Mémento pour la certification LPI-102

Objet :

Ce mémento est la remise au propre de mes notes prises au cours de la formation pour le passage de la certification LPI n° 102, du Linux Professional Institute

Référence du document :

Auteur : David CLAVEAU
Version : 5.1
Date d'enregistrement : 03/12/2012

Tous commentaires est le bienvenue. Merci de m'en faire part sur publication@claveau.net

Notations du document :

Lignes de commandes :	# commande ↵
Chemin :	« /etc/grub/ »
Commande SQL :	mysql> commande ; ↵
Contenu d'un fichier :	HOSTNAME=portable_david = Défini le nom du poste
↵	Appuyez sur la touche « Entrée »
« Ctrl+a » :	Appuyez sur la touche « Contrôle », et la touche « a »
Référence à une image ou un document externe :	http://fr.wikipedia.org/wiki/X_Window_System GNU Free Documentation License version 1.2

Sommaire :

1 Personnaliser et utiliser l'environnement Shell

1.1 Variable

1.1.1 Variable d'environnement

PATH = Liste de répertoire
HOME = Le répertoire personnel (home directory)
USERNAME = Le username
TERM = Le type de terminal texte ou X

1.1.2 Les variables du Shell

pi=3.14 ↵ = Attribue la valeur « 3.14 » à la variable « pi »
echo $pi ↵ = Donne la valeur de la variable « pi », grâce au « $ » qui précède le nom de la variable
3.14
echo pi ↵ = sans « $ »
pi

export pi ↵ = Permet d'exporter la variable pour les autres programmes et les shell script. La variable n'est plus locale

1.2 alias

alias ↵ = Affiche tous les alias
Idem # vi /etc/alias ↵
alias nom_alias = 'commande options' ↵ = Crée un alias pour la commande
alias nom_alias = 'commande options ; commande2 options' ↵ = Crée un alias exécutant 2 commandes
unalias nom_alias ↵ = Supprime l'alias
/chemin/commande ... ↵ = Outre-passe l'alias de la commande

1.3 Fonction

Identique à l'alias mais permet de définir des « petits programmes ». Des arguments peuvent être ajoutés

nom_fonction {commande1 options ; commande2 options } ↵

lsps () { = Permet d'indiquer un argument représenté par « $1 »
> ls -l $1
> ps aux | grep `/bin/basename $1`
> }

lsps /usr/sbin/httpd ↵ = Donne des informations sur le programme httpd et donne la liste des processus
-rwxr-xr-x 1 root root 317072 2010-01-22 14:31 /usr/sbin/httpd = résultat du « ls -l »
root 1882 0.0 1.5 22664 8088 ? Ss Aug10 0:14 /usr/sbin/httpd = résultat du « ps -aux ... »
apache 20869 0.0 0.6 22664 3560 ? S 04:27 0:00 /usr/sbin/httpd

1.4 Fichiers de configuration

Ces fichiers permettent de définir les alias, fonctions, variables, etc. 1 seule fois, sans avoir à tout retaper à chaque login.

Fichier	Description
/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/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.
~/.bash_profile	S'il existe, ce fichier s'exécute automatiquement au login après /etc/profile
~/.bash_login	Si le fichier .bash_profile n'existe pas, ce fichier s'exécute automatiquement au login
~/.profile	S'il n'y a ni .bash_profile, ni .bash_login, ce fichier s'exécute automatiquement au login. C'est le fichier de configuration originale pour le Bourne shell
~/.bashrc	Ce fichier est exécuté automatiquement lorsque le shell se lance. Il contient le login, les alias, les fonctions systèmes, etc.

~/.bash_logout Ce fichier s'exécute automatiquement au logout

1.5 .inputrc

Contient des raccourcis et des variables qui influent sur la réponse du bash à certaines frappes du clavier, comme par exemple la touche d'effacement arrière. Le fichier général est dans /etc/inputrc
Par défaut, bash est configuré pour émuler l'éditeur Emacs, mais une interface d'édition comme VI est également disponible. C'est le « readlines » qui gère toutes les entrées au clavier. Readline peut-être personnalisé via le fichier .inputrc.

set editig-mode vi = Emule VI pour l'édition dans Bash
Control-t : ''top -d1 \C-m'' = Ajoute le raccourcis clavier « Ctrl+t » pour lancer la commande « top » personnalisée. « \C-m » = retour chariot = « Ctrl+m»

2 Écrire de simple script

2.1 Cote et guillement

Entre les guillemets '' '', les méta-caractères comme « $ », « \ » ou « ! » sont interprétés
Entre les cotes, rien n'est interprété.

2.2 Opérateur logique

cmd1 && cmd2 ↵ = cmd1 est exécutée. Si elle se déroule correctement alors cmd2 est lancée
cmd1 || cmd2 ↵ = cmd1 est exécutée Si elle ne se déroule pas correctement, alors cmd2 est également exécutée.
En fait, il faut que cmd1 ne se déroule pas correctement pour que cmd2 s'exécute.

2.3 Lancement d'un script

chmod a+x commande ↵ = Rend la commande exécutable (= « +x ») pour tous (= « a » = all)
./commande option ↵ = La commande est lancée sans invoquer le Bash

#! /bin/bash = Dans le script, indique quel interpréteur le shell doit utiliser, grâce au SheBang (= « # ! »)
SheBang = Sharp (= « # ») et Bang (= « ! »)
Idem pour du Bourne Shell #! /bin/sh
Idem pour du C-Shell #! /bin/csh

2.4 Environnement d'un script Bash

Lors de l'exécution d'un script avec #!/bin/bash, une nouvelle instance de bash est lancée avec son propre environnement pour exécuter les commandes du script. Les variables exportées dans le shell parent sont copiés dans l'environnement du fils. Il exécute les fichiers de configuration du shell (comme bash_profile, .bashrc, etc.).
Avec ces fichiers de configuration, des variables shell supplémentaires peuvent être définies ou remplacées. Si vous êtes dépendant d'une variable dans votre script shell, assurez-vous qu'elle soit paramétrée dans les fichiers de configuration du shell ou exportés dans l'environnement de votre shell fils, mais pas les deux.
L'héritage unidirectionnelle : Bien que l'environnement de votre shell courant soit passé dans un script shell, cet environnement ne repasse pas au shell d'origine lorsque votre programme se termine. Cela signifie que les modifications apportées aux variables pendant l'exécution de votre script ne sont pas conservés à la fin de celui-ci. Au lieu de cela, les valeurs des variables du shell parent restent identiques comme avant que le script fils soit exécuté.

2.5 Localisation, propriétaire et permission

Pour qu'un script s'exécute, il faut :

1. # /usr/local/bin/script.sh ↵ = Indiquer explicitement le chemin du script
   ou bien qu'il soit dans un chemin enregistré dans le PATH (à ajouter dans le fichier .bash_profile par exemple)
   PATH=$PATH:/chemin/du/script

2. que le fichier soit exécutable
   # chmod +x script ↵
   # chmod 700 script ↵ = Permet de protéger l'accès au script. Seul le propriétaire pourra le modifier et l'exécuter

2.6 Droits SUID et SGID

Également traité dans le Mémento LPI 101. Complété dans le chapitre « Sécurité » / « Insécurité du SUID »

Le droit SUID ou SGID permet d'utiliser le fichier avec les droits du user ou du groupe du fichier.

Pour des raisons de sécurité, les FS Linux ne prennent pas en compte les SUID ou SGID sur les fichiers script.

rw**S** rwx rw = SUID
rwx rw**S** rw = SGID
« s » = SUID ou SGID avec le droit exécuter (= « x »), « S » = SUID ou SGID sans le droit exécuter (= « x »)

En octal : SUID=4000, SGID=2000
En modal : SUID = « u+s », SGID= « g+s »

Exemple :
3514 = r-x –s r-T
4511 = /etc/passwd
4755 = /bin/ping

3 Script Bash de base

3.1 Code de résultat ou de retour

Tout programme renvoi un code de résultat à la fin de son exécution.
# echo $? ↵ = Affiche le code de résultat de la dernière commande lancée
Si = 0, alors tout s'est bien déroulé
Si ≠ 0, alors le programme ne s'est pas bien terminé
Si 128 + N , alors la commande a été interrompue par le signal N

Autres codes de retour :
$# = Permet d'afficher le nombre de paramètres passé au script
$0 = Affiche le nom de la commande
$1 = Affiche le 1er argument passé au script ($2 pour le second, etc.)
$$ = Affiche le PID du processus
$! = Affiche le PID du processus père

3.2 Commande de substitution

La sortie de la commande est interprétée par le shell et est stockée dans une variable
LIGNE_RC=$(wl -l fichier) ↵ = Le nombre de ligne du fichier est stocké dans la variable « LIGNE_RC »
echo $LIGNE_RC ↵
13

3.3 Envoyer un mail par script

echo ''Problème du serveur de sauvegarde'' | mail -s ''PB SERVEUR'' root ↵
mail -s ''PB SERVEUR'' root < fichier_log ↵ = Transfert le fichier de log
Idem # cat fichier_log | mail -s ''PB SERVEUR'' root

Le destinataire peut être root, un user ou une adresse mail

3.4 Commandes de références

3.4.1 for

```
for i in 1 2 3 4 5
        do
        echo ''Hello $i fois" = Écrit « Hello 1 fois », « Hello 2 fois », …, « Hello 5 fois »
done

for filename in gros_fichier*
        do
        echo "Compression de $filename" = Écrit « compression de gros_fichier* »
        gzip $filename = Compresse tous les gros_fichiers* trouvés
done
```

3.4.2 break

Sort de la plus petite boucle pour les commandes « for », « while » ou « until ».
Si n est supérieur au nombre de boucle, la boucle externe entourant la plus petite boucle doit être sortis.

```
for i in 1 2 3 4 5
do
```

```
        commande1 = Exécute la commande1 pour toutes les valeurs de « i »
        if (condition)  =  Si la condition n'est pas valide ...
        then
                break = ... la boucle est abandonnée
        fi
        commande2 = Exécute la commande2 tant que la boucle est bonne et que la condition qui lance le
        « break » n'est pas apparue
done
```

3.4.3 continue

```
for i in 1 2 3 4 5
do
        commande1 = Exécute la commande1 et 2 pour toutes les valeurs de « i », tant que la condition
n'est pas valide
        if (condition)
        then
                continue = Passe à la prochaine itération de « i » sans exécuter la commande2
        fi
        commande2
done
```

3.4.4 case

```
case `expr $jours % 7` in
        0)
                echo Lundi = Affiche « Lundi » si l'expression «  expr $jours % 7 » = 0
        1)
                echo Mardi = Affiche « Mardi » si l'expression = 1
        ...
esac
```

3.4.5 echo

```
# echo toto  ↵  = Ecrit « toto » sur la sortie standard avec saut de ligne
# echo  ↵  = Saute une ligne
# echo -n ''toto''  ↵  = Supprime le saut de ligne à la fin de « toto »

# echo -e ''\a''  ↵  = Prend en compte les caractères d'échappement (= « -e)
```

Caractères d'échappement :

```
        \a  =  Joue un son d'alerte
        \b  =  Insère un backspace
        \c  =  Supprime le saut de ligne à la fin. Idem # echo -n ...
        \f  =  Insère un saut de page
        \\  =  Insère un backslash « \ »
        \n  =  Insère un saut de ligne
        \r  =  Insère un retour chariot
        \t  =  Insère une tabulation
```

3.4.6 exit

```
# exit 3  ↵  = Quitte un script shell avec le code de retour « 3 »
```

Les codes de retour sont traités dans le chapitre « Script Bash de base / Code de résultat ou de retour »

3.4.7 function

```
# function ma_func
{
        echo "le paramètre est $1"
}

# ma_func A  ↵
        le paramètre est A
# ma_func two  ↵
        le paramètre est two
```

3.4.8 getopts

Permet de facilement parcourir tous les paramètres passés à un script.

```
while getopts a:b:c:d option  =  A chaque appel au script, « getopt » va placer les paramètres passés dans
```

```
« option »
do
        case $option in
                a)
                        echo "option a : $option"
                        ;;
                b)
                        echo "option b : $option"
                        ;;
                c)
                        echo "option c : $option"
                        ;;
                d)
                        echo "option d" : $option"
                ;;
        esac
done
```

3.4.9 if

Formats possibles pour la commande « if » :

```
if      then    fi
if      then    else    fi
if      then    elsif   then    .....   fi
```

```
if expression1
        then
                commande1 = Exécute la commande1 si l'expression1 est vrai
        elsilf expression2 = Sinon, si l'expression2 est vrai
        then
                commande2 = Alors exécute la commande2
        else
                commande3 = Sinon (si ni l'expression1 ni l'expression2 sont vraies) exécute la commande3
fi
```

3.4.10 kill

kill -signal id_process ↵ = Envoi le signal au processus
Idem # kill -s signal_id id_process ↵
kill 1200 ↵ = Envoie le signal -15 au processus 1200
killall nom_process ↵ = Envoie le signal -15 à tous les processus dont le nom est « nom_process »
pkill motif ↵ = Envoi un signal sigkill (-15) à tous les processus dont le nom répond au motif. A la façon de pgrep, pkill est capable de reconnaître le motif donnée pour sélectionner le ou les processus à tuer.

Liste des signaux :
kill -l ↵ = Affiche la liste des signaux

-1	SIGHUP	HUP	reload
-2	SIGINT	INT	Arrête le lancement. Interrompt le processus = « Ctrl+c »
-9	SIGKILL	KILL	Tue le processus. Arrête sans condition et immédiatement le processus
-1	SIGTER	TERM	Termine gentiment si possible le processus. Demande au processus de se
5	M	TSTP	fermer
-2	SIGTSTP	CON	Arrête l'exécution, mais reste prêt à repartir = « Ctrl+z »
0	SIGCON	T	Continue l'exécution du processus. Relance après l'arrêt par « Ctrl+z »
-1	T		(SIGTSTP)
8			

Toutes les commandes suivantes ont le même résultats : elles envoient un signal SIGTERM aux processus 1000 et 1001 :

```
# kill 1000 1001                    # kill -15 1000 1001          # kill -SIGTERM 1000 1001

# kill -sigterm 1000 1001           # kill -TERM 1000 1001        # kill -s 15 1000 1001

# kill -s SIGTERM 1000 1001
```

3.4.11 read

Lit une ligne de l'entrée standard, et l'affecte à une variable.

```
echo -n "Quel est votre fruit favori? "
read fruit  = Attribue la réponse donné par l'entrée standard à la variable $fruit
echo "Votre fruit favori est $fruit."  = Affiche la phrase avec le nom du fruit entrée à la question
```

3.4.12 return

Renvoi une valeur de retour sans quitter le script, plutôt que d'utiliser « exit ».

```
function script() {
        for (i=0;i<4;i++) {
                box = i+2
                if (box > 4) {
                        return 1;
                }
        }
        return 0;
}
```

3.4.13 seq

Affiche une séquence de nombres sous la forme : 1er nombre / incrément / dernier nombre

```
# seq 5  ↵  =  Le premier et l'incrément = 1 car ils sont omis. Affiche « 1  2  3  4  5 »
# seq 2 5  ↵  = L'incrément = 1 car il est omis. Affiche « 2  3  4  5 »
# seq 5 4 13  ↵  = Affiche « 5  9  13 »
# seq -w 8 12  ↵  = Égalise la sorti par des zéros. Affiche « 08  09  10  11  12 »
        Idem # seq --equal-width ...
# seq -w -s";" 1 10  ↵  = Affiche le séparateur « ; » (= « -s »)
01;02;03;04;05;06;07;08;09;10
# seq -f %e 1 2 6  ↵  = Utilise le style printf (= « -f ») pour le format de la virgule flottante (= « %e »)
1,000000e+00
3,000000e+00
5,000000e+00
```

3.4.14 shift

Permet de décaler les paramètres. La valeur du 1er paramètre ($1) est remplacée par la valeur du 2d paramètre ($2), celle du 2d ($2) par celle du 3ème ($3), etc...
On peut indiquer en argument (shift n) le nombre de pas (position) dont il faut décaler les paramètres.

```
#!/bin/bash
# decale_param.sh
echo "Nombre de paramètres : $#"
echo "Le 1er paramètre est : $1"
echo "Le 3ème paramètre est : $3"
shift
echo "Nombre de paramètres : $#"
echo "Le 1er paramètre est : $1"
echo "Le 3ème paramètre est : $3"
echo "Décalage de quatre pas avec la commande \"shift 4\""
shift 4
echo "Nombre de paramètres : $#"
echo "Le 1er paramètre est : $1"
echo "Le 3ème paramètre est : $3"

# ./decale_param.sh 1 2 3 4 5 6 7 8 9 10
Nombre de paramètres : 10 = Au lancement du script, sans commande shift lancée
Le 1er paramètre est : 1
Le 3ème paramètre est : 3
Nombre de paramètres : 9 = Après le 1er shift
Le 1er paramètre est : 2
Le 3ème paramètre est : 4
Décalage de quatre pas avec la commande \"shift 4\"
Nombre de paramètres : 5 = Après le « shift 4 »
Le 1er paramètre est : 6
```

```
Le 3ème paramètre est : 8
```

3.4.15 source

Lit et exécute le fichier. Par exemple pour .bashrc
Les variables d'environnement du shell père ne sont pas utilisables par un script lancé dans un shell fils, sauf si celui-ci a été lancé par # source
Le fichier n'a pas besoin d'être exécutable mais son chemin doit se trouver dans le PATH
source ./commande option ↵ = Demande au Bash de lancer la commande
Idem # ./commande option ↵
Idem # /bin/bash ./commande option ↵

3.4.16 test

test expression ↵ = Renvoie un code de retour = 0 (vrai) ou = 1 (faux) suivant l'évaluation de l'expression
Idem # [expression] ↵ = Les espaces entre « [« et «] » sont nécessaires
test -r fichier ↵ = Évalue si le fichier existe et s'il est lisibe (= « -r »)
Idem # [-r fichier] ↵

```
if test -r fichier
        then
                echo "Le fichier existe"
        fi
```

test -d fichier ↵ = Évalue si le fichier est un répertoire
test -L fichier ↵ = Évalue si le fichier existe et si c'est un lien symbolique
test fichier1-ot fichier2 ↵ = Évalue si le fichier1 est plus vieux (= « -ot » = older than) que le fichier2
test chaine1 = chaine2 ↵ = Évalue si les 2 chaînes de caractères sont équivalentes
test chaine1!= chaine2 ↵ = Évalue sir les 2 chaînes de caractères sont différentes

Autres options :

-e fichier	si le fichier existe
-f fichier	si le fichier est existe est que c'est un fichier standard
-s fichier	si le fichier existe que que sa taille n'est pas nulle
-x fichier	si le fichier existe est qu'il est exécutable
-z chaine	si la longueur de la chaine est nulle
-n chaine	si la longueur de la chaine n'est pas nulle

3.4.17 until

Teste une condition au début de la boucle et continue à boucler tant que la condition est fausse (l'opposé de la boucle while). Dès que la condition est réalisée, on sort de la boucle

```
until [ condition-est-vraie ]
        do
        commande(s)...
done
```

3.4.18 while

Teste une condition au début de la boucle et continue à boucler jusqu'à ce que la condition devient vraie (l'opposé de la boucle until). Dès que la condition est fausse, on sort de la boucle

```
while
        echo "Chaine ? \c"
        read nom
        [ -z "$nom" ]
do
        echo "ERREUR : pas de saisie"
done
echo "Vous avez saisi : $nom"
```

4 Gestion des données SQL

4.1 Accèder à un serveur MySQL

service mysqld start ↵ = Lance MySQL

netstat -anp | grep ''LISTEN'' | grep « mysqld » ↵
tcp 0.0.0.0:3306 LISTEN mysqld = MySQL communique par défaut sur le port 3306

mysql -uroot -p -hlocalhost ↵ = Se connecte au serveur MySQL en tant que root (= « -u ») avec une demande de mot de passe (= « -p » = affiche un prompt pour entrer le password) sur la machine locale (= « -hlocalhost »).
Les utilisateurs mysql (user et password) sont différents des utilisateurs systèmes, même si ils sont ressemblants.

Enter password : = Mot de passe de la base de données
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 14
Server version: 5.0.45 Source distribution
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql>

4.2 Types de champ

Types	Description
INTEGER	Taille normale pour un entier. Valeur comprise entre –2 147 483 648 et 2 147 483 647 (signée) ou entre 0 et 4 294 967 295
FLOAT	Nombre à virgule
BOOLEAN	Stocké comme un caratère. Une valeur 0 = faux, c'est vrai si la valeur est différente de 0
DATE	Une date entre le 01/01/1000 et le 31/12/9999. Affichage par défaut = YYY-MM-DD
DATETIME	Combinaison d'une date et de l'heure, entre le 01/01/1000 0 heure et le 31/12/9999 à 23:59:59'
CHAR	Chaine de caractères de longueur fixe. Compris entre 0 et 255 caractères
VARCHAR	Chaine de caractère de maximum 65535 (après la version 5.0.3, 255 sinon)
BLOB	format binaire de 65535 octets maximum
TEXT	Texte de 65535 caractères maximum

4.3 Aperçu de la base de données

mysql> show databases ; ↵ = Affiche els bases de données disponibles dans le SGBDR
mysql> create database base_donnees ; ↵ = Crée la base de données
Query OK, 1 row affected (0.02 sec)
mysql> use base_donnees ; ↵
Database changed
mysql> CREATE TABLE famille (id INTEGER UNSIGNED NOT NULL AUTO_INCREMENT, nom_pere VARCHAR(100), nom_mere VARCHAR(100), PRIMARY KEY (id)) ; ↵ = Créé une table dans la base de données, avec 3 colonnes dont une colonne « id » qui sert de clé primaire et qui s'incrémente automatiquement.
Query OK, 0 rows affected (0.05 sec)
mysql> DROP famille ; ↵ = Supprime la table famille
mysql> INSERT into famille (nom_pere, nom_mere) VALUES (''Claveau'', ''Dufay'') ; ↵ = Insert des données dans la table
Query OK, 1 row affected, 0 warnings (0.02 sec)
Idem mysql> INSERT into famille set nom_pere = ''Dupont'', nom_mere = ''Durand'' ; ↵
mysql> SELECT id, nom_pere from famille ; ↵

```
+----+-------------+-------------+
| id | nom_pere    | nom_mere    |
+----+-------------+-------------+
|  1 | Claveau     | Dufay       |
|  2 | Dupont      | Durand      |
+----+-------------+-------------+
1 row in set (0.00 sec)
```

mysql> UPDATE famille set nom_mere = ''Chateau'' WHERE id = ''2'' ; ↵ = Met à jour des données déjà existante identifiées par le champ « id »

```
Query OK, 1 row affected (0.01 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

mysql> SELECT id, nom_pere from famille ; ↵

```
+----+------------+-------------+
| id   | nom_pere | nom_mere  |
+----+------------+-------------+
|  1   | Claveau    | Dufay       |
|  2   | Dupont     | Chateau   |
+----+------------+-------------+
1 row in set (0.00 sec)
```

mysql> DELETE from famille where id = ''2'' ; ↵ = Supprime la ligne dont « id » = 2.

```
Query OK, 1 row affected (0.03 sec)
```

mysql> select id, nom_pere from famille ;↵

```
+----+------------+-------------+
| id   | nom_pere | nom_mere  |
+----+------------+-------------+
|  1   | Claveau    | Dufay       |
+----+------------+-------------+
1 row in set (0.00 sec)
```

Si on ré-insère les mêmes valeurs dans une nouvelle ligne, elle est ajoutée par la suite avec une valeur « id » = 3. La valeur 2 pour « id » a été supprimée et le champ AUTO_INCREMENT ne ré-utilise jamais un n° supprimé dans la colonne.

mysql> ALTER TABLE famille ADD COLUMN ville VARCHAR(100) after nom_mere ; ↵ = Modifie la structure de la table après sa création. Ajoute une colonne « ville » en dernière position

4.4 Fonctions d'agrégations : GROUP BY et ORDER BY

mysql> SELECT count(*), ville from famille GROUP BY ville ; ↵ = Combien de ville différentes sont présentes dans la table. Calcul le nombre de ville pour le champ « ville » de la base « famille », et regroupe les villes identiques.

mysql> SELECT nom_pere, nom_mere ORDER BY nom_mere asc ; ↵ = Trie par le nom de la mère par ordre croissant (= « asc » = ascending). Trier par ordre décroissant = « desc » = descending

4.5 Recherche multi-tables : JOIN

mysql> CREATE TABLE animal (id INTEGER UNSIGNED NOT NULL AUTO_INCREMENT, family_id INTEGER UNSIGNED NOT NULL, type VARCHAR(45) NOT NULL, nom VARCHAR(45) NOT NULL, PRIMARY KEY (id)) ; ↵ = Crée une autre table « animal », avec 4 colonnes (id, family_id, type et nom) dont la colonne « id » qui sert de clé primaire et qui s'incrémente automatiquement.

```
Query OK, 0 rows affected (0.02 sec)
```

mysql> show tables; ↵ = Affiche toutes les tables

```
+------------------------+
| Tables_in_community |
+------------------------+
| famille                |
| animal                 |
+--------------------+
2 rows in set (0.00 sec)
```

mysql> describe animal; ↵ = Affiche l'architecture de la table « animal »

```
+-----------+--------------------+------+-----+---------+-------------------+
| Field      | Type                | Null | Key | Default | Extra              |
+-----------+--------------------+------+-----+---------+-------------------+
| id          | int(10) unsigned | NO   | PRI | NULL    | auto_increment |
| family_id | int(10) unsigned | NO   |      |          |                    |
| type       | varchar(45)        | NO   |      |          |                    |
| nom       | varchar(45)        | NO   |      |          |                    |
+-----------+--------------------+------+-----+---------+-------------------+
4 rows in set (0.02 sec)
```

mysql> insert into animal (family_id,type,name) VALUES ("1","chien","Max"); ↵ = Enregistre un chien pour la famille dont le champ « family_id » = 1

```
Query OK, 1 row affected (0.01 sec)
```
mysql> insert into animal (family_id,type,name) VALUES ("3","chat","Paws"); ↵ = Enregistre un chat pour la famille dont le champ « family_id » = 3
```
Query OK, 1 row affected (0.01 sec)
```

mysql> select a.id, a.nom_pere, a.nom_mere, b.type, b.nom from famille a, animal b where a.id = b.family_id; ↵ = On a créé un alias pour la table famille (= « a ») et animal (= « b ») en les déclarant derrière le FROM. Les 2 tables sont assiciés avec la valeur du champ « id » de la table famille et la valeur du champ 'family_id » de la table animal

```
+----+------------+-------------+-------------+-------------+
| id | nom_pere | nom_mere |   type      |   Nom       |
+----+------------+-------------+-------------+-------------+
|  1 | Claveau  | Dufay       |   chien     |   Max       |
|  3 | Dupont   | Chateau     |   chat      |   Paws      |
+----+------------+-------------+-------------+-------------+
2 row in set (0.02 sec)
```

mysql> DELETE from animal where type = ''chat'' ; ↵ = Supprime la ligne dont le type = chat => La famille Dupont n'a plus d'animal
```
Query OK, 1 row affected (0.03 sec)
```

mysql> select a.id, a.nom_pere, a.nom_mere, b.type, b.nom from famille a, animal b where a.id = b.family_id; ↵ = La famille Dupont n'apparait plus car il n'y a plus de correspondance entre la valeur du champ « id » et celle du champ « famyli_id »

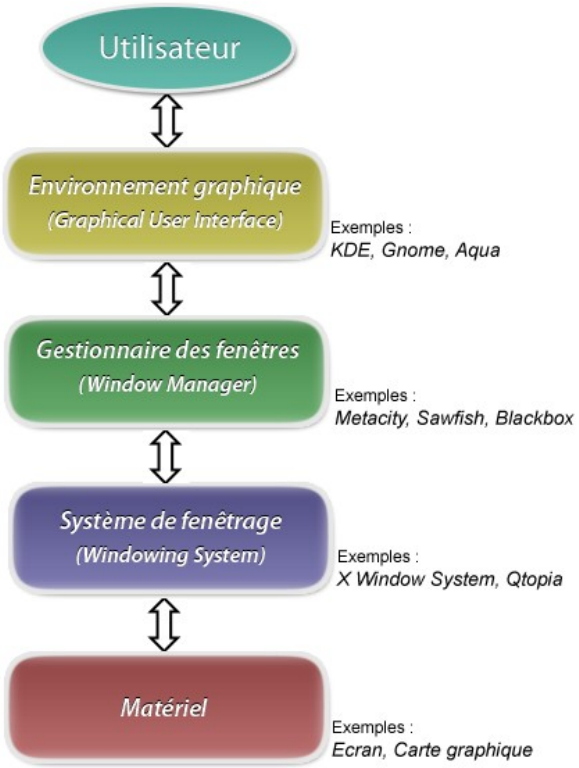
```
+----+------------+-------------+-------------+-------------+
| id | nom_pere | nom_mere |   type      |   Nom       |
+----+------------+-------------+-------------+-------------+
|  1 | Claveau  | Dufay       |   chien     |   Max       |
+----+------------+-------------+-------------+-------------+
2 row in set (0.02 sec)
```

mysql> select famille.id, famille.nom_pere, famille.nom_mere, animal.type, animal.nom from famille LEFT JOIN animal on famille.id = animal.family_id ↵ = Permet d'afficher toutes les familles, même celles qui n'ont pas d'animal.

