DEBIAN

==========

Comenzi pentru procesor:
lscpu
sau:
more /proc/cpuinfo
Pentru RAID:
cat /proc/mdstat

==========

pveversion -v
Note: Please always update a new ISO install to the latest available packages:
apt-get update
apt-get dist-upgrade
apt-get clean

==========

Daca la bootare apare un mesaj de genul "i8042 Can't read CTR while initializing i8042", atunci:
Had to set USB Emulation to "OFF" in the BIOS.

==========

Dezactivarea CTRL+ALT+DEL in DEBIAN:
Se merge in /etc/inittab si se cauta linia:

```
# what to do when CTRL-ALT-DEL is pressed.
ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now
```

Trebuie sa schimbam (sa o stergem, sa o comentam sau sa o modificam) aceasta linie.

Un exemplu de modificare:

```
ca:12345:ctrlaltdel:/sbin/shutdown "CTRL-ALT-DEL is disabled"
```

In cazul in care o modificam, la apasarea CTRL-ALT-DEL, va da sugestii despre comanda shutdown.
In cazul in care o comentam, la apasarea CTRL-ALT-DEL, nu va afisa nimic. Poate ca asta e cea mai buna solutie.

Dupa ce facem modificarea, trebuie sa reincarcam init pentru a activa modificarea:
init q

Sau in Debian 9.4:

```
sudo rm /lib/systemd/system/ctrl-alt-del.target
sudo ln -s /dev/null /lib/systemd/system/ctrl-alt-del.target
sudo systemctl daemon-reload
```

==========
Disable Ctrl+Alt+Delete in Ubuntu (14.04):

First and foremost, anyone that has physical access to the keyboard can simply use the Ctrl+Alt+Delete key combination to reboot the server without having to log on. Sure, someone could simply unplug the power source, but you should still prevent the use of this key combination on a production server. This forces an attacker to take more drastic measures to reboot the server, and will prevent accidental reboots at the same time.

    To disable the reboot action taken by pressing the Ctrl+Alt+Delete key combination, comment out the following line in the file /etc/init/control-alt-delete.conf.

    #exec shutdown -r now "Control-Alt-Delete pressed"

In Ubuntu 16.04LTS:

To disable the reboot action taken by pressing the Ctrl+Alt+Delete key combination, run the following two commands:

```
sudo systemctl mask ctrl-alt-del.target
sudo systemctl daemon-reload
```

==========

Pentru a schimba mesajul de logare in fiecare consola, trebuie editat fisierul /etc/issue
Aici se editeaza mesajul de afisat, de exemplu se inlocuieste numele sistemului si al versiunii cu orice altceva.
Se poate folosi:
Las doar /l
/l <-- Pentru prezentarea numelui de consola
/n <-- Nu stiu exact ce afiseaza (nume server, versiune Debian, etc)
==========
Pentru a edita cu NANO:
nano /home/fisiere/configurari.txt

Pentru a edita cu MCEDIT:
mcedit /home/fisiere/configurari.txt
==========
Editorul implicit in DEBIAN este NANO.
Pentru a schimba editorul implicit:
update-alternatives --config editor
apoi se alege o cifra sau daca se doreste pastrarea se apasa ENTER.

Daca se doreste ca editorul implicit sa fie NANO dar din cadrul MC sa se editeze cu MCEDIT, atunci in MC se seteaza in meniu
acest lucru. Pentru aceasta: F9 --> Options --> Configurarion... --> si se bifeaza: "use internal edit".

==========
Pentru a instala nano in Ubuntu 16.04 LTS
sudo apt-get update
sudo apt-get install nano
==========
Pentru a edita cu VIM:
A --> Se intra in modul insert la sfarsit de linie
La final, cu ESCAPE se iese din modul insert.
:wq ENTER --> Se salveaza si se iese din fisier.
:w --> Se salveaza.
:q --> Se iese din fisier.
:q! --> Se iese din fisier fara salvare.
==========
Ecranul se curata cu clear
==========
Pentru copierea unui fisier:
cp /etc/issue.net /etc/issue.net.original

```
+-------------------------------------------+
| + + + + A C C E S S   D E N I E D + + + + |
+-------------------------------------------+
| All trafic, transmissions and protocols   |
| from and to this machine are being logged. |
+-------------------------------------------+
| Your IP address has been recorded.        |
|                                           |
| Access to this machine is for authorized  |
| administrators only.                      |
| If you are not an authorized user,        |
| please leave now.                         |
|                                           |
| You were warned!                          |
+-------------------------------------------+
```

---

sau:

****

NOTICE TO USERS

This computer system is the private property of its owner, whether individual, corporate or government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to your employer, to authorized site, government, and law enforcement personnel, as well as authorized officials of government agencies, both domestic and foreign.

By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of such personnel or officials. Unauthorized or improper use of this system may result in civil and criminal penalties and administrative or disciplinary action, as appropriate. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

****

==========
Inslatarea serverului OpenBSD Secure Shell sshd in DEBIAN:
apt-get update
apt-get install ssh
Pentru 16.04LTS: apt-get install openssh-server
apt-get clean
Pentru configurarea serverului SSH, editez fisierul:
/etc/ssh/sshd_config
Bannerul afisat la logare il editez in:
/etc/issue.net
Dupa ce termin de editat, restartez serverul:
/etc/init.d/ssh restart
sau:
service ssh restart
sau:
stop ssh
sau:
start ssh
Conectarea SSH se face astfel:
ssh Nume_User@Adresa_IP -p Numar_Port

In cazul in care se conecteaza prea greu la SSH, aceasta se intampla pentru ca serverul verifica rezolutia de nume.
Pentru a corecta asta, sunt 2 metode:

1. Se editeaza in /etc/ssh/sshd_config, optiunea: UseDNS no
2. A 2-a metoda dezactiveaza serviciul Avahi daemon (cauta pe Internet despre asta!)

==========

OpenSSH permite suplimentar transferul securizat de fisiere. Se utilizeaza comanda scp, putandu-se transfera atat fisiere
de la serverul distant pe calculatorul local cat si invers. Pentru aceasta:

```
scp calea/nume_fisier_de_trimis
nume_user@nume_host_sau_IP:/calea/la/locul/unde/pun/fisierul
```

Exemplu: Pentru a copia fisierul password de pe calculatorul local (florin) la serverul distant (earth):

```
steve@florin:~$ scp /etc/passwd steve@earth:
steve@earth's password:
passwd     100% |*****************************|   918       00:00
```

Deoarece nu s-a specifica un folder de destinatie, fisierul va fi transferat in directorul home al userului
de pe masina distanta.

Pentru a transfera mai multe fisiere se poate copia folderul recursiv, cu flagul -r.

Pentru transferul cu o masina Windows se poate folosi WinSCP. Acesta permite transferul cu drag and drop.

Avand OpenSSh instalat, nu mai avem nici un motiv sa rulam sisteme nesigure, precum FTP, pentru transferul de fisiere
spre si de la serverele Linux.

==========

Pentru a crea un nou user, trebuie sa ma loghez ca root, sau din user normal sa folosesc comanda su.
Apoi folosesc comanda:

```
adduser Nume_User
```

Mi se cer informatii precum:

```
Full Name []: Dena Florin
Room Number []: 1
Work Phone []: 0723 20 60 19
Home Phone []: 031 41 999 66
Other []: SysAdmin for CLD.RO
Is the information correct? [Y/n] Y
```

Se poate sterge acest cont si directorul lui home, folosind:

```
deluser --remove-home Nume_User
```

(*** Daca vreau sa adaug un user care sa aiba si drept de login, atunci folosesc comanda:

useradd Nume_User
Apoi setez parola pentru el:
passwd Nume_User
Apoi creez un director pentru acest utilizator, si ii dau drepturi pentru acest director:
mkdir /home/Nume_User
chown Nume_User:users /home/Nume_User
Daca se omite comanda chown, acest user nu va avea permisiuni de a salva fisiere in interiorul folderului lui din home *)

Redenumire user din 'tom' in 'jerry' pe Ubuntu Linux:
Utilizam comanda usermod. Ea poate modifica fisierele de sistem ale conturilor (precum /etc/passwd) pentru a reflecata
schimbarile specificate in linie de comanda. Sintaxa este:
usermod -l {new-login-name} {current-old-login-name}

De exemplu, pentru redenumirea id-ului de logare de la tom la jerry:
$ sudo usermod -l jerry tom
Pentru modificarea noilor schimbari:
$ id jerry

Pentru a schimba numele grupului avem comanda groupmod
$ groupmod --help
Usage: groupmod [options] GROUP
Options:
  -g, --gid GID   change the group ID to GID
  -h, --help   display this help message and exit
  -n, --new-name NEW_GROUP   change the name to NEW_GROUP
  -o, --non-unique   allow to use a duplicate (non-unique) GID
  -p, --password PASSWORD   change the password to this (encrypted) PASSWORD

De exemplu:
$ groupmod -n new_group_name old_group_name

==========
Daca m-am logat ca un alt user decat root, pentru a trece in root am mai multe variante:

Pentru a trece in root cu drepturi depline fara pastrarea mediului userului curent:
su -l
Pentru a trece in root cu pastrarea catorva functionalitati ale mediului userului curent:
su
Se mai poate trece in root si cu:
su root   <<=== Asta o folosesti
Pentru a iesi de sub userul root si a reveni la userul anterior:
exit
altfel, se iese cu:
logout

==========
==========
Pentru a opri serverul:
init 0
sau in mod multiuser:
shutdown -h now
sau in mod singleuser:
poweroff -i -f
Pentru a restarta:
reboot
==========
==========
Administratorul sistemului poate schimba parola oricarui user, folosind:
passwd Nume_User
==========
==========
PROXMOX VE
Template-urile si imaginile ISO, containerele sunt stocate in: /var/lib/vz
De exemplu CT101 se gaseste in /var/lib/vz/private/101/
Pentru a adauga un nou user, mai intai creez un grup. Creez userul si ii atasez grupul anterior creat. Apoi setez
permisiunea de grup atasata unui rol.

Pentru back-up-uri mai intai se creaza un storage - sub forma unui director. L-am creat in /var/lib/vz/storage1

Conectarea web foloseste portul 8006
Consolele Java folosesc porturi intre 5900-...
==========
==========
TCP wrapper
As outlined on the forums post, you can use TCP Wrapper. TCP wrapper uses 2 files, /etc/hosts.allow and /etc/hosts.deny
Edit /etc/hosts.allow and add your subnet
sshd : 192.168.0.

Edit /etc/hosts.deny, and deny all
ALL : ALL

See also
http://ubuntu-tutorials.com/2007/09/02/network-security-with-tcpwrappers-hostsallow-and-hostsdeny/
dupa cum urmeaza:

Network Security with tcpwrappers (hosts.allow and hosts.deny)

I thought today I would outline a few tips on network security with tcpwrappers or, as you’re probably more familiar, the hosts.allow and hosts.deny files. How you can use them? What applications are compatible? etc. I know network security is a really broad topic, but this will hopefully be enough to get you going and

understand some more basics of securing your machine.

tcpwrappers compatibility

The first thing to remember is that not every network-based application on your machine is compatible with tcpwrappers. The restrictions on hosts.allow or hosts.deny are only valid if they refer to the tcpwrappers library. How can you find out if your application is compatible? Use this command:
    ldd /path/to/binary | grep libwrap (general example)
    ldd /usr/sbin/sshd | grep libwrap (shows that the sshd refers to libwrap)
    ldd /usr/sbin/apache2 | grep libwrap (show that apache does not refer to libwrap)

In the basic example above we see that the sshd (ssh server) is referring to the libwrap.so, so we can tell that any restrictions in hosts.allow and hosts.deny are applicable to that service. We also see that apache2 does not refer to libwrap.so, so any restrictions outlined there do not apply to apache2 connections. (ie; you could lock down ssh but apache2 is still wide open)

hosts.allow and hosts.deny

These two files, located in your /etc/ folder, allow you to limit or permit connections from specific hosts or ips. Using these two files you could setup a whitelisting firewall or blacklist. Remember, as mentioned in the compatibility section, this only applies to the services referring to libwrap. If you are running services outside of the scope of libwrap.so this may not be the best solution for you in terms of firewalling.

/etc/hosts.allow

ALL: 127.0. [::1] (the 127.0. range is allowed, as well as the localhost ipv6 address)

sshd : 192.168.0.5 (specific IP) 192.168.0. (specific range) EXCEPT 192.168.0.10 (range exceptions)

/etc/hosts.deny

ALL : ALL (denying all services to all hosts)

This example would allow connections from localhost on ipv4 and ipv6 for all services and also explicitly allow ssh connections from the 192.168.0.5 address, the entire 192.168.0. range, but excluding the 192.168.0.10 host. The hosts.deny then outright denies all services for all hosts. This is a very basic example but hopefully it gets the idea across. You could also reverse the contents of the two files in the example above and do blacklisting. ALL : ALL are allowed with the exceptions of services and ips listed in the hosts.deny.

The syntax of the hosts.allow and hosts.deny files are:

service(s) : ips or hosts

You can comma separate the list of services you want to allow or deny and make a similar list of hosts/ips to allow or deny. Very simple syntax.

conclusion

The hosts.allow and hosts.deny files are very flexible and allow you to lock down your network in very granular ways. The limitation of some applications not honoring hosts.allow and hosts.deny is the biggest thing to remember. Make sure the service you are trying to block refers to libwrap.so before you start writing rules or you may sit and wonder why your rules don’t work, when its really the application itself not being compatible.

==========

UFW - UNCOMPLICATED FIREWALL - Instrument de configurare a firewall-ului (iptables)

Instalarea:

```
apt-get update
apt-get install ufw
```

Verificarea starii:

```
ufw status
```

Pentru a permite totul se da comanda:

```
ufw default allow
```

Se recomanda la inceput sa se blocheze totul:

```
ufw default deny
```

Pentru a porni UFW si a-l face disponibil la pornirea sistemului:

```
ufw enable
```

Pentru a opri UFW si a-l face inactiv la pornirea sistemului:

```
ufw disable
```

Pentru a seta reguli ce permit pachete incoming, sintaxa generala este:

```
ufw allow <port>/<optional: protocol>
```

Exemplu:

```
ufw allow 53
```

sau:

```
ufw allow 53/tcp
```

sau:

```
ufw allow 53/udp
```

Pentru a seta reguli ce interzic pachete incoming, sintaxa este:

```
ufw deny <port>/<optional: protocol>
```

Exemplu:

```
ufw deny 53
```

sau:

ufw deny 53/tcp
sau:
ufw deny 53/udp

Pentru a sterge reguli existente:
Daca regul generala este:
ufw deny 80/tcp
pentru a sterge regula:
ufw delete deny 80/tcp

UFW poate permite sau interzice servicii pe care le citeste din /etc/services
Lista acestora se afiseaza cu:
less /etc/services

Pentru a permite / interzice dupa numele serviciului, sintaxa generala este:
ufw allow <nume_serviciu>
ufw deny <nume_serviciu>

Exemplu:
ufw allow ssh
ufw deny ssh

Pentru a permite / interzice interogarea logurilor:
ufw logging on
ufw logginf off

Pentru a permite / interzice dupa un anumit ip, sintaxa generala este:
ufw allow from <Adresa_IP>
ufw deny from <Adresa_IP>

Pentru a permite / interzice dupa un anumit port si adresa IP, sintaxa este:
ufw allow from <Adresa_IP> to <protocol> port <numar_port>
ufw deny from <Adresa_IP> to <protocol> port <numar_port>

Exemple:
Pentru a permite pachete de la 207.46.232.182
ufw allow from 207.46.232.182

Se poate utiliza o masca de retea:
ufw allow from 192.168.1.0/24

Pentru a permite adresei IP 192.168.0.4 accesul la portul 22:
ufw allow from 192.168.0.4 to any port 22

Implicit, UFW permite cereri PING
Daca se doreste blocarea ping-urilor trebuie sa se editeze fisierul
/etc/ufw/before.rules
Aici se modifica cele 5 linii de la # ok icmp codes, si se schimba cuvantul ACCEPT
cu DROP

Exemple:
Daca nu se specifica in sau out, atunci regula se aplica pentru traficul de intrare.

```
ufw disable && ufw enable
ufw allow in http
ufw reject out smtp
ufw deny proto tcp to any port 80
ufw deny proto tcp from 10.0.0.0/8 to 192.168.0.1 port 25
ufw deny proto tcp from 2001:db8::/32 to any port 25
ufw allow proto tcp from any to any port 80,443,8080:8090
ufw limit ssh/tcp
ufw reject auth
ufw allow in on eth0 to any port 80 proto tcp
ufw delete 3
ufw insert 3 deny to any port 22 from 10.0.0.135 proto tcp
ufw status numbered
ufw allow log 22/tcp
ufw deny proto udp from 1.2.3.4 to any port 514
ufw allow proto udp from 1.2.3.5 port 5469 to 1.2.3.4 port 5469
ufw allow proto tcp from any to any port 22
ufw allow to any port ssh
ufw allow from any to any port openvpn
ufw allow from 10.xxx.xxx.0/24 to 10.xxx.xxx.0/24
ufw app list
ufw allow out 20,21,22,25,80,139,443,5900,8001/tcp
ufw allow out 53,137,138/udp
ufw deny out to any
ufw status numbered
ufw allow 6881:6999/tcp
ufw delete deny out to any
ufw delete deny out to all
ufw logging off
ufw logging on
ufw insert 4 allow 22
ufw logging on|off|LEVEL
ufw allow from 10.0.0.0/8 to any app myapps-1
ufw app list
ufw info myapps-1
ufw allow from 192.168.0.0/16 to any app <name>
ufw app info <name>
ufw app update <name>
ufw app update --add-new <name>
ufw app default <policy>
ufw logging LEVEL     // LEVEL poate fi off, low, medium, high, full
ufw show raw
ufw allow to 10.0.0.1 proto ipv6
ufw allow to 10.0.0.1 from 10.4.0.0/16 proto ipv6
ufw reset       // se sterg toate regulile cu o singura comanda
ufw status verbose
ufw version
```

ATENTIE !!!
Ordinea in care sunt puse regulile conteaza:
- Mai intai se pun regulile specifice si apoi cele generale.
- De citit Exemplele avansate!
==========
PORTURI:
22 TCP Secure Shell (SSH), secure logins, file transfers (scp, sftp) si port forwarding
20 TCP FTP - transfer de date
21 TCP FTP - control (comenzi)
53 TCP si UDP Domain Name System (DNS)
123 UDP Network Time Protocol (NTP) - Utilizat pentru sincronizarea ceasului
80 TCP Hypertext Transfer Protocol (HTTP)
443 TCP Hypertext Transfer Protocol over SSL/TLS (HTTPS)
25 TCP Simple Mail Transfer Protocol (SMTP) - Utilizat pt rutare e-mail-uri intre e-mail servere
110 TCP Post Office Protocol v3 (POP3)
995 TCP Post Office Protocol v3 over SSL/TLS (POP3S)
143 TCP Internet Message Access Protocol (IMAP) - managementul mesajelor de e-mail
993 TCP Internet Message Access Protocol over SSL (IMAPS)
Basic services:
DNS (Domain Name Service) = protocol udp port 53.
Web browsing = http protocol tcp port 80.
Secure web browsing = https protocol tcp port 443.
Mail = protocol tcp port 25.
FTP = protocol tcp port 20 and 21.
SSH = protocol tcp port 22.
VNC = protocol tcp port 5900.
Samba uses multiple ports , protocol udp ports 137 and 138 as well as tcp ports 139, and 445.
IRC protocol tcp, Ubuntu Servers defaults to 8001.
==========
Pentru a downloada un template OpenVZ, trebuie sa accesez:
http://wiki.openvz.org/Download/template/precreated
==========
Pentru a vizualiza numarul de procesoare / core-uri si informatii despre ele:
cat /proc/cpuinfo
Alte comenzi:
uname --help
uname -a
==========

Serverul de timp setat este NTPD

Though timesyncd is fine for most purposes, some applications that are very sensitive to even the slightest perturbations in time may be better served by ntpd, as it uses more sophisticated techniques to constantly and gradually keep the system time on track.

Before installing ntpd, we should turn off timesyncd:

sudo timedatectl set-ntp no

Verify that timesyncd is off:

timedatectl

Look for Network time on: no in the output. This means timesyncd has been stopped. We can now install the ntp package with apt-get:

sudo apt-get install ntp

ntpd will be started automatically after install. You can query ntpd for status information to verify that everything is working:

sudo

Pentru instalare:
apt-get update
apt-get install ntp
El ajusteaza periodic (la intervale de timp de genul zecilor / sutelor de secunde) ceasul sistemului.
Porneste automat prin setarea acestui lucru in /etc/cron.dayly/ntp
Configurarea se face in /etc/ntp.conf
Pentru restartarea serviciului se foloseste:
/etc/init.d/ntp restart
Pentru testare se folosesc interogari (query) ntp:
ntpq -p
sau:
ntpq -pn
sau:
ntpq
peers
Iar pentru verificarea starii:
association
Se iese cu CTRL+C sau q si apoi ENTER

- Asterisk-ul (*) indica sursa cu care suntem sincronizati.
o este sursa PPS pentru ntpd (ppspeer, doar daca avem un sistem capabil PPS si un ceas de referinta)
+ candidat, el este considerat o sursa buna
- outlyer, cand calitatea nu este suficient de buna

x falseticker, aceste este considerat ca distribuie un ceas gresit.

- refid arata identificatorul sursei de timp la care masina distanta este sincronizata. Poate fi de exemplu un ceas
radio sau un alt server ntp.
- st este ordinul stratum al masinii distante. 16 este "nesincronizat". 0 este cea mai buna valoare, si poate fi de
exemplu un ceas radio sau un server ntp privat cu ceas cessium.
- remote listeaza adresa IP sau numele de host al sursei.
- when indica cate secunde au trecut de cand sursa a fost interogata.
- poll indica intervalul de interogare. Aceasta valoare creste in functie de acuratetea ceasului local.
- reach este un numar in octal ce indica increderea in sursa. Valoarea 377 indica ca sursa a raspuns la ultimele
opt interogari succesive. Fiecare bit 1 inseamna ca pachetul de timp a fost receptionat.
- offset este diferenta de timp in milisecunde intre sursa si ceasul local.
- jitter - deplasamentul de timp observat fata de timpul sursei.
- delay - este timpul in milisecunde necesar la programarea datelor intre serverul distant si cel local. Valoarea poate
fi obtinuta si prin comanda ping catre ip-ul serverului distant.

In Debian - Dezacivarea / activarea serviciilor la start-up:

Debian Linux has its own script to enable and disable services across runlevels. It is called update-rc.d. Going by the above example, you can enable apache webserver as follows:

```
# update-rc.d apache2 defaults
```

… this will enable the apache webserver to start in the default run levels of 2,3,4 and 5. Of course, you can do it explicitly by giving the run levels instead of the “defaults” keyword as follows:

```
# update-rc.d apache2 start 20 2 3 4 5 . stop 80 0 1 6 .
```

The above command modifies the sym-links in the respective /etc/rcX.d directories to start or stop the service in the destined runlevels. Here X stands for a value of 0 to 6 depending on the runlevel. One thing to note here is the dot (.) which is used to terminate the set which is important. Also 20 and 80 are the sequence codes which decides in what order of precedence the scripts in the /etc/init.d/ directory should be started or stopped.

And to disable the service in all the run levels, you execute the command:

```
# update-rc.d -f apache2 remove
```

Here -f option which stands for force is mandatory.
But if you want to enable the service only in runlevel 5, you do this instead:

```
# update-rc.d apache2  start 20 5 . stop 80 0 1 2 3 4 6 .

De exemplu, ca sa dezactivez POSTFIX la pornire:
update-rc.d -f postfix remove                          <<====== A functionat

Dupa ce restartez, postfix-ul va aparea ca oprit.

Alta modalitate:
in Debian, you can remove the startup-symlinks in the runlevels:
for ex.
Code:
sudo rm -v /etc/rc*/S[0-9][0-9]postfix          <<====== A functionat
Va aparea:
Code:
removing `/etc/rc2.d/S20postfix'
removing `/etc/rc3.d/S20postfix'
removing `/etc/rc4.d/S20postfix'
removing `/etc/rc5.d/S20postfix'
================================================================================
=======================================
UBUNTU
In Ubuntu:
Pentru a rula o comanda ca root, folosesc in fata comenzii cuvantul: sudo
Exemplu:
sudo mc
Pentru a trece si a rula toate comenzile ca root, folosesc:
sudo su
prin urmare ma transform in root, apoi nu mai e nevoie sa folosesc sudo in fata
comenzilor.
--------------------------------------------------------------------------

http://pve.proxmox.com/wiki/OpenVZ_Console

OpenVZ Console
Contents
[hide]

    1 Introduction
    2 Debian
        2.1 Debian Lenny 5.0
        2.2 Debian Squeeze 6.0
        2.3 Debian Wheezy 7.0
    3 Ubuntu
        3.1 Ubuntu 12.04
        3.2 Ubuntu 10.04
    4 Centos
        4.1 Centos 5
        4.2 Centos 6
    5 Troubleshooting
        5.1 Java browser plugin
```

Introduction

Beginning with Proxmox VE 2.2, we introduced a new console view (with login capability). Especially for beginners it is not that easy to understand and manage containers but with the new console this is big step forward. OpenVZ and KVM console looks now quite similar.

But as most OpenVZ templates have disabled terminals, you need to enable it first. This article describes for the needed changes for already running OpenVZ container.

Note:

All Debian templates created with latest Debian Appliance Builder got this changes already, just download them vie GUI to your Proxmox VE storage (Debian 6 and 7 templates are up2date, 32 and 64 bit)
Debian

    this will work for all Debian releases:

log in to the Proxmox host.

edit all inittabs under /var/lib/vz/root/ :

```
 nano /var/lib/vz/root/*/etc/inittab

 # add this
 1:2345:respawn:/sbin/getty 38400 tty1
```

Debian Lenny 5.0

Login via SSH (or use the VNC "Shell") to your Proxmox VE host and 'vzctl enter CTID' the container:

List all running container:

```
proxmox-ve:~# vzlist
     CTID      NPROC STATUS    IP_ADDR         HOSTNAME
      108         23 running   192.168.9.20    ubuntu-1204.proxmox.com
      109         18 running   192.168.9.21    centos63-64.proxmox.com
      111         15 running   192.168.9.23    centos5-64.proxmox.com
      114         14 running   192.168.9.30    deb6-32.proxmox.com
      115         15 running   192.168.9.31    deb7-32.proxmox.com
      122         14 running   192.168.9.36    deb5.proxmox.com
```

Enter the container:

```
proxmox-ve:~# vzctl enter 122
```

```
root@debian:/# nano /etc/inittab

On the bottom of /etc/inittab just add the following line:

1:2345:respawn:/sbin/getty 38400 tty1

Save the changes and shutdown/start the container via Console.
Debian Squeeze 6.0

Same as Debian Lenny 5.0
Debian Wheezy 7.0

Same as Debian Lenny 5.0

Ubuntu
Ubuntu 12.04

Login via SSH (or use the VNC "Shell") to your Proxmox VE host and 'vzctl enter
CTID' the container:

List all running container:

proxmox-ve:~# vzlist
     CTID      NPROC STATUS    IP_ADDR         HOSTNAME
      108         23 running   192.168.9.20    ubuntu-1204.proxmox.com
      109         18 running   192.168.9.21    centos63-64.proxmox.com
      111         15 running   192.168.9.23    centos5-64.proxmox.com
      114         14 running   192.168.9.30    deb6-32.proxmox.com
      115         15 running   192.168.9.31    deb7-32.proxmox.com
      122         14 running   192.168.9.36    deb5.proxmox.com

Enter the container:

proxmox-ve:~# vzctl enter 108

root@ubuntu-1204:/# nano /etc/init/tty1.conf

Change/Create the file that it looks exactly like this:

--------------
# tty1 - getty
#
# This service maintains a getty on tty1 from the point the system is
# started until it is shut down again.

start on stopped rc RUNLEVEL=[2345]

stop on runlevel [!2345]

respawn
```

```
exec /sbin/getty -8 38400 tty1
--------------
```

Save the changes and shutdown/start the container via Console.

Ubuntu 10.04

Same as Ubuntu 12.04
Centos
Centos 5

Login via SSH (or use the VNC "Shell") to your Proxmox VE host and 'vzctl enter CTID' the container:

List all running container:

```
proxmox-ve:~# vzlist
     CTID      NPROC STATUS    IP_ADDR         HOSTNAME
      108         23 running   192.168.9.20    ubuntu-1204.proxmox.com
      109         18 running   192.168.9.21    centos63-64.proxmox.com
      111         15 running   192.168.9.23    centos5-64.proxmox.com
      114         14 running   192.168.9.30    deb6-32.proxmox.com
      115         15 running   192.168.9.31    deb7-32.proxmox.com
      122         14 running   192.168.9.36    deb5.proxmox.com
```

Enter the container:

```
proxmox-ve:~# vzctl enter 111
```

```
root@centos5-64:/# nano /etc/inittab
```

On the bottom of /etc/inittab just add the following line:

```
1:2345:respawn:/sbin/agetty tty1 38400 linux
```

Save the changes and shutdown/start the container via Console.
Centos 6

Login via SSH (or use the VNC "Shell") to your Proxmox VE host and 'vzctl enter CTID' the container:

List all running container:

```
proxmox-ve:~# vzlist
     CTID      NPROC STATUS    IP_ADDR         HOSTNAME
      108         23 running   192.168.9.20    ubuntu-1204.proxmox.com
      109         18 running   192.168.9.21    centos63-64.proxmox.com
      111         15 running   192.168.9.23    centos5-64.proxmox.com
      114         14 running   192.168.9.30    deb6-32.proxmox.com
      115         15 running   192.168.9.31    deb7-32.proxmox.com
```

```
      122         14 running   192.168.9.36    deb5.proxmox.com
```

Enter the container:

```
proxmox-ve:~# vzctl enter 109

root@centos63-64:/# nano /etc/init/tty.conf
```

Change/Create the file that it looks exactly like this:

```
# This service maintains a getty on tty1 from the point the system is
# started until it is shut down again.

start on stopped rc RUNLEVEL=[2345]

stop on runlevel [!2345]

respawn
exec /sbin/agetty -8 tty1 38400
```

Save the changes and shutdown/start the container via Console.
Troubleshooting

If you still want to use the previous method (vzctl enter CTID) you can open the host "Shell" and just type 'vzctl enter CTID" to manage your containers.
Java browser plugin

The console is using a Java applet, therefore you need latest Oracle (Sun) Java browser plugin installed and enabled in your browser (Google Chrome and Firefox preferred). If you are on Windows desktop, just go to java.com, if you run a Linux desktop you need to make sure that you run Oracle (Sun) Java plugin instead of the default openjdk. For Debian/Ubuntu based desktops, see Java_Console_(Ubuntu)

```
proxmox-ve:~# vzlist
      CTID      NPROC STATUS    IP_ADDR         HOSTNAME
       107         13 running   192.168.9.100   debian6.maurer-it.com
       108         29 running   192.168.9.101   debian.maurer-it.com
proxmox-ve:~# vzctl enter 108
Se iese cu logout
```

Configurarea timpului local:

```
dpkg-reconfigure tzdata
```

daca nu functioneaza:

```
aptitude install tzdata
```

El se instaleaza implicit cu ntp, prin urmare daca instalez ntp, voi avea si tzdata...

Change Time Zone

You may update or change your time zone by

tzconfig
dpkg-reconfigure tzdata (thanks to Mario, see comment below)

This command will guide you through the process of setting a new time zone. You may also choose UTC (GMT) if you want.

If your system does not have tzconfig, you may use something else.

tzselect

If your system does not have tzdata, install it as below:

sudo aptitude install tzdata

This will provide a set of different time zones to choose. If you would like to set the time to UTC, choose the option which says something like ‘none of the above’, or ‘none of these’ or something to this effect. In my case it was option 11. Then it asks for difference from UTC (GMT and GST is also the same thing). I chose GST-0 as the option and it set the time as UTC.

Fisierul de configurare pentru /etc/ntp.conf:

```
# /etc/ntp.conf, configuration for ntpd; see ntp.conf(5) for help

driftfile /var/lib/ntp/ntp.drift

# Enable this if you want statistics to be logged.
# statsdir /var/log/ntpstats/

statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

# Specify one or more NTP servers.

# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
```

```
# server 0.ubuntu.pool.ntp.org
# server 1.ubuntu.pool.ntp.org
# server 2.ubuntu.pool.ntp.org
# server 3.ubuntu.pool.ntp.org

server 0.ro.pool.ntp.org
server 1.ro.pool.ntp.org
server 2.ro.pool.ntp.org
server 3.ro.pool.ntp.org

# Use Ubuntu's ntp server as a fallback.
server ntp.ubuntu.com

# Access control configuration; see /usr/share/doc/ntp-doc/html/accopt.html for
# details.  The web page
<http://support.ntp.org/bin/view/Support/AccessRestrictions>
# might also be helpful.
#
# Note that "restrict" applies to both servers and clients, so a configuration
# that might be intended to block requests from certain clients could also end
# up blocking replies from your own upstream servers.

# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery

# Local users may interrogate the ntp server more closely.
restrict 127.0.0.1
restrict ::1

# Clients from this (example!) subnet have unlimited access, but only if
# cryptographically authenticated.
# restrict 192.168.123.0 mask 255.255.255.0 notrust

# If you want to provide time to your local subnet, change the next line.
# (Again, the address is an example only.)
# broadcast 192.168.123.255

# If you want to listen to time broadcasts on your local subnet, de-comment the
# next lines.  Please do this only if you trust everybody on the network!
# disable auth
# broadcastclient
```

Dupa configurare:

```
systemctl reload ntp.service
```

Setarea SSH-ului in Ubuntu: Fisierul /etc/ssh/sshd_config

```
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
# Port 22
Port 8267

# Use these options to restrict which interfaces/protocols sshd will bind to
# Specify multiple ip address on each new line with ListenAddress (multiple
ListenAddress options are permitted):
# ListenAddress 70.5.1.1
# ListenAddress 10.1.5.1
# ListenAddress ::
# ListenAddress 0.0.0.0

Protocol 2

# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key

# Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
SyslogFacility AUTH

# LogLevel INFO
LogLevel VERBOSE

# Introdusa de mine pentru a elimina intarzierea la logarea userului si parolei
UseDNS no

# Authentication:
# LoginGraceTime 120
LoginGraceTime 20

# PermitRootLogin yes
PermitRootLogin no
```

```
# AllowUsers jim@11.22.33.456
# AllowUsers jim@11.22.33.56 jim@141.212.133.36
# AllowUsers jim@11.22.33.*
# AllowUsers you@192.168.0.0/16
AllowUsers nume_user_1 nume_user_2 nume_user_n

StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes

# AuthorizedKeysFile    %h/.ssh/authorized_keys

# 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
RhostsRSAAuthentication no

# similar for protocol version 2
HostbasedAuthentication no

# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
# IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
# PasswordAuthentication yes

# Kerberos options
# KerberosAuthentication no
# KerberosGetAFSToken no
# KerberosOrLocalPasswd yes
# KerberosTicketCleanup yes

# GSSAPI options
# GSSAPIAuthentication no
# GSSAPICleanupCredentials yes

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
```

```
# UseLogin no

# MaxStartups 10:30:60
MaxStartups 2:50:5

MaxAuthTries 3

# Banner /etc/issue.net
Banner /etc/issue.net

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

Subsystem sftp /usr/lib/openssh/sftp-server

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes
```

La logarea prin SSH se prezinta mesajul existent in /etc/issue.net
Setarea fisierului: /etc/issue.net

Pentru restartare:
systemctl restart ssh

sau

systemctl restart sshd.service

sau

service ssh restart

systemctl status ssh
systemctl start ssh

In cazul in care nu pot primi drepturi sudo prin ssh de la un user oarecare:
sudo: must be setuid root

Verific drepturile si permisiunile pentru /usr/bin/sudo

ls -l /usr/bin/sudo

Daca nu apartin lui root:root, si nu are 4755, atunci:

chown root:root /usr/bin/sudo
chmod 4755 /usr/bin/sudo

Adaug userul la grupul sudo si verific cu visudo drepturile grupului sudo din /etc/sudoers
adduser username sudo

Verific permisiunile pe fisierul /etc/sudoers
Acestea trebuiesc sa fie 0440.

ls -l /etc/sudoers

Daca nu sunt, atunci:
chmod 0440 /etc/sudoers

Verific sintaxa fisierului sa fie ca mai jos, editandu-l cu comanda:
visudo

```
# ------------------------------------------------------------------
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults env_reset
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo ALL=(ALL:ALL) ALL
```

```
# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
# ------------------------------------------------------------
```

La final trebuie sa restartez serverul cu comanda:

```
reboot
```

Toata partea cu editarea cu visudo s-ar mai fi putut rezolva si cu:

```
echo 'Nume_User ALL=(ALL) ALL' >> /etc/sudoers
```

Sau altfel:

Editez ca user root:

```
visudo
```

Si aici adaug o linie noua continand userul care trebuie sa capete drepturi sudo:

```
user_nou ALL=(ALL:ALL) ALL
```

La final salvez si ies.

