Mémento de l'examen LPI 202 pour la certification LPIC-2

Objet du document :

Ce mémento est la remise au propre de mes notes prises au cours de la formation pour le passage de l'examen LPI 202, dans le cadre de la certification LPIC-2, du Linux Professional Institute

Références du document :

Auteur : David CLAVEAU
Version : 6.9
Date d'enregistrement : 08/11/2012

Tout commentaire est le bienvenu. Merci de m'en faire part sur publication@claveau.net

Notations du document :

Lignes de commandes :	# commande ↵
Chemin :	« /etc/grub/ »
Commande SQL :	*mysql* > commande ; ↵
Commande passée à l'invite interactive de Grub :	*grub* > commande ↵
Commande passée à l'invite interactive FTP :	*ftp>commande* ↵
Contenu d'un fichier :	HOSTNAME=portable_david = Nom du poste
Touche « Entrée » appuyée :	↵
Touche « Contrôle » et « a » appuyées :	« Ctrl+a »
Voir le chapitre 1.4.5	→ § 1.4.5
Référence à une image ou un document externe :	Source : http://fr.wikipedia.org/wiki/X_Window_System Licence : GNU Free Documentation License version 1.2
Commande spécifique à Red Hat ou Debian :	 ou 

Sommaire :

1 Serveur Web Apache....5
1.1 Configuration....5
1.1.1 Fichiers de configuration....5
1.1.2 Directives standards : Section 1- Global Environment....5
1.1.3 Directive de conteneur....5
1.1.4 Réseau....6
1.2 Commandes....6
1.2.1 Gestion du service httpd....6
1.2.2 Commande apachectl....6
1.3 Les modules....7
1.3.1 Configuration....7
1.3.2 Choix des modules....7
1.4 Configuration des performances....7
1.5 VirtualHost = Plusieurs serveurs Web sur la même machine....8
1.6 Redirection par alias ou redirect....8
1.7 Méthodes d'authentification....8
1.7.1 Restriction à un répertoire....8
1.7.2 Authentification locale....9
1.7.3 Authentification par annuaire LDAP....10
1.7.4 Authentification par fichier .htaccess....11
1.7.5 Authentification par SSL....11
1.8 Squid = Serveur proxy....12
2 Partage de fichiers....15
2.1 Samba....15
2.1.1 Configuration 15
2.1.2 Partage de répertoire....15
2.1.3 Gestion des identités....16
2.1.4 Client Samba....16
2.1.5 Montage d'un partage SMB....16
2.1.6 Partage conditionnel....17
2.1.7 Corbeil réseau....17
2.2 NFS....19
2.2.1 Voir les partages déjà actifs....19
2.2.2 Partage ponctuel ou permanent....19
2.2.3 Montage NFS....19
2.2.4 L'effet retry....20
2.2.5 Gestion des identités....20
3 Gestion d'un client réseau....21
3.1 DHCP....21
3.1.1 Commande arp....21
3.1.2 Requête réseau....21
3.1.3 Configuration du serveur....22
3.1.4 Configuration du client....24
3.1.5 Agent relais DHCP....24
3.2 PAM....25
3.2.1 Les principaux modules PAM....25
3.2.2 Format du fichier de configuration....26
3.3 LDAP....27
3.3.1 Définitions....27
3.3.2 Installation....27
3.3.3 Outils de migration en scripts Perle....27
3.3.4 Commande ldapadd....28
3.3.5 Commande ldapsearch....29
3.3.6 Commande ldapmodify....29
3.3.7 Commande ldappasswd....29
3.3.8 Autres Commandes....30
3.3.9 Outils en graphique....30
3.4 Authentification par LDAP....31
3.4.1 Configuration de nsswitch.conf....31
3.4.2 Configuration de PAM....31

4 Serveur de mails....32
4.1 MTA, MDA et protocole SMTP....32
4.1.1 MTA et MDA....32
4.1.2 Protocole SMTP....32
4.1.3 Différents MTA....32
4.2 Utiliser un serveur de mail....33
4.2.1 Open mail relay....33
4.2.2 Sendmail....33
4.2.3 PostFix....34
4.2.4 Realtime Blackhole List = RBL....36
4.2.5 Majordomo....37
4.2.6 MAP avec la directive sender_canonical....37
4.3 Gérer un client mail local....38
4.3.1 La commande mail....38
4.3.2 Format mbox et maildir....38
4.3.3 Procmail....39
4.3.4 Autres commande pour l'envoie de message....41
4.4 Gérer un serveur MDA en POP et IMAP....42
4.4.1 Fonctionnement MTA, MDA et MUA....42
4.4.2 Serveur courrier-IMAP et courrier-POP....42
4.4.3 Serveur Dovecot (POP)....42
5 Sécurité du système....44
5.1 Configurer un routeur....44
5.1.1 Configuration....44
5.1.2 NetFilter et la commande IPTables....45
5.1.3 Administration d'un pare-feu....48
5.2 Sécuriser un serveur FTP....51
5.2.1 Protocole et clients FTP....51
5.2.2 Chrooter un serveur FTP....51
5.2.3 Pure-FTPd....51
5.2.4 VSFtpd : Very Secure FTPd....52
5.2.5 ProFTPd....52
5.3 Sécuriser un serveur SSH....53
5.3.1 Paramètres du fichier de configuration....53
5.3.2 Authentification....53
5.3.3 Confidentialité des communications....55
5.4 TCP Wrapper....57
5.4.1 Fichier /etc/hosts.allow et /etc/hosts.deny....57
5.4.2 Denyhosts....57
5.4.3 Avec ProFTPd....57
5.4.4 Restriction horaire du serveur FTP....58
5.4.5 Changement du port du serveur FTP....58
5.5 Actions et tâches de sécurité....59
5.5.1 Détection des intrusions et des vulnérabilités....59
5.5.2 OpenVAS....59
5.5.3 Commande telnet....59
5.5.4 Commande nmap....59
5.5.5 Commande snort....60
5.5.6 Commande Fail2Ban....61
5.5.7 Commande nc (netcat)....61
6 Détection et résolution des problèmes....62
6.1 Identifier les étapes de démarrage et chargeurs de dépannage....62
6.1.1 Reconnaître les 4 étapes du boot....62
6.1.2 La commande grub-install....62
6.1.3 initrd, initramfs....62
6.1.4 MBR Master Boot Record....62
6.1.5 fichier de configuration /etc/lilo.conf....63
6.1.6 Remplacement des options de Lilo en utilisant le shell....63
6.1.7 Emplacement de l'installation de Lilo....63
6.1.8 Sauvegarde de Lilo....63
6.1.9 Les erreurs de Lilo....64
6.2 Dépannage général....65

6.2.1 Commande ldd....65
6.2.2 Commande ldconfig....65
6.2.3 Commande strace....66
6.2.4 Commande strings....66
6.2.5 Commande ltrace....66
6.2.6 Commande lsof....67
6.2.7 Generic issues with hardware problems....67
6.2.8 Commande rdev, ramsize, vidmode et rootflags....67
6.2.9 Résoudre des conflits IRQ/DMA....68
6.3 Dépannage des ressources système....69
6.3.1 Variables systèmes....69
6.3.2 Définition des paramètres du noyau....69
6.4 Configurations d'environnement de dépannage....70
6.4.1 Core system variables....70
6.4.2 La crontab....70
6.4.3 Commande de manipulation des mots de passe....70
7 Annexes....71
7.1 Liste des ports....71
7.2 Commandes sous /bin....71
7.3 Commandes sous /sbin....71
7.4 Répertoires sous /proc....72
8 Licence Créative Commons....73
8.1 Citations des références utilisées dans cet ouvrage....73

1 Serveur Web Apache

C'est le NCSA qui est à l'origine de ce serveur Web = A PATchy server

1.1 Configuration

1.1.1 Fichiers de configuration

/etc/httpd/conf/httpd.conf
/etc/httpd/conf.d/ssl.conf = Fichier de configuration spécifique inclus dans httpd.conf

/etc/apache2/apache2.conf
/etc/apache2/conf.d/ssl.conf = Fichier de configuration spécifique inclus dans apache2.conf

1.1.2 Directives standards : Section 1- Global Environment

ServerTokens Prod = Prod[uctOnly] = Affiche « Apache », en bas d'une page d'erreur par exemple
Major = « Apache/2 »
Minor = « Apache/2.0 »
Min[imal] = « Apache/2.0.41 »
OS = « Apache/2.0.41 (Unix) »
Full (or not specified) = « Apache/2.0.41 (Unix) PHP/4.2.2 MyMod/1.2 »
ServerRoot = "/etc/httpd" = Répertoire racine de configuration d'Apache
User compte_apache = Désigne le compte utilisateur propriétaire des processus Apache
Group groupe_apache = Idem « User » mais pour le groupe propriétaire
ErrorLog /var/log/apache/error.log = Fichier de log des erreurs
DocumentRoot = Répertoire contenant les fichiers HTML
Listen 80 = Port d'écoute du serveur Web
AccessFileName .htaccess = Définit quel fichier sera scruté dans tous les répertoires pour mettre en place un configuration spécifique au répertoire (si AllowOverride l'autorise). Par défaut = « .htaccess »
Include /etc/httpd/conf.d/*.conf = Fichiers supplémentaires de configuration, comme ssl.conf par exemple

```
<IfModule prefork.c>  = Gestion de la mémoire
StartServers                8  = Nombre de serveur lancé au démarrage
MinSpareServers             5  = Nombre minimum de serveurs Web disponibles
MaxSpareServers            20  = Nombre maximum de serveurs Web disponibles
ServerLimit               256  = Nombre de fork possible
MaxClients                256  = Nombre maximum de client Web
MaxRequestsPerChild      4000  = Nombre maximum de requête possible par fils
</IfModule>
```

1.1.3 Directive de conteneur

Les directives conteneurs permettent de grouper un ensemble de directives appliqués à une partie du site Web

<Directory /var/www/rep_special> = La directive « Directory » est une directive conteneur très utilisée. Elle définit des directives et paramètres pour un répertoire spécifique du serveur Web
Options FollowSymLinks = Les liens symboliques peuvent être suivis, mais seulement dans ce répertoire
AllowOverride all = Toutes les directives inscrites dans le fichier « .htaccess » sont prises en compte (fichier définit par AccessFileName) sont prises en compte.
none = Les fichiers « .htaccess » sont ignorés
AuthConfig = Autorise seulement les directives qui concernent les mécanisme d'authentification
UserDir site/html = définit le répertoire réel du serveur pour localiser le répertoire personnel de l'utilisateur à utiliser lors d'une demande d'un document pour un utilisateur est reçue
Par exemple: http://server/~joe/index.html → /home/joe/site/html/index.html
Require valid-user = L'accès à cette zone nécessite un mot de passe pour les autres utilisateurs
Allow from 192.168.1 = les utilisateurs du réseau sont autorisés à accéder à la zone
Satisfy Any = Politique d'accès dans le cas où on utilise à la fois Allow et Require. L'argument est soit All, soit Any. L'utilisation de cette directive n'a de sens que si l'accès à une zone

particulière du serveur est restreinte par utilisateur/mot de passe et en fonction de l'adresse IP de l'hôte client.
All (par défaut) = Le client doit satisfaire à la restriction d'adresse (Allow From), et fournir un couple utilisateur/mot de passe valide (Required valid-user)
Any = Le client se verra accorder l'accès s'il satisfait à la restriction d'adresse ou fournit un couple utilisateur/mot de passe valide. On peut utiliser cette dernière définition pour restreindre l'accès à une zone par mot de passe, mais accorder l'accès aux clients possédant certaines adresses IP sans qu'ils aient à fournir de mot de passe.

</Directory> = La section définit par une directive conteneur est enourée de « < » et « > ». La fin de la section est indiquée par « </...> »

1.1.4 Réseau

netstat -plantu | grep httpd ↵ =

Affiche les ports utilisés = 80 (http) et/ou https (443)

netstat -plantu | grep apache ↵ =

```
tcp        0      0 :::80                   :::*                    LISTEN      2116/httpd
tcp        0      0 :::443                  :::*                    LISTEN      2116/httpd  = HTTPS
```

1.2 Commandes

1.2.1 Gestion du service httpd

service httpd configtest ↵ = Test les fichiers de configuations
Idem # apachectl configtest ↵

service httpd gracefull ↵ = Redémarre le démon Apache. Si Apache n'est pas lancé, il est démarré. Cela diffère d'un redémarrage normal car les connexions ouvertes ne sont pas avortées et les anciens fichiers journaux ne seront pas fermés immédiatement. Cette commande vérifie automatiquement les fichiers de configuration via « configtest »

1.2.2 Commande apachectl

Apachectl est le script de gestion d'Apache = Apache HTTP Server Control Interface

service httpd stop ↵ = # apachectl stop ↵ = httpd -k stop ↵ =

apachectl -l ↵ = Liste des modules compilés dans le noyau d'Apache
Idem # httpd -l ↵

```
Compiled in modules:
  core.c
  mod_log_config.c
  mod_logio.c
  worker.c
  http_core.c
  mod_so.c
```

apachectl -M ↵ = Affiche les modules statiques (compilés avec le noyau) **ET** ceux chargés par la directive « LoadModule » du fichier de configuration
Ide # httpd -M ↵

```
Loaded Modules:
 core_module (static)
 mpm_prefork_module (static)
 http_module (static)
 auth_basic_module (shared)
 ........
 cgi_module (shared)
 version_module (shared)
Syntax OK
```

apachectl -v ↵ = Version du serveur Web
Idem # service httpd configtest ↵

```
Server version: Apache/2.2.22 (Ubuntu)
Server built:   Feb 13 2012 01:37:45
```

apachectl -V ↵ = Affiche tous les paramètres de compilation

```
Server version: Apache/2.2.22 (Ubuntu)
Server built:   Feb 13 2012 01:37:45
Server's Module Magic Number: 20051115:30
Server loaded:  APR 1.4.6, APR-Util 1.3.12
Compiled using: APR 1.4.5, APR-Util 1.3.12
Architecture:   32-bit
Server MPM:     Worker
  threaded:     yes (fixed thread count)
    forked:     yes (variable process count)
Server compiled with....
 -D APACHE_MPM_DIR="server/mpm/worker"
 -D APR_HAS_SENDFILE
 -D APR_HAS_MMAP
........
 -D DEFAULT_ERRORLOG="logs/error_log"
 -D AP_TYPES_CONFIG_FILE="mime.types"
 -D SERVER_CONFIG_FILE="apache2.conf"
```

apachectl -t ↵ = Test le fichier de configuration

```
httpd: apr_sockaddr_info_get() failed for centos55.localdomain
httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for
       ServerName
Syntax OK
```

1.3 Les modules

Les fonctions accessoires sont fournis par des modules chargés suivant la demande.

1.3.1 Configuration

/etc/httpd/conf/httpd.conf :

`LoadModule dir_module /usr/lib/apache2/modules/mod_dir.so` = Le module « dir_module » sera chargé au démarrage. Le fichier exécutable du module est indiqué (= « mod_dir.so »)

`DirectoryIndex index.html` = Il est maintenant possible d'appeler la directive « DirectoryIndex » qui fait appel à ce module

1.3.2 Choix des modules

Les modules chargés doivent répondrent aux besoins du serveur Web.

Pour utiliser la directive « UserDir », la documentation d'Apache indique que le module « mod_userdir » doit être chargé.

1.4 Configuration des performances

Au démarrage d'Apache, le serveur Web lance d'autres processus qui sont prêts à attendre les requêtes sur le port 80

ps -ef | grep apache ↵

`root 3244 1 0 Feb05 ? 00:00:04 /usr/sbin/apache2 -k start` = Le 1er processus lancé par root

obligatoirement, c'est lui qui lance les autres et qui est le seul autorisé à ouvrir le port 80

```
www-data 3245 3244 0 Feb05 ? 00:00:00 /usr/sbin/apache2 -k start
www-data 3247 3244 0 Feb05 ? 00:00:00 /usr/sbin/apache2 -k start
www-data 3252 3244 0 Feb05 ? 00:00:00 /usr/sbin/apache2 -k start
```

= Le nombre de processus httpd (ou apache2) lancé en + de celui de root est défini par « StartServers », dans la partie « <IfModule prefork.c> » ou « <If Module worker.c> »

1.5 VirtualHost = Plusieurs serveurs Web sur la même machine

Il y a 3 types de VirtualHosts pour différencier les sites Webs :

1. Par une IP différente :
   `<VirtualHost @IP_1:80>` = Le serveur Web virtuelle répondra aux requêtes de l'adresse IP 1 sur le port 80
   ```
   ServerName nom1
   DocumentRoot rep1  = Les pages Web de ce serveur Web sont dans le répertoire1
   </VirtualHost>
   <VirtualHost @IP_2:80>  = 2de @IP sur le port 80
   ServerName nom2
   DocumentRoot rep2
   </VirtualHost>
   ```
2. Par un port différent
3. Par un nom différent, avec la même IP et le même port = directive NameVirtualHost
   Il faut alors décommenter « NameVirtualHost *:80 »
   `NameVirtualHost *:80` = Les hôtes virtuelles se différencient par leur nom. Ils écoutent le port 80, sur toutes les adresses IP (= « *:80 »)
   ```
   <VirtualHost *:80>
   ServerName nom1  = Cet hôte virtuel répondra aux requêtes http://nom1
   DocumentRoot rep1  = Les pages Web de cet hôte virtuel sont dans le répertoire1
   </VirtualHost>
   <VirtualHost *:80>
   ServerName nom2
   DocumentRoot rep2
   </VirtualHost>
   ```

1.6 Redirection par alias ou redirect

La directive Alias permet de stocker des documents dans des zones du système de fichiers situées en dehors de l'arborescence du site web DocumentRoot.

```
Alias  /image  /ftp/pub/image
```

La directive alias est prise en charge par le serveur Web.

Redirect vous permet de dire aux clients où trouver un document déplacé.
La directive redirect est prise en charge par le client.

Dans la description d'un VirtualHost : Rediriger les requêtes HTTP vers le site en HTTPS :

```
Redirect  /admin  https://www.claveau.net/admin
```

1.7 Méthodes d'authentification

1.7.1 Restriction à un répertoire

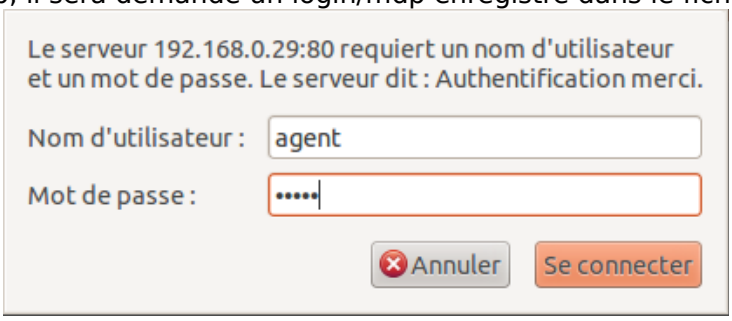
```
<Directory rep_protégé>  = Déclaration du répertoire à protégé, grâce aux directives appliquées pour le contenu de ce répertoire
AuthName "Titre_BdD"  = Titre de la boite de dialogue demandant l'authentification
Require valid-user  = La directive « Require » demande à ce que l'utilisateur soit correctement authentifié (= « valid-user »)
Directive_authentification  paramètre_authentification  = Directive d'authentification avec son paramètre, obligeant l'utilisateur à s'authentifier
</Directory>
```

1.7.2 Authentification locale

1.7.2.1 Création d'une base de données local

htpasswd -c fichier_BdD_locale agent ↵ = Création du 1er compte utilisateur (= « -c ») dans le fichier de base de données locale
New password: *mot_de_passe_de_agent* ↵
Re-type new password: *mot_de_passe_de_agent* ↵ = Confirmation du mot de passe
Adding password for user agent = L'utilisateur est créé

Lors de l'accès au site Web, il sera demandé un login/mdp enregistré dans le fichier_mdp :



htpasswd fichier_BdD_locale utilisateur_2 ↵ = Ajout d'un utilisateur à la base de données locale, ou modifie son mot de passe si utilisateur_2 est déjà dans la base
htpasswd -D fichier_BdD_locale agent ↵ = Suppression du 1er utilisateur (= « -D »)

Fichier_BdD_locale : Exemple d'un fichier de base de données local
cat fichier_BdD_locale ↵
agent:x4OpUoo9KBR1o
utilisateur_2:o9zeMsxnhS45M

1.7.2.2 Chargement des modules

Les modules nécessaires sont :

- auth_basic = Permet l'authentification par un fichier locale.
  Directives AuthBasicAuthoritative et AuthBasicProvider
- authn_file = Pour gérer cette authentification
  Directive AuthUserFile
- authz_user = Gère l'autorisation d'accès aux pages protégées
  Directives AuthzUserAuthoritative

```
LoadModule   auth_basic_module   /chemin/mod_auth_basic.so
LoadModule   authn_file_module   /chemin/mod_authn_file.so
LoadModule   authz_user_module   /chemin/mod_authz_user.so
```

1.7.2.3 Configuration pour l'authentification locale

Les directives suivantes doivent être ajoutées à la section du répertoire à protéger (et qui doit être soumis à cette authentification) :
AuthType Basic
AuthUserFile fichier_BdD_locale = Directive authentification paramètre_authentification

/etc/httpd/conf/httpd.conf : Exemple de fichier de configuration avec authentification

```
ServerRoot /etc/apache2
User www-data
Group www-data
ErrorLog /var/log/apache2/error.log
Listen 80
DocumentRoot /var/www

LoadModule dir_module /usr/lib/apache2/modules/mod_dir.so
DirectoryIndex index.html

LoadModule auth_basic_module /usr/lib/apache2/modules/mod_auth_basic.so
```

```
LoadModule authn_file_module /usr/lib/apache2/modules/mod_authn_file.so
LoadModule authz_user_module /usr/lib/apache2/modules/mod_authz_user.so
<Directory /var/www>  = Le répertoire /var/www est protégé
        Module mod_auth_basic  = Permet d'utiliser l'authentification basique HTTP pour restreindre l'accès
                en recherchant les utilisateurs dans les fournisseurs d'authentification spécifiés
        AuthType basic
        AuthBasicProvider file  = Définir le fournisseur utilisé pour authentifier les utilisateurs (= fichier).
        AuthUserFile  /root/fichier_BdD_locale = Fichier permettant d'authentifier les utilisateurs puisque le
                fournisseur sélectionné est « file ». Module mod_authn_file
        AuthName "Cette page nécessite un mot de passe"  = Message affiché pour l'authentification
        Require valid-user
</Directory>
```

Fournisseurs possibles pour AthBasicProvider :
Assurez-vous que le module implémentant le fournisseur choisi soit bien présent dans le serveur

- file = Fournisseur par défaut. Implémenté par le module mod_authn_file..
- ldap = Implémenté par le module mod_authnz_ldap, il permet d'authentifier les utilisateurs via un annuaire ldap
- dbm = Implémenté par le module mod_authn_dbm, il permet d'authentifier les utilisateurs via des fichiers de mot de passe DBM
- dbd = Implémenté par le module mod_authn_dbd, il permet d'authentifier les utilisateurs via des tables SQL

1.7.3 Authentification par annuaire LDAP

1.7.3.1 Vérification de la disponibilité de l'annuaire

```
ldapsearch -x -D cn=admin,dc=annu,dc=fr -W -h 192.168.1.11 -b ou=users,dc=annu,dc=fr -s sub
        ObjectClass=* ↵
```

= Interrogation des comptes utilisateurs (= « -b ») de l'annuaire avec son adresse IP (= « -h » = hôte), via le compte de l'administrateur (« cn=admin,dc=annu,dc=fr »). La commande demandera le mot de passe (= « -W »), de manière simple (= « -x ») du compte de connexion (= « -D »).
La profondeur de la recherche (= scope) est faite :

- sub = subtree = dans toute la sous-arborescence
- base = uniquement dans l'entrée définie
- one = dans l'entrée définie et le premier sous-niveau

```
Enter LDAP Password:
```
Mot de passe du compte Admin ↵
```
# extended LDIF
#
# LDAPv3
# base <dc=annu,dc=fr> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
# annu.fr
dn: dc=annu,dc=fr
objectClass: domain
dc: annu
.....
# toto, users.annu.fr
dn: uid=toto,ou=users,dc=annu,dc=fr
objectClass: top
objectClass: posixAccount
objectClass: person
.....
```

1.7.3.2 Chargement des modules

Les modules nécessaires pour l'authentification LDAP sont :

- auth_basic = Permet l'authentification par un fichier locale
- authn_file = Pour gérer cette authentification
- authz_user = Gère l'autorisation d'accès aux pages protégées
- authnz_ldap = Permet l'authentification LDAP grâce à la directive « AuthLDAPUrl »

1.7.3.3 Configuration de l'annuaire

```
AuthName  "Authentification LDAP"
AuthType  Basic
Require  Valid-user
AuthLDAPUrl  ldap://192.168.1.11/ou=users,dc=annu,dc=fr?cn?sub?objectclass=*
```

1.7.4 Authentification par fichier .htaccess

Pour restreindre l'accès dans certains répertoire, la bonne pratique est de déclarer une section « <Directory répertoire> » à chaque fois. Il est aussi possible de mettre en place un fichier « .htaccess » dans ces répertoires.