```
+----+------------+-------------+-------------+-------------+
| id | nom_pere | nom_mere |   type      |   Nom       |
+----+------------+-------------+-------------+-------------+
|  1 | Claveau  | Dufay       |   chien     |   Max       |
|  3 | Dupont   | Chateau     |   NULL      |   NULL      |
+----+------------+-------------+-------------+-------------+
2 row in set (0.02 sec)
```

5 X Window = X11 = X

Informations tirées du site www.linuxcertif.com (http://www.linuxcertif.com/doc/X%20window), ainsi que du livre « LINUX Préparation à la certification LPIC-1 (LPI 101 LPI 102) [2e édition] « de Sébastien ROHAUT aux éditions ENI

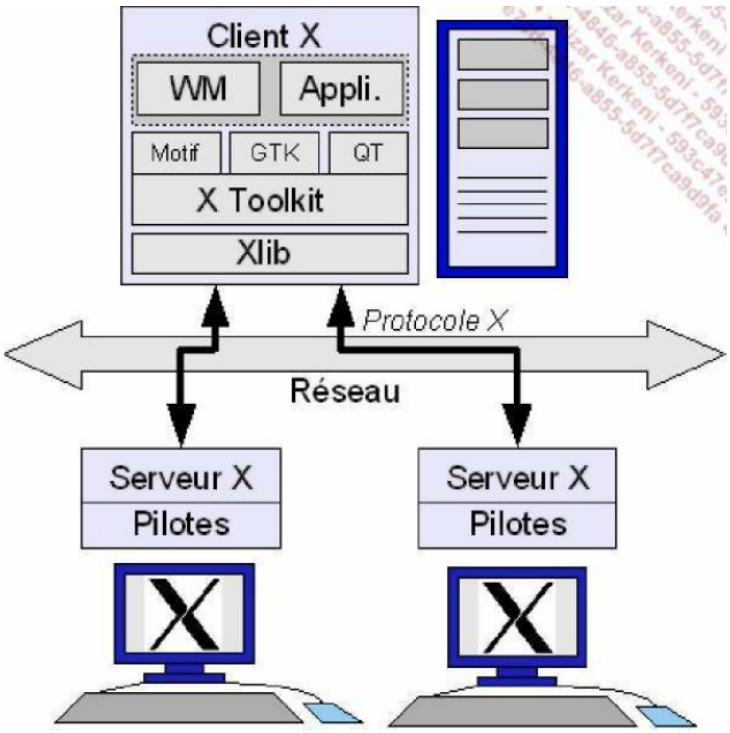


http://fr.wikipedia.org/wiki/Gestionnaire_de_fen%C3%AAtres
GNU Free Documentation License version 1.2

Le système graphique de base s'appelle « X Window System » ou plus couramment « X Window », « X11 » ou tout simplement « X ».
X est un système graphique complet chargé de dessiner et de gérer les événements des composants habituels d'un environnement graphique utilisateur GUI (Graphical User Interface) : fenêtres, boutons, menus, listes, ascenseurs, cases à cocher, curseur de souris, etc.
X peut gérer et afficher ces composants graphiques mais n'est pas chargé de les mettre en place. X ne gère que les interactions entre l'homme et la machine. Le serveur et le client X peuvent être localisés sur la même machine ou bien séparés à travers le réseau, de sorte que le calcul est traité séparément de l''affichage.

5.1 Modèle client/serveur

Le serveur X est souvent un composant logiciel sur un ordinateur disposant d'un clavier, d'une souris et d'un écran. Il reçoit et répond à des ordres d'affichage, ou issus du clavier et de la souris. Le client X se connecte au serveur et lui envoie des ordres d'affichage, des demandes de saisie au clavier ou l'état de la souris. Un client X est un programme qui est capable de dialoguer avec le serveur X.
Dans les faits un client X est un logiciel graphique. Pour pouvoir communiquer avec le serveur il utilise un composant appelé Xlib. Le client et le serveur ne sont pas toujours sur la même machine. Le serveur qui gère l'affichage peut être sur un ordinateur et le client (logiciel graphique) sur un autre. Les ordres, appelés requêtes, entre le client et le serveur passent par le réseau.
Ainsi vous pouvez lancer un programme sur le client qui est affiché sur le serveur. Pour l'utiliser vous devez aller sur le serveur et utiliser son écran, son clavier et sa souris.



Architecture X Window

« LINUX Préparation à la certification LPIC-1 (LPI 101 LPI 102) [2e édition] »
de Sébastien ROHAUT aux éditions ENI

5.2 Serveur X

Le serveur X est la partie permettant d'accéder au matériel d'affichage. Il fournit aux clients X la possibilité de s'afficher sur l'écran et de recevoir les informations sur les interactions de l'utilisateur (clavier, souris, etc).
Le logiciel serveur X tourne sur une machine qui est dotée d'un écran, d'un clavier et d'une souris, appelée terminal X.

Classiquement on retrouve les fichiers de configuration dans le repertoire /etc/X11, mais X est le seul système à posséder sa propre arborescence dans /usr : /usr/X11R6
Il existe deux serveur X largement répandu XFree86 et X.org, le second étant le fork du 1er réalisé en 2004 suite à un changement de licence de Xfree86 incompatible avec la GNU licence.

Le fichier de configuration le plus important du système X est le fichier de configuration du serveur qui se trouve dans /etc/xorg.conf ou xfree86.conf. Ce fichier reprend tout le détail de la configuration permettant au serveur d'utiliser le matériel (carte vidéo, écran, clavier, souris, etc) et les paramètres (font, modules optionels, etc). Le fichier xorg.conf est divisé en sections commençant par le mot clef « Section » et se finissant par « EndSection », par exemple pour mon clavier :

```
Section "InputDevice"
        Identifier      "Generic Keyboard"
        Driver          "kbd"
        Option          "CoreKeyboard"
        Option          "XkbRules"      "xorg"
        Option          "XkbModel"      "pc105"
        Option          "XkbLayout"     "fr"
        Option          "XkbVariant"    "latin9"
EndSection
```

Pour chaque chipset de carte graphique, le serveur X doit charger le module approprié qui permet de prendre en charge la carte graphique. Les modules sont généralement stockés dans /usr/lib/xorg/modules/drivers. Certains constructeurs fournissent des modules pour leur carte graphique.

5.3 Client X

un logiciel **client X** (logiciel graphique) se connecte au serveur X et lui envoie ses requêtes d'affichages en utilisant le *protocole X* au travers de la *bibliothèque X* (Xlib). Le client est simplement l'application

logicielle (jeu, traitement de texte, calculatrice, ...) qui utilise alors le *protocole X* pour déléguer au serveur X les taches d'IHM.
Pour se connecter à un serveur, le client X regarde l'adresse du serveur dans la variable d'environnement $DISPLAY.
system-config-display ↵ = Permet de configurer le serveur X (sous RedHat)
system-config-keyboard ↵ = Permet de configurer le clavier (sous RedHat)

5.4 Window Manager (WM) Gestionnaire de fenêtres

Parmi les logiciels du clients X, on en distingue généralement un en particulier : le gestionnaire de fenêtres dont le rôle est de gérer l'affichage, la sélection, le déplacement, le redimensionnement et les décorations des fenêtres (une fenêtre particulière étant la root-window c'est-à-dire fenêtre-racine).

Parmi les requêtes possibles, certaines indiquent de créer une fenêtre et de la décorer en dessinant les divers éléments de celle-ci : la barre de titre, le cadre, les divers boutons. Comme X ne fournit que le nécessaire de base, il dessine la fenêtre mais ce n'est pas lui qui détermine comment doivent être dessinés ces éléments. Un autre programme client X doit dire au serveur comment dessiner la fenêtre : c'est le gestionnaire de fenêtres ou Window Manager. Le serveur X affiche le résultat dessiné par ce gestionnaire : fenêtres, sélections, déplacements et décorations (styles, couleurs, etc.).
Cela veut aussi dire qu'il n'y a pas qu'un seul gestionnaire de fenêtres mais plusieurs. Certains sont très simples et basiques et se limitent au strict minimum, par exemple TWM. D'autres sont très complets et permettent de travailler dans des conditions très agréables car outre des fenêtres de base ils proposent des thèmes visuels agréables et personnalisables, des menus contextuels et même parfois des panneaux de configuration, comme par exemple WindowMaker.

6 Installer et configurer X11

6.1 Sélectionner et configurer un serveur X

6.1.1 Matériel vidéo supporté

Pour devancer les problèmes, il faut vérifier que le matériel vidéo est supporté
X -version ↵ = Permet d'afficher la version de X
X.org X Server 1.6.1.901 (1.6.2 RC1)
Release Date 2009-5-8
X Protocol Version 11, Revision 0

Il faut vérifier que le chipset de la carte vidéo est supporté par X.Org. La liste des chipsets supportés par X.Org peut être trouvé sur le wiki : http://www.x.org/wiki/

X.Org prend en charge la plupart des moniteurs. Si le votre n'est pas standard, il faut noter la fréquence de synchronisation horizontale (en KHz), la fréquence de rafraîchissement verticale (en Hz), et la résolution.

6.1.2 InstallerX.Org

Le fichier de configuration est : /etc/X11/xorg.conf
Il est créé et modifié durant l'installation du système.
Le serveur X utilise ce fichier pour savoir quels périphériques sont installés (clavier, souris, etc.)

6.1.3 Outils spécifiques de certains Linux

Certaines distributions fournissent leur propre outils de configuration.
system-config-display ↵ = Outils de configuration de RedHat

Depuis Fedora 10, le système n'utilise plus le fichier xorg.conf mais configure le système X à chaque boot. Pour configurer un élément manuellement, il faut d'abord créer le fichier xorg.conf.

Xorg -configure ↵ = Permet de créer le fichier xorg.conf sous Fedora.
X.Org X Server 1.6.1.901 (1.6.2 RC 1)
Release Date: 2009-5-8
X Protocol Version 11, Revision 0
Build Operating System: Linux 2.6.18-128.1.6.el5 i686
Current Operating System: Linux Suffolk 2.6.29.6-213.fc11.i686.PAE #1 \
SMP Tue Jul 7 20:59:29 EDT 2009 i686
Kernel command line: ro root=/dev/mapper/vg_suffolk-lv_root rhgb quiet
Build Date: 18 May 2009 02:47:59PM
Build ID: xorg-x11-server 1.6.1.901-1.fc11
Before reporting problems, check http://wiki.x.org to make sure that you have the latest version.

Markers: (--) probed, (**) from config file, (==) default setting, (++) from command line, (!!) notice, (II) informational,
(WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/var/log/Xorg.1.log", Time: Wed Aug 12 06:32:31 2009
List of video drivers:
glint
nv
vmware
.....
fbdev
vesa
(++) Using config file: "/root/xorg.conf.new"
Xorg detected your mouse at device /dev/input/mice.
Please check your config if the mouse is still not operational, as by default Xorg tries to autodetect the protocol.
Your xorg.conf file is /root/xorg.conf.new
To test the server, run 'X -config /root/xorg.conf.new'

cp /root/xorg.conf.new /etc/X11/xorg.conf ↵ = Copie le fichier sous /etc/X11 une fois modifié

6.1.4 Les sections du fichier xorg.conf

- Files = Chemin par défaut des polices et de la base de données RGB.
  Pour La base de données RGB, c'est une table d'équivalence entre la valeur RGB d'une couleur et son nom (une centaine de correspondances sont définies) :
  255 228 196 bisque
  255 218 185 peach puff
  255 218 185 PeachPuff
- ServerFlags : Permet la personnalisation du serveur X comme les raccourcis clavier
- InputDevice : Utilisé autant de fois qu'il y a de périphérique, mais au moins 2 fois = clavier et souris
- Monitor : Utilisées pour chacun des écrans utilisés, et de la liste des différents modes graphiques qu'ils peuvent prendre
- Device : Définis les différentes carte vidéo installées
- Screen : Relie un périphérique avec l'écran correspondant de la section « Monitor ». Elle comporte des paramètres de configuration supplémentaires.
- ServerLayout : Relie un périphérique avec un ou plusieurs élément de la section « InputDevice »

6.2 Exporter l'affichage X

Un logiciel graphique (client X) tourne sur une machine distante et est affiché sur une station de bureau ou portable (serveur X). le protocole X Window utilise généralement TCP/IP. La station (serveur X) voulant profiter de l'affichage à distance ouvre un port (en général 6000), et le client X peut s'y connecter. Le protocole n'étant pas sûr (sans chiffrage), il est exceptionnel d'ouvrir un serveur directement sur TCP, en général, la connexion se fait via openSSH qui peut transmettre le protocole X dans un tunnel chiffré.
Le serveur X permet une gestion minimaliste de la sécurité via xhost, la commande xhost permet de restreindre l'accès au serveur graphique à certains hôtes sur le réseau et/ou à certains utilisateur. D'autres mécanisme que xhost doivent en général être utilisé pour assurer un niveau de sécurité suffisant.

1. Client X :# export display=10.2.3.4:0.0 ↵ = Exporte l'affichage sur la machine 10.2.3.4, dont le serveur d'affichage X = 0 et l'écran = 0 (1er écran donc)
2. Serveur X : # xhost + ↵ = Autorise tous les clients à exporter en X
   # xhost + @IP_clientX ↵ = Autorise le client à exporter en X

ssh -X @IP_clientX ↵ = Se connecte au client X (serveur) en SSH en lançant l'export de l'affichage
xclock ↵ = S'affiche sur le serveur X (portable par exemple)

Automatiser l'export de l'affichage :
Dans le fichier /etc/ssh/sshd_config (serveur SSH)
X11forwarding yes
Dans le fichier /etc/ssh/ssh_config (client SSH)
forwardingX11 yes : Les clients X11 distants ont un accès total

6.3 Polices de caractère X

Linux est livré avec une collection de polices de caractères, couvrant la plupart des besoins. Il est possible également d'en ajouter (libres ou commerciales). X.Org rend disponible des polices qu'il trouve dans les

chemins des polices des programmes client, mais il est possile de déclarer son propre chemin via la directive « FontPath ''chemin'' » du fichier xorg.conf :

```
Section "Files"
FontPath "/usr/share/X11/fonts/cyrillic"
FontPath "/usr/share/X11/fonts/Type1"
FontPath "/usr/share/X11/fonts/75dpi"
EndSection
```

La déclaration de ces polices créé un répertoire police sous /usr/share/X11/fonts. Lorsque X démarre, il liste l'ensemble de ces répertoires et inclus les polices qui s'y trouvent.

6.3.1 Installer de nouvelles polices de caractères

1. Créez le répertoire qui accueillera la nouvelle police. Sous /usr/share/X11/fonts/local ou bien /usr/local/fonts. Séparer les polices standard des polices personnelles permet de garder ces dernières en cas de mise à jour
2. # mkfontdir chemin ↵ = Permet d'ajouter le chemin des nouvelles polices à la recherche de X
3. Relancez le serveur X afin que ces nouvelles polices soient prises en compte

6.3.2 Serveur de polices X

Les polices sont en générales gérées sur la machine local. Il est tout de même possible d'accéder à des polices sur le serveur X à distance via XFS (X Font Server), et ainsi réduire le travail sur chacune des machines locales.
Le serveur de police X est un démon qui envoie les polices aux clients locaux et réseaux.
Pour inclure XFS dans les chemin de polices du système, il faut ajouter une directive FontPath :

```
Section "Files"
      RgbPath     "/usr/share/X11/fonts/rgb"
      FontPath   "unix/:-1"
EndSection
```

Le chemin de configuration de XFS est : /etc/X11/fs/config
Pour utiliser XFS, il faut qu'il se lance au démarrage de la machine.

6.4 Contrôler des applications X avec .Xresources

Les applications sont programmées pour utiliser des paramètres dans des fichiers de configurations externes, propre à l'application. Plutôt que d'avoir un outils de configuration pour chaque application, elles peuvent être développées pour regarder le contenu d'1 seul fichier situé sous le home directory.
C'est le fichier « ~/.Xresources » qui contient 1 ligne pour chaque ressource configurée :
`application*ressource: valeur` = Permet de configurer la valeur de la ressource pour l'application

```
xterm*background: Black  = Permet de configurer les couleurs de l'application xterm
xterm*foreground: Wheat
xterm*cursorColor: Orchid
xterm*reverseVideo: false
```

7 Mettre en place un « display manager »

Le « display manager » est l'outils qui gère les session X (sur la machine local ou à travers le réseau). Le travail principal est d'authentifier l'utilisateur à travers une interface graphique plutôt qu'en mode texte.
Les 3 principaux « display manager » sous Linux sont : xdm, kdm et gdm
Le « display manager » utilisé par défaut est définit dans /etc/X11/default-display-manager

7.1 Configurer xdm

xdm est distribué à part de X.Org. Il est configuré grâce à différents fichiers situés sous /etc/X11/xmd :

- Xaccess = Contrôle les demandes qui viennent d'hôtes distants.
- Xservers = Associe les noms d'affichage X (: 0, 1, ...) avec le logiciel serveur X local, ou un affichage distant, comme un terminal X.
- Xsession = Contient le script qui lance xdm après une connexion réussie. Il recherche généralement un répertoire « .Xsession » dans le home directory et exécute les commandes qui s'y trouvent. Si un tel fichier n'existe pas, Xsession lance un gestionnaire de fenêtre par défaut (ou environnement) ainsi que les applications.
- Xsetup_0 = Script lancé avant l'écran graphique de login. Il inclus souvent des commandes pour configurer la couleur, l'affichage ou pour lancer d'autres programmes. Ce script est exécuter sous « root »
- sdm-config = Associe les ressources configurées pour xdm avec les autres fichiers de sa liste. Il

n'est pas nécessaire en général de modifier ce fichier.
- Xreset = Scripts lancés lors de la déconnexion
- Xresources = Traité plus bas

7.1.1 Personnalisation simple de xdm

Similaire à. Xresources. Il détient des informations de configuration pour certaines ressources xdm, y compris l'écran de connexion graphique.
Il est possible de personnaliser l'apparence de xdm (= la fenêtre de login), en modifiant le fichier /etc/X11/xdm/Xresources :
! Xresources file = Les lignes en commentaires dans ce fichier commencent par « ! »
xlogin*borderWidth: 10 = Le bord a une épaisseur de 10
xlogin*greeting: Bienvenue sur cette distrib CentOS = Message de bienvenue
xlogin*namePrompt: Login:\040
xlogin*fail: Mauvais login - Recommence encore = Message en cas de mauvais login ou mot de passe
xlogin*failColor: red = Couleur du message en cas d'erreur de login

Pour passer outre la configuration du serveur X du fichier /etc/X11/xorg.conf, il faut inscrire la nouvelle configuration dans le fichier /etc/X11/xdm/Xserver :
Xservers file
:0 local /usr/X11R6/bin/X -bpp 24 = Modifie la profondeur de couleur (= « bpp » = bit per pixel) à 24

Pour ajouter des programmes ou paramètres à la fenêtre de login, il faut les ajouter au fichier /etc/X11/xdm/Xsetup_0 :
#!/bin/sh
Xsetup_0
/usr/X11R6/bin/xsetroot -solid "#356390" = La couleur du fond est fixé avec une valeur héxadécimale.
A noter que la sortie de la commande « xsetroot » se fait dès que la couleur est fixée et Xsetup_0 peut donc continuer la prochaine commande
/usr/X11R6/bin/xclock -digital -update 1 -geometry -5-5 & = Ajoute une horloge dans le coin inférieur droit.
A noter que contrairement à « xsetroot », la commande « xclock » doit être mis en tâche de fond grâce à « & ». Sinon le script Xsetup_0 à toujours la main et la fenêtre de login n'apparaît pas

7.1.2 Lancer xdm manuellement

xdm utilise le serveur X pour se lancer sur la machine local. Il faut donc une configuration X qui fonctionne avant de lancer xdm.
xdm ↵ = Lance xdm
xdm lance le serveur X et affiche la fenêtre de login. Après la déconnexion, xdm se ré-initialise et affiche de nouveau la fenêtre de login.
La plus part des distributions lance xdm lors du boot.

Console virtuelles :
La plupart des distributions Linux utilisent les consoles virtuelles. Vous pouvez basculer entre elles en utilisant les combinaisons de touches Ctrl-Alt-F1, Ctrl-Alt-F2, etc. (La touche Ctrl est nécessaire uniquement lors du passage d'une console X à un texte ou une console X d'autres.) Généralement, les six premières consoles sont en mode texte, et X est lancé sur la console 7 (Ctrl-Alt-F7). Cela signifie que, comme avec startx, votre console en mode texte originale reste inchangé après avoir démarrer manuellement xdm. Par conséquent, vous devez vous déconnecter de votre console en mode texte si vous prévoyez de quitter le système.

7.1.3 Lancer xdm automatiquement

Le niveau 5 est celui qui est utilisé en général pour se loguer avec xdm en mode graphique (pour les distributions utilisant l'initialisation de type Système V), configuré dans le du fichier /etc/inittab :
Lance xdm au niveau 5
x:5:respawn:/usr/X11R6/bin/xdm -nodaemon

Pour les distributions n'utilisant pas les niveaux de démarrage, il est possible de lancer xdm en le plaçant à la fin d'un script d'initialisation, comme rc.local par exemple.

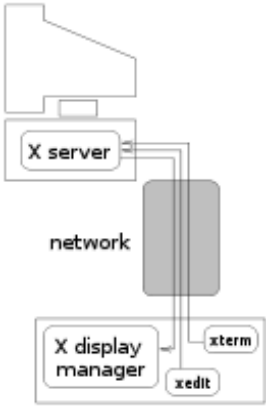
7.2 Terminaux X

On appel « terminal X » un type de périphérique d'affichage très peu onéreux et qui est utilisé en général sans disque.

Ils implémentent simplement un serveur X

Ce périphérique va cherche à se connecter à une machine distante pour trouver un démon xdm.

L'hôte distante trouvé lancera une session X à travers le réseau avec comme « cible d'affichage » le terminal X



7.2.1 xdm pour les terminaux X

Pour utiliser un terminal X avec votre hôte distant, il faut que xdm soit lancé sur l'hôte distant. L'hôte écoute les connexions entrantes depuis des terminaux X en utilisant XDMCP, le XDM Control Protocol (port par défaut = 177). Quand une requête est reçue, xdm répond avec la même fenêtre de login qui serait affiché sur la machine local.

/etc/X11/xdm/Xaccess = Fichier de configuration qui gère l'accès à votre système xdm en listant les machine autorisées.
*.example.com = Le « * »est autorisé pour définir tout un groupe.
!xterm1.anotherexample.com = Pour empêcher un hôte de s'y connecter il suffit de précéder son nom par « ! ».

7.3 Configurer KDM

Le développement de XDM et KDM est séparé.

KDM (acronyme de K Desktop Environnement, mais pourquoi le « K » ?) est le « display manager » pour l'environnement de bureau KDE.

Il est distribué par KDE.org et est configuré par des fichiers placés sous /etc/X11/kdm

yum install kdm ↵ = Installe l'interface KDM, en incluant le « KDE display manager »
/etc/kde/kdm/kdmrc = Fichier de configuration

7.4 Configurer GDM

GDM est le « display manager » pour l'environnement de bureau Gnome (acronyme de GNU Network Object Model Environment).

Gnome est l'environnement graphique par défaut pour Fédora et Ubuntu.

Le « GDM display manager » est chargé automatiquement lors de l'installation graphique de l'un de ces 2 OS.

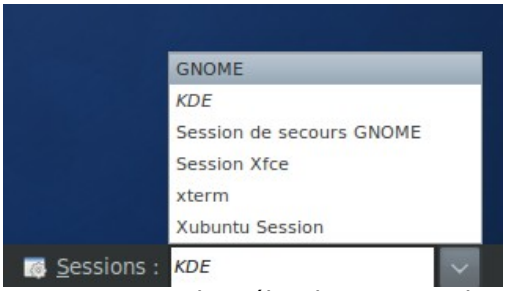
yum groupinstall "GNOME Desktop Environment" ↵ = Installe l'ensemble des éléments de l'environnement Gnome

/etc/gdm/gdm.conf ou /etc/gdm/custom.conf = Fichier de configuratiion de GDM, suivant la distribution. Il est largement commenté

```
# For full reference documentation see the GNOME help browser under
# GNOME|System category.  You can also find the docs in HTML form on
http://www.gnome.org/projects/gdm/
# NOTE: Some values are commented out, but show their default values.  Lines that begin with "#" are
considered
# comments. Have fun!