==========

Comenzi pentru dezactivarea / activarea interfetei de retea:

```
sudo ifdown eth0
sudo ifup eth0
```

sau:

```
/etc/init.d/networking stop
/etc/init.d/networking start
/etc/init.d/networking restart
```

==========

DPKG

dpkg este un manager de pachete pentru sustemele bazate pe Debian. Poate instala, dezinstala si construi pachete,
dar spre deosebire de alte managere de pachete, el nu poate downloada automat si instala pachete si crea dependinte.

Listarea tuturor pachetelor instalate in sistem:

```
dpkg -l
```

In functie de numarul pachetelor, asta poate genera o mare cantitate la iesire.

Pentru a vedea daca un anume pachet este instalat:

```
dpkg -l | grep apache2
```

Pentru a lista fisierele instalate de un pachet (de exemplu, ufw), introduceti:

```
dpkg -L ufw
```

Daca nu suntem siguri care pachet a instalat un fisier, dpkg -S poate spune asta. De exemplu:

```
dpkg -S /etc/host.conf
```

base-files: /etc/host.conf
Iesirea arata ca fisierul /etc/host.conf apartine pachetului base-files.
In orice caz, multe fisiere sunt automat generate in timpul instalarii pachetului, si chiar daca sunt in sistemul de
fisiere, dpkg -S nu poate sti la ce pachet apartine.

Se poate instala un fisier local .deb, introducand:
sudo dpkg -i zip_2.32-1_i386.deb
Schimb zip_2.32-1_i386.deb cu numele actual al fisierului local .deb.

Dezinstalarea unui pachet se realizeaza cu:
sudo dpkg -r zip

Dezinstalarea pachetelor utilizand dpkg nu este recomandata. Este mai bine sa utilizam un manager de pachete care
administreaza si dependintele, pentru a ne asigura ca siste,i; este mentinut intr-o stare consistenta.
De exemplu, dpkg -r poate dezinstala un pachet zip, dar orice pachet care depinde de el va ramane in continuare
instalat si nu va functiona in continuare corect

Instaleaza un pachet descarcat pe calculator dintr-o terta sursa si pentru care nu dorim sa folosim utilitarul gdebi sa
Ubuntu Software Center:
dpkg -i /cale/spre/fisier

Pentru manual:
man dpkg.
==========
Apt-Get
Comanda apt-get este un instrument puternic in linie de comanda care lucreaza cu Ubuntu's Advanced Packaging Tool (APT),
asigurand functii precum instalarea de pachete software noi, upgrade-ul pachetelor existente, update-ul listei indexului
sau chiar upgrade-ul intregului sistem de operare.

Are avantaje precum: usurinta de utilizare prin terminal / SSH, precum si abilitatea de a fi utilizat in scripturile
de administrare, ce pot fi pornite automat de utilitarela cron.

Urmatoarele optiuni ale apt-get pot fi utile:

-h Afiseaza textul de help.
-d Doar Download - Nu instaleaza si nu despacheteaza pachetele.
-f Incearca continuarea in cazul in care verificarea integritatii esueaza.
-s No-act. Executa doar simularea actiunii de instalare si despachetare.
-y Atribuie Yes la toate interogarile de confirmare, fara a mai afisa aceste interogari.
-u Afiseaza in plus si o lista a pachetelor upgrade-ate.

Se pot specifica pachete multiple ce pot fi instalate sau inlaturate, acestea fiind separate prin spatii.
Instalarea unui pachet:
sudo apt-get install nmap
apt-get install PROGRAM1 PROGRAM2 PROGRAM3 ...

Dezinstalarea unui pachet (fisierele de configurare raman intacte in sistem):
sudo apt-get remove nmap

Instaleaza nautilus si dezinstaleaza gnome-panel:
apt-get install nautilus gnome-panel-

Inlatura gnome-panel si instaleaza nautilus:
apt-get --purge remove gnome-panel nautilus+

Pentru o completa inlaturare a unui pachet, rulam:
apt-get --purge remove gnome-panel

Dezinstalarea programelor instalate chiar cu stergerea fisierelor de configurare (în general fisierele din Home
nu sunt sterse de aceasta comanda). Daca doriti ca si fisierul de configurare sa fie sters lansati comanda:
apt-get --purge remove gaim
sau:
apt-get purge NUMEPROGRAM

Daca in vreun fel am deteriorat un pachet instalat, sau pur si simplu dorim sa reinstalam fisierele unui pachet, la cea
mai noua versiune disponibila, putem utiliza optiunea --reinstall, astfel:
apt-get --reinstall install gdm

Adaugand optiunea --purge options la apt-get remove se vor inlatura deasemenea si fisierele de configurare. Aceasta
facilitate poate fi sau nu poate fi ceea ce ne dorim, asa ca trebuie utilizata cu grija.

Indexul pachetelor APT este o baza de date a pachetelor existente din cadrul repositoriu-ului, fiind sefinita in:
fisierul /etc/apt/sources.list.

Pentru update-ul indexului local al pachetelor, cu cele mai noi modificari facute in repozitorii:
sudo apt-get update

De-a lungul timpului, versiunile update-ate ale pachetelor curente instalate in computer, pot sa devina disponibile
din repozitoriile de pachete (de exempllu update-uri de securitate). Pentru upgrade-ul sistemului, mai intai update-am
fisierul cu indexul pachetelor si apoi:

sudo apt-get upgrade

E bine sa rulam comanda insotita de optiunea -u. Aceasta ne arata si lista pachetelor utilizate. Fara ea, upgrade-ul
se va face orbeste.
apt-get -u upgrade

Actiunile comenzii apt-get, pecum instalarile si dezinstalarile pachetelor sunt inregistrate in fisierul:
/var/log/dpkg.log.

Mai multe informatii despre apt-get gasim in Debian APT User Manual1 sau prin:
apt-get help

Repara pachetele deteriorate si care risca sa nu functioneze sau sa impiedice functionarea altora:
apt-get -f install

Adaugarea de repositories/surse de pachete noi
add-apt-repository NUME_REPOSITORY

Stergerea programelor care au fost instalate de alte programe si care nu mai sunt necesare
apt-get autoremove

Curatarea arhivei cache (locul unde se descarca programele înainte de a fi instalate cu comanda apt-get install
sau apt-get upgrade):
apt-get clean
apt-get autoclean

Diferenta între cele doua comenzi este ca apt-get clean sterge toate fisierele din cache, pe când apt-get autoclean sterge
doar acele programe care nu mai sunt instalate în sistem. (apt-get clean removes everything except lock files from
/var/cache/apt/archives/ and /var/cache/apt/archives/partial/. Thus, if you need to reinstall a package APT should
retrieve it again. apt-get autoclean removes only package files that can no longer be downloaded.)

Sterge pachetul, dependentele orfane si fisierele de configurare:
apt-get autoremove --purge {pachet}

Actualizeaza depozitele si instaleaza versiunile noi ale pachetelor invechite pe sistem. Este o comanda foarte utila
pentru ca face ambele lucruri deodata fara a mai fi nevoie de o noua interventie pentru a introduce o noua cumanda:
apt-get update && sudo apt-get dist-upgrade -y

Apt-cache program din pachetul apt (interfata pentru apt), ce poate fi folosit

pentru a obtine informatii despre pachete (
instalate sau nu). Este mai rapid la cautari decât aptitude dar nu stie sa caute
decât în numele pachetelor sau descrieri.
apt-cache

Toate pachetele care contin total si commander în nume sau în descriere:
apt-cache search total commander

Toate pachetele care contin pidgin în denumire:
apt-cache search -n pidgin

Afi?eaza prioritatile surselor de pachete:
apt-cache policy

Afiseaza versiunile pachetului din toate sursele respectiv prioritatea si „versiunea
candidata”, adica cea care va
fi instalata implicit cu apt-get/aptitude/synaptic:
$ apt-cache policy pidgin

Cautarea de pachete / programe care contin un anumit termen
apt-cache search TERMEN_CAUTARE

Aflarea datelor despre un anumit pachet / program: descriere, marime, versiune,
dependinte, conflicte, etc.
apt-cache show NUMEPROGRAM

man apt-get
man apt-cache
==========
==========

Fisierul /etc/apt/sources.list in Ubuntu:

---

deb http://archive.ubuntu.com/ubuntu precise main restricted universe
deb http://archive.ubuntu.com/ubuntu precise-updates main restricted universe
deb http://security.ubuntu.com/ubuntu precise-security main restricted universe
multiverse
deb http://archive.canonical.com/ubuntu precise partner

#

deb cdrom:[Ubuntu-Server 12.04 LTS _Precise Pangolin_ - Release amd64
(20120424.1)]/ dists/precise/main/binary-i386/
deb cdrom:[Ubuntu-Server 12.04 LTS _Precise Pangolin_ - Release amd64
(20120424.1)]/ dists/precise/restricted/binary-i386/
deb cdrom:[Ubuntu-Server 12.04 LTS _Precise Pangolin_ - Release amd64
(20120424.1)]/ precise main restricted

```
#deb cdrom:[Ubuntu-Server 12.04 LTS _Precise Pangolin_ - Release amd64
(20120424.1)]/ dists/precise/main/binary-i386/
#deb cdrom:[Ubuntu-Server 12.04 LTS _Precise Pangolin_ - Release amd64
(20120424.1)]/ dists/precise/restricted/binary-i386/
#deb cdrom:[Ubuntu-Server 12.04 LTS _Precise Pangolin_ - Release amd64
(20120424.1)]/ precise main restricted

# See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to
# newer versions of the distribution.
# deb http://de.archive.ubuntu.com/ubuntu/ precise main restricted
# deb-src http://de.archive.ubuntu.com/ubuntu/ precise main restricted

## Major bug fix updates produced after the final release of the
## distribution.
# deb http://de.archive.ubuntu.com/ubuntu/ precise-updates main restricted
# deb-src http://de.archive.ubuntu.com/ubuntu/ precise-updates main restricted

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team. Also, please note that software in universe WILL NOT receive any
## review or updates from the Ubuntu security team.
# deb http://de.archive.ubuntu.com/ubuntu/ precise universe
# deb-src http://de.archive.ubuntu.com/ubuntu/ precise universe
# deb http://de.archive.ubuntu.com/ubuntu/ precise-updates universe
# deb-src http://de.archive.ubuntu.com/ubuntu/ precise-updates universe

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team, and may not be under a free licence. Please satisfy yourself as to
## your rights to use the software. Also, please note that software in
## multiverse WILL NOT receive any review or updates from the Ubuntu
## security team.
# deb http://de.archive.ubuntu.com/ubuntu/ precise multiverse
# deb-src http://de.archive.ubuntu.com/ubuntu/ precise multiverse
# deb http://de.archive.ubuntu.com/ubuntu/ precise-updates multiverse
# deb-src http://de.archive.ubuntu.com/ubuntu/ precise-updates multiverse

## N.B. software from this repository may not have been tested as
## extensively as that contained in the main release, although it includes
## newer versions of some applications which may provide useful features.
## Also, please note that software in backports WILL NOT receive any review
## or updates from the Ubuntu security team.
# deb http://de.archive.ubuntu.com/ubuntu/ precise-backports main restricted
universe multiverse
# deb-src http://de.archive.ubuntu.com/ubuntu/ precise-backports main restricted
universe multiverse

# deb http://security.ubuntu.com/ubuntu precise-security main restricted
# deb-src http://security.ubuntu.com/ubuntu precise-security main restricted
# deb http://security.ubuntu.com/ubuntu precise-security universe
# deb-src http://security.ubuntu.com/ubuntu precise-security universe
# deb http://security.ubuntu.com/ubuntu precise-security multiverse
```

```
# deb-src http://security.ubuntu.com/ubuntu precise-security multiverse

## Uncomment the following two lines to add software from Canonical's
## 'partner' repository.
## This software is not part of Ubuntu, but is offered by Canonical and the
## respective vendors as a service to Ubuntu users.
# deb http://archive.canonical.com/ubuntu precise partner
# deb-src http://archive.canonical.com/ubuntu precise partner

## Uncomment the following two lines to add software from Ubuntu's
## 'extras' repository.
## This software is not part of Ubuntu, but is offered by third-party
## developers who want to ship their latest software.
# deb http://extras.ubuntu.com/ubuntu precise main
# deb-src http://extras.ubuntu.com/ubuntu precise main
```

==========

Aptitude

Aptitude este un instrument bazat pe text, utilizand meniuri de utilizare, pentru sistemul Advanced Packaging Tool (APT).

Puteti porni Aptitude ca si user normal:

```
sudo aptitude
```

Panelul de sus contine categoriile de pachete, precum New Packages si Not Installed Packages. Panelul de jos contine
informatii referitoare la pachete si categoriile de pachete.

Instalarea pachetelor:

Localizam pachetul in cadrul categoriei Not Installed Packages, prin utilizarea sagetilor si a tastei ENTER, si selectam
pachetul de instalat. Dupa selectare, apasam tasta + si pachetul va deveni verde indicand selectarea pentru instalare.
Apasam g si va prezenta un sumar al actiunilor pachetului. Apasam g inca odatesi se va cere sa devenim root.
Apoi ENTER si o parola. In final, g inca odata pentru download. Enter si va incepe descarcarea si instalarea pachetului.

Inlaturarea pachetelor:

Localizam pachetul in cadrul categoriei Pachetelor Instalate To remove a package, utilizand sagetile si ENTER pentru
selectarea pachetelor ce se doresc inlaturate. Dupa selectare, apasam tasta - si pachetul va deveni roz, indicand
selectarea. Apasam g. Apasam din nou g, ni se va cere sa devenim root. Apasam ENTER, apoi parola. In final, g inca odata.
Apsam ENTER, si inlaturarea pachetului va incepe.

Update-ul indexului pachetelor:

Apasati tasta u si vom fi anuntati sa devenim root pentru a realiza update-ul.

Apasam ENTER, apoi se cere Password.
Introducem parola pantru a deveni root. Update-ul va incepe. Apoi ENTER la afisarea OK, cand dialogul de download
este prezentat pentru finalizarea procesului.

Upgrade-ul pachetelor:
Mai intai face update, ca mai sus, apoi apasam U pentru markarea tuturor pachetelor cu update-uri.
Apoi apasam g, unde vom primi un sumar al pachetelor de upgrade. Apasam g din nou si se va cere sa devenim root pentru
a desavarsi instalarea. Apasam ENTER, apoi se cere parola. In final apasam g inca odata si vom fin anuntati pentru
downloadul de pachete. Apasam ENTER si upgrade-ul va incepe. Prima coloana va afisa lista pachetelor in panelul de sus.
Aici starea curenta a pachetelor afisate este semnalata conform listei de mai jos:
i: Pachete instalate
c: Pachetele neinstalate, dar configuratia pachetelor ramana pe sistem
p: Inlaturate din sistem
v: Pachete virtuale
B: Pachete deteriorate (broken)
u: Fisiere nedespachetate, dar pachete neconfigurate inca
C: Partial configurate - Configurarea a esuat si necesita reparare
H: Partial instalate - Inlaturarea a esuat si necesita reparare

Pentru parasirea Aptitude, apasati q si apoi confirmati iesirea.

Multe alte functii sunt disponibile din meniul Aptitude, apasand F10.
==========
SHOREWALL

Am instalat Shorewall-4.4.26.1

Instalarea se face cu:
```
sudo apt-get update
sudo apt-get install shorewall
```

Pentru a porni firewall-ul la pornirea serverului, editez in /etc/default/shorewall
startup=1

/etc/shorewall/   <--- Stocheaza configurarile programului
/usr/share/shorewall   <--- Stocheaza fisierele suportate si fisierele de actiune

E nevoie sa copiem toate fisierele de configurare astfel:
```
sudo cp /usr/share/doc/shorewall/default-config/* /etc/shorewall/
```

Acum vom face configurari in: /etc/shorewall

Configurarea zonelor:
Mai intai editam fisierul de zone pentru a specifica diferitele zone de retea.

Acestea sunt doar etichete ce vor fi
utilizate in cadrul altor fisiere. Consideram Internetul ca si o zona, si o retea privata ca si alta zona.
Daca avem acestea, atunci fisierul de zona ar putea sa arate astfel:

$ nano /etc/shorewall/zones

Adaugam urmatoarele 2 linii in fisierul de zone:
net ipv4
loc ipv4

Salvam si iesim.

Configurarea interfetelor:

Urmatorul fisier de editat este cel al interfetelor. Aici se specifica interfetele ce sunt utilizate pe masina in cauza.
Aici se va conecta zona definita in pasul anterior cu interfata actuala. Al 3-lea camp este adresa de broadcast a
retelei atasate respectivei interfete (“detect” va figura aceasta iesire pentru noi). Ultimul camp sunt iotiunile
pentru interfata. Optiunile listate mai jos sunt un bun punct de pornire:

$ nano /etc/shorewall/interfaces

Adaugam urmatoarele 2 linii in fisierul de interfete:
net eth0 detect routefilter,norfc1918,logmartians,nosmurfs,tcpflags,blacklist
loc eth1 detect tcpflags

Salvam si iesim.

Configurarea politicilor:

Urmatorul fisier defineste politicile implicite ale firewall-ului. Politica implicita este aplicata daca alte reguli
nu sunt aplicate. Adesea vom seta politicile implicite ca si REJECT sau DROP si atunci configuram specific care
port / servicii sunt permise in urmatorul pas. Un exemplu de politica (bazat pe zonele si interfetele create anterior)
ar putea fi:

$nano /etc/shorewall/policy

Adaugam urmatoarele linii in fisierul de politici:
fw net ACCEPT
fw loc ACCEPT
net all DROP info
The FOLLOWING POLICY MUST BE LAST
all all REJECT info

Salvam si iesim.

Aceasta politica spune: implicit, se accepta orice trafic initiat dinspre masina (fw) catre internet si catre reteaua
locala. Orice vine dinspre internet atat catre masina sau reteaua locala va fi stopat si inregistrat in log cu syslog
level “info”. Ultima linie opreste inchide orice altceva off. Nota: Regula DROP opreste totul in liniste, iar REJECTs
trimite ceva inapoi, lasand expeditorul sa stie ca a fost rejectat.

Configurarea regulilor:

Aici se definesc exceptii la politicile implicite setate anterior.

Cel mai important fisier este fisierul cu reguli. Aici este unde setam ceea ce este permis sau nu. Orice noua conexiune
care vine inspre firewall, trece prin aceste reguli si daca nici una dintre ele nu se aplica, atunci politicile implicite
se vor aplica. Nota: Aceasta este doar pentru conexiunile noi, cele existente sunt automat acceptate. Comentariile in
fisier va dau o buna idee despre cum functioneaza lucrurile, dar urmatoarele vor asigura un exemplu care sa va dea un
bun start:

$nano /etc/shorewall/rules

Adaugam urmatoarele linii in fisierul de reguli, dupa SECTION NEW:

#ACTION SOURCE DEST PROTO DEST SOURCE ORIGINAL RATE USER/
PORT PORT(S) DEST LIMIT GROUP
ACCEPT net fw icmp 8
ACCEPT fw net icmp
ACCEPT net fw tcp ssh,www,https,smtp,pop3,pop3s,imap2,imaps,submission
ACCEPT net fw udp https
ACCEPT net:10.1.1.1 fw tcp ssh

Salvam si iesim.

Exemplul de mai sus spune: “Se accepta orice ping (icmp) din internet catre masina, precum si orice conexiune tcp
dinspre internet, care sunt pe oricare porturi referite in fisierul /etc/services pentru serviciile ssh(22), www(80),
https(443), etc. De asemenea se accepta din internet conexiuni udp connections la https(443). Cat timp sunt la el,
accepta doar conexiuni tcp de la IP 10.1.1.1 venind de la internet catre portul ssh (22).

Pasul final este sa pornim shorewall:

$sudo /etc/init.d/shorewall start

password :

Daca a existat vreo eroare de sintaxa in fisierul de configurari, atunci vom primi o erare ce spune sa citim
/var/log/shorewall-init.log

Daca toate au pornit cum trebuie, trebuie sa fim siguri ca nu am blocat ceva ce nu dorim, de accea ne uitam de
asemenea la fisierul de loguri.

Aici este rezultatul in cazul in care cineva incearca sa atace serverul:

$tail -f /var/log/messages

Oct 9 15:52:06 athena kernel: [1274443.734684] Shorewall:net2all:DROP:IN=eth0 OUT=
MAC=00:0c:29:61:de:33:00:d0:00:6b:54:00:08:00 src=218.232.95.60 DST=216.176.188.107
LEN=404 TOS=0x00 PREC=0x00
TTL=115 ID=43443 PROTO=UDP SPT=3664 DPT=1434 LEN=384
Oct 9 16:00:33 athena kernel: [1274950.625316] Shorewall:net2all:DROP:IN=eth0 OUT=
MAC=00:0c:29:61:de:33:00:d0:00:6b:54:00:08:00 src=121.18.13.107 DST=216.176.188.107
LEN=40 TOS=0x00 PREC=0x00
TTL=113 ID=256 DF PROTO=TCP SPT=12200 DPT=7212 WINDOW=8192 RES=0x00 SYN URGP=0

Hi, thank you for your effort and help.

I’m new to Linux and would like to understand something.
I have followed exactly every step mentioned above. Then, when I launched shorewall I received an error about “norfc1918?
in Interfaces file, line 11. I then completely changed the tow lines in Interfaces file with these :

#ZONE INTERFACE BROADCAST OPTIONS
net eth0 detect dhcp,norfc1918,blacklist

and it works fine now.

I found this help in this link:
http://www.opendocs.net/shorewall/2.0/Documentation.htm#Interfaces

Can someone, please, explain what was the error cause and how it had been solved?
Thank you.
---
ping: icmp open socket: Operation not permitted on ubuntu

Since an update the ping command stopped working on my ubuntu system. I always get to error “ping: icmp open socket:
Operation not permitted”. Because I don’t wan’t to always use sudo with ping, I did following change on my system:

```
$ ls -al /bin/ping
-rwxr-xr-x 1 root root 27140 2006-12-19 21:35 /bin/ping

is WRONG. ping must have the SUID-flag!

$ sudo chmod u+s /bin/ping

$ ls -al /bin/ping
-rwsr-xr-x 1 root root 27140 2006-12-19 21:35 /bin/ping

Now it works again
------
Alte comenzi:
man shorewall-zones
shorewall stop
shorewall start
shorewall restart
shorewall clear  <--- Inlatura total orice urma a Shorewall din cadrul configurariei
Netfilter
sudo shorewall status
shorewall try
sudo /etc/init.d/shorewall restart
shorewall show zones
shorewall check
which ip
ip route ls
shorewall show log              <--- Afiseaza ultimele 20 de mesaje de log ale
Netfilter
shorewall logwatch
shorewall dump          <--- Afiseaza un raport detaliat
================================================================================
=======================================
IPTABLES

Ubuntu vine cu el instalat si initial permite intregul trafic.

Pentru a vedea daca iptables ruleaza si ce module sunt incarcate, tastam:
lsmod | grep ip_tables

Pentru a vedea regulile setate in acel moment, tastam:
sudo iptables -L
sau mai detaliat:
sudo iptables -L -v
si cu afisarea numarului liniei:
iptables -L INPUT -n --line-numbers

Daca iptables nu ruleaza, putem sa-l activam (in Fedora) ruland:
system-config-securitylevel

Mai intai, setez Nodul Hardware.
```

Daca dorim sa utilizam firewall (iptables) in interiorul containerelor, atunci trebuie sa incarcam in Nodul Hardware
urmatoarele module, inainte de a porni containerele:
modprobe xt_tcpudp   <--- Aceasta s-ar putea sa nu fie gasit ca modul
modprobe ip_conntrack

In cazul in care vrem sa utilizam comenzi care sa aplice reguli firewall (chiar trebuie sa facem asta), atunci trebuie sa
ne asiguram ca 'ipt_state' este inclus in interiorul optiunii 'IPTABLES' din fisierul /etc/vz/vz.conf:
nano /etc/vz/vz.conf

IPTABLES="ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl
ipt_length ipt_state"

In plus, trebuie sa ne asiguram ca modulul 'xt_state' este incarcat in Nodul Hardware:
modprobe xt_state

Setari in container dar si in Hardware Node:

Putem permite stabilirea sesiunilor de receptionare a traficului:
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

Regula de mai sus nu are spatii intre virgula si cuvintele ESTABLISHED,RELATED

Daca linia de mai sus nu ruleaza, putem sa ne aflam in situatia in care nu este permisa o anume extensie, in care caz,
o versiune anterioara poate fi utilizata, dupa cum urmeaza:
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Pentru a permite trafic de intrare pe portul implicit SSH (22):
sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT
sau
sudo iptables -A INPUT -p tcp --dport 2202 -j ACCEPT

Pentru a permite trafic web de intrare:
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Asemenea:
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

Pentru DNS:
iptables -I INPUT -p udp -m udp --dport 53 -j ACCEPT
iptables -I INPUT -p tcp -m tcp --dport 53 -j ACCEPT

Problema este ca inclusiv portul de loopback este blocat. Deoarece este o gramada de trafic vom include aceasta regula la
inceput, pentru a fi procesata la inceput.

```
sudo iptables -I INPUT 1 -i lo -j ACCEPT

Pot include o regula pentru a accepta pingurile de intrare:
sudo iptables -I INPUT 3 -p icmp -j ACCEPT

Pentru FTP:
iptables -A INPUT -p tcp --dport 21 -j ACCEPT
iptables -A INPUT -p tcp --dport 20 -j ACCEPT

Pentru FTPS:
iptables -A INPUT -p tcp --dport 40110:40210 -j ACCEPT     <---- Unde porturile le
stabilesc in ce gama sa fie

sau:

iptables -A INPUT -p tcp -m multiport --dports 20,21,989,990 -j ACCEPT

Daca ma conectez cu TLS explicit, conectarea se face prin portul 21, prin urmare nu
mai e nevoie de activarea
porturilor 989 si 990.

Reguli IPTABLES pentru a permite e-mailing:

iptables -A INPUT -i eth0 -p tcp -s 192.168.100.0/24 --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
sau:
iptables -A INPUT -p tcp -s 127.0.0.1 --dport 10023 -j ACCEPT
Postgrey foloseste portul 10023, insa nu e nevoie sa introduc o astfel de regula.

Am nevoie, in schimb de urmatoarele:

iptables -A INPUT -p tcp --dport 25 -j ACCEPT                          <-- SMTP
iptables -A INPUT -p tcp --dport 465 -j ACCEPT                         <-- SMTPS
iptables -A INPUT -p tcp --dport 143 -j ACCEPT                         <-- IMAP
iptables -A INPUT -p tcp --dport 993 -j ACCEPT                         <-- IMAPS
iptables -A INPUT -p tcp --dport 110 -j ACCEPT                         <-- POP3
iptables -A INPUT -p tcp --dport 995 -j ACCEPT                         <-- POP3S

sau:

iptables -A OUTPUT -o eth0 -p tcp --sport 25 -m state --state ESTABLISHED -j ACCEPT

sau

iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -m multiport --sports 22,80,443 -m state --state
ESTABLISHED -j ACCEPT

sau:
```

```
iptables -A INPUT -p tcp -m multiport --dports 25,143,993,110,995 -j ACCEPT
     <--- Asta am aplicat-o
iptables -A OUTPUT -o eth0 -p tcp -m multiport --sports 22,80,443 -m state --state
ESTABLISHED -j ACCEPT
```

21. Allow IMAP and IMAPS
The following rules allow IMAP/IMAP2 traffic.

```
iptables -A INPUT -i eth0 -p tcp --dport 143 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 143 -m state --state ESTABLISHED -j ACCEPT
```

The following rules allow IMAPS traffic.

```
iptables -A INPUT -i eth0 -p tcp --dport 993 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 993 -m state --state ESTABLISHED -j ACCEPT
```

22. Allow POP3 and POP3S
The following rules allow POP3 access.

```
iptables -A INPUT -i eth0 -p tcp --dport 110 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 110 -m state --state ESTABLISHED -j ACCEPT
```

The following rules allow POP3S access.

```
iptables -A INPUT -i eth0 -p tcp --dport 995 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 995 -m state --state ESTABLISHED -j ACCEPT
```

Prin urmare regula iptables folosita este:

```
iptables -A INPUT -p tcp -m multiport --dports 20,21 -j ACCEPT
```

In exemplul de pana aici nu va fi inregistrat ca log nici un trafic. Daca dorim sa inregistram logul traficului in
logurile de sistem, aceasta poate fi cea mai usoara modalitate:

Log Dropped Packets

By default, Iptables log message to a /var/log/messages file. However you can change this location. I will show
you how to create a new logfile called /var/log/iptables.log. Procedure to log the iptables messages to a
different log file:

Open your /etc/syslog.conf file:

```
# vi /etc/syslog.conf
```

Append following line:

```
kern.warning /var/log/iptables.log
```

Save and close the file.

Restart the syslogd (Debian / Ubuntu Linux):

```
/etc/init.d/sysklogd restart
```

Now make sure you pass the log-level 4 option with log-prefix to iptables. For example:
DROP everything and Log it
iptables -A INPUT -j LOG --log-level 4
sau:
iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "IPTables Packet Dropped: " --log-level 7
sau:
iptables -A INPUT -j LOG --log-prefix "IPTables Packet Dropped / Hackers: " --log-level 4   <---- Asta am aplicat

For example, drop and log all connections from IP address 64.55.11.2 to your /var/log/iptables.log file:
iptables -A INPUT -s 64.55.11.2 -m limit --limit 5/m --limit-burst 7 -j LOG --log-prefix '** HACKERS **'--log-level 4
iptables -A INPUT -s 64.55.11.2 -j DROP

Where,
    --log-level 4: Level of logging. The level # 4 is for warning.
    --log-prefix '*** TEXT ***': Prefix log messages with the specified prefix (TEXT); up to 29 letters l
        ong, and useful for distinguishing messages in the logs.

You can now see all iptables message logged to /var/log/iptables.log file:
tail -f /var/log/iptables.log

Odata ce o decizie de a accepta un pachet este luata, nici o alta regula nu o va mai afecta. Deoarece regulile noastre
permit mai intai trafic ssh si web, atata timp cat regulile noastre de a bloca intregul trafic vor veni dupa acestea,
vom putea inca accepa traficul dorit. Tot ce trebuie sa facem este sa punem la sfarsit regula de a bloca intregul trafic.
sudo iptables -A INPUT -j DROP

Daca am restarta serverul acum, toate regulile iptables setate se vor pierde. Prin urmare ar trebui sa le salvam si sa
le incarcam automat la fiecare restartare. Pentru a salva configuratia, putem utiliza: iptables-save si iptables-restore.

Salvam regulile firewall intr-un fisier care se va crea la momentul salvarii:
sudo sh -c "iptables-save > /etc/iptables.rules"

Acum avem cateva optiuni. Putem schimba /etc/network/interfaces sau altfel putem adauga scripturi la
/etc/network/if-pre-up.d/ si /etc/network/if-post-down.d/ pentru a obtine acelasi rezultat. Solutia scripturilor
permite ceva mai multa flexibilitate.

OPTIUNEA 1: Modificarea: /etc/network/interfaces

Aflam exact numele interfetei pe care o utilizam. De exemplu verific daca exista interfete wireless:
iwconfig

Vom primi un raspuns de genul:
lo   no wireless extensions.
eth0   no wireless extensions.

Editam /etc/network/interfaces:
sudo nano /etc/network/interfaces

Introducem la sfarsitul interfetei (de regula eth0) urmatoarea linie:
pre-up iptables-restore < /etc/iptables.rules

Putem deasemenea pregati un set de reguli down, sa le salvam intr-un alt fisier /etc/iptables.downrules si sa le aplicam
automat:
post-down iptables-restore < /etc/iptables.downrules

Exemplul complet:
```
auto eth0
iface eth0 inet dhcp
  pre-up iptables-restore < /etc/iptables.rules
  post-down iptables-restore < /etc/iptables.downrules
```

Daca vrem sa pastram informatiile despre si packet counters.
sudo sh -c "iptables-save -c > /etc/iptables.rules"

OPTIUNEA 2: Modificarea: /etc/network/if-pre-up.d and ../if-post-down.d   # Asta am aplicat-o !!!

NOTE: Solutia utilizeaza iptables-save -c pentru a salva counterii. Daca inlaturam -c salvam doar regula.

Adaugam iptables-restore si iptables-save la folderele if-pre-up.d si if-post-down.d in folderul /etc/network:
Scriptul /etc/network/if-pre-up.d/iptablesload va contine:

Editam cu:
nano /etc/network/if-pre-up.d/iptablesload

```
#!/bin/sh
iptables-restore < /etc/iptables.rules
exit 0
```

si /etc/network/if-post-down.d/iptablessave:
nano /etc/network/if-post-down.d/iptablessave

va contine:

```
#!/bin/sh
iptables-save -c > /etc/iptables.rules
if [ -f /etc/iptables.downrules ]; then
   iptables-restore < /etc/iptables.downrules
fi
exit 0
```

Acordam ambelor scripturi drepturi de executie:

```
sudo chmod +x /etc/network/if-post-down.d/iptablessave
sudo chmod +x /etc/network/if-pre-up.d/iptablesload
```

OPTIUNEA #3: Utilizarea pachetului iptables-persistent

Se instaleaza si se utilizeaza pachetul iptables-persistent.

OPRIREA FIREWALL-ului:

Daca vrem sa oprim temporar firewall-ul:
```
sudo iptables -F
```

sau altfel, putem crea un script:
```
sudo nano -w /root/fw.stop
```

```
echo "Stopping firewall and allowing everyone..."
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
```

Il facem executabil:
```
sudo chmod +x /root/fw.stop
```

Il putem rula cu:
```
sudo /root/fw.stop
```

Prin urmare acuma este oprit (adica toate regulile sunt ACCEPT)

Pentru a reporni, trebuie sa rulam:
iptables-restore < /etc/iptables.rules

Daca folosesc syslog.conf, prin urmare syslogd, restartez cu:

/etc/init.d/sysklogd restart
sau service sysklogd restart

LOGGING utilizand rsyslog
(A mers pentru sistemul gazda PROXMOX, dar nu si pentru container).

service rsyslog status
service rsyslog restart
sau
/etc/init.d/rsyslog restart

Instalare rsyslog:
apt-get update
apt-get upgrade
sudo apt-get install -y rsyslog

Creez un nou fisier (sau mai multe):
sudo touch /etc/rsyslog.d/10-iptables.conf
        // aici am "INVALID_Drop: "
sudo touch /etc/rsyslog.d/15-iptables.conf
        // aici am "INPUT_2/min: "
sudo touch /etc/rsyslog.d/20-iptables.conf
        // aici am "INPUT_Dropped: "
sudo touch /etc/rsyslog.d/30-iptables.conf
        // aici am "OUTPUT_Allow_10/hour: "

In care editez ceva de genul:

:msg, contains, "iptables: " -/var/log/iptables.log
& ~

unde in fiecare din cele 4 fisiere in loc de "iptables: ", pot avea: mesaje
diferite, de genul:
'INVALID_Drop: ', 'INPUT_2/min: ', 'INPUT_Dropped: ' sau 'OUTPUT_Allow_10/hour: '.

