur gratuit et utilisé au ENSMP/CRI & IAR2M : 80 partitions (1 centaine de Go) sauvegardées chaque nuit sur 1 cassette 8 mm de 7 Go. Au ENSTBr/RIRE : DAT DDS4 de 20 Go pour des centaines de Go

Utiliser un outil de ce type !

`http://enstb.org/~keryell/publications/conf/2001/JRES2001/ama`

- Choisir une politique de sauvegarde :
  - Faire un état des lieux des machines et des disques

- Quoi sauvegarder ? Tout si possible ! En priorité les partitions utilisateurs avant celles du système (récupérables en gros sur CD)
- Quand sauvegarder ?
- Durée nécessaire aux sauvegardes
- Centralisation du système de sauvegarde
- Débit du réseau : ne pas écrouler le réseau pendant le fonctionnement normal
- Éviter de faire des sauvegardes sur des systèmes de fichiers très actifs ⇝ sauvegardes la nuit. En théorie, devrait être en mode mono-utilisateur...
- Problème de cohérence avec des systèmes de

base de donnée : sauvegarder plutôt une image instantanée de la base plutôt que la base de donnée

- Utiliser astucieusement les sauvegardes incrémentales : plutôt que de sauvegarder toute une partition, on la sauve une fois complètement et ensuite on ne sauve que les différences par rapport à la sauvegarde complète. Récursion possible sur le concept. Compromis à trouver entre sécurité, facilité de restauration et place occupée sur bande. De toute manière, besoin supérieur à l'incrément quotidien. Exemple à allocation statique pour une partition disque
  - Vendredi soir : niveau 0
  - Lundi soir : niveau 1

- Mardi soir : niveau 2
- Mercredi soir : niveau 3
- Jeudi soir : niveau 4
- Si on perd 1 niveau 0 on perd la semaine
- Si on veut récupérer 1 jeudi il faut lire 5 bandes ☹

Rotation d'un jour sur toutes les partitions de manière cyclique pour répartir la quantité (niveaux 0) sur les bandes de sauvegarde

- Compromis à trouver entre économie, robustesse et confort
- ⇝ Rapidement compliqué... ☹

- Rigidité optimiste (sauvegarde incrémentale même si changements très importants) et pessimiste (sauvegarde niveau 0 même si pas de changement) ☹

⇝ Outils à planification dynamique comme AMANDA

- Pas d'accès direct à l'information
  - Fichiers séparés par des marques de fin de fichier
  - Possible de sauter plus rapidement d'une marque à l'autre
  - Concaténation possible de fichiers si pas de rembobinage (⚠ sport dangereux)
  - Pas possible de modifier fichiers au milieu d'une bande

  Utilisation de la commande `mt` pour contrôler la bande
- ⚠ Faire des accès par gros morceaux (cf option `b` de `tar`) pour éviter arrêts/retour arrière incessants de la bande (↘↘ performances)

- Conducteur matériel : souvent lien `/dev/tape` vers contrôleur périphérique (*device driver*) par défaut
  - Exemple en SCSI décliné en `/dev/nst`x avec x numéro dérouleur
  - Différents noms de périphériques pour choisir densité d'écriture
    - `/dev/nst0`
    - `/dev/nst0l`
    - `/dev/nst0m`
    - `/dev/nst0a`

    `n` pour `n`on rembobinant

- ⚠ ∃ Version contrôleur périphérique qui *rembobine à la fermeture (fin d'accès)* !
  - `/dev/st0`
  - `/dev/st0l`
  - `/dev/st0m`
  - `/dev/st0a`
  - ⚠ ⚠ ⚠ Film d'horreur : suite utilisation du contrôleur de périphérique rembobinant à la fermeture, écriture de chaque fichier de sauvegarde en début de bande en écrabouillant sauvegarde précédente ☹☹
  - ⇝ Sage comportement : toujours utiliser device non-rembobinant et contrôler situation avec `mt`

- ⇝ Faire des tests catastrophes de temps en temps pour vérifier que sauvegardes correctes
- Relire bandes pour vérifier ? Double temps et usure... ☹

- Contrôle de *Magnetic Tape drive*
- `mt [-f device] operation [count] [arguments...]`
- Nombreuses opérations telles que
  - `fsf` *forward space* `count` *files* et positionne sur début fichier suivant
  - `bsf` *backward space* `count` *files* et positionne sur fin fichier précédant
  - `eod` va à la fin des données de la bande (pour faire un rajout ensuite)
  - `rewind` rembobine la bande
  - `eject` rembobine la bande et éjecte cassette ou bande

