Technicien Supérieur Gestionnaire
Exploitant de Ressources Informatiques
et Réseaux

Configuration Express

Debian

Beginner guide

O RLY?

Marchal Ludovic

Table des matières

Installation

BLA BLA photo, etc....

L'installation d'un server debian se déroule sans grande surprise l'installer fonctionnant parfaitement, il assiste l'utilisateur de bout en bout.

C'est un peu le coté windowisation de la chose.

Fraîchement installé notre server à besoin d'être configuré.

Configuration

Privilèges

Sous Debian l'utilitaire sudo n'est pas installé, aussi lorsque l'on souhaite se connecter avec un utilisateur celui-ci ne pourra obtenir les droits su.

Il faudra se logger directement en ROOT pour commencer la configuration.

Je souhaite créer 3 utilisateurs, mes collaborateurs qui pourrons administrer également le serveur.

moi même
steph
sandrine

ROOT

Sous debian seul ROOT (l'homme du train) a les droits d'administration, afin de donner des droits de manière controlée il existe sudo qui est un utilitaire permettant de prendre les droits temporairement, cela évite bien des écueils.

#aptitude -y install sudo

```
sudo vi /etc/network/interfaces

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for username:
```

La ligne 3 est signée Maitre Yoda

Ajouter un utilisateur

Adduser n'est pas une commande interne mais un script qui va organiser l'enchaînement des commandes pour assister la création.

Sudo adduser <NEWUSER>

(steph et sandrine)

Fournir les informations à la console interactive.

VISUDO

Pour ensuite ajouter les utilisateurs dans le groupe SUDO il faut l'utilitaire VISUDO , pour modifier le fichier de contrôle :

/etc/sudoers

Ce peut être VI ou NANO qui sera lancer.

Rtfm : man nano

Bien-sure remplacer USER par votre login (le nom de l'utilisateur concerné)

```
root@srv-debian:~#
visudo
# add to the end : user "votre_login" can use all root privilege

USER    ALL=(ALL)    ALL
```

Nota-benne

On peut également ajouter des utilisateurs dans le groupe SUDO

Aprés installation de l'utilitaire sudo

adduser user sudo

Déconnexion/Reconnexion avec l'utilisateur précédemment ajouté.

C'est par exemple le cas pour wireshark, il faut ajouter son utilisateur au groupe wireshark

adduser user wireshark

Il est possible de renforcer la sécurité de la machine en interdisant certaines commandes.

Comme, reboot, halt... a certains utilisateurs.

Tester avec l'un des meilleur outils d'inforensic :

```
sudo apt-get install cmatrix
```

cmatrix ctrl+c pour arrêter.

Désactiver un compte

Où sont les comptes ?

Les identifiants sont stockés dans :

/etc/passwd

Il se présente de cette manière, tous les champs séparés par le signe :

login:mot-de-passe:UID:GID:info-utilisateur:répertoire-principal:shell

```
doej:x:561:561:Joe Doe:/home/doej:/bin/bash
```

- Nom d'utilisateur, jusqu'à 8 caractères. Case-sensitive, habituellement tout en minuscules
- Un "x" dans le champ mot de passe. Les mots de passe sont stockés dans le fichier "/etc/shadow".
- Numéro d'identification de l'utilisateur. Il est attribué par le script "adduser". Unix utilise ce champ, plus le champ suivant du groupe, pour identifier quels fichiers appartiennent à l'utilisateur.
- Numéro d'identification du groupe. Red Hat utilise le numéro de groupe d'une manière assez unique pour des raisons de sécurité des fichiers renforcée. Habituellement, le numéro de groupe sera le même que le numéro d'utilisateur.
- Nom complet de l'utilisateur. Je ne suis pas sûr de la longueur maximum de ce champ mais essayer de la garder d'une taille raisonnable (mois de 30 caractères).
- Répertoire personnel de l'utilisateur. Habituellement, /home/username (eg. /home/doej). Tous les fichiers personnels de l'utilisateur, ses pages web, ses mails à envoyer, etc,... seront stockés là (en général)..
- User's "Compte shell". Souvent fixé à "/bin/bash" pour permettre l'accès au shell bash (mon shell personnel favori).

C'est la commande passwd qui s'occupe de chiffrer le mot de passe. Ce champ peut prendre plusieurs siginifications :

"*" : il est impossible de s'authentifier sur le système avec ce compte.
"!!" : Le compte est désactivé
"x" ou "!" : le mot de passe est dans un fichier shadow (voir ci-après)
champ vide : Il n'y a pas de mot de passe pour ce compte.

Où sont les mots de passe ?

C'est indiqué plus haut, dans :

/etc/shadow

```
doej:Ep6mckrOLChF.:10063:0:99999:7:::
```

- Nom d'utilisateur, jusqu'à 8 caractères. Case-sensitive, habituellement uniquement des minuscules. Exactement la même entrée que dans le fichier /etc/passwd.
- Mot de passe, 13 caractères codés. Une entrée nulle (eg. ::) indique qu'un mot de passe n'est pas demandé pour entrer dans le système (*une mauvaise idée*), et une entrée "*"indique que le compte a été désactivé.
- Le nombre de jours (depuis le 1er Janvier 1970) depuis le dernier changement du mot de passe.
- Le nombre de jours avant que le mot de passe ne puisse être changé (un 0 indique qu'il peut être changé à n'importe quel moment).
- Le nombre de jours après lesquels le mot de passe *doit* être changé (99999 indique que l'utilisateur peut garder son mot de passe inchangé pendant beaucoup, beaucoup d'années)
- Le nombre de jours pour avertir l'utilisateur qu'un mot de passe ne va plus être valable (7 pour une semaine entière)
- Le nombre de jours avant de désactiver le compte après expiration du mot de passe
- Le nombre de jours depuis le 1er Janvier 1970 pendant lesquels un compte a été désactivé
- Un champ réservé pour une utilisation future possible