[daemon]
# Automatic login, if true the first local screen will automatically logged in as user as set with
AutomaticLogin key.
AutomaticLoginEnable=false
AutomaticLogin=

# Timed login, useful for kiosks.  Log in a certain user after a certain amount of time.
TimedLoginEnable=false
TimedLogin=
TimedLoginDelay=30

# The GDM configuration program that is run from the login screen, you should probably leave this alone.
#Configurator=/usr/sbin/gdmsetup --disable-sound --disable-crash-dialog

# The chooser program.  Must output the chosen host on stdout, probably youshould leave this alone.
#Chooser=/usr/lib/gdm/gdmchooser

# The greeter for local (non-xdmcp) logins.  Change gdmlogin to gdmgreeter to get the new graphical
greeter.
Greeter=/usr/lib/gdm/gdmgreeter

# The greeter for xdmcp logins, usually you want a less graphically intensive greeter here so it's better to
leave this with
# gdmlogin
#RemoteGreeter=/usr/lib/gdm/gdmlogin
```

7.5 Changer de bureau

Il est possible de faire tourner des environnement graphiques différents. Si KDE et Gnome sont installés, vous pouvez choisir lequel lancer en sélectionnant votre choix dans la fenêtre de login :



/etc/sysconfig/desktop = Fichier permettant de sélectionner quel environnement doit être utilisé au démarrage

```
desktop= "kde"
displaymanager= "kdm"
```

switchdesk kde ↵ = L'outils « switchdesk » permet aux users de changer environnement graphique parmi ceux installés sur le système. Il ne supporte que Gnome ou KDE

8 Accessibilité

Afin de palier à certains handicap, la plupart des distribution ont mis en place des outils d'aide ou d'assistance :

- Lecteurs d'écran : Logiciel qui « lit » les éléments textes ou graphiques de l'écran.
  Emacspeak, Junniper Speech System, Speakup ou Orca
- Loupe : Agrandi la partie de l'écran que l'utilisateur sélectionne.
  SVGATextmode, Wzoom, Orca

- Utilisation de périphérique en braille.
  BrLTTY ou BLINUX = Blind + Linux

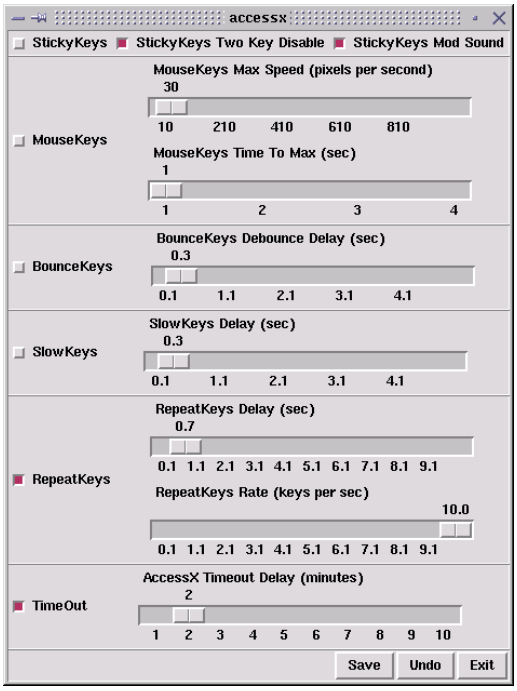
- AccessX : Configuration de l'ensemble des paramètres du clavier et de la souris, via une interface graphique. Cet outils est intégré dans les distributions.
  StickyKeys contrôle les touches Ctrl et Alt

  MouseKeys = permet d'associer des séquences de touches au claviers pour remplacer le mouvement ou les boutons de la souris

  BounceKeys ou DelayKeys = Fixe le délai entre 2 touches au clavier

  SlowKeys : Définie le temps de la frappe d'une touche au clavier = le temps où la touche doit être maintenue

  RepeatKeys = Permet de définir le temps nécessaire à la réalisation d'une séquence de touche

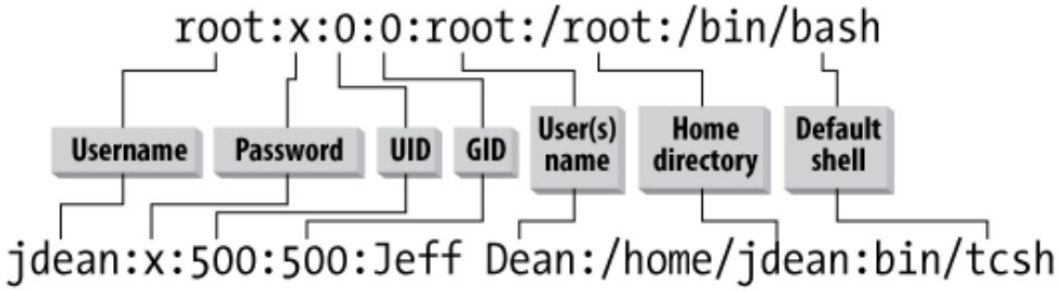


- Clavier graphique : Permet à l'utilisateur de pointer les touches du clavier sur une interface graphique à l'écran.
  Gtkeyboard ou GOK (Gnome Onscreen Keyboard)

9 Gestion des utilisateurs et des groupes

9.1 Les comptes utilisateurs et le fichier de mot de passe

/etc/passwd = Fichier où sont stockés tous les comptes des users. Ce fichier est en lecture pour tous.
vipw ↵ = Permet d'utiliser un éditeur qui modifie /etc/passwd en toute sécurité
Idem # vigr ↵ = Permet d'utiliser un éditeur qui modifie /etc/group en toute sécurité
Il y a une ligne pour chaque compte :



Username = Nom unique de la personne ou du service utilisant le compte
Password = Les mots de passe ne sont plus stockés (cryptés) dans le fichier passwd (en lecture pour tous), mais dans un fichier séparé : /etc/shadow (en lecture pour root seulement), d'où le « x » à l'endroit de cette colonne. Ce fichier a des droits stricts

Les utilisateurs sont identifiés par leur User ID (= UID) et GID, et non pas par le nom du compte.. Chaque UID est unique, il s'agit d'un entier compris entre 0 et 65535.
L'UID = 0 est réservé à root. Le nom importe peut, c'est l'UID = 0 qui est super-utilistateur

UID = 0	0 > UID < 100	100 > UID < 500	UID > 500
root	comtes administratifs	utilisateurs système réguliers	nouveaux utilisateurs

GID = Groupe ID = Chaque nom de compte a un groupe ID par défaut. L'association « nom des groupes » et leur GID est décrite dans le fichier /etc/group. Un utilisateur peut donc avoir plusieurs groupes
Full name ou « comment » = Stocké au format texte, il peut contenir des espaces
Home directory = Répertoire par défaut de l'utilisateur

Default shell = Shell par défaut de l'utilisateur, utilisé dès que le user ouvre une session ou bien une fenêtre shell. En général = /bin/bash, mais peut être aussi un programme. Si le shell = /bin/false cela sécurise le compte le rendant incapable de se loguer (pour un compte système par exemple)

Chercher de fichiers avec l'UID du user ou sans user :
find / -user 501 ↵ Recherche les fichiers et dossiers d'un utilisateur supprimé ayant l'ID 501
find / -nouser ↵ = Recherche les fichiers et dossiers qui n'ont pas de user identifié
Idem pour les groupes non identifiés # find / -nogroup ↵
find / -user 501 -ok chown root {}\ ; ↵ = Rend root propriétaire des fichiers appartenant au user 501

9.2 Les groupes et le fichier /etc/group

/etc/group = Contient différents champs séparés par « : », comme pour /etc/passwd
Group name = Nom unique du groupe
Group passwd = Il n'y a que les user qui ont un mot de passe, mais le groupe peut avoir un mot de passe pour leurs membres. Si le champ est vide, le mot de passe du groupe n'est pas requis
Group ID = GID = ID unique du groupe
Group member list = Liste des user membres du groupe, séparés par « , »

root:x:0:root = Comme pour l'UID, le GID de root = 0
info:x:230:david,guillaume = David et Guillaume sont membres du groupe « info »
finance:x:300: david,guillaume,laurent = David, Guillaume et Laurent sont mémbres du groupe « finance »
david:x:500: = Comme pour l'UID, le GID des nouveaux comptes > 500
guillaume:x:501: = groupe personnel de Guillaume
laurent:x:502

vigr ↵ = Permet d'utiliser un éditeur qui modifie /etc/group en toute sécurité
Idem # vipw ↵ = Pour éditer /etc/passwd

9.3 Le fichier des mots de passe et celui des groupes

Complété dans le chapitre « Sécurité / Mot de passe caché »

9.3.1 Fichier /etc/shadow

Les mots de passe sont cryptés et ont été sortis du fichier /etc/passwd, qui lui était lisible pour tous. Les mots de passe sont maintenant dans le fichier /etc/passwd :

root david	:1oxEaSzzdXZESTGTU :1IviLopPn461z47J	: 10927:0:99999:7:-1:-1:134538444:10927:0:99999:7::11688:134538412
nom du compte	« : » puis le mot de passe crypté Les 1ers caractères indique le type de codage utilisé. Par exemple $1... = MD5	« : » puis d'autres informations en options, comme sur le vieillissement du mot de passe

9.3.2 Mots de passe de groupe

Les groupes aussi peuvent être protégés par un mot de passe. Ceci permet de donner l'accès d'un groupe à un user qui n'est pas membre de ce groupe.

newgrp info ↵ = Change le groupe par défaut du user par le groupe « info ». Le mot de passe du groupe « info » est demandé si ce groupe en possède un.
newgroup - finance ↵ = Ré-initialise les variable d'environnement avec celles du groupe (= « - »)

Comme pour les mots de passe des users (qui ont été sortis du fichier/etc/apsswd), les mots de passe des groupes sont stockés cryptés dans le fichier /etc/gschadow (en lecture pour root seulement).

root:::root
info:!:: = Le groupe « info » n'a pas de mot de passe, un « ! » est placé dans le champ « mot de passe »
finance:0cf7ipLtpSBGg:: = Le groupe « finance » est doté d'un mot de passe
david:!::

9.4 Commandes de gestion des utilisateurs et des groupes

# useradd ↵	# groupadd ↵	Ajoute un utilisateur ou un groupe
# usermod ↵	# groupmod ↵	Modifie un utilisateur ou un groupe

# userdel ↵	# groupdel ↵	Supprime un utilisateur ou un groupe

9.4.1 usermod

Cette commande est traitée dans le chapitre « Sécurité / Les UID et les mots de passe / usermod »

9.4.2 useradd

/ert/default/useradd = Fichier de configuration par défaut

useradd -g clientftp -d /var/clientftp/dupont -s /sbin/nologin dupont ↵
= Crée un user dupont, membre du groupe « clientftp », dont le répertoire de travail est /var/vlientftp/dupont
useradd -m -c ''Société LSF'' david ↵ = Crée un nouvel user « david », son répertoire de travail est créé (= « -m ») et auquel on associe un commentaire (= « -c »)
Avec l'option « -m » le répertoire personnel du nouvel utilisateur est peuplé avec le contenu du répertoire /etc/skel

# id david ↵ = Affiche l'UID du user david
uid=1000(david) gid=1000(david) = Le user de david = 1000
# useradd -o -u 1000 laurent ↵ = Crée un autre utilisateur laurent qui a le même UID (= « -o ») que david (UID=1000)
# id laurent ↵ = Affiche l'UID du user laurent
uid=1000(laurent) gid=1002(laurent) groupes=1000(david) = Le user laurent a le même UID que david

9.4.3 userdel

userdel -r utilisateur ↵ = Supprime l'utilisateur et son répertoire de travail (= « -r ») + spool mail + crontab, mais pas ses fichier sur /tmp

9.4.4 groupadd

groupadd nouveau_groupe ↵ = Ajoute le nouveau groupe au système

9.4.5 groupmod

groupmod -n nouveau_nom groupe ↵ = Modifie le nom du groupe
groupmod -g 512 -p mot_de_passe groupe ↵ = Modifie le GID (= « -g ») du groupe, ainsi que son mot de passe (= « -p »)
groupmod -g 512 -o groupe2 ↵ = Permet au groupe2 d'avoir un GID non unique (= 512), partagé avec « groupe2 »

9.4.6 groupdel

groupdel groupe2 ↵ = Supprime le groupe2

9.4.7 passwd

passwd david ↵ = Définit le mot de passe du user « david » d'une façon interactive. Le mot de passe ne peut être définit en ligne de commande
passwd -l david ↵ = Vérouille le mot de passe pour le user « david ». Change la valeur du mot de passe en une valeur qui ne correspond pas à une valeur chiffrée (il ajoute un « ! » Au début du mot de passe)
passwd -u david ↵ = Déverrouille le mot de passe de david. Cette option réactive un mot de passe en remettant le mot de passe à sa valeur précédente (sans le « ! » devant).
passwd -S -a ↵ = Affiche l'état (= « -S ») de tous les comtes (= « -a » = all). Cet état est décrit en 7 champs :

- nom du compte,
- si le mot de passe est bloqué (LK), n'a pas de mot de passe (NP) ou a un mot de passe utilisable (PS).
- la date de dernière modification du mot de passe
- la durée (en jour) minimum avant modification
- la durée maximum de validité
- la durée d'avertissement
- la durée d'inactivité autorisée pour le mot de passe

passwd -i 12 david ↵ = Désactiver le compte de david pendant 12 jours après que son mot de passe soit arrivé en fin de validité
passwd -d david ↵ = Supprime le mot de passe (le rend vide) de « david ». C'est une façon rapide de supprimer l'authentification par mot de passe pour un compte

Valeurs de retour de la commande passwd :

0 = succès
1 = permission refusée
2 = combinaison d'options non valable
3 = échec inattendu, rien na été fait
4 = échec inattendu, le fichier passwd est manquant
5 = fichier passwd en cours d'utilisation, veuillez réessayer plus tard
6 = paramètre non valable pour l'option

9.4.8 gpasswd

gpasswd groupe ↵ = Définit le mot de passe du groupe d'une façon interactive. Le mot de passe ne peut être définit en ligne de commande

9.4.9 Autres commandes

getent group nom_groupe ↵ = Recherche où est déclaré le groupe (option « group ») appelé nom_groupe
chfn user ↵ = Modifie les informations « finger » du user en mode interactif
id user ↵ = Liste UID, le GID et les groupes auxquels le user appartient
Idem # getent passwd user
user:x:1000:1000:Dupont,,,:/home/user:/bin/bash
groups user ↵ = Liste les groupes du user

10 Automatiser les tâches système en planifiant des jobs

10.1 Dates d'un fichier

atime = Date du dernier accès du fichier
mtime = Date de la dernière modification du fichier (contenu)
ctime = Date du dernier changement du fichier (droits, propriétaire, etc)

10.2 Utiliser cron

10.2.1 Programme et programme pour cron

Composé de :

- crond = Démon de cron. Il est lancé au démarrage du système
- crontab = Fichier de configuration. Il y a la crontab du système + celle tous les utilisateurs. Ce fichier est stocké sous /var/spool/cron

10.2.2 crontab

crontab -e ↵ = Edite la crontab de l'utilisateur mais pas celle du système
crontab -l ↵ = Affiche le contenu de la crontab de l'utilisateur
crontab -r ↵ = Supprime tout le contenu de la crontab de l'utilisateur
crontab -u david ↵ = Permet d'utiliser la crontab de « david » plutôt que la sienne

Format du fichier crontab :

30	16	*	*	*	mail -s « objet » mail
minute	heure	jour du mois = Tous les jours	mois = Tous les mois	jour de la semaine = Tous les jours	commande

30 16 * * 1-5 ... = Avec un « - » = tous les jours ouvrés, à 16:30
30 16 * * mon,wen ... = Avec une « , » = seulement le lundi (= « mon » = monday) et le mercredi (« wen » = wendsay)

Dans la commande, le « % » est remplacé par un ↵. On peut aussi appeler un script en .sh
Le « # » permet de commenter les lignes
crond évalue les lignes de la crontab toutes les minutes.

Exemple :
30 23 * * * df >>/tmp/log_df.txt = Tous les jours à 23h30
5 * * * * df >>/tmp/log_df.txt = Toutes les heures, passées de 5 minutes
30 23 1 * * df >>/tmp/log_df.txt = Tous les premiers du mois à 23h30
28 22 * * 1 df >>/tmp/log_df.txt = Tous les lundis à 22h28
22 11 13 * 5 df >>/tmp/log_df.txt = Tous les vendredis 13 de n'importe quel mois à 11h22

12 10 2-5 * * df >>/tmp/log_df.txt = Du 2 au 5 de chaque mois à 10h12
59 23 */2 * * df >>/tmp/log_df.txt = Tous les jours pairs du mois à 23h59
0 22 * * 1-5 df >>/tmp/log_df.txt = Tous les jours ouvrés à 22h
*/5 * * * * df >>/tmp/log_df.txt = Toutes les 5 minutes

10.2.3 crontab du système

vi /etc/crontab ↵ = Edite la crontab du système
Le champ « user » est ajouté par rapport à la crontab des utilisateurs :

30	16	*	*	*	**root**	mail -s « objet » mail
minute	heure	jour du mois	mois	jour de la semaine	**user**	commande

Dans la plupart des distributions, le répertoire /etc/crontab contient des crontab standard pour exécuter des programmes toutes les minutes, heures, jours, semaines et mois : /etc/cron.daily par exemple

10.3 Utiliser at

Les requêtes at sont stockées sous /var/spool/at/
at 6:15pm tomorrow = Exécute la commande à 18h15 demain
at> commande ↵
at> Ctrl+d
at now +2 days < commande ↵ = Exécute la commande dans 2 jours (à partir de maintenant)
Idem # at now +2 days -f commande ↵
atq ↵ = Liste les requêtes at. root peut voir alors toutes les requêtes de tous les users
Idem # at -l ↵
atrm 1 ↵ = Supprime la 1ère requête affichée dans la liste par atq
Idem # at -d 1 ↵
at -f liste_commandes 9pm + 2 days ↵ = Lance les programmes du fichier « liste_commandes » à 21:00 dans 2 jours

10.4 Contrôler l'accès à « cron » et « at »

Les fichiers suivants permettent d'autoriser ou d'empêcher les utilisateurs :

- cron.allow = Autorise les utilisateurs listés d'utiliser cron
- at.allow = Autorise les utilisateurs listés d'utiliser at
- cron.deny = Empêche les utilisateurs listés d'utiliser cron
- at.deny = Empêche les utilisateurs listés d'utiliser at

Si aucun fichier n'existe pour cron, l'utilisation de la commande ne sera pas limitée.
L'existence du fichier cron.allow seulement a le même effet que de créer un fichier cron.deny avec « ALL »
Si at.allow n'existe pas, le système vérifie les noms dans at.deny

11 Localisation et internationalisation

L'internationalisation est l'adaptation des logiciels aux langues et différences régionales = « i18n »
La localisation permet d'ajouter des comportements locaux spécifiques = « L10n »

11.1 Configurer le fuseau horaire

Le fuseau horaire est défini par un lien symbolique depuis /etc/localtime vers un fichier sous le répertoire /usr/share/zoneinfo/x, où « x » correspond à votre fuseau horaire

ln -s /etc/localtime /usr/share/zoneinfo/UTC ↵ = Configure le système en horaire UTC (universal)
ls -l /etc/localtime ↵
lrwxrwxrwx 1 root root 30 Sep 12 13:56 /etc/localtime -> /usr/share/zoneinfo/US/Central = Si vous habitez au milieu des USA

tzselect ↵ = Configure le fuseau horaire à la place de créer le lien symbolique
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean

```
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#?
```

date -u ↵ = Affiche l'heure en UTC
date +%Z ↵ = Affiche l'abréviation du fuseau horaire
CET

11.2 Variables d'environnement stockant les paramètres locaux

LANG = Défini toutes les paramètres locaux en 1 fois, tout en permettant une personnalisation individuelle plus poussée via les paramètres LC_ *
LC_COLLATE = Ordre alphabétique des chaîne de caractères.
LC_CTYPE = Classification des caractères = Détermine quels caractères sont considérés comme alphabétiques, numériques, etc. Cela détermine également le jeu de caractères utilisé
LC_MESSAGES = Langage des messages
LC_MONETARY = Unité monétaire et le format des valeurs numériques
LC_TIME = Format des dates et de l'heure
LC_PAPER = Taille du papier par défaut
LC_ALL = Variable spéciale qui écrase toutes les autres

locale ↵ = Affiche la valeur de toutes les variables

```
LANG=
LC_CTYPE="POSIX"
LC_NUMERIC="POSIX"
LC_TIME="POSIX"
LC_COLLATE="POSIX"
LC_MONETARY="POSIX"
LC_MESSAGES="POSIX"
LC_PAPER="POSIX"
LC_NAME="POSIX"
LC_ADDRESS="POSIX"
LC_TELEPHONE="POSIX"
LC_MEASUREMENT="POSIX"
LC_IDENTIFICATION="POSIX"
LC_ALL=
```

iconv -f IS6937 -t IS8859 fichier_in.txt > fichier_out.txt ↵ = Converti le contenu du fichier_in.txt vers fichier_out.txt en convertissant le jeu de caractères ISO/IEC 6937:1994 vers le jeu de caractères ISO/IEC 8859-1:1998

12 Maintenir l'heure système

L'heure du système est stockée sous la forme d'un nombre de secondes passé depuis le 01/01/1970
Il existe deux horloges :

- L'horloge système : est l'horloge de référence pour toutes les opérations effectuées dans le système . Cette horloge est maintenue par le noyau grâce à un compteur qui est incrémenté régulièrement, sur la base d'une interruption matérielle (18,6 fois par seconde = 1/20 de seconde).
- L'horloge matérielle est l'horloge qui maintient l'heure de votre ordinateur pendant qu'il est éteint = horloge BIOS, horloge CMOS, ou encore RTC (Real Time Clock).

12.1 NTP

NTP utilise le port 123 par défaut

12.1.1 ntpd

Ntpd est le coeur du système NTP. Il permet :

- de synchroniser l'horloge du PC avec un serveur NTP
- la synchronisation d'autres clients NTP
- d'ajuster le décalage de l'horloge
- de lire l'heure via d'autre périphérique comme un GPS

ntpd -c fichier_config ↵ = Utilise la configuration du fichier plutôt que celle par défaut
ntpd -g ↵ = Démarre ntpd sur un système dont le décalage de l'heure est > 1000 secondes (= seuil « panique »)
ntpd -q ↵ = Démarre ntpd et l'arrête après 1 synchronisation
ntpd -N ↵ = Démarre ntpd avec la plus haute priorité
ntpd -n ↵ = Démarre ntpd mais pas en tant que démon
ntpd -g -n -q ↵ = Synchronise de force un système dont l'heure est fortement décallée

Le fichier de configuration est /etc/ntpd.conf :

```
# Prohibit general access to this service.
restrict default ignore

# Permit all access over the loopback interface. This could be tightened as well, but to do so would affect some of
# the administrative functions.
restrict 127.0.0.1 = Limite l'accès à la machine local

# -- CLIENT NETWORK ------- Permit systems on this network to synchronize with this time service. Do not permit those
#systems to modify the configuration of this service. Also, do not use those systems as peers for synchronization.
restrict 192.168.1.0 mask 255.255.255.0 notrust nomodify notrap

# --- OUR TIMESERVERS ----- Permit time synchronization with our time source, but do not permit the source to query or
# modify the service on this system. time-b.nist.gov
restrict 129.6.15.29 mask 255.255.255.255 nomodify notrap noquery
server 129.6.15.29 = Adresse du serveur NTP

# --- GENERAL CONFIGURATION --- Undisciplined Local Clock. This is a fake driver intended for backup and when no
# outside source of synchronized time is available.
server
127.127.1.0 # local clock
fudge 127.127.1.0 stratum 10

# Drift file. Put this in a directory which the daemon can write to. No symbolic links allowed, either, since the daemon updates the file by creating a temporary in the same directory and then renaming it to the file.
driftfile /etc/ntp/drift
broadcastdelay
0.008
```

12.1.2 ntpdate

Utilisé pour mettre à jour un système local.
Ntpdate sera à terme remplacé par ntpd qui offre les même fonctions.
Ntpdate utilise le port 123 par défaut

ntpdate -b serveur_ntp ↵ = Met à jour le système d'une façon « brutal ».
L'option « -B » permet une est mise à jour de l'heure progressive, si le système local est décalé de plus de 128 ms. Si le système est TRES décalé, l'option « -B » peut rendre la mise à jour très longue
ntpdate -d ↵ = Mode debugging. Affiche des informations de débuggage sans mettre à jour le système
ntpdate -p 5 ↵ = Accède 5 fois au serveur NTP. Le nombre d'essai est comprise entre 1 et 8. Défaut = 4
ntpdate -q serveur_ntp -s ↵ = Interroge (= « -q » = query) le serveur NTP, et renvoie la sorti dans syslog plutôt que vers la sortie standard (= « -s »)
ntpdate -t 2 ↵ = Fixe le time-out d'accès au serveur ntp à 2 secondes. La valeur peut être un chiffre à virgule, elle sera arrondi à la 0,2 seconde la plus proche. Défaut = 1
ntpdate -u ↵ = N'utilise pas le port 123 (port TCP réservé au NTP), mais le port 1024 (non réservé), afin de passer outre certain pare-feu bloquant

12.1.3 ntpq

Programme de requête NTP.

ntpq -c fichier_commande ↵ = Exécute les commandes du fichier comme si elles étaient données d'une façon interactive.
ntpq -i ↵ = Entre dans le mode interactif. C'est le mode par défaut
ntpq -n ↵ = Supprime le reverse DNS. Les adresses IP sont affichées plutôt que les hostnames.

ntpq -n -p pool.ntp.org ↵ = Affiche l'adresse IP (= « -n ») la liste des serveurs NTP (= « -p ») d'un pool

Idem # ntpq -c peers –n pool.ntp.org ↵

Idem # ntpq –n pool.ntp.org ↵ = Par le mode interactif

```
ntpq> peers
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*64.90.182.55    .ACTS.           1 u    - 1024  377    2.983    3.253    0.014
+209.51.161.238  .CDMA.           1 u    - 1024  377    2.456   -2.795    0.096
-128.118.25.3    147.84.59.145    2 u    - 1024  377   18.476   -2.586    0.446
+67.128.71.75    172.21.0.13      2 u    - 1024  377    8.195   -2.626    0.194
-66.250.45.2     192.5.41.40      2 u    - 1024  377    8.119   -6.491    0.421
ntpq>
```

Dans cet exemple « ntp.pool.org » est un groupement de plusieurs serveurs NTP. Le serveur requêté change régulièrement

12.1.4 ntpdc

Idem ntpq. Il supporte quelques commandes supplémentaires.

12.1.5 ntptrace

ntptrace ↵ = Permet de déterminer où la chaine de synchronisation bloque

```
localhost: stratum 4, offset 0.000109, synch distance 0.16133
ntp1.example.net: stratum 3, offset 0.004605, synch distance 0.06682
ntp-1.example.edu: stratum 2, offset 0.001702, synch distance 0.01241
stratum1.example.edu:      *Timeout*
```

= Ce serveur n'est pas accessible

ntptrace serveur1.ntp.org ↵ = Interroge 1 serveur NTP en particulier, s'il est accessible

```
cudns.cit.cornell.edu: stratum 2, offset -0.004214, synch distance 0.03455
dtc-truetime.ntp.aol.com: stratum 1, offset -0.005957, synch distance
0.00000, refid 'ACTS'
```

12.1.6 date

date -s 22:34:00 ↵ = Règle l'heure système
date +%h%m ↵ = Formate la sortie de la commande date

```
janv.01
```

Champs horaires	Champs de date
%H = heure (00..23) %I = heure (01..12) %k = heure (0..23) %l = heure (1..12) %M = minute (00..59) %p = notation locale pour AM ou PM. %r = heure actuelle (sur 12 heures) %s = secondes écoulées depuis le 01-01-1970 %S = secondes (00..61) %T = heure actuelle, (sur 24 heures)	%a = abréviation locale du jour de la semaine (Dim .. Sam) %A = nom local du jour de la semaine (Dimanche .. Samedi) %b = abréviation locale du nom du mois (Jan..Dec) %B = nom local du mois (Janvier .. Décembre) %c = date et heure locales (Sat Nov 04 12:02:33 EST 1989) %d = jour du mois (01..31) %D = date (mm/jj/aa) %h = comme %b %j = jour de l'année (001..366) %m = mois (01..12) %U = numéro de semaine dans l'année (00..53). La semaine commence le Dimanche.

%w = Jour de la semaine (0..6). Le 0 correspond au Dimanche.
%W = numéro de semaine dans l'année (00..53). La semaine commence le Lundi.
%x = représentation locale de la date (mm/jj/aa)
%y = deux derniers chiffres de l'année (00..99)
%Y = année (1970...)

12.2 L'horloge matérielle

Toutes les valeurs de temps sont stockés en tant que nombre de secondes passées depuis le 01/01/1970

12.2.1 hwclock

hwclock --show --localtime ↵ = Affiche l'heure matérielle suivant l'heure locale
Idem # hwclock ↵
Sat 12 Sep 2009 **12:49**:43 PM CDT -0.216537 seconds
hwclock --show --utc ↵ = Affiche l'heure matérielle en heure UTC
Sat 12 Sep 2009 **10:49**:43 PM CDT -0.216537 seconds

hwclock --systohc ↵ = Règle l'horloge matérielle par rapport à l'heure du système
hwclock --systohc --utc ↵ = Règle l'horloge matérielle avec l'heure du système en UTC
hwclock --hctosys ↵ = Règle l'horloge du système avec l'heure matérielle
hwclock --adjust ↵ = Consulte le fichier d'ajustement (créé par « hwclock --set), et ajuste l'horloge machine. Il sauvegarde ensuite l'heure actuelle en tant que dernière heure de calibration.

13 Les logs

13.1 Configurer syslogd

Syslog récupère les logs. de tous les programmes et peut aussi router ces logs. vers un autre syslog.
La configuration du syslog se fait via le fichier /etc/syslog.conf
Le fichier est structuré comme suit : facility.level | action

facility = représente le créateur du message (authpriv, cron, deamon, kern = kernel, lpr, mail, mark, news, syslog, user, uucp ou local0 à local7)
level = définit la sévérité du message à envoyé à syslog (debug, info, notice, warning, err = error, crit, emerg = emergency)
action = représente la destination du message défini par « facility » et « level ».
Cela peut être un fichier, le hostname d'une machine ou bien une liste de user (qui recevront le message s'ils sont connectés)
/... = Ecrit les logs. dans un fichier local
| ... = Envoi les logs. dans un programme
@... = @IP de la machine distante où est envoyé les logs.
-/... = Ecriture assynchrone des logs. (serveur de mail sollicité)

local5.* /var/log/local5 = Configure syslog pour qu'il puisse recevoir tous les niveaux de messages de « local5 ». Ces messages seront inscrit dans un fichier de log spécifique : /var/log/local5
logger -p local5.info ''Message à loguer'' ↵ = Envoi un message à syslog, de la part de « local5 » et de niveau « info ». Ce message sera inscrit dans le fichier de log spécifique : /var/log/local5

Exemple de fichier /etc/syslog.conf :

```
# Log tous les messages sauf ceux venant de mail et authpriv, pour les niveaux info ou plus
*.info;mail.none;authpriv.none     /var/log/messages