Exemple d'utilisation de la directive « Directory » :

```
<Directory /var/www/protege>
        AllowOverride        all  = A noter que cette directive ne fonctionne pas dans une <Location>
        authType             basic
        AuthName             "Veuillez vous identifier"
        Require              valid-user
        AuthUserFile         /etc/httpd/fichier_mdp
</Directory>
```

Exemple d'utilisation du fichier « .htaccess » :

```
authType      basic
AuthName      "Veuillez vous identifier"
Require       valid-user
AuthUserFile  /etc/httpd/fichier_mdp
```

Si les 2 méthodes entrent en conflit (configuration différente sur le même répertoire), c'est la directive « AllowOverride » qui précise laquelle utiliser :

- none = Les fichiers « .htaccess » sont ignorés
- all = Toutes les directives du fichier « .htaccess » sont prises en compte
- AuthConfig = Autorise seulement les directives du fichier « .htaccess » qui concernent les mécanisme d'authentification

1.7.5 Authentification par SSL

1.7.5.1 Cryptographie et certificat

4 types d'algorithmes :

- Algorithme symétrique : 1 seule clé unique chiffre et déchiffre
- Algorithme asymétrique : Utilise 2 clés. Une clé sera privée et ne sera utilisé que par son propriétaire alors que l'autre sera publique.
- Algorithme de hachage : En sens unique n'utilisant pas de clé

Le certificat permet de garantir le lien entre une identité (nom, adresse , IP) et une clé publique. Ils sont signés par des tiers de confiance « Certificate Authority » (autorité de certification) qui signent le certificat.

Pour un site Web en HTTPS, le navigateur se connecte au serveur qui envoie son certificat. Le certificat envoyé par le serveur contient sa clé publique. Le navigateur vérifie sa validité en s'assurant que le nom du serveur connecté est bien celui mentionné par le certificat.

1.7.5.2 Génération d'un certificat

Apache configuré pour SSL doit donc avoir son certificat intégrant sa clé publique. Ponctuellement ou pour des besoins de test, on peut créer localement son certificat. Des utilitaires (liés à la distribution) peuvent le faire. Il est également possible de construire son certificat manuellement. On choisi alors les mêmes clés pour générer le certificat que pour le signer.

```
# openssl req -x509 -nodes -newkey rsa:1024 -keyout cle_serveurW.cle -out certificat.pem ↵
```

= Demande la création d'un certificat (= « req »), autosigné (= « -x509 ») et non une demande de signature. La clé de serveur n'est pas protégée par mot de passe (= « nodes »). Une nouvelle paire de clé est créé (= « -newkey ») en RSA de 1024 bits (= « rsa:1024 »). Le fichier qui contient la clé

privée sera créé (= « -keyout »), ainsi que le fichier qui contient le certificat (= « -out »)
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'serveur.cle'. You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]: FR ↵ = Les champs nécessaires sont demandés interactivement
State or Province Name (full name) [Some-State]: France ↵
Locality Name (eg, city) []: Toulouse ↵
Organization Name (eg, company) [Internet Widgits Pty Ltd]: ↵
Organizational Unit Name (eg, section) []: LinuxSF ↵
Common Name (eg, YOUR name) []: 192.168.1.1 ↵ = Attention à bien remplir le CN, il est intégré formellement au certificat
Email Address []: publication@claveau.net

1.7.5.3 Configuration SSL

yum install mod_ssl ↵ = Installe « mod_ssl » (module nécessaire au fonctionnement de SSL) et « distcache », le fichier de configuration et les certificats

La définition du VirtualHost (VH) sécurisé par le module mod_ssl se fait dans le fichier de configuration

httpd.conf : Fichier de configuration d'Apache
LoadModule ssl_module modules/mod_ssl.so

SSLVerifyClient require = Exige un certificat client signé par le certificat de votre CA
SSLCertificateFile /etc/ssl/fichier_certificat = Configuration du fichier du certificat
SSLCertificateKeyFile /etc/ssl/chemin/fichier_clé = Configuration du fichier de la clé privée

Listen 443 = L'écoute se fait sur le port 443. On ne met plus « * »
SSLEngine on = Activation du moteur SSL

/etc/httpd/cond.d/ssl.conf : Fichier de configuration SSL
<VirtualHost **www.claveau.net**:443> =
</VirtualHost>

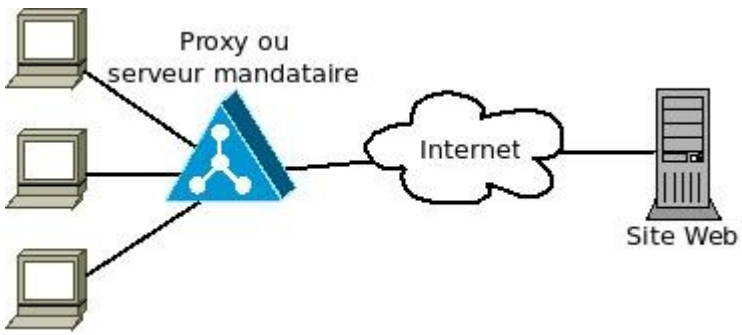
1.7.5.4 Authentification des clients plutôt que la connexion

Le certificat peut servir à garantir une connexion chiffrée, mais également pour garantir l'identité d'un client. Il faut pour cela :

- que le client possède son certificat qui sera vérifié par le serveur Web
- que le serveur Web possède le certificat de l'autorité qui a émis le certificat du client

SSLVerifyClient require = Demande la vérification du certificat du client
SSLCACertificateFile certificat-ca = Configure le certificat le d'autorité de certification

1.8 Squid = Serveur proxy



Un serveur proxy (= « serveur mandataire ») est chargé d'effectuer des requêtes HTTP au nom d'un client. Il protège les clients face aux danger d'Internet car ils sont en 1ère ligne.

Il peut jouer le rôle de cache en gardant sur son disque les réponses d'un 1er client pour les transmettre à un 2d client qui effectuerait la même requête
Il peut filtrer les requêtes en autorisant certain contenu, certaines destinations, etc. Mais seulement pour les protocole HTTP ou HTTPS
Il faut configurer les clients pour qu'ils ne passent que par le serveur proxy.
Utilise le port 3128

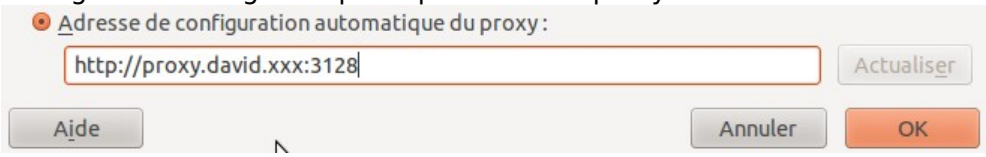
1.8.1.1 Configuration

/etc/httpd/conf.d/squid.conf ou /etc/squid/squid.conf : Fichier de configuration
acl reseau_LAN src 10.0.16.0/20 = Définit « réseau LAN » avec les paramètres du réseau interne
http_port 80 = N° du port sur lequel le serveur écoute (3128 par défaut, 8080 = historique)
http _access allow reseau_LAN = Le réseau est autorisé. Si « deny » (à la place de « allow ») alors tout le réseau est coupé
visible_hostname proxy.david.xxx = Nom du serveur proxy. Apparait dans les logs
cache_dir ufs /var/spool/squid 10000 = Définition d'un cache en UFS (= « ufs ») de 10 Go (= « 10000 » = valeur en Mo par défaut). Cette valeur est faible par défaut (à augmenter suivant le besoin)
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/squid_passwd = Définit quel programme démarre pour l'authentification (ncsa_auth dans cette exemple)

Programmes d'aythentification inclus dans Squid : LDAP, NCSA (nom de user et mot de passe à la forme NCSA), MSNT (Serveur de domain Windows NT), PAM, SMB (serveur Samba), getpwam (utilise un fichier de mot de passe à l'ancienne), SASL (Livrairie SASL), YP (Base de données NIS)

service squid start ↵ = Démarre le service du proxy mandataire

Configurez le navigateur pour qu'il utilise le proxy mandataire :



1.8.1.2 Création d'une liste de contrôle

acl liste_1 src 10.20.23.0/24 = Création de la liste_1 qui définit un réseau précis suivant les adresses IP de la source (= « src »)
acl liste_2 dst 192.168.1.0/24 = Création de la liste_2 qui définit un réseau précis suivant les adresse IP du destinataire (= « dst »)

Exemple :
acl all src all = Liste (= « ALL ») toutes les adresses sources
acl reseau_local src 192.168.1.0/24 = Liste « reseau_locale » pour les adresses IP venant du LAN
acl serveurs_interdits dst 172.11.5.2-172.11.5.5/24 = Liste définissants des adresses IP de destinations qui seront interdites
acl blacklist urlpath_regex "/var/squid/url_blacklist" = Liste d'URL (= « urlpath_regex ») appelé « blacklist » et placée dans le fichier /var/squid/url_blacklist
acl user_authentique proxy_auth REQUIRED = La liste « user_authentique » est obligatoirement passé par le programme d'authification déclaré avec « auth_param »
http_access allow user_authentique = Autorise les membres de la liste user_authentique

D'autres type d'ACL :
srcdomain = Domaine DNS source
dstdomain = Domaine DNS distant
time = Définit une plage horaire
acl plage_horaire_1 time M 9:00-17:00 = La page horaire est féfinit pour une utilisation de lundi de 9:00 à 17:00
port = Définit une liste de ports
acl SSL_ports port 443
acl Safe_ports port 80 = La liste « Safe_ports » est utilisé pour le Web (HTTP)

1.8.1.3 Filtrage des sites par liste noire

squid.conf :
acl liste_noire dstdomain ''/etc/squid/sites_interdits.acl'' = Définition d'une liste noire par un fichier

site_interdits.acl contenant des domaines DNS à contacter (destinataire)
http_access deny liste_noire = Déclare que l'accès est interdit pour ces domaines DNS

/etc/squid/sites_interdits.acl : Définition des sites Webs dans le fichier
www.site-X.fr
www.bloggif.com

1.8.1.4 Filtrage des sites par liste blanche

squid.conf :
acl liste_blanche dstdomain ''/etc/squid/sites_OK.acl'' = Définition d'une liste blanche par un fichier site_OK.acl contenant des domaines DNS à contacter (destinataire)
http_access allow liste_blanche = Déclare que l'accès est autorisé pour ces domaines DNS listés
http_access deny all = Les autres accès sont interdits

Autre exemple :
http_access allow vendeurs plage_horaire_1 = Les users de la liste « vendeurs » accèdent à Internet seulement dans la plage horaire autorisée

/etc/squid/sites_OK.acl : Définition des sites Webs dans le fichier
www.google.fr
www.wikipedia.fr

2 Partage de fichiers

2.1 Samba

2.1.1 Configuration

Samba utilise /etc/bin/smbd et /etc/bin/nmbd.

Ports utilisés :

- 139 et 445 (tcp) pour les partages
- 137 et 138 (udp) pour les connexions réseau (netbios)

/etc/samba/smb.conf : Fichier de configuration
[Global] = Les sections sont entre crochets
workgroup = groupe_de_travail = Nom du domaine ou AD ou Workgroup
server string = commentaire_serveur = Associé au serveur, ce commentaire est affiché dans le voisinage réseau de Windows
log file = /var/log/samba/log.%m = Chemin des fichiers de logs.
1 fichier de log. par machine (= «%m »).
« %S.log » = 1 fichier de log. par partage (= « share »)
max log size = taille_maxi = Taille maximum des fichiers de log.0 = infinie
security = user = Valeur par défaut. Authentification par un compte utilisateur (= workgroup).
« domain » = Contrôleur de domaine NT
encrypt passwords = true = Facultatif car valeur par défaut. Nécessaire pour tous les clients qui transmettent leur mot de passe crypté

testparm ↵ = Vérifie le fichier de configuration, en ignorant les valeurs par défaut
testparm -v ↵ = Toutes les options sont intégrées au compte rendu

```
# testparm smb.conf ↵
Load smb config files from smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
```

2.1.2 Partage de répertoire

/etc/samba/smb.conf = Section partage
[Partage_fichiers] = Nom du partage affiché et vu par les machines Windows
comment = commentaire = Commentaire lié au partage
path = /mnt/partage/repertoire/ = Répertoire à partager. Il doit exister sur le serveur Linux
readonly = yes = Définition d'un partage en lecture seule. Les droits Linux s'appliquent en plus sur le répertoire
browseable = yes = Le partage est visible dans le voisinage réseau Windows. A « no » il est caché mais accessible

Limiter les partages
hide files = /*.mp3/ = Les fichiers MP3 sont cachés (mais accessibles). Les types à cacher sont à placer entre « / »
veto files = /*.mp3/ = Les fichiers MP3 ne sont ni visibles ni accessibles
force create mode = 0755 = Application des droits en effectuant un **OU** logique entre les droits Linux et la valeur de « force create mode ».
Donc les droits définit par la valeur « force create mode » seront OBLIGATOIREMENT mis sur les fichiers créés
create mask = 0660 = Application des droits en effectuant un **ET** logique entre les droits Linux et la valeur de « create mask ».
Donc les droits non définis par la valeur de « create mask » ne seront JAMAIS mis sur les fichiers

créés par samba
A noter que l'application du ET "create mask" ne fonctionne pas avec Windows 2k/XP
force group = claveau = Force la valeur du groupe lors de la création d'un fichier ou d'un répertoire
directory mask = 0755 = Valeur du masque pour la création d'un répertoire
valid users = david = Défini les utilisateurs autorisés à utiliser ou non le partage
valid users = @groupe = tout le groupe est autorisé

Create mask et Force create mode :
Voir http://lugmax.free.fr/IMG/pdf/droits_unix_samba.pdf

2.1.3 Gestion des identités

Les mots de passe sont en général chiffrés sur le système. L'algorithme utilisé appartient à la famille de hachage, c'est un algorithme en sens unique. Avec cet algorithme le mot de passe en clair peut-être chiffré mais pas déchiffré. Les algorithme de hachage les plus courants sont MD4, MD5 ou SHA1.
Le problème est qu'un client Windows présente son mot de passe chiffré en MD4 alors que Linux chiffre les mots de passe MD5 dans le fichier /etc/shadow.
La commande # smbpasswd permet de stocker les fichiers MD4 dans /etc/samba/smbpasswd

smbpasswd -a mon_compte ↵ = Crée un nouveau compte et demande le mot de passe.
smbpasswd mon_compte ↵ = Modifie le mot de passe du compte

/etc/samba/smb.conf
unix password sync = yes = Permet de synchroniser les mots de passe entre Samba et Windows

smbpasswd -d mon_compte ↵ = Désactive le compte Samba
smbpasswd -e mon_compte ↵ = Ré-active le compte Samba
smbpasswd -x mon_compte ↵ = Supprime le compte Samba

2.1.4 Client Samba

smbclient -L serveur_distant -N ↵ = Se connecte sur le serveur Samba distant (= « -L »), en tant qu'anonyme (= « -N ») pour récupérer des informations (services activés sur le serveur, etc.)
Idem -U david … ↵ = Se connecte en tant que « david »

smbclient \\\\192.168.0.1\\data -U david ↵ = Connexion au serveur SMB sur le partage data en tant que user « david ». Les 4 « \ » sont nécessaires si le partage est sous Windows
Enter david's password: *Mot de passe de « david »* ↵
Domain=[WSERVEUR] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
smb: \> ls ↵ = Liste les fichiers sur le partage data

```
  .        D        0  Wed Feb 3 19:28:33 2010
  ..       D        0  Wed Feb 3 19:28:33 2010
  rep1     D        0  Wed Feb 3 18:50:05 2010
  rep2     D        0  Wed Feb 3 19:28:38 2010
  40915 blocks of size 262144. 34718 blocks available
```

smb: \> cd rep1 ↵
smb: \rep1\> ls ↵

```
  .                   D        0  Wed Feb 3 19:28:38 2010
  ..                  D        0  Wed Feb 3 19:28:38 2010
  fichier.txt         A       27  Wed Feb 3 19:15:49 2010
  40915 blocks of size 262144. 34718 blocks available
```

smb: \rep1\> get fichier.txt ↵ = Récupère le fichier. La commande # put permet d'envoyer les fichiers
getting file \un\fichier.txt of size 27 as fichier.txt (2,0 kb/s) (average 2,0 kb/s)
smb: \rep1\> exit ↵

2.1.5 Montage d'un partage SMB

Le protocole cifs a remplacé smbfs, qui n'est plus maintenu. S'il y a des bugs dans smbfs ils ne seront pas corrigés. Le module smbfs est toujours inclus actuellement dans Linux et Samba mais devrait disparaitre à terme.
A l'origine, le protocole cifs ne fonctionnait que pour des clients avec les versions Windows NT4.0 et suivantes ainsi que les serveurs Samba. Pour les versions antérieures de Windows il fallait utiliser smbfs. À partir des kernels Linux 2.6.15 cifs fonctionne avec les anciennes versions de Windows

(9x/Me).

smbmount \\\\serveur_samba\\public point_montage -o user=david ↵
= Monte le partage « public » du serveur Samba sur le point de montage indiqué, en tant que l'utilisateur « david (= « -o user »)

mount -t smbfs -o username = david //adresse_serveur/partage point_montage ↵
= L'option « -t smbfs » permet d'appeler la commande smbmount

mount -t cifs //10.0.20.49/public /mnt/partage_smb ↵ = Monte le partage public du serveur distant sur la partition /mnt/partage.
Idem \\\\ 10.0.20.49\\public … ↵ = Pour un partage sur un serveur Windows

smbstatus ↵ = Affiche les partages et les utilisateurs connectés

/etc/samba/smbusers :
Fait la correspondance Linux ↔ Windows.
Il faut alors ajouter dans le fichier smb.conf : usermap = /etc/samba/smbusers

Commande smbclient
smbclient -a david ↵ = Ajoute le user david dans Samba
smbclient -d david ↵ = Désactive (= disable) le user
smbclient -e david ↵ = Valide (= enable) le user
smbclient -x david ↵ = Supprime le user
smbclient -m PC ↵ = Rattache la machine PC au domaine

2.1.6 Partage conditionnel

Utilise les option « preexec » et « postexec »

/etc/samba/smb.conf
[CD]
root preexec = /bin/mount -o loop /root/boot.iso /mnt/boot
= Dès que l'on accède au partage « CD », le fichier boot.iso est monté dans le répertoire /mnt/boot
root postexec = /bin/umount -f /mnt/boot
= Démonte le fichier boot.iso dès que l'on sort du partage, en forçant (= « -f »)

2.1.7 Corbeil réseau

Informations tirées de l'article « La corbeille dans les partages Samba » du site SynerGeek.fr
Samba HOWTO Collection – VFS
Source : http://www.synergeek.fr/la-corbeille-dans-les-partages-samba/

Lorsque l'on supprime un fichier sur un dossier partagé Windows, il va directement aux oubliettes. Or, tout le monde a pris l'habitude de pouvoir récupérer le fichier via la Corbeille
Il existe sous Samba, une façon d'activer une corbeille sur un partage grâce au module Recycle (/usr/lib/samba/vfs/recycle.so).

smb.conf : Exemple de configuration de la corbeille pour un partage
[Partage]
path = /shares = La corbeille ne s'applique qu'au partage « /shares »
public = yes
writable = yes
browsable = yes
valid users = alice bob eve oscar

vfs object = recycle
recycle:repository = .RecycleBin/%U = Indique où seront stockés les fichiers supprimés. %U = nom de l'utilisateur/ On aura un sous-répertoire dans le dossier .RecycleBin créé portant le nom de l'utilisateur ayant supprimé le fichier. Si Alice supprime un fichier, il sera stocké vers .RecycleBin/alice
recycle:keeptree = Yes = Indique si la structure des répertoires doit être conservée
recycle:touch = Yes = Indique si la date d'accès du fichier doit être modifié lors du déplacement dans la

corbeille
recycle:versions = Yes = En activant cette option, deux fichiers supprimés ayant le même nom seront conservés tous les deux. La version la plus récente supprimée s'appellera "Copy #x of nomdufichier"
recycle:maxsize = 0 = Les fichiers ayant une taille de 0 octet ne seront pas envoyés à la corbeille
recycle:exclude = *.tmp = Liste les fichiers qui ne passeront pas par la corbeille
recycle:exclude_dir = /tmp = Même chose que pour recycle:exclude mais pour les répertoires
recycle:noversions = *.ppt = Spécifie une liste des chemins d'accès (les caractères génériques tels que « * » et « ? » sont pris en charge) pour qui aucun contrôle de version ne doit être utilisée. Seulement utile lorsque "recycle:versions" est activé

2.2 NFS

2.2.1 Voir les partages déjà actifs

exportfs -v ↩ = Gère la liste des systèmes de fichiers partagés par NFS , en mode verbeux (= « -v »)
/data/perso <192.168.0.20> (rw,wdelay,root_squash,no_subtree_check)
= Le répertoire /data/perso est partagé seulement pour l'adresse 192.168.0.20
/nas <world> (ro,wdelay,root_squash,no_subtree_check)
= Le répertoire /nas est partagé pour tout le monde

nfsstat ↩ = Vérifie l'activité (ou l'absence d'activité) d'un serveur NFSen affichant des statistiques sur l'activité des clients et du serveur NFS

Server rpc stats:

calls	badcalls	badauth	badclnt	xdrcall
12	0	0	0	0

Server nfs v3:

null		getattr		setattr		lookup		access		readlink	
2	18%	2	18%	0	0%	2	18%	1	9%	0	0%
read		write		create		mkdir		symlink		mknod	
0	0%	0	0%	0	0%	0	0%	0	0%	0	0%

.....

2.2.2 Partage ponctuel ou permanent

exportfs @IP_client:/chemin_partage ↩ = Le répertoire /chemin_partage est partagé pour l'adresse IP indiqué. Si on indique « * », alors le partage et pour tout le monde
Attention, ici la sécurité est basée sur la seule adresse IP du client

/etc/exports : Déclaration de partage permanent. Fichier lu à chaque démarrage du service NFS
/chemin_partage @IP_client = Les partages sont en chemin absolu, depuis la racine
/data/perso 192.168.0.20
/usr/local/share nfsclient(rw,sync) = Partage du répertoire en lecture/écriture

exportfs -a ↩ = Lit le fichier /etc/exportfs (= « -a ») et monte les partages déclarés

Le service NFS gère le lancement de 3 démons :
- portmap = Gère les requêtes RPC
- nfsd = Démon du client
- mountd = Gère le montage des clients

La commande # rpcinfo peut effectuer des requêtes RPC sur des serveurs distants et ainsi récupérer des informations comme les démons qui sont gérés sur le serveur

2.2.3 Montage NFS

showmount --exports @IP_serveur_nfs ↩ = Affiche les partages du serveur NFS

mount -t nfs 10.0.20.51:/tmp /mnt/partage_nfs ↩ = Monte le partage /tmp du serveur distant 10.0.20.51, dans le répertoire locale /mnt/partage_nfs

mount -o nolock srv1:/data /mnt/data

Tout ce qui est écrit dans un partage NFS est fait en tant que « nfsnobody »

/etc/exports :
no_root_squash = Affiche l'UID du propriétaire plutôt que nfsnobody

service nfsd restart ↩ = A faire après le changement du fichier /etc/exports
OU # exportfs -a ↩ = Recharge le fichier /etc/exports

Attention si des utilisateurs différents ont le même UID, car le partage utilise l'UID du propriétaire.

il faut mettre en place alors NIS.