Solution

Avec passwd options l pour lock

```
# passwd -l {username}
```

Et passwd option u pour unlock

```
# passwd -u {username}
```

Modification manuelle

Il suffit d'ajouter un caractère devant le MdP (chiffré), ce faisant celui ne correspond plus et mécaniquement l'utilisateur ne peut plus se loger. Ajouter un astérisque permet de le modifier très facilement, pour pouvoir le ré-activer plus tard.

Nota benne

Bien que le compte soit verrouillé l'utilisateur peut toujours se logé à un server, si l'authentification est basée sur les clés public (logique...).

Verrouillage total

Avec change age option E pour expire

```
# chage -E 0{username}
```

Deverouillage

```
# chage -E -1 {username}
```

Forcer un utilisateur a changer de mot de passe

A la prochaine connexion.

```
# chage -d 0 {username}
```

Variables d'environnement

Utilitaire

Nous connaissons différent afficheur de texte, avec leur particularité.

Installons most et utilisons-le comme <PAGER> par défaut, c'est l'occasion de voir comment modifier une variable d'environnement.

Installer MOST

Most offre une coloration qui est très pratique pour lire les manpages, c'est la raison pour laquelle je lis les manpages.

```
# aptitude install most
```

Il faut modifier ./bashrc pour rendre les changement permanent.

Export PAGER= "most"

Pour prendre en compte le changement on recharge le bash :

source ~/.bashrc

Sachant maintenant comment modifier le comportement du shell, nous allons pouvoir personnaliser notre bashrc et y inclure des allias, et des fonctions.

/etc/profile Pour tout le system

/home/<user>/.bashrc Pour un utilisateur

Je vais prendre des exemples de mes alias assez régulièrement.

Par exemple des alias pour éditer certains fichiers de configuration rapidement, en choisissant un editeur ou un autre : (j'aurais put mettre v pour vim

```
###°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°°###
###-----------------------Editer--------------------------------------###
###-----------------les fichiers de config'---------------------------###
###~~~~~~~~~~~~~~~~~~~~~~ avec nano~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~###
###__________________________________________________________________###
alias nconky='nano ~/.conkyrc'
alias nbash='nano ~/.bashrc'
alias nmenu='nano ~/.config/openbox/menu.xml'
alias nrc='nano ~/.config/openbox/rc.xml'
alias nautostart='nano ~/.config/openbox/autostart'
###~~~~~~~~~~~~~~~~~~~~~~~avec geany~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~###
alias gconky='geany ~/.conkyrc'
alias gbash='geany ~/.bashrc'
alias gmenu='geany ~/.config/openbox/menu.xml'
alias grc='geany ~/.config/openbox/rc.xml'
alias gautostart='geany ~/.config/openbox/autostart'
###__________________________________________________________________###
```

Manpages

Les manpages sont excessivement pratique les avoir en français c'est pas mal non plus et voilà le résultat de la lecture des manpages avec most.

Aptitude install -y manpages-fr manpages-fr-extra manpages-dev

man man

```
MAN(1)                                Utilitaires de l'afficheur des pages de manuel                                MAN(1)


NOM
       man - Interface de consultation des manuels de référence en ligne

SYNOPSIS
       man  [-C fichier] [-d] [-D] [--warnings[=avertissements]] [-R encodage] [-L locale] [-m système[,...]] [-M chemin] [-S liste] [-e
       extension] [-i|-I] [--regex|--wildcard] [--names-only] [-a] [-u] [--no-subpages] [-P afficheur] [-r invite]  [-7]  [-E  encodage]
       [--no-hyphenation]    [--no-justification]    [-p  chaîne]  [-t]  [-T[périphérique]]  [-H[navigateur]]  [-X[ppp]]  [-Z]  [[section]
       page ...] ...
       man -k [options d'apropos] expression_rationnelle ...
       man -K [-w|-W] [-S liste] [-i|-I] [--regex] [section] term ...
       man -f [options de whatis] page ...
       man -l [-C fichier] [-d] [-D] [--warnings[=avertissements]] [-R encodage] [-L locale] [-P afficheur] [-r invite] [-7]  [-E  enco-
       dage] [-p chaîne] [-t] [-T[périphérique]] [-H[navigateur]] [-X[ppp]] [-Z] fichier ...
       man -w|-W [-C fichier] [-d] [-D] page ...
       man -c [-C fichier] [-d] [-D] page ...
       man [-?V]

DESCRIPTION
       man  est  le programme de visualisation des pages de manuel. Chacun des arguments page, indiqué dans la ligne de commande de man,
       porte, en principe, le nom d'un programme, d'un utilitaire ou d'une fonction. La page de manuel correspondant à  chaque  argument
       est  alors  trouvée  et  affichée.  Si  une  section  est  précisée alors man limite la recherche à cette section. Par défaut, il
       recherche dans toutes les sections disponibles en suivant un ordre prédéfini (« 1 n l 8 3 2 3posix 3pm 3perl 5  4  9  6  7 »  par
       défaut,  à  moins  d'être écrasée par la directive SECTION dans /etc/manpath.config). Il n'affiche que la première page de manuel
       trouvée, même si d'autres pages de manuel existent dans d'autres sections.
```