Creez regulile iptables, de genul:

iptables -F
iptables -A INPUT -m state --state INVALID -j LOG --log-level 4 --log-prefix
'INVALID_Drop: '
iptables -A INPUT -m state --state INVALID -j DROP

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m limit --limit 2/min -j LOG --log-level 4 --log-prefix
'INPUT_2/min: '
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp --sport 80 -j ACCEPT
iptables -A INPUT -p udp --sport 53 -j ACCEPT
iptables -A INPUT -j LOG --log-level 4 --log-prefix 'INPUT_Dropped: '
iptables -A INPUT -j DROP
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A OUTPUT -m limit --limit 10/hour -j LOG --log-level 4 --log-prefix
'OUTPUT_Allow_10/hour: '
iptables -A OUTPUT -j ACCEPT
iptables-save -c > /etc/iptables.rules
```

Restartez rsyslog:
```
sudo service rsyslog restart
```

Creez ceva trafic (de genul ping-uri, conectare ssh, etc), dupa care verific fisierul cu loguri:
```
tail -f /var/log/iptables.log
```

Creem un nou fisier: /etc/logrotate.d/iptables:
```
sudo touch /etc/logrotate.d/iptables
```
in care introduc ceva de genul:

```
/var/log/iptables.log                          <------ Asta am aplicat !!!
{
        rotate 30
        daily
        missingok
        notifempty
        delaycompress
        compress
        postrotate
                invoke-rc.d rsyslog reload > /dev/null
        endscript
}
```

sau alta varianta asemanatoare:

```
/var/log/iptables.log
{
 rotate 4
 weekly
 missingok
 notifempty
 compress
 delaycompress
 sharedscripts
 postrotate
```

```
  reload rsyslog >/dev/null 2>&1 || true
 endscript
}
```

Restartez rsyslog:

```
sudo service rsyslog restart
```

In cazul containerului, aceasta metoda ocupa 100% din resursele procesorului.
For those running OpenVZ/Proxmox containers, one simple workaround is to disable the imklog module using this :

```
  sed -i -e 's/^\$ModLoad imklog/#\$ModLoad imklog/g' /etc/rsyslog.conf
```

This fixes the 100% CPU usage of rsyslog in Natty, Oneiric and Precise containers.

Reguli aplicate in configurari de catre mine:

```
sudo iptables -A INPUT -m state --state INVALID -j LOG --log-level 4 --log-prefix
'INVALID_Drop: '
sudo iptables -A INPUT -m state --state INVALID -j DROP
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A INPUT -m limit --limit 2/min -j LOG --log-level 4 --log-prefix
'INPUT_2/min: '
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -p udp -m udp --dport 53 -j ACCEPT
sudo iptables -A INPUT -p tcp -m tcp --dport 53 -j ACCEPT
sudo iptables -A INPUT -p tcp -m multiport --dports 80,443,38869 -j ACCEPT
sudo iptables -A INPUT -p icmp -j ACCEPT
sudo iptables -A INPUT -p tcp -m multiport --dports 25,465,143,993,110,995 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 24969 -j ACCEPT
sudo iptables -A INPUT -p tcp -m multiport --dports 20,21 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 40210:40215 -j ACCEPT
sudo iptables -A INPUT -j LOG --log-level 4 --log-prefix 'INPUT_Dropped: '
sudo iptables -A INPUT -j DROP
sudo iptables -A OUTPUT -o lo -j ACCEPT
sudo iptables -A OUTPUT -m limit --limit 10/hour -j LOG --log-level 4 --log-prefix
'OUTPUT_Allow_10/hour: '
sudo iptables -A OUTPUT -j ACCEPT
sudo iptables -N PORT-SCAN
sudo iptables -A PORT-SCAN -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit
1/s -j RETURN
sudo iptables -A PORT-SCAN -j DROP
sudo sh -c "iptables-save > /etc/iptables.rules"
```

Pentru stergerea unei reguli:

```
iptables -D INPUT 12                    // Sterge regula a 12-a-l
```

Pentru a insera i regula pe o pozitie:

```
iptables -I INPUT 12 -p tcp --dport 24969 -j ACCEPT                    // Adauga o
regula pe pozitia a 12-a
```

OPTIUNI DE BAZA IPTABLES

-A - Append this rule to a rule chain. Valid chains for what we're doing are INPUT, FORWARD and OUTPUT, but we mostly
deal with INPUT in this tutorial, which affects only incoming traffic.
-L - List the current filter rules.
-m conntrack - Allow filter rules to match based on connection state. Permits the use of the --ctstate option.
--ctstate - Define the list of states for the rule to match on. Valid states are:
    NEW - The connection has not yet been seen.
    RELATED - The connection is new, but is related to another connection already permitted.
    ESTABLISHED - The connection is already established.
    INVALID - The traffic couldn't be identified for some reason.
-m limit - Require the rule to match only a limited number of times. Allows the use of the --limit option. Useful
for limiting logging rules.
--limit - The maximum matching rate, given as a number followed by "/second", "/minute", "/hour", or "/day"
depending on how often you want the rule to match. If this option is not used and -m limit is used, the default
is "3/hour".
-p - The connection protocol used.
--dport - The destination port(s) required for this rule. A single port may be given, or a range may be given as
start:end, which will match all ports from start to end, inclusive.
-j - Jump to the specified target. By default, iptables allows four targets:
    ACCEPT - Accept the packet and stop processing rules in this chain.
    REJECT - Reject the packet and notify the sender that we did so, and stop processing rules in this chain.
    DROP - Silently ignore the packet, and stop processing rules in this chain.
    LOG - Log the packet, and continue processing more rules in this chain. Allows the use of the --log-prefix
and --log-level options.
--log-prefix - When logging, put this text before the log message. Use double quotes around the text to use.
--log-level - Log using the specified syslog level. 7 is a good choice unless you specifically need something else.
-i - Only match if the packet is coming in on the specified interface.
-I - Inserts a rule. Takes two options, the chain to insert the rule into, and the rule number it should be.
-I INPUT 5 would insert the rule into the INPUT chain and make it the 5th rule in the list.
-v - Display more information in the output. Useful for if you have rules that look similar without using -v.
-s --source - address[/mask] source specification
-d --destination - address[/mask] destination specification
-o --out-interface - output name[+] network interface name ([+] for wildcard)

```
EXEMPLE DE REGULI:
iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
iptables -A FORWARD -j DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A INPUT -i eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
iptables --list    <--- Afiseaza statusul
iptables -t mangle --list
iptables -t nat --list
iptables -X nume_chain_de_sters                 // sterge un chain
iptables -N nume_chain_de_creat                 // creaza un nou chain
iptables -t raw --list
iptables -t filter --list
iptables -I INPUT -p udp -m udp --dport 53 -j ACCEPT
iptables -I INPUT -p tcp -m tcp --dport 53 -j ACCEPT
iptables-save > /etc/iptables-rules
------
Sintaxa generala este: iptables -A chain firewall-rule
-p is for protocol
-s is for source
-d is for destination
-j is target
-i is for in interface
-o is for out interface
–sport is for source port (for -p tcp, or -p udp)
–dport is for destination port (for -p tcp, or -p udp)
–tcp-flags is for TCP flags (for -p tcp)
–icmp-type is for ICMP Type (for -p icmp)
------
iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -j DROP
lsmod | grep ip_tables
system-config-securitylevel    <--- Daca nu ruleaza iptables, se pot porni astfel
(in Fedora)
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i eth0 -j ACCEPT
iptables -A INPUT -i ppp0 -j ACCEPT
iptables -A INPUT -s 192.168.0.4 -j ACCEPT
iptables -A INPUT -s 192.168.0.0/24 -j ACCEPT
iptables -A INPUT -s 192.168.0.0/255.255.255.0 -j ACCEPT
```

```
iptables -A INPUT -s 192.168.0.4 -m mac --mac-source 00:50:8D:FD:E6:32 -j ACCEPT
iptables -A INPUT -p tcp --dport 6881 -j ACCEPT
iptables -A INPUT -p tcp --dport 6881:6890 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 192.168.0.0/24 --dport 22 -j ACCEPT
iptables -D INPUT -s 202.100.85.0/24 -j DROP   <--- Sterge aceasta regula
sau:
------
Cu comanda:
iptables -L INPUT -n --line-numbers
Primim o lista cu regulile de blocare. Folosind numarul din stanga din dreptul
fiecarei linii, pentru a sterge linia:
iptables -D INPUT <<numarul_liniei>>
------
iptables -D INPUT -s 127.0.0.1 -p tcp --dport 111 -j ACCEPT
iptables -D INPUT 4
iptables -vnL --line-numbers
iptables -A INPUT -s 192.168.0.1 -j DROP
iptables -L -v #
iptables -L -v --line-numbers
iptables -L -t nat
iptables -L INPUT
iptables -t nat -L PREROUTING
iptables -L -t mangle
iptables -A INPUT -s 192.168.0.1 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j DROP
iptables -I INPUT 1 -s 192.168.0.1 -j ACCEPT
iptables -I INPUT 10 -p tcp --dport 22 -j DROP
iptables -F
iptables -F -t nat
iptables -F -t mangle
iptables -D INPUT 10
iptables -D PREROUTING 10 -t nat
iptables -D INPUT -s 192.168.0.1 -j ACCEPT
INPUT -s 192.168.0.1 -j ACCEPT
iptables-save >rules.txt
iptables-restore <rules.txt
iptables -P INPUT DROP
------
10 iptables rules to help secure your Linux box
Mastering iptables could take a while, but if you have a few rules to cover the
basic security needs,
you'll be well on your way to protecting your Linux system. Jack Wallen explains
some key rules to
get you started.

The iptables tool is a magnificent means of securing a Linux box. But it can be
rather overwhelming.
Even after you gain a solid understanding of the command structure and know what to
lock down and how
```

to lock it down, iptables can be confusing. But the nice thing about iptables is that it's fairly universal
in its protection. So having a few iptables rules to put together into a script can make this job much easier.

With that in mind, let's take a look at 10 such commands. Some of these rules will be more server oriented,
whereas some will be more desktop oriented. For the purpose of this article, I'm not going to explain all
of the various arguments and flags for iptables. Instead, I'll just give you the rule and explain what it
does. For more information on the specifics of the rule, you can read the man page for iptables, which
will outline the arguments and flags for you.

Note: This article is also available as a PDF download.

1: iptables -A INPUT -p tcp -syn -j DROP
This is a desktop-centric rule that will do two things: First it will allow you to actually work normally
on your desktop. All network traffic going out of your machine will be allowed out, but all TCP/IP traffic
coming into your machine will simply be dropped. This makes for a solid Linux desktop that does not need
any incoming traffic. What if you want to allow specific networking traffic in – for example, ssh for remote
management? To do this, you'll need to add an iptables rule for the service and make sure that service rule
is run before rule to drop all incoming traffic.

2: iptables -A INPUT -p tcp –syn –destination-port 22 -j ACCEPT
Let's build on our first command. To allow traffic to reach port 22 (secure shell), you will add this line.
Understand that this line will allow any incoming traffic into port 22. This is not the most secure setup
alone. To make it more secure, you'll want to limit which machines can actually connect to port 22 on the
machine. Fortunately, you can do this with iptables as well. If you know the IP address of the source
machine, you can add the -s SOURCE_ADDRESS option (Where SOURCE_ADDRESS is the actual address of the source
machine) before the –destination-port portion of the line.

3: /sbin/iptables -A INPUT -m state –state ESTABLISHED,RELATED -j ACCEPT
This will allow all previously initiated and accepted exchanges to bypass rule checking. The ESTABLISHED
and RELATED arguments belong to the –state switch. The ESTABLISHED argument says, "Any packet that belongs
to an existing connection," and the RELATED argument says, "Any packet that does not belong to an already

existing connection but is related to an existing connection.” The “state machine” of iptables is a means
for iptables to track connections with the help of the kernel level “conntrack” module. By tracking connections,
iptables knows what connections can be allowed and what can’t. This reduces the amount of work the administrator
has to do.

Here’s how state works. If the local user initiates a connection, that packet (to that connection) is set as
NEW in the prerouting chain. When the local user gets a return packet, the state is changed to ESTABLISHED
in the prerouting chain. So when a state is set as ESTABLISHED, it can be allowed with the right iptables rule.

4: iptables -N LOGDROP
With this handy chain, iptables will log all dropped packets. Of course, this is only part of the chain.
To complete it, you need to add the follow two rules:
iptables -A LOGDROP -J LOG
and
iptables -A LOGDROP -J DROP.
Now all matching packets (in this case, anything that has been dropped) will be added to the logdrop chain
which will log them and then drop them.

5: iptables -t nat -A PREROUTING -i WLAN_INTERFACE -p tcp –dportPORTNUMBERS -j DNAT –to-destination DESTINATION_IP
When you need to route packets from external sources to specific ports on specific internal machines, this
is what you want to do. This rule takes advantage of network address translation to route packets properly.
To suit your needs, the WLAN_INTERFACE must be changed to the WLAN interface that bridges the external network
to the internal network, the PORTNUMBERS must be changed, and DESTINATION_IP must be changed to match the IP
address of the destination machine.

6: iptables -A INPUT -p tcp –syn –dport 25 -j ACCEPT
This is the beginning of a SYN flood protection rule. This portion of the rule blocks DoS attacks on a mail
server port. (You can change this to suit your mail server needs.) There are three more portions of this
rule set. The first is to add the same rule but modify the port to whatever is being served up by whatever ports
you have open. The next portion is iptables -A INPUT -p tcp –syn -m limit –limit 1/s –limit-burst 4 -j ACCEPT,
which is the actual SYN flood protection. Finally, iptables -A INPUT -p tcp –syn -j DROP will drop all SYN
flood packets.

7: iptables -A INPUT -p tcp -m tcp -s MALICIOUS_ADDRESS -j DROP
This is where you can take care of malicious source IP addresses. For this to work properly, you must make
sure you know the offending source IP address and that, in fact, it's one you want to block. The biggest problem
with this occurs when the offending address has been spoofed. If that's the case, you can wind up blocking
legitimate traffic from reaching your network. Do your research on this address.

8: iptables -N port-scan
This is the beginning of a rule to block furtive port scanning. A furtive port scan is a scan that detects
closed ports to deduce open ports. Two more lines are needed to complete this rule:
iptables -A port-scan -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j RETURN
iptables -A port-scan -j DROP

Notice that the above rule set is adding a new chain called "port-scan". You don't have to name it such;
it's just easier to keep things organized. You can also add timeouts to the above rule set like so:
iptables -A specific-rule-set -p tcp --syn -j syn-flood
iptables -A specific-rule-set -p tcp --tcp-flags SYN,ACK,FIN,RST RST -j port-scan

9: iptables -A INPUT -i eth0 -p tcp -m state –state NEW -m multiport –dports ssh,smtp,http,https -j ACCEPT
What you see here is a chain making use of the multiport argument, which will allow you to set up multiple ports.
Using the multiport argument lets you write one chain instead of multiple chains. This single rule saves you
from writing out four separate rules, one each for ssh, smtp, http, and https. Naturally, you can apply this
to ACCEPT, DENY, REJECT.

10: iptables -A PREROUTING -i eth0 -p tcp –dport 80 -m state –state NEW -m nth –counter 0 –every 4 –packet 0 -j DNAT –to-destination 192.168.1.10:80
If you're looking to load balance between multiple mirrored servers (in the example case, load balancing a
Web server at 192.168.1.10), this rule is what you want. At the heart of this rule is the nth extension, which
tells iptables to act on every "nth" packet. In the example, iptables uses counter 0 and acts upon every 4th packet.
You can extend this to balance out your mirrored sites this way. Say you have four mirrored servers up and you
want to balance the load between them. You could have one line for each server like so:
iptables -A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m nth --counter 0 --every 4 --packet 0 -j DNAT --to-destination 192.168.1.10:80
iptables -A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m nth

```
--counter 0 --every 4 --packet 1 -j DNAT --to-destination 192.168.1.20:80
iptables -A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m nth
--counter 0 --every 4 --packet 2 -j DNAT --to-destination 192.168.1.30:80
iptables -A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m nth
--counter 0 --every 4 --packet 3 -j DNAT --to-destination 192.168.1.40:80
As you can see the server on .10 will be routed every 0 packet, the server on .20
will be routed every 1st
packet, the server on .30 will be routed every 2nd packet, and the server on .40
will be routed every 3rd packet.

-----------

# 1) Clear old Rules
iptables -F                                                    # Delete all existing
rules

# 2) Default Drop
iptables -P INPUT DROP                                           # Set default
chain policies to DROP
iptables -P FORWARD DROP                                       # Set default chain
policies to DROP
iptables -P OUTPUT DROP                                          # Set default
chain policies to DROP

# 3) Loopback
iptables -A INPUT -i lo -j ACCEPT                                  # Allow
loopback access from INPUT
iptables -A OUTPUT -o lo -j ACCEPT                                  # Allow
loopback access from Output

# 4) BLACKLIST IP's
# iptables -A INPUT -s "BLOCK_THIS_IP" -j DROP                                  #
Block a specific ip-address
# iptables -A INPUT -s "BLOCK_THIS_IP" -j DROP                                  #
Block a specific ip-address
# iptables -A INPUT -s "BLOCK_THIS_IP" -j DROP                                  #
Block a specific ip-address
# iptables -A INPUT -s "BLOCK_THIS_IP" -j DROP                                  #
Block a specific ip-address

# 5) WHITELIST IP's
iptables -A INPUT -s 127.0.0.1/32 -j ACCEPT                                 # Allow
Anything from localhost
iptables -A INPUT -s "ALLOW_THIS_IP"/32 -j ACCEPT                                  #
Allow Anything from KeyServer


# 6) ALLOWED SERVICES
iptables -A OUTPUT -o eth0 -p tcp --sport 25 -m state --state ESTABLISHED -j ACCEPT
          # PORT 25   SMTP   - Allow connections to outbound
```

```
iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT                          #
PORT 54   DNS    - Allow connections to outbound
iptables -A INPUT -p tcp -m tcp --dport 80 -m state --state NEW,ESTABLISHED -j
ACCEPT            # PORT 80   httpd  - Allow connections from anywhere
iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j
ACCEPT        # PORT 80   httpd  - Rate Limit from outside
iptables -A INPUT -p tcp -m tcp --dport 443 -m state --state NEW,ESTABLISHED -j
ACCEPT            # PORT 443  SSL    - Allow connections from anywhere
iptables -A INPUT -p tcp -m tcp --dport 2082 -m state --state NEW,ESTABLISHED -j
ACCEPT            # PORT 2082 cPanel - Allow connections to outbound
iptables -A INPUT -p tcp -m tcp --dport 2083 -m state --state NEW,ESTABLISHED -j
ACCEPT            # PORT 2083 cPanel - Allow connections to outbound
iptables -A INPUT -p tcp -m tcp --dport 2086 -m state --state NEW,ESTABLISHED -j
ACCEPT            # PORT 2086 WHM    - Allow connections to outbound
iptables -A INPUT -p tcp -m tcp --dport 2087 -m state --state NEW,ESTABLISHED -j
ACCEPT            # PORT 2087 WHM    - Allow connections to outbound

# 7) PING
iptables -A INPUT -p icmp -m icmp --icmp-type address-mask-request -j DROP
     # Drop Ping from address-mask-request
iptables -A INPUT -p icmp -m icmp --icmp-type timestamp-request -j DROP
      # Drop Ping from timestamp-request
iptables -A INPUT -p icmp -m icmp -m limit --limit 1/second -j ACCEPT
     # Rate Limit Ping from outside

# 8) Validate packets
iptables -A INPUT   -m state --state INVALID -j DROP                            #
Drop invalid packets
iptables -A FORWARD -m state --state INVALID -j DROP                            #
Drop invalid packets
iptables -A OUTPUT  -m state --state INVALID -j DROP                            #
Drop invalid packets
iptables -A INPUT -p tcp -m tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
  # Drop TCP - SYN,FIN packets
iptables -A INPUT -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j DROP
  # Drop TCP - SYN,RST packets

# 9) Reject Invalid networks (Spoof)
iptables -A INPUT -s 10.0.0.0/8       -j DROP                                   #
(Spoofed network)
iptables -a INPUT -s 192.0.0.1/24     -j DROP                                   #
(Spoofed network)
iptables -A INPUT -s 169.254.0.0/16   -j DROP                                   #
(Spoofed network)
iptables -A INPUT -s 172.16.0.0/12    -j DROP                                   #
(Spoofed network)
iptables -A INPUT -s 224.0.0.0/4      -j DROP                                   #
(Spoofed network)
iptables -A INPUT -d 224.0.0.0/4      -j DROP                                   #
(Spoofed network)
```

```
iptables -A INPUT -s 240.0.0.0/5      -j DROP                                  #
(Spoofed network)
iptables -A INPUT -d 240.0.0.0/5      -j DROP                                  #
(Spoofed network)
iptables -A INPUT -s 0.0.0.0/8        -j DROP                                  #
(Spoofed network)
iptables -A INPUT -d 0.0.0.0/8        -j DROP                                  #
(Spoofed network)
iptables -A INPUT -d 239.255.255.0/24 -j DROP                                  #
(Spoofed network)
iptables -A INPUT -d 255.255.255.255  -j DROP                                  #
(Spoofed network)

# 10) CHAINS

# FTP_BRUTE CHAIN
iptables -A INPUT -p tcp -m multiport --dports 20,21 -m state --state NEW -m recent
--set --name FTP_BRUTE
iptables -A INPUT -p tcp -m multiport --dports 20,21 -m state --state NEW -m recent
--update --seconds 60 --hitcount 4 --rttl --name FTP_BRUTE -j DROP

# SYNFLOOD CHAIN
iptables -A INPUT -m state --state NEW -p tcp -m tcp --syn -m recent --name
SYNFLOOD--set
iptables -A INPUT -m state --state NEW -p tcp -m tcp --syn -m recent --name SYNFLOOD
--update --seconds 1 --hitcount 60 -j DROP

# Logging CHAIN
iptables -N LOGGING                                                  # Create
`LOGGING` chain for logging denied packets
iptables -A INPUT -j LOGGING                                              # Create
`LOGGING` chain for logging denied packets
iptables -A LOGGING -m limit --limit 2/min -j LOG --log-prefix "IPTables Packet
Dropped: " --log-level 6    # Log denied packets to /var/log/messages
iptables -A LOGGING -j DROP

Limit ping responses
Any iptables rule can be tuned to respond only to a limited number of times per time
unit by using the limit module.
This can be extremely useful for log entries (A ping flooding will not lock down
your computer by writing to
log files). I will show an example on how to limit on ICMP responses. This is not
really useful, because it
imposes a maximum number of responses for ALL source IP addresses, but it may help
to reduce network traffic
on brute force attacks (and reduce volume in the log file).

iptables -A INPUT  -p icmp -m limit --limit 10/second -j ACCEPT
iptables -A INPUT  -p icmp -j DROP
```

This will limit the ICMP responses to a maximum of 10 replies per second. All the rest is silently dropped.
Beware: dropping ICMP responses may slow down or cut off legitimate users (for example when ICMP "Fragmentation
Needed" packets are dropped).

Dealing with brute force ssh attacks
A stateful firewall can make brute force ssh scans more painful to the attacker by slowing down the responses.
I will present a simple teergrubing strategy against ssh scans. This method relies on the IPTables/Netfilter
Recent Module, written by Snow-man. The idea is simple: permit only a limited number of new connections per
source IP address; drop any further connection attempt for a while.

```
iptables -A INPUT -p tcp --dport 22 -m recent --rcheck --seconds 60 --hitcount 2
--name SSH -j LOG --log-prefix "SH "
iptables -A INPUT -p tcp --dport 22 -m recent --update --seconds 60 --hitcount 2
--name SSH -j DROP
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name SSH
-j ACCEPT
iptables -A INPUT  -i $int_if -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Line 1 of the script checks if the source IP has already marked as 'Bad Guy' and logs the packet, if so.
The second line drops the packet if it comes from a marked IP address and marks the source again. This
ensures that the source will stay blacklisted as long as the attack continues. The third line marks the
source IP as 'Bad Guy' if there are more than 2 connection attempts per minute. Note that already
established connections continue to work (because the packets will no more arriving on 22).

Anti-spoofing rules

Generally speaking, IP spoofing is a technique of generating IP packets with a source address that
belongs to someone else. Spoofing creates a danger when hosts on the LAN permit access to their
resources and services to trusted hosts by checking the source IP of the packets. Using spoofing,
an intruder can fake the source address of his packets and make them look like they originated on
the trusted hosts. The basic idea of anti-spoofing protection is to create a firewall rule assigned
to the external interface of the firewall that examines source address of all packets crossing that
interface coming from outside. If the address belongs to the internal network or the firewall itself,

the packet is dropped.

Simple anti-spoofing rule looks like shown on Figure 14.15. Unlike the rule in the previous example,
anti-spoofing rule requires matching of the interface and direction. The idea is that packets that come
from outside must not have source addresses that match internal network or the firewall itself. The only
way to distinguish packets coming from outside from those coming from inside is to check which interface
of the firewall they cross and in which direction. Here the rule matches interface eth0, which is external,
and direction inbound.

Section 5.2.2 explains how a firewall object and its interfaces can be created. Section 5.2.5 has more
details on the firewall's interfaces, their types, and other properties. Section 7.2.4 explains the
concept of direction.

Figure 14.15. A Basic Anti-Spoofing Rule
A Basic Anti-Spoofing Rule

Here are the iptables commands generated for this rule:

```
# Rule 0 (eth0)
#
# anti spoofing rule
#
$IPTABLES -N In_RULE_0
$IPTABLES -A INPUT  -i eth0   -s 192.0.2.1   -j In_RULE_0
$IPTABLES -A INPUT  -i eth0   -s 192.168.1.1   -j In_RULE_0
$IPTABLES -A INPUT  -i eth0   -s 192.168.1.0/24   -j In_RULE_0
$IPTABLES -A FORWARD  -i eth0   -s 192.0.2.1   -j In_RULE_0
$IPTABLES -A FORWARD  -i eth0   -s 192.168.1.1   -j In_RULE_0
$IPTABLES -A FORWARD  -i eth0   -s 192.168.1.0/24   -j In_RULE_0
$IPTABLES -A In_RULE_0  -j LOG  --log-level info --log-prefix "RULE 0 -- DENY "
$IPTABLES -A In_RULE_0  -j DROP
```

The iptables commands were placed in INPUT and FORWARD chains to match both packets that are headed for
the firewall and through the firewall to hosts behind it. Rules match source address of the packets and
then log and drop them. Firewall Builder generated iptables commands to match all addresses of the firewall
(192.168.1.1, 192.0.2.1) and network behind it (192.168.1.0/24).

Let's see what gets generated for the same rule for PF:

```
# Tables: (1)
table <tbl.r0.s> { 192.0.2.1 , 192.168.1.1 }

# Rule  0 (en0)
# anti spoofing rule
#
block in   log  quick on en0 inet  from <tbl.r0.s>  to any
block in   log  quick on en0 inet  from 192.168.1.0/24  to any
#
```

Here, the compiler uses tables to make generated PF code more compact. Table tbl.r0.s can be used in other
rules wherever we need to operate with all addresses of the firewall.

Here is the same rule, compiled for PIX:

```
! Rule  0 (Ethernet1/0)
! anti-spoofing rule
!
access-list outside_acl_in  remark 0 (Ethernet1/0)
access-list outside_acl_in  remark anti-spoofing rule
access-list outside_acl_in deny   ip host 192.0.2.1 any
access-list outside_acl_in deny   ip host 192.168.2.1 any
access-list outside_acl_in deny   ip host 192.168.1.1 any
access-list outside_acl_in deny   ip 192.168.1.0 255.255.255.0 any

access-group outside_acl_in in interface outside
```

How to Log Linux IPTables Firewall Dropped Packets to a Log File

This article is part of our ongoing Linux IPTables series of articles. When things are not working as
expected with your IPTables rules, you might want to log the IPTables dropped packets for troubleshooting
purpose. This article explains how to log both incoming and outgoing dropped firewal packets.

If you are new to IPTables, first get yourself comfortable with the IPTables fundamental concepts.
Log All Dropped Input Packets

First we need to understand how to log all the dropped input packets of iptables to syslog.

If you already have whole bunch of iptables firewall rules, add these at the bottom, which will log all
the dropped input packets (incoming) to the /var/log/messages

```
iptables -N LOGGING
```

```
iptables -A INPUT -j LOGGING
iptables -A LOGGING -m limit --limit 2/min -j LOG --log-prefix "IPTables-Dropped: "
--log-level 4
iptables -A LOGGING -j DROP
```

In the above example, it does the following:

    iptables -N LOGGING: Create a new chain called LOGGING
    iptables -A INPUT -j LOGGING: All the remaining incoming packets will jump to the LOGGING chain
    line#3: Log the incoming packets to syslog (/var/log/messages). This line is explained below in detail.
    iptables -A LOGGING -j DROP: Finally, drop all the packets that came to the LOGGING chain. i.e now it
        really drops the incoming packets.

In the line#3 above, it has the following options for logging the dropped packets:

    -m limit: This uses the limit matching module. Using this you can limit the logging using –limit option.
    –limit 2/min: This indicates the maximum average matching rate for logging. In this example, for the
        similar packets it will limit logging to 2 per minute. You can also specify 2/second, 2/minute, 2/hour,
        2/day. This is helpful when you don’t want to clutter your log messages with repeated messages of the same
        dropped packets.
    -j LOG: This indicates that the target for this packet is LOG. i.e write to the log file.
    –log-prefix “IPTables-Dropped: ” You can specify any log prefix, which will be appended to the log messages
        that will be written to the /var/log/messages file
    –log-level 4 This is the standard syslog levels. 4 is warning. You can use number from the range 0
        through 7. 0 is emergency and 7 is debug.

Log All Dropped Outgoing Packets

This is same as above, but the 2nd line below has OUTPUT instead of INPUT.

```
iptables -N LOGGING
iptables -A OUTPUT -j LOGGING
iptables -A LOGGING -m limit --limit 2/min -j LOG --log-prefix "IPTables-Dropped: "
--log-level 4
iptables -A LOGGING -j DROP
```

Log All Dropped Packets (both Incoming and Outgoing)

This is same as before, but we’ll be taking the line number 2 from the previous two examples, and adding it here.

i.e We'll have a separate line for INPUT and OUTPUT which will jump to LOGGING chain.

---

1. Delete Existing Rules

Before you start building new set of rules, you might want to clean-up all the default rules, and existing rules.

Use the iptables flush command as shown below to do this.

```
iptables -F
(or)
iptables --flush
```

2. Set Default Chain Policies

The default chain policy is ACCEPT. Change this to DROP for all INPUT, FORWARD, and OUTPUT chains as shown below.

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
```

When you make both INPUT, and OUTPUT chain's default policy as DROP, for every firewall rule requirement you have,
you should define two rules. i.e one for incoming and one for outgoing.

In all our examples below, we have two rules for each scenario, as we've set DROP as default policy for both INPUT
and OUTPUT chain.

If you trust your internal users, you can omit the last line above. i.e Do not DROP all outgoing packets by default.

In that case, for every firewall rule requirement you have, you just have to define only one rule. i.e define rule
only for incoming, as the outgoing is ACCEPT for all packets.

Note: If you don't know what a chain means, you should first familiarize yourself with the IPTables fundamentals.

3. Block a Specific ip-address

Before we proceed further will other examples, if you want to block a specific ip-address, you should do that first
is shown below. Change the "x.x.x.x" in the following example to the specific ip-address that you like to block.

```
BLOCK_THIS_IP="x.x.x.x"
iptables -A INPUT -s "$BLOCK_THIS_IP" -j DROP
```

This is helpful when you find some strange activities from a specific ip-address in your log files, and you want
to temporarily block that ip-address while you do further research.

You can also use one of the following variations, which blocks only TCP traffic on eth0 connection for this
ip-address.

```
iptables -A INPUT -i eth0 -s "$BLOCK_THIS_IP" -j DROP
iptables -A INPUT -i eth0 -p tcp -s "$BLOCK_THIS_IP" -j DROP
```

4. Allow ALL Incoming SSH

The following rules allow ALL incoming ssh connections on eth0 interface.

```
iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```
Note: If you like to understand exactly what each and every one of the arguments means, you should read How to
Add IPTables Firewall Rules

5. Allow Incoming SSH only from a Specific Network
The following rules allow incoming ssh connections only from 192.168.100.X network.
```
iptables -A INPUT -i eth0 -p tcp -s 192.168.100.0/24 --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```
In the above example, instead of /24, you can also use the full subnet mask. i.e “192.168.100.0/255.255.255.0?.

6. Allow Incoming HTTP and HTTPS
The following rules allow all incoming web traffic. i.e HTTP traffic to port 80.
```
iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```
The following rules allow all incoming secure web traffic. i.e HTTPS traffic to port 443.
```
iptables -A INPUT -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT
```

7. Combine Multiple Rules Together using MultiPorts
When you are allowing incoming connections from outside world to multiple ports, instead of writing individual
rules for each and every port, you can combine them together using the multiport extension as shown below.
The following example allows all incoming SSH, HTTP and HTTPS traffic.
```
iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -m multiport --sports 22,80,443 -m state --state
ESTABLISHED -j ACCEPT
```

8. Allow Outgoing SSH
The following rules allow outgoing ssh connection. i.e When you ssh from inside to an outside server.
```
iptables -A OUTPUT -o eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A INPUT -i eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```
Please note that this is slightly different than the incoming rule. i.e We allow both the NEW and ESTABLISHED
state on the OUTPUT chain, and only ESTABLISHED state on the INPUT chain. For the incoming rule, it is vice
versa.

9. Allow Outgoing SSH only to a Specific Network

The following rules allow outgoing ssh connection only to a specific network. i.e You an ssh only to
192.168.100.0/24 network from the inside.

```
iptables -A OUTPUT -o eth0 -p tcp -d 192.168.100.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```

10. Allow Outgoing HTTPS

The following rules allow outgoing secure web traffic. This is helpful when you want to allow internet traffic
for your users. On servers, these rules are also helpful when you want to use wget to download some files
from outside.

```
iptables -A OUTPUT -o eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT
```

Note: For outgoing HTTP web traffic, add two additional rules like the above, and change 443 to 80.

11. Load Balance Incoming Web Traffic

You can also load balance your incoming web traffic using iptables firewall rules. This uses the iptables nth extension. The following example load balances the HTTPS traffic to three different
ip-address. For every 3th packet, it is load balanced to the appropriate server (using the counter 0).

```
iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth
--counter 0 --every 3
--packet 0 -j DNAT --to-destination 192.168.1.101:443
iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth
--counter 0 --every 3
--packet 1 -j DNAT --to-destination 192.168.1.102:443
iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth
--counter 0 --every 3
--packet 2 -j DNAT --to-destination 192.168.1.103:443
```

12. Allow Ping from Outside to Inside

The following rules allow outside users to be able to ping your servers.

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

13. Allow Ping from Inside to Outside

The following rules allow you to ping from inside to any of the outside servers.

```
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

14. Allow Loopback Access

You should allow full loopback access on your servers. i.e access using 127.0.0.1

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

15. Allow Internal Network to External network.
On the firewall server where one ethernet card is connected to the external, and another ethernet card
connected to the internal servers, use the following rules to allow internal network talk to external network.
In this example, eth1 is connected to external network (internet), and eth0 is connected to internal network
(For example: 192.168.1.x).