- `defdensity` et `defcompression` change densités et compression par défaut (pour DAT par exemple)

- ⚠ ⚠ ⚠ Bien utiliser device non-rembobinant sinon résultats fâcheux... ☹

- Outils de sauvegarde de base de UFS (gestion via inodes...)
- ⇝ Ne change pas dates de dernier accès aux fichiers
- Sauvegarde d'abord la table des matières ⇝ si gros changements pendant la sauvegarde...
- Niveaux incrémentaux de 0 à 9
- `dump` pour la sauvegarde d'une liste de fichiers ou 1 système de fichier. Il faut préciser la taille de la bande (même si sauvegarde dans un fichier...) car possibilité d'utiliser plusieurs bandes
  - `dump 0uf /dev/st0 /` : niveau 0
  - `ufsdump 1uf /dev/st0 /export/home` : niveau 1

« `u` » a pour effet de mettre à jour `/etc/dumpdate` qui note la date des sauvegardes pour chaque niveau d'incrément. Ne sont sauvegardés pour un niveau donné que les fichiers modifiés après la date des sauvegardes de niveau inférieur

- `restore` pour la restauration de fichiers
  - `restore rf /dev/st0` : récupère le contenu de la partition sur la bande
  - `restore if moret.c0t1d0s7.19981201.1` : récupération en mode interactif

```
deauville-keryell > restore if moret.c0t1d0s7.19981201.1
restore > ls
.:
 WWW/     users/
restore > cd WWW
```

```
restore > cd conf
restore > ls
./WWW/conf:
 srm.conf
restore > add srm.conf
restore > extract
You have not read any volumes yet.
Unless you know which volume your file(s) are on you should start
with the last volume and work towards the first.
Specify next volume #: 1
set owner/mode for '.'? [yn] n
restore > quit
```

En général ne pas changer les droits/modes de « . » si restauration ailleurs que dans le répertoire d'origine

- Lors d'une restauration complète, il y a ré-allocation des inodes et il ne faut pas commencer la sauvegarde suivante par une incrémentale mais par une de niveau 0

- ⚠ Sauvegarde loin d'être atomique...
- ⇝ Incohérences possibles dans les fichiers entre le début et la fin de la sauvegarde ☹
- ⚠ Problème typique avec des bases de données (format binaire interne opaque)
- Généralement impossible d'arrêter le système
- ⇝ Faire une photo instantanée du système de fichier juste avant de lancer la sauvegarde
- Les données ayant changé depuis l'instantané sont conservées dans un fichier (*backing store*)
- En production depuis longtemps sous Solaris mais pas vraiment sous Linux

Création de snapshot

- Le plus simple est de passer par gestionnaire de partitions virtuelles LVM

- Problème : des morceaux du noyau risquent d'être écrasés lors de la restauration...
- Démarrer sans utiliser ces disques : depuis le CD-ROM, depuis un serveur d'installation (toujours en avoir un sous le coude), en tant que *diskless* depuis le réseau ou depuis un autre disque le cas échéant
- Monter le disque à restaurer dans `/mnt` et faire la restauration dedans puis démonter
- Comme la sauvegarde ne gère pas le boot, réinstaller la zone de démarrage sur le disque `/` avec `lilo` ou `grub`

- `dump`/`restore` efficace pour systèmes Unix mais non portable ☹
- Outils portables pour transporter une arborescence
- `tar` + GNU
- `cpio` plus portable et multivolume + GNU
- `pax` gère les formats POSIX `cpio` et `ustar`. Fusion du projet avec tar
- Utile pour recopier des arborescences sous Unix
  `tar cf - ici | ( cd là-bas ; tar xf -)`
  ou un `cp -ap` de GNU
- si sauvegarde avec des noms absolus, restauration avec des noms absolu depuis `/`. Pour rattraper la sauce :

changer la racine du processus de restauration via `chroot`...