# Les logs de authpriv ont un accès plus sctrict et sont donc stockés dans un autre fichier de log
authpriv.*                         /var/log/secure

# On logue tous les message de mail dans 1 seul fichier
mail.*                             /var/log/maillog

# Tous les user connectés reçoivent les messages de niveau emergency
*.emerg                            *

# On sauvegarde les messages venant de local7 dans le fichier log du boot
```

local7.* /var/log/boot.log

13.1.1 logger

logger evenement1 ↵ = Produit l'envoi de l'évènement 1 dans le syslog
logger -p mail.warning evenement2 ↵ = Produit l'envoi de l'évènement 2 avec une priorité « warning » créé par mail

13.1.2 Processus du service syslog

syslog est lié à 2 processus :

- syslogd pour les événement utilisateur
- klogd pour les événements du kernel

Ils travaillent ensemble et utilisent le même fichier de configuration

ps ax | egrep -i "(syslogd|klogd)"
2078 ? Ss 0:04 syslogd -m 0
2081 ? Ss 0:00 klogd -x

13.2 Système de log en client/serveur

syslogd peut envoyer des messages à travers le réseau.
Le port utilisé est le 514 par défaut.
syslogd -r ... ↵ = syslogd écoute le réseau pour des messages syslog entrants
Il est possible de configurer un serveur syslog sur le réseau récupérant tous les messages des autres serveurs.

Fichier /etc/syslog.conf du client :
. @10.0.0.1 = Tous les messages (de tous les auteurs et de tous niveaux), seront envoyés au serveur syslog dont l'adresse IP = 10.0.0.1

netstat -anp | grep -i ":514" ↵ = Permet de déterminer si la machine est bien un serveur syslog « écoutant » les messages venant des syslog client
udp 0 0 0.0.0.0:514 0.0.0.0:* 26645/syslogd

13.3 Rotation des logs

Permet de faire rouler les logs. toutes les nuits (paramétrable).
Le fichier maillog (par exemple) est alors renommé en mailog.1, mailog.2, etc.
La rotation des logs est configurable via le fihier /etc/logrotate.conf
Ce fichier de conf. est placé dans /etc/cron.daily

Exemple de fichier /etc/logrotate.conf :

```
# global options
# La rotation se fait toutes les semaines
weekly
# Garde 4 semaines d'anciens logs
rotate 4
# Envoi les erreurs à root
errors root
# Créé un nouveau (mais vide) fichier de log après la rotation
create
# Compresse les fichiers de logs
compress
# Fichiers traités spécifiquement
/var/log/wtmp {  =  La rotation des logs du fichier wtmp est définie en dessous
   monthly  =  La rotation se fait tous les mois
   create 0664 root utmp  =  Une fois la rotation faite, crée un nouveau fichier de log avec les droits 664, dont le propriétaire est root. Le groupe de ce fichier est utmp
   rotate 1  =  Ne garde qu'1 seul ancien fichier de log
}

/var/log/messages {  =  La rotation des logs du fichier messages est définie en dessous
   postrotate  =  Les lignes entre postrotate et endscript (chacun devant apparaître sur une ligne isolée) sont exécutées après permutation du journal
      /usr/bin/killall -HUP syslogd = Ici le script killall
   endscript
}
```

13.4 Examen des fichiers de logs

Les fichiers de logs construit par syslog sont écrit avec les champs suivants :

- Date et heure
- Hostname de la machine source du message
- Expéditeur du message, au sens « user » (kernel, sendmail, etc.), différent du « facility »
- Le message en lui-même

```
Aug  3 18:45:16 moya kernel: Partition check:   =  Le message vient de la machine « moya », par le kernel
Aug  3 18:45:16 moya kernel: sda: sda1 sda2 sda3 < sda5 sda6 sda7 sda8 sda9 sda10 > sda4
Aug  3 18:45:16 moya kernel: SCSI device sdb: 195369520 512-byte hdwr sectors (100029 MB)
Aug  3 18:45:16 moya kernel:  sdb: sdb1
Aug  3 18:45:16 moya kernel: Journalled Block Device driver loaded
Aug  3 18:45:16 moya kernel: kjournald starting.  Commit interval 5 seconds
Aug  3 18:45:16 moya kernel: EXT3-fs: mounted filesystem with ordered data mode.
Aug  3 18:45:16 moya kernel: Freeing unused kernel memory: 116k freed
Aug  3 18:45:16 moya kernel: Adding Swap: 1044216k swap-space (priority -1)
```

grep '[Mm]ouse' /var/log/messages ↵ = Filtre sur les messages concernant la souris

```
Dec  8 00:15:28 smp kernel: Detected PS/2 Mouse Port.
Dec  8 10:55:02 smp gpm: Shutting down gpm mouse services:
```

grep 'sendmail:' /var/log/messages* ↵ = Filtre tous les messages envoyés par sendmail
Idem mais sur des fichiers de logs compressés # **zgrep** 'sendmail:' /var/log/messages* ↵

Un problème détecté dans un fichier de log peut être résolu rapidement en regardant en 1er le hostname de la machine source et l'expéditeur, avant de regarder le message en lui-même.

13.5 Afficher plus messages

Il peut être utile également d'augmenter le nombre de message affiché par syslog en modifiant le niveau dans /etc/syslog.conf

Avant :

```
# Log tous les messages sauf ceux venant de mail
#et authpriv, pour les niveaux info ou plus

*.info;mail.none;authpriv.none      /var/log/messages
```

Après :

```
# Log tous les messages sauf ceux venant de mail
#et authpriv, pour les niveaux debug ou plus

*.debug;mail.none;authpriv.none
                /var/log/messages
```

14 Courrier

Le service de courrier n'écoute que le broadcast à la base.
Les logiciels les plus connus sont : sendmail, postfix, qmail et exim

14.1 SMTP

mail -s ''Sujet du mail'' adresse@mail.fr < fichier_du_contenu_du_mail ↵ = Envoie un mail
La commande mail permet également de lire les mails reçus
mailq ↵ = Intérroge la file d'attente des mails pour savoir si elle est pleine
server-switch-mail ↵ = Permet de sélectionner le serveur de mail à utiliser (sous RedHat)
Le fichier /etc/aliases permet de transférer des mail d'un alias vers une autre boite mail.

14.2 Sendmail

sendmail est un programme unique avec 1 seul fichier exécutable qui envoi et reçoit les mails.
Il est possible d'utiliser sendmail avec un autre propotocle que SMTP
Il écoute par défaut sur le port utilisé pour le SMTP = 25

Installation de Sendmail :

1. # yum install sendmail.cf ↵
2. # vi /etc/sendmail/sendmail.cf ↵ = Edite le fichier de configuration
   DAEMON_OPTIONS (Port...)
3. # make ↵ = Compile le fichier de configuration pour qu'il puisse être utiliser par sendmail
4. # service sendmail restart ↵
5. # netstat -plantu | grep -w 25 ↵ = Liste les services utilisant le port 25
   0.0.0.0:25 SMPT / Sendmail

Toutes les actions de sendmail sont logées via syslog dans le fichier /var/log/maillog

Exemple d'envoi d'un mail de test :
netstat -anpl --tcp | grep sendmail ↵ =
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN 1847/sendmail: accepting connections

ls -l /var/spool/mail/adamh ↵ = Le fichier de log pour les mail de « adamh » existe (mais est vide)
-rw-rw---- 1 adamh mail **0** 2009-04-24 01:23 /var/spool/mail/adamh

echo "Test du mail" | mail adamh ↵ = Envoi d'un mail à adamh

ls -l /var/spool/mail/adamh ↵ = Le fichier de log s'est bien rempli
-rw-rw---- 1 adamh mail **689** 2010-02-07 13:21 /var/spool/mail/adamh

tail /var/log/maillog ↵ = Le mail a été bien envoyé
Feb 7 13:22:42 server sendmail[5387]: o17JMgbM005387: from=root, size=32, class=0, nrcpts=1, msgid=<201002071922.o17JMgbM005387@server>, relay=root@localhost
Feb 7 13:22:42 server sendmail[5388]: o17JMghc005388: from=<root@server>, size=353, class=0,nrcpts=1, msgid=<201002071922.o17JMgbM005387@server>, proto=ESMTP, daemon=MTA, relay=server [127.0.0.1]
Feb 7 13:22:42 server sendmail[5387]: o17JMgbM005387: to=adamh, ctladdr=root (0/0), delay=00:00:00, xdelay=00:00:00, mailer=relay, pri=30032, relay=[127.0.0.1] [127.0.0.1], dsn=2.0.0, stat=Sent (o17JMghc005388 Message accepted for delivery)
Feb 7 13:22:42 server sendmail[5389]: o17JMghc005388: **to=<adamh@server>**,ctladdr=<root@server> (0/0), delay=00:00:00, xdelay=00:00:00, mailer=local, pri=30607, dsn=2.0.0, **stat=Sent**

cat /var/spool/mail/adamh ↵ = Log spécifique pour adamh
From root@server Sun Feb 7 13:22:42 2010
Return-Path: <root@server>
Received: from server (server [127.0.0.1])
by server (8.14.2/8.14.2) with ESMTP id o17JMghc005388
for <adamh@server>; Sun, 7 Feb 2010 13:22:42 -0600
Received: (from root@localhost)
by server (8.14.2/8.14.2/Submit) id o17JMgbM005387
for adamh; Sun, 7 Feb 2010 13:22:42 -0600
Date: Sun, 7 Feb 2010 13:22:42 -0600
From: root <root@server>
Message-Id: <201002071922.o17JMgbM005387@server>
To: adamh@server
Test du mail

14.2.1 mail

mail ↵ = Démarre l'envoi d'un mail en mode interractif
Envoi un mail depuis la ligne de commande: ↵ = Le corps est données en mode interractif, terminé par « : »

# mail -s "Ceci est le sujet" -c "root" adamh ↵ = On précise le sujet (= « -s ») et l'expéditeur (= « -c »)
Hello = Le corps du mail est données en mode interractif
C'est moi

echo "Ceci est le corps du mail" > /tmp/corps.msg ↵ = On crée un fichier contenant le corps du mail
cat /tmp/corps.msg | mail –s "Ceci est le sujet" –c "root" adamh ↵ = Le contenu du fichier est envoyé par mail en précisant le sujet (= « -s ») et l'expéditeur (= « -c »). Cet exemple fonctionne car le user « adamh » est déclaré sur le système

14.2.2 Les alias et le fichier .forward

Pour recevoir dans la même boite des mails venant d'adresses différentes, il faut créer des alias via le fichier /etc/aliases.
Le format est :

- alias
- user
- compte

cat /etc/aliases
Aliases in this file will NOT be expanded in the header from Mail, but WILL be visible over networks or from /bin/mail
NOTE > The program "newaliases" must be run after this file is updated for any changes to show through to sendmail.

Alias basiques du système -- Ils DOIVENT être présents
mailer-daemon: postmaster
postmaster: root

Redirections générales pour des comptes
bin: root
daemon: root
adm: root
lp: root

Alias utilisateurs = Les mails envoyés à adam, adam.haeder et haeder sont en fait placés dans la boite de adamh
adam: adamh
adam.haeder: adamh
haeder: adamh

newaliases ↵ = A exécuter après chaque modification du fichier /etc/aliases (en tant que root)

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 $HOME/.forward sur machine_de_Ulam :
labo@machine_de_Ulam, labo = Permet d'obtenir, sur la machine de Ulam, une copie de tous les messages envoyés à la machine labo

14.2.3 mailq

Les mails non envoyés (en cas de défaillance du serveur par exemple) sont placés dans une queue pour être envoyés plus tard.
sendmail retente d'envoyer les mails toutes les 4 heures pendant 5 jours. Après coup, il envoi un message « Delivery failure »
La queue des mails est stockée dans le répertoire /var/spool/mqueue et est géré par le programme « mailq »

echo "Test" | mail user@inconnue.com ↵ = Envoi un mail à un destinataire inconnue
View the mail queue
mailq ↵ = Affiche la liste des mails en attente dans la queue
o1591AmX005615 7182 Fri Feb 5 03:01 MAILER-DAEMON = Ce mail sera ré-envoyé toutes les 4 heure → 5 jours
  8BITMIME (Deferred: Connection refused by unknown.com.) <user@unknown.com>

sendmail –q –v ↵ = Relance l'envoi de tous les mails en attente dans la queue (= « -q) en mode verbeux (= « -v »)

14.3 Postfix

postfix garde le plus possible une compatibilité avec sendmail
Ceci est possible car il intègre le programme /usr/sbin/sendmail, qui agit comme un «pont» entre les appels à sendmail et l'utilitaire postfix.
La plupart des commandes utilisées avec sendmail fonctionnent avec postfix
which sendmail ↵
/usr/sbin/sendmail
for file in /usr/sbin/sendmail /usr/bin/mailq /usr/bin/newaliases; { echo -n "$file: " && rpm -q --whatprovides ${file}; } ↵

/usr/sbin/sendmail: postfix-2.3.2-32
/usr/bin/mailq: postfix-2.3.2-32
/usr/bin/newaliases: postfix-2.3.2-32

Contrairement à sendmail, postfix est fait d'une multitude de programmes.
Le programme principal est /usr/lib/postfix/master. C'est le démon qui écoute sur les ports SMTP
Les autres applications sont sous /usr/lib/postfix/

Le fichier de configuration est /etc/postfix/main.cf
La file d'attente se trouve sous /var/spool/postfix

postfix check ↵ = Vérifie le fichier de configuration
postconf -e option=paramètre ↵ = Ajouter une option et son paramètre au fichier de configuration

postconf ↵ = Liste toutes les valeurs

postconf -n ↵ = Liste les valeurs de configuration différentes de celles par défaut
postconf -d ↵ = Liste les valeurs de configuration par défaut (« -d » = default)
postconf -v ↵ = Liste toute les valeurs de configuration
postconf -m ↵ = Liste les types de tables supportées par PostFix

postsuper -d ALL ↵ = Vider intégralement la file d'attente de postfix qui se trouve sous /var/spool/postfix

14.4 Qmail

Qmail est constitué de différents programmes
L'objectif de conception derrière Qmail est la sécurité. Les programmes tournent avec de faibles privilèges

Le programme faisant passerelle avec sendmail est /var/qmail/bin/sendmail

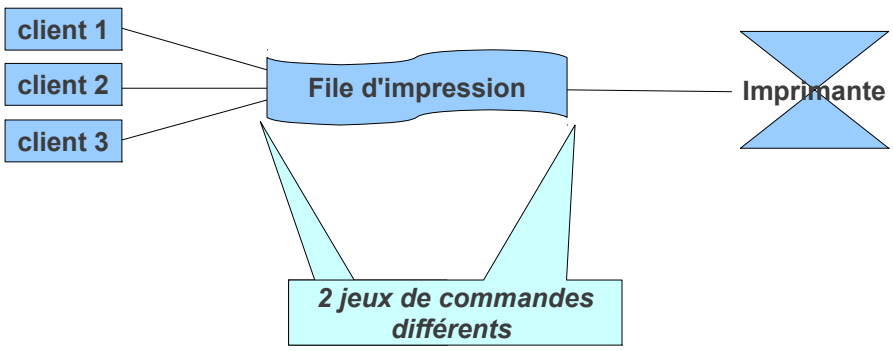
14.5 Exim

Des programmes d'aide et la conservation des options de sendmail en ligne de commande permettent une transition plus facile depuis à Sendmail.
Exim est monolithique comme sendmail

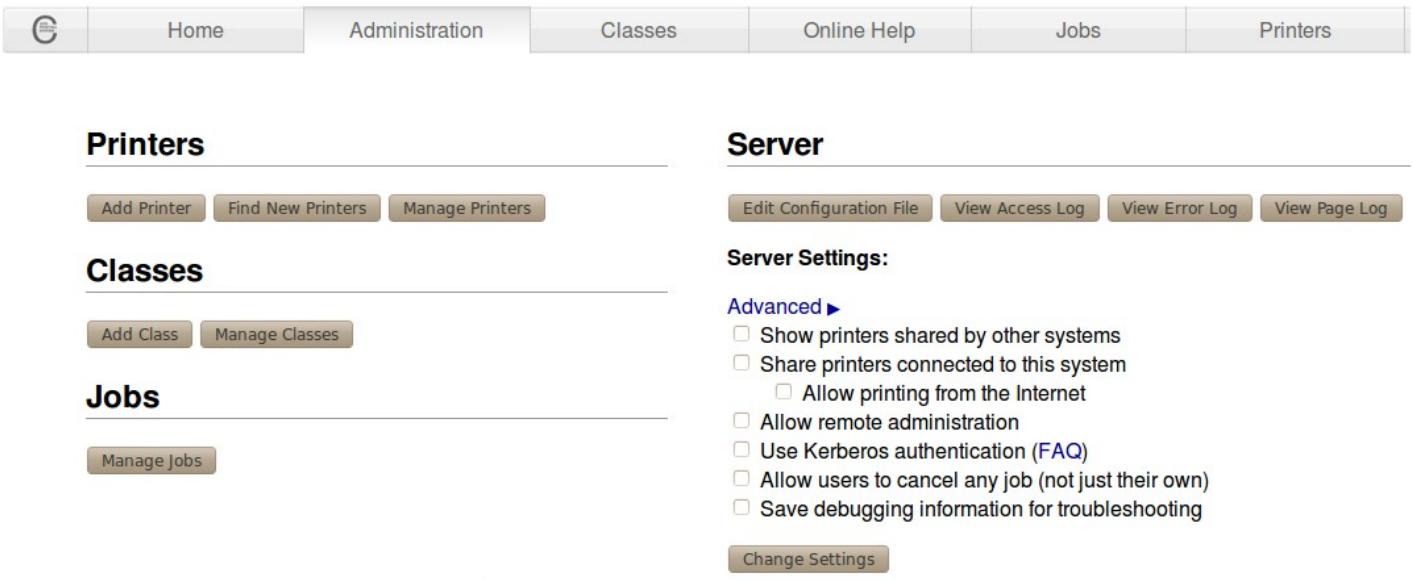
15 Gestion de l'impression

15.1 CUPS

CUPS utilise lprlpd et ipp.



Il y a 2 jeux de commande différents pour gérer les impressions à l'entrée ou à la sortie de la file d'attente.
Un flitre (HPGL, PS, PCL, etc.) est appliqué à chaque file.
Pour configurer une imprimante, accédez via un navigateur : http://@IP-du-poste:631/



1. Un job d'impression est produit par une application côté client
2. Le job est envoyé au serveur d'impression spécifié par le protocol sélectionné (IPP ou CIFS)
3. Côté serveur CUPS, le spool d'impression « cupsd » attend le flux de données et sauvegarde les données dans le répertoire de la file d'impression, par défaut = /var/spool/cups.
4. Si un filtre d'impression est déclaré dans la configuration, CUPS le traite.
   Dans tous les cas, après tous les filtres, le job est envoyé au « backend »
5. Le « backend » envoi les données vers l'imprimante
6. Une fois le job imprimé, cupsd supprime les fichiers du répertoire du spool, suivant la configuration du temps de rétention.

15.1.1 Fichiers nécessaires à CUPS

cupsd = Le démon est lancé au démarrage du système et écoute en continue les requêtes d'impression. Lorsqu'un job est soumis à une queue d'impression, cupsd récupère le job depuis cette queue

/etc/cups/cupsd.conf = Fichier de configuration du démon cupsd. Les directives sont similaires à celles d'un serveur Apache

/etc/cups/printers.conf = Fichier de définition des imprimantes locales. Ce fichier est créé automatiquement par cupsd lors de l'ajout, de la suppression ou de la modification d'une imprimante. Il ne doit pas être modifié manuellement

/var/spool/cups = Répertoires de spool que cupsd utilise pour stoker les jobs dans les queues d'impression

/etc/printcap = Ce fichier permet à d'anciennes applications d'imprimer. Il est automatiquement généré par cupsd depuis le fichier /etc/cups/printers.conf. Toutes modifications seront perdues au re-démarrage du service CUPS
Ce fichier permet de nommer l'imprimante et d'indiquer certaines informations essentielles :

- cm = Commentaire
- sd = Répertoire de spool = spool directory
- af = Nom du fichier de comptabilité associé à l'imprimante. Permet de collecter des informations pour facturer les services d'impression aux services utilisateurs
- lp = Nom du périphérique de sortie. /dev/lp1 correspond à LPT1.
- if = "input filter". C'est le nom du filtre d'impression, programme recevant les données à imprimer sur son entrée standard et écrivant sur sa sortie standard les données converties sous une forme adaptée à l'imprimante.
- mx = Taille maximale d'un travail d'impression en octets. Une valeur nulle signifie qu'on ne doit pas faire de contrôle.
- sh = Supprime l'impression de la page de garde.
- rm = Machine distante = remote machine
- rp = Impirmante distante = remote print

Exemple :

```
stylus820:\
    :cm=Epson Stylus 820 on LPT1:\
```

```
    :sd=/var/spool/lpd/stylus820:\
    :af=/var/spool/lpd/stylus820/acct:\
    :lp=/dev/lp1:\
    :if=/usr/local/bin/unifilter:\
    :mx#0:\
    :sh:
```

15.1.2 Programmes d'interface = backend

Plusieurs programmes d'interface (système → imprimante) sont utilisables :

- Parallèle, série, SCSI et USB.
- Via le réseau : HTTP, HTTPS, and IPP (Internet Printing Protocol)
- Protocole CIFS appelé SMB

Ces programmes sont sous /usr/lib/cups/backend
Ce sont les derniers programmes exécutés dans la chaine d'impression d'un job.

15.1.3 Filtres CUPS

Ghostscript est la base du système de filtres pour CUPS. Il traduit différents formats de données dans un langage de description de page.
Pour une imprimante PostScript, le fichier PPD contient les options spécifique à cette imprimante (et rien d'autre) avec les extraits correspondants du code PostScript qui doit être envoyée à l'interpréteur PostScript pour activer une option donnée.
Pour une imprimante non-PostScript, le fichier PPD contient des information supplémentaires concernant le driver de l'imprimante à utiliser et les options possibles pour ce driver particulier. Si plusieurs drivers peuvent être utilisés, il y aura plusieurs fichier PPD sur le système.

15.1.4 lp

Line print. Imprime un fichier ou modifie un travail d'impression

lp -d imprimante -n 3 fichier ↵ = Imprime le fichier en 3 fois (= « -n ») sur l'imprimante
lp -o sides=two-sided-long-edge fichier ↵ = Imprime le fichier en recto-verso
lp -d imprimante -o media=legal -o sides=two-sided-long-edge fichier ↵ = Imprime le fichier en recto-verso dans un format normal
lp -d imprimante -o scaling=200 fichier ↵ = Imprime le fichier sur l'imprimante sur 2 pages (= 200%)
lp -d imprimante -o cpi=12 -o lpi=8 -o page-left=72 fichier ↵ = Imprime le fichier sur l'imprimante avec 12 caractères par pouce (= « cpi »), 8 lignes par pouce (= « lpi) et 1 pouce de marge à gauche (= « page-left », 1 pouce = 72 points)

15.1.5 cancel

Supprime un job de la queue d'impression

cancel -a imprimante ↵ = Supprime tous les jobs (= « -a » = all) de l'imprimante
cancel -a ↵ = Supprime tous les travaux sur toutes les imprimantes
cancel -u david imprimante ↵ = Supprime les jobs de l'utilisateur david
cancel -E -U root -h serveur_impression:port 3 imprimante ↵ = Supprime le job n° 3 sur l'imprimante, crypte la connexion au serveur d'impression (= « -E »), utilise le user root pour la connexion au serveur (= « -U ») au serveur d'impression spécifié (= « -h »)

15.1.6 lpstat

Affiche des informations sur l'état des jobs et des imprimantes.

lpstat ↵ = Affiche des informations sur la queue d'impression de l'utilisateur courrant
lpstat -a imprimante ↵ = Affiche si les files d'attentes de l'imprimante peuvent accepter des travaux d'impression
Idem pour toutes les imprimantes # lpstat -a ↵
lpstat -t imprimante ↵ = Affiche toutes les informations sur l'état de l'imprimante.
Équivaut aux options :

- « -r » = Affiche si le serveur CUPS est actif
- « -d » = Affiche l'imprimante par défaut
- « -c » = Affiche la classe des imprimantes et ses imprimantes associées
- « -v » = Affiche les imprimantes et à quel matériel elles sont rattachées
- « -a » = Affiche l'état de la queue d'impression
- « -p » = Affiche si les imprimantes sont prêts à imprimer ou non
- « -o » = Affiche la file d'attente des destinations spécifiées

15.1.7 lpadmin

Configure les imprimante. Peut définir l'imprimante par défaut

lpadmin -d file_impression ↵ = Configure la file d'impression
lpadmin -m modele ↵ = Définit un script d'interface System V ou un fichier PPD du répertoire des modèles
lpadmin -E -d imprimante ↵ = Rend opérationnel (= « -E ») l'imprimante pour quelle accepte les jobs d'impression.
Idem avec les programmes # accept ↵ ou # cupsenable ↵

15.1.8 lpq

Interroge et affiche le status et le contenu des queues d'impression

lpq ↵ = Affiche les impressions de la file par défaut

```
lp is ready and printing
Rank    Owner      Job     Files                 Total Size
active  root       193     filter                9443 bytes  =  Le fichier filter est en cours d'impression
1st     root       194     resume.txt            11024 bytes  =  Le fichier resume.txt est le prochain à être imprimé
2nd     root       196     (standard input)      18998 bytes
```

lpq -l ↵ = Affiche les impressions au format long (= « -l »)

```
lp is ready and printing
root: active                    [job 193AsJRzIt]
      filter                    9443 bytes
root: 1st                               [job 194AMj9Io9]
      resume.txt                11024 bytes
root: 2nd                        [job 196A6rUGu5]
      (standard input)                  18998 bytes
```

lpq -P file_impression ↵ = Affiche les impressions de la file d'impression

lpq david ↵ = Affiche les travaux de david