```
iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
```

16. Allow outbound DNS
The following rules allow outgoing DNS connections.

```
iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT
iptables -A INPUT -p udp -i eth0 --sport 53 -j ACCEPT
```

17. Allow NIS Connections
If you are running NIS to manage your user accounts, you should allow the NIS connections. Even when the SSH
connection is allowed, if you don't allow the NIS related ypbind connections, users will not be able to login.
The NIS ports are dynamic. i.e When the ypbind starts it allocates the ports.
First do a rpcinfo -p as shown below and get the port numbers. In this example, it was using port 853 and 850.

```
rpcinfo -p | grep ypbind
```

Now allow incoming connection to the port 111, and the ports that were used by ypbind.

```
iptables -A INPUT -p tcp --dport 111 -j ACCEPT
iptables -A INPUT -p udp --dport 111 -j ACCEPT
iptables -A INPUT -p tcp --dport 853 -j ACCEPT
iptables -A INPUT -p udp --dport 853 -j ACCEPT
iptables -A INPUT -p tcp --dport 850 -j ACCEPT
iptables -A INPUT -p udp --dport 850 -j ACCEPT
```

The above will not work when you restart the ypbind, as it will have different port numbers that time.
There are two solutions to this: 1) Use static ip-address for your NIS, or 2) Use some clever shell scripting
techniques to automatically grab the dynamic port number from the "rpcinfo -p" command output, and use those in
the above iptables rules.

18. Allow Rsync From a Specific Network
The following rules allows rsync only from a specific network.

```
iptables -A INPUT -i eth0 -p tcp -s 192.168.101.0/24 --dport 873 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 873 -m state --state ESTABLISHED -j ACCEPT
```

19. Allow MySQL connection only from a specific network
If you are running MySQL, typically you don't want to allow direct connection from outside. In most cases,
you might have web server running on the same server where the MySQL database runs.

However DBA and developers might need to login directly to the MySQL from their laptop and desktop using
MySQL client. In those case, you might want to allow your internal network to talk to the MySQL directly as
shown below.

```
iptables -A INPUT -i eth0 -p tcp -s 192.168.100.0/24 --dport 3306 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 3306 -m state --state ESTABLISHED -j ACCEPT
```

20. Allow Sendmail or Postfix Traffic

The following rules allow mail traffic. It may be sendmail or postfix.

```
iptables -A INPUT -i eth0 -p tcp --dport 25 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 25 -m state --state ESTABLISHED -j ACCEPT
```

21. Allow IMAP and IMAPS

The following rules allow IMAP/IMAP2 traffic.

```
iptables -A INPUT -i eth0 -p tcp --dport 143 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 143 -m state --state ESTABLISHED -j ACCEPT
```

The following rules allow IMAPS traffic.

```
iptables -A INPUT -i eth0 -p tcp --dport 993 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 993 -m state --state ESTABLISHED -j ACCEPT
```

22. Allow POP3 and POP3S

The following rules allow POP3 access.

```
iptables -A INPUT -i eth0 -p tcp --dport 110 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 110 -m state --state ESTABLISHED -j ACCEPT
```

The following rules allow POP3S access.

```
iptables -A INPUT -i eth0 -p tcp --dport 995 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 995 -m state --state ESTABLISHED -j ACCEPT
```

23. Prevent DoS Attack

The following iptables rule will help you prevent the Denial of Service (DoS) attack on your webserver.

```
iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT
```

In the above example:

- -m limit: This uses the limit iptables extension
- –limit 25/minute: This limits only maximum of 25 connection per minute. Change this value based on your specific requirement
- –limit-burst 100: This value indicates that the limit/minute will be enforced only after the total number of connection have reached the limit-burst level.

24. Port Forwarding
The following example routes all traffic that comes to the port 442 to 22. This means that the incoming ssh
connection can come from both port 22 and 422.
iptables -t nat -A PREROUTING -p tcp -d 192.168.102.37 --dport 422 -j DNAT --to 192.168.102.37:22
If you do the above, you also need to explicitly allow incoming connection on the port 422.
iptables -A INPUT -i eth0 -p tcp --dport 422 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 422 -m state --state ESTABLISHED -j ACCEPT

25. Log Dropped Packets
You might also want to log all the dropped packets. These rules should be at the bottom.
First, create a new chain called LOGGING.
iptables -N LOGGING
Next, make sure all the remaining incoming connections jump to the LOGGING chain as shown below.
iptables -A INPUT -j LOGGING
Next, log these packets by specifying a custom “log-prefix”.
iptables -A LOGGING -m limit --limit 2/min -j LOG --log-prefix "IPTables Packet Dropped: " --log-level 7
Finally, drop these packets.
iptables -A LOGGING -j DROP
All of the above 25 iptables rules are in shell script format: iptables-rules
---

Good collection of iptables rules!

Just wanted to mention that ” -m limit ” does match packets not connections, so in your example you will match 25 packets per minute, which I think is not what you want to.

The solution to limit the number of connections is to use connlimit match.

an example:

iptables -A INPUT -p tcp –syn –dport 80 -m connlimit –connlimit-above 15 –connlimit-mask 32 -j REJECT –reject-with tcp-reset

that will reject connections above 15 from one source IP – a very good rule to defend a web server.

Also it will be great to add to your list of rules an example with “hashlimit” match, which has more options when you want to protect from a DDoS attack.

With “limit” match you can limit the global rate of packets per time interval, but with “hashlimit”, you can limit them per IP, per combination IP + port, etc.

So an example for a web server will be something like that:

iptables -A INPUT -p tcp –dport 80 -m hashlimit –hashlimit 45/sec –hashlimit-burst 60 –hashlimit-mode srcip –hashlimit-name DDOS –hashlimit-htable-size 32768 –hashlimit-htable-max 32768 –hashlimit-htable-gcinterval 1000 –hashlimit-htable-expire 100000 -j ACCEPT

Hope this will help someone.
Anyway, thanks for a good article!

Hey Sharad,
Actually need to open port 53 for INPUT. Something like this will work:
dnsserver=ipaddress
iptables -A INPUT -p udp –sport 53 –dport 1024:65535 -d $dnsserver -j ACCEPT
That worked for me, please some advice if there’s a better or safer way

---

In our previous IPTables firewall series article, we reviewed how to add firewall rule using “iptables -A”.
We also explained how to allow incoming SSH connection. On a high-level, it involves following 3 steps.

Delete all existing rules: “iptables -F”
Allow only incoming SSH: “iptables -A INPUT -i eth0 -p tcp –dport 22 -j ACCEPT”
Drop all other incoming packets: “iptables -A INPUT -j DROP”

The above works. But it is not complete. One problem with the above steps is that it doesn’t restrict
the outgoing packets.
Default Chain Policy
The default policy of a chain is ACCEPT. If you don’t what what a chain means, you better read our iptables
introduction article. So, both the INPUT and OUTPUT chain’s default policy is ACCEPT. In the above 3 steps
we dropped all incoming packets at the end (except incoming ssh). However, we didn’t restrict the outgoing traffic.
As you notice below, it says “(policy ACCEPT)” next to all the three chain names (INPUT, OUTPUT, and FORWARD).
This indicates that the default chain policy is ACCEPT.

```
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
DROP       all  --  anywhere             anywhere
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

So, you have two options here.
Option 1: Add drop rules
At the end, add the following three drop rules that will drop all incoming, outgoing, and forward packets
(except those that are defined above these three rules). If you do this, the default chain policy is still
ACCEPT, which shouldn’t matter, as you are dropping all the packets at the end anyway.

```
iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
iptables -A FORWARD -j DROP
```

Option 2: Change the default chain policy to DROP

At the beginning, execute the following three commands that will change the chain's default policy to DROP.

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Now, if you add the allow ssh rule: "iptables -A INPUT -i eth0 -p tcp –dport 22 -j ACCEPT", and do iptables -L,
you'll notice that it says "(policy DROP)" next to all the three chains.

```
# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
DROP       all  --  anywhere             anywhere
Chain FORWARD (policy DROP)
target     prot opt source               destination
Chain OUTPUT (policy DROP)
target     prot opt source               destination
```

But there is a problem here. The allow ssh incoming connection rule will not work anymore, because all the
outgoing packets are dropped.

Allow Incoming Connections

When the default policy is DROP for INPUT and OUTPUT chains, for every incoming firewall rule, you need to
specify the following two rules.

Request rule: This is the request that comes from the client to the server for the incoming connection.

Response rule: This is for the response that goes out from the server to the client (for the corresponding
incoming request).

Example 1: Allow incoming SSH connection

This is to allow SSH connection from outside to your server. i.e You can ssh to your server from outside.
This involves two steps. First, we need to allow incoming new SSH connections. Once the incoming ssh connection
is allowed, we also need to allow the response back for that incoming ssh connection.

First, Allow incoming SSH connection request, as shown below.

```
iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
```

In the above example:

iptables -A INPUT: Append the new rule to the INPUT chain. For incoming connection request, this always
has to be INPUT.

-i eth0: This refers to the input interface. For incoming connections, this always has to be '-i'.

-p tcp: Indicates that this is for TCP protocol.

–dport 22: This refers to the destination port for the incoming connection. Port 22 is for ssh.

-m state: This indicates that the "state" matching module is used. We'll discuss more about "-m" option (

and all available matching modules for iptables) in future article.
–state NEW, ESTABLISHED: Options for the “state” matching module. In this example, only NEW and ESTABLISHED
states are allowed. The 1st time when a SSH connection request is initiated from the client to the server,
NEW state is used. ESTABLISHED state is used for all further request from the client to the server.

Next, Allow outgoing (ESTABLISHED state only) SSH connection response (for the corresponding incoming SSH
connection request).

```
iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```

In the above example:

iptables -A OUTPUT: Append the new rule to the OUTPUT chain. Since this is for the response rule (for the
corresponding incoming request) that goes out from the server, this should be OUTPUT.
-o eth0: This refers the output interface. For outgoing connections, this always has to be ‘-o’.
-p tcp: Indicates that this is for TCP protocol.
–sport 22: This refers to the source port for the outgoing connection. Port 22 is for ssh. Since the incoming
request (from the previous rule) came to the “destination” port, the outgoing response will go through the
“source” port.
-m state: This indicates that the “state” matching module is used.
–state ESTABLISHED: Since this is a response rule, we allow only ESTABLISHED connection (and not any
NEW connection).

Example 2: Allow incoming HTTP connection

This is to allow HTTP connection from outside to your server. i.e You can view your website running on the
server from outside.

Just like the above SSH incoming rules, this also involves two steps. First, we need to allow incoming new
HTTP connection. Once the incoming HTTP connection is allowed, we need to allow the response back for that incoming
HTTP connection.

First, Allow incoming HTTP connection request, as shown below.

```
iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
```

Next, Allow outgoing (ESTABLISHED only) HTTP connection response (for the corrresponding incoming SSH
connection request).

```
iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

Note: In the above HTTP request and response rule, everything is same as the SSH example except the port number.

Allow Outgoing Connections

When the default policy is DROP for the INPUT and OUTPUT chains, for every outgoing firewall rule, you need
to specify the following two rules.

Request rule: This is the request that goes out from the server to outside for the outgoing connection.

Response rule: This is for the response that comes back from the outside to the server (for the corresponding outgoing request).

Example 3: Allow outgoing SSH connection

This is to allow SSH connection from your server to the outside. i.e You can ssh to outside server from your server.

This involves two steps. First, we need to allow outgoing new SSH connection. Once the outgoing ssh connection is allowed, we also need to allow the response back for that outgoing ssh connection.

First, Allow outgoing SSH connection request, as shown below.

```
iptables -A OUTPUT -o eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
```

In the above example:

iptables -A OUTPUT: Append the new rule to the OUTPUT chain. For outgoing connection request, this always has to be OUTPUT.

-o eth0: This refers the output interface. For outgoing connections, this always has to be '-o'.

-p tcp: Indicates that this is for TCP protocol.

–dport 22: This refers to the destination port for the outgoing connection.

-m state: This indicates that "state" matching module is used.

–state NEW, ESTABLISHED: Options for the "state" matching module. In this example, only NEW and ESTABLISHED states are allowed. The 1st time when a SSH connection request is initiated from the server to the outside, NEW state is used. ESTABLISHED state is used for all further request from the server to the outside.

Next, Allow outgoing (ESTABLISHED only) SSH connection response (for the corresponding incoming SSH connection request).

```
iptables -A INPUT -i eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```

In the above example:

iptables -A INPUT: Append the new rule to the INPUT chain. Since this is for the response rule (for the corresponding outgoing request) that comes from the outside to the server, this should be INPUT.

-i eth0: This refers the input interface. For incoming connections, this always has to be '-i'.

-p tcp: Indicates that this is for TCP protocol.

–sport 22: This refers to the source port for the incoming connection. Since the outgoing request (from the previous rule) went to the "destination" port, the incoming response will come from the "source" port.

-m state: This indicates that the "state" matching module is used.

–state ESTABLISHED: Since this is a response rule, we allow only ESTABLISHED connection (and not any NEW connection).

Putting it all together
Create rules.sh shell script which does the following:
    Delete all existing rules
    Set default chain policies
    Allow inbound SSH
    Allow inbound HTTP
    Allow outbound SSH
First, create the rules.sh
$ vi rules.sh
```
# 1. Delete all existing rules
iptables -F
# 2. Set default chain policies
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
# 3. Allow incoming SSH
iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
# 4. Allow incoming HTTP
iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
# 5. Allow outgoing SSH
iptables -A OUTPUT -o eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A INPUT -i eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```
Next, execute the rules.sh and view the rules.
```
# chmod u+x rules.sh
# ./rules.sh
# iptables -L
Chain INPUT (policy DROP)
target     prot opt source      destination
ACCEPT     tcp  --  anywhere    anywhere      tcp dpt:ssh state NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere    anywhere      tcp dpt:http state NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere    anywhere      tcp spt:ssh state ESTABLISHED
Chain FORWARD (policy DROP)
target     prot opt source      destination
Chain OUTPUT (policy DROP)
target     prot opt source      destination
ACCEPT     tcp  --  anywhere    anywhere      tcp spt:ssh state ESTABLISHED
ACCEPT     tcp  --  anywhere    anywhere      tcp spt:http state ESTABLISHED
ACCEPT     tcp  --  anywhere    anywhere      tcp dpt:ssh state NEW,ESTABLISHED
```
Using this as a basis you should be able to write your own incoming and outgoing iptables firewall rules.
There is lot more to cover in IPTables. Stay tuned!
Previous articles in the iptables series:
==========
Comenzi afisare:

```
cat /etc/hostname
cat /etc/hosts
cat /etc/resolv.conf
================================================================================
=====================================
Setare DNS --->> BIND9
Instalare BIND9 si utilitare:
apt-get update
apt-get install bind9 dnsutils
apt-get install bind9 bind9utils bind9-doc                    <<---- Instalare in
16.04 LTS

systemctl restart bind9
sau
service bind9 restart
---------------

In fisierul /etc/hosts trebuie sa am:
----------------

# IP Address    Hostname.DOMAIN         Alias
#-----------------------------------------------------------------

# The following lines are desireble for IPv6 capable hosts
::1             localhost               ip6-localhost ip6-loopback
fe00::0         ip6-localnet
ff00::0         ip6-mcastprefix
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

127.0.0.1 localhost.localdomain localhost
# Auto-generated hostname. Please do not remove this comment.
86.107.58.227 nume_host.domeniu.ro  nume_host

---------------

In fisierul /etc/hostname trebuie sa am:
----------------

numele_hostului

---------------------------------
In fisierul /etc/resolv.conf, trebuie sa am:
search inovatop.ro
nameserver 127.0.0.1

In PROXMOX, acest fisier se completeaza in format web, alegand pentru container la
DNS Server --> Edit, si completand
127.0.0.1
---------------
```

Editam fisierul /etc/bind/named.conf.options unde sa setam adresele IP ale serverelor DNS externe (ale ISP-ului)

```
---------------
options {
        directory "/var/cache/bind";

        allow-transfer {none;};

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                193.138.192.2;
                193.138.192.22;
                8.8.8.8;
                8.8.4.4;
        };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
        version "Please, contact our SysAdmin";     # to hide BIND version
        allow-recursion { 127.0.0.1; };
};

---------------
Editam /etc/bind/named.conf.local, unde vom crea zona domeniului si cea de reverse:
---------------
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
// include "/etc/bind/zones.rfc1918";

// FORWARD LOOKUP ZONE - Holds a record and maps hostnames to IPs.
zone "inovatop.ro"
{
```

```
     type master;
     file "/etc/bind/zones/db.inovatop.ro";
};

// REVERSE LOOKUP ZONE - Holds PTR records and maps IP addresses to hostnames.
// 86.107.58.226
zone "58.107.86.in-addr.arpa"
{
     type master;
     file "/etc/bind/reverse/rev.58.107.86.in-addr.arpa";
};

logging {
    channel bind_log {
        file "/var/log/bind.log" versions 1 size 50m;
        // Set the severity to dynamic to see all the debug mesages.
        // critical | error | warning | notice | info | debug [level] | dynamic |
        severity dynamic;
        print-time yes;
        print-severity yes;
        print-category yes;
        // severity warning;
        // severity debug 3;
    };
    category default {
        bind_log;
    };
    category queries {
        bind_log;
    };
};

----------------
Tot aici, jos de tot pot seta unde si la ce nivel se vor salva mesajele de log
pentru DNS Server:
----------------
logging {
    channel bind_log {
        file "/var/log/bind.log" versions 1 size 25m;
        // Set the severity to dynamic to see all the debug mesages.
        // critical | error | warning | notice | info | debug [level] | dynamic |
        severity dynamic;
        print-time yes;
        print-severity yes;
        print-category yes;
        // severity warning;
        // severity debug 3;
    };
    category default {
        bind_log;
```

```
    };
    category queries {
        bind_log;
    };
};
----------------
Creez fisierul /var/log/bind.log, si il aloc grupului bind:
sudo touch /var/log/bind.log
sudo chown bind /var/log/bind.log

Merg in fisierul: /etc/apparmor.d/usr.sbin.named si adaug acolo linia:
/var/log/bind.log w,

apoi reincarc profilul:
cat /etc/apparmor.d/usr.sbin.named | sudo apparmor_parser -r
----------------
Creem fisierele de zona (principala si reverse) si le asezam in folderele zones si
reverse:
mkdir /etc/bind/zones
mkdir /etc/bind/reverse
Editez fisierul: /etc/bind/zones/db.inovatop.ro
----------------

; BIND data file for INOVATOP.RO zone;
;
$TTL    172800                                          ; (2 days) Conform
RIPE.NET
;(name) (ttl)   Class   SOA     Origin                  Postmaster      Comments
;-------------------------------------------------------------------------------
---------
@               IN      SOA     ns.inovatop.ro.         sysadmin.inovatop.ro. (
                                     2012100801                 ; Serial no. - based
on date
                                          86400                 ; Refresh after 1
day
                                           7200                 ; Retry after 2
hours
                                        3542400                 ; Expire after 41
days
                                         172800 )               ; Negative Cache TTL
(2 days)
;-------------------------------------------------------------------------------
---------
;(name) (ttl)   Class   NS      Nameserver      Name
;-------------------------------------------------------------------------------
---------
; Nameservers definition
@               IN      NS      ns.inovatop.ro.                 ; Inet address of
name server
;-------------------------------------------------------------------------------
```

```
---------
; Mail exchanger definition
@               IN      MX 10   invtmtax.inovatop.ro.           ; Primary Mail
Exchanger
;-------------------------------------------------------------------------------
---------
; A Records definition
@                       IN      A       86.107.58.226           ; Main Domain
Address
ns                      IN      A       86.107.58.226           ; Name Server
www                     IN      A       86.107.58.226           ; Web Server
invtmtax                IN      A       86.107.58.226           ; Mail Server
invtwmsx                IN      A       86.107.58.226           ; Web Mail
invtftpx                IN      A       86.107.58.226           ; ftp server
invtpmax                IN      A       86.107.58.226           ; PhpMyAdmin
invtpadx                IN      A       86.107.58.226           ; Postfix Web Admin
invtcacx                IN      A       86.107.58.226           ; Web Monitoring
invtphlx                IN      A       86.107.58.226           ; Newsletter
;-------------------------------------------------------------------------------
---------
; SPF (Sender Policy Framework) Records
; version 1 of SPF and servers which are allowed to send e-mail from @inovatop.ro
email
; address are the one listed in the a records, mx records and also xxx.xxx.xxx.xxx
address.
; inovatop.ro.          IN      TXT     "v=spf1 a mx ~all"
; inovatop.ro.          IN      SPF     "v=spf1 a mx ~all"
inovatop.ro.            IN      TXT     "v=spf1 a mx a:inovatop.ro ip4:86.107.58.226
mx:invtmtax.inovatop.ro ~all"
inovatop.ro.            IN      SPF     "v=spf1 a mx a:inovatop.ro ip4:86.107.58.226
mx:invtmtax.inovatop.ro ~all"
;-------------------------------------------------------------------------------
---------
; DKIM Records  InovaSep2012 for inovatop.ro
/etc/opendkim/InovaSep2012.txt
; Public key records:
InovaSep2012._domainkey.inovatop.ro.            IN      TXT
"k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC4oEFybiCVSSx6myYpiODMHt1CBfm0VjnR+Cs
MoIc592ea9ibJUz36++q0X9SH/cEfYrJWel6PNg1rDWuZ36M0oVTso6LvsVvEplv3Hax5YcSvsILmXLu2BYh
s9dJRhiYEvx1I5pIpdqJ0EYraB2fLSU/JYI2q9aBTFkfCsMZb/QIDAQAB"
; DKIM Author Domain Signing Practices
_adsp._domainkey.inovatop.ro                    IN      TXT     "dkim=unknown"
;-------------------------------------------------------------------------------
---------
; Domainkeys Records    InovaDKSep2012 for inovatop.ro
/etc/dk-filter/public.key
; Create the policy sub-domain:
_domainkey.inovatop.ro.                         IN      TXT     "o=~;
r=sysadmin@inovatop.ro"
; Public key records:
```

```
InovaDKSep2012._domainkey.inovatop.ro.          IN      TXT
"k=rsa;p=MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAK74+N3D79K9l8Yt6gcJ/u3NCTMPtOa9h2KF5rhfkpV
mouLciwx0bhVX094yqO76rdFGJZxvHiPySkSgPMmGTikCAwEAAQ=="
;-------------------------------------------------------------------------------
---------

----------------
Editez fisierul de reverse, /etc/bind/reverse/rev.58.107.86.in-addr.arpa:
----------------

; BIND reverse data file for local 86.107.58.XXX net
;
$TTL    172800                                  ; (2 days) Conform RIPE.NET
;(name) (ttl)   Class   SOA     Origin                  Postmaster      Comments
;-------------------------------------------------------------------------------
-----
@               IN      SOA     ns.inovatop.ro.         sysadmin.inovatop.ro. (
                                     2012100801         ; Serial no. - based on date
                                          86400         ; Refresh after 1 day
                                           7200         ; Retry after 2 hours
                                        3542400         ; Expire after 41 days
                                         172800 )       ; Negative Cache TTL (2
days)
;-------------------------------------------------------------------------------
-----
;(name) (ttl)           Class   NS      Nameserver      Name
;-------------------------------------------------------------------------------
-----
; Nameserver definition
58.107.86.in-addr.arpa. IN      NS      ns.inovatop.ro. ; Inet Address of name
server
;-------------------------------------------------------------------------------
-----
; PTR definition
226             IN      PTR     inovatop.ro.            ; Reverse for Main Domain
226             IN      PTR     ns.inovatop.ro.         ; Reverse for Web Server
226             IN      PTR     invtmtax.inovatop.ro.   ; Reverse for MX Server
226             IN      PTR     www.inovatop.ro.        ; Reverse for Web Server
226             IN      PTR     invtwmsx.inovatop.ro.   ; Reverse for Web Mail
226             IN      PTR     invtpmax.inovatop.ro.   ; Reverse for PMA
226             IN      PTR     invtpadx.inovatop.ro.   ; Reverse for Web Mail Admin
226             IN      PTR     invtftpx.inovatop.ro.   ; Reverse for FTP Server
226             IN      PTR     invtcacx.inovatop.ro.   ; Reverse for Web Monitoring
226             IN      PTR     invtphlx.inovatop.ro.   ; Reverse for Newsletter
;-------------------------------------------------------------------------------
-----


Fisierul /etc/bind/db.0
```

```
---------------------
;
; BIND reverse data file for broadcast zone
;
$TTL    172800                                          ; 2 days
;(name) (ttl)   Class   SOA     Origin          Postmaster      Comments
;-------------------------------------------------------------------------------
-----
@       IN              SOA     localhost.      sysadmin.inovatop.ro. (
                                2012102201                      ; Serial no. - based
on date
                                86400                           ; Refresh after 1
day
                                7200                            ; Retry after 2
hours
                                3542400                         ; Expire after 41
days
                                172800 )                        ; Negative Cache TTL
(2 days)
;-------------------------------------------------------------------------------
-----
;(name) (ttl)   Class   NS      Nameserver      Name
;-------------------------------------------------------------------------------
-----
; Nameserver definition
@               IN      NS      localhost.
;-------------------------------------------------------------------------------
-----
----------------------


Fisierul /etc/bind/db.127

----------------------
;
; BIND reverse data file for local loopback interface
;
$TTL    172800                                  ; 2 days
;(name) (ttl)   Class   SOA     Origin          Postmaster      Comments
;-------------------------------------------------------------------------------
-----
@       IN              SOA     localhost.      sysadmin.inovatop.ro. (
                                2012102201                      ; Serial no. - based
on date
                                86400                           ; Refresh after 1
day
                                7200                            ; Retry after 2
hours
                                3542400                         ; Expire after 41
days
```

```
                                172800 )                        ; Negative Cache TTL
(2 days)
;-------------------------------------------------------------------------------
-----
;(name) (ttl)   Class   NS      Nameserver      Name
;-------------------------------------------------------------------------------
-----
; Nameserver definition
@               IN      NS      localhost.
;-------------------------------------------------------------------------------
-----
; PTR definition
1.0.0           IN      PTR     localhost.
;-------------------------------------------------------------------------------
-----
```

Fisierul /etc/bind/db.255

```
;
; BIND data file for broadcast zone
;
$TTL    172800                                          ; 2 days
;(name) (ttl)   Class   SOA     Origin          Postmaster      Comments
;-------------------------------------------------------------------------------
---------
@               IN      SOA     localhost.      sysadmin.inovatop.ro. (
                                2012102201                      ; Serial no. - based
on date
                                86400                           ; Refresh after 1
day
                                7200                            ; Retry after 2
hours
                                3542400                         ; Expire after 41
days
                                172800 )                        ; Negative Cache TTL
(2 days)
;-------------------------------------------------------------------------------
---------
;(name) (ttl)   Class   NS      Nameserver      Name
;-------------------------------------------------------------------------------
---------
; Nameservers definition
@               IN      NS      localhost.
;-------------------------------------------------------------------------------
---------
```

Fisierul /etc/bind/db.local

```
;
; BIND data file for local loopback interface
;
$TTL    172800                                          ; 2 days
;(name) (ttl)   Class   SOA     Origin          Postmaster      Comments
;-------------------------------------------------------------------------------
---------
@               IN      SOA     localhost.      sysadmin.inovatop.ro. (
                                2012102201                      ; Serial no. - based
on date
                                86400                           ; Refresh after 1
day
                                7200                            ; Retry after 2
hours
                                3542400                         ; Expire after 41
days
                                172800 )                        ; Negative Cache TTL
(2 days)
;-------------------------------------------------------------------------------
---------
;(name) (ttl)   Class   NS      Nameserver      Name
;-------------------------------------------------------------------------------
---------
; Nameservers definition
@               IN      NS      localhost.
;-------------------------------------------------------------------------------
---------
; A Records definition
@               IN      A       127.0.0.1
@               IN      AAAA    ::1
;-------------------------------------------------------------------------------
---------
```

Now a very important step is to stop this server from being an open DNS server. To the outside world it should only
respond to queries for domains it is configured as an authoritative server. Otherwise, anyone can use your DNS server
like opendns :/
vi /etc/bind/named.conf.options

```
 # at the end of the file, just above the enclosure "};" which ends the options
part, insert this line
 # this is assuming you want to allow all lookups from your internal network
 # and that your internal network is 192.168.24.0/24
allow-recursion { 127.0.0.1; 192.168.24.0/24; };
----------------
Pornire / oprire server:
/etc/init.d/bind9 stop
/etc/init.d/bind9 start
/etc/init.d/bind9 restart
service bind9 stop
service bind9 start
service bind9 restart
----------------
Trebuie sa setez regulile iptables pentru a permite accesul pe portul 53 pentru
protocoalele tcp si udp:
iptables -I INPUT -p udp -m udp --dport 53 -j ACCEPT
iptables -I INPUT -p tcp -m tcp --dport 53 -j ACCEPT
iptables-save > /etc/iptables-rules
----------------
TESTE

dig face parte din dnsutils
in cazul in care nu functioneaza trebuie instalate cu:
apt-get update
apt-get install dnsutils

dig @localhost example.com
dig @localhost -x 86.107.58.226

Configuram serverul sa utilizeze DNS serverul nostru ca si principal
vi /etc/resolv.conf
 # add the below line as the first nameserver entry
nameserver 127.0.0.1
 # save the file, no need to restart anything

-----------------------

In Ubuntu >= 14.04, se editeaza fisierul:
/etc/resolvconf/resolv.conf.d/base
cu urmatoarele linii:

nameserver 127.0.0.1
search nume_domeniu.ro

Dupa care se restarteaza serviciul:
service resolvconf restart

-----------------
```

Test final:
dig example.com
dig -x 86.107.58.226

Alte teste:
ping example.com
dig -x 127.0.0.1
named-checkconf /etc/bind/named.conf
named-checkconf /etc/bind/named.conf.local
named-checkconf /etc/bind/named.conf.options
named-checkconf /etc/bind/named.conf.default-zones
Daca nu sunt erori, atunci la iesire nu apare nici un mesaj, altfel sunt afisate erorile de sintaxa.
named-checkzone localhost /etc/bind/db.local
named-checkzone inovatop.ro /etc/bind/zones/db.inovatop.ro
named-checkzone 58.107.86.in-addr.arpa /etc/bind/reverse/rev.58.107.86.in-addr.arpa
nslookup www.inovatop.ro
nslookup 86.107.58.226
- Line 1: The server should ALWAYS be localhost, unless you're renamed /etc/resolve.conf as a temporary test,
in which case it should be the hostname.
- Line 2: The server's address should ALWAYS be 127.0.0.1, unless you've renamed /etc/resolv.conf as a
temporary test, in which case it should be 0.0.0.0.
- Line 3: The name should always be the fully qualified domain name appearing as an nslookup arg (forward dns)
or serving as an answer to a lookup on the IP arg to nslookup (reverse dns).
- Line 4: The Address should always be the IP appearing as an nslookup arg (reverse dns) or serving as an
answer to a lookup on the Fully Qualified Doman Name arg to nslookup (forward dns).

nslookup www.example.com 192.168.255.53
nslookup -type=MX inovatop.ro
nslookup -all imta.inovatop.ro
nslookup -type=SOA inovatop.ro 86.107.58.226

host inovatop.ro
host www
host -l inovatop.ro

dig 86.107.58.226
dig www.inovatop.ro
dig inovatop.ro
dig @86.107.58.226 www.inovatop.ro
dig @192.168.135.130 -x 192.168.0.10
dig -t txt -c chaos VERSION.BIND @86.107.58.226

Test procedure: Run on a terminal:
1. Start bind: service named start

2. Zone transfer must be denied:
dig +short @127.0.0.1 intranet.mydomain axfr
; Transfer failed
3. IP address for dhcp019.intranet.mydomain:
dig +short @127.0.0.1 dhcp019.intranet.mydomain
10.0.1.19
4. Reverse DNS for 10.0.1.19:
dig +short @127.0.0.1 -x 10.0.1.19
dhcp019.intranet.mydomain
5. MX register:
dig +short @127.0.0.1 intranet.mydomain mx
10 mail.intranet.mydomain
6. Start Of Authority (SOA):
dig +short @127.0.0.1 intranet.mydomain soa
dns.intranet.mydomain. hostmaster.intranet.mydomain 1 10800 3600 604800 86400
7. Nameserver cname:
dig +short @127.0.0.1 ns1.intranet.mydomain cname
dns.intranet.mydomain
8. Localhost reverse address:
dig +short @127.0.0.1 -x 127.0.0.1
localhost.

In cazul in care BIND nu porneste, pot sa rulez:

/usr/sbin/named -g

sau

named -p 53 -g

sau

netstat -punta | grep named

sau

netstat -paln | grep 953

acesta imi va intoarce un raport... in care imi va spune ce nereguli a gasit... De exemplu:
29-Dec-2011 04:31:37.922 /etc/bind/named.conf.local:15: missing ';' before 'zone'
sau:
23-Oct-2012 01:08:47.817 none:0: open: /etc/bind/rndc.key: permission denied
23-Oct-2012 01:08:47.818 couldn't add command channel 127.0.0.1#953: permission denied

Daca vreau sa vad care sunt porturile la care se asculta:
netstat -aunt

Update a running Proxmox Virtual Environment 2.x to latest 2.3

Check your sources.list file, should look like this:

```
deb http://http.at.debian.org/debian squeeze main contrib

# PVE packages provided by proxmox.com
deb http://download.proxmox.com/debian squeeze pve

# security updates
deb http://security.debian.org/ squeeze/updates main contrib
```

Update your repository and packages:

```
apt-get update
```

If you get any errors, your sources.list (or your network) has a problem. Before you update your system, you should stop all your running VM´s.

Now upgrade the packages:

```
apt-get dist-upgrade
```

Reboot to activate the new Kernel, to check if you got all packages, run 'pveversion -v' and compare your output (all packages should have equal or higher version numbers):

```
pve-server:~#pveversion -v

pve-manager: 2.3-13 (pve-manager/2.3/7946f1f1)
running kernel: 2.6.32-19-pve
proxmox-ve-2.6.32: 2.3-96
pve-kernel-2.6.32-19-pve: 2.6.32-96
lvm2: 2.02.95-1pve2
clvm: 2.02.95-1pve2
corosync-pve: 1.4.4-4
openais-pve: 1.1.4-2
libqb: 0.10.1-2
redhat-cluster-pve: 3.1.93-2
resource-agents-pve: 3.9.2-3
fence-agents-pve: 3.1.9-1
pve-cluster: 1.0-36
qemu-server: 2.3-20
pve-firmware: 1.0-21
libpve-common-perl: 1.0-49
libpve-access-control: 1.0-26
libpve-storage-perl: 2.3-7
```

```
vncterm: 1.0-4
vzctl: 4.0-1pve2
vzprocps: 2.0.11-2
vzquota: 3.1-1
pve-qemu-kvm: 1.4-10
ksm-control-daemon: 1.1-1

pve-server:~#
-------------------------------------------------------
Comenzi retea:
netstat -rn                     // to print the Kernel IP Routing table
ip link list            // vizualizeaza conexiunile     <==> ip route ls
ip address show         // vizualizeaza adresele IP
ip route show           // vizualizeaza rutele
route -n                        // vizualizeaza rutele - tabela de rutare
ip neigh show       // vizualizeaza tabela ARP (Address Resolution Protocol) a
vecinilor
ping -c 1 dkfbmtax
ip neigh show           // acum se vor gasi mai multi vecini in tabele ARP
ip neigh delete 9.3.76.43 dev eth0
ip neigh show
ip rule list            // afiseaza prioritatea tuturor regulilor (Regulile
prestabilite)
ip route list table local                       // afiseaza tabela locala
ip route list table main                        // afiseaza tabela principala
ip route list table default                     // tabela default este goala
echo 200 Ion >> /etc/iproute2/rt_tables         // creaza o regula numita Ion
ip rule add from 10.0.0.10 table Ion
ip rule ls
ip route add default via 195.96.98.253 dev ppp2 table Ion               // se
genereaza tabela lui Ion
ip route flush cache                            // se sterge cache-ul cu rute
Crearea a doua tabele de rutare aditionale, T1 si T2 care vor fi adaugate in
/etc/iproute2/rt_tables:
ip route add $P1_NET dev $IF1 src $IP1 table T1         // $P1_NET = Adresa primei
retele | $IF1 = prima interfata | $IP1 = adresa IP asociata primei interfete | T1 =
Primul tabel aditional de rutare
ip route add default via $P1 table T1                           // $P1 = adresa de
gateway pentru Provider 1
ip route add $P2_NET dev $IF2 src $IP2 table T2
ip route add default via $P2 table T2
Trebuie configurata tabela main (principala) de rutare. E bine sa se faca rutarea
catre un vecin conectat direct.
ip route add $P1_NET dev $IF1 src $IP1
ip route add $P2_NET dev $IF2 src $IP2
ip route add default via $P1                                            // Ruta
prestabilita
Regulile care aleg tabela de rutare potrivita. Rutarea se face pe o anumita
interfata pentru adresa IP corespunzatoare.
ip rule add from $IP1 table T1
```

```
ip rule add from $IP2 table T2
```

Adding Persistent Static Routes in Debian

Adding a static Route in Debian can be easily done by using the command:

```
route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.1.2 dev eth1
```

Here, the network 192.168.2.0 is accessible through next hop 192.168.1.2 exit interface eth1. However, the problem is that the system forgets the route if the network service restarts. Here's how the route can be made permanent:

```
# The primary network interface
auto eth1
allow-hotplug eth1
iface eth1 inet static
    address 192.168.1.3
    netmask 255.255.255.0

up route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.1.2 dev eth1
up route add -net 192.168.10.0 netmask 255.255.255.0 gw 192.168.1.2 dev eth1

down route del -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.1.2 dev eth1
down route del -net 192.168.10.0 netmask 255.255.255.0 gw 192.168.1.2 dev eth1
```

The route is would now be updated every time the network service is restarted. Works like a charm :)

HowTo: Add persistent Static Routes in Debian/Ubuntu Linux

Adding a Static route in Debain Linux can be done using the "route" command and editing the network script files.