- *Tape ARchive*
- Sérialise arborescence de fichier en 1 fichier avec méta-données (droits, dates...)
- Portable entre systèmes
- Variante de `ar` (archives de bibliothèques en programmation)
- Des tonnes d'options au format long (nouveau) ou court (vieux)
  - `-list` ou `[-]t` affiche contenu archive
  - `-verbose`
  - `-create` ou `[-]c` crée archive
  - `-extract` ou `[-]x` extrait archive

- `-preserve-permissions` ou `[-]p` essaye préserver droits lors restauration
- `-gzip` ou `[-]z` (dé)comprime
- `-bzip2` ou `[-]j` (dé)comprime

- Possibilité archive distantes

```
1 tar␣--rsh-command=ssh␣--file=leon:/dev/nst0␣--create␣--v
```

- Gestion multivolume
- Archives incrémentales (vient avec des scripts d'aide)
- Faire des savegardes en utilisant système de fichiers *modifie* date de dernier accès des fichiers... ☹Sinon passer système en lecture seule

- Vieille syntaxe : mélange possibles options & arguments peu clair

```
1  tar␣jxvf␣/usr/src/linux-2.6.13.tar.bz2
```

- `man tar` et `info tar`

- Capture de toute l'information au niveau de `/dev/`*`disque`*
- Peut être utile pour une restauration de `/` avec la zone de démarrage
- Duplication rapide de disquette

```
dd if=/dev/fd0 of=devcfg-2.7-disquette bs=1440k
eject floppy
```

puis avec une nouvelle disquette

```
fdformat -d -U
dd if=devcfg-2.7-disquette of=/dev/fd0 bs=1440k
eject
```

- Clonage d'une installation de Windows NT multi-OS via Unix

```
cd /export/verre4
ssh roosevelt "dd if=/dev/hda1 bs=512 | gzip -9" > nt-4.0.server.roosevelt.gz
```

puis installation depuis une autre machine lors de la procédure d'installation automatique

```
mkdir /tmp/verre4
mount palo-alto:/export/verre4 /tmp/verre4
gunzip -c /tmp/verre4/nt-4.0.server.roosevelt.gz | dd bs=512 of=/dev/hda1
```

- Transfert de hiérarchie de fichiers entre machine
  - Copie que ce qui est nécessaire (dates ou différences via hachage ou octet par octet)
  - Transferts incrémentaux
  - Comprime transferts
- Typiquement `rsync [option]... src [src]... [user@]host:dest`
- Nombreuses options dont
  - `-a` transfert récursivement
  - `-e ssh` utilise par exemple `ssh` pour communiquer
  - `-partial` reprend des fichiers en cours de transfert après interruption

- `-H` garde liens hard
- `-v` verbeux
- `-z` comprime
- `-exclude=`*PATTERN* saute certains fichiers
- `-bwlimit=`*Ko/s*

- ∃ Serveur `rsync` anonyme ou pas : utilisé pour miroir `debian.enstb.org`
- Sauvegarde ordinateur portable

```
# Synchronisation du monde avec an-dro.
#TEST="-n --ignore-times --checksum"
#TEST="-n"
DEST=root@leon.info.enstb.org
DEST_FAI=root@minou.info.enstb.org
```

```
RSYNCSAUV='rsync␣'$TEST'␣--archive␣--hard-links␣--delete␣\
␣␣␣␣␣␣␣␣␣␣--force␣--partial␣--compress␣--verbose␣-e␣ssh'
$RSYNCSAUV␣/users/lit/keryell/public_html␣$DEST_FAI:/home/keryell
$RSYNCSAUV␣/users/lit/keryell␣$DEST:/home/sauvegardes/an-dro/users/lit
```

- Copie photos appareil numérique

```
#␣Synchronisation␣d'an-dro␣avec␣l'appareil␣photo
#TEST="-n␣--ignore-times␣--checksum"
#TEST="-n"
RSYNCSAUV='rsync␣'$TEST'␣--archive␣--update␣--force␣--verbose␣-e␣ssh'
$RSYNCSAUV␣␣/misc/sdb/dcim/101msdcf/␣$HOME/perso/photo/DSC-W17/101_sony
```

- Création d'instantané de système de fichier avec répertoires style
  - `H-1`, `H-2`, `H-3`...
  - `J-1`, `J-2`, `J-3`...
  - `Semaine-1`, `Semaine-2`, `Semaine-2`...
- Moins besoin de restaurations
- À base de PERL, `rsync` et liens hards ⇝ retour aux versions de fichier de VMS ☺
- ⇝ Tout en mode utilisateur, pas besoin de snapshot au niveau système d'exploitation
- Double la taille en disque + modifs
- Disques pas chers ⇝ simplification vie ingénieur système

- Mettre plein de disques de 1 To lents et peu chers sur vieilles machines pour ça
- `http://www.rsnapshot.org`

- Sauvegarde de partitions entières au format EXT2/3, UFS, JFS, NTFS...
- Compression des fichiers images
- Via réseau sécurisé avec TLS vers serveur `partimaged`
- Permet restaurations rapides (clonage...)
- Gère restauration de partitions systèmes via démarrage de Linux+`partimage` sur 1 CD ou 2 disquettes