EG

Eg vous donne des exemples rapide de certaines commandes.

sudo pip install eg

Pour connaître la liste taper

eg -l

```
Legend:
    + only custom files
    * custom and default files
      only default files (no symbol)

Programs supported by eg:
adb
awk
cat
cd
chmod
chown
clang -> gcc
clang++ -> gcc
```

Installer VIM

Vim est une version améliorée de VI

```
sudo aptitude install -y vim
```

Modifier l'éditeur de texte

Une commande très simple permet ceci :

```
sudo select-editor

Select an editor.  To change later, run 'select-editor'.
  1. /bin/nano        <---- easiest
  2. /usr/bin/vim.basic
  3. /usr/bin/vim.gnome
  4. /usr/bin/vim.tiny

Choose 1-4 [1]:
```

Configuration réseau

```
sudo vi /etc/network/interfaces
```

Ceci est un fichier de configuration « type » il suffit d'y modifier les adresses en fonction de son propre réseau.

Aprés modification recharger le fichier et relancer le service :

```
sudo service networking force-reload
sudo service networking restart
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
# comment out

#
iface eth0 inet dhcp
# add follows

iface eth0 inet static
address 10.0.0.30
# IP address

network 10.0.0.0
# network address

netmask 255.255.255.0
# subnet mask

broadcast 10.0.0.255
# broadcast address

gateway 10.0.0.1
# default gateway

dns-nameservers 10.0.0.10
```

name server

systemctl restart ifup@eth0

Voir les services qui tournent :

systemctl -t service

```
UNIT                    LOAD   ACTIVE SUB     DESCRIPTION
acpid.service             loaded active running ACPI event daemon
atd.service               loaded active running Deferred execution scheduler
console-setup.service           loaded active exited  LSB: Set console font and keymap
cron.service              loaded active running Regular background program
processing daemon
dbus.service              loaded active running D-Bus System Message Bus
```

systemctl list-unit-files -t service

```
UNIT FILE                STATE
acpid.service              disabled
atd.service               enabled
autovt@.service              disabled
bootlogd.service             masked
bootlogs.service             masked
```

Stop service systèm

Desactive l' « autostart » pour des applications system

systemctl stop XYZ

systemctl disable XYZ

MaJ

Il peut arriver qu'une source en trop soit indiquée dan le fichier source.list par exemple le CDRom d'installation. (Ca m'est arrivé et cela a pour conséquence des messages d'erreurs.

Commenter le CDRom dans :

/etc/apt/sources.list

Rafraichissement de la liste des paquets

sudo aptitude update

aptitude -y upgrade

SSH

Génération des paires de clés pour chacun de l'équipe.

Je crée un répertoire, pour y placer les PUB_KEY

sudo mkdir /etc/ssh/k-team

sudo ssh-keygen -f /etc/ssh/k-team/ID_RSA_DEBIAN_SRV_STEPH -C « Stephane »

-f indique le fichier

-C indique un ID

Distribuer ensuite les clés privées aux équipiers.

Copier avec scp

SYNTAXE : scp <fichier> <login>@<IP@distant>:/<répertoire home>/<fichier>
tsgeri@srvmaster:~$ scp monit.tar.gz adminoc@172.25.0.7:/home/adminoc/monit.tar.gz

3. Sur le serveur distant créer un dossier et depuis ce dossier décompresser/décompacter le fichier
adminoc@oc2:~$ mkdir monit
adminoc@oc2:~$ cd monit/
adminoc@oc2:~/monit$ tar zxvf ../monit.tar.gz

10. Commande SSH

Objectif : utiliser la commande SSH pour les accès distants aux serveurs avec Putty

Générer une paire de clés pub/privée

ssh-keygen

Copier la clé .pub avec Ctrl-Insert

se connecter au serveur distant

ssh tsgeri@172.25.5.10

Coller la clé dans .ssh/autorized_keys du serveur distant avec Shift-Insert

vi .ssh/autorized_keys

exit pour revenir au premier serveur

Se connecter de nouveau au serveur distant

ssh tsgeri@172.25.5.10

Le serveur distant ne demande plus le mot de passe.

Depuis le premier serveur exécuter des commandes sur le serveur distant

```
ssh tsgeri@172.25.5.10 "echo $HOME"
ssh tsgeri@172.25.5.10 "ps -ef"
ssh tsgeri@172.25.5.10 "df -h"
ssh tsgeri@172.25.5.10 "uname -r"
ssh tsgeri@172.25.5.10 "ls -l /boot"
ssh -t tsgeri@172.25.5.10 "sudo apt-get update && sudo apt-get upgrade -y"
```

Activer rsyslog

Envoyer les sortie vers le tty8 en modifiant :

/etc/rsyslog.conf

```
# Emergencies are sent to everybody logged in.
#
*.emerg                         :omusrmsg:*

#
# I like to have messages displayed on the console, but only on a virtual
# console I usually leave idle.
#
daemon,mail.*;\
        news.=crit;news.=err;news.=notice;\
        *.=debug;*.=info;\
        *.=notice;*.=warn       /dev/tty8

# The named pipe /dev/xconsole is for the `xconsole' utility.  To use it,
# you must invoke `xconsole' with the `-file' option:
#
#    $ xconsole -file /dev/xconsole [...]
#
# NOTE: adjust the list below, or you'll go crazy if you have a reasonably
#      busy site..
#
daemon.*;mail.*;\
        news.err;\
        *.=debug;*.=info;\
        *.=notice;*.=warn       |/dev/xconsole
```

Je continue la config en ssh.