To keep the Static Route persistent or you want to add the route entries to the network script files (not using the route command) then all you need to do is to edit the file /etc/network/interfaces

view plaincopy to clipboardprint?

```
    iface eth1 inet static
            address 192.168.0.1
            netmask 255.255.255.0
            broadcast 192.168.0.255
            gateway 192.168.0.1

            # static route
           up route add -net 192.168.1.1/24 gw 192.168.1.1 dev eth1
```

view plaincopy to clipboardprint?

```
    /etc/init.d/networking restart

-----------------------------------------
```

Howto add permanent static routes in Ubuntu

Static routing is the term used to refer to the manual method used to set up routing. An administrator enters routes into the router using configuration commands. This method has the advantage of being predictable, and simple to set up. It is easy to manage in small networks but does not scale well.

Advantages of Static Routes:
- Easy to configure
- No routing protocol overhead

Disadvantages of Static Routes:
- Network changes require manual reconfiguration
- Network outages cannot be automatically routed around
- Does not scale well in large networks.

Add a Static route using "route" command
route add [-net|-host] <IP/Net> netmask <Mask> gw <Gateway IP> dev <Int>X

Example:
route add -net 10.10.10.0 netmask 255.255.255.0 gw 192.168.1.1 dev eth0
route add -host 10.10.1.1 netmask 255.255.255.0 gw 192.168.1.1 dev eth0

This adds the route immediatly to the Kernel IP routing table. To confirm the route has been successfully, simply type the "route" command with no arguements:
route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.1.254 * 255.255.255.0 U 0 0 0 eth0
localnet * 255.255.255.0 U 0 0 0 eth0
10.10.10.0 * 255.255.255.0 U 0 0 0 eth0
10.10.1.1 * 255.255.255.0 U 0 0 0 eth0
default 192.168.1.1 0.0.0.0 UG 0 0 0 eth0

Use
netstat -rn
to print the Kernel IP Routing table.

To keep the Static Route persistent or you want to add the route entries to the network script files (not using the route command) then all you need to do is to edit the file /etc/network/interfaces and the static routes in the following format:
up route add [-net|-host] <host/net>/<mask> gw <host/IP> dev <Interface>

Example:
up route add -net 172.20.11.0/16 gw 172.20.10.254 dev eth1

And the file will like the following:
sudo cat /etc/network/interfaces

The output should show something like this:
sudo cat /etc/network/interfaces

The output should show something like this:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
auto eth0 eth1
iface eth0 inet static
        address 192.168.1.2
        netmask 255.255.255.0
        network 192.168.1.0
        broadcast 192.168.1.255
        gateway 192.168.1.254
# dns-* options are implemented by the resolvconf package, if installed
iface eth1 inet static
        address 172.20.10.1
        netmask 255.255.255.0
        broadcast 172.20.10.255
        gateway 172.20.10.254
# static route
up route add -net 172.20.11.0/16 gw 172.20.10.254 dev eth1
```

The above has 2 Ethernet interfaces and the static route is added to the interface eth1.

For the change to /etc/network/interface to take effect. please restart the "networking" service as follows:
sudo /etc/init.d/networking restart

NOTE: If you added the route already using the "route" then there is no need to restart the networking service because, the next time server is restarted this takes effect.

==========
PROXMOX Clustering

Trebuie permis portul 22 pentru SSH
Si de asemenea este utilizata conectarea prin ssh pentru userul root

Ne logam prin SSH la cele 2 servere (noduri) - master si slave si rulam pe fiecare

in parte:
apt-get update
apt-get dist-upgrade
apt-get clean

sau altfel:

aptitude update
aptitude upgrade
apt-get clean

Pe serverul master trebuie sa deschid in firewall porturile 5404, 5405, 5406 si 5407, protocol udp:
IPTABLES -L -n --line-numbers
iptables -I INPUT 10 -p udp --dport 5404:5407 -j ACCEPT <<==== Aici am grija pe ce linie introduc regula
sh -c "iptables-save > /etc/iptables.rules"

Dupa care merg la serverul care va fi master si creez clusterul cu comanda:
pvecm create [Numele_clusterului]
de exemplu:
pvecm create cluster

dupa care pot verifica starea cu:
pvecm status

Apoi rulez pe serverul SLAVE, urmatoarea comanda:
pvecm add [IP-ul_Serverului_nod_Master]
De exemplu:
pvecm add 89.35.233.222
password: <<====== Imi va cere sa introduc parola de root a serverului Master

dupa care pot verifica starea cu:
pvecm status

==========
==========
SERVER DE WEB
Instalare:
sudo apt-get update
sudo apt-get upgrade
sudo apt-get clean
sudo apt-get install apache2

Verific daca ruleaza:
sudo service apache2 status
sau:

sudo /etc/init.d/apache2 status

Creez un fisier de configurare in care sa stochez numele serverului:
sudo nano /etc/apache2/conf.d/servername.conf

Editam in el, de exemplu:
ServerName InovaTopWebServer
Don't use the domain names of any of your sites for this value. We'll want to use those when we set up virtual hosts
later in this series.

Odata ce i-am spus serverului care ii este numele, il vom restarta cu greceful:
sudo /usr/sbin/apache2ctl graceful
In acest moment nu trebuie sa vedem nici un mesaj de eroare, altfel inseamna ca am gresit ceva in pasul anterior.

Utilizam apache2ctl sa restartam serverul.
Daca dau comanda de mai jos voi vedea optiunile apache2ctl:
/usr/sbin/apache2ctl
Va afisa:
Usage: /usr/sbin/apache2ctl
start|stop|restart|graceful|graceful-stop|configtest|status|fullstatus
       /usr/sbin/apache2ctl <apache2 args>

Argumente:
graceful|graceful-stop   <-- Tine cont de utilizatorii conectati
configtest <-- Verifica configuratia fisierelor
status|fullstatus

Logurile sunt pastrate in: /var/log/apache2/

Verific daca se vede pagina implicita:
http://xxx.xxx.xxx.xxx

In caz ca serverul nu e pornit, pot porni cu:
/usr/sbin/apache2ctl start

Daca nu, se verifica regulile din iptables:
sudo iptables -L -n --line-numbers

In cazul in care este blocat portul 80, atunci permit acest port adaugand o noua regula in iptables:
iptables -A INPUT -p tcp --dport 80 -i eth0 -j ACCEPT

Asemenea:
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Acum ar trebuie sa vizulizam pagina implicita.

Pornirea / oprirea / restartarea:

```
sudo service apache2 stop
sudo service apache2 start
sudo service apache2 restart
sudo /etc/init.d/apache2 stop
sudo /etc/init.d/apache2 start
sudo /etc/init.d/apache2 restart

sau

sudo apache2 reload

Fisierul principal de configurare este /etc/apache2/apache2.conf. El contine
directivele include, pentru specificarea
celorlalte fisiere de configurare specifice.

Site-urile se vor gasi in /var/www
La inceput se va afisa pagina implicita de la: /var/www/index.html

Se creaza un nou folder in care se va pune noul site, de exemplu folderul:
/var/www/inovatop.ro/

Pentru a preveni Apache sa porneasca la bootare:
sudo update-rc.d -f apache2 remove

Pentru a face ca Apache sa porneasca la bootare:
sudo update-rc.d apache2 defaults

Creem noua setare pentru vizualizarea noului site, cel aflat in
/var/www/inovatop.ro.
sudo cp /etc/apache2/sites-available/default
/etc/apache2/sites-available/inovatop.ro

Editam fisierul /etc/apache2/sites-available/inovatop.ro
sudo mcedit /etc/apache2/sites-available/inovatop.ro

si modificam urmatoarele:
Schimbam la
DocumentRoot /var/www
modificand in
DocumentRoot /var/www/inovatop.ro

Schimbam la
<Directory /var/www/>
modificand in
<Directory /var/www/inovatop.ro/>

Main pot adauga in partea de sus:
<VirtualHost *:80>
        ServerName inovatop.ro
        ServerAlias www.inovatop.ro
```

```
        ServerAdmin webmaster.inovatop.ro
...
```

La fel pot seta ca alte site-uri sa fie stocate si servite de la alte locatii, de exemplu:
/home/florin/public_html/inovatop.ro/

In fisierul /etc/hosts ar trebui sa am:

```
# 127.0.0.1             localhost.localdomain           localhost InovaTop226
inovatop.ro www.inovatop.ro
127.0.0.1               localhost.localdomain           localhost
86.107.58.226   InovaTop226.inovatop.ro         InovaTop226
```

Salvam si iesim din fisier, dupa care dezactivam pagina implicita si vom activa noul site, apoi restartam serverul:

```
sudo a2dissite default && sudo a2ensite inovatop.ro
sudo /etc/init.d/apache2 restart
```

Pentru a activa mod rewrite:

```
a2enmod rewrite
```

Dupa vechea metoda:
old style, you can skip this portion

now use locate to find if the mod_rewrite.so is availble on your server

```
updatedb
locate mod_rewrite.so
```

it will found in “/usr/lib/apache2/modules”

new apache follow some folders to enable and disable mods.
so now do this:

```
cd /etc/apache2/mods-enabled
touch rewrite.load
gedit rewrite.load (you may use any editor to edit this file)
```

now paste this following line

```
LoadModule rewrite_module /usr/lib/apache2/modules/mod_rewrite.so
```

end of old style

Activarea fisierului .htaccess:

.htaccess este un fisier puternic utilizat la controlul si configurarea unui server web, fara editarea modulului
core Apache. Implicit, functionarea .htaccess este oprita si toate instantele disierelor .htaccess sunt ignorate.
Pentru activarea fisierului .htaccess file, deschidem fisierul creat anterior:
sudo mcedit /etc/apache2/sites-available/inovatop.ro

si in sectiunea “<Directory /var/www/inovatop.ro/>“, schimbam AllowOverride None cu AllowOverride All.

Salvam, iesim din fisier si restartam serverul.

Instrument de generare a fisierului: .htaccess. You can just do a create a .htaccess file and add a redirect.
You can try this tool: http://www.htaccessredirect.net/. Once created, place the .htaccess in the inovatop.ro folder.
http://www.htaccessredirect.net/

Pentru a activa si dezactiva module utilizez:
sudo /usr/sbin/a2enmod userdir
sudo /usr/sbin/a2dismod status

Alte configurari:
In fisierul /etc/apache2/apache2.conf:

Timeout 300
pot sa-l schimb in Timeout 30 sau chiar mai putin, pentru a evita atacurile de top DoS.

KeepAlive On <-- E bine asa! In felul acesta se deschide doar o singura conexiune ptr toate elementele din pagina.

MaxKeepAliveRequests 100 <-- Pot sa modifica aici chiar si la mai mult de 500 ptr o cat mai buna performanta,
in cazul paginilor cu foarte multe imagini, elemente, JavaScript, etc.

KeepAliveTimeout 15 <-- Se poate reduce chiar la 2 sau 3. In felul acesta serverul devine mult mai Responsive.

HostnameLookups Off <-- E bine sa ramana Off

ServerName demo.example.com <-- Se poate adauga de exemplu in propriul fisier din directorul /etc/apache2/conf.d/

AccessFileName .htaccess   <-- Este fisierul ce se poate adauga in fiecare folder al site-ului in cazul in care utilizez
virtualhosts si doresc ca prin acest fisier sa suprascriu optiunile generale din fisierul general de configurare.

ErrorLog /var/log/apache2/error.log   <-- Indica fisierul unde vor fi scrise logurile de erori.

/etc/apache2/conf.d/security <-- Indica locatia unde sunt configurarle de securitate. Aici trebuie sa verific
cateva setari:

ServerTokens OS   <-- Indica cate informatii vor fi trimise de servere catre client. De exemplu OS va trimite:
Apache/2.2.14 (Ubuntu) Server
Full:
Apache/2.2.14 (Ubuntu) PHP/5.3.2-1ubuntu4.1 with Suhosin-Patch
Minimal
Apache/2.2.14 Server
Minor
Apache/2.2 Server
Major
Apache/2 Server
Prod
Apache Server

Prin urmare ar fi cel mai bine sa specific:
ServerTokens Prod   <-- Aceasta ofera hackerilor cat mai putine informatii.

ServerSignature On   <-- Ar fi bine s-o modific in Off. Aceasta nu va include in mesajul de footer al paginii de eroare
404 produsa cand cineva acceseaza o pagina care nu exista, informatii despre server. Trebuie avut grija ca aceste setari se pot suprascrie prin fisierele de configurare ale hosturilor virtuale, deci trebuie
sa am grija ca si acolo optiunea sa nu fie cu On.

Crearea hosturilor virtuale:
Pentru 2 domenii: domain1.com si domain2.com.

In folderul /home, creem un folder 'public_html':
cd ~
mkdir public_html

Pentru fiecare domeniu creem un folder cu un numar standard de subfoldere:
mkdir -p public_html/domain1.com/{public,private,log,cgi-bin,backup}
si:
mkdir -p public_html/domain2.com/{public,private,log,cgi-bin,backup}

Pentru fiecare domeniu creez un fisier index.html
nano public_html/domain1.com/public/index.html

si adaug in ele urmatorul continut:

```
<html>
  <head>
```

```
    <title>domain1.com</title>
  </head>
  <body>
    <h1>domain1.com</h1>
  </body>
</html>
```

La fel si pentru public_html/domain2.com/public/index.html

Setam permisiunile necesare procesului Apache pe aceste site-uri:
sudo chmod -R a+rX ~/public_html
sudo chmod a+rx ~

Daca adaugam mai multe domenii virtuale cu alte foledere, rulam prima comanda pentru ane asigura ca si acele foldere
vor putea fi citite si accesibile de catre toti userii din sistem.

NameVirtualHost:
Pentru fiecare interfata si port la care apache este configurat sa asculte, avem nevoie sa setam o directiva
NameVirtualHost. Putem defini doar una per port. Putem verifica asta si trebuie sa avem ceva de genul:

cat /etc/apache2/ports.conf

```
NameVirtualHost *:80
Listen 80
<IfModule mod_ssl.c>
    # If you add NameVirtualHost *:443 here, you will also have to change
    # the VirtualHost statement in /etc/apache2/sites-available/default-ssl
    # to <VirtualHost *:443>
    # Server Name Indication for SSL named virtual hosts is currently not
    # supported by MSIE on Windows XP.
    Listen 443
</IfModule>
<IfModule mod_gnutls.c>
    Listen 443
</IfModule>
```

Creem hosturile virtuale:
sudo nano /etc/apache2/sites-available/domain1.com

Ca si template general putem utiliza asta:

```
# Place any notes or comments you have here
# It will make any customization easier to understand in the weeks to come
# domain: domain1.com
# public: /home/demo/public_html/domain1.com/
<VirtualHost *:80>
  # Admin email, Server Name (domain name) and any aliases
```

```
  ServerAdmin webmaster@domain1.com
  ServerName  www.domain1.com
  ServerAlias domain1.com
  # Index file and Document Root (where the public files are located)
  DirectoryIndex index.html
  DocumentRoot /home/demo/public_html/domain1.com/public
  # Custom log file locations
  LogLevel warn
  ErrorLog  /home/demo/public_html/domain1.com/log/error.log
  CustomLog /home/demo/public_html/domain1.com/log/access.log combined
</VirtualHost>
```

Dupa care activez site-ul:

```
sudo /usr/sbin/a2ensite domain1.com
```

La iesire voi vedea:

```
Site domain1.com installed; run /etc/init.d/apache2 reload to enable.
```

Apoi dau:

```
sudo /etc/init.d/apache2 reload
```

Pentru a testa functionarea fara crearea zonelor de DNS avem nevoie sa modificam fisierul /etc/hosts, de genul:

```
127.0.0.1    localhost
...
# entries related to the demo slice
123.45.67.890   domain1.com
123.45.67.890   www.domain1.com
123.45.67.890   domain2.com
...
```

Aceste intrari trebuie sa le inlaturam dupa ce setam DNS-ul.

La fel repet pasii si pentru al 2-lea site:

```
sudo nano /etc/apache2/sites-available/domain2.com
...
sudo a2ensite domain2.com
...
sudo /etc/init.d/apache2 reload
http://domain2.com
or
http://www.domain2.com
```

Fisierele de LOG:

```
ls /home/demo/public_html/domain1.com/log/
Iesirea ar trebui sa dea:
access.log  error.log
```

Pastrand logurile pentru fiecare domeniu separat, ne va ajuta sa identificam mai usor problemele respectivului site.

Daca introduc acum http://xxx.xxx.xxx.xxx, pagina default va fi servita. Aceasta trebuie dezactivata.

Apache serveste raspunsul la cereri in ordine alfabetica. !!!

Alte configurari:

```
ServerAdmin webmaster@domain.com   <-- Va fi utilizata daca avem un server de
e-mail, pentru a trimite e-mail-uri
despre erori.

ServerName www.domain.com
ServerAlias domain.com   <-- Putem seta de exemplu aici ca si domain.com si
domain.net sa duca catre aceeasi pagina.

DirectoryIndex index.php index.html  <-- Atentie si la ordine. Serverul o va servi
pe prima gasita.

DocumentRoot /home/demo/public_html/domain.com/public
Exemplu:
Cand cineva acceseaza: http://www.example.com/main/sub/waffles.html
Serverul se va uita dupa fisier aici:
{the DocumentRoot for that virtual host}/main/sub/waffles.html

LogLevel warn
ErrorLog  /home/demo/public_html/domain.com/log/error.log   <-- Aici va inregistar
mesajele de eroare
CustomLog /home/demo/public_html/domain.com/log/access.log combined  <-- Aici orice
altceva

ErrorDocument 404 /errors/404.html
ErrorDocument 403 /errors/403.html

ServerSignature On  <-- Am mai discutat

ScriptAlias /cgi-bin/ /home/demo/public_html/domain.com/cgi-bin/
<Location /cgi-bin>
  Options +ExecCGI
</Location>
Activeaza locatia cgi-bin.

<Directory /home/demo/public_html/domain.com/public>
  Options FollowSymLinks
</Directory>
Activeaza optiunile pentru folderul specificat.

Options -Indexes   <-- Dezactiveaza (din cauza minusului) afisarea in browser a
```

continutului (indexului) folderului
in cazul in care un fisier nu este gasit. Pentru a-l activa utilizez +Indexes

Options -Includes <-- Dezactiveaza Server Site Includes. Daca nu stiu ce inseamna si ce face e mai bine sa o dezactivez.

Options -FollowSymLinks <-- Dezactiveaza optiunea de a urma legaturile symlinks. Trebuie sa fiu atent cu ea din motive
de securitate. Daca este link catre un fisier de sistem, acesta poate fi afisat in pagina. Mai bine se utilizeaza
SymLinksIfOwnerMatch care verifica daca ownerul fisierului este acelasi cu ownerul celui care cere fisierul.

AllowOverride None   <-- Activeaza .htaccess, care preia controlul configurarilor in afara fisierelor de configurare
generale ale Apache. Se poate specifica care optiuni sa fie activate in htaccess, astfel:
AllowOverride AuthConfig Indexes

Putem sa ascundem acest fisier numindu-l altfel, si sa-l protejam de la afisari nedorite:

```
AccessFileName .myobscurefilename
<Files ~ "^\.my">
    Order allow,deny
    Deny from all
    Satisfy All
</Files>
```

Options None   <-- Dezactiveaza toate optiunile inclusiv pe cele implicite

Directivele Options, pot fi setate per director astfel:

```
<Directory />
  AllowOverride None
  Options None
</Directory>

<Directory /home/demo/public_html/domain.com/public>
  AllowOverride All
</directory>
```

==========
Pornind de la fisierul default:
Configurare fisier: /etc/apache2/sites-available/inovatop.ro

```
# Place any notes or comments you have, here.
# It will make any customization easier to understand in the weeks to come
```

```
# Domain: inovatop.ro
# Public: /var/www/inovatop.ro/

<VirtualHost *:80>
        # Admin email, Server name (domain name) and any aliases.
        ServerAdmin sysadmin@inovatop.ro
        ServerName www.inovatop.ro
        ServerAlias inovatop.ro

        DocumentRoot /var/www/inovatop.ro
        DirectoryIndex index.php index.html index.htm

        RewriteEngine On

        RewriteCond %{HTTP_HOST} ^inovatop\.ro
        RewriteRule (.*) http://www.inovatop.ro [L]

        RewriteCond %{HTTP_HOST} !^www\.inovatop\.ro
        RewriteRule (.*) [L]

        RewriteCond %{HTTP_HOST} ^86.107.58.226$
        RewriteRule (.*) http://www.inovatop.ro [L]

        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>

        <Directory /var/www/inovatop.ro/>
                Options -Indexes FollowSymLinks -MultiViews
                # Activarea fisierului .htaccess (AllowOverride All, in loc de
AllowOverride None):
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
                AllowOverride None
                Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log

        # Possible values include: debug, info, notice, warn, error, crit, alert,
emerg.
        LogLevel warn
```

```
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        Alias /doc/ "/usr/share/doc/"
        <Directory "/usr/share/doc/">
                Options -Indexes -MultiViews FollowSymLinks
                AllowOverride None
                Order deny,allow
                Deny from all
                Allow from 127.0.0.0/255.0.0.0 ::1/128
        </Directory>

</VirtualHost>

-----------------------------------------------------------------
Pornind de la fisierul default, creez subdomeniu.
Configurare subdomeniu invtpmax - fisier: /etc/apache2/sites-available/invtpmax-80:

# SubDomain: invtpmax.inovatop.to
# Public: /usr/share/phpmyadmin

<VirtualHost *:80>

        ServerAdmin webmaster@inovatop.ro
        ServerName invtpmax.inovatop.ro

        DocumentRoot /usr/share/phpmyadmin
        DirectoryIndex index.php

        <Directory /usr/share/phpmyadmin/>
                Options Indexes FollowSymLinks MultiViews +Includes
                # Activarea fisierului .htaccess (AllowOverride All, in loc de
AllowOverride None):
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

</VirtualHost>

-----------------------------------------------------------------
Setare si securizare PhpMyAdmin:
(Conform:
http://paynedigital.com/2011/09/setting-up-and-securing-a-phpmyadmin-install-on-ubun
tu-10-04)

In folderul /etc/apache2/conf.d/, exista un fisier phpmyadmin.conf care este un
symlink la /etc/phpmyadmin/apache.conf.

Vom muta fisierul /etc/apache2/conf.d/phpmyadmin.conf, in folderul
```

```
/etc/apache2/sites-available/
mv /etc/apache2/conf.d/phpmyadmin.conf /etc/apache2/sites-available/

Dupa care il vom edita conform listingului de mai jos:

## ----------------- Virtual Host for PHPMyAdmin --------------------------
<VirtualHost *:443>
        ServerName invtpmax.inovatop.ro
        ServerAdmin sysadmin@inovatop.ro

        DocumentRoot /usr/share/phpmyadmin

        RewriteEngine On
        RewriteCond %{HTTP_HOST} !invtpmax.inovatop.ro
        RewriteRule (.*) [L]

        <Directory /usr/share/phpmyadmin/>
                Options +FollowSymLinks -Indexes
                DirectoryIndex index.php
                AllowOverride None
                Order Deny,Allow
                Deny from ALL
                Allow from 89.35.233.244        # TQM LAN
                Allow from 86.125.50.152        # SER LAN
                # Allow from 89.35.233.245      # Sala INFO

                <IfModule mod_php5.c>
                        AddType application/x-httpd-php .php
                        php_flag magic_quotes_gpc Off
                        php_flag track_vars On
                        php_flag register_globals Off
                        php_value include_path .
                </IfModule>
        </Directory>

        # Authorize for setup
        <Directory /usr/share/phpmyadmin/setup>
            <IfModule mod_authn_file.c>
                AuthType Basic
                AuthName "phpMyAdmin Setup"
                AuthUserFile /etc/phpmyadmin/htpasswd.setup
            </IfModule>
            Require valid-user
        </Directory>

        # Disallow web access to directories that don't need it
        <Directory /usr/share/phpmyadmin/libraries>
            Order Deny,Allow
            Deny from All
        </Directory>
```

```
        <Directory /usr/share/phpmyadmin/setup/lib>
            Order Deny,Allow
            Deny from All
        </Directory>

        # SSL Engine Switch: Enable/Disable SSL for this virtual host.
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/webcert.crt
        SSLCertificateKeyFile /etc/apache2/ssl/webcert.key

        ErrorLog ${APACHE_LOG_DIR}/error.log
        # Possible values include: debug, info, notice, warn, error, crit, alert,
emerg.
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined
</VirtualHost>

##-------------- END FILE -------------------------------
```

Certificatele sunt generate conform metodei prezentate la phpmyadmin.

Dupa care, activam domeniul virtual:
a2ensite phpmyadmin.conf

si restartam apache:
service apache2 restart

Atunci cand creez mai multe Hosturi Virtuale ca subdomenii, la restartarea Apache imi apare o eroare:
[warn] _default_ VirtualHost overlap on port 443, the first has precedence
Pentru a dezactiva acest lucru introduc urmatoarea linie in /etc/apache2/apache2.conf
NameVirtualHost *:443

Dupa care putem testa functionarea subdomeniului.

Daca am facut precum mai sus, trebuie sa am grija ca phpmyadmin isi instaleaza un symlink sub forma fisierului:
/etc/apache2/conf.d/phpmyadmin.conf
Trebuie sa mut acest fisier de aici, de exemplu:
cp /etc/apache2/conf.d/phpmyadmin.conf /etc/apache2/sites-available/altele/
Dupa care il sterg din /etc/apache2/conf.d/

O alta varianta pentru PHPMyAdmin (in final am renuntat la ea in favoarea celei anterioare, care este si oficiala):
Pornind de la fisierul default-ssl, creez subdomeniu.
Configurare subdomeniu invtpmax - fisier: /etc/apache2/sites-available/invtpmax-ssl:

```
<IfModule mod_ssl.c>
<VirtualHost invtpmax.inovatop.ro:443>
        ServerAdmin webmaster@inovatop.ro
        ServerName invtpmax.inovatop.ro:443
        ServerAlias invtpmax.inovatop.ro:443
        DocumentRoot /usr/share/phpmyadmin
        DirectoryIndex index.php
        <Directory /usr/share/phpmyadmin/>
                Options -Indexes +FollowSymLinks MultiViews
                AllowOverride None
                RewriteBase /phpmyadmin/
                Order allow,deny
                allow from all
        </Directory>
        RewriteEngine on
        RewriteCond %{HTTP_HOST} !^invtpmax\.inovatop\.ro$ [NC]
        RewriteRule ^(.*)$ http://www.inovatop.ro [R=301,L]
        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
                AllowOverride None
                Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>
        ErrorLog ${APACHE_LOG_DIR}/error.log
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined
        Alias /doc/ "/usr/share/doc/"
        <Directory "/usr/share/doc/">
                Options Indexes MultiViews FollowSymLinks
                AllowOverride None
                Order deny,allow
                Deny from all
                Allow from 127.0.0.0/255.0.0.0 ::1/128
        </Directory>
        SSLEngine on
        SSLCertificateFile    /etc/apache2/ssl/apachepma.crt
        SSLCertificateKeyFile /etc/apache2/ssl/apachepma.key
        <FilesMatch "\.(cgi|shtml|phtml|php)$">
                SSLOptions +StdEnvVars
        </FilesMatch>
        <Directory /usr/lib/cgi-bin>
                SSLOptions +StdEnvVars
        </Directory>
        BrowserMatch "MSIE [2-6]" \
                nokeepalive ssl-unclean-shutdown \
                downgrade-1.0 force-response-1.0
        # MSIE 7 and newer should be able to use keepalive
        BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
</VirtualHost>
```

```
</IfModule>
<IfModule !mod_rewrite.c>
        ErrorDocument 404 /index.php
</IfModule>

================================================================================
=======================================

Reguli rewrite folosite in fisiere .htaccess:

<IfModule mod_rewrite.c>
    Options +FollowSymLinks
    Options -Indexes
    RewriteEngine On

        RewriteBase /phpmyadmin/
        RewriteCond %{HTTP_HOST} !^invtpmax\.inovatop\.ro$ [NC]
        RewriteRule ^(.*)$ http://www.inovatop.ro [R=301,L]

        # RewriteCond %{HTTP_HOST} ^inovatop\.ro
        # RewriteRule ^(.*)$ http://www.inovatop.ro/$1 [L,R=301]

        # RewriteCond %{REQUEST_METHOD} !=POST  # if it's not POST
        # RewriteCond %{HTTP_HOST} ^domain\.com
        # RewriteRule ^(.*)$ http://www.domain.com/$1 [L,R=301]

        # redirect all www (http or https) to https://domain.com
        # RewriteCond %{HTTP_HOST} ^www.domain.com [nc]
        # RewriteRule (.*) https://domain.com:80/$1 [R=301,L]

        # redirect http://domain.com to https://domain.com
        # RewriteCond %{HTTP_HOST} ^domain.com [nc]
        # RewriteCond %{HTTPS} !=on
        # RewriteRule (.*) https://domain.com:80/$1 [R=301,L]

        # redirect all sub domain (http or https) to https://domain.com
        # RewriteCond %{HTTP_HOST} ^([a-z0-9\-]+)\.domain\.com$  [NC]
        # RewriteCond %1 !^www$ [NC]
        # RewriteRule (.*) https://domain.com:80/$1 [R=301,L]

        # RewriteCond %{HTTP_HOST} !www.yournewsdomain.com$ [NC]
        # RewriteCond %{HTTP_HOST} ^(www.)?([a-z0-9-]+).yournewsdomain.com [NC]
        # RewriteRule (.*) index.php?topic=%2 [NC,QSA]

        # RewriteCond %{HTTPS} !^invtpmax\.inovatop\.ro$ [NC]

        # RewriteCond %{HTTP_HOST} ^(www.)?([a-z0-9-]+).iovatop.ro [NC]

        ### RewriteRule !^invtpmax\.inovatop\.ro$ http://www.inovatop.ro [R=301,L]
```

```
        # RedirectMatch 400 !^invtpmax\.inovatop\.ro$

        # RewriteCond %{HTTPS} !=on             # if it`s not HTTPS

        # RewriteCond %{REQUEST_FILENAME} !-f
        # RewriteCond %{REQUEST_FILENAME} !-d
        # RewriteRule ^(.*)$ index.php/$1

        # RewriteCond %{HTTPS} off
        # RewriteCond %{REQUEST_URI} (auth|register|secure|payment)
        # RewriteRule ^(.*)$ https://%{SERVER_NAME}%{REQUEST_URI} [R=301,L]

        # RewriteCond %{HTTPS} on
        # RewriteCond %{REQUEST_FILENAME} !-f
        # RewriteCond %{REQUEST_FILENAME} !-d
        # RewriteCond %{REQUEST_URI} !(static|auth|register|secure|payment)
        # RewriteRule ^(.*)$ http://%{SERVER_NAME}%{REQUEST_URI} [R=301,L]

        # If https off and in the cart dir
        # RewriteCond %{HTTPS} =off [NC]
        # RewriteCond %{REQUEST_URI} ^/cart/(.*) [NC]
        # RewriteRule ^(.*)$ https://%{HTTP_HOST}/cart/%1 [R=301,L]

        # If https on and not in cart dir
        # RewriteCond %{HTTPS} =on
        # RewriteCond %{REQUEST_URI} !^/cart [NC]
        # Above line actually used to read RewriteCond %{REQUEST_URI}
!^/cart|media|images|thumbs|css|js [NC]
        # to allow js/css/images to be served so there were no mixed ssl messages
popping up to visitors
        # RewriteCond %{REQUEST_FILENAME} !index\.php$ [NC]
        # RewriteRule ^(.*)$ http://%{HTTP_HOST}/$1 [R=301,L]

        # RewriteCond %{REQUEST_FILENAME} !-d
        # RewriteCond %{REQUEST_FILENAME} !-f
        # RewriteRule ^(.*)$ index.php?url=$1 [QSA,L]

        # RewriteCond %{HTTPS} off
        # RewriteCond %{REQUEST_URI} (evaluate/purchase*)
        # RewriteRule (.*) https://mydomain.com%{REQUEST_URI}

        # RewriteCond %{HTTPS} off
        # RewriteCond %{REQUEST_URI} (another_dir/file.php)
        # RewriteRule (.*) https://mydomain.com%{REQUEST_URI}

        # RewriteCond %{HTTPS} off
        # RewriteCond %{REQUEST_URI} (please_secure_me.php)
        # RewriteRule (.*) https://mydomain.com%{REQUEST_URI}

        # RewriteCond %{HTTPS} off
```

```
        # RewriteCond %{REQUEST_URI} (evaluate/purchase*) [OR]
        # RewriteCond %{REQUEST_URI} (another_dir/file.php) [OR]
        # RewriteCond %{REQUEST_URI} (please_secure_me.php)
        # RewriteRule (.*) https://mydomain.com%{REQUEST_URI}

        # RewriteEngine On
        # RewriteCond %{SERVER_PORT} 80
        # RewriteRule ^(.*)$ https://www.example.com/$1 [R,L]

        # RewriteEngine On
        # RewriteCond %{SERVER_PORT} 80
        # RewriteCond %{REQUEST_URI} somefolder
        # RewriteRule ^(.*)$ https://www.domain.com/somefolder/$1 [R,L]

        # RewriteEngine On
        # Send everyone in these dirs and pages to https
        # RewriteCond %{HTTP_HOST} ^www\.somewebsite\.com$ [NC]
        # RewriteCond %{REQUEST_URI} clubs [OR,NC]
        # RewriteCond %{REQUEST_URI} dealer/ [OR,NC]
        # RewriteCond %{REQUEST_URI} login.html [OR,NC]
        # RewriteCond %{REQUEST_URI} dealer_registration.html [OR,NC]
        # RewriteCond %{REQUEST_URI} club_registration.html [OR,NC]
        # RewriteCond %{REQUEST_URI} contact.html [OR,NC]
        # RewriteCond %{REQUEST_URI} dealer_club_contact.html [OR,NC]
        # RewriteCond %{REQUEST_URI} members [OR,NC]
        # RewriteCond %{REQUEST_URI} secure/ [NC]
        # RewriteCond %{SERVER_PORT} 80
        # RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [R,L,QSA]