Options de montage « -o ... » :
Peuvent être utilisées avec la commande # exportfs ou dans /etc/exports. Si il y a plusieurs options, elles sont séparées par une virgule
ro = Accès en lecture seule
rw = Accès en lecture et écriture
sync = Accès en écriture synchrone (écriture immédiate)
async = Accès en écriture asynchrone (utilise un cache pour l'écriture)
root_squash ou no_root_squash= Spécifie que le root de la machine cliente n'a pas les droits de root sur le répertoire partagé. « no_root_squash » spécifie que le root de la machine cliente a les droits de root sur le répertoire partagé. L'option *root_squash* est l'option par défaut
nolock = Ne pas utiliser de verrouillages, ne pas lancer lockd. Utilisé pour d'ancien montage NFS

Exemple de partage /data en lecture seule
exportfs -o ro *:/data ↵
Ou bien
/data *(ro) = Dans le fichier /etc/exports

Exemple de partage /data en lecture/écriture, pour « user »
/data user (rw,sync) = Dans le fichier /etc/exports. L'option « sync » est par défaut

2.2.4 L'effet retry

L'effet retry du NFS permet de retenter la montage NFS pendant 10000 minutes (≈ 7 jours).

/etc/fstab :
10.0.20.51:/tmp /mnt/partage_nfs nfs defaults,retry=10,rsize=8192,wsize=8192,intr,soft,bg 0 0
retry=10 = Modifie la valeur du retry à 10 minutes au lieu de 10000
intr = Autorise le Ctrl+c
soft = Spécifie si le programme utilisant un fichier via une connexion NFS doit s'arrêter et attendre (= « hard ») que le serveur NFS revienne en ligne, s'il n'est pas disponible ou s'il doit au contraire émettre un message d'erreur (= « soft »). Si l'option « hard » est spécifiée, l'utilisateur ne peut pas mettre fin au processus attendant le rétablissement de la communication NFS à moins que l'option « intr » soit également spécifiée
bg = backgroud

2.2.5 Gestion des identités

Lors d'une connexion à un partage NFS, aucune demande d'authentification n'est faite. L'utilisateur qui se connecte se présente au serveur NFS avec son UID, et obtient les mêmes droits que le user ayant le même UID sur le serveur.
L'option « root_no_squash » considère l'utilisateur root distant comme root local. Si cette option est sélectionnée, l'utilisateur root n'est pas lié à l'utilisateur anonyme et le compte root d'un client dispose de privilèges root sur les répertoires exportés. Cette option peut considérablement réduire le niveau de sécurité du système. Ne la sélectionnez que si cela s'avère absolument nécessaire.

3 Gestion d'un client réseau

3.1 DHCP

Mots clés certification LPI 202 : dhcpd.conf, dhcpd.leases, /var/log/daemon.log, /var/log/messages, arp, dhcpd

Ports utilisés :

- 67 = Serveurs
- 68 = Client

/var/lib/dhcp/dhcp.leases : Fichier de log

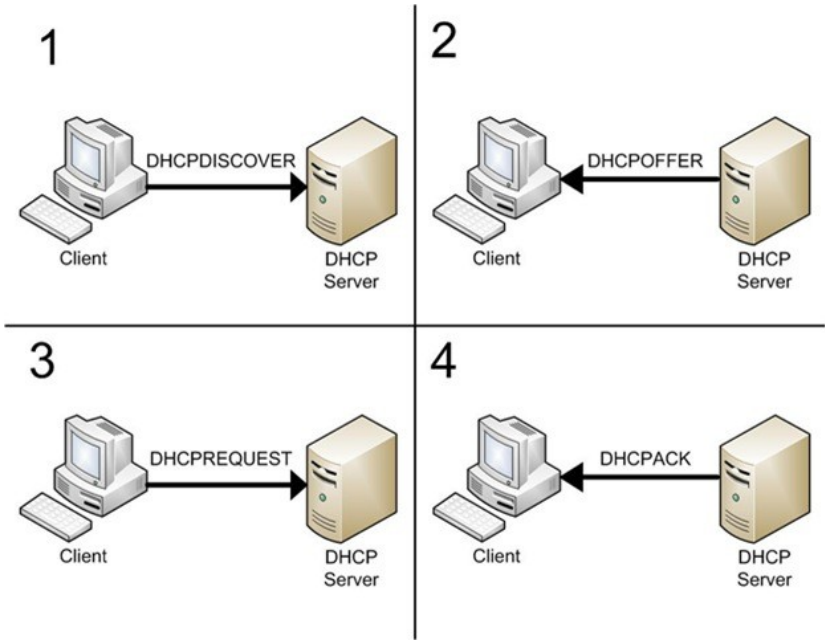
3.1.1 Commande arp

arp -a -n ↵ = Affiche la table ARP (= « -a ») sans réaliser de résolution de nom (= « -n »)
arp -s @_IP @_MAC ↵ = Ajoute une nouvelle résolution entre l'adresse IP de la machine → son adresse MAC
arp -d @_IP ↵ = Supprime l'adresse IP dans le cache

vim /etc/ethers ↵ = Renseigne des nouvelles résolutions
00:24:D4:A4:21:B5 192.168.0.250
00:22:5F:6E:B9:B5 192.168.0.11

arp -f ↵ = Intègre les nouvelles résolutions du fichier /etc/ethers (= « -f »), dans la table ARP
arp -f fichier_arp ↵ = Intègre les nouvelles résolutions du fichier arp

3.1.2 Requête réseau



Tirée du site : http://www.tech-juice.org/2011/06/21/the-dhcp-protocol-for-ipv4-explained/
Source : http://www.tech-juice.org/wp-content/uploads/2011/06/dhcp_steps.jpg
Creative Commons Attribution 3.0 Unported License

DHCPDISCOVER = Paquet envoyé par le client en broadcast, pour la découverte d'un serveur DHCP sur le réseau
DHCOFFER = Paquet envoyé par un ou plusieurs serveurs DHCP en broadcast, pour proposer au client une adresse IP et des paramètres réseau
DHCPREQUEST = Paquet envoyé par le client en broadcast, pour informer le serveur DNS que le client accepte les paramètres réseau envoyés. Cette requête est en broadcast afin d'avertir tous les autres serveurs DHCP (car ils peuvent être plusieurs) de cette acceptation
DHCPACK = Paquet envoyé par le serveur au client qui clos la transaction. Le serveur informe le client de

la durée du bail (durée de l'allocation de l'adresse IP)

3.1.3 Configuration du serveur

3.1.3.1 /etc/dhcp.conf : Fichier de configuration

authoritative ; = Facultatif. Un client ne pourra pas demander le renouvellement d'une adresse IP en dehors de la plage d'adresses IP configurée par le serveur
log-facility auth ; = Renvoie les événements vers le « facility » configuré = authpriv, cron, daemon, ftp, kern, lpr, mail, mark, news, ntp, security, syslog, etc.

option domain-name claveau.net ; = Suffixe DNS pour les clients
option domain-name-servers dns1.claveau.net,dns2.claveau.net ; = Serveurs DNS utilisé par les clients (séparés par une « , »)

ddns-update-style interim ; = Permet de synchroniser un serveur DHCP avec un serveur DNS (bind)
ignore client-updates ; = La mise à jour est faite par le serveur DHCP

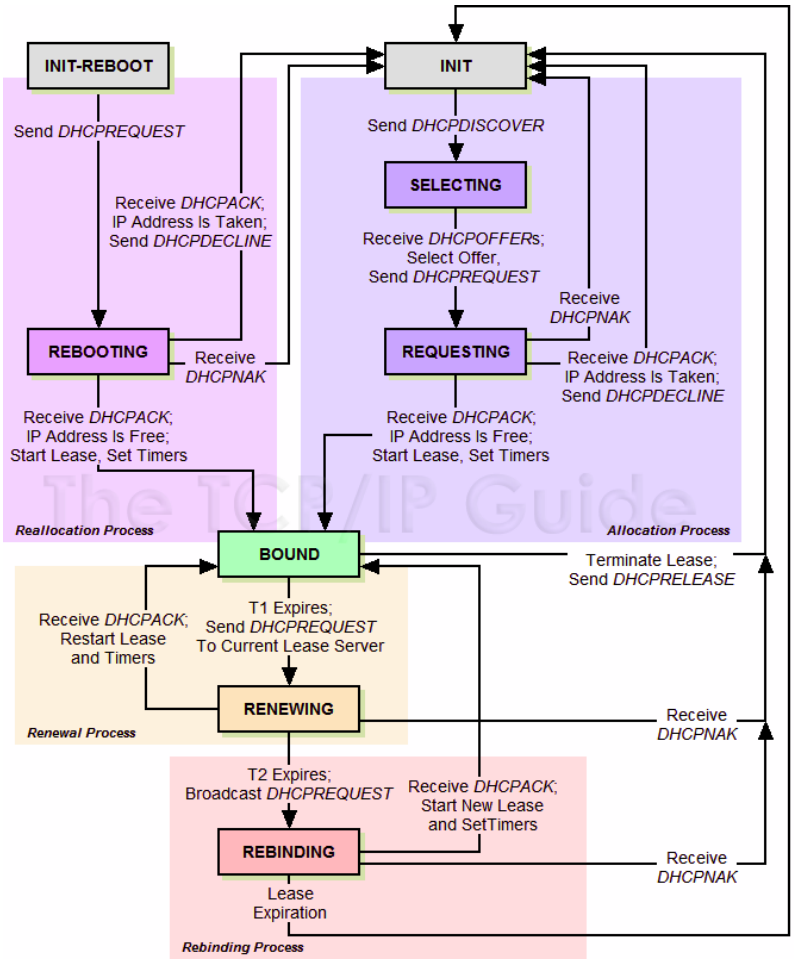
subnet 192.168.0.0 netmask 255.255.255.0 { = Obligatoire. Le serveur DHCP doit se trouver sur le réseau pour lequel il loue les adresses IP
options routers 10.0.31.254 ; = Informations transmises aux clients. Il peux y avoir plusieurs GW, d'où « router**s** »
option subnet-mask 255.255.255.0 ; = Masque de sous-réseau transmis au client
range dynamic-bootp 10.0.20.57 10.0.20.60 ; = Plage des @IP qui seront louées. Lorsque la plage se réduit à une seule adresse, l'adresse supérieure (high-address) peut être omise.
« dynamic-bootp » peut être spécifiée pour indiquer que les adresses de la plage peuvent être assignées dynamiquement aussi bien aux clients DHCP que BOOTP.
default-lease-time 21600 ; = Durée du bail par défaut en seconde
max-lease-time 43200 ; = Durée maximale (en seconde) avant le renouvellement du bail
option domain-name-servers dns3.claveau.net ; = Serveur DNS pour ce réseau
options broadcast 10.0.31.255 = Adresse de broadcast pour ce réseau
}
}

host PC1 { = Définition d'une machine spécifique. Si l'identification par @MAC est utilisée, alors le nom de la machine (= « PC1 ») n'est pas nécessaire
hardware ethernet 08:00:27:0C:59:D1 ; = @MAC de la machine
fixed-address 10.0.20.56 ; = @IP à attribuer à la machine
option routers 10.0.31.254 ; = @IP de la passerelle (1 seule GW dans ce cas)
option domain-name claveau.net ; = Suffixe DNS pour cette machine
option domain-name-servers dns1.claveau.net ; = Serveur DNS pour cette machine
next-server serveur_DHCP2 ; = Précise un autre serveur DHCP si nécessaire pour lui donner la main
}

3.1.3.2 Ecoute sur plusieurs interfaces

/etc/default/dhcp3-server : Spécifier toutes les interfaces
INTERFACES="eth0 eth1" = L'écoute se fait sur eth0 et eth1.

3.1.3.3 Voir les baux DHCP



Tirée du site : http://www.tcpipguide.com/free/t_DHCPGeneralOperationandClientFiniteStateMachine.htm de Junefire DTP
Source : http://www.tcpipguide.com/free/diagrams/dhcpfsm.png
Licence : http://www.tcpipguide.com/la.htm

/var/lib/dhcp/dhcpd.leases = Fichier de log. Conserve une information sur chacun des baux alloués

```
lease  {
        interface "eth0" ;
        fixed-address 192.168.1.51 ;
        option subnet-mask 255.255.255.0 ;
        option routers 192.168.1.254 ;
        option dhcp-lease-time 864000 ;
        option dhcp-message-type 5 ;
        option domain-name-servers 194.2.0.20,194.2.0.50 ;
        option dhcp-server-identifier 192.168.1.1 ;
        renew 6 2010/07/10 14:55:34 ;
        rebind 3 2010/07/14 14:33:58 ;
        expire 4 2010/07/15 20:33:58 ;
}
```

MEDIUM = Le client DHCP est en train de demander la configuration du type de support physique d'une interface
PREINIT = Le client DHCP client est en train de demander la configuration de l'interface avant de recevoir une véritable adresse
BOUND = Le client DHCP a fait l'acquisition d'une nouvelle adresse
RENEW = Lorsque qu'une concession a été renouvelée, les paramètres persistants qui peuvent avoir changés doivent être effacés (par exemple, si une route locale associée à une adresse est en train d'être configurée, l'ancienne route locale doit être effacée)
REBIND = Le client DHCP a été réassocié à un nouveau serveur DHCP
REBOOT = Le client DHCP a récupéré avec succès son ancienne adresse IP après un redémarrage
EXPIRE = Le client DHCP a échoué dans le renouvellement ou dans l'acquisition d'une nouvelle concession, et la sienne a expiré. L'adresse IP doit être abandonnée, et tous les paramètres associés doivent

être effacés, comme dans RENEW et REBIND
FAIL = Le client DHCP a été incapable de contacter un serveur DHCP et toutes les concessions testées étaient invalides
TIMEOUT = Le client DHCP a été incapable de contacter un serveur DHCP dans les temps

3.1.4 Configuration du client

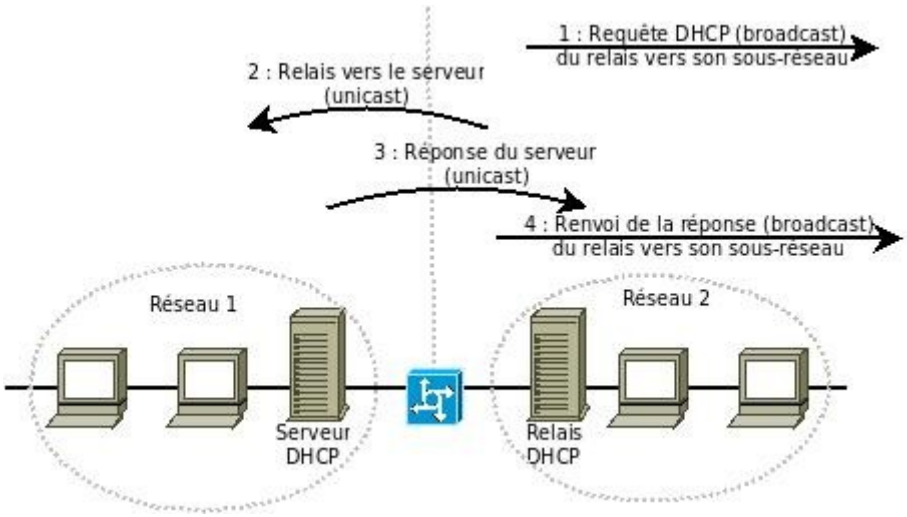
Le démon du client est dhcp**c**d

dhclient eth1 ↵ = Effectue une requête DHCP pour demander une adresse IP
Internet Systems Consortium DHCP Client V3.1.3
.....
Listening on LPF/eth1/00:22:68:98:8a:da
Sending on LPF/eth1/00:22:68:98:8a:da
Sending on Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 8
DHCPOFFER of 172.18.142.243 from 172.18.142.225
DHCPREQUEST of 172.18.142.243 on eth1 to 255.255.255.255 port 67
DHCPACK of 172.18.142.243 from 172.18.142.225
bound to 172.18.142.243 -- renewal in 49 seconds.

dhclient -r eth1 ↵ = Libère (= « -r ») une adresse IP
There is already a pid file /var/run/dhclient.pid with pid 2735
.....
Listening on LPF/eth1/00:22:68:98:8a:da
Sending on LPF/eth1/00:22:68:98:8a:da
Sending on Socket/fallback
DHCPRELEASE on eth1 to 172.18.142.225 port 67

3.1.5 Agent relais DHCP

La fonction DHCP utilise des requêtes brodcast. Ces requêtes ne passent pas les routeurs (contrairement aux requêtes unicast). Il est possible de mettre en place 1 serveur par segment réseau mais on peut également utiliser des relais DHCP



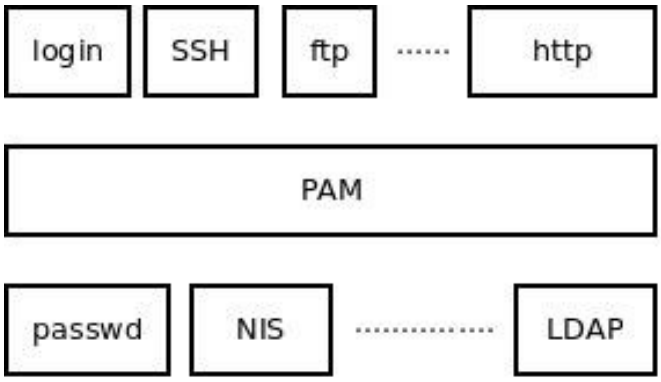
La configuration des 2 réseaux est centralisée dans le serveur DHCP. La communication entre le serveur et son relais se fait en unicast (qui peut passer les réseaux).

dhcrelay -i eth1 @serveur_dhcp ↵ = Sur le relais DHCP, la commande démarre le service en précisant l'interface eth1 (= « -i » = facultatif) et l'adresse IP du serveur DHCP

Autres options :
-p = Port sur lequel dhcrelay écoute
-q = « quiet » = N'affiche pas la configuration au démarrage

3.2 PAM

Mots clés certification LPI 202 : /etc/pam.d, pam.conf, nsswitch.conf, pam_unix, pam_cracklib, pam_limits, pam_listfile



Le principe de PAM est qu'il propose une couche d'abstraction entre les applications et les méthodes d'authentification. L'application n'a qu'à être compatible PAM. Elle demandera à PAM si un utilisateur est autorisé et PAM appellera le module correspondant à la méthode d'authentification. Si l'utilisateur est autorisé, PAM en informera l'application.

Il existe un nombre très important de modules correspondant à de nombreuses méthodes d'authentification.
Certains modules ne sont pas en relation avec une méthode d'authentification et permettent le déclenchement d'actions.

3.2.1 Les principaux modules PAM

/lib/security = Répertoire des modules PAM

pam_security.so : Vérifie que root se connecte depuis une console sécurisée, listée dans le fichier /etc/security

pam_nologin.so et le fichier /etc/nologin : Module « pam_nologin » = Si le fichier /etc/nologin existe (même vide), alors aucune connexion n'est possible hormis pour root. Le contenu du fichier est affiché pour les autres users

ls -l /etc/nologin ↵
-rw-r--r-- 1 root root 51 Oct 17 17:15 /etc/nologin
ssh agent@192.168.0.29 ↵ = Tente de se connecter au serveur malgré la présence du fichier nologin
agent@192.168.0.29's password: *mot_de_passe* ↵
Ce serveur est en maintenance = Affiche le contenu du fichier /etc/nologin
Pas de connexion possible, merci
Connection closed by 192.168.0.29 = La connexion est coupée

pam_env.so : Déclare les variables d'environnement qui sont inscrites dans /etc/environnement ou dans le fichier déclaré par la variable « envfile = »

pam_unix.so : Permet d'utiliser les fichiers /etc/passwd et /etc/shadow pour l'authentification

pam_permit.so : Renvoie un retour positif à chaque demande
pam_deny.so : Renvoie un retour négatif à chaque demande

pam_limit.so : Utilise le ficher /etc/security/limits.conf pour limiter certaines fonctions à des utilisateurs

pam_cracklib.so : S'assure que le mot de passe envoyé a un niveau de sécurité suffisant

pam_console.so : Permet de contrôler l'accès aux périphériques par la console

pam_selinux.so : Si SELinux est activé, s'assure que le shell est exécuté dans un contexte adéquat

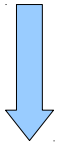
pam_lastlog.so : Affiche des informations sur la dernière ouverture de session réussie

pam_mail.so : Vérifie la présence de nouveaux mails pour un utilisateur

pam_list.so :
Autorise ou refuse les services suivant le contenu d'un fichier
auth required **pam_listfile** item=user sense=allow file=/etc/ssh/liste_blanche = Si « sense=deny », alors il s'agira d'une liste noire

Par exemple pour une authentification : Plusieurs modules peuvent se suivre successivement

1. failday = Change le délai d'échec
2. issue
3. securetty
4. env
5. unix
6. deny



3.2.2 Format du fichier de configuration

/etc/pam.d/XXX : Emplacement des fichiers de configuration. Le fichier pam.conf n'est plus utilisé

Type d'action	Contrôle = Comment le module doit réagir au succès ou à l'échec	Module	Arguments
auth, account, password ou session	required, optional, binding, sufficient ou requisit	Fichier pam_*module*.so (= Static Object) Stockés sous /lib/security	Paramètres optionnels

3.2.2.1 Type d'action

auth = Activité d'authentification
account = Gestion des comptes
session = Gestion de la session
password = Gestion des mots de passe

3.2.2.2 Contrôle

Requisite = Doit réussir, on ne continue pas à lire les autres modules, Echec est renvoyé immédiatement.
Required = Doit réussir, mais on continue à tester les autres modules malgré tout. Échec est renvoyé à la fin. L'avantage par rapport à « requisite » est que l'on ne donne pas la raison de l'échec
Optional = Est ignoré, en fait que le test réussisse ou pas cela ne change pas la suite.
Sufficient = Si le test est correct, on obtient immédiatement une acceptation. Sinon le reste de la chaîne est exécuté.
Binding = Idem Sufficient mais un échec est envoyé si le test ne réussit pas

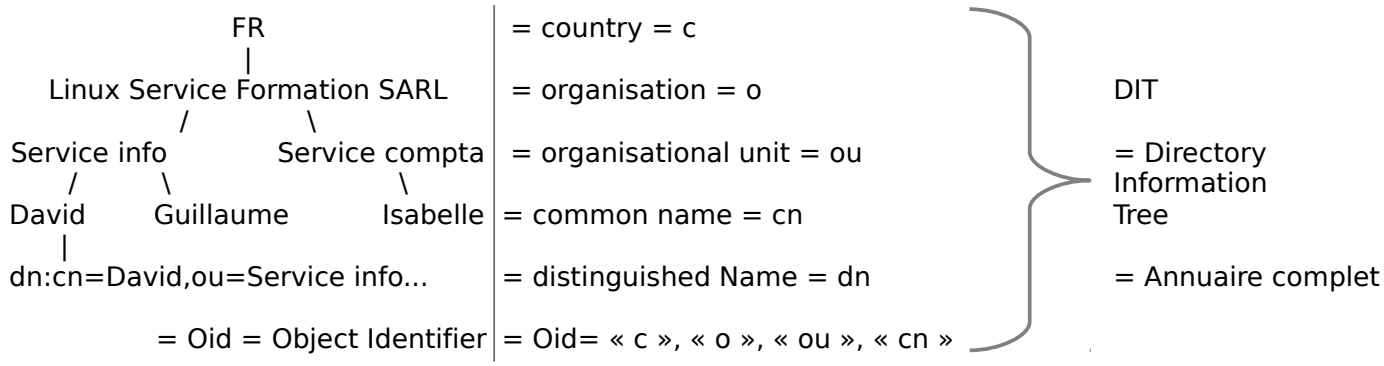
Exemple :
auth required pam_securetty.so = Vérifie que le compte qui se connecte n'est pas celui de root
auth required pam_unix.so = Réalise l'authentification avec le fichier /etc/passwd
account required pam_unix.so = Même module mais sous le type d'action « account », pour que les applications qui en ont besoin puissent récupérer des informations sur le compte qui se connecte
session required pam_env.so readenv=1 envfile=/etc/default/locale = Sous le type « session » le module « pam_env » est exécuté et déclare les variables d'environnement du fichier « locale »
password required pam_cracklib.so retry=3 minlen=6 = Si une application de gestion de mot de passe (compatible PAM) souhaite modifier un mot de passe, elle devra le faire avec les contraintes de pam_cracklib = 3 essais maximum et une longueur de 6 caractères minimum

3.3 LDAP

Mots clés certification LPI 202 : ldapsearch, ldappasswd, ldapadd, ldapdelete

3.3.1 Définitions

Format LDIF = LDAP Data Interchange Format = Format des fichiers échangés sur serveur LDAP