```
Rank    Owner      Job     Files                 Total Size
7th     david      202     .bash_history         1263 bytes
9th     david      204     .bash_profile         5676 bytes
```

Il est possible d'avoir une réponse « no entries » alors que l'imprimante est en cours d'impression. Ceci est expliqué par le fait que le spool de l'imprimante a été vidé dans le buffer de l'imprimante. Pour supprimer ce job, il faut alors agir sur l'imprimante.

15.1.9 lprm

Supprime un job d'une queues d'impression

lprm - ↵ = Supprime tous les travaux d'impression de l'utilisateur courant
lprm -a -all ↵ = Supprime tous les travaux d'impression pour tous les utilisateurs
lprm -Pqueue_impression - ↵ = Supprime (= « - ») tous les travaux d'impression de la queue d'impression en tant que root
Idem # lprm -P queue_impression ...
lprm -U david - ↵ = Supprime tous les travaux d'impression de david

15.1.10 lpr

Envoi un fichier ou l'entrée standard à une queue d'impression. Une copie du job est placé sous le répertoire /var/spool/lpr jusqu'à ce que le job soit imprimé

lpr fichier ↵ = Envoi le fichier sur la file d'impression par défaut
lpr -Pqueue_impression2 fichier ↵ = Envoi le fichier sur la queue d'impression n°2
man -t 5 ls | lpr ↵ = Envoi la sortie de la commande « man -t » sur la queue d'impression par défaut
lpr -#3 fichier ↵ = Envoi 3 fois le fichier sur la file d'impression par défaut
Idem # lpr -K 3 fichier ↵
lpr -s fichier ↵ = Plutôt que de copier le job sous /var/spool/lpr, la commande fait un lien symbolique vers le fichier. Cela élimine le temps de transfert et la place nécessaire au stockage sous

/var/spool/lpr. Utile pour soulager le démon lors de l'impression de documents très lourds

15.1.11 lpc

Commande remplacée par lpadmin

16 Corriger un problème d'impression

Modifier au préalable la valeur indiqué par la ligne « loglevel » dans le fichier /etc/cups/cupsd.conf. Le niveau « debug » semble judicieux.

16.1 Fichier de log « error_log »

Les erreurs récentes peuvent être trouvées dans le fichier /var/log/cups/error_log :

I [16/Nov/2009:11:19:07 +0100] [Job 102] Adding start banner page "none". = Le « I » du début de ligne indique une information, il n'y a pas de warning ou d'erreur
I [16/Nov/2009:11:19:07 +0100] [Job 102] Adding end banner page "none".
I [16/Nov/2009:11:19:07 +0100] [Job 102] File of type application/postscript queued by "brunop".
I [16/Nov/2009:11:19:07 +0100] [Job 102] Queued on "PDF" by "brunop".
I [16/Nov/2009:11:19:07 +0100] [Job 102] Started filter /usr/libexec/cups/filter/pstops (PID 18223)
I [16/Nov/2009:11:19:07 +0100] [Job 102] Started backend /usr/libexec/cups/backend/cups-pdf (PID 18224)
I [16/Nov/2009:11:19:07 +0100] [Job 102] Completed successfully.

16.2 Fichier de log « page_log »

Ce fichier de log est sous /var/log/cups/page_log. Il donne des information sur chaque page envoyé à l'imprimante.
Format de chaque ligne :

- imprimante
- user
- identifiant du job
- date et heure
- nombre de page
- nombre d'exemplaire
- facturation du job
- hostname de la source du job
- nom du job
- média
- recto ou recto-verso

Photosmart_C4500 brunop 86 [31/Oct/2009:12:48:36 +0100] 1 1 - localhost
adamp23 brunop 87 [02/Nov/2009:13:40:33 +0100] 1 1 - localhost
PDF root 100 [16/Nov/2009:11:11:52 +0100] 1 1 - localhost
PDF brunop 101 [16/Nov/2009:11:16:38 +0100] 1 1 - localhost

16.3 Fichier de log « access_log »

Ce fichier de log est sous /var/log/cups/access_log. Il permet de voir toutes les connexions HTTP.
Sont format reprend le format des fichiers de logs des serveurs Web

localhost - - [16/Nov/2009:17:28:29 +0100] "POST / HTTP/1.1" 200 138 CUPS-Get-Default successful-ok
localhost - root [16/Nov/2009:17:28:29 +0100] "GET /printers HTTP/1.1" 200 11258 - -
localhost - root [16/Nov/2009:17:28:29 +0100] "GET /images/button-search.gif HTTP/1.1" 200 332 - -

16.4 Utiliser l'utilitaire cups-config

Cet utilitaire a différentes options :

- --api-version = Affiche la version d'API actuelle (majeur.mineur)
- --version = Affiche la version complète de l'installation CUPS (majeur.mineur.patch).
- --cflags = Affiche les options de compilations nécessaires
- --datadir = Affiche le répertoire de données par défaut de CUPS
- --help = Affiche un message d'aide.
- --ldflags = Affiche les options nécessaires pour l'édition des liens
- --libs = Affiche les bibliothèques nécessaires pour l'édition des liens
- --serverbin = Affiche le répertoires par défaut des binaires, où se trouvent les filtres et dorsaux
- --serverroot = Affiche le répertoire de configuration par défaut de CUPS.
- --image = Lorsqu'elle est utilisée avec --libs, cette option ajoute la bibliothèque de gestion des images CUPS des bibliothèques affichées.

- --static = Lorsqu'elle est utilisée avec --libs, les bibliothèques statiques seront affichées au lieu des bibliothèques partagées qui sont affichées par défaut.

17 Les principaux protocoles Internet

17.1 Adressage réseau

IPV4 permet d'utiliser 4,29 millions d'adresses
Classes d'adresses :

	Plage d'adresses IP	Notation CIDR	Masque de sous-réseau par défaut
Classe A	0.0.0.0 → 127.255.255.255	/8	255.0.0.0
Classe B	128.0.0.0 → 191.255.255.255	/16	255.255.0.0
Classe C	192.0.0.0 → 223.255.255.255	/24	255.255.255.0
Classe D		/4	Non défini
Classe E	224.0.0.0 → 239.255.255.255		Non défini
	240.0.0.0 → 247.255.255.255		

Adresses remarquables :

- 0.0.0.0= N'importe qu'elle destination
- 255.255.255.255 = broadcast = adresse de diffusion
- 127.0.0.1 = Adresse locale = localhost

17.1.1 Adresses IP privées et NAT

Classe d'adresse	Plage d'adresses IP privées	
Classe A	10.0.0.0 → 10.255.255.255	10.0.0.0 / 8
Classe B	172.16.0.0 → 172.31.255.255	172.16.0.0 / 16
Classe C	192.168.0.0. → 192.168.255.255	192.168.0.0 / 24

17.1.2 IPV6

Définit en 1995, permet d'utiliser 2^{128} adresses IP. Plus besoin de mettre en place des réseaux en CIDR ou bien du NAT.
Une adresse IPv6 est longue de 128 bits (16 octets) contre 32 bits pour IPv4. La notation décimale pointée employée pour les adresses IPv4 (par exemple 172.31.128.1) est abandonnée au profit d'une écriture hexadécimale, où les 8 groupes de 2 octets (16 bits par groupe) sont séparés par un signe deux-points :

`2001:0db8:0000:85a3:0000:0000:ac1f:8001`

Il est permis d'omettre de 1 à 3 chiffres zéros non significatifs dans chaque groupe de 4 chiffres hexadécimaux. Ainsi, l'adresse IPv6 ci-dessus est équivalente à :

`2001:db8:0:85a3:0:0:ac1f:8001`

De plus, une unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls peut être omise, en conservant toutefois les signes deux-points de chaque côté de la suite de chiffres omise, c'est-à-dire une paire de deux-points (::)16. Ainsi, l'adresse IPv6 ci-dessus peut être abrégée en :

`2001:db8:0:85a3::ac1f:8001`

Une même adresse IPv6 peut être représentée de plusieurs façons différentes, comme 2001:db8::1:0:0:1 et 2001:0DB8:0:0:1::1

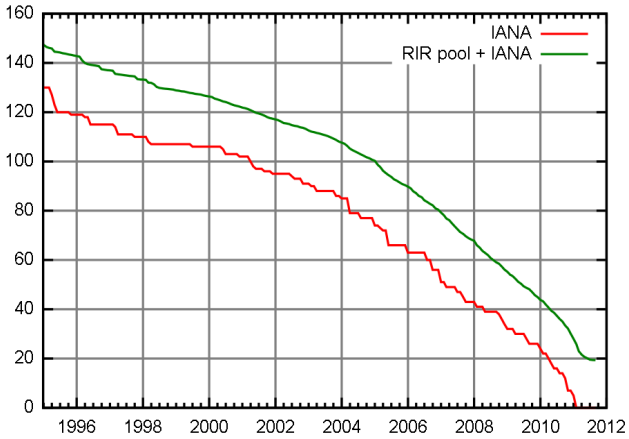
Une adresse IP V6 est construite avec l'adresse MAC (64 derniers bits)
Le préfixe de l'IP V6 est donné à vie et est indépendant de l'opérateur Internet
Traceroute et ping peuvent fonctionner en IPV6

Avantage de l'IPV6 :

Limitation du nombre d'adresses : 10^4 adresses pour IPV4 et 2^{128} adresses IP pour l'IPV6

Sécurité = IPsec a été conçu pour être intégré dans l'adressage IPv6 et pour être utilisée avec le protocole, tandis que IPv4 le traite comme une fonction optionnelle. Les processus de cryptage sont également inclus dans l'adressage Ipv6.

Configuration = Les périphériques IPV6 se configurent automatiquement une fois connectés à un routeur IPV6. C'est une version du DHCP IPV4 plus précise. IPV6 permet l'adressage des périphériques mobiles



Performance = Les en-têtes IPv6 ont été modifiés pour travailler avec des routeurs haut débit, ce qui augmente la vitesse et la performance sur les réseaux

17.2 Masque

On considérait autrefois que l'adresse du réseau était définie par sa classe, et obtenue en appliquant l'opérateur booléen ET bit à bit entre le masque par défaut associé et l'adresse IPv4. La notion de classe est cependant considérée comme désuète depuis l'avènement du routage sans classe.
Un masque de sous-réseau (désigné par subnet mask, netmask ou address mask en anglais) est un masque indiquant le nombre de bits d'une adresse IPv4 utilisés pour identifier le sous-réseau, et le nombre de bits caractérisant les hôtes (ce qui indique aussi le nombre d'hôtes possibles dans ce sous-réseau).

L'adresse du sous-réseau est obtenue en appliquant l'opérateur ET binaire entre l'adresse IPv4 et le masque de sous-réseau. L'adresse de l'hôte à l'intérieur du sous-réseau est quant à elle obtenue en appliquant l'opérateur ET entre l'adresse IPv4 et le complément à un du masque.

Address	**192.168.1.127**	11000000.10101000.00000001.01111111
Mask	**255.255.255.0**	11111111.11111111.11111111.00000000
Network address	**192.168.1.0**	11000000.10101011.00000001.00000000
Host interface address	**127**	01111111

Les masques de sous-réseau utilisent la même représentation que celles des adresses IPv4. En IPv4, une adresse IP est codée sur 4 octets, soit 32 bits (représentés en notation décimale à point). Un masque de sous-réseau possède lui aussi 4 octets. Bien que la norme IPv4 n'interdise pas que la partie significative du masque contienne des bits à 0, on utilise en pratique des masques constitués (sous leur forme binaire) d'une suite de 1 suivis d'une suite de 0, il y a donc 32 masques réseau possibles.

Exemple :

adresse 192.168.1.2 et masque 255.255.255.0

192.168.1.2 & 255.255.255.0 = 192.168.1.0 = Adresse du réseau
192.168.1.2 & 0.0.0.255 = 0.0.0.2 = Adresse de l'hôte dans ce réseau

soit en binaire :

```
  11000000.10101000.00000001.00000010        11000000.10101000.00000001.00000010
& 11111111.11111111.11111111.00000000      & 00000000.00000000.00000000.11111111
= 11000000.10101000.00000001.00000000      = 00000000.00000000.00000000.00000010
```

Autrement dit, il suffit pour obtenir l'adresse du sous-réseau de conserver les bits de l'adresse IPv4 là où les bits du masque sont à 1 (un certain nombre de bits en partant de la gauche de l'adresse). La partie numéro d'hôte est, elle, contenue dans les bits qui restent (les plus à droite).

Deux adresses IP appartiennent à un même sous-réseau si elles ont en commun les bits du masque de sous-réseau.

À partir de la connaissance de l'adresse IPv4 et du masque de sous-réseau il est possible de calculer le nombre d'interfaces que l'on peut numéroter à l'intérieur d'un sous-réseau. Le nombre de sous-réseaux possibles est donné par 2r-n, où n représente le nombre de bits à 1 dans le masque réseau et r le nombre de bits du masque de sous-réseau. Le nombre d'hôtes est $2^{32-n}-2$, deux adresses de ce sous-réseau étant réservées au sous-réseau lui-même et au broadcast et ne peuvent pas être utilisées pour numéroter une interface.

17.3 CIDR

La notation CIDR utilise le format adresse/préfix.
Le préfixe désigne le nombre de bits qui sera utilisé par le masque de sous-réseau.
206.24.94.105/24 = Plage d'adresses IP composée de 206.24.94.105 et un masque de sous réseau 255.255.255.0

/32 désigne un réseau qui ne comporte qu'une seule adresse IP, c'est-à-dire une adresse IP individuelle.

Le masque /31 était autrefois considéré comme inutilisable, car ce réseau ne comporte que deux adresses, dont l'adresse du sous-réseau et l'adresse de broadcast. Pour numéroter des adresses de liens point à point, on utilisait donc des /30, soit quatre adresses dont deux utilisables pour adresser des interfaces. Le RFC 3021 permet cependant d'utiliser plus efficacement l'espace d'adressage en permettant le /31 (il n'y a dans ce cas pas d'adresse de broadcast et l'adresse du sous-réseau est utilisée pour numéroter une interface).

17.4 Les couches OSI

5	Application	HTTP, FTP, DNS, etc
4	Transport	**TCP**, **UDP**, RTP, SCTP, etc
3	Réseau	**IP**, **ICMP**, etc
2	Liaison	Ethernet, **PPP**, Token Ring, etc.
1	Physique	Lignes RTC, RNIS, ADSL, téléphonie sans fil, satellite, etc

17.5 Les protocoles

Certains protocoles utilisent « handshake » (échange d'informations de contrôle entre les systèmes communicants) pour établir et maintenir une connexion. Un tel protocole est dit « connection-oriented » (orienté connexion) et est considéré fiable, parce que le protocole lui-même est responsable de la gestion des erreurs de transmission, les paquets perdus, et l'ordre d'arrivée des paquets. Un protocole qui n'a pas d'informations de contrôle des changes est dit « connectionless » (sans connexion) et n'est pas considéré comme fiable, ce qui veut dire simplement que ce protocole ne prend pas en charge lui-même les problèmes de connexions.

TCP/IP est une suite de protocoles Internet qui inclut :

- TCP = Transmission Control Protocol = « connection-oriented », utilisé par les application (FTP, Telnet, SMTP, etc.) pour établir une connexion sur le réseau. Il transporte les informations à travers le réseau par « handshaking ». Il garanti l'arrivé des paquets et gère la retransmission en cas d'erreur. utilisent TCP.
- IP = Internet Protocol = « connectionless », il est à la base de l'Internet. Définit les datagrammes (unité de base de transmission), établit le schéma d'adressage (adresse IP), et prévoit l'acheminement des datagrammes entre réseaux. IP est dit produire un « datagram delivery service » (service de livraison de datagramme).
- UDP = User Datagram Protocol = « connectionless », fournit aux application (DNS, NFS, etc.) un accès en IP directe leur permettant d'échanger des information sur le réseau avec un minimum d'effort au niveau du protocole. UDP n'offre aucune garanti que les paquets sont biens arrivés à leur destination. Les applications doivent gérées les erreurs réseaux (paquets perdus ou erreur dans l'ordre).
- ICMP = Internet Control Message Protocol = « connectionless », échange des informations de contrôle sur le réseau. Utilisé par la commande « ping », il utilise les datagrammes pour ces

différentes fonctions :
  - flow control = Le système qui reçoit peut envoyer un message via ICMP pour l'informer que le système est trop encombré. La connexion est ainsi arrêté temporairement et les datagrammes ne sont plus envoyés
  - Détection de destination « unreachable » = Plusieurs éléments du réseau peuvent déterminer si une destination est valide ou non. ICMP permet d'interroger le bon système.
  - Redirection de routes réseaux = ICMP est utilisé en amont pour prévenir un expéditeur de datagramme d'utiliser une autre passerelle
  - Vérification de l'hôte distant = L'hôte peut envoyer un message par la commande « echo » afin de vérifier que la couche IP fonctionne sur l'hôte distant
- PPP = Utiliser pour des communications TCP/IP à travers un modem

17.6 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 et 21	FTP	Les données transitent par le port 20 et les informations de contrôles par le port 21
22	SSH	
23	Serveur Telnet	
25	Serveur SMTP	
53	Serveur DNS	
67	Serveur BootTP et DHCP	
80	Serveur HTTP	
110	POP3	
119	NNTP	Serveur de news
123	NTP	
143	IMAP	
514	Syslog	

17.7 Utilitaires réseaux

17.7.1 ftp

ftp -i hote_distant ↵ = Ouvre une connexion FTP vers l'hôte distant, mais sans mode interactif (= « -i »)
ftp-v hote_distant ↵ = Ouvre une connexion FTP vers l'hôte distant, en mode verbeux (= « -v »)

Commandes FTP :

- ascii ou binary = Passe en mode ASCII ou binaire. Le mode ACSII permet de transférer correctement du texte entre des systèmes qui encodent leurs caractères de manières différentes.
- get fichier = Demande la réception d'un fichier unique depuis le serveur vers le système local
- mget fichier* = Demande la réception de plusieurs fichiers depuis le serveur
- ls = Liste le contenu du répertoire du serveur
- put fichier = Demande la transmission d'un fichier unique sur le serveur depuis le système local
- mput fichier* = Demande le transfert de plusieurs fichiers
- prompt = Passe du mode interactif au mode non-interactif durant un mput ou un mget
- pwd = Affiche le répertoire courant sur le serveur FTP
- quit ou exit = Termine proprement une session FTP

ftp serveur_ftp ↵ = Établie une connexion FTP interactive
Connected to smp.
220 smp FTP server (Version wu-2.4.2-VR17(1)
Mon Apr 19 09:21:53 EDT 1999) ready.
Name (smp:root): jdean ↵ = Nom du user reconnu par le serveur FTP
331 Password required for jdean. = Le mot de passe du user Jdean est nécessaire
Password: mot_de_passe ↵ = Jdean entre ici son mot de passe
230 User jdean logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls myfile ↵ = Liste les fichiers dont le nom est « myfile »
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
-rw-r--r-- 1 jdean jdean 29 Jan 24 01:28 myfile = Un fichier est trouvé
226 Transfer complete.
ftp> binary ↵ = Passe en mode binaire plutôt qu'en mode ASCII
200 Type set to I.
ftp> get myfile ↵ = Demande la réception du fichier « myfile » sur le système local
local: myfile remote: myfile
200 PORT command successful.
150 Opening BINARY mode data connection for myfile
(29 bytes).
226 Transfer complete.
29 bytes received in 0.000176 secs (1.6e+02 Kbytes/sec) = Les 29 octets du fichier « myfile » ont été bien reçus
ftp> quit ↵ = Termine la session FTP proprement
221-You have transferred 29 bytes in 1 files.
221-Total traffic for this session was 773 bytes in 3 transfers.
221-Thank you for using the FTP service on smp.
221 Goodbye.

ftp -v serveur_ftp ↵ = Établie une connexion FTP interactive en mode verbeux
Connected to smp.
220 smp FTP server (Version wu-2.4.2-VR17(1)
Mon Apr 19 09:21:53 EDT 1999) ready.
Name (smp:root): anonymous ↵ = Le compte « anonymous » n'est pas un user du serveur FTP
331 Guest login OK, send your complete e-mail address as password.
Password: mon@adresse_mail.com ↵ = Le mot de passe pour « anonymous » est son adresse mail perso
230 Guest login OK, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

17.7.2 ping

Envoi un écho en ICMP.
Un datagramme « ICMP ECHO REQUEST » est envoyé à destination d'un hôte distant, et s'attend à une réponse « ECHO_RESPONSE ICMP »

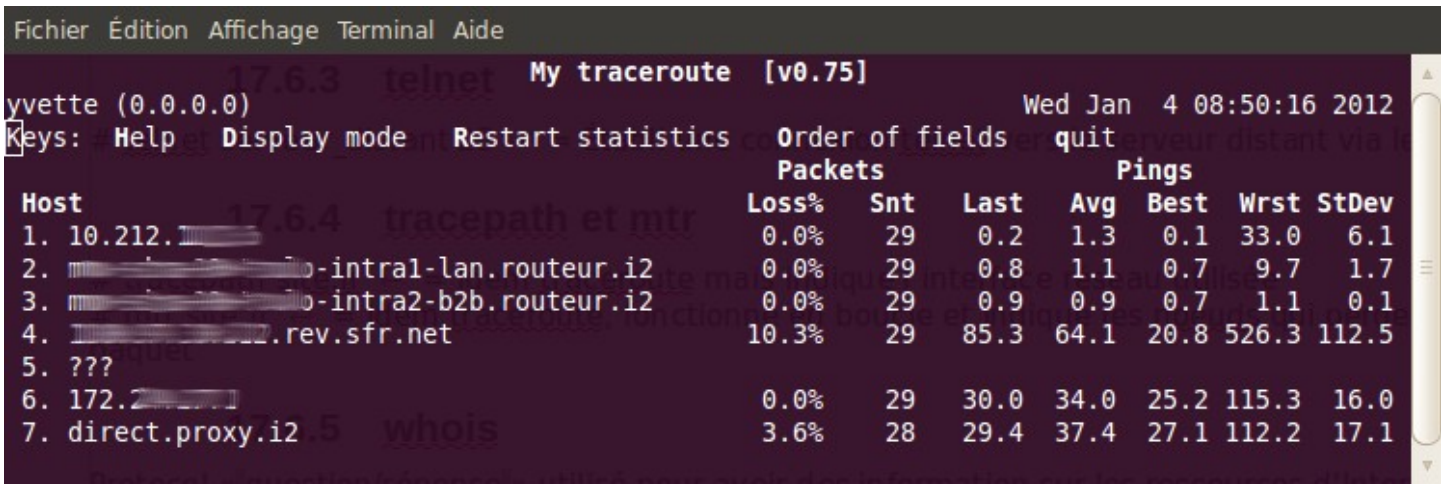
ping -c 5 serveur_distant ↵ = Envoi 5 requêtes (= « -c ») au serveur distant
ping -q serveur_distant ↵ = En mode silencieux (= « -q » = quiet), affiche seulement un condensé de ligne où la commande démarre et celle où la commande se termine

17.7.3 telnet

telnet serveur_distant 23 ↵ = Établi une connexion telnet vers le serveur distant via le port 23

17.7.4 tracepath et mtr

tracepath site.fr ↵ = Idem traceroute mais indique l'interface réseau utilisée
mtr site.fr ↵ = Idem traceroute, fonctionne en boucle et indique les noeuds qui perdent le plus de paquet



17.7.5 whois

Protocol « question/réponse » utilisé pour avoir des information sur les ressources d'Internet. Ces informations sont :
le contact
les noms de domaine
les adresses IP
les serveurs DNS
whois claveau.net ↵ = Recherche des informations sur le site web claveau.net

18 Configuration réseau

18.1 Interfaces réseau

18.1.1 Fichiers de configuration

- /etc/hosts = Contient une liste d'adresse IP mis en relation avec des noms de machines. C'est le 1er fichier utilisé pour la résolution de nom. Cela peut-être suffisant pour un petit réseau
- /etc/nsswitch.conf = Certains programmes fonctionnant en réseau, notamment pour la résolution de nom, peuvent utiliser ce fichier pour connaître quel fichier de configuration utiliser pour le routage réseau (fichier hosts, DNS, annuaire LDAP, etc.)
  # traceroute -n site.fr ↵ = Permet à traceroute de travailler en numérique (adresse IP) et non par nom d'hote, et donc de passer outre le fichier /net/nsswitch
  Chaque entrée du fichier est composée : base: source1 [action] source2 [action]
  Le bases est l'objet de votre recherche:
  hosts: Résoudre le nom d'une machine sur le réseau
  network: Résoudre le nom d'un réseau
  group: Résoudre le nom d'un groupe d'utilisateurs
  passwd: Résoudre le nom d'un utilisateur
  shells: Résoudre le nom d'un interpréteur de commandes.
  sources
  files: fichiers disponibles en local : /etc/hosts , /etc/passwd , /etc/shells
  dns: Serveur de domaine
  nis: annuaire réseau
  Les actions sont l'attitude à adopter selon les réponses d'une source. Soit interroger la source suivante (continue), soit cesser la consultation (return).
  [status=action]
  Les «status» peuvent être :
  success: La source a résolu la demande.
  notfound: La source n'a pas reconnu le nom demandé.
  tryagain: La source est débordée, essayez plus tard.
  unavail: La source n'a pas répondu.

  hosts: files [success=return] dns = La recherche d'un nom de machine s'effectuera d'abord dans le fichiers /etc/hosts, puis, si la recherche est infructueuse, le système interroge le DNS.
  passwd: nis [unavail=continue] files = Les fichiers locaux ne sont interrogés que si l'annuaire NIS est indisponible, par exemple s'il a été coupé.

- /etc/host.conf = Permet de contrôler la résolution de noms pour les système pré-glibc2. On utilisera plutôt /etc/nsswitch.conf
  order hosts,bind = Le fichier /etc/hosts est lu en premier puis le DNS
  multi on = Permet plusieurs adresses IP par hôte
- /etc/resolv.conf = Permet de contrôler la partie DNS coté client. Désigne entre autre l'adresse IP du serveur DNS
  nameserver 192.168.1.5
  nameserver 192.168.250.2
- /etc/networks = Comme pour le fichier /etc/hosts, il met en relation des adresses et des noms, mais ici les adresses représentent des réseaux entiers. C'est pratique pour du NFS ou la configuration des routes réseaux. La commande « netstat » utilise ce fichier.
  loopback 127.0.0.0
  mylan 192.168.1.0

18.2 Configuration réseau standard

1. Installez une carte réseau Ethernet. Utilisez lsmod, lspci et dmesg pour résoudre les conflits matériels
2. Attribuez une adresse IP et son masque à une interface réseau (par exemple eth0). Ils peuvent être fixés manuellement ou via un serveur DHCP.
   Sur une distribution RedHat, le fichier de configuration est /etc/sysconfig/network-scripts/ifcfg-eth0. Le contenu de ce fichier est lu par le script de démarrage /etc/init.d/network. Ce script appel à son tour la commande ifconfig avec les bons paramètres.
3. Configurez la passerelle par défaut afin de communiquer avec d'autres sous-réseaux, dans le fichier /etc/sysconfig/network. Le contenu de ce fichier est lu par le script de démarrage /etc/init.d/network. Ce script appel à son tour la commande route pour configurer la passerelle par défaut.
4. Configurez un serveur DNS dans le fichier /etc/resolv.conf

18.2.1 Configuration d'un système RedHat

Les paramètres du réseau sont placés sous /etc/sysconfig pour RedHat
/etc/sysconfig/network est le fichier générique

NETWORKING=yes = Lance l'interface réseau au démarrage
HOSTNAME=portable_david
GATEWAY=... = Ancienne version, maintenant dans le fichier /etc/sysconfignetwork-script/ifcfg-eth0

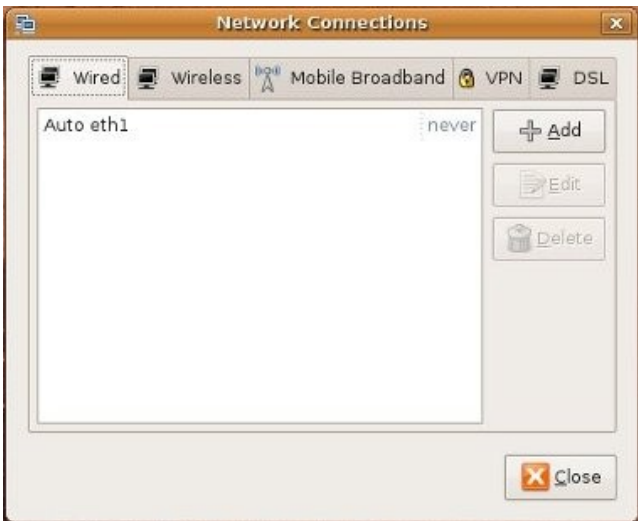
hostname ↵ = Affiche le contenu de la directive « HOSTNAME » du fichier /etc/syscofig/network

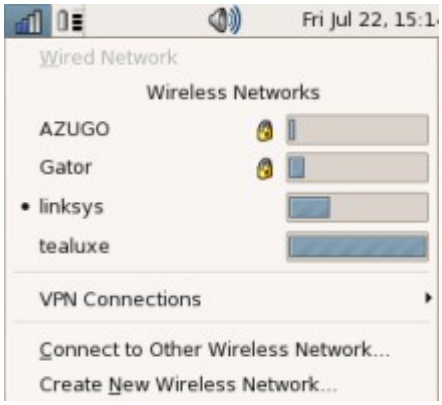
/etc/sysconfig/network-script/ifcfg-eth0 = Fichier de configuration de l'interface réseau eth0

BOOTPROTO=static ou none = Configuration manuelle
bootp = Configuration par bootp = DHCP sans bail
dhcp
HWADRESS=... = Facultatif, sauf en cas de plusieurs interfactes sur la même carte
BROADCAST=... = Facultatif et obsolète, la valeur est maintenant calculée automatiquement
NETWORK=... = Facultatif et obsolète, la valeur est maintenant calculée automatiquement
GATEWAY=... = Passerelle (plutôt que dans le fichier /etc/sysconfig/network)

18.2.2 Configuration d'un système Debian

Les paramètres du réseau sont placés sous /etc/default pour Debian.
/etc/sysconfig/interfaces est le fichier générique
L'utilitaire « Network Manager » configure automatiquement le réseau et courcircuite le fichier /interfaces :





18.2.3 Accès d'un navigateur à une page Web

Voici un exemple de ce qui se passe «en coulisses» lorsqu'un navigateur Web demande une page Web à partir d'un serveur distant:

1. L'utilisateur tape « http://www.claveau.net » sur son navigateur
2. Le système doit résoudre le nom en une adresse IP. Le fichier /etc/nsswitch (/etc/host.conf pour un système pré-glibc2) est consulté pour déterminer quel système interroger. Ce fichier est configuré comme suit :
   hosts: files dns = Pour la recherche d'un hôte, on interroge d'abord le fichier /etc/hosts puis le DNS
3. Si il y a une entrée dans le fichier /etc/hosts pour « www.claveau.net », alors c'est l'adresse IP inscrite en face qui sera utilisé dans la requête HTTP. Sinon, on utilise le DNS
4. Le fichier /etc/resolv.conf est utilisé pour déterminer quel est le serveur DNS primaire à intéroger. Une requête est donc envoyé au DNS et l'adresse IP reçu en retour est utilisée dans la requête HTTP.
   Si il n'y a pas de réponse, le second serveur DNS configuré dans /etc/resolv.conf est utilisé
5. Dans le cas où toutes les possibilités de résoudre le nom sont épuisées, le navigateur affiche une erreur

18.3 Commandes

18.3.1 ifconfig, ifup et ifdown

```
# ifconfig ↵ = Affiche toutes les interfaces valident du système
eth0      Link encap:Ethernet  HWaddr 00:A0:24:D3:C7:21
          inet addr:192.168.1.30  Bcast:192.168.1.255  Mask:255.255.255.0
          ....
lo        Link encap:Local Loopback = Interface de « loopback »
          inet addr:127.0.0.1  Mask:255.0.0.0
          ....