</IfModule>

<IfModule !mod_rewrite.c>
        ErrorDocument 404 /index.php
</IfModule>
================================================================================
======================================
```

LOGROTATE:
Sistemul ruleaza logrotate odata pe zi, luand decizii de a arhiva logurile, a crea un nou fisier de loguri si a le sterge
pe cele vechi.

Sistemul ruleaza logrotate pe baza unei agende configurata in:
/etc/cron.daily/logrotate
Daca am vrea sa-l rulam in fiecare ora atunci ar trebui sa avem un fisier de script in /etc/cron.hourly.

Principalul fisier de configurare este /etc/logrotate.conf

include /etc/logrotate.d   <-- Aici gasim aplicatiile setate sa utilizeze

logrotate

Daca vrem sa vizualizam care sunt acestea:
ls /etc/logrotate.d

Exemplu pentru apache2:

```
/var/log/apache2/*.log {
    weekly
    missingok
    rotate 52
    compress
    delaycompress
    notifempty
    create 640 root adm
    sharedscripts
    postrotate
        if [ -f "`. /etc/apache2/envvars ; echo
${APACHE_PID_FILE:-/var/run/apache2.pid}`" ]; then
            /etc/init.d/apache2 reload > /dev/null
        fi
    endscript
}
```

rotate 4 <-- Spune ca trebuie sa se pastreze 4 arhive inainte ca cea mai veche sa fie stearsa.

daily
weekly
monthly
yearly
Specifica cat de des sa se faca rotatia unui log

size 100k
size 100M
size 100G
Specifica daca logrotarea sa se faca in functie de dimensiunea fisierului.

compress   <-- Specifica comprimarea fisierului (in format gzip)

nocompress
sau
delaycompress

```
postrotate
    /usr/sbin/apache2ctl restart > /dev/null
endscript
```

sharedscripts

==========
Serverul MySQL

Pentru instalare MySQL:
```
sudo apt-get update
sudo ap-get upgrade
sudo apt-get install mysql-server
```

In Ubuntu 12.04, MySQL 5.5 este instalat implicit. In timpul procesului de instalare, va trebui sa setez o parola de root.

Dupa instalarea serverului, acesta va porni automat. Pentru a verifica daca serverul ruleaza, introduc:
```
sudo netstat -tap | grep mysql
```

Daca totul este OK, ar trebui sa apara o linie similara cu aceasta:
```
tcp 0 0 localhost:mysql *:* LISTEN 2556/mysqld
```

Daca serverul nu ruleaza corect, pot sa-l pornesc cu:
```
sudo service mysql restart
```

Configurare:
Va trebui sa configuram fisierul: /etc/mysql/my.cnf

Daca nu stiu unde este fisierul de configurare, pot sa-l gasesc astfel:
```
/usr/sbin/mysqld --help --verbose
```
sau:
```
/usr/sbin/mysqld --help --verbose | less
```
se va afisa o gramada de text, dar cautam ceva de genul (pe la inceput):
Default options are read from the following files in the given order:
/etc/my.cnf /etc/mysql/my.cnf /usr/etc/my.cnf ~/.my.cnf

De exemplu, pentru ca MySQL sa asculte la conexiuni de la reteaua hosturilor schimbam adresa bindaddress:
```
bind-address = 192.168.0.5
```

Daca setez ca serverul mysql sa fie accesat de pe calculatoare din retea (nu e cazul serverului nostru), atunci trebuie
sa setez iptables sa permita aceasta conexiune:
```
-I INPUT -p tcp --dport 3306 -m state --state NEW,ESTABLISHED -j ACCEPT
-I OUTPUT -p tcp --sport 3306 -m state --state ESTABLISHED -j ACCEPT
```
sau:
```
iptables -I INPUT -p tcp --dport 3306 -m state --state -j ACCEPT
```

Dupa ce rezolvam cu configurarile, restartam serverul:
```
sudo service mysql restart
```

Pentru a face ca mysql sa porneasca automat la bootare (ceea ce nu e cazul nostru, deoarece aceasta este setata

implicit la instalare), dar pentru orice situatie:
sudo /usr/sbin/update-rc.d mysql defaults

mysql shell-ul:
/usr/bin/mysql -u root -p
mysql>

Daca dorim sa schimbam parola de root:
sudo dpkg-reconfigure mysql-server-5.5

Daca vrem sa schimbam parola de root, putem aplica si asta:
UPDATE mysql.user SET Password = PASSWORD('password') WHERE User = 'root';
Dupa care:
FLUSH PRIVILEGES;

Daca vreau sa vad userii setati pe server:
SELECT User, Host, Password FROM mysql.user;

User	Host	Password
root	localhost	*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19
root	demohost	*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19
root	127.0.0.1	*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19
debian-sys-maint	localhost	*03C2F472E5290DDE27E889681C90EA91FD6800F3
	%	

Coloana host arata calculatorul de la care se poate conecta respectivul user.
Trebuie sa am grija sa securizez serverul.
Pentru asta nu trebuie sa am useri anonimi care sa se poata conecta fara parola de oriunde (Host = %).

Pentru a sterge o inregistrare:
delete from mysql.user where host='%';
sau
delete from mysql.user where User='';

Crearea unei baze de date:
CREATE DATABASE demodb;

Vizualizarea bazelor de date:
SHOW DATABASES;

Database
information_schema
demodb
mysql

3 rows in set (0.00 sec)

Adaugarea unui user:

```
INSERT INTO mysql.user (User,Host,Password)
VALUES('demouser','localhost',PASSWORD('demopassword'));
FLUSH PRIVILEGES;
SELECT User, Host, Password FROM mysql.user;
+------------------+-----------+-------------------------------------------+
| User             | Host      | Password                                  |
+------------------+-----------+-------------------------------------------+
| root             | localhost | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
| root             | demohost  | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
| root             | 127.0.0.1 | *2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 |
| debian-sys-maint | localhost | *03C2F472E5290DDE27E889681C90EA91FD6800F3 |
<--- Acest user nu trebuie sters !!!
| demouser         | localhost | *0756A562377EDF6ED3AC45A00B356AAE6D3C6BB6 |
+------------------+-----------+-------------------------------------------+
```

Acordarea privilegiilor:

```
GRANT ALL PRIVILEGES ON demodb.* to demouser@localhost;
FLUSH PRIVILEGES;
```

Vizualizarea depturilor:

```
SHOW GRANTS FOR 'demouser'@'localhost';
+-------------------------------------------------------------------------------
------------------------------+
| Grants for demouser@localhost
                              |
+-------------------------------------------------------------------------------
------------------------------+
| GRANT USAGE ON *.* TO 'demouser'@'localhost' IDENTIFIED BY PASSWORD
'*0756A562377EDF6ED3AC45A00B356AAE6D3C6BB6' |
| GRANT ALL PRIVILEGES ON `demodb`.* TO 'demouser'@'localhost'
                              |
+-------------------------------------------------------------------------------
------------------------------+
2 rows in set (0.00 sec)
```

MySQL creaza implicit un folder pentru fiecare baza de date, in cadrul folderului:
/var/lib/mysql

Daca vrem sa copiem o baza de date, s-ar putea ca in acel moment serverul sa scrie date in acea baza de date, ceea ce va
face ca datele sa fie corupte. Pentru a face o copie curata a bazei de date, ar trebui sa oprim serverul mai intai. Aceasta
va salva, dar nu e cea mai buna metoda.

O alta metoda este sa blocam baza de date ca read-only pe perioada copierii. Dupa ce copierea s-a facut, se va debloca
baza de date. Fiind read-only, serverul poate pe perioada copierii sa citeasca date.

Blocarea bazei de date se face cu:

```
mysql -u root -p -e "FLUSH TABLES WITH READ LOCK;"
```

Deblocarea bazei de date se face cu:

```
mysql -u root -p -e "UNLOCK TABLES;"
```

Daca s-ar pune aceste comenzi intr-un script se poate introduce si parola:

```
mysql -u root -p"password" -e "FLUSH TABLES WITH READ LOCK;"
mysql -u root -p"password" -e "UNLOCK TABLES;"
```

O alta abordare se poate face folosind instrumentul mysqldump. Acesta genereaza un fisier text care reprezinta baza de date.
Textul contine instructiuni SQL care recreaza baza de date. In plus se poate exporta baza de date si in alte formate precum
CSV sau XML. De exemplu:

```
mysqldump -u root -p demodb > dbbackup.sql
```

Pentru a restaura o baza de date folosind mysqldump:

```
mysql -u root -p demodb < dbbackup.sql
```

De mentionat ca trebuie sa avem o baza de date noua in care se vor restaura tabelele vechi.

Exista 2 modalitati de stocare in functie de motorul utilizat: InnoDB si MyISAM (modalitatea mai veche). Modalitatea de
stocare este transparenta pentru utilizator.

- MyISAM: mai veche, si uneori mai rapida. Suporta Fulltext, care permite cautari rapide in mari cantitati de text.
Blocarea pentru scriere se face la nivel de tabel. Doar un singur proces poate lucra cu un tabel la un moment dat. In plus, nu asigura jurnalizare, ceea ce face aproape imposibila recupararea datelor.
- InnoDB: mai moderna, ACID compatibila, ceea ce permite realizarea tranzactiilor de date. Blocarea la scriere se face la nivel
de rand, ceea ce permite ca multiple procese sa poata faca simultan actualizari in tabel. Cache-ul de memorie este
manuit in cadrul memoriei. Prin jurnalizare, restaurarea datelor se face mult mai usor.

Pentru MySQL 5.5, InnoDB este engine-ul implicit folosit.

Pentru a vedea ce motor este folosit pentru o baza de date:

```
SHOW TABLE STATUS FROM demodb;
```

Cateva setari pentru a porni cu InnoDB pe un server cu 256 Mb de RAM sunt:

```
innodb_buffer_pool_size = 32M
innodb_log_file_size = 8M
innodb_thread_concurrency = 8
innodb_file_per_table
```

MySQL Tuner - Este un instrument prin care putem imbunatati activitatea / setarile

serverului MySQL:
sudo apt-get install mysqltuner

Odata instalat, pot sa-l rulez:
mysqltuner

La pornire ne va cere sa introducem userul si parola cu drepturi de administrare pe server (root sau cum i-am zis si parola acestui user).
si va prezenta un raport de rezultate si recomandari. Pentru ca acestea sa fie relevante, e bine sa-l rulam dupa cel
putin 24 de ore de la pornire. Rezultatele si recomandarile pot fi folosite la modificari de configurare in /etc/mysql/my.cnf.
Pentru instalari diferite /servere diferite, my.cnf poate fi setat diferit.

In Ubuntu 16.04 am mysql 5.7
In mysql 5.7 in mysql.user, coloana password a devenit authentication_string
Prin urmare, trebuie sa adaptez mysql tuner la ultima varianta si ultimele modificari.
Pentru asta inlocuiesc codul din fisierul /usr/bin/mysqltuner cu cel de la pagina:
https://github.com/major/MySQLTuner-perl
adica:
https://raw.githubusercontent.com/major/MySQLTuner-perl/master/mysqltuner.pl
respectiv fisierul:
mysqltuner.pl

Alta metoda de a seta parola de root:
mysql -u root -p
La consola mysql:
mysql> SET PASSWORD FOR 'root'@'localhost' = PASSWORD('yourpassword');
Daca e ok, vom vedea:
Query OK, 0 rows affected (0.00 sec)
mysql -u root -p

Crearea unui user:
mysql> GRANT ALL PRIVILEGES ON *.* TO 'yourusername'@'localhost' IDENTIFIED BY 'yourpassword' WITH GRANT OPTION;
sau acordand doar unele privilegii:
mysql> GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX, ALTER, CREATE TEMPORARY TABLES, LOCK TABLES ON
database1.* TO 'yourusername'@'localhost' IDENTIFIED BY 'yourpassword';

Comenzi mysql:
CREATE DATABASE databasename;
SHOW DATABASES;
DROP DATABASE databasename;
USE databasename;
INSERT INTO mysql.user (Host,User,Password)

```
VALUES('localhost','demouser',PASSWORD('demopassword'));
SET PASSWORD FOR 'username'@'localhost' = PASSWORD('password');
FLUSH PRIVILEGES;
GRANT ALL PRIVILEGES ON databasename.* TO username@localhost;
FLUSH PRIVILEGES;
SELECT User, Host, Password FROM mysql.user;
DROP USER 'username'@'localhost';
FLUSH PRIVILEGES;
SHOW TABLES FROM databasename;
SELECT COUNT(*) FROM databasename.tablename;
SELECT * FROM databasename.tablename;
REPAIR TABLE databasename.tablename;   <-- Doar pentru MyISAM engine
OPTIMIZE TABLE databasename.tablename;
DROP TABLE databasename.tablename;
mysqladmin -u root password 'My-Secret-Password'

Pentru resetarea parolei de root, mai intai opresc serverul. Apoi:
mysqld_safe --skip-grant-tables &   <-- Reseteaza parola de root
Apoi:
mysql -u root
Apoi setam o noua parola:
UPDATE mysql.user SET password=PASSWORD("password") WHERE User='root';
FLUSH PRIVILEGES;

Redenumire user root:
update mysql.user set user = 'the_secret_user' where user = 'root';
flush privileges;

Exista o baza de date numita test, care de regula nu este folosita. O pot sterge:
DROP database test;
================================================================================
======================================
Instalare PHP
Se instaleaza doar dupa instalarea si configurarea Apache si MySQL.

Pot sa verific ce instalari exista:
dpkg --list|grep -e httpd -e apache -e mysql -e php

sudo apt-get update
sudo apt-get upgrade
sudo apt-get install php5 libapache2-mod-php5

Pentru rularea de scripturi PHP in linie de comanda, se poate instala pachetul:
sudo apt-get install php5-cli

Pentru rularea de scripturi CGI se poate instala:
sudo apt-get install php5-cgi

Pentru rularea mysql impreuna cu PHP, se instaleaza pachetul:
sudo apt-get install php5-mysql
```

Pentru rularea postgresql impreuna cu PHP, se instaleaza pachetul:
sudo apt-get install php5-pgsql

Alte module:
sudo apt-get install php5-common php5-curl php5-gd

Pentru cresterea vitezei:
apt-get install php5-xcache

Configurari:
PHP5 odata instalat, el implicit poate rula scripturi. Daca avem cli package instalat, atunci putem sa le rulam in
linie de comanda.

Implicit Apache2 este setat sa ruleze scripturi PHP. Adica, modulul PHP este activat in Apache.
Putem sa verificam daca fisierele /etc/apache2/mods-enabled/php5.conf si /etc/apache2/mods-enabled/php5.load exista.
Daca nu exista, le adaugam folosind comanda a2enmod, dupa care restartam serverul:
sudo a2enmod php5
sudo service apache2 restart

Testare:

Creem un fisier php si il asezam in /var/www/myste.com/, dupa care vizualzam pagina in browser.
```
<?php
phpinfo();
?>
```

Putem afla care module php5 sunt disponibile, astfel:
aptitude search php5

Fisierul de configurare pentru PHP5 este: /etc/php5/apache2/php.ini

Configurari in fisier:

short_open_tag = Off
Short open tags arata astfel: <? ?>. Trebuie setat Off daca utilizam functii XML.

safe_mode = Off
Daca este setat On, probabil a fost compilat PHP cu flagul --enable-safe-mode flag. Safe mode este relevant cand
utilizam CGI.

safe_mode_exec_dir = [DIR]
Optiunea este relevanta doac cand safe mode este on; Aceasta nu are nimic de a face cu servirea paginilor PHP/HTML.

error_reporting = E_ALL & ~E_NOTICE
Valoarea implicita este E_ALL & ~E_NOTICE, insemnand toate erorile cu exceptia notificarilor.

file_uploads = [on/off]
Se seteaza On, daca dorim sa uploadam fisiere utilizand scripturi PHP

upload_tmp_dir = [DIR]
Nu decomentati acesasta linie decat daca intelegeti semnificatia si implicatiile HTTP uploads!

session.save-handler = files
Exceptand rare circumstante, nu aveti nevoie sa schimbati aceasta setare, asa ca n-o modificati!

ignore_user_abort = [On/Off]
Setarea controleaza ce se intampla cand utilizatorul face clik pe butonul Stop al browserului. Implicit este On, care inseamna
ca scriptul va rula pana la completarea timpului. Daca e Off, scriptul va fi abandonat. Setarea ruleaza daca suntem in modul
module, nu CGI.

mysql.default_host = hostname
Serverul implicit utilizat cand ne conectam la serverul de baze de date, daca nu este specificat nici un alt host.

mysql.default_user = username
Numele de user implicit cand ne conectam la serverul de baze de date, daca nici un alt nume nu este specificat.

mysql.default_password = password
Parola implicita cand ne conectam la serverul de baze de date daca nici o alta parola este specificata.

Cresterea Limitei de upload fisier la 64Mb:
upload_max_filesize = 64M
post_max_size = 64M
max_execution_time = 500
max_input_time = 500

date.timezone = "Europe/Bucharest"

Pentru inregistrarea logurilor:
log_errors = 1
error_log = /home/USERNAME/php.log

Transmiterea de e-mail-uri:
SMTP = mail.inovatop.ro
smtp_port = 25
sendmail_from = office@inovatop.ro

sendmail_path = /usr/sbin/sendmail
==
=====================================
SERVER FTP - PUREFTP - Instalare cu MySQL si PHPMyAdmin

Se va instala PureFTPd server care utilizeaza virtual users dintr-o baza de date MySQL in loc de useri de sistem.
Aceasta implementare este mult mai performanta putandu-se seta sute sau chiar mii de utilizatori ftp pe o singura masina.
In plus va putea fi vizibila / controlata largimea de banda pentru upload / download. Parolele vor fi setate criptat MD5 in
cadrul bazei de date. Instalarea s-a facut pentru Ubuntu 12.04 LTS. Pentru administrarea bazei de date MySQL se poate
utiliza un instrument precum phpMyAdmin care, de asemenea, va fi instalat.

Deoarece vom rula mai toate comenzile ca root, ne logam ca root:
sudo su

Instalam MySQL si phpMyAdmin:
apt-get install mysql-server mysql-client phpmyadmin apache2
in cazul meu deja am instalat mysql-server si apache2, prin urmare voi instala doar phpmyadmin:
apt-get install phpmyadmin

Voi fi intrebat 2 intrebari la care voi raspunde conform mai jos:
Web server to reconfigure automatically: <-- apache2
Configure database for phpmyadmin with dbconfig-common? <-- No

Mai jos am sectiune separata referitoare la configurarea phpMyAdmin ca si subdomeniu al domeniului, precum si cu
autentificare SSL.

Instalam PureFTPd cu suport pentru MySQL. Pentru Ubuntu 12.04 exista disponibil un pachet pre-configurat pure-ftpd-mysql.
Il instalam:
apt-get install pure-ftpd-mysql

Dupa instalare, verific daca ruleaza:
service pure-ftpd-mysql status

Apoi vom crea un grup ftp (ftpgroup) si un user (ftpuser) la care vor fi mapati toti userii virtuali pentru ftp. Inlocuiti
grupul si user-ul 2001 cu un numar care este liber in sistemul nostru:
groupadd -g 2001 ftpgroup
useradd -u 2001 -s /bin/false -d /bin/null -c "pureftpd user" -g ftpgroup ftpuser
usermod -a -G www-data ftpuser

Creem baza de date pentru PureFTPd:

Vom crea o baza de date numita pureftpd si un user numit pureftpd pe care PureFTPd daemon il va utiliza mai tarziu
cand se va conecta la baza de date pureftpd:

```
mysql -u root -p
```

Inlocuiti mai jos sirul ftpdpass cu o parola pe care o va utiliza userul pureftpd.

```
CREATE DATABASE pureftpd;
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP ON pureftpd.* TO
'pureftpd'@'localhost' IDENTIFIED BY 'ftpdpass';
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP ON pureftpd.* TO
'pureftpd'@'localhost.localdomain' IDENTIFIED BY 'ftpdpass';
```

sau:

```
GRANT ALL ON pureftpd.* TO 'pureftpd'@'localhost' IDENTIFIED BY 'ftpdpass';

FLUSH PRIVILEGES;
```

Verific:

```
SELECT User, Host, Password FROM mysql.user;
```

Selectez baza de date:

```
USE pureftpd;
```

Va exista un singur tabel. Creez tabelul:

```
CREATE TABLE ftpd (
User varchar(16) NOT NULL default '',
status enum('0','1') NOT NULL default '0',
Password varchar(64) NOT NULL default '',
Uid varchar(11) NOT NULL default '-1',
Gid varchar(11) NOT NULL default '-1',
Dir varchar(128) NOT NULL default '',
ULBandwidth smallint(5) NOT NULL default '0',
DLBandwidth smallint(5) NOT NULL default '0',
comment tinytext NOT NULL,
ipaccess varchar(15) NOT NULL default '*',
QuotaSize smallint(5) NOT NULL default '0',
QuotaFiles int(11) NOT NULL default 0,
PRIMARY KEY (User),
UNIQUE KEY User (User)
) ENGINE=MyISAM;
```

Eu am modificat astfel:

```
CREATE TABLE ftpd (
User varchar(50) NOT NULL default '',
status enum('0','1') NOT NULL default '0',
Password varchar(64) NOT NULL default '',
```

```
Uid varchar(11) NOT NULL default '-1',
Gid varchar(11) NOT NULL default '-1',
Dir varchar(128) NOT NULL default '',
ULBandwidth int(11) NOT NULL default '0',
DLBandwidth int(11) NOT NULL default '0',
comment tinytext NOT NULL,
ipaccess varchar(15) NOT NULL default '*',
QuotaSize int(11) NOT NULL default '0',
QuotaFiles int(11) NOT NULL default 0,
PRIMARY KEY (User),
UNIQUE KEY User (User)
) ENGINE=MyISAM;
```

Dupa care ma deconectez de la server:

```
quit;
```

Configuram PureFTPd:

Editam /etc/pure-ftpd/db/mysql.conf. El trebuie sa arate precum:

```
cp /etc/pure-ftpd/db/mysql.conf /etc/pure-ftpd/db/mysql.conf_orig      <--- creez o
copie a fisierului original
cat /dev/null > /etc/pure-ftpd/db/mysql.conf            <--- il initializez fara
nimic in el
nano /etc/pure-ftpd/db/mysql.conf
```

Editez fisierul astfel:

```
MYSQLSocket      /var/run/mysqld/mysqld.sock
#MYSQLServer     localhost
#MYSQLPort       3306
MYSQLUser       pureftpd
MYSQLPassword   ftpdpass
MYSQLDatabase   pureftpd
#MYSQLCrypt md5, cleartext, crypt() or password() - md5 is VERY RECOMMENDABLE uppon
cleartext
MYSQLCrypt      md5
MYSQLGetPW      SELECT Password FROM ftpd WHERE User="\L" AND status="1" AND
(ipaccess = "*" OR ipaccess LIKE "\R")
MYSQLGetUID     SELECT Uid FROM ftpd WHERE User="\L" AND status="1" AND (ipaccess =
"*" OR ipaccess LIKE "\R")
MYSQLGetGID     SELECT Gid FROM ftpd WHERE User="\L" AND status="1" AND (ipaccess =
"*" OR ipaccess LIKE "\R")
MYSQLGetDir     SELECT Dir FROM ftpd WHERE User="\L" AND status="1" AND (ipaccess =
"*" OR ipaccess LIKE "\R")
MySQLGetBandwidthUL SELECT ULBandwidth FROM ftpd WHERE User="\L" AND status="1" AND
(ipaccess = "*" OR ipaccess LIKE "\R")
MySQLGetBandwidthDL SELECT DLBandwidth FROM ftpd WHERE User="\L" AND status="1" AND
(ipaccess = "*" OR ipaccess LIKE "\R")
MySQLGetQTASZ   SELECT QuotaSize FROM ftpd WHERE User="\L" AND status="1" AND
(ipaccess = "*" OR ipaccess LIKE "\R")
```

```
MySQLGetQTAFS   SELECT QuotaFiles FROM ftpd WHERE User="\L" AND status="1" AND
(ipaccess = "*" OR ipaccess LIKE "\R")
```

Apoi creez fisierul /etc/pure-ftpd/conf/ChrootEveryone care pur si simplu contine sirul yes:

```
echo "yes" > /etc/pure-ftpd/conf/ChrootEveryone
```

Asta va face ca PureFTPd sa chroot fiecare virtual user in propriul sau home folder astfel incat el sa nu poata sa
fie capabil sa navigheze prin directoare si foldere din afara directorului sau home.

Apoi creez fisierul /etc/pure-ftpd/conf/CreateHomeDir care pur si simplu contine sirul yes:

```
echo "yes" > /etc/pure-ftpd/conf/CreateHomeDir
```

Asta va face ca PureFTPd sa creeze un folder home cand utilizatorul se logheaza in directorul home, daca el nu exista.

In final creez fisierul /etc/pure-ftpd/conf/DontResolve care de asemenea va contine sirul yes:

```
echo "yes" > /etc/pure-ftpd/conf/DontResolve
```

Asta va face ca PureFTPd sa nu se uite dupa host names, ceea ce poate sa creasca semnificativ viteza conexiunii si sa
reduca banda utilizata.

Dupa toate acestea, restartam PureFTPd:

```
/etc/init.d/pure-ftpd-mysql restart
```

Populam si testam baza de date:

```
mysql -u root -p
USE pureftpd;
```

Vom crea userul exampleuser cu status 1 (care inseamna ca contul lui ftp este activ), parola secret (care va fi stocata
criptat utilizand functia MySQL MD5), UID-ul si GID-ul 2001 (utilizam userid si groupid a user/group pe care l-am creat
anterior), directorul gazda /home/www.example.com, o banda de upload si download de 100 KB/sec, si o cota de 50 MB:

```
INSERT INTO `ftpd` (`User`, `status`, `Password`, `Uid`, `Gid`, `Dir`,
`ULBandwidth`, `DLBandwidth`, `comment`, `ipaccess`, `QuotaSize`, `QuotaFiles`)
VALUES ('exampleuser', '1', MD5('secret'), '2001', '2001', '/home/www.example.com',
'100', '100', '', '*', '50', '0');
```

```
quit;
```

E bine ca pentru serverul de web folderul in care va sta site-ul (Ex: /var/www/inovatop.ro/) sa fie creat in urma conectarii
ftp, in felul acesta el fiind detinut in proprietate de catre ftp user si grup. Altfel, userul ftp nu va avea acces la

scriere pe acest folder.

Ar trebui sa adaug si regula iptables pentru FTP:
iptables -L -n --line-numbers
iptables -A INPUT -p tcp --dport 21 -j ACCEPT
iptables -A INPUT -p tcp --dport 20 -j ACCEPT

Acum deschid clientul FTP (FileZilla, WS_FTP, SmartFTP sau gFTP) si incerc sa ma conectez.
Ca si hostname utilizez server1.example.com (sau adresa IP a sistemului), numele de user si parola. Daca suntem capabili
sa ne conectam, e foarte bine! Altfel, ceva este gresit.

Setarea PassivePortRange in pure-ftpd:

Daca rulam un firewall si dorim utilizarea de conexiuni pasive FTP (care sunt implicite), trebuie sa definim o gama de
porturi in pure-ftpd si in firewall pentru ca, conexiumile ftp sa nu fie blocate:
echo "40110 40210" > /etc/pure-ftpd/conf/PassivePortRange
/etc/init.d/pure-ftpd-mysql restart

Configuram firewall-ul:
iptables -A INPUT -p tcp --dport 40110:40210 -j ACCEPT

Acum, daca rulam:
ls -l /home

ar trebui sa vedem ca directorul /home/www.example.com a fost creat automat si este detinut de ftpuser si ftpgroup
(user/group creat anterior):

```
root@server1:~# ls -l /home
total 8
drwxr-xr-x 3 administrator administrator 4096 Apr 27 11:54 administrator
drwxr-xr-x 2 ftpuser       ftpgroup      4096 Jul  3 22:23 www.example.com
root@server1:~#
```

Administrarea bazei de date:

Se poate face in clientul de MySQL sau folosind
http://server1.example.com/phpmyadmin/).

Tabelul ftpd - explicatii:

User: Numele userului virtual PureFTPd (e.g. exampleuser).
status: 0 or 1. 0 contul este dezactivat, userul neputand sa se logheze.
Password: Parola userului virtual. Fiti siguri ca utilizati functia MD5 a MySQL la salvarea parolei criptate.
UID: UserId-ul userului ftp pe care l-am creat (Ex: 2001).
GID: GroupId-ul grupului ftp creat anterior two (Ex: 2001).

Dir: Directorul gazda al userului virtual PureFTPd (Ex: /home/www.example.com). Daca acest director nu exista
el va fi creat cand noul user se va loga pentru prima data prin FTP. Userul virtual va fi jailed in interiorul
acestui director gazda, i.e., userul neputand accesa alte foldere din afara directorului sau gazda.
ULBandwidth: Largimea de banda de upload a userului virtual, masurata in KB/secunda. 0 inseamna nelimitat.
DLBandwidth: Largimea de banda de download a userului virtual, masurata in KB/secunda. 0 inseamna nelimitat.
comment: Aici se poate introduce orice comentariu (Ex: pentru administrare interna). In mod normal puteti lasa acest
camp gol.
ipaccess: Introduceti aici adresa IP de la care este permisa conectarea la acest cont FTP. * inseamna ca oricarei adrese
IP i se permite conectarea.
QuotaSize: Spatiul de stocare in MB pe care userul virtual il poate utiliza pe serverul FTP. 0 inseamna nelimitat.
QuotaFiles: Cantitatea / numarul de fisiere pe care userul virtual le poate salva pe serverul FTP. 0 inseamna nelimitat.

Dezactivam posibilitatea de conectare prin FTP a userilor din sistem (PAM / Unix): S-ar fi conectat prin FTP la folderul lor /home/...

Disable PAM authentication unless you need it:
```
echo no > /etc/pure-ftpd/conf/PAMAuthentication
```

Disable UNIX authentication unless you need it
```
echo no > /etc/pure-ftpd/conf/UnixAuthentication
```

FTP - userul anonim.

Daca doriti sa creati un cont ftp anonymous (un cont ftp prin care orice utilizator se poate conecta fara parola),
se va proceda astfel:

Creem userul ftp (cu folderul gazda /home/ftp, in cazul meu /var/ftp-anonim) si grup ftp:
```
groupadd ftp
useradd -s /bin/false -d /home/ftp -m -c "anonymous ftp" -g ftp ftp
```

Practic eu adaug asa:
```
useradd -s /bin/false -d /var/ftp-anonim -m -c "anonymous ftp" -g ftp ftp
```

Apoi creati fisierul /etc/pure-ftpd/conf/NoAnonymous care va contine urmatorul sir: no.
```
echo "no" > /etc/pure-ftpd/conf/NoAnonymous
```

Daca schimb cu yes, userul anonim este inactiv.

Cu aceasta configuratie, PureFTPd va permite logarea userului anonymous.

Restartam PureFTPd:
/etc/init.d/pure-ftpd-mysql restart

Ar trebui sa ma conectez acum cu userul anonymous pentru a se crea automat acel folder (/var/ftp-anonim)

Apoi creem folderul /home/ftp/incoming (in cazul meu /var/ftp-anonim/upload) care va permite userilor anonymous
sa uploadeze fisiere. Vom da folderului /home/ftp/incoming permisiuni 311 astfel incat acesti useri
sa poata uploada, dar nu vor vedea / nu vor putea sa downloadeze nici un fisier in / din acest folder.
Folderul /home/ftp va avea permisiuni 555 care permit vizualizarea si downloadarea de fisiere:
cd /home/ftp
mkdir incoming
chown ftp:nogroup incoming/
chmod 311 incoming/
cd ../
chmod 555 ftp/

Astfel userii anonymous se pot loga, si pot sa downloadeze fisiere din /home/ftp, dar uploadul este limitat la
/home/ftp/incoming (si odata ce un fisier este uploadat in /home/ftp/incoming, el nu poate fi citit nici downloadat
de aici; administratorul serverului va trebui sa mute fisierul in /home/ftp pentru a-l face disponibil celorlalti).

Userul anonim, creaza in cadrul folderului sau inca 3 sau 4 fisiere care nu sunt accesibile insa sunt vizibile de catre el
dupa logarea cu clientul. Le-am sters de acolo (si le-am mutat in folderul meu home) si e in continuare functional.

PureFTPd Logging

Pentru a porni verbose logging (Ex: Pentru depanarea conexiunilor FTP sau a problemelor de autentificare), executati
urmatoarele comenzi ca si user root:
echo 'yes' > /etc/pure-ftpd/conf/VerboseLog ====>> In Ubuntu 16.04 nu mai e nevoie ptr ca am AltLog (vezi mai jos)

Apoi restartati pure-ftpd:
/etc/init.d/pure-ftpd-mysql restart

Iesirea de debug va fi logata la syslog. Pentru vizualizarea continutului de log, executati:
tail -n 100 /var/log/syslog

Pentru a dezactiva verbose logging, executati:
rm -f /etc/pure-ftpd/conf/VerboseLog
/etc/init.d/pure-ftpd-mysql restart

Cum sa integram pe Ubuntu 12.04, ClamAV in PureFTPd pentru scanarea virusilor.

Fisierele care vor fi uploadate cu PureFTPd, vor fi verificate de ClamAV si sterse in cazul in care sunt malware.

Devenim root:
sudo su

Instalam ClamAV:
apt-get update
apt-get upgrade
apt-get install clamav clamav-daemon clamav-data

In Ubuntu 16.04:
apt-get install clamav clamav-freshclam clamav-daemon libclamunrar7

Pentru a downloada cea mai noua lista de samnaturi de virusi, rulam:
freshclam

Dupa care restartam daemonul ClamAV:
/etc/init.d/clamav-daemon start

sau:
systemctl enable clamav-daemon
systemctl restart clamav-daemon
freshclam

Daca totul este OK se va afisa ceva de genul:
* Starting ClamAV daemon clamd

Configuram PureFTPd pentru a lucra cu ClamAV. Mai intai vom crea un fisier /etc/pure-ftpd/conf/CallUploadScript care
va contine sirul yes:
echo "yes" > /etc/pure-ftpd/conf/CallUploadScript

Vom crea fisierul: /etc/pure-ftpd/clamav_check.sh (care va chema /usr/bin/clamdscan de fiecare data cand un fisier este
uploadat prin PureFTPd):
nano /etc/pure-ftpd/clamav_check.sh

In el introducem urmatorul continut:
#!/bin/sh
/usr/bin/clamdscan --remove --quiet --no-summary --fdpass "$1"

in unele instalari, in linia de mai sus lipseste: --fdpass

Il facem executabil:
chmod 755 /etc/pure-ftpd/clamav_check.sh

Acum editam fisierul: /etc/default/pure-ftpd-common
nano /etc/default/pure-ftpd-common

... si schimbam linia UPLOADSCRIPT, dupa cum urmeaza:

```
[...]
# UPLOADSCRIPT: if this is set and the daemon is run in standalone mode,
# pure-uploadscript will also be run to spawn the program given below
# for handling uploads. see /usr/share/doc/pure-ftpd/README.gz or
# pure-uploadscript(8)

# example: UPLOADSCRIPT=/usr/local/sbin/uploadhandler.pl
UPLOADSCRIPT=/etc/pure-ftpd/clamav_check.sh
[...]
```

In final, restartam PureFTPd:
/etc/init.d/pure-ftpd-mysql restart

Acum, de fiecare data cand cineva incearca sa uploadeze un malware pe serverul nostru prin PureFTPd, fisierul "rau"
va fi sters in liniste.

Daca vreau sa verific, creez un virus (EICAR Standard Anti-Virus Test File), editand urmatorul sir de caractere:
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
in interiorul unui fisier pe care il numesc eicar. Dupa care uploadez fisierul prin FTP, si verificand daca acesta
a fost sters automat.

Configuram PureFTP pentru a permite sesiuni FTP si TLS:

FTP este un protocol foarte nesigur, deoarece toate parolele si toate datele sunt transferate prin retea ca si text
in clar. Utilizand TLS, intreaga comunicatie poate fi criptata, aceasta facand FTP mult mai sigur.

Daca doriti sa permiteti sesiuni FTP si TLS, rulati:
echo 1 > /etc/pure-ftpd/conf/TLS

Pentru a putea utiliza TLS, trebuie sa creem un certificat TLS. Il vom crea in cadrul /etc/pure-ftpd/ssl/, dar mai intai
vom crea acest director:
mkdir -p /etc/ssl/private/

Apoi generam certificatul SSL:

```
openssl req -x509 -nodes -days 7300 -newkey rsa:2048 -keyout
/etc/ssl/private/pure-ftpd.pem -out /etc/ssl/private/pure-ftpd.pem

Country Name (2 letter code) [AU]: <-- Enter your Country Name (e.g., "DE").
State or Province Name (full name) [Some-State]: <-- Enter your State or Province
Name.
Locality Name (eg, city) []: <-- Enter your City.
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter your
Organization Name (e.g., the name of your company).
Organizational Unit Name (eg, section) []: <-- Enter your Organizational Unit Name
(e.g. "IT Department").
Common Name (eg, YOUR name) []: <-- Enter the Fully Qualified Domain Name of the
system (e.g. "server1.example.com").
Email Address []: <-- Enter your Email Address.