3.3.2 Installation

yum install openldap-servers ↵

/etc/openldap/slapd.conf : Fichier de configuration du serveur
include /etc/openldap/schema/core.schema = Brique de base permettant de catégoriser les objets ...
include /etc/openldap/schema/cosine.schema ... et donne accès à des directives
include slapd.access = SASL = Couche d'authentification et de sécurité simple (Simple Authentication and Security Layer)= Un cadre d'authentification et d'autorisation standardisé
database bdb = Format de la base de données = Berkeley DataBase ou « hdb » = Développé ensuite
suffixe ''dc=mon_domaine''
rootdn ''cn=compte_admin,dc=mon_domaine'' = distinguished name du compte administrateur de l'annuaire. Il n'est pas nécessaire qu'il soit également administrateur du système
rootpw secret = Mot de passe du gestionnaire du site (en clair)
rootpw {MD5}sdF943SDFE05 = A la place de mettre le mot de passe en clair, on peut déclarer le format de cryptage (= MD5 ou SHA1 ou crypt, entre « { } ») et le mot de passe crypté.
La commande # slappasswd permet de générer le mot de passe crypté

service ldap start ↵
Le serveur tourne sur le port 389

3.3.3 Outils de migration en scripts Perle

Ensemble de scripts Perl pour migrer les utilisateurs, les groupes, les alias, les hôtes, les groupes réseau, les réseaux, les protocoles, les CPR et les services de nameservices existantes (fichiers plats, NIS et NetInfo) à LDAP.

ls /usr/share/openldap/migration ↵
migrate_networks.pl migration-tools.txt migrate_all_nisplus_offline.sh migrate_fstab.pl
migrate_aliases.pl migrate_all_offline.sh migrate_hosts.pl migrate_protocols.pl
migrate_netgroup.pl migrate_slapd_conf.pl migrate_all_nis_online.sh migrate_common.ph
migrate_rpc.pl migrate_all_netinfo_online.sh migrate_automount.pl
migrate_passwd.pl migrate_all_nisplus_online.sh migrate_group.pl migrate_profile.pl
migrate_all_netinfo_offline.sh migrate_all_online.sh migrate_netgroup_byhost.pl
migrate_netgroup_byuser.pl migrate_services.pl migrate_all_nis_offline.sh migrate_base.pl

Les fichiers /usr/share/openldap/migration/README et migration-tools.txt fournissent davantage de renseignements sur ces scripts

Les scripts Perl peuvent convertir les mots de passe des utilisateurs du système (/etc/passwd) en mot de passe LDAP :

1. # vi /usr/share/openldap/migration/migrate_common.ph ↵ = Le fichier doit être modifié de

manière à ce qu'il reflète le domaine approprié.
Default DNS domain
$DEFAULT_MAIL_DOMAIN = "claveau.net";
Default base
$DEFAULT_BASE = "dc=claveau,dc=net";

2. # ./migrate_passwd.pl /etc/passwd > passwd.ldif ↵ = Lance le script de conversion des mots de passe des utilisateurs = convertis le fichier /etc/passwd + shadow dans 1 seul fichier

3. # ./migrate_group.pl /etc/group > group.ldif ↵ = Idem pour les groupes

4. # ./migrate_base.pl > base.ldif ↵ = Crée le « tronc commun » de l'annuaire en LDIF
cat base.ldif ↵
dn: dc=claveau,dc=net
dc: claveau
objectClass: top
objectClass: domain

dn: ou=Hosts,dc=claveau,dc=net
ou: Hosts
objectClass: top
objectClass: organizationalUnit

5. Il ne reste plus qu'à ajouter les fichiers base + groupe + mot de passe à l'annuaire

ldapadd -x -h @IP_serveur_ldap -D ''cn=root'' -W -f fichier.ldif ↵ = Le fichier est ajouté à l'annuaire

Exemple d'un fichier LDIF :
dn: cn=toto,dc=claveau,dc=net
objectClass: person
cn: toto
sn: toto
telephoneNumber: 0123456789

6. # ldapadd -x -h localhost -D ''cn=root'' -W -f base.ldif ↵
= La base est ajouté à l'annuaire. Une authentification « simple » est utilisé (= « -x » = login ni mdp), sans passer par SASL ou Kerberos, sur la machine locale (= « -h » = host). La connexion se fait en tant que (= « -D »), le mot de passe est demandé de façon interactive (= « -W »)

7. # ldapadd -x -h localhost -D ''cn=root'' -W -f passwd.ldif ↵ = La base des utilisateurs est ajoutée à l'annuaire

8. # ldapadd -x -h localhost -D ''cn=root'' -W -f group.ldif ↵ = Idem que pour le fichier « passwd.ldif », on ajoute dans ce cas la base des groupes

9. # export LDAPBASE=dc=linuxfoo,dc=com ↵
OU # vi ldap.conf ↵ =
BASE dc=linuxfoo,dc=com = L'attribut BASE indique le DN de la base ldap

3.3.4 Commande ldapadd

Options de # ldapsearch :
-D dn_admin = S'authentifie avec le distinguished name « dn_admin »
-W = Demande le mot de passe de façon interactive
-w mot_de_passe = Passe le mot de passe en clair dans la ligne de commande
-h @IP_serveur_ldap = S'adresse au serveur LDAP en précisant son adresse IP
-H http://url_serveur_ldap:port = S'adresse au serveur LDAP en précisant son URL et le port
-s sub = Effectue une recherche récursive dans tous les niveaux subordonnés au contexte
-b = Base de recherche dans l'annuaire

3.3.5 Commande ldapsearch

Ldapsearch intègre les même options que # ldapadd

ldapsearch -x -H ldap://localhost -b "dc=claveau,dc=net" "(uid=garf*)" ↵
= Recherche de tous les uid commençant par "garf" à partir de la racine de l'annuaire, sur le contexte donné par « -b »

ldapsearch -x -H ldap://localhost -b dc=claveau,dc=net "(gidNumber=2000)" ↵
= On recherche toutes les entrées ayant un gidNumber égal à 2000

ldapsearch -x -H ldap://localhost
-b dc=claveau,dc=net "(&(gidNumber=2000)(objectClass=posixAccount))" ↵
= La dernière recherche retourne les 2 utilisateurs, mais aussi le groupe lui-même car il possède lui aussi l'attribut « gidNumber ». Cette dernière requête ne retourne que les deux comptes utilisateurs

ldapsearch -x -D cn=admin,dc=pas,dc=net -w password -h 172.17.7.20 -b dc=claveau,dc=net -s sub telephoneNumber=01* ↵
= Recherche tous les utilisateurs dont le téléphone commence par « 01 »

```
# extended LDIF
#
# LDAPv3
# base <dc=pas,dc=net> with scope subtree
# filter: telephoneNumber=01*
# requesting: ALL
#
# toto, lyon, claveau.net
dn: cn=toto,ou=lyon,dc=pas,dc=net
objectClass: person
cn: toto
sn: toto
telephoneNumber: 0123456789
```

ldapsearch -x "(&(cn=marie)(telephoneNumber=9*))" ↵ = Recherche toutes les entrée qui ont l'attibue cn = « marie » et un n° de téléphone commençant par 9

3.3.6 Commande ldapmodify

Ldapmodify fonctionne avec les mêmes options que ldapadd

Exemple d'un fichier modif ldif :

```
dn: cn=toto,dc=pas,dc=net
changetype: modify
replace: telephoneNumber
telephoneNumber: 9876543210
```

ldapmodify -D dn_admin -W -h ip_serveur -f modif_ldif ↵ = Modifie le téléphone pour « toto »

3.3.7 Commande ldappasswd

ldapsearch -x -D cn=admin,dc=pas,dc=net -w password -h 172.17.7.20 -s sub -b dc=pas,dc=net cn=tata ↵
= Affiche les informations sur « tata ». Le mot de passe attribué est maintenant crypté

```
# LDAPv3
# base <dc=pas,dc=net> with scope subtree
# filter: cn=tata
# requesting: ALL
dn: cn=tata,ou=paris,dc=pas,dc=net
objectClass: person
cn: tata
sn: tata
telephoneNumber: 9876543210
userPassword:: e1NTSEF9RVpNNVV6RFN1M2xKbUgwZVhDTmpVWGhacEtSOTNxSFU=
```

3.3.8 Autres Commandes

ldapdelete -D cn=admin,dc=pas,dc=net -w password -h 127.0.0.1 **-x cn=toto,dc=pas,dc=net** ↵
= Supprime le cn « toto »

slapcat ↵ = Affiche le contenu de l'annuaire

slapcat > sauvegarde.ldif ↵ = Effectue un "dump" de la base LDAP au format LDIF. Il est conseillé de l'utiliser régulièrement pour effectuer des sauvegardes de l'annuaire

slapadd < sauvegarde.ldif ↵ = Permet de peupler notre annuaire en utilisant un fichier LDIF = restaure une sauvegarde effectuée avec slapcat

slappasswd -s "secret" -h {md5} = Le mot de passe du rootdn peut être soit en clair, soit un hash
{md5}hKCmXZ7Pqmm4Y
Idem en SSHA « {ssha} », ce qui est préconisé
La valeur affichée est alors à copier-coller dans la valeur de la directive "rootpw" du fichier slapd.conf :
rootpw "{md5}hKCmXZ7Pqmm4Y", ou en SSHA rootpw "{SSHA}bvM1BfEOiEx2oqahiLEwAIF14g43YCbK '', ou en CRYPT rootpw "{CRYPT}W5MsxKtFzy6g. ''

3.3.9 Outils en graphique

GQ LDAP Client: http://sourceforge.net/projects/gqclient/
Jxplorer : http://jxplorer.org/
Gosa2 : https://oss.gonicus.de/labs/gosa/
luma : http://luma.sourceforge.net/
lat : LDAP Administration Tol : http://ldap-at.sourceforge.net/

3.4 Authentification par LDAP

On ne peut s'authentifier avec LDAP que si NSS est configuré pour récupérer les informations des utilisateurs

3.4.1 Configuration de nsswitch.conf

/etc/ldap.conf : Fichier utilisé par nsswitch pour gérer les informations LDAP

```
host 127.0.0.1
base dc=claveau,dc=net  = L'attribut BASE indique le DN de la base ldap
ldap_version 3
rootbinddn cn=admin,dc=claveau,dc=net
```

/etc/nsswitch.conf : Référencer LDAP comme source de noms prioritaire

```
passwd : ldap files
group: ldap files
shadow: ldap files
```

getent passwd titi ↵ = Vérification d'un compte avec la commande # getent. Validation du bon fonctionnement pour /etc/ldap.conf et /etc/nsswitch.conf

```
titi:*:1101:1101:titi:/home/titi/bin/bash
```

3.4.2 Configuration de PAM


system-auth


common-action

= Fichiers permettant de configurer les application devant utiliser l'authentification LDAP

Il faut modifier les actions « accunt » et « auth » pour s'authentifier à travers PAM.
On ajoute ces actions à l'authentification traditionnel, mais par le module pam_ldap.so

System-auth : Extrait d'une distribution RedHat

```
auth        sufficient    pam_unix.so  nullok
auth        sufficient    pam_ldap.so  use_first_pass  = Permet d'utiliser le mot de passe entré la 1ère fois pour ne pas l'entrer une seconde fois
account     sufficient    pam_unix.so
account     sufficient    pam_ldap.so
```

4 Serveur de mails

Mots clés certification LPI 202 : postfix, sendmail, /etc/aliases, /etc/mail/, /etc/postfix/*, /var/spool/mail, /var/log/, sendmail emulation layer commands*

4.1 MTA, MDA et protocole SMTP

4.1.1 MTA et MDA

Un MTA (Mail Transfert Agent) est un serveur qui assure l'envoie et la réception des messages. Ils communiquent par le protocole SMTP.

La lecture du message peut se faire sur le serveur directement, ou bien en utilisant un MDA (Mail Delivery Agent) par le protocole POP ou SMTP

4.1.2 Protocole SMTP

Le protocole SMTP (Simple Mail Transfert Protocol) sert à envoyer des courriers électronique au serveur de messagerie. L'enregistrement « MX » d'un serveur DNS permet de trouver l'adresse IP de ce serveur de messagerie.

telnet 192.168.199.10 25 ↵ = Connexion au serveur de messagerie sur le port 25
Trying 192.168.199.10...
Connected to 192.168.199.10.
Escape character is '^]'.
220 alpha.localdomain ESMTP Postfix
ehlo toto.com ↵
= Lance la conversation en s'authentifiant par son nom d'hôte. La commande « ehlo » permet d'afficher les extensions SMTP du serveur. Contrairement à la commande plus ancienne « helo »
250-alpha.localdomain = Seule cette ligne est affichée avec la commande # helo
250-PIPELINING
250-SIZE 1000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM: <toto@toto.com> ↵ = Début du mail, en spécifiant l'adresse source
250 2.1.0 Ok
RCPT TO: <toto> ↵ = Identifie le destinataire du mail. A répéter si plusieurs destinataires
250 2.1.5 Ok
DATA ↵ = Indique qu'un flux de données va être envoyé (le corps du message)
354 **End data with** <CR><LF>**.**<CR><LF>
Bonjour ↵
Comment ca va ? ↵
. ↵ = Le « . » termine le flux de données
250 2.0.0 Ok: queued as E264474E02
QUIT ↵ = Termine la connexion SMTP.
221 2.0.0 Bye
Connection closed by foreign host.
MAIL FROM: ↵ = Recommence un nouveau mail

4.1.3 Différents MTA

Sendmail est le plus ancien MTA. Il fonctionnat avant le protocole SMTP (par FTP entre serveurs) et la lecture des mails se fait directement sur le serveur. Sa configuration n'est pas très aisée. Mal sécurisé dans un premier temps, il a favoriser l'explosion des spams. Il est maintenant fiable, très puissant et sans doute le plus rapide

Exim est récent, distribué par défaut sur Debian. Il se veut robuste et fiable : http://www.exim.org/

PostFix est très populaire car assez simple à configurer : http://www.postfix.org/

4.2 Utiliser un serveur de mail

4.2.1 Open mail relay

Un Open mail relay est un serveur de messagerie qui accepte les connexions SMTP à partir de n'importe où. Cela signifie que tout le monde peut se connecter au port 25 sur ce serveur mail et envoyer des messages à n'importe qui. Si vous êtes malchanceux, les administrateurs système peuvent ajouter l'aresse IP de votre serveur à leur liste DENY / REJECT (ou équivalent)

/etc/mail/access : Utilisé pour autoriser ou refuser l'accès des users
192.168.1 RELAY = Autorise le relais des mails depuis le réseau désigné à travers le serveur de mail

telnet mail.home.nl 25 ↵ = A partir d'une machine qui ne devrait pas être en mesure d'utiliser votre serveur de messagerie comme relais, tentez de vous connecter au port 25 de votre serveur de messagerie et essayez d'envoyer un e-mail

```
Trying 213.51.129.253...
Connected to mail.home.nl. Escape character is '^]'.
220 mail2.home.nl ESMTP server (InterMail vM.4.01.03.00 201-229-121) ready Fri,
HELO ↵
250 mail2.home.nl
MAIL FROM: david@claveau.net ↵
.....
Hahaha, open mail relay test
.
250 Message received: 20020111162325.GOJI8897.mail2.home.nl@snow.castel.nl
QUIT
221 mail2.home.nl ESMTP server closing connection
Connection closed by foreign host.
```

4.2.2 Sendmail

4.2.2.1 Installation

yum install sendmail ↵ = Installe le MTA
yum install sendmail-cf ↵ = Installe le fichier de configuration pour reconfigurer sendmail

4.2.2.2 Fichier de configuration sendmail.cf

/etc/mail/sendmail.cf : Fichier de configuration

1. Recompiler
   # make -C /etc/mail ↵
   make: entrant dans le répertoire « /etc/mail »
   make: quittant le répertoire « /etc/mail »

2. Générer la table genericstable :
   # makemap hash /etc/mail/genericstable < /etc/mail/genericstable ↵

3. Vérifier le ficher des aliases
   # cd /etc ↵
   # newaliases ↵
   /etc/aliases: 76 aliases, longest 10 bytes, 765 bytes total

4. Redémarrez le service sendmail
   # service sendmail restart ↵

5. Faire un test
   # mail -s ''Test de mail pour le nouveau serveur'' publication@claveau.net < /etc/motd ↵

Surveillez les éventuelles erreurs dans le fichier /var/log/maillog

4.2.2.3 Fichier d'accès /etc/mail/access

/etc/mail/access : Utilisé pour autoriser ou refuser l'accès des users
192.168.1 RELAY = Autorise le relais des mails depuis le réseau désigné à travers le serveur de mail
badspammer.com 550 = Renvoie une erreur 550 pour le domaine « badspammer.com »
tux.badspammer.com OK = Le domaine « tux... » est autorisé à utiliser le serveur de mail

Actions définis dans le fichier /etc/mail/access :

- OK = Accepter le courrier, même si d'autres règles dans le jeu de règles en cours d'exécution ne serait-il rejeter, par exemple, si le nom de domaine est insoluble. «Accepter» ne signifie pas «relais», mais tout au plus d'acceptation pour les bénéficiaires locaux. Autrement dit, OK permet moins de RELAIS.
- RELAY = Accepter le courrier adressé au domaine indiqué ou reçus à partir du domaine indiqué pour relayer via votre serveur SMTP. RELAIS sert aussi OK implicite pour les autres contrôles.
- REJECT = Rejeter l'expéditeur ou le destinataire d'un message
- DISCARD = Pour supprimer le message complètement. Cela ne devrait être utilisée que si vraiment nécessaire.
- SKIP = Annule la recherche actuelle de cette entrée sans accepter ni la rejeter, mais provoquant l'action par défaut.

4.2.3 PostFix

Écoute sur le port 25 de l'interface localhost et de l'adresse IP du serveur mail

4.2.3.1 Les fichiers de configuration

Les deux fichiers de configuration sont main.cf et master.cf. Ces fichiers doivent appartenir à root.

/etc/postfix/master.cf : Il définit les démons à lancer, leur nombre et les " transports "

```
# ==========================================
# service type  private unpriv  chroot  wakeup  maxproc command args
#               (yes)   (yes)   (yes)   (never) (50)
# ==========================================
smtp      inet  n       -       y       -       -       smtpd
smtps     inet  n       -       y       -       -       smtpd \
          -o smtpd_tls_wrappermode=yes -o smtpd_sasl_auth_enable=yes
submission inet n       -       y       -       -       smtpd \
          -o smtpd_enforce_tls=yes -o smtpd_sasl_auth_enable=yes
pickup    fifo  n       n       y       60      1       pickup
```

dpkg-reconfigure postfix ↵ = A utiliser si postfix n'a pas été préalablement configuré. Vous n'avez alors pas de fichier de configuration main.cf

/etc/postfix/main.cf : Contient tous les paramètres de postfix. Ceux-ci peuvent être affichés avec la commande # postconf ↵

```
command_directory = /usr/sbin
daemon_directory = /usr/lib/postfix
program_directory = /usr/lib/postfix

smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
setgid_group = postdrop
biff = no
2bounce_notice_recipient = postmaster

# appending .domain is the MUA's job.
append_dot_mydomain = no
myhostname = NomHote.foo.org
mydomain = foo.org
mydestination = $myhostname, localhost.$mydomain $mydomain
myhostname = NomHote.foo.org
myorigin = $mydomain
myorigin = /etc/mailname

alias_maps = hash:/etc/aliases
```

```
alias_database = hash:/etc/aliases
# /etc/mailname contient l'équivalent de $MYHOSTNAME

mynetworks = 127.0.0.0/8 192.168.0.0/24
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
relay_domains = $mydestination
relayhost = $mydomain
smtpd_recipient_restrictions = permit_mynetworks,check_relay_domains
```

postfix reload ↵ = A chaque changement des fichiers main.cf ou master.cf, relancez le service

4.2.3.2 Les alias et le ficher ~/.forward

Le fichier /etc/aliases fait la correspondance entre les boites mail et les comptes du système, et permet donc de transférer des mail d'un alias vers une autre boite mail

/etc/aliases :

```
user1:      user2   = Permet de transférer les mails de user1 → user2 ...
user3:      user2   = ... et de user3 → user2
postmaster: root
usenet:     news
ftpadmin:   ftp
www:        webmaster
```

newaliases ↵ = Met à jour les alias en mettant à jour le fichier /etc/aliases.db (fichier compilé pour sa rapidité contrairement à un fichier ASCII

postalias /etc/aliases ↵ = Lien symbolique pour Postfix. # newaliases assure la compabilité pour Sendmail

Pour envoyer les mails destinés à un user vers un autre sur un système différent, il faut utiliser le fichier ~/.forward

Ce fichier texte contient les adresses vers lesquelles envoyer tous les mails.

Cela peut être le nom de user du système ou même d'adresse mail complète

Le fichier forward se trouvant sous le home directory du user, il peut le maintenir lui-même, alors que le fichier /etc/aliases n'est accessible que par root

Fichier alice@chicoago/.forward :

alice@miami, \alice, liste_alice = Les mails envoyés à alice sur la machine chicago seront envoyés à alice sur la machine miami, sur son compte locale et à la liste de diffusion

4.2.3.3 Configuration

/etc/postfix/main.cf : Fichier de configuration

myorigin = claveau.net = Domaine de l'expéditeur. Ce que le serveur met après l' « @ »

mydestination = claveau.net = Le serveur de mail traite les messages qui viennent de ce domaine

mynetwork = 10.0.20.40/24 = Le serveur relaiera les mails provenant de ce réseau

myhostname = mail.david.xxx = Nom de machine Internet de ce système de messagerie.
Par défaut = résultat de gethostname(). « $myhostname » est utilisé comme valeur par défaut pour beaucoup d'autres paramètres de configuration

relayhost = serveur_MTA_ext = Si utilisé, les mails seront envoyés uniquement par ce serveur.
Non obligatoire mais sécurise l'envoie des mails via un MTA précis

mydomain = david.xxx = Nom de domaine Internet de ce système de messagerie.
Par défaut = $myhostname oté de son premier composant

inet_interfaces = $myhostname,localhost = Adresses réseau par lesquelles le système de messagerie doit recevoir les messages. Par défaut, le logiciel accepte toutes les interfaces de la machine (= « all »)

home_mailbox = Mailbox = Chemin optionnel d'un fichier de boîte-aux-lettres relatif au répertoire personnel d'un utilisateur local(8).

Les messages sont stockés sous /var/mail/*user/* en attendant la transmission ou la récupération de mails par un client.

4.2.3.4 Commande postfix

postfix abort ↵ = Stoppe de façon brutale le système de mail Postfix. Les processus actifs doivent s'arrêter immédiatement.
postfix flush ↵ = Force la délivrance : essaye d'envoyer tous les messages de la file d'attente. Normalement, tente de livrer les messages retardés à des intervalles réguliers, l'intervalle double après chaque tentative qui a échoué.
postfix start ↵ = Vérifie et démarre le service
postfix stop ↵ = Arrête le service proprement
postfix check ↵ = Vérifie la validité de l'environnement et le fonctionnement du service. Avertit sur l'appartenance à un mauvais propriétaire ou sur de mauvaises permissions, et crée les répertoires manquants.
postfix reload ↵ = Recharge les services
postuser -d david ↵ = Supprime la queue de david.
« -d ALL » pour supprimer les queues de tous les utilisateurs

Commandes de vérification:
postfix check ↵ = décrit plus haut
postconf ↵ = Liste toutes les options possibles
postconf -n ↵ = Liste de tous les paramètres modifiés par rapport à la version par défaut
mailq ↵ = Affiche le contenu de la queue des mails
La commande # mail ↵ est fournie par le paquet  mailx ou  mailutils

4.2.3.5 Domaines virtuels

Les domaines virtuels permettent de gérer plusieurs de messagerie (pour un hébergeur, société à plusieurs entités, etc.)
La directive « mydomain » devient alors le domaine principal, appelé « canonique »

virtual_alias_domain=domaineA,domaineB = déclaration de 2 domaines virtuels gérés par le serveur
virtual_alias_maps = hash:/etc/postfix/virtual = Le fichier /etc/postfix/virtual (par défaut) définit la correspondance entre le nom des boites et l'un des domaine virtuel

/etc/postfix/virtual:
toto@domaine.com toto
titi@domaineA.com chti
tutu@domaineB.com tutu

postmap /etc/postfix/virtual ↵ = Crée le fichier alias utilisable par Postfix

ls -l /etc/postfix/virtual* ↵
virtual
virtual.db

file /etc/postfix/virtual.db ↵
virtual.db: **Berkeley DB** (Hash, version 9, native byte-order)

4.2.3.6 Gestion des quotas

Fichier main.cf :
mailbox_size_limit = 2000 = Taille max. de la boite aux lettres = 2000 octets
message_size_limit = 500 = Taille max. d'un message = 500 octets

4.2.4 Realtime Blackhole List = RBL

La liste noire de Paul Vixie est apparue en 1997. Elle offrait une arborescence DNS construite à partir des adresses IP de domaines *spammeurs* (ou ayant relayé un *spam*). Ainsi, lorsqu'une connexion venait de la machine d'adresse a.b.c.d, il suffisait de regarder si le *resource record* a.c.b.a.rbl.maps.vix.com existait dans le DNS.
Ainsi, la communauté avait à sa disposition une *liste noire*, maintenue de manière centralisée et diffusée facilement et rapidement.
En 2000, les règles d'utilisation ont changé : outre la migration du domaine vers mail-abuse.com, il faut dorénavant une licence (gratuite dans certains cas, payante dans les autres) rebute nombre de

personnes. On a alors vu se développer d'autres listes noires de ce type, avec des règles d'utilisation libres, telles que relays.ordb.org ou inputs.orbz.org.