Concernant le copié/collé des lignes qui suivent, en particulier pour la configuration de DNS.

Ceci est à proscrire, le texte n'étant pas formaté de la même manière, je ne parle pas de format de type : .DOC, ou .ODT, ou DOCX.

Il s'agit du formatage système, comme les fins de ligne.

A savoir également que des espaces et des tabulations ont été modifiés, ce qui rend les configurations inexploitables.

DNS

configuration par défaut

Named.conf

/etc/bind# ls

```
bind.keys                                   named.conf.local.grp3
db.0                    db.local
db.127                  db.root             named.conf.logging
db.255                  named.conf                  named.conf.options
db.empty                named.conf.default-zones
        named.conf.options.bak
db.grp3.info-msj.net    named.conf.grp3     rndc.key
db.grp3.info-msj.net.inv    zones.rfc1918   named.conf.local
```

/etc/bind/named.conf

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

named.conf.options

```
options {
directory "/var/cache/bind";
forwarders {
172.25.0.6;
};
listen-on-v6 {
internals;
};
allow-query {
internals;
};
```

```
allow-recursion {
internals;
};
version none;
auth-nxdomain no; # conform to RFC1035
};
```

named.conf.local

Concerne l'adresse du réseau et le fichier de configuration signalé par include

```
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
acl internals { 127.0.0.0/8; 172.25.3.0/24; };
//include "/etc/bind/named.conf.logging";
include "/etc/bind/named.conf.local.info-msj.net";
//include "/etc/bind/rndc.key";
//       controls {
//        inet 127.0.0.1 port 953
//        allow { 127.0.0.1; } keys "/etc/bind/rndc-key"; };
//};
```

Named.default-zones

Ne pas modifier celui ci

```
// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
```

Reseau TSGERI

Zone de recherche et zone inverse

db.grp3.info-msj.net

```
$ORIGIN grp3.info-msj.net.
$TTL    1600
@ IN SOA ns1.grp3.info-msj.net. @root.grp3.info-msj.net. (
                    2013112801          ;Serial
                    604800              ;Refresh
                    86400               ;Retry
                    2419200             ;Expire
                    604800 ); Negative Cache TTL

@                   IN    NS      ns1.grp3.info-msj.info-msj.net.
@                   IN    MX  10      mail.grp3.info-msj.net.
ns1                 IN    A       172.25.3.1
mail                IN    A       172.25.3.4
www                 IN    A       172.25.3.107
rtfm                IN    A       172.25.3.113
www3                IN    A       172.25.3.123
webmail             IN    CNAME   mail
```

db.grp3.info-msj.net.inv

```
$ORIGIN 3.25 .172.in-addr.arpa.
$TTL    1600
@       IN    SOA       ns1.grp3.info-msj.net. @root.grp3.info-msj.net. (
                    2013112801          ;Serial
                    604800              ;Refresh
                    86400               ;Retry
                    2419200             ;Expire
                    604800 )            ;Negative Cache TTL
@       IN      NS      ns1.grp3.info-msj.net.

100       IN      PTR     www.grp3.info-msj.net.
113       IN      PTR     rtfm.grp3.info-msj.net.
123       IN      PTR     www3.grp3.info-msj.net.
1         IN      PTR     ns1.grp3.info-msj.net.
4         IN      PTR     mail.grp3.info-msj.net.
```

Named.conf.grp3

```
zone "grp3.info-msj.net" {
        type master;
        file "/etc/bind/db.grp3.info-msj.net";
                allow-update { key rndc-key; };
};

zone "3.25.172.in-addr.arpa" {
        file master;
        file "/etc/bind/db.grp3.info-msj.net.inv";
                allow-update { key rndc-key; };
};
```

Named.conf.local.grp3

```
zone "grp3.info-msj.net" {
        type master;
        file "/etc/bind/db.grp3.info-msj.net";
                allow-update { key rndc-key; };
};
```

```
zone "3.25.172.in-addr.arpa" {
        type master;
        file "/etc/bind/db.grp3.info-msj.net.inv";
                allow-update { key rndc-key; };
};
```

Test

Sudo service bind9 reload

sudo service bind9 restart

sudo service bind9 status

Si la configuration est correcte il n'y a pas de message d'erreur.

```
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled)
  Drop-In: /run/systemd/generator/bind9.service.d
           └─50-insserv.conf-$named.conf
   Active: active (running) since mer. 2015-12-09 07:02:15 CET; 2s ago
     Docs: man:named(8)
  Process: 1499 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
  Process: 1491 ExecReload=/usr/sbin/rndc reload (code=exited, status=0/SUCCESS)
 Main PID: 1502 (named)
   CGroup: /system.slice/bind9.service
           └─1502 /usr/sbin/named -f -u bind

déc. 09 07:02:15 srv-debian named[1502]: managed-keys-zone: loaded serial 3
déc. 09 07:02:15 srv-debian named[1502]: zone 0.in-addr.arpa/IN: loaded serial 1
déc. 09 07:02:15 srv-debian named[1502]: zone 255.in-addr.arpa/IN: loaded serial 1
déc. 09 07:02:15 srv-debian named[1502]: zone localhost/IN: loaded serial 2
déc. 09 07:02:15 srv-debian named[1502]: zone 127.in-addr.arpa/IN: loaded serial 1
déc. 09 07:02:15 srv-debian named[1502]: zone 3.25.172.in-addr.arpa/IN: loaded serial
2013112801
déc. 09 07:02:15 srv-debian named[1502]: zone grp3.info-msj.net/IN: loaded serial
2013112801
déc. 09 07:02:15 srv-debian named[1502]: all zones loaded
déc. 09 07:02:15 srv-debian named[1502]: running
déc. 09 07:02:15 srv-debian named[1502]: zone grp3.info-msj.net/IN: sending notifies
(serial 2013112801)
```

DHCP

Vocation faire DHCP dans un LAN.