Schimbam permisiunile pentru certificatul SSL:
chmod 600 /etc/ssl/private/pure-ftpd.pem

In final restartam PureFTPd:
/etc/init.d/pure-ftpd-mysql restart

--------------------------------------

ftps-data 989/tcp ftp protocol, data, over TLS/SSL
ftps-data 989/udp ftp protocol, data, over TLS/SSL
ftps 990/tcp ftp protocol, control, over TLS/SSL
ftps 990/udp ftp protocol, control, over TLS/SSL

versus the usual

ftp-data 20/tcp File Transfer [Default Data]
ftp-data 20/udp File Transfer [Default Data]
ftp 21/tcp File Transfer [Control]
ftp 21/udp File Transfer [Control]

Prin urmare stabilesc regula IPTABLES:

iptables -A INPUT -p tcp -m multiport --dports 20,21,989,990 -j ACCEPT

Daca ma conectez cu TLS explicit, conectarea se face prin portul 21, prin urmare nu
mai e nevoie de activarea
porturilor 989 si 990.

Prin urmare regula iptables folosita este:
iptables -A INPUT -p tcp -m multiport --dports 20,21 -j ACCEPT

--------------------------------------

Pentru pureFTPd am cam astea:
```

```
echo "clf:/var/log/pure-ftpd/transfer.log" > /etc/pure-ftpd/conf/AltLog
echo "" > /etc/pure-ftpd/conf/ChrootEveryone
echo "yes" > /etc/pure-ftpd/conf/CreateHomeDir
echo "yes" > /etc/pure-ftpd/conf/DontResolve
echo "UTF-8" > /etc/pure-ftpd/conf/FSCharset
echo "/etc/pure-ftpd/db/mysql.conf" > /etc/pure-ftpd/conf/MySQLConfigFile
echo "yes" > /etc/pure-ftpd/conf/NoAnonymous
echo "no" > /etc/pure-ftpd/conf/PAMAuthentication
echo "/etc/pure-ftpd/pureftpd.pdb" > /etc/pure-ftpd/conf/PureDB
echo "0" > /etc/pure-ftpd/conf/TLS
echo "ALL:!aNULL:!SSLv3" > /etc/pure-ftpd/conf/TLSCipherSuite
echo "117 007" > /etc/pure-ftpd/conf/Umask
echo "no" > /etc/pure-ftpd/conf/UnixAuthentication

+ poate cel cu verboselogging
si cel cu clamav

================================================================================
=====================================

Putem accesa phpMyAdmin la http://server1.example.com/phpmyadmin/ (putem deasemenea
sa utilizam adresa de IP in locul
server1.example.com) in browser si sa ne logam ca user pureftpd. Aici putem sa
aruncam o privire la baza de date.


Force SSL in phpMyAdmin:

// place this at the bottom somewhere
$cfg['ForceSSL'] = TRUE;

--------

Daca vrem sa nu dam acces in phpMyAdmin decat de pe serverul local, putem sa facem
ceva de genul:

<Directory "/usr/share/phpmyadmin">
  Order Deny,Allow
  Deny from all
  Allow from 127.0.0.1
</Directory>

---------

Dupa ce instalam phpMyAdmin ar trebui sa verificam / modificam 2 lucruri in
/etc/phpmyadmin/config.inc.php:
vim config.inc.php

$cfg['Servers'][$i]['auth_type'] = ‘cookie’;
Asigurati-va ca este decomentata si ca parametrul este setat la cookie.
```

$cfg['Servers'][$i]['AllowRoot'] = FALSE;
Asigurati-va ca este decomentata si ca parametrul este setat la ‘false’. Daca nu gasim linia, o adaugam. In felul acesta
nu permitem utilizatorului root administrarea din cadrul phpMyAdmin.

Apoi force SSL la valoarea true sau TRUE. Daca nu gasim linia, o adaugam.
$cfg['ForceSSL'] = TRUE;

Cautam si gasim linia de mai jos, si setam parametrul la true sau TRUE. Daca nu o gasim, o adaugam.
$cfg['Servers'][$i]['ssl'] = TRUE;

Configurari gasim aici:
http://wiki.phpmyadmin.net/pma/Config

==========
GENERAREA CERTIFICATELOR SSL Auto semnate pe Apache in Ubuntu 12.04 si activarea HTTPS / SSL in Apache

Un certificat SSL este o modalitate de a cripta informatia site-ului cat si de a crea o conexiune mult mai sigura.
Suplimentar, certificatul poate sa arate vizitatorilor, identitatea serverului. Autoritatile de certificare pot emite
certificate care sa ateste identitatea serverului, pe cand cele auto-semnate nu sunt avizate de o a 3-a parte.

Setare:
Trebuie sa aveti privilegii de root. Pentru asta, folositi:
sudo su
sau astfel, insotiti fiecare comanda introdusa de, sudo.

Trebuie sa aveti instalat si pornit apache. Altfel, va trebui sa-l instalati:
sudo apt-get update
sudo apt-get install apache2

Activati modulul SSL, dupa care restartati Apache:
sudo a2enmod ssl
sudo service apache2 restart

Creem un nou folder unde vom stoca certificatele server key:
sudo mkdir /etc/apache2/ssl

Creem Certificatele SSL auto-semnate. Cand vom cere un nou certificat, trebuie sa specificat cat timp certificatul
va ramane valid, schimband 365 cu numarul de zile pe care il dorim. Mai jos, certificatul va expira intr-un an:
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

<----- Am generat certificate pe 10 ani.

In comanda de mai sus am creat atat certificatul SSL auto-semnat cat si cheia care protejeaza serverul, si le-am plasat
pe ambele in noul folder. Aceasta comanda ne va cere sa completam o lista de campuri. Cel mai important dintre ele este
"Common Name". Aici introducem numele domeniului oficial sau daca nu avem unul, adresa IP a site-ului nostru. Vom fi
intrebati informatii care vor fi incorporate in certificatul cerut. Ceea ce trebuie sa introducem este Distinguished Name
sau DN. Mai sunt cateva campuri, dar aceste pot fi lasate libere. Pentru altele, pot fi valori implicite. Daca introducem
'.', campurile vor fi lasate libere.

Iata un exemplu:

Country Name (2 letter code) [AU]:US   <----- RO
State or Province Name (full name) [Some-State]:New York   <----- Bucharest
Locality Name (eg, city) []:NYC   <----- Bucharest
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Awesome Inc   <----- S.C. Inovatop S.R.L.
Organizational Unit Name (eg, section) []:Dept of Merriment   <----- IT Dept.
Common Name (e.g. server FQDN or YOUR name) []:example.com   <-- Aici eu am folosit wildcards: *.inovatop.ro
Email Address []:webmaster@awesomeinc.com   <----- webmaster@inovatop.ro / sysadmin@inovatop.ro
-----

Setarea Certificatelor:
Acum avem toate componentele necesare pentru a incheia configurarea. Trebuie sa setam hosturile virtuale ca sa afiseze
noile certificate. Deschidem fisierul de configurare SSL:
sudo nano /etc/apache2/sites-available/default-ssl

In interiorul sectiunii care incepe cu: <VirtualHost _default_:443>, vom face urmatoarele schimbari:
Adaugam o linie cu numele serverului, imediat sub ServerAdmin email:
ServerName example.com:443
Inlocuiti example.com cu numele de domeniu DNS aprobat sau cu adresa de IP a serverului (trebuie sa fie acceasi inregistrare
ca si cea completata la common name cand s-a generat certificatul).

Gasiti urmatoarele trei linii si asigurati-va ca ele au extensiile ca mai jos:
SSLEngine on
SSLCertificateFile /etc/apache2/ssl/apache.crt
SSLCertificateKeyFile /etc/apache2/ssl/apache.key

Salvati si iesiti din fisier.

Activati noul Virtual Host:
Inainte sa activati site-ul web care va raspunde la portul 443, trebuie sa activam acel Virtual Host:
sudo a2ensite default-ssl

Acum avem totul setat. Restartam serverul Apache care va incarca toate schimbarile facute.
sudo service apache2 reload

Introducem in browser: https://youraddress, si vom fi capabili sa vedem noile certificate.

Recomand deschiderea portului 443 în Firewall numai dupa ce site-ul si certificatul au fost configurate cu succes, pentru
a evita atacurile de tip brute-force asupra portului 443. De asemenea având în vedere ca folositi un certificat propriu si
nu unul cumparat este necesar sa adaugati o exceptie pentru certificat în cadrul browserului preferat; acest lucru este
singura diferenta dintre un certificat generat de voi si cel cumparat de la firmele specializate.

==========
==========
POSTFIX:

https://www.exratione.com/2014/05/a-mailserver-on-ubuntu-1404-postfix-dovecot-mysql/
sau:
http://flurdy.com/docs/postfix/

- A Mailserver on Ubuntu 12.04: Postfix, Dovecot, MySQL:
http://www.exratione.com/2012/05/a-mailserver-on-ubuntu-1204-postfix-dovecot-mysql/
- How to set up a mail server on a GNU / Linux system
http://flurdy.com/docs/postfix/
- Virtual Users And Domains With Postfix, Courier, MySQL And SquirrelMail (Ubuntu 12.04 LTS):
http://www.howtoforge.com/virtual-users-and-domains-with-postfix-courier-mysql-and-squirrelmail-ubuntu-12.04-lts
- Install Postfix to configure SMTP Server:
http://www.server-world.info/en/note?os=Ubuntu_12.04&p=mail
- Setup DKIM (DomainKeys) for Ubuntu, Postfix and Mailman:
http://askubuntu.com/questions/134725/setup-dkim-domainkeys-for-ubuntu-postfix-and-mailman
- PostfixCompleteVirtualMailSystemHowto
https://help.ubuntu.com/community/PostfixCompleteVirtualMailSystemHowto
- Setting up MX records with a DNS registrar:
http://ubuntuguide.org/wiki/Mail_Server_setup

Rezultatul va fi instalarea unui mail server sigur, pentru domeniul dedicat, echipat cu urmatoarele pachete software /
functionalitati:

- Postfix: trimite si primeste mailuri via protocolului SMTP. Daca mailurile vor fi trimise de un user autentificat, el va
retransmite acel e-mail catre un alt mailserver. In plus, altcineva va trimite mailuri catre acest server, pentru a fi livrate
local.
- Dovecot: Un server POP si IMAP care va gestiona local folderele de mail si va permite userilor logarea si downloadul
mailurilor. De asemenea, gestioneaza autentificarea utilizatorilor.
- Postgrey: Aseaza mailurile de intrare in greylists, cerand expeditorilor necunoscuti sa astepte o vreme, dupa care sa
retrimita. Acesta este unul dintre cele mai bune instrumente de oprire a spamurilor.
- amavisd-new: Un manager pentru organizarea variatelor filtre de continut antivirus su antispam.
- Clam AntiVirus: O suita de detectie antivirus.
- SpamAssassin: Pentru sniffing out spam din e-mail-uri.
- Postfix Admin: Un instrument web pentru administrarea userilor / conturilor de e-mail si a domeniilor.
- Horde Groupware Webmail Edition / Squirelmail: O interfata web pentru utilizatori.

Serverul va accepta conexiuni SMTP si POP/IMAP, plain text sau criptat, pe porturile standard, dar nu va permite
autentificarea utilizatorilor fara criptare. Acesta va trece e-mail-ul trimis de utilizatorii locali, printr-un set minim
de antete e-mail, prin înlaturarea informatiilor de identificare de la software-ul de e-mail al expeditorului original.

Cateva configurari de baza:

Trebuie sa ne logam ca si root:
sudo su

Trebuie sa setam o adresa IP elastica (vezi: http://aws.amazon.com/articles/1346) si sa ne asiguram ca serverul are un
IP static (permanent). Implicit instanta AWS va avea propriul verificator al numelor de host ciudate, astfel incat
primul lucru pe care ar trebui sa-l facem este sa setam numele de domeniu. Vom da comanda:
hostname mail.example.com   <--- In cazul meu: hostname invtmtax.inovatop.ro

Setam continutul fisierului: /etc/hostname pentru a fi numele de host:
mail.example.com   <--- In cazul meu: invtmtax

Adaugam numele de host pe prima linie a fisierului:/etc/hosts:
127.0.0.1 mail.example.com localhost   <--- In cazul meu: 127.0.0.1
invtmtax.inovatop.ro localhost
De obicei, cateva configurari IPv6 mai urmeaza dupa prima linie, dar ar trebui sa
le lasam asa.
...

Eu am pus in /etc/hosts doar invtmtax
Iar in /etc/hosts am pus:
127.0.0.1   localhost.localdomain   localhost   <----
Asta am lasat !
86.107.58.226   invtmtax.inovatop.ro   invtmtax   <---- Asta am
lasat !

Proxmox a generat ceva de genul:
127.0.0.1   invtmtax.inovatop.ro   localhost invtmtax
localhost.localdomain

Acum, vom dori sa regeneram certificatele SSL auto-semnate, implicite, ale
serverului, astfel incat ele sa se potriveasca cu
numele de domeniu. Putem sa platim un cetificat SSL pentru serverul nostru de
e-mail, dar este perfect posibil si totodata
complet sigur sa rulam un server utilizand certificate auto-semnate. Singura
consecinta vor fi ferestrele de avertizare
cand utilizam webmail gazduit de server precum si din partea Microsoft Outlook cand
ne conectam via POP, IMAP, or SMTP.
apt-get update
apt-get upgrade
apt-get install ssl-cert
make-ssl-cert generate-default-snakeoil --force-overwrite

Mai departe, vom construi un server LAMP

Vom avea nevoie totodata ca mailservarul sa fie un LAMP (Linux, Apache, MySQL, PHP)
web server, deoarece vom dori webmail,
precum si o interfata de administrare web pentru administarrea conturilor de e-mail.
Asa ca setarea serverului nostru Linux
ca si web server este un bun punct de plecare Exista chiar o scurtatura sa instalam
pachetul de baza LAMP:
apt-get update
apt-get upgrade
apt-get install lamp-server^
apt-get clean

In timpul acestei instalari ni se va cere sa alegem o parola de root pentru MySQL.
Alegem ceva cat mai bun dupa care vom adauga
cateva pachete de baza pentru PHP, precum APC bytecode caching, suport memcache,

cURL, si un XML parser, precum si GD image processing. Adaugati si altele la suita voastra LAMP.
apt-get install php-apc php5-memcache php5-curl php5-gd php-xml-parser

sau:

```
apt-get install --assume-yes \
  php-apc \
  php5-mcrypt \
  php5-memcache \
  php5-curl \
  php5-gd \
  php-xml-parser
```

You'll find that php5-memcrypt isn't enabled by default, where "enabled" here means a symlink is created under /etc/php5/apache2/conf.d to point to the module configuration file in /etc/php5/mods-available. You'll notice its absence when webmail fails to work later on. The following command fixes that issue by enabling the module:

```
php5enmod mcrypt
```

Configurare PHP:

Configuratia implicita de PHP precum si pachetele suplimentare mentionate anterior sunt suficiente pentru majoritatea
utilizarilor obisnuite. Prin urmare, daca nu aveti in minte ceva complicat sau high-powered, atunci va trebui probabil doar
sa schimbati setarea expose_php setting din fisierul: /etc/php5/apache2/php.ini. Setati-o sa fie "Off":

```
; Decides whether PHP may expose the fact that it is installed on the server
; (e.g. by adding its signature to the Web server header).  It is no security
; threat in any way, but it makes it possible to determine whether you use PHP
; on your server or not.
; http://php.net/expose-php
expose_php = Off
```

Use OpenSSL to Create a Unique Diffie-Helman Group

Security is becoming ever harder these days. One of the more recent attacks on SSL is known as Logjam, and defending against it requires what is presently a non-standard addition to your SSL configuration in applications using it. Creating your own Diffie-Helman groups and saving them to configuration files is the first step:

```
openssl dhparam -out /etc/ssl/private/dhparams.pem 2048
```

```
chmod 600 /etc/ssl/private/dhparams.pem

--------------------------------
```

Configurare Apache:

Rezultatul asteptat pentru Apache este acele ca el va servi un singur site, cu un numar de aplicatii web: webmail si
Postfix Admin, ascunse intr-un subdirector. Tot traficul va fi directat ca HTTPS - nu exista nici un bun motiv sa permitem
acces nesecurizat la orice va fi pe serverul web.

Intai de toate configuram urmatoarele linii in fisierul:
/etc/apache2/conf-enabled/security.conf, pentru a minimiza
informatia pe care Apache o furnizeaza in antetele sale de raspuns:

```
#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of:  Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#
ServerTokens Prod

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
#
ServerSignature Off
```

Asigurati-va ca mod_rewrite, mod_ssl, si site-ul virtual SSL implicit sunt activate - vom avea nevoie ca toate acestea sa
fie disponibile pentru a forta utilizatorii sa utilizeze HTTPS.

```
a2enmod rewrite ssl
a2ensite default-ssl
```

Edit these lines in /etc/apache2/mods-available/ssl.conf to ensure that protocols that are no longer secure are not used:

```
# Aiming for perfect forward secrecy where possible, and protecting against
# attacks such as Logjam. See:
# https://weakdh.org/sysadmin.html
# https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/
SSLCipherSuite
```

```
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA38
4:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:
kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:E
CDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AE
S256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES
128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SH
A256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:AES:CAMELLI
A:DES-CBC3-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SH
A:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA
SSLHonorCipherOrder on

#   The protocols to enable.
#   Available values: all, SSLv3, TLSv1, TLSv1.1, TLSv1.2
#   SSL v2  is no longer supported
SSLProtocol all -SSLv2 -SSLv3
```

Configuratia site-ului default in fisierul:
/etc/apache2/sites-available/000-default.conf poate fi editata sa arate ca mai jos:

```
<VirtualHost *:80>
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www
  <Directory "/">
    Options FollowSymLinks
    AllowOverride All
  </Directory>
  ErrorLog ${APACHE_LOG_DIR}/error.log
  # Possible values include: debug, info, notice, warn, error, crit,
  # alert, emerg.
  LogLevel warn
  CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

sau:

```
<VirtualHost *:80>
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html
  <Directory "/var/www/html">
    Options FollowSymLinks
    AllowOverride All
  </Directory>
  ErrorLog ${APACHE_LOG_DIR}/error.log
  # Possible values include: debug, info, notice, warn, error, crit,
  # alert, emerg.
  LogLevel warn
  CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Dar, bineinteles, gusturile si nevoile voastre pot fi diferite. Pastrati aceeasi abordare simpla. Portiunea de sus a
fisierului de configurare SSL: /etc/apache2/sites-available/default-ssl.conf poate fi setata precum:

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www
    <Directory "/">
      Options FollowSymLinks
      AllowOverride All
    </Directory>
    ErrorLog ${APACHE_LOG_DIR}/error.log
    # Possible values include: debug, info, notice, warn, error, crit,
    # alert, emerg.
    LogLevel warn
    CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined
    #   SSL Engine Switch:
    #   Enable/Disable SSL for this virtual host.
    SSLEngine on
    #
    # ... more default SSL configuration ...
    # You will probably need to change this next Directory directive as well
    # in order to match the earlier one.
    <Directory "/">
      SSLOptions +StdEnvVars
    </Directory>
    # ... yet more default SSL configuration ...
```

sau:

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    <Directory "/var/www/html">
      Options FollowSymLinks
      AllowOverride All
    </Directory>
    ErrorLog ${APACHE_LOG_DIR}/error.log
    # Possible values include: debug, info, notice, warn, error, crit,
    # alert, emerg.
    LogLevel warn
    CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined
    #   SSL Engine Switch:
    #   Enable/Disable SSL for this virtual host.
    SSLEngine on
    #
    # ... more default SSL configuration ...
```

```
    # You will probably need to change this next Directory directive as well
    # in order to match the earlier one.
    <Directory "/var/www/html">
      SSLOptions +StdEnvVars
    </Directory>
    # ... yet more default SSL configuration ...
```

If you are using a purchased rather than self-signed SSL certificate, then you probably also have a CA certificate bundle
from the issuer. You may have a wildcard certificate for *.example.com, a less costly certificate covering several
subdomains such as www.example.com and mail.example.com, or you may have separate certificates for the subdomains
that you care about. Place the relevant certificate, private key, and CA certificate bundle in the following locations:

```
/etc/ssl/private/example.com.key
/etc/ssl/certs/example.com.crt
/etc/ssl/certs/ca-bundle.crt
```

The key must not be password protected, and it must be locked down such that only the root user can read it:

```
chmod 600 /etc/ssl/private/example.com.key
```

Now change these lines in /etc/apache2/sites-enabled/default-ssl.conf:

```
#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
SSLCertificateFile    /etc/ssl/certs/example.com.crt
SSLCertificateKeyFile /etc/ssl/private/example.com.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
SSLCertificateChainFile /etc/ssl/certs/ca-bundle.crt
```

Pentru a forta vizitatorii spre utilizarea HTTPS, puneti ceva similar cu urmatoarele randuri, fisierul /var/www/html/.htaccess:

```
RewriteEngine On
# Redirect all HTTP traffic to HTTPS.
RewriteCond %{HTTPS} !=on
```

```
RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]

sau:

RewriteEngine On
RewriteCond %{SERVER_PORT} 80
RewriteRule ^(.*) https://mail.example.com/$1 [L]

--------------------------------

In cazul meu am creat un subdomeniu la domeniul de baza, de genul
https://pfad.inovatop.ro

Iata si fisierul din cadrul /etc/apache2/sites-available/subdomeniu-ssl:

## Virtual Host for POSTFIX ADMIN
<VirtualHost *:443>
        ServerName invtpadx.inovatop.ro
        ServerAdmin sysadmin@inovatop.ro

        DocumentRoot /var/www/postfixadmin

        RewriteEngine On
        RewriteCond %{HTTP_HOST} !invtpadx.inovatop.ro
        RewriteRule (.*) [L]

        <Directory /var/www/postfixadmin/>
                Options +FollowSymLinks -Indexes
                DirectoryIndex index.php
                AllowOverride None
                Order Deny,Allow
                Deny from ALL
                Allow from 89.35.233.244        # TQM LAN
                Allow from 86.125.50.152        # SER LAN
                # Allow from 89.35.233.245      # Sala INFO

                <IfModule mod_php5.c>
                        AddType application/x-httpd-php .php
                        php_flag magic_quotes_gpc Off
                        php_flag track_vars On
                        php_flag register_globals Off
                        php_value include_path .
                </IfModule>
        </Directory>

        # Restrictionez accesul la fisierul /var/www/postfixadmin/setup.php
        <Files "setup.php">
            Deny from ALL
        </Files>
```

```
        # SSL Engine Switch: Enable/Disable SSL for this virtual host.
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/webcert.crt
        SSLCertificateKeyFile /etc/apache2/ssl/webcert.key

        ErrorLog ${APACHE_LOG_DIR}/error.log
        # Possible values include: debug, info, notice, warn, error, crit, alert,
emerg.
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined
</VirtualHost>
```

Deoarece mai am inca un subdomeniu la acelasi domeniu, dupa ce activez site-ul si restartez serverul voi avea
o eroare de genul: [warn] _default_ VirtualHost overlap on port 443, the first has precedence
Pentru a dezactiva acest lucru introduc urmatoarea linie in /etc/apache2/apache2.conf

```
NameVirtualHost *:443
```

Make Use of that Diffie-Helman Group

What to do with the Diffie-Helman group in /etc/ssl/private/dhparams.pem depends on the version of Apache. You can find your version by running:

```
apachectl -V
```

If you are running 2.4.8 or later, then add or edit this line in /etc/apache2/mods-available/ssl.conf:

```
SSLOpenSSLConfCmd DHParameters "/etc/ssl/private/dhparams.pem"
```

If using an earlier version, then append the contents of /etc/ssl/private/dhparams.pem to your certificate file. For example:

```
cat /etc/ssl/private/dhparams.pem >> /etc/ssl/certs/example.com.crt
```

Now restart Apache to pick up the changes, after which you should be able to load the default Apache homepage and see that you are automatically redirected to HTTPS.

```
service apache2 restart
```

Instalare si Configurare Memcached

Vom instala Memcached pentru suport pentru aplicatiile webmail ce vor rula pe acest

server:
apt-get install memcached

Configuratia fisierului implicit de la /etc/memcached.conf este suficient de buna pentru un server mic: ea blocheaza
accesul la localhost si asigura valori generale ale parametrilor. Daca construim o masina mare, pentru utilizare heavy, probabil va trebui sa marim alocarea memoriei la o valoarea mai mare decat cea implicita de 64M:

```
# Start with a cap of 64 megs of memory. It's reasonable, and the daemon default
# Note that the daemon will grow to this size, but does not start out holding this
much
# memory
-m 64
```

Instalam pachetele Mailserver

Precum in cazul LAMP, exista o scurtatura pentru instalarea pachetelor de baza pentru un mail server:
apt-get install mail-server^

Cand se instaleaza Postfix, vom fi intrebati daca alegem un tip general de configurare mail - selectam "Internet site".
Vom fi intrebati de numele sistemului de mail, care va fi numele de host al serverului de mail - Ex: mail.example.com.
Ceea ce se va instala va fi un mailserver care va administra utilizatorii ca si Unix useri, neutilizand o baza de date
SQL pentru stocarea informatiilor. Prin urmare, va fi nevoie de MySQL suport pentru Postfix si Dovecot, cat si suport pentru
pachetele antispam:
apt-get install postfix-mysql dovecot-mysql postgrey
apt-get install amavis clamav clamav-daemon spamassassin
apt-get install php5-imap

sau:

```
apt-get install --assume-yes \
  postfix-mysql \
  dovecot-mysql \
  postgrey \
  amavis \
  clamav \
  clamav-daemon \
  spamassassin \
  php5-imap
```

Pachetul php5-imap, ofera suport POP3 cat si IMAP, si vor folosi lui Postfix Admin si multor posibile optiuni pentru aplicatiile

webmail PHP. Activam modulul:

```
php5enmod imap
```

apoi restartam Apache:

```
service apache2 restart
```

Vom dori in plus si alte pachete optionale care extind abilitatile pachetelor de detectie spam si virus, precum permiterea
de inspectii asupra fisierelor atasate:

```
apt-get install libnet-dns-perl pyzor razor
apt-get install arj bzip2 cabextract cpio file gzip nomarch pax unzip zip
```

sau:

```
apt-get install --assume-yes \
  pyzor \
  razor \
  arj \
  cabextract \
  lzop \
  nomarch \
  p7zip-full \
  ripole \
  rpm2cpio \
  tnef \
  unzip \
  unrar-free \
  zip \
  zoo
```

Probabil vom dori un pachet pentru lucrul cu arhive format RAR.

Instalare Postfix Admin si schema bazei de date MySQL

Va trebui sa creem baza de date pe care o va utiliza Postfix Admin
Ne conectam la serverul MySQL.

```
mysql -u root -p
```

Creem baza de date:

```
mysql> CREATE DATABASE nume_baza_de_date;
mysql> GRANT ALL ON nume_baza_de_date.* to nume_user@nume_host identified by
"parola_aleasa";
```

---

sau:

```
mysql> CREATE DATABASE nume_baza_de_date;
```

```
mysql> CREATE USER nume_user@localhost IDENTIFIED BY 'your_password';
mysql> GRANT ALL PRIVILEGES ON nume_baza_de_date.* TO nume_user;
-------------
```

La final reincarc noile privilegii:

```
mysql> FLUSH PRIVILEGES;
```

Postfix Admin se instaleaza dupa cum urmeaza. Se downloadeaza pachetul de la Sourceforge, se dezarhiveaza, apoi se muta
intr-un subdirector al radacinii web. Vom dori, probabil sa schimbam proprietarul la userul www-data:

```
wget
http://downloads.sourceforge.net/project/postfixadmin/postfixadmin/postfixadmin-2.3.5/postfixadmin-2.3.5.tar.gz
mkdir /home/nume_user/documente/kituri
cd /home/nume_user/documente/kituri
gunzip postfixadmin-2.3.5.tar.gz
tar -xf postfixadmin-2.3.5.tar
mv postfixadmin-2.3.5 /var/www/postfixadmin
chown -R www-data:www-data /var/www/postfixadmin
```

sau:

```
wget
http://downloads.sourceforge.net/project/postfixadmin/postfixadmin/postfixadmin-2.3.7/postfixadmin-2.3.7.tar.gz
tar -xf postfixadmin-2.3.7.tar.gz
rm -f postfixadmin-2.3.7.tar.gz
mv postfixadmin-2.3.7 /var/www/html/postfixadmin
chown -R www-data:www-data /var/www/html/postfixadmin
```

In continuare se va aplica un proces se setari in doua faze. Prima data, modificam urmatoarele linii in fisierul:
/var/www/postfixadmin/config.inc.php:

```
/**********************************************************************
 *  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 * You have to set $CONF['configured'] = true; before the
 * application will run!
 * Doing this implies you have changed this file as required.
 * i.e. configuring database etc; specifying setup.php password etc.
 */
$CONF['configured'] = true;

// Postfix Admin Path
// Set the location of your Postfix Admin installation here.
// YOU MUST ENTER THE COMPLETE URL e.g. http://domain.tld/postfixadmin
$CONF['postfix_admin_url'] = 'https://mail.example.com/postfixadmin';
```

```
// Database Config
// mysql = MySQL 3.23 and 4.0, 4.1 or 5
// mysqli = MySQL 4.1+
// pgsql = PostgreSQL
$CONF['database_type'] = 'mysql';
$CONF['database_host'] = 'localhost';
$CONF['database_user'] = 'mail';
$CONF['database_password'] = 'mailpassword';
$CONF['database_name'] = 'mail';

// Site Admin
// Define the Site Admins email address below.
// This will be used to send emails from to create mailboxes.
$CONF['admin_email'] = 'me@example.com';

// Mail Server
// Hostname (FQDN) of your mail server.
// This is used to send email to Postfix in order to create mailboxes.
//
// Set this to localhost for now, but change it later.
$CONF['smtp_server'] = 'localhost';                                        <<-----
Atentie !!! Aici voi schimba mai tarziu !!!
$CONF['smtp_port'] = '25';

------
De exemplu:
Mai setez si:
$CONF['admin_email'] = 'sysadmin@inovatop.ro';
$CONF['min_password_length'] = 8;
$CONF['page_size'] = '30';
$CONF['default_aliases'] = array (
    'abuse' => 'abuse@inovatop.ro',
    'hostmaster' => 'hostmaster@inovatop.ro',
    'postmaster' => 'postmaster@inovatop.ro',
    'webmaster' => 'webmaster@inovatop.ro'
);
$CONF['domain_path'] = 'YES';
$CONF['domain_in_mailbox'] = 'YES';
$CONF['maildir_name_hook'] = 'NO';
$CONF['vacation'] = 'YES';
$CONF['vacation_domain'] = 'autoreply.inovatop.ro';
$CONF['alias_control'] = 'YES';
$CONF['alias_control_admin'] = 'YES';
$CONF['show_header_text'] = 'YES';
$CONF['header_text'] = ':: Postfix Admin System for InovaTop ::';
$CONF['user_footer_link'] = "https://invtpadx.inovatop.ro/users/login.php";
$CONF['footer_text'] = 'Return to main page and Login as Postfix SuperAdmin';
$CONF['footer_link'] = 'https://invtpadx.inovatop.ro';
$CONF['theme_logo'] = 'images/inovatop_2.png';
```

```
------

// Encrypt
// In what way do you want the passwords to be crypted?
// md5crypt = internal postfix admin md5
// md5 = md5 sum of the password
// system = whatever you have set as your PHP system default
// cleartext = clear text passwords (ouch!)
// mysql_encrypt = useful for PAM integration
// authlib = support for courier-authlib style passwords
// dovecot:CRYPT-METHOD = use dovecotpw -s 'CRYPT-METHOD'. Example: dovecot:CRAM-MD5
$CONF['encrypt'] = 'md5crypt';

// Mailboxes
// If you want to store the mailboxes per domain set this to 'YES'.
// Examples:
//   YES: /usr/local/virtual/domain.tld/username@domain.tld
//   NO:  /usr/local/virtual/username@domain.tld
$CONF['domain_path'] = 'NO';
// If you don't want to have the domain in your mailbox set this to 'NO'.
// Examples:
//   YES: /usr/local/virtual/domain.tld/username@domain.tld
//   NO:  /usr/local/virtual/domain.tld/username
// Note: If $CONF['domain_path'] is set to NO, this setting will be forced to YES.
$CONF['domain_in_mailbox'] = 'YES';

----------------------
In alta parte am gasit alt set de setari:

### Configure postfixadmin
### A special hash required, it can be generated at
http://se.rv.e.r/postfixadmin/setup.php
### On the local filesystem, the mail layout is as following:
### /mail/domain_name/user/
### This can be changed if desired, using other values for 'domain_path' and
'domain_in_mailbox'

# cd /usr/local/www/postfixadmin
# vi /config.local.php
$CONF[configured] = true;
$CONF['database_type'] = 'mysqli';
$CONF['database_user'] = 'postfixadmin';
$CONF['database_password'] = 'oeshieGhieng2ieT';
$CONF['generate_password'] = 'YES';
$CONF['show_password'] = 'YES';
$CONF['page_size'] = '30';
$CONF['domain_path'] = 'YES';
$CONF['domain_in_mailbox'] = 'NO';
$CONF['quota'] = 'YES';
```

```
$CONF['transport_options'] = array('virtual', 'relay');
$CONF['vacation'] = 'YES';
$CONF['alias_control'] = 'YES';
$CONF['alias_control_admin'] = 'YES';
$CONF['fetchmail']='NO';
$CONF['create_mailbox_subdirs_prefix']='';
$CONF['xmlrpc_enabled']=true;

----------------------
```

In cazul meu am creat un subdomeniu la domeniul de baza, de genul https://pfad.inovatop.ro

Iata si fisierul din cadrul /etc/apache2/sites-available/subdomeniu-ssl:

```
## Virtual Host for POSTFIX ADMIN
<VirtualHost *:443>
        ServerName invtpadx.inovatop.ro
        ServerAdmin sysadmin@inovatop.ro

        DocumentRoot /var/www/postfixadmin

        RewriteEngine On
        RewriteCond %{HTTP_HOST} !invtpadx.inovatop.ro
        RewriteRule (.*) [L]

        <Directory /var/www/postfixadmin/>
                Options +FollowSymLinks -Indexes
                DirectoryIndex index.php
                AllowOverride None
                Order Deny,Allow
                Deny from ALL
                Allow from 89.35.233.244        # TQM LAN
                Allow from 86.125.50.152        # SER LAN
                # Allow from 89.35.233.245      # Sala INFO

                <IfModule mod_php5.c>
                        AddType application/x-httpd-php .php
                        php_flag magic_quotes_gpc Off
                        php_flag track_vars On
                        php_flag register_globals Off
                        php_value include_path .
                </IfModule>
        </Directory>

        # Restrictionez accesul la fisierul /var/www/postfixadmin/setup.php
        <Files "setup.php">
            Deny from ALL
        </Files>
```

```
        # SSL Engine Switch: Enable/Disable SSL for this virtual host.
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/webcert.crt
        SSLCertificateKeyFile /etc/apache2/ssl/webcert.key

        ErrorLog ${APACHE_LOG_DIR}/error.log
        # Possible values include: debug, info, notice, warn, error, crit, alert,
emerg.
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined
</VirtualHost>
```

Apoi, deschidem un browser web si vizitam mail serverul la:
https://mail.example.com/postfixadmin/setup.php

Urmam instructiunile de la acea pagina si alegem parola de setup, si generam un hash al acelei parole. Adaugam acel hash
la fisierul de configurare si apoi salvam:

```
// In order to setup Postfixadmin, you MUST specify a hashed password here.
// To create the hash, visit setup.php in a browser and type a password into the
field,
// on submission it will be echoed out to you as a hashed value.
$CONF['setup_password'] = '...a long hash string...';
```

Apoi ne reintoarcem la pagina de setare. Acum putem utiliza parola tocmai setata pentru a crea un cont de administrare
initial. Postfix Admin va crea de asemenea propria sa schema de baze de date.

Este foarte bine sa restrictionam accesul la fisierul /var/www/postfixadmin/setup.php dupa ce l-am utilizat. Creati un
fisier: /var/www/postfixadmin/.htaccess si puneti in el urmatoarele instructiuni:

```
<Files "setup.php">
        deny from all
</Files>
```

Crearea domeniilor si a conturilor de e-mail in Postfix Admin

Navigati acum la principala pagina de logare a Postfix Admin:
https://mail.example.com/postfixadmin/

Logati-va cu contul de administrator nou creat, si apoi alegeti optiunea "New domain" sub "Domain List", pentru a crea
example.com. Veti putea apoi adauga utilizatori de mail ("Add mailbox") si aliasuri ("Add alias") cat timp vizualizati

domeniul respectiv. Toate acestea vor popula baza de date, dar nu vor face alte setari cu privire la componentele serverului
de mail.

Postfix Admin are o alta functie folositoare in timpul acestui proces de setare - el permite trimiterea de mailuri catre
utilizatorii locali, prin intermediul interfetei web, ceea ce este util cand testam configuratia.

Instalarea modulului de VACANTA in PostfixAdmin

PostfixAdmin permet a chaque utilisateur du serveur mail de gérer les réponses automatiques via l'interface utilisateur de postfixadmin. Ce tutoriel explique comment installer cette fonctionnalité (Ubuntu server, 10.04 LTS).

Tout d'abord, un certain nombre de packages supplémentaires doivent etre installés:

```
apt-get update
apt-get install libmail-sender-perl libdbd-mysql-perl libemail-valid-perl
libmime-perl liblog-log4perl-perl liblog-dispatch-perl libgetopt-argvfile-perl
libmime-charset-perl libmime-encwords-perl libdbd-pg-perl
apt-get clean
```

Ensuite, on crée un utilisateur et un groupe pour gérer le systeme de vacances ; on affecte un répertoire utilisateur /var/spool/vacation a cet utilisateur :

```
mkdir /var/spool/vacation
groupadd vacation
useradd -g vacation -d /var/spool/vacation -s /sbin/nologin vacation
```

Le module de vacation est inclus dans un des répertoire de postfix, éventuellement compressé : il faut le décompresser, le copier dans le répertoire précédemment créé et donner les droits a l'utilisateur vacation sur ce répertoire.