Interaction avec Windows

- Utilise SAMBA
- `smbclient -T <tar-options>`
- Permet de restaurer ou sauvegarder partage SMB/CIFS au format `tar`

  ```
  smbclient //mypc/myshare -Tc backup.tar users/docs
  ```
- Utilisé aussi par AMANDA
-
  - Notion de fichiers en ouverture qu'une seule fois... y compris pour `tar` ☹
  - Attributs spéciaux/cachés non POSIX
  - ∃ mécanismes pour faire des sauvegardes mais non POSIX, spécifications non libres

the Advanced Maryland Automatic Network Disk Archiver

- Né au début des années 1990 des constatations précédentes
- Fournir une solution satisfaisante à la problématique des sauvegardes
- Logiciel libre
  - On peut voir comment sont faites les sauvegardes
  - On peut récupérer les données (logiciellement) longtemps après pour sauvegardes et archivage
  - Va dans le sens des mesures gouvernementales sur l'usage de formats libres et de logiciels libres
  - Pas prisonnier des licences pour décider ce qu'on peut sauvegarder

- AMANDA a la masse critique suffisante pour s'entretenir
- SAV assuré par les pairs sur 2 listes de diffusion

- Machine maître
  - Contrôle typiquement un dérouleur de bande
  - Supervise un ensemble de clients à sauvegarder
- Machines clientes
  - Envoient à la demande du maître taille ou contenu des sauvegardes

Disques tampons

- Sauvegarde en réseau : débit non constant ou insuffisant
- Obligé d'arrêter la bande et de réaligner au début d'un enregistrement
  $=:$ performances $\searrow\searrow$
- Sauvegarde sur des disques tampons sur le serveur
- Quand un disque est suffisament plein : écriture rapide sur la bande
- Prix des disques tampons négligeables
- Permet la parallélisation sur les clients
- Évite l'entrelacement sur bande
- Problème de bande ? Sauvegarde en mode dégradé sur disque

Planification automatique

- Sauvegardes incrémentales trop compliquées à planifier et à optimiser
- Automatisation à partir d'un cahier des charges basé sur
  - Cycle de sauvegarde : nombre de jours maximal entre les sauvegardes complètes des partitions
  - Nombre de cassettes : utilisées pour faire les sauvegardes
  - Débit réseau : ce qui est autorisé
  - Nombre de sauvegardeurs maximal à faire tourner sur chaque client
  - Priorités (importances) entre différentes partitions

- Optimisation à partir de
  - Performances des sauvegardes passées
  - Interrogation des clients sur les données à sauvegarder
- Plus souple : s'adapte à de forts changements de contenu en retardant certaines sauvegardes totales superflues
- Changements de consigne possibles
  - Forcer une sauvegarde complète d'une partition
  - Ne faire que des sauvegardes complètes
  - Ne faire que des sauvegardes incrémentales (on a une référence ailleurs) Antidatage...

- AMANDA optimise le remplissage
  - Le plus de données fraîches sur la bande : optimise la tolérance aux pannes
  - Use au maximum le dérouleur de bande par rapport à une planification statique intrinsèquement pessimiste
- Recyclage automatique des cassettes
  - Protection par un label pour empêcher un recyclage anticipé par erreur
  - Marquage des cassettes par `amlabel`
  - Vérification dans la journée que la cassette est la bonne avec `amcheck`

- Dérouleurs modernes : compression intégrée
- Compression logicielle possible sur chaque client AMANDA
  - Compression souvent meilleure que celle du dérouleur
  - Souvent plus lente (`gzip`, `bzip2`)
  - Mais parallélisée sur tous les clients
  - Seules les données comprimées passent sur le réseau : ↘ pression
  - Compression directement mesurée sur chaque client, utilisable dans la planification

Sauvegardes de données comprimées avec compression dérouleur : capacité ↘

AMANDA utilise les outils disponibles sur les clients

- `dump`
  - − Spécifique à un système de fichiers, voire à un système d'exploitation. Sauvegardes portables et éternelles : bof
  - + Mode de restauration interactive
  - + Ne change pas les dates des fichiers
- `tar`
  - + Format portable, documenté, logiciel libre. On pourra relire (si les bandes ne sont pas endommagées et qu'il reste un lecteur en état de marche...) les sauvegardes sur une autre machine

+ Pas de conflit sur le fichier de gestion incrémentale des sauvegardes. Permet facilement de mélanger plusieurs instances d'AMANDA (archivage + sauvegardes)
– Modifie la date d'accès des fichiers

- Possible de créer avant une sauvegarde un « instantané » (*snapshot*) de la partition si le système le permet (`fssnap` sous SOLARIS)
- Donne une vue stable et cohérente du système de fichiers pendant toute la durée de la sauvegarde

Un seul dérouleur par serveur AMANDA mais possibilité chargement automatique

- Automatisation complète de la sauvegarde
- Possibilité de remplir plusieurs bandes par sauvegarde
- Quasi disparition des problèmes d'écriture et donc de l'usage d'`amflush`
- Si la pièce contenant le chargeur brûle, on perd tout... Si pas de chargeur, on peut très bien entreposer les cassettes loin...