Sudo aptitude -y install isc-dhcp-server

sudo vi /etc/dhcp/dhcpd.conf

```
LAN TSGERI
###-----------------------------------------------###
###------------LAN3 TSGERI------------------###
###_____________________________________###

subnet 172.25.3.0 netmask 255.255.255.0 {
        range   172.25.3.100 172.25.3.140;
        option routers  172.25.3.254;
        option broadcast-address 172.25.3.255 ;
        option domain-name-servers 172.25.3.106, 192.168.131.21 ;
        default-lease-time 600;
###-----------------------------------------------###
###---------------------------------------###
###_____________________________________###
```

Configuration par défaut, y modifier l'interface d'écoute pour le service.

sudo vi /etc/default/isc-dhcp-server

```
# Defaults for isc-dhcp-server initscript
# sourced by /etc/init.d/isc-dhcp-server
# installed at /etc/default/isc-dhcp-server by the maintainer scripts

#
# This is a POSIX shell fragment
#

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPD_CONF=/etc/dhcp/dhcpd.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPD_PID=/var/run/dhcpd.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="eth0"                                       a indiquer entre les guillemets
```

Test

```
xtbushido@srv-debian:~$ /etc/init.d/isc-dhcp-server status
● isc-dhcp-server.service - LSB: DHCP server
                Loaded: loaded (/etc/init.d/isc-dhcp-server)
                Active: active (running) since mar. 2015-12-08 16:03:27 CET; 10s ago
                Process: 16139 ExecStop=/etc/init.d/isc-dhcp-server stop (code=exited,
status=0/SUCCESS)
                Process: 16146 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited,
status=0/SUCCESS)
                CGroup: /system.slice/isc-dhcp-server.service
```

└─16155 /usr/sbin/dhcpd -q -cf /etc/dhcp/dhcpd.conf -pf /var/run/dhcpd.pid eth0

Apache

vi /etc/apache2/conf-enabled/security.conf

ServerTokens Prod

vi /etc/apache2/conf-enabled/security.conf

vi /etc/apache2/mods-enabled/dir.conf

line 2: add file name that it can access only with directory's name

DirectoryIndex
index.html index.htm

sudo vi /etc/apache2/apache2.conf

line 70: add to specify server name

ServerName www.server.world

sudo vi /etc/apache2/sites-enabled/000-default.conf

line 11: change to webmaster's email

ServerAdmin
webmaster@server.world

systemctl restart apache2

Youpi

VirtualHost

Création de site virtuel en associant un répertoire avec une adresse IP également virtuelles.

sudo vi /etc/apache2/sites-available/virtualhosts.conf

```
<VirtualHost 172.25.5.107:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error_1.log
        CustomLog ${APACHE_LOG_DIR}/access_1.log combined
</VirtualHost>

<VirtualHost 172.25.5.113:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/rtfm
        ErrorLog ${APACHE_LOG_DIR}/error_2.log
        CustomLog ${APACHE_LOG_DIR}/access_2.log combined
</VirtualHost>

<VirtualHost 172.25.5.123:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html3
        ErrorLog ${APACHE_LOG_DIR}/error_3.log
        CustomLog ${APACHE_LOG_DIR}/access_3.log combined
```

```
</VirtualHost>
```

Test

```
xtbushido@srv-debian:~$ sudo service apache2 status
● apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2)
   Active: active (running) since mer. 2015-12-09 05:50:24 CET; 7s ago
  Process: 1259 ExecStart=/etc/init.d/apache2 start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/apache2.service
           ├─810 /usr/sbin/apache2 -k start
           ├─869 /usr/sbin/apache2 -k start
           └─870 /usr/sbin/apache2 -k start

déc. 09 05:50:24 srv-debian apache2[1259]: Starting web server: apache2.
```

VsFTP

FTP pour utilisateur locaux ; modifier :

/etc/vsftpd.conf

```
.# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES                        Autoriser l'ecriture
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
# You may fully customise the login banner string:
ftpd_banner=Welcome to Read The Fucking Manual.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may restrict local users to their home directories.  See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list
```

Donc créons le fichier :

/etc/vsftpd.chroot_list

Ce pendant

Monitorer un serveur

Glances

Découvrez glances un superbe outils de monitoring proposant une représentation graphique de l'activité du system, en console ou à travers un navigateur.