# ifconfig eth0 down ↵ = Désactive l'interface eth0. Les routes associées sont supprimées de la table de
          routage (route pour l'interface et celle de la passerelle)
          Idem mais en gardant en mémoire ces paramètre (RedHat) # ifdown eth0 ↵
# ifconfig eth0 up ↵ = Ré-active l'interface eth0
          Idem mais en ré-appliquant les paramètres sauvegardés (RedHat) # ifup eth0 ↵
# ifconfig eth0 nouvelle_@IP netmask 255.255.0.0 ↵ = Modifie l'adresse IP de eth0
          Idem ...nouvelle_@IP/16 ↵
          La commande # ip peut être utiliser à la place de # ifconfig
# ifconfig eth0:0 10.2.3.177/24 ↵ = Ajoute une adresse IP virtuelle à eth0 appelée eth0:0
# sipcalc 10.1.2.3 255.255.252.0 ↵ = Informe sur les adresses disponibles pour la plage d'adresse IP
          Idem ...10.1.2.3/22 ↵
# ifconfig eth0 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.25 ↵ = configure totalement
l'interface eth0
```

18.3.2 route

```
# route ↵ = Affiche la table de routage
          Idem # route -F ↵
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Met	Ref	Use	Iface	
192.168.1.30	*	255.255.255.255	UH	0	0	0	eth0	= La route du système local utilise eth0 et son masque = / 32
127.0.0.0	*	255.0.0.0	U	0	0	0	lo	
default	gate	0.0.0.0	UG	0	0	0	eth0	= La route par défaut est sur eth0 sans masque (= /0)

route add -host 192.168.1.30 eth0 ↵ = Ajoute la route pour l'interface, nécessaire après « ifconfig ... down »
route add default gw 192.168.1.1 eth0 ↵ = Ajoute la route pour la passerelle par défaut, nécessaire après « ifconfig ... down »

Champs affichés par route :

- Destination = L'hôte ou le réseau de destinations
- Gateway = L'adresse de la passerelle ou bien « * » s'il n'y en a pas
- Genmask = « 255.255.255.255 » est utilisé pour l'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 = Utilise la 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 commande
- Use = Un compte des recherches sur cette route. Indique la route non trouvée dans le cache si l'option « -F » est utilisé, ou bien indique si la route est trouvée avec l'option « -C »
- Iface = Interface où sont envoyés les paquets de cette route

route -C -n -v ↵ = Affiche la table de routage en cache (= « -C »), en mode numérique (= « -n » = sans résoudre les noms) et en mode verbeux (= « -v »)

route add -net default -gw @IP_gateway eth0 ↵ = Enregistre une route où la destination est un réseau (= « -net ») par défaut (= « default ») vers l'adresse IP gateway (= « -gw ») pour eth0.
L'option « -net » est incompatible avec « -host » qui spécifié que la destination est un hôte unique

18.3.3 host

host -l ↵ = Affiche la totalité du domaine présent sur le serveur DNS, ce qui peut prendre beaucoup de temps

host oreilly.com ↵ = Interroge le serveur DNS avec l'adresse IP ou le nom d'hôte du système
oreilly.com has address 208.201.239.37
oreilly.com has address 208.201.239.36

host -v oreilly.com ↵ = Idem mais en mode verbeux

```
Trying "oreilly.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60189
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;oreilly.com.                IN      A

;; ANSWER SECTION:
oreilly.com.         877    IN      A       208.201.239.100
oreilly.com.         877    IN      A       208.201.239.101
```

```
Received 61 bytes from 192.168.1.220#53 in 0 ms
Trying "oreilly.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1045
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;oreilly.com.                   IN      AAAA

;; AUTHORITY SECTION:
oreilly.com. 3577 IN SOA nsautha.oreilly.com. \
        nic-tc.oreilly.com. 86 600 1800 604800

Received 80 bytes from 192.168.1.220#53 in 0 ms
Trying "oreilly.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18547
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;oreilly.com.                   IN      MX

;; ANSWER SECTION:
oreilly.com.            3577    IN      MX      20 smtp1.oreilly.com.
oreilly.com.            3577    IN      MX      20 smtp2.oreilly.com.

;; ADDITIONAL SECTION:
smtp1.oreilly.com.      3577    IN      A       209.204.146.22
smtp2.oreilly.com.      3577    IN      A       216.204.211.22
Received 105 bytes from 192.168.1.220#53 in 0 ms
```

18.3.4 dig

Utilitaire DNS. Il utilise le serrveur DNS par défaut défini dans /etc/resolv.conf

```
# dig www.oreilly.com ↵ = Interroge le serveur DNS par défaut pour le site  www.oreilly.com
; <<>> DiG 9.4.3-P1 <<>> www.oreilly.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17863
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.oreilly.com.        IN      A

;; ANSWER SECTION:
www.oreilly.com.    161     IN      CNAME   oreilly.com.
oreilly.com.        448     IN      A       100.201.239.100
oreilly.com.        448     IN      A       100.201.239.101

;; Query time: 4 msec
;; SERVER: 100.100.0.43#53(100.100.0.43)
;; WHEN: Mon Dec 14 14:48:55 2009
;; MSG SIZE  rcvd: 79

  # dig @10.20.10.10 www.oreilly.com ↵ = Interroge le serveur DNS 10.20.1010 (qui n'est pas celui par
        défaut) grâce au « @ »
; <<>> DiG 9.4.3-P1 <<>> www.oreilly.com
. . . . .
;; SERVER: 10.20.10.10#53(10.20.10.10)
;; WHEN: Mon Dec 14 14:48:55 2009
;; MSG SIZE  rcvd: 79
```

Les enregistrements inverses sont configurés en même temps que le nouvel enregistrement. Ils permettent de relier une adresse IP à un nom. S'ils manquent, certains services ne peuvent plus

fonctionner (comme SSH). La commande peut valider que le PTR d'un site est valide.
dig –x 208.201.239.100 ↵ = Interroge le serveur DNS sur les enregistrements PTR (inverse).
```
; <<>> DiG 9.4.3-P1 <<>> -x 208.201.239.100
. . . . .

;; QUESTION SECTION:
;100.239.201.208.in-addr.arpa.    IN    PTR

;; ANSWER SECTION:
100.239.201.208.in-addr.arpa. 3600 IN    PTR    oreilly.com.
. . . . .
```

dig mx www.oreilly.com ↵ = Recherche l'enregistrement MX (mail exhange) pour le domaine oreilly.com
```
; <<>> DiG 9.4.3-P1 <<>> mx oreilly.com
. . . . .

;; QUESTION SECTION:
;oreilly.com.           IN    MX

;; ANSWER SECTION:
oreilly.com.       3600    IN    MX    20 smtp10.oreilly.com.
oreilly.com.       3600    IN    MX    20 smtp20.oreilly.com.
. . . . .
```

18.3.5 traceroute

Affiche la route réseau que les paquets prennent afin d'arriver à leur destination. Traceroute et ping peuvent fonctionner en IPV6
Le principe de fonctionnement de Traceroute consiste à envoyer des paquetsUDP avec un paramètre Time-To-Live (TTL) de plus en plus grand (en commençant à 1). Chaque routeur qui reçoit un paquet IP en décrémente le TTL avant de le transmettre. Lorsque le TTL atteint 0, le routeur émet un paquet ICMP d'erreur « Time to live exceeded »vers la source. Traceroute découvre ainsi les routeurs de proche en proche.

Il existe cependant un certain nombre d'éléments qui peuvent compliquer l'interprétation du résultat :

- le chemin suivi par les paquets peut être asymétrique et traceroute ne montre que l'aller ;
- le chemin suivi peut être radicalement différent depuis un autre point, même proche géographiquement ;
- les routeurs émettent le paquet ICMP avec l'adresse source de l'interface utilisée pour vous joindre. Si vous avez plusieurs interfaces réseau, ce n'est pas forcément l'interface par laquelle votre paquet sonde est passé ;
- les routeurs ne traitent pas nécessairement les paquets ICMP en transit de la même façon que le trafic de données. Les temps de réponse peuvent ne pas refléter ceux que l'on observerait au niveau du trafic applicatif. Ce sera particulièrement le cas si le réseau fait usage de qualité de service
- la création du paquet ICMP « TTL exceeded » est une opération complexe qui sollicite le CPU du routeur, alors que le trafic est habituellement traité au niveau du matériel spécialisé. Il se peut qu'un délai supplémentaire soit observé si le CPU est occupé à d'autres tâches plus essentielles (gestion des tables de routage, traitement des requêtes de gestion du réseau)
- un routeur peut ne pas répondre aux requêtes ICMP. Dans ce cas, on voit généralement des signes astérisques (*) sur les nœuds intermédiaires qui ne répondent pas aux requêtes ICMP. Il se peut aussi que, pour des raisons de performance, le routeur limite le nombre de paquets ICMP généré par unité de temps, ce qui cause l'apparition d'étoiles sur le parcours, qui ne sont cependant pas le symptôme d'un problème.
- l'adresse IP de la réponse ICMP TTL Exceeded peut être privée (RFC 1918), et donc bloquée en cas de transit par Internet, ou impossible à identifier.

traceroute -f 2 -n -v site.fr ↵ = Tente de relier site.fr, avec un TTL initial (= « -f ») de 2 (au lieu de 1 par défaut), en mode verbeux (= « -v ») et en mode numérique (= « -n ») pour n'afficher que les adresse et pas les noms

traceroute -w 10 site.fr ↵ = Tente de relier le site.fr en fixant le délai de timeout à 10 secondes plutôt que 5 par défaut pour la réponse ICMP

traceroute site.fr ↵ = Tente de relier le site.fr en affichant tous les noeuds réseau traversés
traceroute to site.fr (24.215.7.162), 30 hops max, 40 byte packets
1 96.64.11.1 (96.64.11.1) 12.689 ms 5.018 ms 9.861 ms = Chaque ligne est numérotée par son TTL initial
2 ge-1-28-ur01.comcast.net (68.85.20.18) 8.712 ms * 10.868 ms = Le signe « * » montre que la passerelle ne revoi pas le message « time exceeded » ou bien qu'elle le revoie mais fixe une valeur de TTL très basse
3 te-8-1-ar01.comcast.net (68.86.136.30) 15.109 ms 6.932 ms 24.996 ms
4 * te-0-8-0-4-crs01.b0atlanta.ga.atlanta.comcast.net (68.85.232.97) 41.966 ms 51.914 ms
5 24.215.7.110 (24.215.7.110) 50.487 ms 114.975 ms 44.655 ms
6 site.fr (24.215.7.162) 54.705 ms 84.838 ms 46.562 ms = Il y a eu 5 sauts pour atteindre site.fr puisque la dernière valeur de TTL = 6

18.3.6 netstat

Suivant le options, netstat affiche les connexions réseau, la table de routage, des statistiques sur les interfaces réseau, les connexions masquées et les membres du multicast.

netstat -i -c ↵ = Affiche les interfaces réseau et leurs statistiques (= « -i »), en mode « continus » (= « -c ») ce qui permet d'afficher le résultat toutes les secondes

```
Kernel Interface table
Iface   MTU   Met    RX-OK        RX-ERR      RX-DRP      RX-OVR          TX-OK
eth0    1500  0      1518801      37          0           0               713297
lo      3924  0      365816       0           0           0               365816
```

netstat -an --tcp ↵ = Affiche les connexions actives (= « -a »), en mode numérique (= « -n ») et seulement les connexions TCP

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address      Foreign Address      State
tcp        0      0 0.0.0.0:34031      0.0.0.0:*           LISTEN
tcp        0      0 0.0.0.0:6000       0.0.0.0:*           LISTEN
tcp        0      0 127.0.0.1:631      0.0.0.0:*           LISTEN
tcp        1      0 10.41.81.148:59667  10.41.0.47:3268     CLOSE_WAIT
tcp        0      0 10.41.81.148:42262  74.125.77.83:443    ESTABLISHED
tcp        0      0 10.41.81.148:46150  212.100.160.43:5222  ESTABLISHED
tcp        0      0 :::6000             :::*                LISTEN
udp        0      0 127.0.0.1:46958     0.0.0.0:*
udp        0      0 0.0.0.0:34031       0.0.0.0:*
```

netstat -p -v ↵ = Affiche en mode verbeux (= « -v ») le PID et le nom des processus (= « -p » = mode programme) auquel appartient chaque socket, afin de déterminer quel processus pose problème

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 server01.domain.:60032 ew-in-f18.1e100.n:https ESTABLISHED 4698/firefox-bin
tcp 0 0 server01.domain.:40343 messaging.n:xmpp-client ESTABLISHED 4680/pidgin
tcp 0 0 server01.domain.:53533 srdc-mail-01 :imap ESTABLISHED 4679/evolution
```

netstat -r ↵ = Affiche la table de routage (= « -r » = mode route) dans le format de la commande « route »

18.3.7 ethtool

ethtool est utilisé pour le diagnostique

ethtool eth0 ↵ = Affiche des informations sur la connexion eth0

```
Settings for eth0:
Supported ports: [ TP MII ]
Supported link modes: 10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
Supports auto-negotiation: Yes
Advertised link modes: 10baseT/Half 10baseT/Full
100baseT/Half 100baseT/Full
Advertised auto-negotiation: Yes
```

Speed: 10Mb/s Duplex: Half
Port: MII
PHYAD: 32
Transceiver: internal
Auto-negotiation: on
Supports Wake-on: pumbg
Wake-on: d
Current message level: 0x00000007 (7)
Link detected: yes

ethtool -p eth0 ↵ = Fait clignoter la LED de la carte eth0
ethtool -i eth0 ↵ = Affiche les informations sur le driver de la carte eth0 = module kernel
ethtool -s eth0 speed 100 duplex full ↵ = Modifie les paramètres de la carte eth0 (= « -s »), ici en 100 Mbps full duplex

18.4 DHCP

Le DHCP (Dynamic Host Configuration Protocol) est une extension du protocole BootTP. Il permet l'attribution automatique d'une adresse IP à un hôte du réseau, mais aussi du serveur DNS, de la passerelle et d'autres éléments réseaux spécifiques à l'architecture.

18.4.1 Récupération de l'adresse

Elle peut-être faite de 3 manières :

- Allocation dynamique = L'administrateur maintien une liste d'adresse IP sur le serveur DHCP. Le serveur se sert dans cette liste pour assigner une adresse IP à un nouvel hôte. Elle peut être utilisée ou louée pour une certaine période. Afin de garder son adresse IP après le délai, le client renégocie avec le serveur DHCP. Une fois la location terminée, l'adresse IP est replacée dans la liste afin qu'elle soit ré-attribuée à un autre hôte.
- Allocation manuelle = L'administrateur peut désigner certaines adresses IP pour certaines interfaces réseau spécifiques (adresse MAC par exemple). Cela permet d'avoir la facilité du serveur DHCP pour l'attribution de l'adresse IP tout en gardant la maîtrise de quelle adresse IP va à quel hôte.
- Allocation automatique = Le serveur DHCP ne sert qu'à attribuer une adresse IP à un hôte. Le délai de location est infini.

18.4.2 Fonctionnement du serveur DHCP

1. Le client DHCP envoi un massage en broadcast afin de déterminer qui est le serveur DHCP
2. Le ou les serveur(s) DHCP répondent via leur brodcast
3. Le client choisi un serveur DHCP et envoi une validation au serveur sélectionné
4. Le serveur valide à son tour. Les autres serveurs DHCP ne font rien car le client à décliné leur offre

18.4.3 Sous-réseaux et relais

La communication DHCP est initiée en broadcast, elle est restreinte à un réseau simple. Lorsque les serveurs DHCP sont dans un sous-réseau, on utilise des relais. Ils écoutent les messages DHCP en broadcast sur un sous-réseau et les transmettent aux serveurs situés dans un autre sous-réseau. Pareil au retour du broadcast.

18.4.4 Location

L'adresse IP est louée au client DHCP par le serveur pour une durée définit d'1 ou plusieurs jours. Une durée courte favorise le turn-over des adresses, par exemple lorsqu'il n'y a pas assez d'adresse pour tous les postes en même temps, ou bien lorsque le parc de machine est composé d'un nombre important d'appareils mobiles.
Une durée plus longue permet de réduire l'activité du serveur DHCP et de réduire le broadcast sur le réseau.
Si l'adresse n'est pas renégociée avant la fin de la location, le système hôte (client DHCP) devient invalide et son adresse IP retourne dans le pool d'adresses disponibles.
La location peut se terminer par le client s'il n'en a plus besoin. Le serveur DHCP place alors l'adresse IP ainsi libérée dans le pool.

18.4.5 dhcpd

Le processus du serveur DHCP est dhcpd (dhcpcd = processus du client). Il démarre au démarrage et écoute les demandes en broadcast. Il peut servir pour différents sous-réseaux via différentes interfaces.
Fichier de configuration = /etc/dhcpd.conf :
subnet 192.168.0.0 netmask 255.255.255.0 { = Paramètres réseaux pour ce sous-réseau, transmis au client DHCP
range 192.168.1.200 192.168.1.204; = Plage des adresses IP disponibles = 5 adresses (entre .200 et .204)

```
        default-lease-time 600;  =  Temps de location par défaut en seconde = 10 minutes
        option subnet-mask 255.255.255.0;  =  Masque de sous réseau
        option broadcast-address 192.168.1.255;  =  Adresse de broadcast
        option routers 192.168.1.1;  =  Adresse du routeur = passerelle
        option domain-name-servers 192.168.1.25;  =  Adresse du DNS
subnet 10.10.0.0 netmask 255.255.0.0 {  =  Paramètres d'un aute sous-réseau
        autre paramètres ...
        autre paramètres ...
}
```

Le fichier des location est également nécessaire à dhcpd : /var/state/dhcp/dhcpd.leases ou /var/lib/dhcp/dhcpd.leases
Le démon se lance de lui-même en backgroud

dhcpd -cf fichier_config ↵ = Lance dhcpd avec un auter fichier de configuration autre que /etc/dhcpd.conf
dhcpd -lf fichier_loc ↵ = Lance dhcpd avec un autre fichier de location autre que celui par défaut
dhcpd -q eth1 ↵ = Lance dhcpd en mode silencieux (= « -q » = quiet). Cela supprime le message sur le copyright et rend plus léger des fichiers de logs. dhcpd n'écoutera que sur l'interface eth1 plutôt que toutes les interfaces (par défaut)

La sortie standard de dhcpd est redirigée vers syslog :

```
Apr 24 02:27:00 rh62 dhcpd: DHCPDISCOVER from 00:60:97:93:f6:8a via eth0
Apr 24 02:27:00 rh62 dhcpd: DHCPOFFER on 192.168.1.200 to 00:60:97:93:f6:8a via eth0
Apr 24 02:27:01 rh62 dhcpd: DHCPREQUEST for 192.168.1.200 from 00:60:97:93:f6:8a via eth0
Apr 24 02:27:01 rh62 dhcpd: DHCPACK on 192.168.1.200 to 00:60:97:93:f6:8a via eth0
```

19 Sécurité

19.1 Insécurité du SUID

Sujet initié dans le chapitre « Écrire de simple script / SUID et GUID »

Le droit SUID ou SGID permet d'utiliser le fichier avec les droits du user ou du groupe du fichier.
Si un programme a un droit SUID, il s'exécute sous les droits du propriétaire du programme (par exemple root), plutôt que sous les droits du user qui le lance.
Pour VI cela est dangereux dans le sens où un user lançant VI qui aurait le droit SUID root pourrait modifier n'importe quel fichier du système (comme root). Ce user pourrait également ouvrir un shell dans VI et exécuter n'importe quel commande (comme root).

find /bin -perm -4000 -type f ↵ = Permet de connaître tous les fichiers (= « -type f ») ayant un droit SUID (= « perm 4000 »)
        Idem # find /bin -perm -u=s -type f ↵

```
/bin/mount
/bin/su
/bin/ping
/bin/ping6
/bin/umount
/bin/fusermount
```

19.2 su

su (= substitute user) permet de lancer un shell en tant qu'un autre user/groupe.
C'est surtout utilisé pour qu'un user « devienne » root, mais aussi pour que root « devienne » utilisateur standard.

su user ↵ = Ne lit pas les scripts d'initialisation
su - user ↵ = Lit les scripts d'initialisation (= « - »)
su -c commande ↵ = Lance la commande en tant que root. Pratique pour les scripts

$ wc -l /etc/shadow ↵ = Lance la commande « wc » sur le fichier /etc/shadow en tant que user standard
wc: /etc/shadow: Permission denied = Un user n'a pas les droits suffisants

$ su -c wc -l "/etc/shadow" ↵ = Lance la même commande (= « -c ») mais en tant que root (= « - »)

Password: mot_passe_root ↵ = Demande le mot de passe de root
48 /etc/shadow = La commande « wc » se déroule normalement car exécuté en tant que root

$ whoami ↵ = Demande le nom du user
adam
$ su ↵ = Devient root mais sans récupérer ses variables d'environnement (PATH, etc)
Password: mot_passe_root ↵ = Demande le mot de passe de root
$ whoami ↵ = Demande le nom du user
root
fdisk –l /dev/sda ↵ = Lance la commande « fdisk » mais avec les chemins du PATH pour le user adam
bash: fdisk: command not found = La commande n'est pas trouvée
# exit ↵ = Quitte le schell « root » et re-devient « adam »
$ su – ↵ = Devient root en récupérant toutes ses variables
Password: mot_passe_root ↵ = Demande le mot de passe de root
$ whoami ↵ = Demande le nom du user
root
fdisk –l /dev/sda ↵ = Lance la commande « fdisk » mais avec les chemins par défaut de root
Disk /dev/sda: 200.0 GB, 200049647616 bytes
....etc....

19.3 sudo

Un utilisateur a un UID, un RUID (Real user IN, user qui a lancé la commande) et un EUID (Effectif user ID, sous lequel la commande est lancée)
sudo -s ↵ = substitute user do = Permet de lancer une commande en tant que root ou d'un autre user.
Idem # sudo -i ↵

Fichier de configuration : /etc/sudoers
La commande est utilisée lorsque que l'on souhaite donner à un user standard la possibilité de lancer une commande particulière en tant que root (ou d'un autre user). Une fois configuré dans le fichier /etc/sudoers, l'utilisateur utilise son propre mot de passe pour lancer cette commande particulière, pas besoin de lui donner le mot de passe root.
Toutes les commandes exécutées (et même celles qui sont justes tentées) sont loguées
On peut configurer le fichier /etc/sudoers en ne déclarant qu'un compte utilisateur bien précis, un groupe, une machine ou bien un nom de chemin
Le fichier de configuration peut être transposable sur différents systèmes
Attention de mentionner les chemin exacts pour accéder aux programmes.

visudo ↵ = Permet d'affiche le fichier sudoers en toute sécurité. Il affiche une erreur lorsque le chemin des programmes n'est pas correct

```
# Format is:
# user    MACHINE=COMMANDS
# The COMMANDS section may have other options added to it.

Defaults    requiretty,passwd_timeout=10

# Allows members of the users group to mount and unmount the cdrom as root
%users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

# Allow the user adam to run the dumpe2fs command on any locally attached disk using scsi emulation (/dev/sd*)
# on the computer 'fileserv', don't prompt for a password
adam   fileserv=NOPASSWD: /sbin/dumpe2fs /dev/sd*
```

= Permet à « adam » de lancer la commande dumpe2fs sans indiquer son mot de passe. Pratique pour les scripts.
Sans cette option, « adam » doit indiquer la 1ère fois son mot de passe, il est ensuite mis en cache.