4 systèmes de contrôle de changeurs de bande (dont 1 assisté par humain)

Problèmes des sauvegardes et archivages en général, en réseau en particulier,...

- Toutes les cassettes possèdent des copies de logiciels autorisant *la* copie de sauvegarde
- Les copies transitent sur un autre ordinateur (serveur de sauvegarde) : pas forcément autorisé
- Lois de la CNIL sur les données d'authentification et de traçage : que faire s'il faut les effacer au bout d'un an ?
  - Bandes : pénible...
  - CD-ROM, média à écriture une seule fois,... : difficile

Suivi des opérations

- Courriel de fin de sauvegardes (`amdump`)
- Courriel de vérification (`amcheck`)
- Informations sur une sauvegarde en cours ou passée (`amstatus`, `amplot`)
- Restaurations avec `amrecover` et `amrestore`

```
From: bin@cri.ensmp.fr
Subject: chailly99_jour AMANDA MAIL REPORT FOR December 6, 2001
To: sauvegardes-amanda-chailly99@cri.ensmp.fr
Date: Fri, 7 Dec 2001 01:28:38 +0100 (MET)

These dumps were to tape CHAILLY99-J-03@27-11-2000.
Tonight's dumps should go onto 1 tape: CHAILLY99-J-04@13-06-2000.


STATISTICS:
                          Total       Full      Daily
                        --------    --------    --------
Dump Time (hrs:min)        2:19        0:23        0:11   (0:08 start,
Output Size (meg)        5555.2      3868.4      1686.8
Original Size (meg)     12403.4      9391.5      3011.9
```

```
Avg Compressed Size (%)     43.7        40.1        55.1
Tape Used (%)               27.8        19.3         8.4    (level:#disk
Filesystems Dumped            48           8          40    (1:40)
Avg Dump Rate (k/s)        742.0       760.5       702.7
Avg Tp Write Rate (k/s)   2788.3      2923.8      2520.4
NOTES:
  taper: tape CHAILLY99-J-03@27-11-2000 kb 5690016 fm 48 [OK]
DUMP SUMMARY:
                                              DUMPER STATS
HOSTNAME  DISK            L  ORIG-KB   OUT-KB COMP%  MMM:SS   KB/s  M
------------- ------------------- -------
abisko    c0t0d0s4        1    26303     2272   8.6    0:11  198.8
abisko    c0t0d0s5        1   165023   101728  61.6    2:25  701.6
blonville c0t0d0s6        1     6080     6080   -     0:23  261.3
chailly99 c0t0d0s0        1      191       32  16.8    0:04    8.0
```

chailly99	c0t0d0s3	1	735	64	8.7	0:04	14.5
chailly99	c0t0d0s5	1	95	32	33.7	0:18	1.8
chailly99	c0t0d0s6	0	999999	429216	42.9	8:28	844.7
chailly99	c0t1d0s3	0	1613183	928448	57.6	15:18	1011.5
chailly99	c0t1d0s4	1	63	32	50.8	0:03	11.9
chailly99	c1t0d0s5	0	223	32	14.3	0:02	19.9
chailly99	c1t0d0s6	0	191	32	16.8	0:01	22.4
chailly99	c1t0d0s7	1	95	32	33.7	0:02	17.8
chailly99	c1t1d0s0	1	831	128	15.4	0:03	36.9
chailly99	c1t1d0s3	1	95	32	33.7	0:17	1.9
chailly99	c1t1d0s4	0	4012511	702368	17.5	28:51	405.8
chailly99	c1t1d0s5	1	95	32	33.7	0:02	17.4
chailly99	c1t1d0s6	1	351	32	9.1	0:06	5.2
chailly99	c1t3d0s0	1	940991	861504	91.6	12:12	1177.4
chailly99	c1t3d0s1	1	1247	96	7.7	1:53	0.8