Les DNSBL font l'objet de controverse depuis la création du premier système en 1997. Les gestionnaires de serveur de messagerie qui y ont recours les considèrent comme des outils anti-spam efficaces, tandis que d'autres y voient une forme de censure arbitraire. Les critères d'inclusion et d'exclusion relevant du seul gestionnaire du DNSBL. Certains DNSRBL ont fait l'objet de poursuites judiciaires intentées par des spammeurs.

4.2.5 Majordomo

Majordomo est un logiciel serveur propriétaire de listes de diffusion, créé en 1992. Avant cette date, les listes de diffusion étaient gérées manuellement.

/etc/majordomo.cf = Fichier de configuration
/usr/local/majordomo/lists/ma_liste_diffusion = Emplacement du fichier des listes de diffusions

help : Majordomo répond avec la liste des commandes disponibles.
subscribe nom_liste : Inscription de l'expéditeur à la liste
subscribe nom_liste addresses : Inscription des adresses à la liste
unsubscribe nom_liste : Désinscription de l'expéditeur à la liste
unsubscribe nom_liste adresses : Désinscription des adresses à la liste
which : L'expéditeur reçoit les listes auxquelles il est inscrit
which address : L'expéditeur reçoit les listes auxquelles l'adresses transmise est inscrite
lists : Transmet le catalogue des listes de diffusion
info nom_liste : Affiche des informations de base sur la liste
who nom_liste: Transmets la liste des adresses inscrites à la liste de diffusion
end : Majordomo ignorera tout ce qui vient après « end ». Pratique pour insérer une signature par exemple

4.2.6 MAP avec la directive sender_canonical

man canonical ↵ = Documentation de la directive
La directive permet de ré-écrire certaines adresses d'expéditeur

Fichier sender_canonical :
/etc/postfix/files/sender_canonical
root publication@claveau.net = l'adresse d'émission des mails expédiés par "root" sera remplacée par "publication@claveau.net"

postmap /etc/postfix/files/sender_canonical ↵ = Prend en compte la mapage. Un fichier /etc/postfix/files/sender_canonical.db est généré

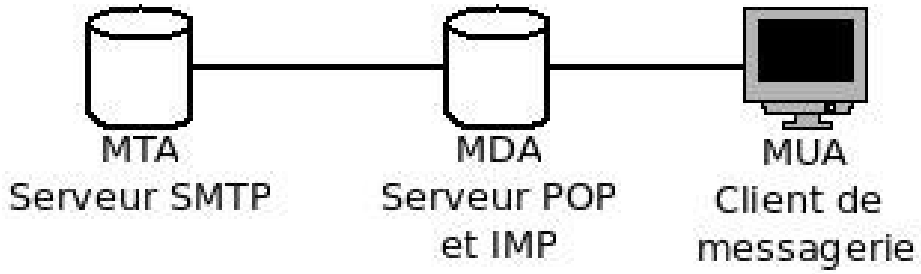
/etc/postfix/main.cf : Ajouter au fichier
sender_canonical_maps = hash:/etc/postfix/files/sender_canonical = Sans « .db »

postfix reload ↵
postfix flush ↵ = Supprime la queue des mails
postsuper -d ALL ↵ = Supprime (= « -d ») tous les mails (= « ALL ») dans la queue des mails et purge les fichiers temporaires

4.3 Gérer un client mail local

Mots clés certification LPI 202 : ~/.procmail, /etc/procmailrc, procmail, mbox and Maildir formats

Si le MTA gère l'envoie des messages de son domaine, le MDA (Mail Delivery Agent) permet la récupération de ces messages par un MUA (Mail User Agent = logiciel de courrier de messagerie).



4.3.1 La commande mail

4.3.1.1 Envoie d'un mail

mail corinne ↵ = Envoie d'un mail à Corinne
Subject: Invitation à dîner ↵ = Objet du message
Salut, ↵ = Texte du message
Tu viens dîner ce soir ? ↵ = Autant de ligne que l'on souhaite (pas d'invite)
David ↵
. ↵ = Fin du texte du mail
Cc: ↵ = Pas de destinataire en copie

4.3.1.2 Lecture d'un mail

mail ↵
Mail version 8.1.2 01/15/2001. Type ? for help.
"/var/mail/tac": 4 messages 4 new
>N 1 david@claveau.net Sun Mar 7 02:12 15/398 salut
N 2 david@claveau.net Sun Mar 7 02:14 17/438 **Invitation**
N 3 david@claveau.net Sun Mar 7 09:10 14/402 Hello
& 2 ↵ = Lecture du 2ème message
Message 2:
From david@claveau.net Sun Mar 7 02:14:01 2010
X-Original-To: Corinne
To: david@claveau.net
Subject: Invitation
Date: Sun, 7 Mar 2010 02:14:01 +0100 (CET)
From: David@claveau.net (root)
Salut,
Tu viens diner ce soir ?
David
& q ↵ = Quitte la commande # mail, *et va dîner ce soir avec David !*

4.3.2 Format mbox et maildir

Les messages sont stockés dans le MTA avant sa livraison au client. Les formats de stockage sont mbox ou maildir

4.3.2.1 Format mbox

Format assez ancien qui concatène tous les mails dans 1 seul fichier. Chaque mail commence par « From ». Assez simple d'utilisation.
Par contre, l'accès concurrent est dangereux (écriture par 2 programmes sur le même fichier = corruption). Des mécanismes de verrouillage permettent de limiter ce problème
Les logiciels de courrier qui utilisent ce format sont : Thunderbird, Eudora, squirrelmail, etc.

4.3.2.2 Format maildir

Utilise 1 fichier par mail, dans une structure de répertoire. Il est donc possible de manipuler plusieurs messages en même temps.
Chaque répertoire au format maildir contient 3 sous-répertoire : tmp, new et cur
Un nouveau mail est stocké sous « tmp » puis déplacé dans « new ». Une fois lu, il est placé sous « cur ».
Les logiciels de courrier qui utilisent ce format sont : Kmail, Mutt, Gnus (Emacs), Novell Evolution, Balsa, Sylpheed, Thunderbird 12 (expérimental)

4.3.2.3 Format pour Postfix

home_mailbox = Maildir/ = Utilisation du format « maildir » plutôt que mbox (format par défaut)
La commande # mail reconnaît seulement le format mbox

4.3.3 Procmail

Le MTA peut effectuer un traitement sur les messages entrants avant stockage. Postfix peut-être configuré pour utiliser Procmail à cet usage.
Le traitement peut-être de classer certains messages entrants dans un répertoire spécifique, d'effectuer du filtrage (refuser des mots interdits par ex.), ou bien d'appeler un autre programme pour des traitements plus lourd

4.3.3.1 Configuration Postfix pour utiliser Procmail

mailbox_command = /usr/local/bin/procmail = Demande à Postfix d'utiliser Procmail

4.3.3.2 Configuration de Procmail

Fichier de configuration : /etc/procmailrc ou ~/.procmailrc

Format d'une règle :
:0 *drapeau(x)* : *fichier_verrou*
* *condition*
action

:0: fichier_verrou	**Ligne du début du test**
:0	Début du test
:	Utilise un fichier verrou
fichier_verrou	Nom du fichier verrou
*** ^Objet:.*test**	**Ligne de la condition**
*	Début de la condition
^Objet:	Si il y a « Objet » au début de la ligne ...
.*test	...suivi par un nombre de caractère (= « * ») qui inclus le mot « test »
IN.testing	**Ligne de l'action**
IN.testing	Place le message dans le répertoire « IN.testing »

Expressions régulières pour les actions :
Pour spécifier les conditions, on se sert d'expressions régulières

- ^ = Début de ligne
- $ = Fin de ligne
- . = Un caractère quelconque
- [xy] = N'importe quel caractère dans l'ensemble spécifié
- [^xy] = N'importe quel caractère hors de l'ensemble spécifié
- foo|bar = foo ou bar
- c* = Un nombre quelconque (même 0) de répétitions du caractère c

Exemples d'actions :
^From: : cette condition vise toutes les chaînes de caractère From: au début d'une ligne. On dirait une en-tête de courrier électronique, non ? :-)
^From:.*choupi.* : cette condition vise toutes les chaînes de caractère From: au début d'une ligne, suivies

d'un ou plusieurs caractères, puis de choupi, puis d'un ou plusieurs autres caractères. Cette fois, on a défini l'ensemble des mails provenant d'une adresse contenant l'expression choupi : de cette façon, on vise tous les mails provenant de Choupi, votre meilleur ami.

^(From|Cc|To).*choupi.* cette fois, on vise tous les mails qui viennent de Choupi, ceux où Choupi est en Cc:, et ceux adressés à Choupi.

~./procmailrc : Fichier de configuration

```
:0 H  = Début de la règle n°0
        Facultatif = « H » pour l'entête (par défaut) ou « B » pour le corps du message
* ^TO.*publication@claveau.net  = Expression régulière pour sélectionner les mails
        = Transfert les mails adressés à publication...
!david@claveau.net  = Action (= « ! ») = vers david...

:1  = Règle n°1
* < 1000  = Lorsque le message fait moins de 1000 octets ...
| /usr/bin/lp  = ... imprime le mail

:2  = Règle n°2
* ^From.*toto  = Sélectionne les messages dont l'entête (par défaut) commence par « From » et contient
        dans la même ligne le mot « toto »
tousmesamis/toto  = ... pour les pacer dans le répertoire indiqué

:3c:  = Règle n°3 = Copy de mail (= « c »). Utilisation d'un fichier verrou (= « : » après « 3c »)
| /usr/bin/vacation nobody  = Le programme « vacation » gère la copie de mail

:4fw
* < 256000  = Si le message est < à 256000 octets ...
| /usr/bin/foo  = ... alors le programme foo le gère
```

Autres exemples de règles :

```
:0fw  = Suit le courriel au travers du démon spamc qui est l'interface de SpamAssassin
| /usr/bin/spamc

:0:
* ^X-Spam-Level: \*\*\*  = Déplace le courriel reconnu comme spam ...
.Trash/  = ... dans la poubelle (anglais US : trash) '.Trash/'

:0:
* ^From.*henry  = tout ce qui vient d'Henry ...
henries                 = ....va dans $MAILDIR/henries
```

Flags des règles :

```
0:H  = Examine l'en-tête = Header
0:B  = Examine le coprs du message = Body
0:HB  = Examine l'en-tête et le corps du message

0:c  = Génère une copie conforme du message électronique pour un traitement ultérieur
0:D  = Rend la comparaison egrep sensible à la casse. Par défaut, le processus de comparaison n'est pas
        sensible à la casse.
0:A  = Exécute cette règle si les conditions de la recette précédente (sans indicateur A ou a) ont été
        atteints.
0:E  = Semblable à l'indicateur A sauf que les conditions dans cette recette sont comparées à un message
        seulement si la recette précédant immédiatement et sans indicateur E n'a pas obtenu la
        concordance.
        Cette action ressemble à une action else.
0:e  = Établit la comparaison de la recette au message seulement si l'action spécifiée dans la recette
        présente juste avant échoue
0:f  = Utilise le tube comme filtre
0:w  = Indique à Procmail d'attendre que le filtre ou le programme spécifiés aient terminé leurs opérations
        et rapporte si l'opération précédente a réussi ou échoué, avant de considérer le message comme
        étant filtré.
```

4.3.4 Autres commande pour l'envoie de message

4.3.4.1 Commandes write et wall

write david ↵ = Envoie un message au user « David »
Ceci est mon message [Ctrl+d] ↵ = Le message se termine par Ctrl+d

write < fichier_message ↵

wall Attention arrêt dans 1 minute ↵ = Diffusion en broadcast d'un message. wall = « write all »
Broadcast message from root (pts/0) (Sun Mar 18 20:55:49 2012):
Attention arrêt dans 1 minute

4.3.4.2 /etc/issue et /etc/issue.net

Informations tirées de l'article « Les fichiers /etc/issue et /etc/issue.net » du site http://www.linux-france.org/ de Mathieu DECORE
Source : http://www.linux-france.org/~mdecore/linux/doc/memo2/node46.html

Ces fichiers sont affichés respectivement lors d'une connexion en console (fichier issue) et à distance (fichier issue.net) par ssh par exemple. Ils contiennent le message affiché, ainsi que des mots-clefs.
Les messages sont affichés avant l'ouverture d'une session, contrairement au message enregistré dans /etc/motd qui s'affiche après l'ouverture d'une session réussie

4.3.4.3 /etc/motd

Message Of The Day. Affiché à chaque connexion, après l'ouverture d'une session réussie.
Contrairement aux messages enregistrés dans /etc/issue ou /etc/issue.net qui s'affichent avant l'ouverture d'une session

4.4 Gérer un serveur MDA en POP et IMAP

Mots clés certification LPI 202 : /etc/courier/, dovecot.conf*

4.4.1 Fonctionnement MTA, MDA et MUA

Le MTA récupère et stocke les messages. Le MUA fonctionne en POP ou IMAP pour récupérer les mails sur un logiciel de courrier. Postfix n'est q'un MTA et ne gère donc pas ces protocoles. Il faut lui joindre un MDA pour offrir ce service de retrait de messages

POP 3 :
Port 110 en TCP. Il récupère les mails du serveur à destination du logiciel de courrier. Les mails sont effacés du serveur mais peuvent y rester quelques temps.

IMAP 4 :
Port 110 en TCP. Les messages sont conservés sur le serveur. Il est possible de le configuré pour synchroniser les mails pour une consultation hors-ligne

4.4.2 Serveur courrier-IMAP et courrier-POP

Les serveurs courrier-pop et courrier-imap font partis d'une suite « Courier Mail Server » qui fournis les services de gestion des mails. Ils fonctionnenent avec le format « maildir » et ne peuvent pas utiliser « mbox »
La file d'attente des mails est sous : /var/spool/mqueue.

/etc/courier/pop3d ou /etc/courier/imapd : Fichier de configuration
MAILDIRPATH=/var/mail = Répertoire utilisé pour le stockage des messages au format maildir
address = 10.0.20.34 = Adresse IP de l'interface apte à recevoir les connexions des clients

La bibliothèque « courier » permet l'authentification du client qui vient récupérer ses mails. Elle est commune aux 2 services

authtest david mdp_david ↵ = Vérifie que le compte « david » (avec son mot de passe) est apte à répcupérer ses messages
Authentication succeeded.
Authenticated: david (system username: david)
Home Directory: /home/david
Maildir: (none)
Quota: (none)
Encrypted Password: 1YSIbmjnM$makfir51Gla3ZpfRq5dmu.
Cleartext Password: mdp_david
Options: (none)

4.4.3 Serveur Dovecot (POP)

Dovecot est un serveur IMAP pour les systèmes de type Linux/UNIX, conçu en prêtant une grande importance à la sécurité. Il contient également un petit serveur POP3. Il prend en charge le courrier en formats maildir ou mbox.

yum install dovecot ↵ = Installe le paquet Dovecot

/etc/dovecot/dovecot.conf : Fichier de configuration
disable_plaintext_auth = no = Le mot de passe transitera en clair. Le message est de toute façon non crypté sur le réseau

dovecot -a ↵ = Affiche toutes les options (= « -a »)
1.0.15: /etc/dovecot/dovecot.conf
base_dir: /var/run/dovecot
log_path:
info_log_path:
log_timestamp: %Y-%m-%d %H:%M:%S
syslog_facility: mail
protocols: imap imaps pop3 pop3s
listen: *
ssl_listen:
ssl_disable: no
ssl_ca_file:
ssl_cert_file: /etc/ssl/certs/dovecot.pem
ssl_key_file: /etc/ssl/private/dovecot.pem
ssl_key_password:
.....

4.4.3.1 Configuration

/etc/dovecot/dovecot.conf : Fichier de configuration
protocols = imap pop3 ~~imaps~~ = La liste est à mettre en relation avec le fichier /etc/services.
Le protocole imaps est à supprimer car il correspond à de l'imap en SSL (port 993)
mail_location = mbox:~/mail:INBOX = /var/spool/mail/%u = Dans la plupart des installations, vos mails vont sous /var/mail/username = (INBOX) Depuis que IMAP supporte plusieurs boîtes aux lettres, il est possible de les stocker sous /var/spoll/mail/username («%u » = username)
mechanisms = plain login cram-md5 = Définit le type d'authentification. « plain » = mot de passe non crypté, « login » = utilisé par SMTP (non crypté), « cram-md5 » = crypté
passdb passwd-file { = Définit la gestion des mots de passe
# Each domain has a separate passwd-file:
args = /etc/users.dovecot = Les mots de passe sont stockés dans le fichier
}

4.4.3.2 Création des mots de passe

echo ''pascal:{PLAIN}password'' > /etc/users.dovecot ↵ = Crée le fichier des mots de passe

dovecotpw ↵ = Crée un mot de passe à insérer dans le fichier des mots de passe
Enter new password: mot de passe ↵
Retype new password: mot de passe ↵
{HMAC-MD5}595e6e69809606773671749d005255f59c3c9fdfa030db6d80efc4305ec73bc4

5 Sécurité du système

5.1 Configurer un routeur

Document PREPA_LPIC2.pdf = p. 263

La fonction de routage et intégrée au noyau Linux mais elle n'est pas activée par défaut

5.1.1 Configuration

echo 1 > /proc/sys/net/ipv4/ip_forward ↵ = Activation de la fonction routage, mais seulement jusqu'au prochain démarrage
Idem # sysctl net.ipv4.ip_forward=1 ↵

echo 0 > /proc/sys/net/ipv4/ip_forward ↵ = Désactivation de la fonction routage

Fichier /etc/sysctl.conf :
net.ipv4.ip_forward = 1 = Activation de la fonction routage, même après le redémarrage du serveur

Consultation de la table de routage :
route -n ↵ = Affiche la table sans résolution DNS (= « -n » = numérique)

Table de routage IP du noyau

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
0.0.0.0	192.168.0.1	0.0.0.0	UG	0	0	0	eth0

Idem # netstat -nr ↵ = Affiche la table de routage (= « -r ») sans résolution de nom (= « -n »)

Champs affichés par route :

- Destination = L'hôte ou le réseau de destination
- Gateway = L'adresse de la passerelle ou bien « * » s'il n'y en a pas
- Genmask = « 255.255.255.255 » est utilisé pour un hôte et « 0.0.0.0 » pour la route par défaut
- Route status flag =
  - ! = route rejetée
  - D = Installé dynamiquement par le démon qui gère le routage ou bien redirigé
  - G = Gateway
  - H = La destination est un hôte.
  - M = Modifié par le démon qui gère le routage ou bien redirigé
  - R = Route rétablie pour le routage dynamique
  - U = La route est valide = « up »
- Metric = La distance en saut jusqu'à la destination
- Ref = Nombre de références à cette route. Non utilisé par le routage du noyau, seulement par d'autres commandes
- Use = Un compte des recherches sur cette route. Indique la route non trouvée dans le cache si l'option « -F » est utilisée, ou bien indique si la route est trouvée avec l'option « -C »
- Iface = Interface où sont envoyés les paquets de cette route

Ajout d'une route statique :
route add -net 10.0.0.0 netmask 255.0.0.0 gw 192.168.1.99 ↵ = Ajout la route statique pour le réseau 10.0.0.0 (= « -net »), devant passer par la passerelle 192.168.1.99 (= « gw »)

route -n ↵ = Affiche la nouvelle table de routage

Table de routage IP du noyau

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
10.0.0.0	**192.168.1.99**	**255.0.0.0**	**U**	**0**	**0**	**0**	**eth1**
0.0.0.0	192.168.0.1	0.0.0.0	UG	0	0	0	eth0

route add default gw routeur ↵ = Ajoute une passerelle par défaut
Idem # route add -net 0.0.0.0 gw routeur ↵
= « -net 0.0.0.0 » représente la route par défaut = « default »

Suppression d'une route statique :
route del -net 10.0.0.0 netmask 255.0.0.0 ↵ = Supprime la route déclarée précédemment

5.1.2 NetFilter et la commande IPTables

Document PREPA_LPIC2.pdf = p. 265

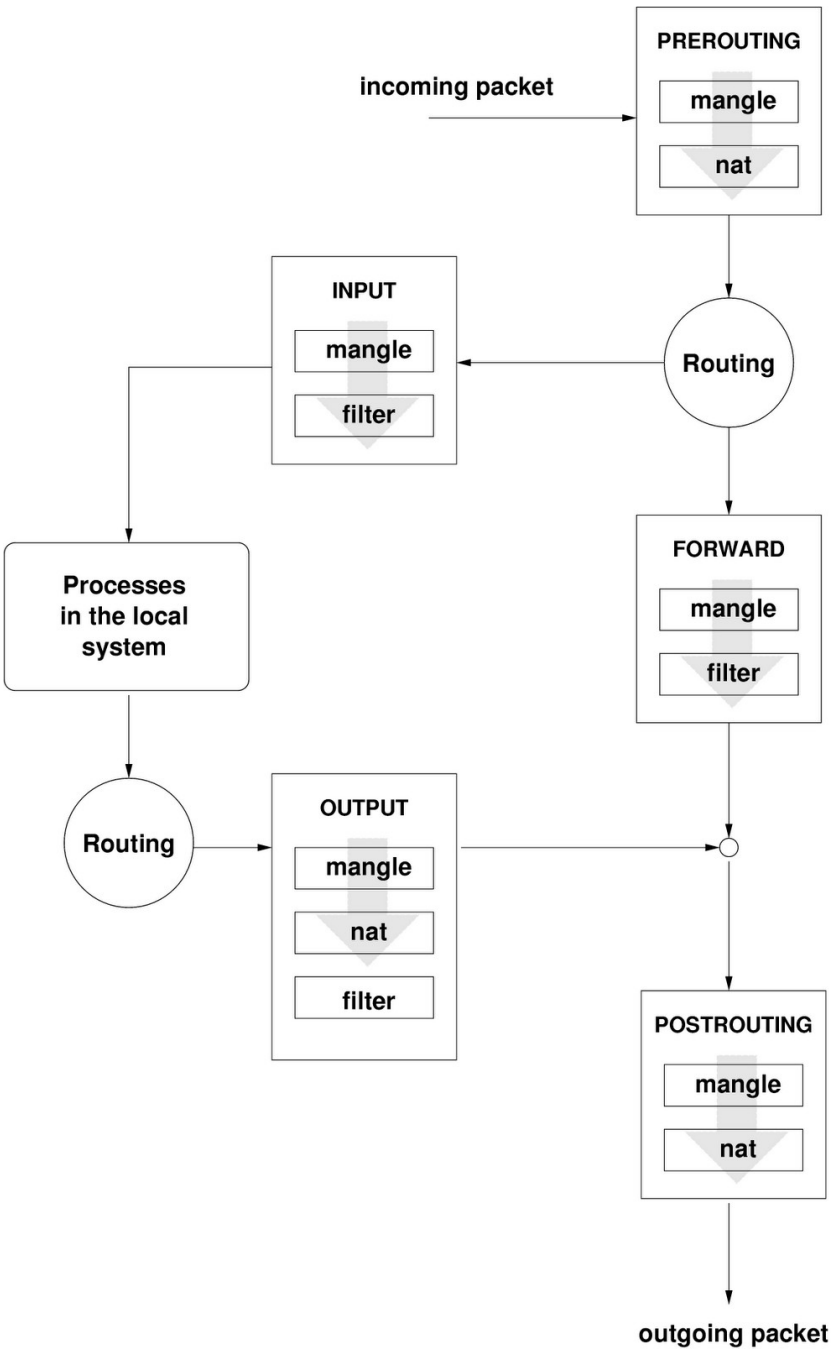
Utilisé pour mettre en place, maintenir et inspecter les tables des règles de filtrage des paquets IP du noyau Linux. Différentes tables peuvent être définies. Chaque table contient plusieurs chaînes prédéfinies et peut aussi contenir des chaînes définies par l'utilisateur.