Utiliser le script d'auto-installation

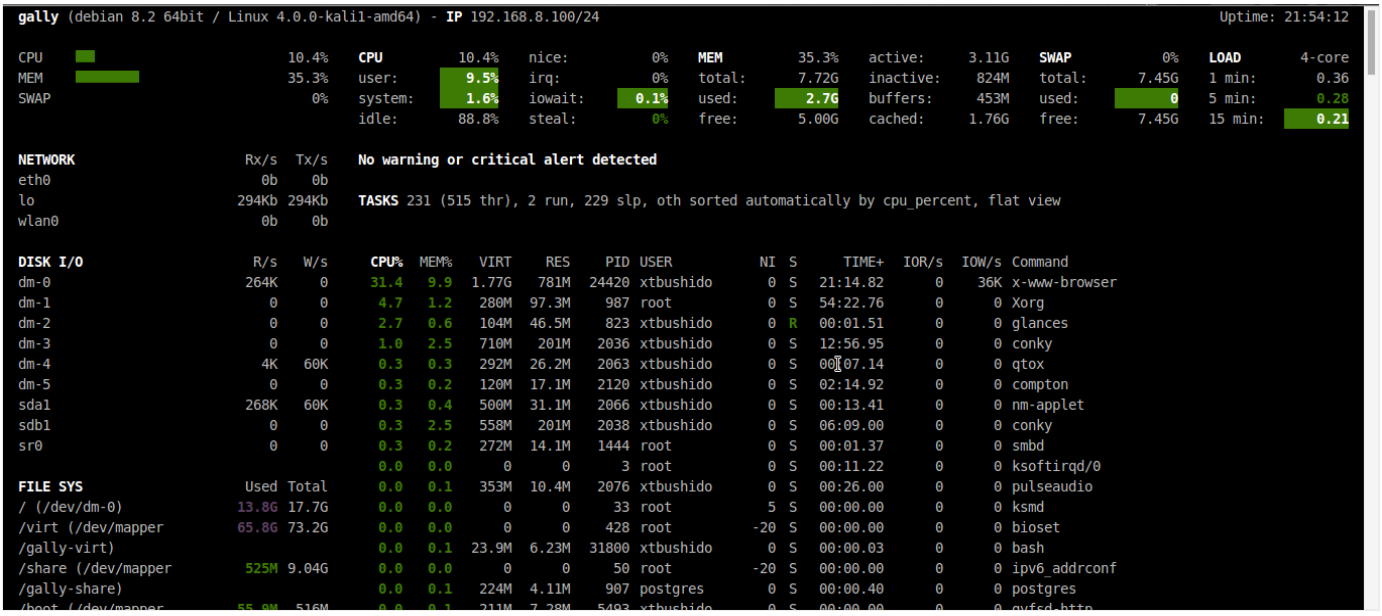
```
wget -O- http://bit.ly/glances | /bin/bash
```

Qui récupérera par exemple :
sudo apt-get install -y --force-yes python-dev python-pip lm-sensors

Lancer avec

```
glances -w
```

Glances web server started on http://0.0.0.0:61208/



rkhunter

Execution :

```
sudo rkhunter -c
```

Rkhunter est un outil permettant de vérifier les modifications des fichiers de configuration et la présence de rootkit ; backdoor etc...etc...

A l'installation rkhunter scanne l'intégralité des fichiers de configuration, appliquera un hash afin d'opérer des comparaisons dans les prochaine execution .

Rkhunter enregistrera un fichier de log dans :

/var/log/rkhunter.log

```
       System checks summary
=====================

File properties checks...
    Files checked: 145
    Suspect files: 0

Rootkit checks...
    Rootkits checked : 379
    Possible rootkits: 0

Applications checks...
    All checks skipped

The system checks took: 2 minutes and 38 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

Lynis

Lynis est un second utilitaire qui recherchera la présence de fichiers suspect.

Il analysera également l'intégralité du system de fichiers et produira un fichier de log dans :

/var/log/lynis.log

Execution :

sudo lynis --auditor "username" -c

```
[ Lynis 1.6.3 ]

################################################################################
 Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
 welcome to redistribute it under the terms of the GNU General Public License.
 See the LICENSE file for details about using this software.

 Copyright 2007-2014 - Michael Boelen, http://cisofy.com
 Enterprise support and plugins available via CISOfy - http://cisofy.com
################################################################################

[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Clearing log file (/var/log/lynis.log)...                 [ DONE ]

  ---------------------------------------------------
  Program version:           1.6.3
  Operating system:          Linux
  Operating system name:     Debian
  Operating system version:  8.2
  Kernel version:            3.16.0
  Hardware platform:         x86_64
  Virtual machine:           Unknown
  Hostname:                  srv-debian
  Auditor:                   xtbushido
  Profile:                   /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
```

Netstat -tulpn

Mieux encore que netstat -an, -tulpn classera de manière claire les connexions internet actives.

Très pratique !

A faire en ROOT sans quoi vous n'aurez pas les même résultats, je n'ai pas mis ici l'intégralité du retour.

```
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat        PID/Program
name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      1423/mysqld
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      1444/smbd
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1080/apache2
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      796/cupsd
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      887/postgres
tcp        0      0 127.0.0.1:666           0.0.0.0:*               LISTEN      951/darkstat
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      1444/smbd
tcp        0      0 0.0.0.0:1022            0.0.0.0:*               LISTEN      745/sshd
```

netstat -ns

Triera par type de connexion : IP, ICMP, TCP ; UDP

Watch

Dédier un terminal avec watch :

watch netstat -tulpn

ps -ef |grep bind9

```
xtbushi+ 14644   883  0 15:31 pts/1    00:00:00 grep bind9
```

ps -ef |grep dhcpd

```
root       710     1  0 13:08 ?        00:00:00 /usr/sbin/dhcpd -q -cf
/etc/dhcp/dhcpd.conf -pf /var/run/dhcpd.pid
xtbushi+ 14650   883  0 15:31 pts/1    00:00:00 grep dhcpd
```

ps -ef |grep apache2