Fichier de log :
Par défaut, c'est syslog qui logue tous les événements de sudo (si l'accès est réussi ou non)

Dec 4 15:07:20 fileserv **sudo**: **adam** : TTY=pts/0 ; PWD=/sbin ; USER=**root** ; COMMAND=/sbin/**dumpe2fs** /dev/sda3
= « adam » a réussi à lancer la commande dump2fs en tant que root grâce à sudo

Dec 4 15:27:29 fileserv **sudo**: **joe** : **user NOT in sudoers** ; TTY=pts/0 ; PWD=/home/joe ; USER=**root** ; COMMAND=**/bin/ls /tmp** = L'utilisateur « joe » à tenté de lancer la commande « /bin/ls /tmp » ce qui lui a été interdit

19.4 Les UID et les mots de passe

19.4.1 usermod

Permet de maintenir les fichiers /etc/passwd, /etc/group et par extension /etc/shadow et /etc/gshadow
La commande accepte les même options que « useradd ».

usermod -l david2 david ↵ = Change le nom d'utilisateur david → david2, mais le répertoire personnel ne change pas
usermod -g 888 david ↵ = Change le GID du groupe principal
usermod -G 889,890,891 david ↵ = Change le GID des groupes secondaires
usermod -G -a 892 david ↵ = Ajoute le GID 892 en groupe secondaire
usermod -d /home/david2 david ↵ = Change le répertoire de travail de david
usermod -c ''Autre commentaire'' david ↵ = Change le commentaire pour le user « david »

usermod -L david ↵ = Verrouille le compte (= « -L » = lock)
Débloque le compte # usermod -U david ↵

19.5 Mots de passe cachés

Le 2ème champ du fichier /etc/passwd est un « x », car auparavant ce champ stockait le mot de passe crypté des comptes.
Le cryptage est de type « one way hash », de sorte qu'il est facile de crypter une chaine de caractère mais mathématiquement très compliqué de faire le travail inverse.
Pour que le système vérifie que vous avez tapés le bon mot de passe :

1. Le prompt demande à l'utilisateur de rentrer son mot de passe
2. Le système regarde dans /etc/passwd si le compte est bien existant
3. Si c'est le cas, le système crypte le mot de passe entré par l'utilisateur
4. Le système compare alors le fichier ainsi crypté avec celui stocké dans /etc/passwd

Le problème est que tous les utilisateurs peuvent lire le fichier /etc/passwd et un utilisateur pourrait alors encrypter un nombre important de chaîne de caractère pour les comparer et ainsi déterminer les mots de passe stockés dans /etc/passwd. S'il est patient, cela peut fonctionner = attaque par force brute

Les mots de passe ont alors été déplacés dans un fichier qui n'est pas en lecture pour tout le monde : /etc/shadow
Seul root peut lire ce fichier. Les champs du fichier sont :

- Nom de l'utilisateur = Doit correspondre à une entrée dans /etc/apsswd
- Mot de passe crypté =
  - « ! » ou « nul » = Ce compte n'a pas de mot de passe
  - « * » = Ce compte est dé-validé
  - «!mot_de_passe_crypté » = Le compte est bloqué
  - « !! » = Le mot de passe n'a jamais été enregistré
- Dernier changement = En nombre de jour
- Minimum = Nombre de jour (depuis le 1/1/1970) avant que l'utilisateur ne puisse plus changer son mot de passe. Si 0 = l'utilisateur peut changer son mot de passe n'importe quand
- Maximum = Nombre de jour maximum avant que l'utilisateur change son mot de passe.
- Warning = Nombre de jour avant l'expiration du mot de passe pour qu'une alerte soit envoyée à l'utilisateur
- Inactif = Nombre de jour avant que le compte soit dé-validé
- Expiration = Nombre de jour (depuis le 1/1/1970) que le compte a été dé-validé
- Champ réservé

root:$1$8jp/RdHb$D1x/6Xr2.puE0NX3nIgdX/:14617:0:99999:7:::
bin:*:13993:0:99999:7:::
daemon:*:13993:0:99999:7:::
adm:*:13993:0:99999:7:::
lp:*:13993:0:99999:7:::
adamh:1IqH21LHP$BJPha9o6/XoOsSoJfWLfZ0:14617:0:99999:7:::

19.5.1 chage

chage = change + age. Permet de maintenir un mot de passe dans la limite d'age (en jour) définie par le maximum et le minimum du fichier /etc/shadow

chage -l root ↵ = Affiche des informations sur l'age du mot de passe de root
Last password change : Jan 08, 2010
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7

chage -d 0 david ↵ = Force le user « david » à changer son mot de passe à la prochaine connexion
chage -l david ↵ = Affiche des informations sur l'age du mot de passe de david
Last password change : **password must be changed**
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7

login as: david ↵ = Le user « david » se logue
david@server's password: mot_de_passe ↵
You are required to change your password immediately (root enforced)
Last login: Fri Jan 8 14:50:42 2010 from 10.0.0.112
WARNING: Your password has expired. You must change your password now and login again!
Changing password for user david
(current) UNIX password: mot_de_passe ↵
New UNIX password: nouveau_mdp ↵
Retype new UNIX password: nouveau_mdp ↵

Autres options de chage :

-d nbre_jour = Fixe le nombre de jour depuis lequel le mot de passe a été chagé
-E date_expiration = Fixe la date d'expiration d'un compte
-I jour_inactif = Fixe le nombre de jour d'inactivité d'un compte qui aurait un mot de passe expiré. Doit être fixé avant que le compte expire
-m minimum = Fixe le nombre de jour minimum avant que l'utilisateur puisse changer son mot de passe
-M maximum = Fixe le nombre de jour maximum de validité d'un mot de passe
-W warning = Fixe le nombre de jour avant l'envoi d'une alerte à l'utilisateur, avant l'expiration de son mot de passe
-x 60 = Force le user à changer son mot de passe tous les 60 jours

19.6 Fixer des limites aux utilisateurs

19.6.1 ulimit

Permet de modifier le fichier /etc/security/limits.conf qui fixe certaines limites aux user
Les limites sont hard et soft. Les limites hard sont fixées par root et ne peuvent pas être dépassées
Les limites soft sont aussi fixées par root mais peuvent pas être dépassées temporairement

Fichier /etc/security/limits.conf :

```
# user adamh cannot create a file larger than 200 MB
adamh hard fsize 204800
# user adamh cannot create a file larger than 100 MB
# unless he increases his own ulimit value
adamh soft fsize 102400
# don't create core files for any user unless they
# change this ulimit value for themselves
* soft core 0
# limit all users in the group 'students' to no more
# than 20 processes running at once
```

```
@student hard nproc 20
# limit all users in the group 'faculty' to no more
# than 20 processes running at once, but allow
# them to increase their own limit temporarily
@faculty soft nproc 20
```

```
# ulimit -a ↵  = Affiche toutes les limites en places
core file size              (blocks, -c) 0
data seg size               (kbytes, -d) unlimited
scheduling priority         (-e) 0
file size                   (blocks, -f) unlimited
pending signals             (-i) 8192
max locked memory           (kbytes, -l) 32
max memory size             (kbytes, -m) unlimited
open files                  (-n) 1024
pipe size                   (512 bytes, -p) 8
POSIX message queues        (bytes, -q) 819200
real-time priority          (-r) 0
stack size                  (kbytes, -s) 10240
cpu time                    (seconds, -t) unlimited
max user processes          (-u) 8192
virtual memory              (kbytes, -v) unlimited
file locks                  (-x) unlimited
```

20 Interroger les services du systèmes

20.1 netstat

Suivant les options, la commande donnes des informations conternant :

- Les connexions réseaux (lesquelles existent et dans quelles état elles sont),
- La table de routage,
- Les statistiques des interfaces,
- Les ports ouverts sur le système,

```
# netstat -s ↵  = Affiche les statistiques des protocoles présents sur le réseau
Ip:
    996714394 total packets received
    0 forwarded
.............
Icmp:
    308127 ICMP messages received
    488 input ICMP message failed.
.............
Tcp:
    4092366 active connection openings
    6613024 passive connection openings
.............
Udp:
    30804 packets received
    18657 packets to unknown port received.
.............
TcpExt:
    77483 invalid SYN cookies received
    22981 resets received for embryonic SYN_RECV sockets
.............
```

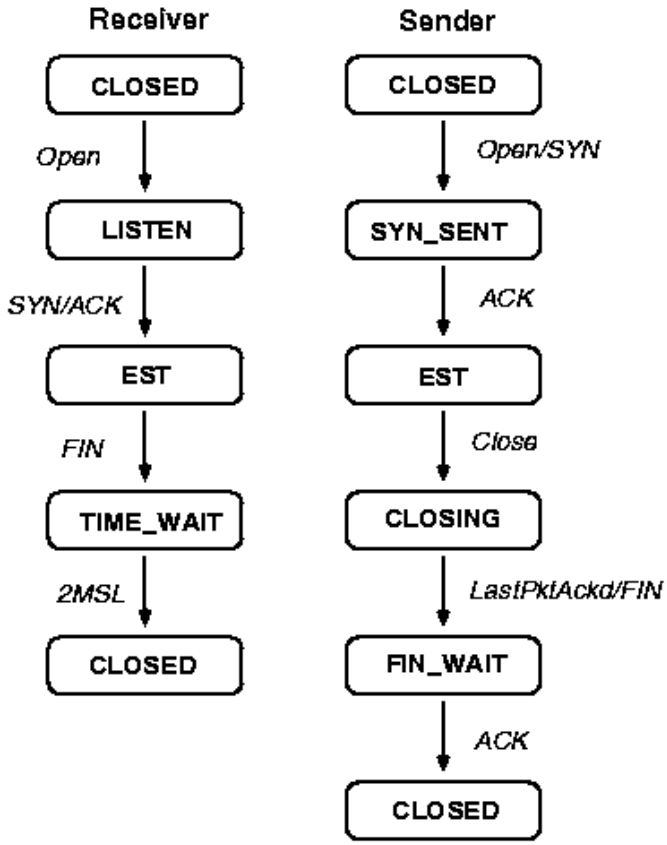
```
# netstat --tcp -n ↵  = Affiche les connexions TCP actives. Le serveur est en 192.168.23.11
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q        Local Address          Foreign Address          State
tcp        0      0        192.168.23.11:80       209.34.195.194:4898      SYN_RECV
tcp        0      0        192.168.23.11:80       71.126.90.107:50254      SYN_RECV
tcp        0      0        192.168.23.11:769   192.168.23.10:2049      ESTABLISHED
```

```
tcp        0      0        192.168.23.11:992      192.168.23.10:2049       ESTABLISHED
tcp        0      0        192.168.23.11:80           66.199.0.164:32211          TIME_WAIT
tcp        0      0 192.168.23.11:80       68.13.184.187:3249     ESTABLISHED
tcp        0      0 192.168.23.11:80       68.13.85.103:2972      TIME_WAIT
tcp        0      0 192.168.23.11:80       70.165.111.157:14068    TIME_WAIT
tcp        0      0 192.168.23.11:80       68.110.27.241:32808     TIME_WAIT
tcp        0      0 192.168.23.11:80       71.199.119.34:49469     TIME_WAIT
.....
```

L'état de la connexion est important : La connexion est créée, les données sont transmises et la connexion est fermée.
L'état « TIME_WAIT » peut signifier qu'une attaque par déni de service est en cours.

Etat d'une connexion :

CLOSED = La connexion est fermée (ou clôturée)
LISTEN = En écoute sur un port pour un connexion entrante
SYN_RCVD = Le signal SYN attend le signal SYNCHRONIZE. Ces signaux sont utilisés pour initier et établir une connexion. Cet état indique que la connexion reçoit des paquets
SYN_SENT = La connexion envoie des paquets
ESTABLISHED = La connexion est maintenant établie. L'établissement cette connexion a eu lieu par l'envoi des 3 signaux pour le handshake
FIN_WAIT_1 = Le signal FIN attend le signal FINISH. Cela indique qu'un des périphériques veux terminer la connexion.
FIN_WAIT_2 = Après qu'un élément d'un bout à l'autre de la connexion ait reçu le signal d'accusé de réception ACK, il se met dans l'état FIN_WAIT_2
CLOSING = La connexion est en cours de fermeture
CLOSE_WAIT = La connexion a envoyé un signal ACK, en réponse au signal FIN
LAST_ACK = Un élément d'un bout à l'autre de la connexion est en cours d'envoi du signal FIN
TIME_WAIT = Après qu'une connexion soit fermée, le noyau garde la connexion dans l'état TIME_WAIT, en attendant les paquets qui ont été retardés. Cela permet de ne pas utiliser une nouvelle socket pour lemême port recevant des données d'une ancienne connexion.



netstat -rn ↵ = Affiche l'état de la table de routage (= « -r ») au format numérique (= « -n »)

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS   Window irtt  Iface
192.168.1.0     *               255.255.255.0   U             1500   0       0    eth0
127.0.0.0       *               255.0.0.0       U       3584  0       0    lo
```

netstat -i ↵ = Affichage de statistiques

```
Iface MTU  Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flags
Lo    3584 0   89    0      0      0      89    0      0      0      BLRU
eth0  1500 0   215   0      0      0      210   0      0      0      BRU
```

netstat -nar --tcp ↵ = Affichage de l'ensemble des connexions (= « -a » = all) en demandant d'obtenir les tables de routage (= « -r ») sans résolution de nom (= « -n » économise des ressources et du temps, surtout que parfois, les résolutions plantent), et uniquement le protocole TCP (= « --tcp » fonctionne aussi avec udp)

```
Local Address                 Remote Address       Swind  Send-Q        Rwind         Recv-Q
        State
*.*                     *.*                     0       0               24576                 0                IDLE
```

```
*.22                *.*                 0      0            24576              0           LISTEN
*.32775             *.*                 0      0            24576              0           LISTEN
*.32776             *.*                 0      0            24576              0           LISTEN
*.*                 *.*                 0      0            24576              0           IDLE
192.168.1.184.22    192.168.1.186.56806      38912 0            24616              0
        ESTABLISHED
192.168.1.184.22    192.168.1.183.58672      18048 0            24616              0
        ESTABLISHED
```

20.2 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
Idem # nmap -sS 192.168.1.220 ↵ = Lance un scan furtif (= « -sS » = stealth SYN scan) contre chaque machine active dans le réseau

nmap -sU 192.168.1.220 ↵ = Idem pour les ports UDP

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-01-14 21:11 CST
Interesting ports on server.domain.com (192.168.1.220):
Not shown: 979 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
.....
3389/tcp  open  ms-term-serv
MAC Address: 00:07:E9:82:6B:D8 (Intel)
Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds
```

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

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-01-14 21:15 CST
Interesting ports on server.domain.com (192.168.1.220):
Not shown: 65512 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
.....
9675/tcp  open  unknown
10000/tcp open  snet-sensor-mgmt
MAC Address: 00:07:E9:82:6B:D8 (Intel)
Nmap done: 1 IP address (1 host up) scanned in 17.80 seconds
```

nmap -O 192.168.1.220 ↵ = Tente de déterminer l'OS

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-01-14 21:18 CST
Interesting ports on server.domain.com (192.168.1.220):
Not shown: 979 closed ports
PORT     STATE SERVICE
42/tcp   open  nameserver
.....
10000/tcp open  snet-sensor-mgmt
MAC Address: 00:07:E9:82:6B:D8 (Intel)
Device type: general purpose
Running: Microsoft Windows 2003
OS details: Microsoft Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
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)
Host router (10.0.0.210) appears to be up.
MAC Address: 00:12:17:30:B4:9C (Cisco-Linksys)
Nmap done: 256 IP addresses (8 hosts up) scanned in 4.928 seconds

nmap -sV ↵ = Teste les ports ouverts pour déterminer le service en écoute et sa version
Starting nmap 3.81 (http://www.insecure.org/nmap/) at 2005-06-07 04:18 CEST
Interesting ports on haypopc (127.0.0.1):

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

Nmap finished: 1 IP address (1 host up) scanned in 0.121 seconds

20.3 lsof

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

pwd ↵ = Affiche quel est le chemin courant
/public
umount /public ↵ = Tente de démonter le partage
umount: /public: device is busy = Le partage est utilisé, il ne peut être démonté
lsof | grep "/public" ↵ = Liste les processus qui ont un fichier ouvert sur le partage

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. Dans cet exemple, notre 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

nmap -u david ↵ = Affiche les fichiers ouverts par l'utilisateur « david »

21 Configuration de la sécurité sur l'hôte : inetd et xinted

Dans le passé, lorsque la consommation mémoire était un enjeux fort, il n'était pas possible de laisser tous les processus utilisant une fonction réseau de la gérer lui-même. la solution a été de trouver un service d'écoute, ou «super-serveur », qui traite les connexions entrantes et démarre le service approprié = inetd
Certains service utilisent leurs propres fonctions réseaux (comme ssh par exemple) = standalone. Sinon ils laissent inetd (ou xinetd) gérer ces fonctions. Inetd apporte des fonctions supplémentaires que les programmes utilisant ces fonctions réseaux n'ont pas développés.
inetd est un processus unique qui limite ainsi la mémoire consommé, et qui permet de contrôler très finement la gestion des connexions réseaux (mieux que les programmes eux-même).

21.1 inetd

Méta-démon inetd = internet deamon
daemon = Disk And Execution MONitor

- écoute sur tous les ports pour charger le processus respectif, avec 1 seul processus
- lance le service concerné par la connexion réseau qui est initiée
- relie la connexion entrante avec le service

Configurer le fichier /etc/inetd.conf ne fait pas démarrer le service (par exemple Imap). C'est le TCP_WRAPPER qui s'en charge

inetd n'a pas de contrôle concernant le nombre de connexion maximale ou le délai entre 2 commandes, notamment pour détecter les attaques en DoS, comme xinetd.

21.1.1 Fichier de configuration /etc/inetd.conf

```
#echo          stream          tcp     nowait          root    internal
#echo          dgram           udp     wait            root    internal
#discard       stream          tcp     nowait          root    internal
#discard       dgram           udp     wait            root    internal
#daytime       stream          tcp     nowait          root    internal
#daytime       dgram           udp     wait            root    internal
#chargen       stream          tcp     nowait          root    internal
#chargen       dgram           udp     wait            root    internal
#time          stream          tcp     nowait          root    internal
#time          dgram           udp     wait            root    internal
#
# These are standard services. = Les services FTP et Telnet sont gérés par inetd
#
ftp             stream          tcp     nowait          root            /usr/sbin/tcpd      in.ftpd -l -a
telnet          stream          tcp     nowait          root            /usr/sbin/tcpd      in.telnetd
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
#shell         stream          tcp     nowait          root    /usr/sbin/tcpd          in.rshd
#login         stream          tcp     nowait          root    /usr/sbin/tcpd          in.rlogind
#exec          stream          tcp     nowait          root    /usr/sbin/tcpd          in.rexecd
#comsat        dgram           udp     wait            root    /usr/sbin/tcpd          in.comsat
#talk          dgram           udp     wait            root    /usr/sbin/tcpd          in.talkd
#ntalk         dgram           udp     wait            root    /usr/sbin/tcpd          in.ntalkd
#dtalk         stream          tcp     wait                    nobody          /usr/sbin/tcpd          in.dtalkd
#
# Pop and imap mail services et al = Le service Imap est géré par inetd
#
#pop-2         stream          tcp     nowait          root    /usr/sbin/tcpd          ipop2d
#pop-3         stream          tcp     nowait          root    /usr/sbin/tcpd          ipop3d
imap            stream          tcp     nowait/10/0/5   root            /usr/sbin/tcpd      imapd = Déclare le service imap avec une limite de 10 connexions simultanées et de 5 connexions de la même IP
# The Internet UUCP service.
#
#uucp                   stream          tcp     nowait          uucp    /usr/sbin/tcpd
        /usr/lib/uucp/uucico -l
#
# Tftp service is provided primarily for booting.  Most site run this only on machines acting as "boot servers.
#" Do not uncomment this unless you *need* it.
#
#tftp                   dgram           udp     wait            root    /usr/sbin/tcpd          in.tftpd
#bootps        dgram           udp     wait            root    /usr/sbin/tcpd          bootpd
#
# Finger, systat and netstat give out user information which may be valuable to potential "system crackers."
# Many sites choose to disable some or all of these services to improve security.
#
#finger        stream          tcp     nowait          root    /usr/sbin/tcpd          in.fingerd
#cfinger       stream          tcp     nowait          root    /usr/sbin/tcpd          in.cfingerd
#systat        stream          tcp     nowait          guest   /usr/sbin/tcpd          /bin/ps -uwwx
#netstat       stream          tcp     nowait          guest   /usr/sbin/tcpd          /bin/netstat -f inet
#
# Authentication
#
#auth                   stream          tcp     nowait          nobody          /usr/sbin/in.identd     in.identd -l -e -o
#
```

```
# End of inetd.conf
```

21.1.2 Champs du fichier /etc/inetd.conf

1. Nom du service : Doit correspondre aux services décrits dans /etc/services. Le nom détermine le n° du port
2. Type de socket : stream (TCP), dgram (UDP), raw ou seqpacket.
3. Protocole :
   tcp ou tcp4 = TCP IPV4
   udp ou udp4 = UDP IPV4
   tcp6 = TCP IPV6
   udp6 = UDP IPV6
   tcp46 = TCP IPV4 ou IPV6
   udp46 = UDP IPV4 ou IPV6
4. Options de connexion : wait ou nowait, max-child, max-connection
5. Utilisateur : Sous quelle user le service doit démarrer
6. Serveur : Chemin complet du service qu'inetd doit lancer
7. Options du serveur : Arguments de la ligne de commande (s'il y a en a) à passer au serveur

21.2 xinetd : eXtend INTErnet Deamon

Remplace inetd en offrant des fonctions supplémentaires :
contrôle d'accès pour des services TCP, UDP et RPC (pour ces derniers, tout ne fonctionne pas très bien) ;

- Contrôle d'accès fondé sur des plages horaires
- Logue puissant, en cas de succès ou d'échec de la connexion
- Prévention efficace contre les attaques de type *Deny of Services* (DoS) qui bloquent une machine en saturant ses ressources : limitations du nombre de serveurs d'un même type qui peuvent tourner en même temps ; limitations du nombre total de serveur ; limitations sur la taille des fichiers de log.
- Attachement d'un service à une interface particulière : ceci permet, par exemple, de rendre des services accessibles à votre réseau interne mais pas au reste du monde ;

21.2.1 Fichier de configuration /etc/xinetd.conf

/etc/xinetd.conf est le fichier de configuration générique :

- Liste les services utilisant xinetd
- Configure les services par défaut s'il n'y a pas de fichier de configuration, mais la plus part des services sont configurés via un fichier individuel sous /etc/xinetd.d (plus pratique pour la configuration)

```
# This is the master xinetd configuration file. Settings in the default section will be inherited by all service configurations
# unless explicitly overridden in the service configuration. See xinetd.conf in the man pages for a more detailed
# explanation of these attributes.
defaults
{
# The next two items are intended to be a quick access place to temporarily enable or disable services.
#       enabled         =
#       disabled        =
# Define general logging characteristics.
        log_type        = SYSLOG daemon info
        log_on_failure          = HOST
        log_on_success  = PID HOST DURATION EXIT

# Define access restriction defaults
#       no_access               =
#       only_from               =
#       max_load                = 0
        cps             = 50 10  =  nombre de connexions par seconde, une fonction strictement xinetd
        instances       = 50
        per_source              = 10

# Address and networking defaults
#       bind            =
#       mdns            = yes
        v6only          = no
```

```
# setup environmental attributes
#       passenv         =
        groups          = yes
        umask           = 002
        service, une fonction strictement xinetd

# Generally, banners are not used. This sets up their global defaults
#       banner          =
#       banner_fail             =
#       banner_success  =
}
includedir /etc/xinetd.d
```

umask = 002 = possibilité de fixer le umask pour la création de fichier par le

Exemple de la configuration du service imap via le fichier /etc/xinetd.d/imap:

```
service imap
{
        socket_type             = stream
        wait                    = no
        user                    = root
        server                  = /usr/sbin/imapd
        log_on_success          += HOST DURATION
        log_on_failure                  += HOST
        disable                 = no
}
```

Détermine si le service est lancé ou non

21.2.2 Champs du fichier /etc/xinetd.conf

- **id =** Nom du service
- **disable =** Détermine si le service est lancé ou non
- **socket_type =**
  - stream (tcp)
  - dgram (udp)
  - raw (accès direct IP)
  - seqpaquet
- **protocol =** Doit être un protocole listé dans le fichier /etc/protocols
- **wait =** Cet attribut détermine si le service est de type mono-thread ou multi-thread. Si la valeur est yes le service est de type mono-thread ; cela signifie que xinetd démarrera le serveur et ne prendra plus en charge aucune requêtes pour ce service jusqu'à l'arrêt du serveur. Si la valeur de l'attribut est no, le service est de type multi-thread et xinetd continuera à prendre en charge les requêtes pour ce service.
- **user =** Nom du user sous lequel le service est lancé
- **type =**
  - INTERNAL = Service pris en charge directement par xinetd
  - RPC = Services décrit dans /etc/rpc
  - UNLISTED = Service ni RPC ni INTERNAL
- **server** : Chemin complet du service qu'inetd doit lancer
- IPv6 = Utilise seulement IPV6
- flags = Les « flags » communs sont :
  - NORETRY = Ne pas ré-essayer dans le cas où le service ne fonctionne pas (service failure)
  - KEEPALIVE = Met le flag « keepalive » pour la socket TCP
  - SENSOR = Ne lance pas le service, mais écoute simplement sur le port et logue toutes tentatives de connexions
  - IPv4 = Utilise seulement IPV4
  - IPv6 = Utilise seulement IPV6
- group = Nom du groupe sous lequel le service est lancé
- instances = Le nombre de services qui peuvent fonctionner en même temps. Par défaut il n'y a pas de limite
- nice = Priorité du processus (valeur de nice)
- server_args = Arguments de la ligne de commande (s'il y a en a) à passer au serveur
- only_from = Permet de limiter l'accès par l'adresse IP, le réseau ou le hostname
- no_access = Interdit l'accès par l'accès par l'adresse IP, le réseau ou le hostname

- access_times = Détermine quelles sont les heures où le serrvice est utilisable : HH:MM – HH:MM
- log_type = SYSLOG ou bien FILE
- log_on_success = Quelles variables sont loguées pour une connexion réussie
- log_on_failure = Quelles variables sont loguées pour une connexion qui échoue
- port = Quel port xinetd doit écouter pour ce service
- bind = Quelle adresse IP xinetd doit écouter pour ce service. Utile pour un serveur hébergeant plusieurs hôtes
- per_source = Nombre de connexion maximum pour une adresse IP unique
- max_load = Permet de ne plus accepter de connexion tant que la charge dy système n'est pas redescendu sous la valeur moyenne de la charge, après 1 minute.

21.3 Service TCP_WRAPPER : Sécurisation par tcpd

xinetd et inetd sont capables d'utiliser le service TCP_WRAPPER pour faciliter le contrôle d'accès. Notamment pour l'accès à des vieux services qui n'intègrent pas d'options avancées concernant ce contrôle d'accès.
Pour utiliser le service TCP_WRAPPER, intetd doit appeler le programme /usr/bin/tcpd dans l'environnement utilisateur, avec comme argument le service à « wrapper » afin de contrôller son accès.

21.3.1 Déterminer si un programme peut utiliser le service TCP_WRAPPER

ldd $(which programme) | grep libwrap ↵ = Pour savoir si un programme utilise la protection du tcp wrappers
libwrap.so.0 => /usr/bin...

Script shell permettant d'afficher les programme ayant la librairie libwrap et donc pouvant utiliser la protection du tcp wrappers :