5.1.2.1 Les tables

Table FILTER : C'est la table par défaut (sauf si on précise une autre table par l'option « -t »). Elle contient les chaînes prédéfinies INPUT, FORWARD et OUTPUT
Table NAT : Cette table est consultée lorsqu'on rencontre un paquet qui crée une nouvelle connexion. La table est composée de trois chaînes prédéfinies : PREROUTING (pour modifier les paquets dès qu'ils entrent), OUTPUT et POSTROUTING (pour modifier les paquets lorsqu'ils sont sur le point de sortir).
Table MANGLE : Cette table est employée pour effectuer une modification spéciale des paquets. Jusqu'au noyau 2.4.17, elle offrait deux chaînes prédéfinies : PREROUTING et OUTPUT. Depuis le noyau 2.4.18, trois autres chaînes prédéfinies sont aussi prises en charge : INPUT, FORWARD et POSTROUTING

5.1.2.2 Les chaînes

Chaîne INPUT : Trafic entrant, à destination de la machine = Table FILTER, MANGLE
Chaîne OUTPUT : Trafic sortant, venant de la machine = Table FILTER, MANGLE, NAT
Chaîne FORWARD : Trafic traversant la machine (d'une interface réseau à une autre) = Table FILTER, MANGLE, NAT
Chaîne POSTROUTING et PREROUTING = Configuration du NAT = Table MANGLE, NAT

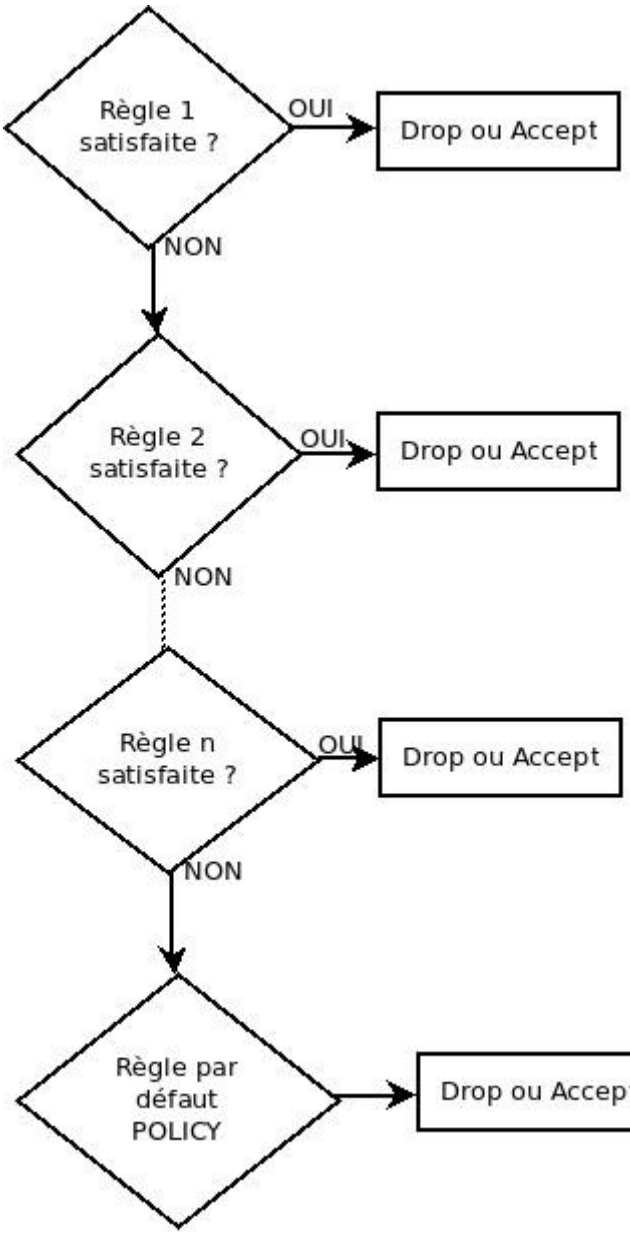


Site : Corail Numérique (http://corailnumerique.blogspot.fr) de Sylvain.B | No.Morgan (http://www.myspace.com/voileonirique)
Source : http://2.bp.blogspot.com/_moYrkba8wKU/TLXWKGP_jjI/AAAAAAAAAOE/1Hu-bN21tXw/s1600/fire_tables.png
Licence : http://www.google.com/intl/fr/policies/terms/

5.1.2.3 Les actions

Action ACCEPT : Laisse passer le paquet
Action DROP : Détruit le paquet
Action QUEUE : Le paquet est transmis à l'espace utilisateur (si cette option est reconnue par le noyau)
Action RETURN : On cesse de parcourir cette chaîne pour retourner dans la chaîne précédente (appelante) en passant à la règle suivante. Si le paquet avec la cible RETURN correspond à une certaine règle appelée depuis une autre chaîne, le paquet est renvoyé à la première chaîne pour que le contrôle de la règle reprenne au point où il s'était arrêté.
Dans le cas où la règle RETURN est utilisée dans une chaîne intégrée et que le paquet ne peut pas aller vers sa chaîne précédente, c'est la cible par défaut qui est utilisée.

5.1.2.4 Traitement dune règle



Si la règle n°1 est satisfaite, alors on l'exécute (l'action ACCEPT ou DROP est appliquée).
Sinon, on passe à la règle n°2

Si la règle n°2 est satisfaite, alors on l'exécute (l'action ACCEPT ou DROP est appliquée).
Sinon, on passe à la règle suivante.

Et ainsi de suite pour toutes les règles définies.
Si la dernière règle est satisfaite, alors on l'exécute, sinon on exécute la politique par défaut = POLICY

La règle par défaut POLICY est toujours exécutée si aucune règle précédente n'a été satisfaite

```
# iptables -L  ↵  =  Affiche les règles dans l'ordre pour chacune des chaînes
Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain FORWARD (policy ACCEPT)
target prot opt source destination

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

```
# iptables -S  ↵  =  Affiche les règles avec leur syntaxe
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
```

5.1.2.5 États d'une connexion

Les états possibles sont :

- NEW (nouveau paquet) signifiant que le paquet a initié une nouvelle connexion, ou bien qu'il est associé à une connexion qui n'a pas vu passer de paquets initial

- ESTABLISHED (état d'un paquet NEW au retour) signifiant que le paquet est associé à une connexion qui a déjà vu passer des paquets dans un sens,
- RELATED signifiant que le paquet initie une nouvelle connexion, mais qu'il est associé avec une connexion existante, comme un transfert de données FTP ou une erreur ICMP.
- INVALID signifiant que le paquet n'est associé à aucune connexion connue

5.1.3 Administration d'un pare-feu

5.1.3.1 Politique

« Tout ce qui n'est pas autorisé est interdit » ou bien « Tout ce qui n'est pas interdit est autorisé »

iptables -P OUTPUT DROP ↵ = Définit la règle par défaut « = -P », qui rejète (= « DROP ») tous les flux sortants (= « OUTPUT »)
ping -c 1 192.168.0.10 ↵ = Tente d'atteindre une machine distante
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
ping: sendmsg: **Operation not permitted** = Le flux sortant est interdit comme configuré
--- 192.168.0.10 ping statistics ---
1 packets transmitted, 0 received, **100% packet loss**, time 0ms

iptables -P INPUT DROP ↵
iptables -P FORWARD DROP ↵ = Pour un pare-feu, tout est interdit par défaut

5.1.3.2 Filtrage de paquet

Une fois les règles par défaut définit, il faut autoriser les flux 1 par 1 par les règles dans la table FILTER

iptables -A INPUT -p icmp -j ACCEPT ↵ = Autorise les ping entrants = Accepte (= « -j ») le retour (= « INPUT ») du protocole (= « -p ») icmp. La règle est ajoutée à la fin (= « -A »)

Ajouter le retour du DNS (= « -p UDP --sport 53 ») et l'interface loopback (= « -i lo »)

iptables -A INPUT -p tcp -j ACCEPT -s 0/0 -d 10.0.20.49 --sport 80 ↵ = Accepte pour le protocole TCP, sur le port 80 (= « sport » = « --source-ports » = HTTP), lorsque la source est « toutes @IP » et « tous les réseaux » (= « -s 0/0 »), vers la destination 10.0.20.49 (= « -d »)

iptables -A INPUT -p tcp --dport 22 -j ACCEPT ↵ = Permet le SSH vers la machine

Toujours autoriser le trafic entrant vers l'interface localhost, car certains programmes communiquent entre eux grâce à cette interface (gdm, xdm, etc.)

Autres options
« dports » = « --destination-ports » = Établit la correspondance si le port destination est l'un des ports spécifiés.
« -i » = Nom de l'interface qui reçoit les paquets (pour les chaînes INPUT, FORWARD et PREROUTING).
« -o » = Nom de l'interface qui envoie les paquets (pour les chaînes INPUT, FORWARD et PREROUTING).

Gestion des règles :
nmap -F 192.168.0.11 ↵ = Test les ports ouverts et bloqués rapidement (= « -F » = fastmode)

Nmap scan report for 192.168.0.11
Host is up (0.0010s latency).

PORT	STATE	SERVICE
80/tcp	open	http
111/tcp	open	rpcbind
2049/tcp	open	nfs

iptables -L FORWARD --line-numbers -n ↵ = Affiche la liste des règles (= « -L ») en numérique (= « -n »), en les numérotant (= « --line-numbers »)
Chain FORWARD (policy DROP) = Configure la chaîne FORWARD
num target prot opt source destination
1 ACCEPT tcp -- 192.168.1.0/24 0.0.0.0/0 tcp dpt:23

```
2 ACCEPT udp -- 192.168.1.0/24 0.0.0.0/0 udp dpt:53
3 ACCEPT tcp -- 192.168.1.0/24 0.0.0.0/0 tcp dpt:80
```

iptables -D FORWARD 1 ↵ = Supprime la règle n°1 de la chaîne FORWARD

iptables -I FORWARD 2 -s 192.168.1.0/24 -p tcp --dport 22 -j ACCEPT ↵ = Insère une règle (= « -I »), dans la chaîne FORWARD, en n°2

iptables-save > sauve_mon_FW ↵ = Sauvegarde toutes les règles dans le fichier de sauvegarde
iptables-restore < sauve_mon_FW ↵ = Restaure la sauvegarde du FW

iptables -F ↵ = Supprime (= « -F » = flush) toutes les règles
iptables -L ↵ = Liste les règles après la suppression

```
Chain INPUT (policy ACCEPT)
target                  prot    opt     source          destination
RH-Firewall-1-INPUT     all     –       anywhere        anywhere

Chain FORWARD (policy ACCEPT)
target                  prot    opt     source          destination
RH-Firewall-1-INPUT     all     --      anywhere        anywhere

Chain OUTPUT (policy ACCEPT)
target                  prot    opt     source          destination
```

L'outil Fail2Ban (http://www.fail2ban.org/wiki/index.php/Main_Page) permet de créer des règles de pare-feu dynamiquement, interdisant les clients qui n'ont pas réussi à s'authentifier au bout de plusieurs fois

Règles des flux retours :

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT ↵ = Autorise de façon implicite les flux retours, puisque tous les états sont acceptés, sauf NEW et INVALID. Utilise le module « state » (= « m state »), qui permet de filtrer en fonction de l'état des flux (= « --state »)

Exemple complet de configuration :

iptables -P INPUT DROP ↵ = Interdit tous les flux entrants
iptables -P OUTPUT DROP ↵ = Interdit tous les flux sortants
iptables -P FORWARD DROP ↵ = Interdit tous les flux traverssants
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT ↵
= Autorise de façon implicite les flux retours
iptables -A FORWARD -s 192.168.1.0/24 -p tcp --dport 80 -j ACCEPT ↵
= Autorise les flux traversants pour les flux HTTP (port 80) depuis le LAN 192.168.1.0/24 en tcp
iptables -A FORWARD -s 192.168.1.0/24 -p tcp --dport 443 -j ACCEPT ↵
= Autorise les flux traversants pour les flux HTTPs (port 443)
iptables -A FORWARD -s 192.168.1.0/24 -p udp --dport 53 -j ACCEPT ↵
= Autorise les flux traversants pour les flux DNS (port 53)

5.1.3.3 Gestion du NAT

Le NAT est géré dans la table « NAT »

iptables -t nat -L ↵ = Liste toutes les règles (= « -L »), de la table NAT (= « -t »)


iptables -t nat -S ↵ = Liste les règles par défaut de la table NAT avec la syntaxe

iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE ↵
= Ajoute la règle à la chaîne POSTROUTING, dans la table NAT, pour les flux sortant par l'interface réseau eth1 (= « -o »). Les adresses IP sortantes sont translatées dans une adresse IP dynamique (= « -j MASQUERADE ») ou une IP fixe avec « SNAT »

iptables -A POSTROUTINE -t nat -s 10.0.16.0/20 -d 0/0 -j MASQUERADE ↵
= Remplace l'@IP source (= « -s ») par celle du routeur (= « -d 0/0 »)

5.1.3.4 Scripts de configuration des règles de filtrage

La gestion du pare-feu de manière dynamique est trop compliqué. Il est préférable de créer un script regroupant les règles

```
#!/bin/bash
# nom du fichier : /etc/parefeu_on
# Politique de base
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
# NAT avec eth0 en interne et eth1 en sortie - adresse IP publique fixe
iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to-source 81.2.3.4
# gestion des paquets retours
iptables -A FORWARD -i eth1 -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
# trafic autorisé en sortie
iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -p udp --dport 53 -j ACCEPT
```

Exemple de script d'annulation : Permet d'autoriser tous les flux temporairement

```
#!/bin/bash
# nom du fichier : parefeu_off
# Effacement des règles
iptables -F
# Politique permissive
iptables -P INPUT ACCEPT  = Accepte tous les flux entrants par défaut
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
```

Script de gestion du pare-feu :

```
#!/bin/bash
# nom du fichier : parefeu
case $1 in
start)
/etc/parefeu_on
;;
stop)
/etc/parefeu_off
;;
status)
iptables -L
;;
*)
echo "Syntaxe : /etc/init.d/parefeu start|stop|status
;;
esac
```

5.1.3.5 Outils

FireWall Builder : www.fwbuilder.org
Guarddog : http://www.simonzone.com/software/guarddog/
FireStarter : http://www.fs-security.com/

5.2 Sécuriser un serveur FTP

Mots clés certification LPI 202 : vsftpd.conf, Pure-FTPd command line

5.2.1 Protocole et clients FTP

Ports utilisés :

- Passif = 21
- Actif = 21 pour les commandes et 20 pour les données. Ce ce comportement n'est plus généralisé

Commandes FTP en ligne de commande :
ftp> open 192.168.0.29 ↵ = Ouvre une session FTP sur le serveur indiqué
Connected to 192.168.0.29.
220 (vsFTPd 2.0.5)
Name (192.168.0.29:agent):

ftp> ls ↵ = liste le contenu du répertoire distant (idem la commande système)
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.

ftp> close ↵ = Ferme la session en cours
221 Goodbye.

ftp> cd ↵ = Change le répertoire distant (idem la commande système)
ftp> get ↵ = Récupère un fichier distant depuis le serveur vers le répertoire local
ftp> put ↵ = Transfert un fichier local vers le serveur FTP distant

5.2.2 Chrooter un serveur FTP

Les conditions listées sont nécessaires au chrootage du serveur FTP:

- Créez un /dev et /etc/ dans l'environnement chroot
- Créez un fichier /etc/passwd dans l'environnement chroot
- Créez un user « ftp » dans l'environnement chroot

5.2.3 Pure-FTPd

Informations tirées du post de chatonhub (12/03/2011) sur le site Team-AAZ
Source : http://www.team-aaz.com/forum/les-tutoriels/pure-ftpd-t2314.html

Serveur FTP simple, stable et efficace. Il peut se lancer en ligne de commande sans fichier de configuration

pure-ftpd ↵ = Lance le serveur avec son fonctionnement par défaut = Les utilisateurs du système déclarés sur le serveur peuvent ouvrir une session distante FTP avec leur nom et leur mot de passe. Attention, non conseillé, car le mot de passe circule en clair !

Le mode de fonctionnement en accès anonyme est activé si un user « ftp » a été créé sur le serveur FTP. Les utilisateur distant travaillent alors dans le répertoire /home/ftp

pure-ftpd --anonymousonly ↵ = Autorise uniquement les utilisateurs anonymes, mais il faut que le compte « ftp » existe

Options :
--help = Affiche les options possibles
--displaydotfile = Permet d'afficher les fichiers cachés. Cachés par défaut
--anonymousonly = Autorise uniquement les utilisateurs anonymes
--noanonymous = Empêche toute connexion anonyme, même si le compte « ftp » existe
--maxidletime = Temps max. d'inactivité avant déconnexion
--anonymouscantupload = Empêche le téléchargement pour un user anonyme
--anonymouscantcreatedirs = Empêche la création de répertoire pour un user anonyme

5.2.4 VSFtpd : Very Secure FTPd

/etc/vsftpd/ftpusers = Users qui NE SONT PAS autorisés à se connecter en FTP. Inscrire 1 user / ligne

/etc/vsftpd/vsftpd.conf : Fichier de configuration
ftp_banner = Bienvenue sur ce serveur FTP = Affiche le message et ne montre pas la version
listen-port = 222 = change le port d'écoute
# chroot_local_user = Active ou non (si commenté) les users (de la liste définit par « chroot-list-file ») qui NE SONT PAS chrootés
chroot_list_enable = YES = chroot les users qui sont inscrit dans la liste « chroot_list_file »
chroot_list_file = /etc/vsftpd/chlist = Liste des users qui doivent être chrooté
anonymous_enable = YES = Autorise (ou non) l'accès anonyme
local_enable = YES = Autorise (ou non) les utilisateurs locaux (déclarés sur le système) à accéder à leur répertoire personnel
write_enable = YES = Autorise (ou non) le téléchargement vers le serveur (commande # put)
anon_upload_enable = YES = Idem « write_enable » mais pour les comptes anonyme
anon_mkdir_write_enable = YES = Autorise (ou non) la création de répertoire pour les compte anonyme

Le répertoire de travail d'un user chroot est son propre répertoire /home définit dans /etc/passwd :
agent:x:1000:1000:agent,,,:/home/agent:/bin/bash

ftp> prompt ↵ = Active ou désactive le prompt = Ne pose pas de question et répond toujours « yes »
Interactive mode off.
ftp> prompt
Interactive mode on.

5.2.5 ProFTPd

Informations tirées du site « Marcel du Deux Ter ». Licence GNU GPLv2 http://moinmo.in/GPL
Source : http://www.md2t.eu/serveur/proftpd.conf

Utilise la même syntaxe que Apache

/etc/proftpd.conf : Fichier de configuration

```
ServerName "nom du serveur FTP"
ServerIdent  on ''Bannière du site FTP''  = Affiche (ou non) la bannière
ServerType  Standalone  = Le serveur FTP écoute lui-même les ports ouverts. Si « inetd » alors cette écoute est prise en charge par xinted
DefaultServer  on  = Permet de déclarer des VirtualHosts
DeferWelcome  off  = Permet de ne pas donner d'informations sur le serveur.
DefaultRoot  ~  !adm  = Le répertoire par défaut est le « home directory » des users (= « ~ »), sauf pour les « admin » (= «!adm »)
MaxClientsPerHost  20  = Nombre de connexion max
Port 21
Umask 022  = Interdit la création de fichier et de répertoire
User userftp  = User sous lequel le processus tournera
Group groupeftp