```
root     13614     1  0 15:07 ?        00:00:00 /usr/sbin/apache2 -k start
www-data 13617 13614  0 15:07 ?        00:00:00 /usr/sbin/apache2 -k start
www-data 13618 13614  0 15:07 ?        00:00:00 /usr/sbin/apache2 -k start
xtbushi+ 14662   883  0 15:31 pts/1    00:00:00 grep apache2
```

Scanner un serveur distant

Il existe un outil nommé nmap de scanne de port, le scann de port n'est pas vraiment légal, il est perçu comme une attaque par le serveur scanné.

Il fournit des renseignements très, très complet.

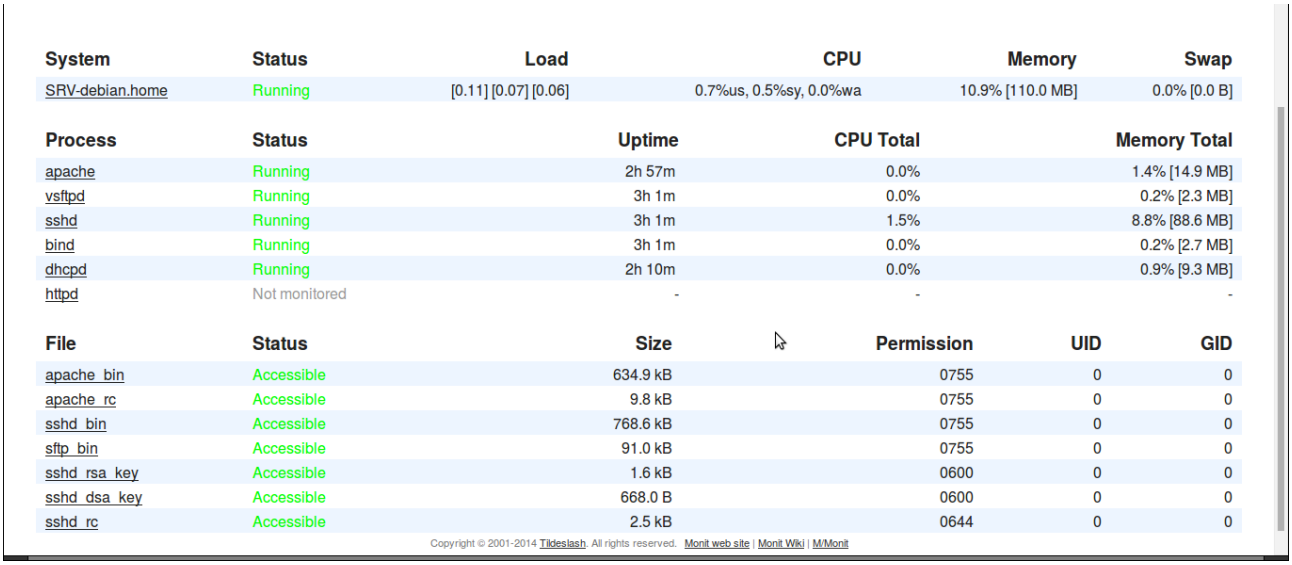
sudo apt-get install nmap
sudo nmap -v 172.25.0.6

Intense scan

sudo nmap -T4 -A -v 172.25.3.106

Starting Nmap 7.00 (https://nmap.org) at 2015-12-09 09:51 CET

Monit



System	Status	Load	CPU	Memory	Swap
SRV-debian.home	Running	[0.11] [0.07] [0.06]	0.7%us, 0.5%sy, 0.0%wa	10.9% [110.0 MB]	0.0% [0.0 B]

Process	Status	Uptime	CPU Total	Memory Total
apache	Running	2h 57m	0.0%	1.4% [14.9 MB]
vsftpd	Running	3h 1m	0.0%	0.2% [2.3 MB]
sshd	Running	3h 1m	1.5%	8.8% [88.6 MB]
bind	Running	3h 1m	0.0%	0.2% [2.7 MB]
dhcpd	Running	2h 10m	0.0%	0.9% [9.3 MB]
httpd	Not monitored	-	-	-

File	Status	Size	Permission	UID	GID
apache_bin	Accessible	634.9 kB	0755	0	0
apache_rc	Accessible	9.8 kB	0755	0	0
sshd_bin	Accessible	768.6 kB	0755	0	0
sftp_bin	Accessible	91.0 kB	0755	0	0
sshd_rsa_key	Accessible	1.6 kB	0600	0	0
sshd_dsa_key	Accessible	668.0 B	0600	0	0
sshd_rc	Accessible	2.5 kB	0644	0	0

Monit se charge de surveiller des processus avec leurs identifiants :les pid, processus que l'on doit lui indiquer, il doit ensuite constater leurs présences ;

en cas d'absence, il nous retourne des informations (comme les constantes pour un patient à l'hôpital).

Si il ne voit pas le PID, il relance le service.

Pour activer Monit et y accéder via un navigateur , modifier le fichier :

/etc/monit/monitrc

et décommenter les lignes suivantes.

```
 set httpd port 2812 and
#    use address localhost  # only accept connection from localhost
#    allow localhost        # allow localhost to connect to the server and
 allow admin:monit      # require user 'admin' with password 'monit'
#    allow @monit           # allow users of group 'monit' to connect (rw)
#    allow @users readonly  # allow users of group 'users' to connect readonly
```

Commande de service

service monit (start|stop|reload|start)

/etc/monit/conf.d/

Ce répertoire contient des fichiers complémentaires de configuration :

ATTENTION A LA SYNTAXE

Vérifier la syntaxe avec :

monit -t

cette option indiquera l'erreur dans le fichier.

Ci dessous les fichiers pour :

SSH, BIND, et DHCP

Ssh

Note : le check file est compris dans le fichier .