```
# cd /usr/sbin ↵
# for file in * ↵
> {
> if [ -f $file ]; then
> result=`ldd $file | grep -c libwrap`
> if [ "$result" -gt "0" ]; then
> echo "/usr/sbin/$file is linked to libwrap.so"
> fi
> fi
> }
```

/usr/sbin/**exportfs** is linked to libwrap.so
/usr/sbin/**gdm-binary** is linked to libwrap.so
.....
/usr/sbin/**sendmail** is linked to libwrap.so
.....
/usr/sbin/**vsftpd** is linked to libwrap.so
/usr/sbin/**xinetd** is linked to libwrap.so

21.3.2 Configuration

Utilise 2 fichiers : /etc/hosts.allow et /etc/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 ...1.10
vsftpd: 192.168.1.0/24 EXCEPT 192.168.1.10 = Toutes les machines sur le réseau ...1.0/24 peuvent se connecter en FTP sauf pour la machine ...1.10

Ces fichiers sont lus en temps réel et toute modification est prise en compte de suite.
Le système sera d'autant plus sécurisé que ces fichiers seront configurés simplement.

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

tail /var/log/messages ↵
Jan 26 15:22:42 server xinetd[15959]: xinetd Version 2.3.14 started **with libwrap options compiled in.**
Jan 26 15:22:42 server xinetd[15959]: **Started working**: 1 available service
Jan 26 15:26:30 server xinetd[15959]: **START: imap** pid=16035 from=::ffff:**10.0.0.112**
Jan 26 15:26:30 server xinetd[16035]: **libwrap refused connection to imap** (libwrap=imapd) from

::ffff:10.0.0.112
= Tous les accès réseaux aux services sont bloqués par défaut et le service IMAP n'est pas dans le fichier /etc/hosts.allow
Jan 26 15:26:30 server xinetd[16035]: **FAIL: imap libwrap from=::ffff:10.0.0.112** = La machine ...0.112 ne peut se connecter en IMAP
Jan 26 15:26:30 server xinetd[15959]: **EXIT: imap status=0** pid=16035 duration=0(sec)

On ajoute la ligne suivante au fichier /etc/hosts.allow : imapd: ALL

L'accès est maintenant autorisé :
tail /var/log/messages ↵
Jan 26 15:34:37 fileserv xinetd[15959]: **START: imap** pid=16083 from=::ffff:**10.0.0.112**
Jan 26 15:34:42 fileserv xinetd[15959]: **EXIT: imap status=1** pid=16083 duration=5(sec) = La machine ...0.112 réussi à se connecter

22 Serveur FTP et SFTP

22.1 Serveur FTP

Les informations de ce chapitre sont tirées du site de Jean-Baptiste Yunes(Jean-Baptiste.Yunes@liafa.jussieu.fr)
http://www.liafa.jussieu.fr/~yunes/cours/internet/ftp/

- /etc/ftpusers = Utilisé afin d'interdire tout accès ftp aux utilisateurs sensibles. Il suffit donc d'y faire figurer entre autres les comptes d'administration système :
  root, daemon, bin, sys, adm, lp
- ftpusers = permet de créer des serveurs virtuels très similaires à ce que l'on peut obtenir avec un serveur Web Apache.
- ftphosts = Outre le contrôle d'accès réalisé par l'intermédiaire du fichier /etc/ftpusers, il est possible d'autoriser ou interdire explicitement le service ftp en contrôlant l'accès à partir de la machine cliente. Deux directives sont utilisables :
  - allow = allow <utilisateur> <adresse> [<adresse>...]. Cela autorise explicitement l'utilisateur indiqué à se connecter depuis les adresses précisées. Les adresses peuvent être précédées du caractère ! pour indiquer une négation. Le caractère * est utilisable en tant que joker.
  - deny = deny <utilisateur> <adresse> [<adresse>...]. Cela interdit explicitement à l'utilisateur indiqué de se connecter depuis les adresses précisées.
- ftpconversions = permet aux utilisateurs de réaliser des compressions ou décompressions à la volée des données à télécharger. Plutôt que d'offrir les mêmes données compressées sous divers formats afin que les utilisateurs économisent du temps lors des transferts, il est possible d'économiser de la place sur le serveur en n'offrant qu'un exemplaire de base tout en permettant aux clients de choisir son format préféré de compression.
- ftpaccess = Permet de configurer le démon. Il contient de très nombreuses directives (que nous ne verrons pas toutes) classées dans les catégories suivantes : contrôles d'accès, informations, traces, ratios, divers et permissions.
- ftpgroups = Contient une liste de pseudo-groupes associés à de véritables groupes identifiés dans le système et protégés par un mot de passe permettant au serveur ftp d'utiliser les droits d'accès de ce dernier pour accéder aux fichiers et répertoires. format = pseudo-groupe:mot de passe:groupe
- ftpservers = Permet de créer des serveurs virtuels très similaires à ce que l'on peut obtenir avec un serveur Web Apache.

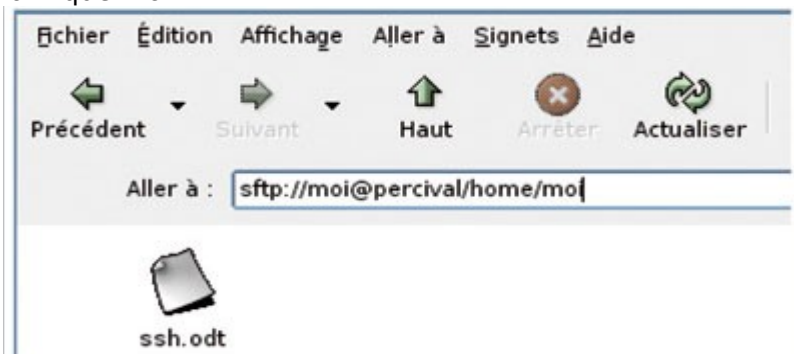
22.2 SFTP

SFTP n'est pas une version de FTP sur SSH, mais un nouveau protocole. Toutefois, les commandes supportées par le client sont très semblables à celle d'un client FTP :
sftp user_serveur@serveur ↵
Connecting to percival...
Password:
sftp> ls
Desktop Bin
sftp> put monfichier.txt
Uploading monfichier.txt to /home/lui/monfichier.txt
monfichier.txt 100% 12KB 12.1KB/s 00:00

sftp> quit

Il est possible de passer par un serveur SSH pour accéder à des fichiers distants avec KDE ou Gnome, via SFTP.
Il suffit de préciser un emplacement sous une forme similaire à celle utilisée pour scp, préfixé de sftp://...
Cette syntaxe peut être utilisée dans n'importe quelle boîte d'ouverture/d'enregistrement de fichiers, ou tout simplement dans la barre d'URL d'un navigateur (Konqueror ou Nautilus)

sftp://moi@percival/home/moi/ ↵ = Vous place dans le répertoire /home/moi de percival, en vous authentifiant en tant que moi.



23 Utiliser SSH

Il remplace RSH, RCP, Rlogin, Telnet, etc.
SSH est un protocole client/serveur offrant sshd sur le serveur et ssh ou scp sur le client.

La commande ssh peut :
- exécuter une commande unique et retourner à la session locale
- ou bien donner l'accès à une session distante identique à une session locale.

La commande scp copie des fichiers et des répertoires entre le système local et le système distant

SSH peut de façon transparente produire du transfert de port, ainsi que de l'authentification X et de la redirection de protocole X.

http://www.openssh.com/images/shherrif.jpg

L'implémentation du protocole SSH utilisé est en général OpenSSH
Le chiffrage des données se fait par échange de clés public / privée
Il travail sur le port 22. La version 1 du protocole est réputé pour avoir un algorithme de chiffrement faible qui a été brisé

23.1 Installation et configuration

OpenSSH peut ne pas être installé par défaut.
Les fichiers de configuration sont sous /etc/ssh
- sshd_config = Pour la configuration du serveur
- ssh_config = Pour la configuration du client

Fichier sshd_config pour Débian :
What ports, IPs and protocols we listen for
Port 22 = Le port 22 est le port standard pour SSH
Protocol 2 = Ne support que la version 2, plus sécurisante. Mettre « 2, 1 » pour accepter les 2 versions

Fichier sshd_config :
Authentication:
PermitRootLogin yes = OpenSSH ignore les paramètres de l'OS de l'hôte pour permettre ou non les connexions root. A la place, il utilise son propre paramètre
PubkeyAuthentication yes = Autorise ou non l'authentification basé seulement sur l'échange de clé

publique

rhosts authentication should not be used
RhostsAuthentication no = Permet ou refuse l'authentification rhost (vielle et non sécurisé) utilisé par la suite rsh/rlogin/rcp
Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
For this to work you will also need host keys in /etc/ssh_known_hosts (for protocol version 2)
HostbasedAuthentication no

To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes = Autorise ou non l'authentification par rhost (ancienne)

X11Forwarding yes = Permet d'activer le transfert X11 sur le serveur. Si un client le demande avec l'option « -X » les données pourront êtres transmises sur le port « DISPLAY » du client. Le serveur définit l'affichage à distance sur le port local, pour que sshd transfert le trafic du système X Window du serveur vers votre écran local.
Pour sécuriser ce transfert, le serveur va installer un jeton d'authentification xauth qu'il appliquera pour toutes les nouvelles connexions.

Fichier /etc/nologin :
Si le fichier /etc/nologin existe, la connexion sur le système distant ne sera autorisée que pour root. Les autres utilisateurs verront s'afficher le contenu du fichier (généralement un message comme « Maintenance système en cours ») et la connexion sera refusée.
ls -l /etc/nologin ↵ = Vérifie si le fichier est présent
-rw-r--r-- 1 root root 51 Oct 17 17:15 /etc/nologin
cat /etc/nologin ↵ = Affiche le message qui apparaîtra lorsque qu'un user voudra se connecter sur le système distant
Système indisponible jusqu'à 09:30 (maintenance)

23.2 Commandes ssh

ssh user_distant@machine_distante ↵ = Se connecte en SSH sur la machine distance en tant que user_distant
ssh user_distant@machine_distante commande ↵ = Exécute la commande sur la machine distante. La connexion est coupée dès que la commande est exécutée
ssh -X user_distant@machine_distante ↵ = Permet de rediriger l'affichage des programmes Xwindow vers le serveur X du client. Si vous lancez un programme X tel que xeyes ou xclock sur le serveur, celui-ci s'exécutera sur ce dernier mais s'affichera sur l'écran du client.
ssh -C user_distant@machine_distante ↵ = permet de compresser les données transférées. Cette option est souvent utilisée conjointement à -X pour soulager les lignes à bas débit.
ssh -v user_distant@machine_distante ↵ = Option utile si le serveur SSH vous refuse l'accès. « = -v » = mode verbeux
Idem de plus en plus verbeux # ssh -vv ... et # ssh -vvv ...

23.3 commandes scp

scp fichier_local user_distant@machine-distante:/chemin/ ↵ = copie le fichier_local vers le chemin de la machine distante, en tant que user_distant
scp -r ... ↵ = Copie récursivement
scp -p ... ↵ = Préserve au mieux les droits, attributs, etc.
scp -P 2222 ... ↵ = Se connecte sur le port distant 2222

23.4 Configuration de OpenSSH

Le programme est disponible ici : http://www.openssh.com/portable.html

sshd ↵ = Une fois installé, il faut lancer sshd sur le serveur. Le programme gère lui-même sa mise en background
ssh serveur_distante ↵ = Depuis l'hôte, la commande ssh permet de connecter au serveur distant

24 Aperçu de DSA et RSA

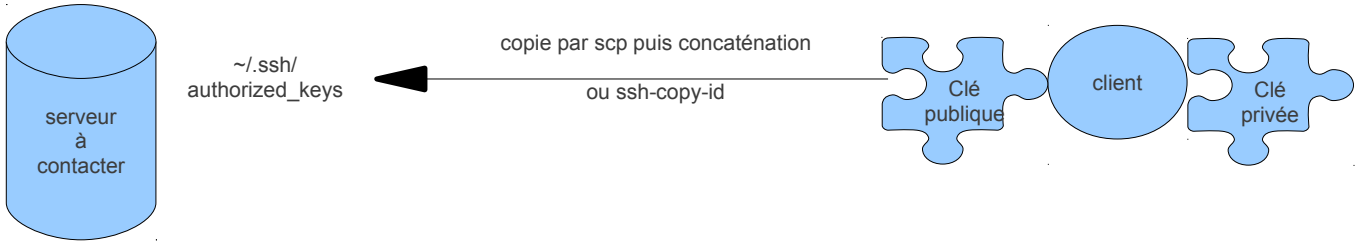
DSA = Digital Signature Algorithm
RSA = Rivest, Shamir, Adleman. 1er algorithm très utilisé mais sujet à des restrictions de copyright.

SSH utilise RSA par défaut alors de GPG utilise DSA. 1024 ou 2048 sont des longueurs utilisées en standard, mais étant donné l'augmentation de la vitesse des processeurs qui permettent toujours plus rapides attaques par force brute, 2048 est actuellement considéré comme la longueur minimale pour assurer la sécurité.

24.1 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 ↵ = Envoi la clé publique du client 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/hnow_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

24.1.1 Utiliser l'algorithme RSA

C'est l'algorithme par défaut utilisé par SSH.

- 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.

24.1.2 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 que ~/.ssh/

ssh_keygen -c ↵ = Permet de changer le commentaire des clefs (seulement pour les clefs RSA1). Le

programme demande le fichier contenant la clef privée, le mot de passe (passphrase) si la clef en a un, et le nouveau commentaire

24.2 Clé privée d'un serveur publique

Lorsque SSH démarre la 1ère fois sur une serveur, sa paire de clés privée et publique est créée :

- Algorithme RSA
  - /etc/ssh/ssh_host_rsa_key = Clé privée
  - /etc/ssh/ssh_host_rsa_key**.pub** = clé publique (toujours avec une extension en .pub)
- Algorithme DSA
  - /etc/ssh/ssh_host_dsa_key = Clé privée
  - /etc/ssh/ssh_host_dsa_key**.pub** = clé publique

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

24.2.1 ssh-agent

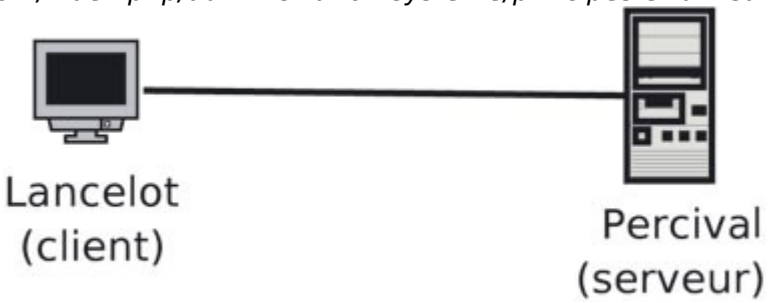
Permet d'utiliser plus facilement la passphrase. Le principe est d'utiliser ssh-agent pour qu'il garde vos clés. Lorsque vous ajoutez vos clés, vous ne donnez la passphrase qu'une seule fois.
Attention, car l'utilisateur root peut également demander les clés sans que vous le remarquiez .
ssh_agent configure 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 $ ↩ = 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)

25 SSH et les tubes

Les informations de ce chapitre sont tirées du magazine « Linux Magazine / France » n°82
http://www.unixgarden.com/index.php/administration-systeme/principes-et-utilisation-de-ssh



Les tubes permettent de relier la sortie d'une commande à l'entrée d'une autre. Le fait de passer par SSH ne rompt pas cette chaîne, et il est ainsi possible de brancher la sortie de commandes locales sur des commandes distantes, et vice-versa.
Lorsque l'on demande à SSH d'exécuter une simple commande distante, cette commande peut être branchée avec une commande locale. SSH redirige en effet son entrée standard vers l'entrée standard de la commande distante, et la sortie standard de la commande distante vers la sienne.

tar czf - Documents | ssh percival "cat > sauvegarde.tar.gz" ↩ = Ligne de commande permettant de faire une sauvegarde du répertoire Documents sur percival. Le paramètre « - » donné à tar lui demande de sortir le flux compressé sur la sortie standard. Ce flux est récupéré par SSH qui le transfère sur percival et l'utilise comme entrée standard de cat. Tel qu'il est appelé, cat ne fait que copier son entrée standard vers le fichier sauvegarde.tar.gz. Ainsi, nous avons réalisé une sauvegarde distante et compressée en une seule ligne.

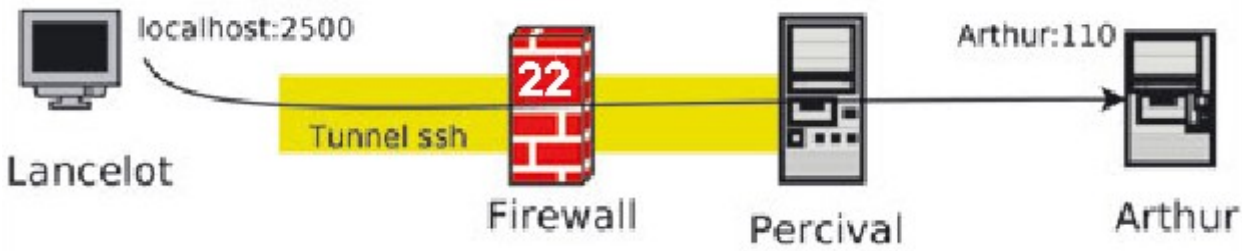
Idem mais la compression se fait côté serveur # tar cf - Documents |ssh percival "gzip -c >sauvegarde.tar.gz" ↩

ssh percival "cat sauvegarde.tar.gz" |tar xzf ↵ = Restauration de cette sauvegarde

On peut donc faire passer les sorties standards de commandes à travers une connexion SSH.

25.1 Tunnels SSH

Des informations complémentaires de ce chapitre peuvent être tirées du post de djib (24 février 2007, 17:02)
http://www.think-underground.com/post/2007/02/24/398-tunnel-ssh-ssh-l-local-et-ssh-r-remote-en-bref



lancelot et percival ne sont pas dans le même réseau local, mais appartiennent à deux réseaux différents connectés par internet. percival est derrière un pare-feu qui filtre tous les ports à l'exception du port 22 (le port utilisé par SSH). Derrière percival se trouve arthur, qui est un serveur POP3 (email). À partir de lancelot, nous voudrions récupérer nos mails qui se trouvent sur arthur.
Plusieurs problèmes :

- arthur n'est pas directement accessible depuis lancelot. Seul percival a une adresse internet publique, arthur n'étant pas visible de l'extérieur du réseau.
- Le pare-feu filtre tous les ports à l'exception du port 22. Or, le serveur POP3 écoute sur le port 110

25.1.1 Création d'un tunnel avec ssh -L

ssh -L port_local:machine_a_atteindre:port_machine_a_atteindre serveur_intermediaire_distant

L'option -L de SSH permet de créer un tunnel. Il s'agit d'employer un port de la machine locale pour transporter des données à travers la connexion SSH et les rediriger où l'on veut à partir de la machine distante. Le tunnel est également utilisable en sens inverse. Cette option est très puissante. Dans notre cas, nous voulons nous servir de percival comme intermédiaire pour nous connecter à arthur
ssh -L 2500:arthur:110 percival ↵ = Connexion à percival en redirigeant le port local 2500 (= « -L 2500») vers le port 110 du serveur arthur

Du côté du client mail (Thunderbird par exemple sur lancelot), il suffira de d'indiquer « localhost » comme serveur de mail à atteindre avec le port 2500. Tant que la connexion SSH restera ouverte, une connexion réseau sur le port 2500 équivaudra à se connecter sur le port 110 du serveur de mail arthur, à travers le port 22 (ssh) du pare-feu via Perceval.
Le tunnel se fermera avec la cloture de la session ssh.

25.1.2 Redirection de port distant avec ssh -R

ssh -R port:host:host_port [user@]hostname [command]

Lorsque vous utilisez l'option « -R », l'inverse de l'option « -L » se produit. Le port de l'interface localhost du serveur distant est relié à la machine locale, et les connexions seront transmises à la machine locale précisée (= « host:host_port »)

Pour illustrer cette option, prenons le cas ou le "support" doit prendre la main en SSH sur la machine du "client"..mais sans que le "client" ne soit contraint d'autoriser dans son FireWall une connexion entrante vers le port SSH de son serveur.

- Blocage de l'accès en SSH à distance vers "client" (simulation d'un FireWall)
  ListenAddress 127.0.0.1 dans le /etc/ssh/sshd_config de "client"
  yannick@client:~$ netstat -ant|grep 22
  tcp 0 0 127.0.0.1:22 0.0.0.0:* LISTEN
  yannick@client:~$

Il est donc impossible à une autre machine distante, de se connecter de manière "normale" sur le port 22 de "client"...

- Rien de spécial pour l'instant sur la machine "support":
  yannick@support:~$ netstat -ant |grep 1111
  yannick@support:~$
- On fait lançer (par le client) la commande "ssh -R" sur la machine "client":

ssh -R port-distant:HOSTNAME:port-local machine-distante
yannick@client:~$ ssh -R 1111:127.0.0.1:22 support
...on entre le mot de passe de "support"...on est connecté a "support"....

- Sur la machine "support":

... on a désormais le port 1111 d'ouvert:

yannick@support:~$ netstat -ant |grep 1111
tcp 0 0 127.0.0.1:1111 0.0.0.0:* LISTEN
yannick@support:~$

...en se connectant sur le port 1111 de "support" on arrive donc sur le port 22 du "client":

yannick@support:~$ ssh -p1111 127.0.0.1
...demande le mot de passe de "client"...on est connecté sur le ssh de "client"

- Fin:

Il suffira au "client" de faire exit et un CTRL+C pour couper la connexion du "support"

yannick@client:~$ Connection to 127.0.0.1 closed by remote host.
Connection to 127.0.0.1 closed.
yannick@support:~$

- Il est à noter qu'il est possible de maintenir le tunnel ouvert même en quittant la session en utilisant screen.

25.1.3 Screen

Cette commande n'est pas traitée dans le cadre de la certification LPIC-1

screen est une application console dont le principal avantage est pouvoir se « détacher » de la console. C'est à dire qu'on peut lancer une application dedans, détacher le screen (volontairement ou en étant déconnecté brutalement par exemple) et l'application continue de tourner comme si de rien était. Une fois reconnecté il suffit de "rattacher" le screen pour recuperer la main.

Mais ce n'est pas le seul avantage de screen. En fait screen peut être considéré comme « le window manager de la console ». En effet, il permet d'afficher une barre des taches, ouvrir plusieurs consoles, passer de l'une à l'autre, splitter l'écran.

screen se configure avec le fichier ~/.screenrc. Par défaut, il n'y a pas de barre des taches et il affiche un message au demarrage. Ces deux lignes permettent de remedier à ça :

```
hardstatus alwayslastline "%d/%m/%Y [%c] | %w"
startup_message off
```

Les touches de bases :

Ctrl + D : se déloguer = ferme la fenêtre
Ctrl + (A, D) : détacher le screen (screen -r pour le rattacher)
Ctrl + (A, C) : nouvelle fenêtre
Ctrl + (A, A) : fenêtre précédente
Ctrl + A, n : passe à la fenêtre "n"

Utilisation

Nous allons lancer dans le *screen* une application en ligne de commande, puis «nous détacher» de la session du *screen* en laissant l'application tourner dedans. Ensuite, à partir du même poste ou d'un poste distant (avec ssh par exemple) nous pourrons «nous rattacher» à la session du *screen* et récupérer exactement la même chose que lorsque nous nous étions détaché.

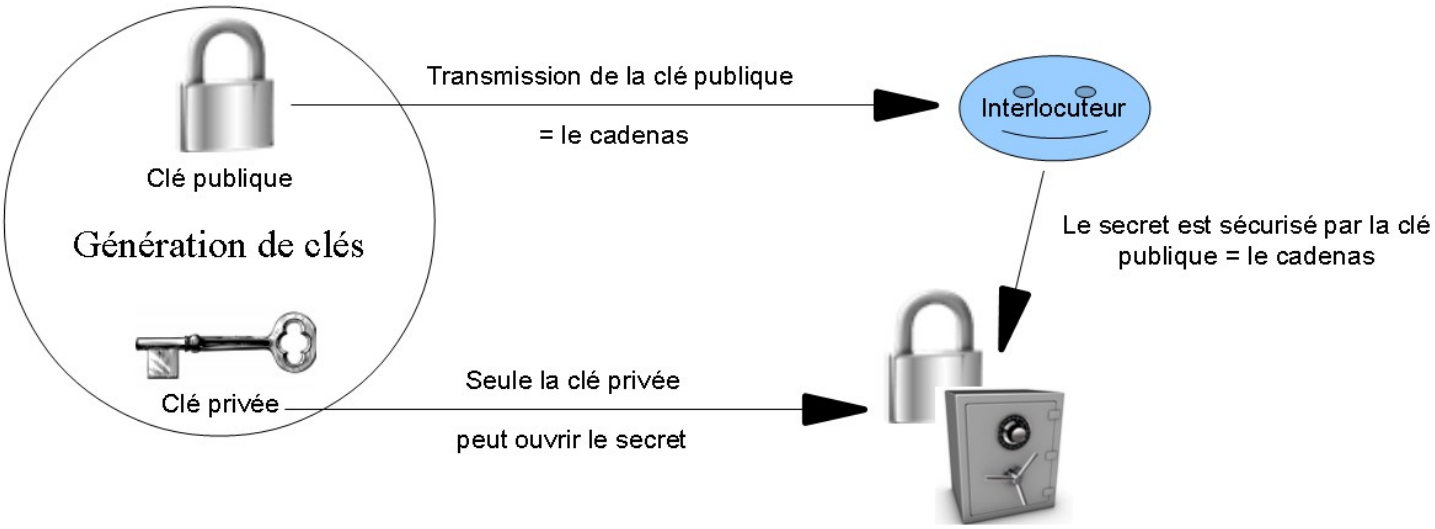
- Créer un nouveau *screen* en nommant la session :
  # screen -S nom_de_la_session
  Un message annonçant la version utilisée et indiquant que ce programme est publié sous licence GPL s'affiche à l'écran. Il ne reste plus qu'à presser la touche [ESPACE].

- La nouvelle session du *shell* s'affiche et attend qu'on saisisse une commande, par exemple :
  # echo test
  test
- Pour se détacher de la session du *screen* :
  # [CTRL]+[a] suivi de [d]
  OU fermer le terminal et/ou ouvrir un autre terminal
- Pour se rattacher à la session du *screen* :
  # screen -r nom_de_la_session

Le rattachement à la session du *screen* peut très bien se faire à distance. Nous accédons alors à notre machine via un accès ssh par exemple.

26 Clé GPG

GPG est un concurrent de PGP qui est devenu payant



26.1.1 Générer une parie de clés

$ gpg --gen-key ↵ = Crée une paire de clés sous ~/.gnupgp
pg (GnuPG) 1.2.1; Copyright (C) 2008 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software: you are free to change and redistribute it. There is NO WARRANTY, to the extent permitted by law.

gpg: keyring '/home/james/.gnupg/secring.gpg' created
gpg: keyring '/home/james/.gnupg/pubring.gpg' created
Please select what kind of key you want:
(1) DSA and ElGamal (default)
(2) DSA (sign only)
(5) RSA (sign only)
Your selection? **5**
What keysize do you want? (1024) **2048**
Requested keysize is 2048 bits
Please specify how long the key should be valid.
0 = key does not expire
<n> = key expires in n days
<n>w = key expires in n weeks
<n>m = key expires in n months
<n>y = key expires in n years
Key is valid for? (0) **3y**
Key expires at Fri Sep 18 00:23:00 2009 CET
Is this correct (y/n)? **y**
You need a User-ID to identify your key; the software constructs the user id from Real Name, Comment and Email Address in this form: "James Stanger (James Stanger) <stangernet@comcast.net>"
Real name: **James Stanger**
Email address: **stangernet@comcast.net**
Comment: (rien)
You selected this USER-ID: "James Stanger <stangernet@comcast.net>"
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? **o**
You need a Passphrase to protect your secret key.
Enter passphrase: **passphrase**
Repeat passphrase: **passphrase**
We need to generate a lot of random bytes. It is a good idea to perform some other action (type on the keyboard, move the mouse, utilize the disks) during the prime generation; this gives the random number

generator a better chance to gain enough entropy.
..+++++
+++++
public and secret key created and signed. key marked as ultimately trusted.

pub 2048R/97DAFDB2 2004-01-12 James Stanger <stangernet@comcast.net>
Key fingerprint = 85B2 0933 AC51 430B 3A38 D673 3437 9CAC 97DA FDB2

Note that this key cannot be used for encryption. You may want to use the command "--edit-key" to generate a secondary key for this purpose

Une fois la création de clés terminée, il y a plusieurs options :

- DSA and ElGamal = Une paire de clés DSA est créée pour signer des fichiers, et une paire de clés ElGamal est créée pour crypter des fichiers
- DSA sign only = Méthode plus rapide, mais cela crée une paire de clés qui permettent de signer des fichiers
- RSA sign only = Idem pour le « DSA sign only » mais avec un cryptage RSA plutôt que DSA

26.1.2 Importer une clé publique dans un porte-clés GPG

Le référentiel clé GPG publique est appelé un "porte-clés." Le porte-clés contient votre clé privée ainsi que toutes les clés publiques des hôtes distants avec lesquels vous devez communiquer de manière sécurisée.

gpg --import cle_publique.asc ↵ = Importe la clé publique dans mon porte-clés

26.1.3 Signer les clés

Avant de pouvoir utiliser une clé publique qui vient d'être importée, il faut la signer.

gpg --edit-key nom_cle ↵ = Demande si il faut signer la clé. Il faut alors entrer le mot de passe de votre clé privée pour que la clé publique soit signée avec votre clé privée

26.1.4 Lister les clés

gpg --list-keys ↵ = Liste la clé privée et toutes les clé publiques importées
/home/james/.gnupg/pubring.gpg
---
pub 2048g/CC7877gh 2009-09-11 James (Stanger) <stangernet@comcast.net>
sub 2048g/89G5B4KM 2009-09-11 = sub = clé ElGamal (pour crypter les fichiers)
pub 2048D/4g37NJ27 2009-12-09 Andyo (Oram) <andyo@oreilly.com> = pub = clé DSA (pour signer les fichiers)
sub 2048D/4g37GK38 2009-12-09

gpg --list-secret-keys ↵ = Liste la clé privée
gpg --list-public-keys ↵ = Liste la clé publique

26.1.5 Exporter la clé publique et privée ensemble

Exporter la clé privée permet de la sauvegarder en cas de problème du système

gpg --export -o gpg_fichier_sauvegarde ↵ = Exporte toutes les clés dans 1 seul fichier de sauvegarde (= « -o » = output)
gpg --export-secret-key -a "David" -o privee.key ↵ = Exporte seulement la clé privée (= « --export-secret-key ») de David (= « -a ») dans le fichier privée (= « -o » = output)
gpg -- export-public-key -a "James Stanger" -o publique.pub ↵ = Export toutes les clés publiques (= « --export-public-key ») de David dans le fichier publique

26.1.6 Crypter un fichier

gpg -e -u "David" -r "Guillaume" fichier_a_crypter ↵ = Crypte (= « -e » = encrypte) le fichier, utilise le nom « David » pour la signature, (= « -u » = user) et « Guillaume » en tant qu'utilisateur (= « -r » = recipient). Seul Guillaume pourra lire le fichier à crypter
gpg -d fichier_a_crypter ↵ = Guillaume décrypte le fichier (= -d » = décrypte)

26.1.7 Le répertoire ~/.gnupg/

Tous les fichiers utiles à GPG se trouvent sous 26.1.7 ~/.gnupg/ :

- gpg.conf = Paramètres par défaut de GPG, incluant le serveur de clé par défaut qui contient la clé publique de tous les utilisateurs qui souhaitent diffuser leur clé

- pubring.gpg = Contient les clés publiques importées
- random_seed = Contient les paramètres permettant à GPG de créer des nombres aléatoires plus facilement et plus rapidement
- secring.gpg = Contient votre clé privée
- trustdb.gpg = Base de données « trust » qui contient les valeurs de confiances attribuées à différentes clés publiques. Un utilisateur peut définir une valeur de confiance différente pour les clés de son porte-clés.

27 Licence Créative Commons

27.1 Citations des références utilisées dans cet ouvrage

Site internet « Certif Linux » : http://www.linuxcertif.com
Site internet « Certification-Linux » : http://www.certification-linux.net/lpic-106.php
Site Internet « Wikipédia » : http://www.wikipedia.org
Le contenu de ce site est soumis à la licence CC-BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0/deed.fr)
Site Internet de Jean-Baptiste Yunes (http://www.liafa.jussieu.fr/~yunes/cours/internet/ftp/)
Site Internet « Think-Underground.com » : Logiciels libres, photographie, musique, énigmes, humour et coups de cœur
Post de djib (24 février 2007, 17:02)
http://www.think-underground.com/post/2007/02/24/398-tunnel-ssh-ssh-l-local-et-ssh-r-remote-en-bref