<Anonymous  ~ftp>  = Section pour les users anonyme = « ftp »
        UserAlias  ftp  anonyme  = Les clients peuvent se connecter en tant que « ftp » ou « anonyme »
        MaxClients 10
        DefaultChdir  /pub  = Le répertoire ~/pub est celui par défaut pour un user « ftp »
        <Directory  upload  /*>  = Définit une partie téléchargement
                AllowOverwrite  yes  = Autorise la publication = Commande « put »
                <Limit  READ>
                        Deny  All  = Personne ne peut lire sous uploads
                </Limit>
                <Limit STOR>
                        Allow  All  = Le compte « ftp » (= tous), peut déposer des fichiers
                </Limit>
        </Directory>
</Anonymous>
```

proftpd ↵ = Permet d'avoir un message d'erreur si la configuration n'est pas correcte

5.3 Sécuriser un serveur SSH

Mots clés certification LPI 202 : ssh, sshd, /etc/ssh/sshd_config, Private and public key files, ~/.ssh/authorized_keys, PermitRootLogin, PubKeyAuthentication, AllowUsers, PasswordAuthentication, Protocol

5.3.1 Paramètres du fichier de configuration

/etc/ssh/sshd_config :
protocol 2 = La version 1 est cassable. Il ne faut plus l'utiliser
LoginGraceTime 30 = Le serveur se déconnecte après ce délai si l'utilisateur ne s'est pas connecté (entre la commande, la demande de login et le mot de passe). Si la valeur est 0, il n'y a aucune limite de temps. Par défaut 600 (secondes).
MaxAuthTries 3 = 3 essaies maximum. Un faible nombre permet de minimiser le risque de votre serveur SSH être attaqué en force brute.
PermitRootLogin yes = Autorise la connexion en SSH du compte « root »
AllowUsers claveau@10.0.29.49 = Seul cet utilisateur peut se connecter. Inhibe toutes les autres options. Le compte doit être créé sur le système
Si « @* » alors tous les réseaux sont autorisés
Port 2200 = Le port d'écoute est modifié

5.3.2 Authentification

5.3.2.1 Authentification du serveur contacté

L'empreinte du serveur contacté est enregistré dans le fichier know_host

/home/david/.ssh/know_host : Fichier des empreintes des serveurs déjà contactés, dans le home directory

|1|LPx02U8nHnkSb0czyqVrdXPcW04=|jS0/QdS0HydzPZj8QXxHXC4j6EM= ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAv+kXth0/RSAroNfqeV+IkEMetdWRWYBvbNOqUDDSL/fLylBip9le40xfTe1jFXuYqAWR+mQMo8Pg.....itiggcYNetxaNkPKfW8DdClq+

newton,128.138.249.8 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEA0d7Aoure0toNJ+YMYi61QP2ka8m5x5ZQlT7obP8CK3eropfqsMPPY6uiyIh9vpiFX2r1LHcbx139+vG6HOtVvuS8+IfMDtawm3WQvRuOopz3vVy5GtMwta

5.3.2.2 Échange de clé pour SSH

DSA = Digital Signature Algorithm
RSA = Rivest, Shamir, Adleman. 1er algorithm très utilisé mais sujet à des restrictions de copyright.

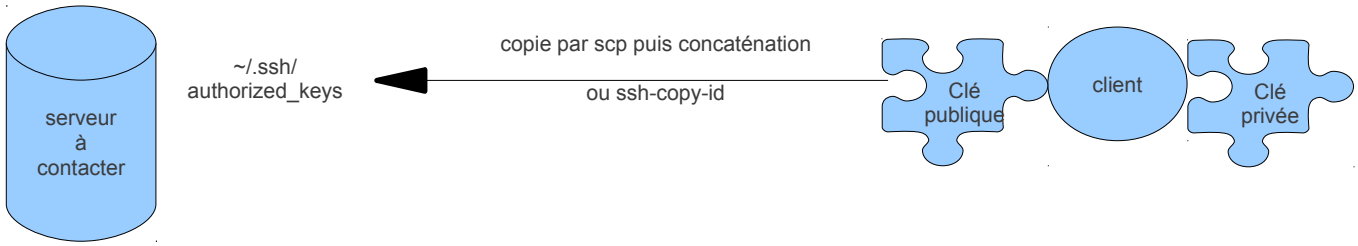
SSH utilise RSA par défaut (alors de GPG utilise DSA). 1024 ou 2048 sont des longueurs de clé utilisées en standard, mais 2048 est actuellement considéré comme la longueur minimale pour assurer la sécurité (attaque par force brute).

1lgorithme RSA :

- Fichier ~/.ssh/id_rsa = Contient la clé privée. Modifiable seulement par le propriétaire et personne d'autre. A ne jamais diffuser.
- Fichier ~/ssh/.id_rsa.pub = Contient la clé publique. A donner à tout ceux qui doivent décrypter un fichier ou un flux de données cryptés avec la clé privé.

Créer et utiliser les clés :
L'échange de clés permet au serveur de ne pas demander le mot de passe du client qui souhaite établir une connexion en SSH.

1. # ssh-keygen -t rsa ↵ = Crée un couple de clés privée-publique sur le client : ~/.ssh/id-rsa (clé privée) et ~/.ssh/id-rsa.pub (clé publique)
2. Il ne reste plus qu'à copier la clé publique (fichier id-rsa.pub) sur le serveur et de concaténer son contenu au fichier ~/.ssh/authorized_keys



ssh-copy-id user_serveur@serveur -i ~/.ssh/id_rsa.pub ↵ = Envoi la clé publique du client (= « -i rsa.pub ») sur le serveur et concatène le bon fichier en une seule opération, pour le user identifié sur le serveur

A chaque connexion, la clé publique du serveur (hôte distant) est enregistrée dans le fichier ~/.ssh/know_hosts
ssh-keygen -R nom_serveur ↵ = Permet de supprimer un serveur dans le fichier know_hosts sous Débian, car le nom de la machine est chiffré. Sous RedHat, le nom du serveur est en clair
fail2ban et denyhost sont 2 logiciels qui permettent de bannir les users qui tentent de se connecter à un serveur en commettant des erreurs

Commande ssh-keygen :
Permet de générer les clés privée et publique pour identifier les hôtes.

ssh-keygen -t dsa -b 2048 ↵ = Génère les clés privée et publique d'une longeur de 2048 bits (= « -b 2048 »), avec l'algorithme DSA (= « -t dsa »)
Generating public/private dsa key pair. Enter file in which to save the key (/home/janl/.ssh/id_dsa): ↵
Created directory '/home/janl/.ssh'.Enter passphrase (empty for no passphrase): passphrase ↵
Enter same passphrase again: passphrase ↵
Your identification has been saved in /home/janl/.ssh/id_dsa. = Génération de la clé privée
Your public key has been saved in /home/janl/.ssh/id_dsa.pub. = Génération de la clé publique
The key fingerprint is : c2:be:20:4a:17:2e:3f:b2:73:46:5c:00:ef:38:ca:03 janl@debian

ssh-keygen -p -t dsa ↵ = Change la passphrase (= « -p ») pour la clé DSA (= « -t dsa »)
Enter file in which the key is (/home/janl/.ssh/id_dsa): ↵ (touche Entrée)
Enter old passphrase: passphrase ↵
Key has comment '/home/janl/.ssh/id_dsa'
Enter new passphrase (empty for no passphrase): nouvelle_passphrase ↵
Enter same passphrase again: nouvelle_passphrase ↵
Your identification has been saved with the new passphrase

ssh_keygen -t rsa -f /etc/ssh/repertoire ↵ = Génère les clés privée et publique avec l'algorithme DSA, dans un autre répertoire (= « -f ») que ~/.ssh/

ssh_keygen -c ↵ = Permet de changer le commentaire des clefs mais seulement pour les clefs RSA1

ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key.pub ↵ = Affiche le contenu de la clé publique
1024 98:2g:h8:k9:de:9f:fg:90:34:v3:35:3j:26:24:26:7k ssh_host_rsa_key.pub

ssh-agent :
Permet d'utiliser plus facilement la passphrase. Le principe est d'utiliser ssh-agent pour qu'il garde vos clés. Lorsque vous ajoutez vos clés, vous ne donnez la passphrase qu'une seule fois.
Attention, car l'utilisateur root peut également demander les clés sans que vous le remarquiez .
ssh_agent configure 2 variables d'environnement :
SSH_AUTH_SOCKS : Nomme la socket qui doit communiquer avec l'agent
SSH_AGENT_PID : PID de l'agent. Permet de tuer le processus facilement

echo $SSH_AGENT_PID ↵ = Affiche le PID de l'agent configuré dans les variables d'environnement
11487
eval `ssh-agent` ↵ = Permet de sécuriser la procédure en comparant la valeur du PID de l'agent avec la valeur de la variable d'environnement SSH_PID_AGENT
Agent pid 11487

ssh-add ↵
Enter passphrase for /home/janl/.ssh/id_dsa: passphrase ↵
Identity added: /home/janl/.ssh/id_dsa (/home/janl/.ssh/id_dsa)

ssh-add -l ↵ = Permet de lister les clés et de vérifier si elles sont bien enregistrées
2048 f3:5c:f1:34:6c:1b:a6:4c:5b:c4:6d:30:48:01:76:f4 tata@stotion (RSA)
2048 f3:5c:f1:34:6c:1b:a6:4c:5b:c4:6d:30:48:01:76:f4 **/home/tata/.ssh/id_rsa (RSA)**

5.3.3 Confidentialité des communications

5.3.3.1 Connexion et copie

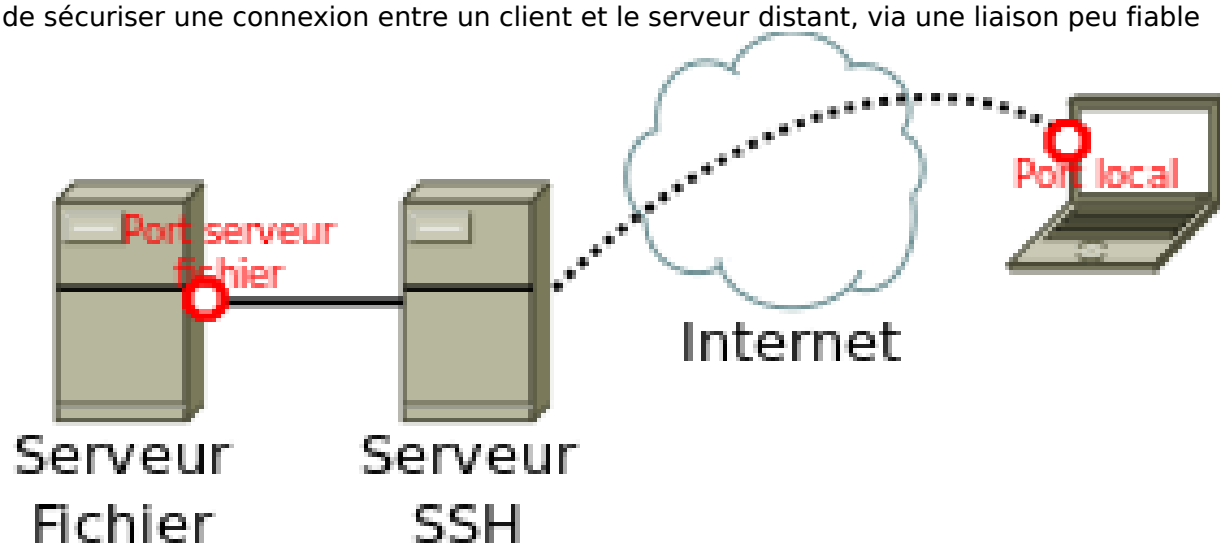
ssh david@serveur_fichier ↵ = Se connecte en tant que « david » au serveur de fichier

scp /home/david/fichier david@serveur_fichier:/data/david/ ↵ = Copie le fichier local sur le serveur distant

5.3.3.2 Tunnel SSH

Informations tirées du site « Linux France » http://www.linux-france.org
Source : http://www.linux-france.org/prj/edu/archinet/systeme/ch13s04.html

Permet de sécuriser une connexion entre un client et le serveur distant, via une liaison peu fiable



Sur le portable :
ssh -L port_local:@IP_serveur_fichier:port_serveur_fichier user_serveur_SSH@serveur_SSH ↵
= Établi un tunnel (= « -L ») entre le portable et le serveur de fichier via le serveur SSH. Le trafic destiné à un port local (sur le portable) est en fait transmis via le tunnel sur le serveur de fichier (et son port spécifié)

Autre exemple :
ssh -L 110:mailhost:110 -L 25:mailhost:25 -1 user -N mailhost ↵
= Le port 110 et le port 25 de la machine locale sont tunelés sur les ports 110 et 25 de la machine localhost, en utilisant le service SSH de la même machine
= Crée un tunnel SSH pour les protocoles POP et SMTP

user@MO # ssh -L 1234:localhost:80 M1 ↵ = Le port 1234 de M0 est tunnelé vers le port 80 de la machine M1 en utilisant le servuce SSH (port 22) de M1

Options :
-N = Ne pas exécuter de commande distante
-f = Exécute le programme en tâche de fond
-l = Passer en paramètre le login de connexion
-g = Autoriser des machines distantes à se connecter sur des ports locaux exportés

5.3.3.3 Renvoi de session X11

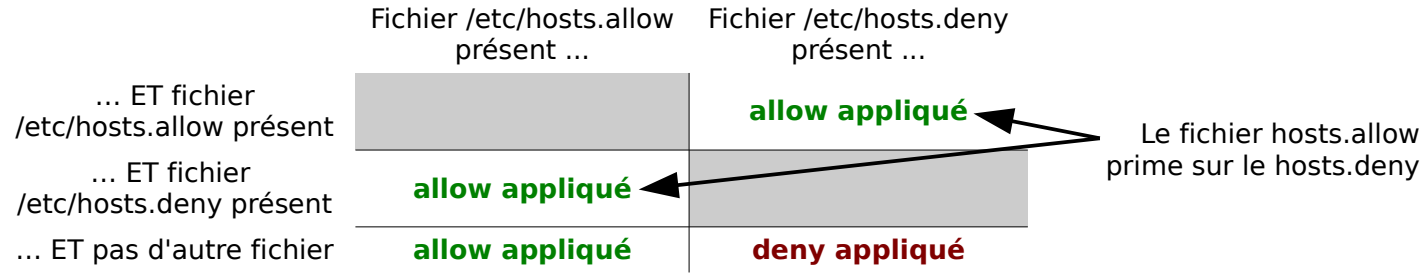
/etc/ssh/sshd_config : Fichier de configuration du serveur SSH
X11Forwarding yes = Autorise le renvoie de connexion X11

ssh -X david@serveur_distant ↵ = Se connecte au serveur distant, en tant que « david ». Les applications X s'ouvriront alors sur le poste local

5.4 TCP Wrapper

5.4.1 Fichier /etc/hosts.allow et /etc/hosts.deny

TCPwrapper s'appuie sur la librairie libwrap
Le démon tcpd lit les fichiers /etc/hosts.allow et /etc/hosts.deny
Ces fichiers sont lus en temps réel et chaque modification est prise en compte de suite.



tcpdchk ↵ = Vérifie le contenu des fichiers hosts.allow et hosts.deny

more /etc/hosts.deny ↵
ALL: ALL= Bloque tous les accès par défaut de tous les services

more /etc/hosts.allow ↵
sshd: ALL EXCEPT 192.168.1.10 = N'importe quel hôte distant peut se connecter en SSH sauf le 192.168.1.10
sshd : 192.168.1.0/255.255.255.0 : ALLOW = Le réseau mentionné est autorisé à utiliser SSH
ftp: 10.1 = Toutes les adressese qui commencent par 10.1 peuvent utiliser le ftp
vsftpd: 192.168.1.0/24 EXCEPT 192.168.1.10 = Toutes les machines sur le réseau 192.168.1.0/24 peuvent se connecter en FTP sauf pour la machine 192.168.1.10
sshd : 192.168.1.
sshd : 192.168.1.0/255/255.255.0 = Syntaxe différente autorisant seulement le réseau 192.168.1.0/24

5.4.2 Denyhosts

Programme en Python qui sécurise les accès SSH : http://denyhosts.sourceforge.net/
Fail2Ban fonctionne le même principe : http://www.fail2ban.org/wiki/index.php/Main_Page
Le programme travaille avec le fichier de logue de la sécurité :

 /var/log/secure

 /var/log/auth.log

Lit les adresses IP rejetées et les ajoute au fichier /etc/hosts.deny

/etc/denyhosts/denyhosts.cfg : Fichier de configuration
SECURE_LOG = /var/log/secure
HOST_DENY = /etc/hosts.deny
PURGE_DENY = « rien » = On ne purge jamais
BLOCK_SERVICE = sshd = Quel service scruter (plusieurs possibles) ou « all »
DENY_THRESHOLD_INVALID = 5 = Lors d'une problème de compte invalide, la connexion est considérée comme avoir échoué au bout de 5 fois
DENY_THRESHOLD_VALID = 10 = Lors d'un problème de mot de passe invalide (lorsque le compte est bien déclaré dans le système), le compteur est placé à 10 fois
DENY_ THRESHOLD_ROOT = 1 = Pour le compte root, le compteur est mis à 1

/var/lib/denyhosts/allowed-hosts :
10.0.20.45 = Cette adresse ne sera jamais bloquée, même si Denyhosts l'enregistre dans /etc/hosts.deny

5.4.3 Avec ProFTPd

/etc/proftpd.conf :

ServerType inetd = À la place de « standalone », inetd prend alors en charge les communications réseaux

/etc/services :
ftp-data 20/tcp
ftp 21/tcp

/etc/xinetd.d/xproftpd :
service ftp = Déclaration de la prise en charge du service FTP, en lien avec /etc/services (ftp = port 21 en tcp)
{
socket_type = stream = Flux TCP
wait no = Pas d'attente que la connexion se termine
user = root = Obligation de lancer le service avec un port < 1024
server = /usr/bin/ftp = Binaire à lancer ou alors lien symbolique vers celui-ci
log_on_success += DURATION USERID = Enregistre en cas de succès, des informations supplémentaires (= « += ») comme la durée de la connexion (= « DURATION ») et l'ID de l'utilisateur (= « USERID »)
log_on_failure += ATTEMPT RECORD = Enregistre en cas d'échec, des informations supplémentaires (= « += ») comme le fait qu'une tentative a été avortée (= « ATTEMPT ») où bien des informations sur le système distant dans le cas où le service ne peut pas être démarré.
disable = no = Actif. Si « yes » alors proftpd ne sera pas lancé a avec xinetd
}

service xinetd start ↵ = On ne lance que xinetd. C'est xinetd qui gère maintenant proftpd

netstat plantu | grep 21 ↵
tcp 0 0 0.0.0.0:**21** 0.0.0.0:* LISTEN2118/**xinetd** = C'est bien xinetd qui gère le FTP (sur le port 21)

5.4.4 Restriction horaire du serveur FTP

/etc/xinetd.d/xproftpd : On ajoute la directive « access_times »
service ftp = Déclaration de la prise en charge du service FTP, en lien avec /etc/services
{
.....
access_times = 2:00-9:00 12:00-24:00 = On définit la période où l'accès est possible
.....
}

5.4.5 Changement du port du serveur FTP

/etc/services : On ajoute un port spécifique pour le serveur FTP
mon_ftp 666/tcp = mon service FTP personnel sur le port n°666

/etc/xinetd.d/monxftp : On ajoute à xinetd la prise en charge de ce nouveau serveur FTP spécifique
service mon_ftp = Déclaration de mon nouveau serveur FTP. En relation avec /etc/services
{
only_from = 10.0.20.51 = Spécifie l'accès à 1 seule adresse IP
no_access = @IP = Inverse de « only_from »
..... = ... et d'autres restrictions
}

service xinetd restart ↵

netstat plantu | grep 666 ↵
tcp 0 0 0.0.0.0:**666** 0.0.0.0:* LISTEN2118/**xinetd** = C'est bien xinetd qui gère le serveur FTP mon_ftp (sur le port 666)

ftp serveur_ftp:666 ↵ = Se connecte sur le port spécifique 666 déclaré dans /etc/services, et c'est xinetd qui écoute le port

5.5 Actions et tâches de sécurité

Mots clés certification LPI 202 : telnet, nmap, snort, fail2ban, nc, iptables
Document PREPA_LPIC2.pdf = p. 274

5.5.1 Détection des intrusions et des vulnérabilités

5.5.1.1 IDS : Intrusion Detection System

Le pare-feu filtre sur l'adresse IP et le port. Si un programme malveillant utilise un flux réseau autorisé (sur le port 80 par exemple), le pare-feu ne bloquera rien.
La sonde IDS permet d'analyser le contenu du flux réseau (applicatif) sans se faire tromper par le n° du port

Technique d'analyse :
Détection d'anomalie = Détecte un comportement anormal (volume ICMP trop important par exemple)
Analyse de protocole = Analyse finement le protocole et vérifie que toutes les règles sont respectées
Analyse de signature = Analyse la signature d'attaques déjà connues

Ces analyse ne fonctionnement si la sonde se met à jour régulièrement

Organismes de veille et de recherche sur la sécurité :
BUGtrack : http://www.bugtrack.net/
CERT : http://www.cert.org/ : Computer Emergency Response Team
CIAC : http://www.doecirc.energy.gov/ : Computer Incident Advisory Capability
ANSSI : http://www.ssi.gouv.fr/ : Agence Nationale de la Sécurité des Systèmes d'Information

5.5.2 OpenVAS

Open Vulerability Assessment Scanner, variante libre du scanner de vulnérabilité Nessus
Le serveur permet de scanner et d'analyser les hôtes du réseau pour rechercher les vulnérabilités (NVT = Network Vulnérability Test)
Les clients analysent les hôtes et renvoient les résultats au serveur
« OpenVAS NVT Feed » est une source publique des vulnérabilités pour mettre à jour le serveur. Elle contient + de 15000 NVT (Network Vulnerability Test)

5.5.3 Commande telnet

telnet serveur_distant ↵ = Se connecte en Telnet sur le serveur distant
telnet 125.64.124.77 80 ↵ = On précise le port à utiliser

Commande	Description
?	Affiche l'aide
close	Termine la session Telnet
display	Affiche à l'écran les paramètres de la connexion (type de terminal, port)
environ	Permet de définir les variables d'environnement du système d'exploitation
logout	Permet de se déconnecter
mode	Bascule entre les modes de transfert ASCII (transfert d'un fichier en mode texte) et BINARY (transfert d'un fichier en binaire)
open	Permet de lancer une autre connexion à partir de la connexion en cours
quit	Quitte l'application Telnet
set	Modifie les paramètres de la connexion
unset	Charge les paramètres de connexion par défaut

5.5.4 Commande nmap

nmap = network mapper, utilitaire de scanne de port. Il permet de scanner un hôte distant ou bien tout un réseau et rapporte les ports TCP et UDP ouverts.

nmap 192.168.1.220 ↵ = Affichage des ports TCP ouverts parmi ceux que nmap trouve intéressant
nmap -F ↵ = Ne scanne que les ports listés dans le fichier nmap-services (= « -F » = fast)

nmap -sS 192.168.1.0/24 ↵ = Lance un scan furtif (= « -sS » = stealth scan = scanne infiltré) contre chaque machine active dans le réseau

nmap -sU 192.168.1.220 ↵ = Idem pour les ports UDP

PORT	STATE	SERVICE
53/tcp	open	domain
80/tcp	open	http

.....

nmap -p 1-65535 192.168.1.220 ↵ = Scanne tous les ports (= « -p ») de 1 à 65535

PORT	STATE	SERVICE
53/tcp	open	domain
80/tcp	open	http
88/tcp	open	kerberos-sec

.....

nmap -O 192.168.1.220 ↵ = Tente de déterminer l'OS
Running: Microsoft Windows 2003
OS details: Microsoft Windows Server 2003 SP1 or SP2
OS detection performed. Please report any incorrect results at http://nmap.org/submit/.

nmap -sP -n 10.0.0.0/24 ↵ = Découvre les machines présentes sur un réseau, en mode numérique (= « -n »)
Starting Nmap 4.52 (http://insecure.org) at 2010-01-14 21:21 CST
Host 10.0.0.1 appears to be up.
Host 10.0.0.100 appears to be up.
MAC Address: 00:1B:EA:F2:C4:70 (Nintendo Co.)
Host 10.0.0.104 appears to be up.
MAC Address: 00:19:21:27:8E:83 (Elitegroup Computer System Co.)
Host 10.0.0.106 appears to be up.
MAC Address: 00:14:22:61:E3:D9 (Dell)
.....

nmap -sV ↵ = Teste les ports ouverts pour déterminer le service en écoute et sa version

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	**ProFTPD**	**1.2.10**

5.5.5 Commande snort

Système IDS libre.
Snort utilise un langage de description des règles simple et léger qui est souple et assez puissant.

La plupart des règles Snort sont écrites sur une seule ligne.
Cela était nécessaire dans les versions antérieures à 1.8. Dans les versions actuelles de Snort, les règles peuvent s'étendre sur plusieurs lignes en ajoutant un \ barre oblique inverse à la fin de la ligne.

Les règles de Snort sont divisés en deux sections logiques, les règles d'en-tête et les règles d'options.
La règle d'en-tête contient les règles action, protocole, adresse source, adresses de destination et masque de réseau, ainsi que l'information sur les ports source et destination.
La section des règles d'option contient les messages d'alerte et des informations sur les parties du paquet doit être inspecté afin de déterminer si l'action de la règle doit être appliquée.

La commande # oinkmaster permet de mettre à jour les règles (abonnement nécessaire, ou bien récupération sur des sites gratuits)

/etc/snort/oinkmaster.conf : Fichier de configuration des règles
url = http://www.snort.org/snort-rules/fichier_règles.tar.gz

oinkmaster -o /etc/snort/rules ↵ = Recharge les règles du répertoire. A faire via un script cron

/etc/snort/snort.conf : Fichier de configuration
output alert_syslog: host=IP_serveur_syslog, LOG_ALERT = Lors de la détection d'une faille, l'alerte est envoyé à un serveur Syslog (= « alert_syslog ») définit par son adresse IP, sous la catégorie « ALERTE »

```
##################################################
# Step #7: Customize your rule set for more information, see Snort Manual, Writing Snort Rules
# NOTE: All categories are enabled in this conf file
##################################################

# site specific rules
include $RULE_PATH/local.rules  = Appel chaque fichier de règle

include $RULE_PATH/attack-responses.rules
.........
```

5.5.6 Commande Fail2Ban

Installer le paquet « fail2ban »

/etc/fail2ban/jail.conf : Fichier de configuration
[ssh]
enabled = true = Active la surveillance pour SSH par Fail2Ban
port = ssh,sftp,2276 = Port à bloquer si une règle Fail2Ban est validée (préciser le numéro, si le port par défaut a été changé)
filter = sshd
logpath = /var/log/auth.log = Fichier de log à analyser
maxretry = 6 = 6 tentatives échouées amènent à bloquer le port

5.5.7 Commande nc (netcat)

nc -u adresse_IP 80 ↵ = En UDP (= « -u »), communique sur l'adresse IP via le port 80
GET ↵ = Envoi la commande « GET » sur le site Web (port 80)

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
        <head>
        <title>Apache HTTP Server Test Page powered by CentOS</title>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
```

6 Détection et résolution des problèmes

Mots clés certification LPI 202 : /etc/, /etc/inittab, /etc/rc.local, /etc/rc.boot, /var/spool/cron/crontabs/, /etc/login.defs, /etc/syslog.conf, /etc/passwd, /etc/shadow, /etc/group, /sbin/init, /usr/sbin/cron, /usr/bin/crontab

6.1 Identifier les étapes de démarrage et chargeurs de dépannage

Mots clés certification LPI 202 : The contents of /boot/ and /boot/grub/, GRUB, grub-install, initrd, initramfs, Master boot record, /etc/init.d, lilo, /etc/lilo.conf

6.1.1 Reconnaître les 4 étapes du boot

- Le boot loader se charge et passe la main au kernel = En général, vous pouvez reconnaître ce stade parce que LILO affiche les quatre lettres "L", "I", "L" et "O". Chacune de ces lettres identifie un certain stade du processus de boot. Voir le chapitre « Les erreurs de LILO »
- Chargement du noyau = Cette étape peut être reconnue, car le noyau affichera différents messages.
  Exemple :
  Loading Linux-2.2.20
  ide_setup:hdc=ide-scsi
- Initialisation matérielle et configuration = Peut être identifiés par les différents messages qui vous informent sur les différents composants matériels qui ont été trouvés et initialisé.
  Exemple
  Ide0: BM-DMA at 0xff00-0xff07, BIOS settings: hda:DMA, hdb:DMA
- L'initialisation et la configuration démons = C'est spécifique à la distribution, mais cette étape peut être reconnu par des messages qui contiennent généralement des lignes comme Starting the xx daemon

dmesg est utilisé pour examiner ou contrôler le tampon des messages du noyau
dmesg > boot.messages ↵ = Redirige les messages qui sont apparus depuis le démarrage de la machine vers un fichier à consulter plus tard

6.1.2 La commande grub-install

grub-install -v ↵ = Affiche la version de Grub installée
grub-install /dev/sda ↵ = Installe Grub sur /dev/sda
grub-install --recheck /dev/sda ↵ = Vérifie que Grub s'est bien installé

6.1.3 initrd, initramfs

Comme initrd est un ram disque, le paquet cramfs doit être installé pour lire ce fichier
Ce fichier est en fait une archive cpio compressé au format gzip


mkinitramfs -k -o initramfs-2.6.21-686 2.6.21-686 ↵ = Crée une image initramfs par le fichier initramfs-*version* (= « -o » = output), en gardant les fichiers temporaires (= « -k » = keep), pour la version du noyau 2.6.21-686


Sous RedHat cette phase est incluse dans la phase ④ # ./make install ↵
Le fichier initrd-*version* sous /boot
Sinon, # mkinitrd /boot/init:img-2.6.39 2.6.39 ↵
Cette commande s'appuie sur devfs et non udev, et ne gère donc pas les disques sata

/boot/grub/menu.lst :
title CentOS (2.6.18-274.18.1.el5)
root (hd0,0)
kernel /vmlinuz-2.6.18-274.18.1.el5 ro root=/dev/VolGroup00/LogVol00
initrd /initrd-2.6.18-274.18.1.el5.img

6.1.4 MBR Master Boot Record

MBR = 512 octets

- 446 octets = Boot loader n°1, Grub ou LILO
- 64 octets = 4 X 16 octets = 4 partitions primaires
- 2 octets = magic number. Informe sur l'utilité des 64 octets précédents

dd if=/dev/sda of=fichier.mbr bs=512 count=1 ↩ = Sauvegarde le MBR

6.1.5 fichier de configuration /etc/lilo.conf

lilo -t ↩ = Vérifie la syntaxe du fichier /etc/lilo.conf
lilo -u ↩ = Désinstalle LILO et remet l'ancien MBR, sauvegardé par LILO lors de son installation
Idem -U
lilo ↩ = Lance LILO et écrase le MBR initial

Fichier de configuration /etc/lilo.conf
# Début de la section générale
boot = /dev/hda = Disque sur lequel on installe LILO, emplacement du MBR
prompt
default=linux = Nom de la section par défaut
label = linux = Début de la section « linux », invite au lancement de LILO
timeout=120 = en 1/10 seconde
compact = Optimisation; ne fonctionne pas sur tous les systèmes
ou lba = Large Bloc Access
read-only = Au boot Linux lance « fsck ». Pour faire cette opération il est indispensable que la partition soit en lecture seule.
image = /boot/vmlinuz = Nom et chemin du noyau Linux présent sur le système
ou /vmlinuz
root = /dev/hda2 = Emplacement du « / », indique la partition Linux à lancer
initrd = /initrd.img

6.1.6 Remplacement des options de Lilo en utilisant le shell

Commande Lilo :
/sbin/lilo -A ↩ = Affiche la partition active
/sbin/lilo -E ↩ = Édite le header ou met à jour le fichier image
/sbin/lilo -I ↩ = Affiche le chemin du noyau actuel
/sbin/lilo -M ↩ = Configure Lilo sur un disque
/sbin/lilo -q ↩ = Interroge le map
/sbin/lilo -R ↩ = Configure la ligne de commande par défaut pour le prochain reboot
/sbin/lilo {-u|-U} ↩ = Désinistalle LILO

Pour changer la configuration de Lilo au démarrage, dès que le système a booté et que l'écran de Lilo s'affiche, sélectionnez une entrée et appuyez sur [Tabulation]

Booter avec Lilo en single user :
linux init=/bin/bash ↩ = Boot le noyau Linux et vous place directement dans une copie du shell Bash
mount -o remount,rw -n / ↩ = Remonte le FS root pour qu'il soit accessible en lecture/écriture

6.1.7 Emplacement de l'installation de Lilo

Le 1er chargeur de Lilo peut être soit installé dans le MBR ou sur un secteur d'amorçage

6.1.8 Sauvegarde de Lilo

/sbin/lilo peut créer le bootprogram dans le MBR ou dans le 1er secteur d'une partition. Le bootprogram, parfois appelé le chargeur première étape va essayer de charger le 2d chargeur de démarrage. Le 2d chargeur est contenue dans un fichier sur la partition de démarrage. Par défaut il est dans le fichier /boot/boot.b.