```
  check process sshd with pidfile /var/run/sshd.pid ##c'est ce que monit doit
surveiller
    group system
    group sshd
    start program = "/etc/init.d/ssh start" ##Commande pour démarrer le service
    stop  program = "/etc/init.d/ssh stop" ##Commande pour stopper le service
    if failed host localhost port 22 with proto ssh then restart
    if 5 restarts with 5 cycles then timeout
    depend on sshd_bin
    depend on sftp_bin
    depend on sshd_rc
    depend on sshd_rsa_key
    depend on sshd_dsa_key

  check file sshd_bin with path /usr/sbin/sshd
    group sshd
    include /etc/monit/templates/rootbin

  check file sftp_bin with path /usr/lib/openssh/sftp-server
    group sshd
    include /etc/monit/templates/rootbin

  check file sshd_rsa_key with path /etc/ssh/ssh_host_rsa_key
    group sshd
    include /etc/monit/templates/rootstrict

  check file sshd_dsa_key with path /etc/ssh/ssh_host_dsa_key
    group sshd
    include /etc/monit/templates/rootstrict

  check file sshd_rc with path /etc/ssh/sshd_config
    group sshd
    include /etc/monit/templates/rootrc
```

Bind

Tous les services ne semble pas s'identifier de la même manière.

```
check process bind
 matching bind
 start program = "/etc/init.d/bind9 start"
 stop program = "/etc/init.d/bind9 stop"
 if failed host 127.0.0.1 port 53 type tcp protocol dns then restart
 if failed host 127.0.0.1 port 53 type udp protocol dns then restart
 if 5 restarts within 5 cycles then timeout
```

Vsftp

```
Check process vsftpd
 matching vsftpd
start program = "/usr/sbin/vsftpd start"
stop program = "/usr/sbin/vsftpd stop"
if failed port 21 protocol ftp then restart if 5
restarts within 5 cycles then timeout
```

Status

service monit status

```
● monit.service - LSB: service and resource monitoring daemon
   Loaded: loaded (/etc/init.d/monit)
   Active: active (running) since jeu. 2015-12-10 22:30:15 CET; 9s ago
  Process: 8240 ExecStop=/etc/init.d/monit stop (code=exited, status=0/SUCCESS)
  Process: 1204 ExecReload=/etc/init.d/monit reload (code=exited, status=0/SUCCESS)
  Process: 8268 ExecStart=/etc/init.d/monit start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/monit.service
           ├─2594 /usr/sbin/dhcpd -q -cf /etc/dhcp/dhcpd.conf -pf /var/run/dhcpd.pid eth0
           └─8272 /usr/bin/monit -c /etc/monit/monitrc

déc. 10 22:30:15 srv-debian monit[8268]: Starting daemon monitor: monit.
```

Memento

Commande pour controler la syntaxe des fichiers de configuration

OpenSSH

/usr/sbin/sshd -t && echo $?

/usr/sbin/sshd -T

Apache

/usr/sbin/apache2 -t

apachectl configtest

nginx

/usr/local/nginx/sbin/nginx -t

/usr/local/nginx/sbin/nginx -t -c /usr/local/nginx/conf/nginx.conf

lighttpd

/usr/local/sbin/lighttpd -t -f /usr/local/etc/lighttpd/cyberciti.biz/lighttpd.conf

Bind (named server config)

named-checkconf /etc/named.conf

Bind (zone syntx)

named-checkzone nomdedomai.ne /var/named/zone.nodedomai.ne

Squid proxy

/usr/sbin/squid -k check

/usr/sbin/squid -k parse

MySQL server

mysqld --verbose --help

/usr/libexec/mysqld --verbose --help 1>/dev/null

Postfix MTA

postfix check

postfix -vvv

Samba SMB/CIFS

testparm -v

tcpd

tcpdchk

tcpdchk -v

dhcpd (DHCP / BOOTP) server

dhcpd -t -cf /path/to/dhcpd.testing.conf

vsftpd server

vsftpd -olisten=NO /path/to/vsftpd.testing.conf

nagios

```
nagios -v /path/to/testing/nagios.cfg
```

Openntpd NTPD server

```
ntpd -d -f /usr/local/etc/ntpd.conf -n
```

Xorg (X11 Server)

```
Xorg -config /path/to/xorg.conf.new -retro
```

syslogd / rsyslogd

```
rsyslogd -c4 -f /etc/rsyslog.testing.conf -N 1
```

CUPS Printing System

```
cupsd -f -c /path/to/cupsd.testing.conf -t
```

slapd (OpenLDAP)

```
slapd -Tt
```

varnishd

```
varnishd -C -f /path/to/wordpress.vlc
```

exim MTA

```
exim -bV
```

Bash/Ksh scripts

```
bash -n ./myscript
ksh -n /path/to/script.ksh
```

BSD pf firewall

```
pfctl -nf /etc/pf.conf
```

proftpd

```
proftpd -t -c /path/to/proftpd.testing.conf
```

Perl scripts

```
perl -c /path/to/script.pl
perl -wc /path/to/script.pl
```

References

Debian

Debian_hand_book

Linuxsecurity

linux-administrator_guide

Manpages-fr

Linux

Linux-france

Monitoring

Shinken

rtfm:shinken

Monit

rtfm:monit

Glances

rtfm:glances

Wireshark tshark

DNS

Bind9

Unbound

ChaosComputerClub