chailly99	c1t3d0s3	1	159	32	20.1	0:07	4.8
chailly99	c1t3d0s4	1	107711	48064	44.6	1:45	459.2
chailly99	c1t3d0s5	1	3359	1184	35.2	0:43	27.7
chailly99	c1t3d0s6	1	412735	169280	41.0	3:17	858.4
chailly99	c1t3d0s7	1	159	32	20.1	0:02	13.6
champeaux	c0t0d0s4	1	32383	3104	9.6	0:15	211.5
champeaux	c0t0d0s5	1	784543	249536	31.8	6:17	661.8
esmans	c0t0d0s4	1	10847	1088	10.0	0:09	120.2
esmans	c0t0d0s5	1	32383	18368	56.7	1:09	267.5
forges	c0t0d0s4	1	5855	896	15.3	0:11	78.6
forges	c0t0d0s5	1	77151	19488	25.3	0:54	361.3
lavaur	c0t0d0s4	1	5791	864	14.9	0:10	84.9
lavaur	c0t0d0s5	1	26879	10784	40.1	0:30	355.2
montereau	c0t0d0s4	1	6591	992	15.1	0:06	155.1
montereau	c0t0d0s5	1	63	32	50.8	0:18	1.8

Courriel de fin de sauvegarde

orgenoy	c0t0d0s3	1	255	32	12.5	0:04	7.3
orgenoy	c0t0d0s4	1	47871	6560	13.7	0:33	197.1
orgenoy	c0t0d0s5	1	95	32	33.7	0:02	15.4
orgenoy	c0t0d0s6	1	63	32	50.8	0:15	2.2
orgenoy	c0t0d0s7	1	799	64	8.0	0:05	13.2
orgenoy	c1t2d0s0	1	324543	168064	51.8	4:33	616.4
pamfou	c0t0d0s4	1	6015	896	14.9	0:09	94.6
pamfou	c0t0d0s5	0	2813375	1723712	61.3	32:42	878.5
rhune	c0t0d0s6	1	5760	5760	-	0:16	350.0
thomery	c0t0d0s4	0	70016	70016	-	0:36	1957.3
thomery	c0t0d0s5	1	7360	7360	-	0:14	510.8
viroflay	c0t0d0s6	1	5856	5856	-	0:15	393.5
vulaines	c0t0d0s4	0	107424	107424	-	0:51	2111.1
vulaines	c0t0d0s5	1	36736	36736	-	0:34	1086.8

Courriel de fin de sauvegarde

```
(brought to you by Amanda version 2.4.1p1)
```

Amanda Dump 20010928
Bandwidth = 850
Holding disk = 10000
Tape Policy = LFFO
Dumpers= 8
Driver alg = drain-ends At big end 5
Elapsed Time = 6:00:08
Final status = TAPE ERROR
Dumped/Failed = 47/1
Output data size = 12
Estimated data size = 19999
Run Queue
Tape Queue
Dumps Finished
Bandwidth Allocated
%Disk Allocated
%Tape Wait
Taper Idle
Dumpers Idle
QUEUES
%BANDWIDTH
HOLDING
DISK
TAPE
%DUMPERS
Active
Idle
0:00
0:20
0:40
1:00
1:20
1:40
2:00
2:20
2:40
3:00
3:20
3:40
4:00
Minutes

Permet d'ajuster les paramètres

- Autoriser plus de bande passante réseau
- Rajouter des disques tampons
- Lancer plus de sauvegardeurs par client en parallèle (en précisant les partitions qui ne sont pas sur le même disque pour éviter de perdre du temps à bouger les têtes...)

Vérification des sauvegardes

- Pas la peine de faire des sauvegardes si cela ne marche pas...
- `amverify` essaye de comprendre la sauvegarde si format libre ou outil propriétaire disponible sur le serveur
- Vérification plus frustre : lancer une restauration d'une partition inexistante
- Faire des vérifications dans le stock de temps en temps
- Essayer de lire avec un *autre* lecteur...

☹Vérifier use matériel et cassettes...

```
orgenoy-root > amrecover chailly99_jour -s chailly99 -t chailly99
AMRECOVER Version 2.4.1p1. Contacting server on chailly99 ...
220 chailly99 AMANDA index server (2.4.1p1) ready.
200 Access OK
Setting restore date to today (2001-10-02)
200 Working date set to 2001-10-02.
200 Config set to chailly99_jour.
200 Dump host set to orgenoy.
$CWD '/export/interne' is on disk 'c0t0d0s7' mounted at '/export/int
200 Disk set to c0t0d0s7.
/export/interne
amrecover> ls
2001-10-01 .
2001-09-27 lost+found/
2001-10-01 save_system/
```

```
amrecover> cd save_system/
/export/interne/save_system
amrecover> ls
2001-10-01 .
2001-10-01 jumpstart/
2001-09-27 modeles/
2001-09-27 root/
amrecover> add jumpstart/
Added dir /save_system/jumpstart at date 2001-10-01
Added dir /save_system/jumpstart at date 2001-09-27
amrecover> extract

Extracting files using tape drive /dev/null on host chailly99.
The following tapes are needed: CHAILLY99-J-26@13-11-2000
                                CHAILLY99-J-27@30-05-2000
```

```
Restoring files into directory /export/interne
Continue? [Y/n]:
```