Si vous utilisez /sbin/lilo pour écrire le bootprogram il va essayer de faire une copie de sauvegarde de l'ancien contenu du secteur d'amorçage et d'écrire l'ancien contenu dans un fichier /boot/boot.####.Les symboles de hachage sont en fait remplacés par les numéros majeur et mineur du périphérique sur lequel se trouve le secteur d'amorçage.
Par exemple, la copie de sauvegarde du MBR sur le premier disque IDE serait stocké sous /boot/boot.0300. Le chiffre 3 est le nombre majeur pour le fichier de périphérique /dev/hda, et 0 est le numéro mineur. /sbin/lilo n'écrasera pas un fichier de sauvegarde existant.

6.1.9 Les erreurs de Lilo

Lorsque Lilo se charge il affiche le mot « LILO ». Chaque lettre est écrit avant ou après une étape, afin d'identifier l'étape qui pose problème en cas de plantage.

« rien » = aucune partie de Lilo n'a été chargée. Soit Lilo n'est pas installé ou bien la partition contenant le boot secteur n'est pas active.
« L » = Le 1er chargeur a été chargé et démarré mais il ne peut lancer le 2d chargeur. Le nombre affiché indique le type de problème
« LI » = Le 1er chargeur peut lancer le 2d chargeur mais il n'a pas pu le l'exécuter
« LIL » = Le 2d chargeur a été lancé mais il ne peut charger la table de description
« LIL? » = Le 2d chargeur a été chargé à une mauvaise adresse
« LIL- » = La tableude description est corrompue
« LILO » = Toutes les parties de Lilo ont été chargées

6.2 Dépannage général

lsdev ↵ = Affiche des informations sur les périphériques (= device) en 4 colonnes : nom du périphérique, adresse DMA, adresse IRQ et ports I/O.
La commande lit les fichiers /proc/dma, /proc/interrupts et /proc/ioports
lspci ↵ = Informe sur les périphériques à l'instar du « gestionnaire de périphérique » sous Windows
Sous forme d'arbre # lspci -t ↵
lshal ↵ = Informe sur tous les périphériques dépendants de la couche d'abstraction matériel (= HAL)
lshw ↵ = Scan tous les matériels de la machine
dmidecode ↵ = Donne des informations sur le matériel à la façon « base de registre »
arch ↵ = Donne l'architecture du système (i386 ou 64 bits)
uname -m ↵ = Affiche des informations sur le matériel
uname -n ↵ = Affiche le nom d'hôte
Idem # hostname ↵
uname -r ↵ = Affiche la version du système
uname -s ↵ = Indique le système d'exploitation de la machine
uname -a ↵ = Affiche toutes les informations
uptime ↵ = Affiche le temps de fonctionnement du système et la charge système
lsusb ↵ = Liste les périphériques USB du système
lsusb -v ↵ = Idem avec plus d'information (« v » = verbose)
lsusb -t ↵ = Idem mais affiche les périphérique en arbre, en les rattachant à leur bus
lsmod ↵ = Affiche les informations sur les modules
Idem # cat /proc/modules ↵
modinfo module ↵ = Informe sur un module
-a = Affiche l'auteur du module
-d = Affiche la description du module
-p = Affiche les paramètres du module
-s = Redirige la sortie vers syslog plutôt que la sortie standard
insmod -s module ↵ = Insère un module en enregistrant les informations dans Syslog (= « -s ») plutôt que la sortie standard
rmmod module ↵ = Supprime un module
rmmod -s module ↵ = Supprime un module en enregistrant les informations dans Syslog (= « -s ») plutôt que la sortie standard
rmmod -a ↵ = Supprime tous les modules non utilisés
modprobe -l ↵ = Liste tous les modules
modprobe -l -t net ↵ = Liste les modules du type (=« t ») net = dans le répertoire du type : /lib/modules/kernel-version/kernel/net
modprobe -c module ↵ = Affiche la configuration complète du module
modprobe module ↵ = Charge un module
modprobe -r module ↵ = Supprime un module (« r » = remove), et tente de supprimer les modules non-utilisés liés au module à supprimer
modprobe -r module1 module2 ↵ = Supprime les 2 modules

6.2.1 Commande ldd

ldd /bin/ls ↵ = Affiche les bibliothèques nécessaires (dépendances) à l'exécution de la commande

```
linux-gate.so.1 =>  (0x00a49000)
librt.so.1 => /lib/librt.so.1 (0x0054c000)
libacl.so.1 => /lib/libacl.so.1 (0x007fe000)
.....
```

6.2.2 Commande ldconfig

ldconfig ↵ = Reconstruis le cache. Les fichiers à analyser sont dans le fichier /etc/ld.so.conf.
Un fichier ld.so.cache est alors créé. C'est important à faire après chaque modification dans le système des librairies pour être sûr que le cache est à jour

ldconfig -p ↵ = Affiche le contenu du cache de /etc/ld.so.cache (fichier compilé)

```
316 libs found in cache `/etc/ld.so.cache'
        libz.so.1 (libc6) => /lib/libz.so.1
```

```
        libz.so.1 (libc6) => /usr/lib/libz.so.1
        .....
        libz.so (libc6) => /usr/lib/libz.so
```

export LD_LIBRARY_PATH=chemin1:chemin2 ↵ = Permet de déclarer ponctuellement un chemin à analyser

6.2.3 Commande strace

Affiche les appels système d'un programme

Exemple d'un programme exécutable :

```
#include <stdio.h>
int main(void) {
      printf("Hello Word\n") ;
      return 1 ;
}
```

strace HelloWord ↵ = Affiche les appels systèmes

```
execve("/home/sedoglav/Enseignements/Informatiques/Licence/GMI/OS/TP/1/HelloWord", ["HelloWord"], [/*
        43 vars */]) = 0
uname({sys="Linux", node="erichtonios", ...}) = 0
brk(0)                                  = 0x80494bc
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=51700, ...}) = 0
old_mmap(NULL, 51700, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40012000
close(3)                                = 0
open("/lib/i686/libc.so.6", O_RDONLY)   = 3
read(3, "\177ELF\1\1\1\0\0\0\0\0\0\0\0\0\3\0\3\0\1\0\0\0\220\201"..., 1024) = 1024
fstat64(3, {st_mode=S_IFREG|0755, st_size=1167240, ...}) = 0
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x4001f000
old_mmap(NULL, 1179584, PROT_READ|PROT_EXEC, MAP_PRIVATE, 3, 0) = 0x40020000
mprotect(0x40137000, 36800, PROT_NONE)  = 0
old_mmap(0x40137000, 20480, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED, 3, 0x117000) =
        0x40137000
old_mmap(0x4013c000, 16320, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1,
        0) = 0x4013c000
close(3)                                = 0
munmap(0x40012000, 51700)               = 0
fstat64(1, {st_mode=S_IFCHR|0622, st_rdev=makedev(136, 2), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x40012000
write(1, "Hello Word\n", 11)            = 11
munmap(0x40012000, 4096)                = 0
_exit(11)                               = ?
```

6.2.4 Commande strings

Utiliser la commande strings pour trouver les chaînes de caractères affichables dans un fichier binaire ou de données. Elle listera les séquences de caractères affichables trouvées dans le fichier cible. C'est intéressant pour un examen rapide (et sale) d'un core dump ou pour regarder un fichier image inconnu

strings fichier-image | more ↵ = Pourrait afficher quelque chose comme JFIF, qui identifierait le fichier en tant que graphique jpeg)

6.2.5 Commande ltrace

Le fonctionnement de ltrace est relativement similaire à celui de strace, à la différence près que ltrace ne montre pas les appels systèmes, mais les appels aux fonctions de bibliothèques

Exemple :

```
strftime (" Thu", 1024, "%a", 0xb7f64380) =4
fwrite ("Thu", 3, 1, 0xb7f614e0) =1
fputc (' ', 0xb7f614e0) =32
```

```
strftime (" Feb", 1024, " %b", 0xb7f64380) =4
fwrite ("Feb", 3, 1, 0xb7f614e0) =1
fputc (' ', 0xb7f614e0) =32
fwrite ("19", 2, 1, 0xb7f614e0) =1
```

6.2.6 Commande lsof

Liste les fichiers ouverts sur le système, informe sur les processus qui utilisent ces fichiers et quelles connexions les utilisent (TCP ou UDP).

lsof | grep "/public" ↵ = Liste les processus qui ont un fichier ouvert sur le partage « public »

smbd	17728	adamh	cwd	DIR	8,65	8192	5 /public
bash	21712	root	cwd	DIR	8,65	8192	5 /public
lsof	21841	root	cwd	DIR	8,65	8192	5 /public
grep	21842	root	cwd	DIR	8,65	8192	5 /public
lsof	21843	root	cwd	DIR	8,65	8192	5 /public

lsof -P -i@10.0.0.104 ↵ = Détermine la connexion entre 2 machines. La machine = 10.0.0.104 et fait tourner un processus Samba (smbd). Ne converti pas les n° de ports dans leur nom (= « -P »). Ne montre pas les fichiers ouverts mais les sockets (= « -i ») dont l'adresse = 10.0.0.104

```
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
```
smbd 1329 root 5u IPv4 252713 TCP 10.0.0.1:139->10.0.0.104:1568 (ESTABLISHED) = C'est la machine distante = 10.0.0.1 qui est connecté en Samba (sur le port 139)

6.2.7 Generic issues with hardware problems

Le script ci-dessous peut faire apparaître des erreurs matériels (s'il y en a). La boucle va compiler à l'infinie un noyau. Chaque compilation créé un fichier de log. En comparant les différents fichiers avec les commande # sum ou # md5sum, ils doivent être identiques sinon il y a un problème matériel

```
# adapted from http://www.bitwizard.nl/sig11
# site : http://www.bitwizard.nl/     Contact : info@bitwizard.nl
#
cd /usr/src/linux
c=0
while true
do
  make clean &> /dev/null
  make -k bzImage > log.${c} 2> /dev/null
  c=`expr ${c} + 1`
done
```

6.2.8 Commande rdev, ramsize, vidmode et rootflags

rdev ↵ = Sans arguments, rdev affiche une ligne de /etc/mtab pour le système de fichiers racine actuel. Sans arguments, ramsize, vidmode, et rootflags affichent l'aide

```
/dev/root /
```

ramsize ... ↵ = rdev -r ... ↵
vidmode ... ↵ = rdev -v ... ↵
rootflags ... ↵ = rdev -R ... ↵

Dans une image du noyau Linux, il y a des octets qui spécifient le périphérique racine, le mode vidéo et la taille du disque mémoire. rdev changera ces valeurs.

Lors de l'invocation de la commande rdev, le paramètre root_device peut être quelque chose comme : /dev/hda1, /dev/hdf13, /dev/sda2 ou /dev/sdc4
Pour la commande ramsize, le paramètre size spécifie la taille du disque mémoire en kilo-octets.
Pour la commande rootflags, le paramètre flags contient des informations supplémentaires utilisées lors du montage de la racine. Actuellement, le seul effet de ces drapeaux et de forcer le noyau à monter le système de fichiers en lecture-seule si flags est non nul.
Pour la commande vidmode, le paramètre mode spécifie le mode vidéo :

- -3 = Pose la question

- -2 = VGA étendu
- -1 = VGA normal
- 0 = comme si « 0 » était choisi comme réponse à la question
- 1 = comme si « 1 » était choisi comme réponse à la question
- 2 = comme si « 2 » était choisi comme réponse à la question
- n = comme si « n » était choisi comme réponse à la question

6.2.9 Résoudre des conflits IRQ/DMA

Pour résoudre ces conflits, il faut utiliser la commande # dmesg, et comparer les résultats avec le contenu de /proc/interrupts ou avec le résultat de la commande # lsdev.
L'IRQ du bus PCI est également affiché avec la commande # lspci en regardant le contenu /proc/pci

6.3 Dépannage des ressources système

6.3.1 Variables systèmes

Les commandes # set et # env permettent d'afficher les variables d'environnement

/etc/profile = Fichier global d'initialisation du système, lors du login. Il contient les variables d'environnement (comme TMOUT), incluant le PATH et les programmes de démarrages
/etc/profile.d = Répertoire contenant les fichiers de démarrage spécifiques pour les différents shells. Tous ces fichiers seront exécutés par n'importe quel shell.
/etc/bashrc = Autre fichier global d'initialisation, qui peut être exécuté par le .bashrc de l'utilisateur pour chaque shell bash lancé. Il contient généralement les fonctions et les alias. pour le shell.
/etc/shells = Liste tous les shell disponibles sur le système (/bin/bash, /bin/sh, /bin/tcsh, /bin/false, etc.). /bin/false répondra toujours faux

Informations tirées du site « Gnu.org » http://www.gnu.org
Source : http://www.gnu.org/software/bash/manual/html_node/Bash-Startup-Files.html
Licence : Licence Publique Générale GNU http://www.gnu.org/licenses/licenses.html#GPL

Les fichiers suivants sont lus pour chacune des façons dont le shell peut être appelé: /etc/profile, /etc/bashrc, ~/.bash_profile et ~/.bashrc.
Le fichier ~/.bash_logout n'est pas utilisé pour une invocation du shell. Il est lu par le shell quand un utilisateur se déconnecte du système.
Les fichiers /etc/profile et ~/.bash_profile sont lus quand le shell est invoqué comme shell interactif de connexion.
Le fichier ~/.bashrc est lu quand le shell est invoqué comme shell interactif sans fonction de connexion.
/etc/rc.d/rc.local = Dernier fichier à être lu au démarrage du système

6.3.2 Définition des paramètres du noyau

6.3.2.1 Nommage des objets paratagés

Un objet partagé a un « real name », un « soname » et un « linkname ».

- real name = Nom du fichier qui contient l'ojet partagé complié. libNAME.so[.major][.minor][.patchlevel]. Par exemple : /lib/libpam.so.0.72
- sonanme = real name sans le nombre de la version mineure /lib/libpam.so.0
- linkname = soname sans aucune information sur la version /lib/libpam.so

6.4 Configurations d'environnement de dépannage

6.4.1 Core system variables

etc/profile est exécuté seulement lorsqu'un nouveau shell démarre.
Les commandes de /etc/profile sont exécutées au moment du login.
Les commandes du fichier .bashrc du home directory du user sont lancées à chaque shell.
Le contenu du répertoire /etc/skell permet de s'assurer que tous les nouveaux utilisateurs sur votre système LFS commencent avec la même configuration. Le répertoire /etc/skel est utilisé par le programme /usr/sbin/useradd.
Le fichier /etc/login.defs défini la configuration des mots de passe. Ce fichier est nécessaire pour le fonctionnement du système

6.4.2 La crontab

crontab -u david -l ↵ = Liste la contrab de david (= « -u ») sur la sortie standard (= « -l »)
crontab -r ↵ = Supprime la contrab en cours
contrab -e ↵ = Edite la contrab courante

6.4.2.1 Fichiers cron.deny et cron.allow

Si le fichier cron.allow existe, alors vous devez être mentionnés dans celui-ci pour pouvoir utiliser cette commande.
Si le fichier cron.allow n'existe pas, mais que le fichier cron.deny existe, alors vous ne devez pas être mentionnés dans celui-ci, si vous désirez utiliser cette commande.
Si aucun de ces deux fichiers n'existe, seul le super-utilisateur a le droit d'utiliser cette commande.

6.4.3 Commande de manipulation des mots de passe

- # pwconv ↵ = Crée le fichier shadow à partir du fichier passwd et d'un éventuel fichier shadow.
- # pwunconv ↵ = Crée le fichier passwd à partir des fichiers passwd et shadow puis supprime shadow
- # grpconv ↵ = Crée gshadow à partir de group et d'un éventuel fichier gshadow
- # grpunconv ↵ = Crée group à partir des fichiers group et gshadow puis supprime gshadow
- # chage david ↵ = Modifie l'age et la date d'expiration du mot de passe de david

6.4.3.1 Problème lié à l'authentification

home# ls -l ↵
total 8
dr-xr-xr-x 6 root **0** 1024 Dec 6 19:07 ftp = La commande n'affiche que les n° des groupes
drwxr-xr-x 6 www **33** 1024 Oct 8 17:18 omproject
drwxr-xr-x 5 piet **1003** 1024 Dec 6 23:34 piet

Cela devrait être :
dr-xr-xr-x 6 root **root** 1024 Dec 6 19:07 ftp
drwxr-xr-x 6 www **www** 1024 Oct 8 17:18 omproject
drwxr-xr-x 5 piet **info** 1024 Dec 6 23:34 piet

Le problème est lié au fichier /etc/group qui n'est sans doute pas définit. La commande # pwconv peut re-synchroniser le fichier passwd

7 Annexes

7.1 Liste des ports

Ports 1 → 1023 = réservés, seul root peut les utiliser
Ports 1024 → 49151 = non réservés
Ports 49152 → 65535 = Utilisés pour test

cat /etc/services ↵ = Liste des « ports bien connus » (= well-know ports)

N° du port	Applications assignée	Description
20 21	FTP	Actif : Les données transitent par le port 20 et sur le port 21 pour les informations Passif : Seule la demande se fait par le port 20
22	SSH	
23	Serveur Telnet	
25	Serveur SMTP	
53	Serveur DNS	
67	Serveur BootTP et DHCP	
80	Serveur HTTP	
109	POP2	
110	POP3	
115	SFTP	
119	NNTP	Serveur de news
123	NTP	
143	IMAP2 et IMAP4	
161	SNMP	
220	IMAP3	
389	LDAP	
443	HTTPS	
445	CIFS	Common Internet File System de Microsoft, ancien SMB
514	Syslog	
546	DHCP	
631	IPP	Internet Printing Protocol
873	Rsync	
1194	OpenVPN	
5432	PostgreSQL	

7.2 Commandes sous /bin

bash, bunzip2, bzcat, bzdiff, bzgrep, bzip2, bzmore, cat, chgrp, chmod, chown, cp, cpio, date, dd, df, dir, dmesg, dnsdomainname, domainname, echo, ed, egrep, false, fgrep, fuser, fusermount, grep, gunzip, hostname, ip, kill, less, ln, ls, lsmod, mkdir, more, mount, mt , mv, nano, nc, netstat, ping, ps, pwd, rm, rmdir, sed, sh, sleep, sync, tar, touch, true, umount, uname

7.3 Commandes sous /sbin

badblocks, debugfs, depmod, dhclient, dumpe2fs, e2fsck, e2image, e2label, fdisk, fsck, getty, halt, hdparm, hwclock, ifconfig, ifdown, ifquery, ifup, init, insmod, ip, ip6tables, iptables, iw, iwconfig,

ldconfig, lsmod, lspcmcia, MAKEDEV, mke2fs, mkfs, mkswap, modinfo, modprobe, parted, partprobe, poweroff, reboot, resize2fs, resolvconf, restart, rmmod, route, runlevel, sfdisk, shutdown, status, stop, swapoff, swapon, sysctl, telinit, tune2fs, udevadm

7.4 Répertoires sous /proc

8 Licence Créative Commons

Tout commentaire est le bienvenu. Merci de m'en faire part sur publication@claveau.net

8.1 Citations des références utilisées dans cet ouvrage

Livre « LPI », de Sébastien Bobillier, aux Editions Eni (12/2010, ISBN : 2746059142)

Site « snow.nl», de Heinrich W. Klöpping, Beno T.J. Mesman, Piet W. Plomp, Willem A. Schreuder, Many, many
Edité par : Jos Jansen et Joost Helberg
http://snow.nl/dist/xhtmlc/index.html

Site « Wikipédia France » : Contenu soumis à la licence CC-BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0/deed.fr) Source : Wikipédia en français (http://fr.wikipedia.org/).
http://fr.wikipedia.org/wiki/Portail:Informatique

Site « noisette.ch » de Benoit Perroud
http://www.noisette.ch/wiki/index.php/Mdadm

Site « Apache Software Fondation »
Copyright © 2012 The Apache Software Foundation
Licensed under the Apache License, Version 2.0.
http://www.apache.org/

Site des contributions de MartyMac, de Gaël Laplanche
http://contribs.martymac.org/
Copyright (c) 2005-2010, Ganaël LAPLANCHE. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation;

Kit Sendmail v8 de Jussieu, par Pierre David (CRC, ULP), Jacky Thibault (CCR, Jussieu) et Sébastien Vautherot (CCR, Jussieu). Version 5.4, novembre 2001
°c Pierre David, 1994-2001
ftp://ftp.jussieu.fr/jussieu/sendmail/kit/ et http://www.kit-jussieu.org/

Site Penguin Tutor - Linux Website and Certification Help, de Stewart Watkiss
Licence : Creative Commons Attribution 2.0 UK: England & Wales License
A website of the Watkiss Online Group
http://www.penguintutor.com/certification.php

Site IBM « DeveloppperWorks » - Linux Professional Institute (LPI) exam prep
http://www.ibm.com/developerworks/linux/lpi/

Site http://www.tuteurs.ens.fr de Joël Riou (tuteurs@clipper.ens.fr)
Source : http://www.tuteurs.ens.fr/internet/courrier/procmail.html#procmailrc

Site de l'université du Delaware
http://www.udel.edu
Source : http://www.udel.edu/topics/e-mail/procmail/inst.html