Demande d'insérer à tour de rôle cassettes pour niveaux incrémentaux si nécessaire

- Trouver la bonne bande

```
amadmin chailly99_jour find champeaux
Scanning /home/chailly99/bibendum5/amanda/work/chailly99_jour...

date       host      disk     lv tape or file              file stat
2001-08-08 champeaux c0t0d0s4  1 CHAILLY99-J-28@17-07-2000   15 OK
2001-08-09 champeaux c0t0d0s4  1 CHAILLY99-J-29@31-05-2000   26 OK
[...]
2001-09-25 champeaux c0t0d0s4  0 CHAILLY99-J-24@24-05-2000   29 OK
2001-09-26 champeaux c0t0d0s4  1 CHAILLY99-J-25@25-05-2000    1 OK
2001-09-27 champeaux c0t0d0s4  1 CHAILLY99-J-26@13-11-2000   14 OK
2001-10-01 champeaux c0t0d0s4  1 CHAILLY99-J-27@30-05-2000   10 OK
2001-08-08 champeaux c0t0d0s5  1 CHAILLY99-J-28@17-07-2000   12 OK
[...]
2001-09-24 champeaux c0t0d0s5  0 CHAILLY99-J-23@10-07-2000   47 OK
```

```
2001-09-25 champeaux c0t0d0s5  1 CHAILLY99-J-24@24-05-2000   37 OK
2001-09-26 champeaux c0t0d0s5  1 CHAILLY99-J-25@25-05-2000   12 OK
2001-09-27 champeaux c0t0d0s5  1 CHAILLY99-J-26@13-11-2000   27 OK
2001-10-01 champeaux c0t0d0s5  1 CHAILLY99-J-27@30-05-2000   31 OK
```

- on insère la bonne bande et on récupère depuis la machine `champeaux` par exemple avec

```
ssh chailly99 amrestore -p /dev/rmt/0hn champeaux c0t0d0s5 | ufsrest
```

Restauration dans le néant

- Pas de restauration automatique *bootable* (non portable...)
- Si on a au moins 2 serveurs d'installation : pas de problème
- Lancer une installation automatique
- Si serveur AMANDA encore en vie ou index récupérables : restauration luxueuse
- Peut être intéressant de répliquer les index...
- Sinon, travailler à la main avec un format de bande simple :
  - Premier fichier donne nom bande et date sauvegarde

    `AMANDA: TAPESTART DATE 20010808 TAPE CRI-21@20-09-1999`
  - Autres fichiers commencent par 32 Ko de mode d'emploi !

```
AMANDA: FILE 20010808 deauville c0t2d0s4 lev 1 comp N program
To restore, position tape at start of file and run:
        dd if=<tape> bs=32k skip=1 | /usr/sbin/ufsrestore -f.
```

ou

```
AMANDA: FILE 20010809 orgenoy c0t0d0s4 lev 1 comp .gz program
To restore, position tape at start of file and run:
        dd if=<tape> bs=32k skip=1 | /usr/local/bin/gzip -dc
```

- Extraction de la table des matières facile :

```
mt -f /dev/rmt/0hn rewind
while dd bs=32k count=1 if=/dev/rmt/0hn; do echo; done;
```

- Voir les travaux pratiques...
- Visualisation des processus : `ps augxww` (BSD) ou `ps -ef` (SVR4), `top`
- Tracer les appels systèmes et appels de fonction d'un processus : `strace`
  Pratique pour voir quels sont les fichiers cherchés par une application
- Debugguer un processus : `gdb -p` *pid*
- Avoir des infos sur un processus : regarder dans `/proc/`*pid*
- Regarder des paquets sur le réseau : `tcpdump`, `ethereal`
- Associer des fichiers ou sockets à des processus : `lsof`

- Lister les connexions réseaux, des statistiques,... : `netstat`

- GNU/Linux devenu un système Linux mature
  - Parti du monde PC ⇝ distributions grand public (Ubuntu...)
  - Va vers le monde professionnel & couvre tous les types d'ordinateur
    - Ordinateurs haute performance
    - Grappes tolérantes aux pannes
    - 64 bits : gros fichiers, grosse mémoire pour chaque processus
    - Systèmes embarqués
    - Extensions temps-réel

- Robustesse (famille Unix développée depuis années 1970)

- Administration à plusieurs niveaux en fonction des besoins : basique avec interface graphique jusqu'aux systèmes très spécialisés avec les fichiers textuels
  - Administration sous forme de fichiers textes : simplifie automatisation administration système
- Installation automatique avec installation de plusieurs OS sur la même machine
- Logiciel libre : pas cher, forte communauté compétente, retour aux *sources* en cas de problèmes, $\exists$ consultants
- Ouvert : accepte les standards

1 Titre 0
2 Copyright (c) 1
3 Plan 2
2 Introduction 1
2 Plan 1
4 Interaction avec d'autres systèmes 3
3 Connexions à distance 2
3 Interactions autres systèmes 2
5 Client FTP 6
4 FTP 5
6 Serveur FTP 8
7 SSH — *Secure Shell* 16
6 SSH 15
8 Utilisations simplifiées 23
9 Utilisation 25
10 Service d'authentification 28
11 Utilisation de ssh 30
12 Commandes interactives de ssh 33
13 Utilisation de scp et sftp 34
14 SSH — exemple d'utilisation en Intranet . 36
15 Plan 42
16 Système d'impression 43
15 Système d'impression 42
17 Rajouter une imprimante en BSD — client 45
18 Contrôle imprimante à la System V . . . 47
19 Common UNIX Printing System (CUPS) . 49
18 CUPS 48
20 Interfaces utilisateur graphique 51

21 CUPS et BSD 52
22 Interface WWW CUPS 53
23 CUPS et interface System V 54
24 CUPS, PPD et PostScript 57
25 Détection imprimantes dans CUPS . . . 59
26 Plan 61
27 Systèmes de nommage 62
26 Systèmes de nommage 61
28 Système de nommage par fichiers 64
29 NIS 65
28 NIS 64
30 NIS+ 69
31 Introduction DNS 70
30 DNS 69
32 Données cruciales... 72
33 Histoire 73
34 Naissance du DNS 75
35 Principe du DNS 76
36 Hiérarchie de nommage 77
37 Espace de nommage dans Internet . . . 81
38 Nom dans le DNS 84
39 Délégation 86
40 Zones 87
41 Système de résolution 88
42 Résolution d'un nom 89
43 Traduction numéro IP vers nom de domaine 91
44 Mécanisme de cache 94
45 Types de ressources du DNS 97
46 Format d'une zone 102
47 Fichier /etc/resolv.conf 107
48 Fichier /etc/nsswitch.conf 110

49 Vers un resolver indépendant 111
50 Programmes de mise au point 112
51 Programme dig 113
52 BIND 9 117
53 Plan 120
54 Installation (Linux/Debian) 121
55 Exemple de configuration 125
56 Network File System — NFS 128
55 Partage de fichiers avec NFS . 127
57 Exportation de fichiers 131
58 Montage de fichiers via NFS 134
59 Plan 137
60 Auto-monteur 138
59 Auto-montage 137
61 Cartes de montage 140
62 Plan 145
63 Nécessité des sauvegardes 146
62 Archivage des données 145
64 Organisation de sauvegardes 148
65 Dérouleurs de bande 154
66 mt 158
67 dump/restore 160
68 Création de snapshot 163
69 Restauration de / et /usr 165
70 Transport portable de système de fichiers 166
71 tar 168
72 Clonage de système de fichiers 171
73 rsync 173
74 rsnapshot 176

75 partimage 178
76 Interaction avec Windows 179
77 AMANDA 180
76 AMANDA 179
78 Architecture clients-serveur 182
79 Disques tampons 183
80 Planification automatique 184
81 Bandes 186
82 Compression des données 187
83 Formats de sauvegarde 188
84 Changeur de bande 190
85 Y a-t-il un juriste dans la salle ? 191
86 Suivi des opérations 192
87 Courriel de fin de sauvegarde 193
88 amplot 199
89 Vérification des sauvegardes 201
90 Restauration avec index 202
91 Restauration sans index 205
92 Restauration dans le néant 207
93 Résoudre les problèmes 209
92 Conclusion 208
92 Résoudre problèmes . . 208
94 Conclusion 211
93 Finale 210
95 Table des matières 213
96 Index 214