```
cd /usr/share/doc/postfixadmin/examples/VIRTUAL_VACATION
sau dupa caz:
cd /var/www/postfixadmin/VIRTUAL_VACATION
```

apoi, dupa caz:

```
gunzip vacation.pl.gz
cp vacation.pl vacation.pl.save
cd ..
cp -a VIRTUAL_VACATION /usr/share/postfixadmin/
```

Ceea ce ma intereseaza de fapt este sa:

```
cp vacation.pl /var/spool/vacation/
cd /var/spool/
```

```
chown -R vacation:vacation vacation
chmod -R 700 vacation
```

On édite alors le fichier /var/spool/vacation/vacation.pl pour configurer les parametres :

```
our $db_type = 'mysql';
# leave empty for connection via UNIX socket
our $db_host = '';
# connection details
our $db_username = 'postfixadmindb';
our $db_password = 'passwd';
our $db_name     = 'postfixadminuser';
our $vacation_domain = 'autoreply.nathalievilla.org';
# smtp server used to send vacation e-mails
our $smtp_server = 'localhost';
our $smtp_server_port = 25;
# SMTP authentication protocol used for sending.
# Can be 'PLAIN', 'LOGIN', 'CRAM-MD5' or 'NTLM'
# Leave it blank if you don't use authentification
our $smtp_auth = '';
# username used to login to the server
our $smtp_authid = '';
# password used to login to the server
our $smtp_authpwd = '';
```

ou les parametres doivent etre adaptés a votre serveur.

On met alors a jour le fichier de configuration de postfixadmin : /var/www/postfixadmin/config.inc.php

```
$CONF['vacation'] = 'YES';
$CONF['vacation_domain'] = 'autoreply.nathalievilla.org';
```

Puis on reconfigure postfix : /etc/postfix/master.cf en y ajoutant la ligne suivante vers la fin du fichier :

```
vacation unix - n n - - pipe
        flags=Rq user=vacation argv=/var/spool/vacation/vacation.pl -f ${sender}
${recipient}
```

et /etc/postfix/main.cf

```
transport_maps = hash:/etc/postfix/transport
```

puis, finalement, en créant un fichier /etc/postfix/transport contenant

```
autoreply.nathalievilla.org vacation
```

Les changements sont pris en compte dans postfix avec :

```
postmap /etc/postfix/transport
/etc/init.d/postfix reload
```

... et c'est parti pour les vacances !!!

Crearea unui user care sa manevreze directoarele mail virtuale

Userii de mail virtuali sunt aceeia care nu exista ca si useri ai sistemului Unix. Ei nu utilizeaza metodele standard de
autentificare sau livrare a mailurilor si nu au un director home. Lucrurile, in acest caz se vor desfasura in felul
urmator:
- Userii de mail sunt definiti in baza de date creata de Postfix Admin in loc de a fi definiti in cadrul sistemului
Unix. Mailurile vor fi pastrate in subfoldere per fiecare domeniu si cont in folderul /var/vmail - Exemplu: me@example.com
va avea un director /var/vmail/example.com/me. Toate aceste directoare de mailuri vor fi detinute de un singur user numit
vmail, iar Dovecot va utiliza userul vmail pentru a si updata fisierele de mail.

```
useradd -r -u 150 -g mail -d /var/vmail -s /sbin/nologin -c "Virtual maildir handler" vmail
mkdir /var/vmail
chmod 770 /var/vmail
chown vmail:mail /var/vmail
```

Retineti ca folderul pentru user si mail virtual utilizeaza grupul "mail", si permite altor utilizatori din cadrul grupului
sa modifica continutul.

Configurare Dovecot

Dovecot va gestiona conexiunile IMAP si POP3, directoarele de mail locale si va receptiona mailurile de intrare venite de
la Postfix. De asemenea va gestiona autentificarile pentru conexiuni SMTP - nu exista nici un avantaj in a avea doua sisteme
separate de autentificare atunci când Dovecot se poate ocupa de ambele cazuri. Configurarea este facuta pentru mai multe fisiere
din cadrul subfolderului /etc/dovecot, si ar putea parea un pic intimidanta, dar totul este facut cat se poate de logic.

Primul lucru care trebuie facut este sa ne asiguram ca Dovecot se uita dupa datele userilor in baza de date creata cu
Postfix Admin, prin urmare vom crea sau edita fisierul
/etc/dovecot/conf.d/auth-sql.conf.ext, pentru a avea urmatorul continut:

```
# Look up user passwords from a SQL database as
# defined in /etc/dovecot/dovecot-sql.conf.ext
passdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
}
# Look up user information from a SQL database as
# defined in /etc/dovecot/dovecot-sql.conf.ext
userdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
}
```

Acum vom edita liniile urmatoare in fisierul /etc/dovecot/dovecot-sql.conf.ext
astfel incat sa utilizeze baza de date
MySQL creata de Postfix Admin:

```
# Database driver: mysql, pgsql, sqlite
driver = mysql

# Examples:
#   connect = host=192.168.1.1 dbname=users
#   connect = host=sql.example.com dbname=virtual user=virtual password=blarg
#   connect = /etc/dovecot/authdb.sqlite
#
connect = host=localhost dbname=mail user=mail password=mailpassword

# Default password scheme.
#
# List of supported schemes is in
# http://wiki2.dovecot.org/Authentication/PasswordSchemes
#
default_pass_scheme = MD5-CRYPT

# Define the query to obtain a user password.
password_query = \
  SELECT username as user, password, '/var/vmail/%d/%n' as userdb_home, \
  'maildir:/var/vmail/%d/%n' as userdb_mail, 150 as userdb_uid, 8 as userdb_gid \
  FROM mailbox WHERE username = '%u' AND active = '1'

# Define the query to obtain user information.
user_query = \
  SELECT '/var/vmail/%d/%n' as home, 'maildir:/var/vmail/%d/%n' as mail, \
  150 AS uid, 8 AS gid, concat('dirsize:storage=', quota) AS quota \
  FROM mailbox WHERE username = '%u' AND active = '1'
```

Apoi schimbam definitiile de control in fisierul /etc/dovecot/conf.d/10-auth.conf
astfel incat Dovecot sa citeasca
fisierele de configurare SQL. Cat timp suntem aici, trebuie totodata sa ne asiguram

ca autentificarea plaintext este
dezactivata cu exceptia cazului cand conexiunea este criptata sau locala:

```
# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
disable_plaintext_auth = yes

# Space separated list of wanted authentication mechanisms:
#   plain login digest-md5 cram-md5 ntlm rpa apop anonymous gssapi otp skey
#   gss-spnego
# NOTE: See also disable_plaintext_auth setting.
auth_mechanisms = plain login

##
## Password and user databases
##

#
# Password database is used to verify user's password (and nothing more).
# You can have multiple passdbs and userdbs. This is useful if you want to
# allow both system users (/etc/passwd) and virtual users to login without
# duplicating the system users into virtual database.
#
# <doc/wiki/PasswordDatabase.txt>
#
# User database specifies where mails are located and what user/group IDs
# own them. For single-UID configuration use "static" userdb.
#
# <doc/wiki/UserDatabase.txt>

#!include auth-deny.conf.ext
#!include auth-master.conf.ext

#!include auth-system.conf.ext
# Use the SQL database configuration rather than any of these others.
!include auth-sql.conf.ext
#!include auth-ldap.conf.ext
#!include auth-passwdfile.conf.ext
#!include auth-checkpassword.conf.ext
#!include auth-vpopmail.conf.ext
#!include auth-static.conf.ext
```

Apoi, vom spune lui Dovecot unde sa puna directoarele de mail pentru userii
virtuali. Asta necesita urmatoarele schimbari
in fisierul /etc/dovecot/conf.d/10-mail.conf:

```
# Location for users' mailboxes. The default is empty, which means that Dovecot
# tries to find the mailboxes automatically. This won't work if the user
```

```
# doesn't yet have any mail, so you should explicitly tell Dovecot the full
# location.
#
# If you're using mbox, giving a path to the INBOX file (eg. /var/mail/%u)
# isn't enough. You'll also need to tell Dovecot where the other mailboxes are
# kept. This is called the "root mail directory", and it must be the first
# path given in the mail_location setting.
#
# There are a few special variables you can use, eg.:
#
#   %u - username
#   %n - user part in user@domain, same as %u if there's no domain
#   %d - domain part in user@domain, empty if there's no domain
#   %h - home directory
#
# See doc/wiki/Variables.txt for full list. Some examples:
#
#   mail_location = maildir:~/Maildir
#   mail_location = mbox:~/mail:INBOX=/var/mail/%u
#   mail_location = mbox:/var/mail/%d/%1n/%n:INDEX=/var/indexes/%d/%1n/%n
#
# <doc/wiki/MailLocation.txt>
#
mail_location = maildir:/var/vmail/%d/%n

# System user and group used to access mails. If you use multiple, userdb
# can override these by returning uid or gid fields. You can use either numbers
# or names. <doc/wiki/UserIds.txt>
mail_uid = vmail
mail_gid = mail

# Valid UID range for users, defaults to 500 and above. This is mostly
# to make sure that users can't log in as daemons or other system users.
# Note that denying root logins is hardcoded to dovecot binary and can't
# be done even if first_valid_uid is set to 0.
#
# Use the vmail user uid here.
first_valid_uid = 150
last_valid_uid = 150

Daca venim cu propriile certificate SSL, trebuie sa-i spunem lui Dovecot despre ele,
editand urmatoarele linii din
fisierul /etc/dovecot/conf.d/10-ssl.conf. Amintiti-va sa includeti certificatul CA,
daca este asigurat de un emitent
de certificate.

# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = yes

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
```

```
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
ssl_cert = </path/to/my/cert.pem
ssl_key = </path/to/my/key.pem

# If key file is password protected, give the password here. Alternatively
# give it when starting dovecot with -p parameter. Since this file is often
# world-readable, you may want to place this setting instead to a different
# root owned 0600 file by using ssl_key_password = <path.
#ssl_key_password =

# PEM encoded trusted certificate authority. Set this only if you intend to use
# ssl_verify_client_cert=yes. The file should contain the CA certificate(s)
# followed by the matching CRL(s). (e.g. ssl_ca = </etc/ssl/certs/ca.pem)
#ssl_ca = </path/to/ca.pem
```

You must also update the following lines in /etc/dovecot/conf.d/10-ssl.conf to ensure that some SSL protocols that are no longer secure are not used:

```
# DH parameters length to use. In light of Logjam, has to be 2048 or more.
# See: https://weakdh.org/sysadmin.html
ssl_dh_parameters_length = 2048

# SSL protocols to use. Don't use the no-longer secure protocols.
ssl_protocols = !SSLv2 !SSLv3

# SSL ciphers to use. See:
# https://weakdh.org/sysadmin.html
# https://hynek.me/articles/hardening-your-web-servers-ssl-ciphers/
ssl_cipher_list =
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA38
4:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:
kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:E
CDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AE
S256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES
128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SH
A256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:AES:CAMELLI
A:DES-CBC3-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SH
A:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA

# Prefer the server's order of ciphers over client's.
ssl_prefer_server_ciphers = yes
```

Apoi, editati urmatoarele linii in cadrul /etc/dovecot/conf.d/10-master.conf pentru a adauga optiunile Postfix:

```
service auth {
  # auth_socket_path points to this userdb socket by default. It's typically
  # used by dovecot-lda, doveadm, possibly imap process, etc. Its default
```

```
  # permissions make it readable only by root, but you may need to relax these
  # permissions. Users that have access to this socket are able to get a list
  # of all usernames and get results of everyone's userdb lookups.
  unix_listener auth-userdb {
   mode = 0600
    user = vmail
    group = mail
  }

  unix_listener /var/spool/postfix/private/auth {
    mode = 0660
    # Assuming the default Postfix user and group
    user = postfix
    group = postfix
  }
```

You may have to explicitly set a postmaster address in /etc/dovecot/conf.d/15-lda.conf; if you see "Invalid settings: postmaster_address setting not given" showing up in the mail log, then this is the fix for that. Make sure that a suitable alias or mailbox exists for your chosen postmaster address:

```
# Address to use when sending rejection mails.
# Default is postmaster@<your domain>.
postmaster_address = postmaster@example.com
```

Veti dori apoi sa schimbati configuratia Dovecot pentru a fi accesibila atat pentru Dovecot cat si pentru userii de mail:

```
chown -R vmail:dovecot /etc/dovecot
chmod -R o-rwx /etc/dovecot
```

O observatie finala referitoare la Dovecot: Se va crea un folder al userului de mail doar cand un e-mail va fi livrat pentru
prima data catre acel user virtual. Prin urmare, crearea unui user in Postfix Admin nu va insemana si crearea imediata a unui
director de mailuri in interiorul lui si asta este chiar foarte bine.

Proper SSL certificates for Postfix and Dovecot

So far you will have received warning on the SSL certificates you use for Postfix, Dovecot and the RoundCube email web interface. SSL/TLS is a great way to automatically encrypt the passwords between the email user and your mail server. So you want to have proper certificates. There are three ways you can handle your certificate:

Either: Leave it like it is

The users will receive a warning that the certificate is invalid and likely does not

even match the name of the mail server.

Advantage: lazy, no costs
Disadvantage: some email clients will refuse the certficate because not even the server name matches
Conclusion: only do this if you don't care

Or: Create a self-signed certificate

This will at least give your users a certificate with with the proper name of the mail server.

Advantage: little work, no costs
Disadvantage: you train your users to accept any certificate (even a malicious one)
Conclusion: do this if you have a very small group of users who you can tell about the certificate

Creating SSL certificates can be tricky due to the syntax of the "openssl" command line tool that often reminds me of text adventures.

Dovecot:

Here comes the command to create a Dovecot certificate:

```
openssl req -new -x509 -days 7300 -nodes -out /etc/ssl/certs/dovecot.pem -keyout /etc/ssl/private/dovecot.pem
```

What you enter in the fields is entirely your choice. The only notable exception is the "Common Name" which has to be exactly the name of your server in the way that users will access it. So if you tell your users to access your mail server at "mail.example.org" then this has to be entered here. This certificate will be valid for 10 years (20 times 365 days).

Do not forget to set the permissions on the private key so that no unauthorized people can read it:

```
chmod o= /etc/ssl/private/dovecot.pem
```

And you will have to restart Dovecot to make it read your new certificate:

```
/etc/init.d/dovecot restart
```

Postfix

To create a certificate to be used by Postfix use:

```
openssl req -new -x509 -days 3650 -nodes -out /etc/ssl/certs/postfix.pem -keyout /etc/ssl/private/postfix.pem
```

Do not forget to set the permissions on the private key so that no unauthorized

people can read it:

```
chmod o= /etc/ssl/private/postfix.pem
```

You will have to tell Postfix where to find your certificate and private key because by default it will look for a dummy certificate file called "ssl-cert-snakeoil":

```
postconf -e smtpd_tls_cert_file=/etc/ssl/certs/postfix.pem
postconf -e smtpd_tls_key_file=/etc/ssl/private/postfix.pem
```

Or: Use a free certification authority

    Advantage: a little work, no costs
    Disadvantage: these certification authorities are not included in all email clients
    Conclusion: if you don't want to spend money then this is your best chance

There are barely any free services like that. I have had good experience with StartSSL although their web site is sometimes confusing. Once you have created a key file and certificate then use these files as shown in the previous section about creating self-signed certificates.
Or: Buy an SSL certificate

    Advantage: certificate will be accepted automatically by the user's email program
    Disadvantage: you throw a lot of money at the certification mafia that doesn't deserve it
    Conclusion: do this if you will run a professional public mail server

Honestly I dislike any commercial certification authority I have been in contact with. So choose the lesser evil yourself.

Configurare Amavis, ClamAV si SpamAssassin

Inainte de a configura Postfix, putem sa dam un scurt tur in ceea ce inseamna configurarea instrumentelor antivirus si
antispam. Configurarile lor implicite sunt aproape de ceea ce majoritatea oamenilor au nevoie, iar instrumente precum
SpamAssassin auto-detecteaza majoritatea pachetelor suplimentare cat si optionale pe care le aveti instalate. Aici vom trata
o portiune referitoare la integrarea cu Postfix.

Mai intai adaugam Amavis si ClamAV la inca un grup, pentru a le permite sa colaboreze intre ele:

```
adduser clamav amavis
adduser amavis clamav
```

Apoi pornim Amavis prin editarea fisierului
/etc/amavis/conf.d/15-content_filter_mode - software-ul implicit este dezactivat
prin urmare vom decomenta liniile @bypass...:

```
use strict;

# You can modify this file to re-enable SPAM checking through spamassassin
# and to re-enable antivirus checking.

#
# Default antivirus checking mode
# Please note, that anti-virus checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:

@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);

#
# Default SPAM checking mode
# Please note, that anti-spam checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:

@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);

1;  # ensure a defined return
```

Acum vom activa SpamAssassin prin editarea urmatoarelor linii in fisierul
/etc/default/spamassassin:

```
# Change to one to enable spamd
ENABLED=1

# Cronjob
# Set to anything but 0 to enable the cron job to automatically update
# spamassassin's rules on a nightly basis
CRON=1
```

SpamAssassin under Amavis will only check mail that's determined to be arriving for local delivery. There are a couple of ways to tell Amavis which mails are for local delivery, but here we'll set it up to check the database set up by Postfix Admin. Edit /etc/amavis/conf.d/50-user to look like this:

```
use strict;

#
```

```
# Place your configuration directives here.  They will override those in
# earlier files.
#
# See /usr/share/doc/amavisd-new/ for documentation and examples of
# the directives you can use in this file
#

# Three concurrent processes. This should fit into the RAM available on an
# AWS micro instance. This has to match the number of processes specified
# for Amavis in /etc/postfix/master.cf.
$max_servers  = 3;

# Add spam info headers if at or above that level - this ensures they
# are always added.
$sa_tag_level_deflt  = -9999;

# Check the database to see if mail is for local delivery, and thus
# should be spam checked.
@lookup_sql_dsn = (
    ['DBI:mysql:database=mail;host=127.0.0.1;port=3306',
     'mail',
     'mailpassword']);
$sql_select_policy = 'SELECT domain from domain WHERE CONCAT("@",domain) IN (%k)';

# Uncomment to bump up the log level when testing.
# $log_level = 2;

#------------ Do not modify anything below this line -------------
1;  # ensure a defined return
```

Next make sure the ClamAV database is up to date by running freshclam. It should be:

```
freshclam
```

Va trebui sa restartam aceste procese, pentru a activa noua configuratie:

```
service clamav-daemon restart
service amavis restart
service spamassassin restart
```

Configurare Postfix

Postfix manevreaza mailurile de intrare via protocol SMTP, si fisierele lui de configurare trebuiesc setate sa
permita integrarea cu variate alte pachete pe care trebuie sa le instalam mai tarziu. La nivel inalt, dorim ca Postfix

sa dea mailurile de intrare catre verificatoarele de virusi si spam, inainte ca ele sa fie transmise catre Dovecot
si sa autentifice userii virtuali care s-ar conecta peste SMTP in vederea trimiterii de e-mail-uri.

Mai intai, vom crea pentru Postfix fisierele ce vor descrie unde sa gaseasca informatiile referitoare la useri si domenii.
De notat ca directiva "hosts" din aceste fisiere trebuie sa fie exact aceeasi ca si directiva "bind-directive" (bind-address)
din fisierul /etc/mysql/my.cnf. Daca o parte spune "localhost" si in alta parte se spune "127.0.0.1", atunci veti
constata ca Postfix nu se poate conecta la MySQL - ciudat dar adevarat.

Iata fisierele de care are nevoie Postfix, si pe care trebuie sa le creem:

Fisierul: /etc/postfix/mysql_virtual_alias_domainaliases_maps.cf

```
user = mail
password = mailpassword
hosts = 127.0.0.1
dbname = mail
query = SELECT goto FROM alias,alias_domain
  WHERE alias_domain.alias_domain = '%d'
  AND alias.address=concat('%u', '@', alias_domain.target_domain)
  AND alias.active = 1
```

Fisierul: /etc/postfix/mysql_virtual_alias_maps.cf

```
user = mail
password = mailpassword
hosts = 127.0.0.1
dbname = mail
table = alias
select_field = goto
where_field = address
additional_conditions = and active = '1'
```

Fisierul: /etc/postfix/mysql_virtual_domains_maps.cf

```
user = mail
password = mailpassword
hosts = 127.0.0.1
dbname = mail
table = domain
select_field = domain
where_field = domain
additional_conditions = and backupmx = '0' and active = '1'
```

Fisierul: /etc/postfix/mysql_virtual_mailbox_domainaliases_maps.cf

```
user = mail
password = mailpassword
hosts = 127.0.0.1
dbname = mail
query = SELECT maildir FROM mailbox, alias_domain
  WHERE alias_domain.alias_domain = '%d'
  AND mailbox.username=concat('%u', '@', alias_domain.target_domain )
  AND mailbox.active = 1
```

Fisierul: /etc/postfix/mysql_virtual_mailbox_maps.cf

```
user = mail
password = mailpassword
hosts = 127.0.0.1
dbname = mail
table = mailbox
select_field = CONCAT(domain, '/', local_part)
where_field = username
additional_conditions = and active = '1'
```

Acum, creati fisierul /etc/postfix/header_checks, care va contine cateva directive pentru eliminarea catorva antete, atunci
cand mailurile sunt relocate. Aceasta imbunatateste confidentialitatea pentru userii expeditori, prin aceea ca, de exemplu
ascunde adresa IP originala si identificatorul software-ului de e-mail. Acest fisier va fi referit in configuratia principala
a Postfix:

```
/^Received:/                IGNORE
/^User-Agent:/              IGNORE
/^X-Mailer:/                IGNORE
/^X-Originating-IP:/        IGNORE
/^x-cr-[a-z]*:/             IGNORE
/^Thread-Index:/            IGNORE
```

In cele ce urmeaza, este prezentat principalul fisier de configurare al Postfix, /etc/postfix/main.cf, care contine
o serie de alegeri complexe si optiuni despre cum mailurile sunt retransmise, si cum se comporta SMTP. Recomandam
insistent sa petreceti ceva timp citind cu atentie configuratia Postfix, deoarece aceasta este cea mai simpla cale
prin care puteti gresi in realizarea configurarii, ceea ce duce la un sever de mail nefunctional.

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version

# The first text sent to a connecting process.
smtpd_banner = $myhostname ESMTP $mail_name
biff = no
# appending .domain is the MUA's job.
```

```
append_dot_mydomain = no
readme_directory = no

# SASL parameters
# --------------------------------

# Use Dovecot to authenticate.
smtpd_sasl_type = dovecot
# Referring to /var/spool/postfix/private/auth
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
broken_sasl_auth_clients = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain =
smtpd_sasl_authenticated_header = yes

# TLS parameters
# --------------------------------

# Replace this with your SSL certificate path if you are using one.
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
# The snakeoil self-signed certificate has no need for a CA file. But
# if you are using your own SSL certificate, then you probably have
# a CA certificate bundle from your provider. The path to that goes
# here.
#smtpd_tls_CAfile=/path/to/ca/file
smtpd_use_tls=yes
smtp_tls_security_level = may
smtpd_tls_security_level = may
#smtpd_tls_auth_only = no
smtp_tls_note_starttls_offer = yes
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
#smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
#smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

# SMTPD parameters
# --------------------------------

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
# will it be a permanent error or temporary
unknown_local_recipient_reject_code = 450
# how long to keep message on queue before return as failed.
```

```
# some have 3 days, I have 16 days as I am backup server for some people
# whom go on holiday with their server switched off.
maximal_queue_lifetime = 7d
# max and min time in seconds between retries if connection failed
minimal_backoff_time = 1000s
maximal_backoff_time = 8000s
# how long to wait when servers connect before receiving rest of data
smtp_helo_timeout = 60s
# how many address can be used in one message.
# effective stopper to mass spammers, accidental copy in whole address list
# but may restrict intentional mail shots.
smtpd_recipient_limit = 16
# how many error before back off.
smtpd_soft_error_limit = 3
# how many max errors before blocking it.
smtpd_hard_error_limit = 12

# This next set are important for determining who can send mail and relay mail
# to other servers. It is very important to get this right - accidentally producing
# an open relay that allows unauthenticated sending of mail is a Very Bad Thing.
#
# You are encouraged to read up on what exactly each of these options accomplish.

# Requirements for the HELO statement
smtpd_helo_restrictions = permit_mynetworks, warn_if_reject
reject_non_fqdn_hostname, reject_invalid_hostname, permit
# Requirements for the sender details
smtpd_sender_restrictions = permit_sasl_authenticated, permit_mynetworks,
warn_if_reject reject_non_fqdn_sender, reject_unknown_sender_domain,
reject_unauth_pipelining, permit
# Requirements for the connecting server
smtpd_client_restrictions = reject_rbl_client sbl.spamhaus.org, reject_rbl_client
blackholes.easynet.nl, reject_rbl_client dnsbl.njabl.org
# Requirement for the recipient address. Note that the entry for
# "check_policy_service inet:127.0.0.1:10023" enables Postgrey.
smtpd_recipient_restrictions = reject_unauth_pipelining, permit_mynetworks,
permit_sasl_authenticated, reject_non_fqdn_recipient,
reject_unknown_recipient_domain, reject_unauth_destination, check_policy_service
inet:127.0.0.1:10023, permit
smtpd_data_restrictions = reject_unauth_pipelining

# require proper helo at connections
smtpd_helo_required = yes
# waste spammers time before rejecting them
smtpd_delay_reject = yes
disable_vrfy_command = yes

# General host and delivery info
# ----------------------------------
```

```
myhostname = mail.example.com
myorigin = /etc/hostname
mydestination = mail.example.com, localhost
#relayhost =
# If you have a separate web server that sends outgoing mail through this
# mailserver, you may want to add its IP address to the space-delimited list in
# mynetworks, e.g. as 111.222.333.444/32.
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
mynetworks_style = host

# This specifies where the virtual mailbox folders will be located.
virtual_mailbox_base = /var/vmail
# This is for the mailbox location for each user. The domainaliases
# map allows us to make use of Postfix Admin's domain alias feature.
virtual_mailbox_maps = mysql:/etc/postfix/mysql_virtual_mailbox_maps.cf,
mysql:/etc/postfix/mysql_virtual_mailbox_domainaliases_maps.cf
# and their user id
virtual_uid_maps = static:150
# and group id
virtual_gid_maps = static:8
# This is for aliases. The domainaliases map allows us to make
# use of Postfix Admin's domain alias feature.
virtual_alias_maps = mysql:/etc/postfix/mysql_virtual_alias_maps.cf,
mysql:/etc/postfix/mysql_virtual_alias_domainaliases_maps.cf
# This is for domain lookups.
virtual_mailbox_domains = mysql:/etc/postfix/mysql_virtual_domains_maps.cf

# Integration with other packages
# ---------------------------------------

# Tell postfix to hand off mail to the definition for dovecot in master.cf
virtual_transport = dovecot
dovecot_destination_recipient_limit = 1

# Use amavis for virus and spam scanning
content_filter = amavis:[127.0.0.1]:10024

# Header manipulation
# ---------------------------------------

# Getting rid of unwanted headers. See: https://posluns.com/guides/header-removal/
header_checks = regexp:/etc/postfix/header_checks
# getting rid of x-original-to
enable_original_recipient = no
```

Inca odata, daca utilizati un certificat SSL platit - si aveti un certificat CA generat de un provider, atunci va trebui sa

modificati aceste linii in fisierul: /etc/postfix/main.cf:

```
# Replace this with your SSL certificate path if you are using one.
smtpd_tls_cert_file=/path/to/my/cert.pem
smtpd_tls_key_file=/path/to/my/key.key
# The snakeoil self-signed certificate has no need for a CA file. But
# if you are using your own SSL certificate, then you probably have
# a CA certificate bundle from your provider. The path to that goes
# here.
#smtpd_tls_CAfile=/path/to/ca/file
```

Va trebui de asemenea sa adaugati cate ceva in fisierul /etc/postfix/master.cf, iar aici este intregul fisier, pentru
a fi cat mai clar, incluzand totodata si comentariile pachetului de instalare - ca si optiuni comentate:

```
#
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master").
#
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================

# SMTP on port 25, unencrypted.
smtp      inet  n       -       -       -       -       smtpd
#smtp      inet  n       -       -       -       1       postscreen
#smtpd     pass  -       -       -       -       -       smtpd
#dnsblog   unix  -       -       -       -       0       dnsblog
#tlsproxy  unix  -       -       -       -       0       tlsproxy

# SMTP with TLS on port 587. Currently commented.
#submission inet n       -       -       -       -       smtpd
#  -o syslog_name=postfix/submission
#  -o smtpd_tls_security_level=encrypt
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_enforce_tls=yes
#  -o
smtpd_client_restrictions=permit_sasl_authenticated,reject_unauth_destination,reject
#  -o smtpd_sasl_tls_security_options=noanonymous

# SMTP over SSL on port 465.
smtps     inet  n       -       -       -       -       smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_tls_auth_only=yes
```

```
  -o
smtpd_client_restrictions=permit_sasl_authenticated,reject_unauth_destination,reject
  -o smtpd_sasl_security_options=noanonymous,noplaintext
  -o smtpd_sasl_tls_security_options=noanonymous

#628       inet  n       -       -       -       -       qmqpd
pickup    fifo  n       -       -       60      1       pickup
  -o content_filter=
  -o receive_override_options=no_header_body_checks
cleanup   unix  n       -       -       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
#qmgr     fifo  n       -       n       300     1       oqmgr
tlsmgr    unix  -       -       -       1000?   1       tlsmgr
rewrite   unix  -       -       -       -       -       trivial-rewrite
bounce    unix  -       -       -       -       0       bounce
defer     unix  -       -       -       -       0       bounce
trace     unix  -       -       -       -       0       bounce
verify    unix  -       -       -       -       1       verify
flush     unix  n       -       -       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       -       -       -       smtp
relay     unix  -       -       -       -       -       smtp
#       -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix  n       -       -       -       -       showq
error     unix  -       -       -       -       -       error
retry     unix  -       -       -       -       -       error
discard   unix  -       -       -       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       -       -       -       lmtp
anvil     unix  -       -       -       -       1       anvil
scache    unix  -       -       -       -       1       scache
#
# ====================================================================
# Interfaces to non-Postfix software. Be sure to examine the manual
# pages of the non-Postfix software to find out what options it wants.
#
# Many of the following services use the Postfix pipe(8) delivery
# agent.  See the pipe(8) man page for information about ${recipient}
# and other message envelope options.
# ====================================================================
#
# maildrop. See the Postfix MAILDROP_README file for details.
# Also specify in main.cf: maildrop_destination_recipient_limit=1
#
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
#
# ====================================================================
```

```
#
# Recent Cyrus versions can use the existing "lmtp" master.cf entry.
#
# Specify in cyrus.conf:
#   lmtp    cmd="lmtpd -a" listen="localhost:lmtp" proto=tcp4
#
# Specify in main.cf one or more of the following:
#  mailbox_transport = lmtp:inet:localhost
#  virtual_transport = lmtp:inet:localhost
#
# ====================================================================
#
# Cyrus 2.1.5 (Amos Gouaux)
# Also specify in main.cf: cyrus_destination_recipient_limit=1
#
#cyrus     unix  -       n       n       -       -       pipe
#  user=cyrus argv=/cyrus/bin/deliver -e -r ${sender} -m ${extension} ${user}
#
# ====================================================================
# Old example of delivery via Cyrus.
#
#old-cyrus unix  -       n       n       -       -       pipe
#  flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} ${user}
#
# ====================================================================
#
# See the Postfix UUCP_README file for configuration details.
#
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
#
# Other external delivery methods.
#
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender $recipient
scalemail-backend unix  -       n       n       -       2       pipe
  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store ${nexthop}
${user} ${extension}
mailman   unix  -       n       n       -       -       pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}

# The next two entries integrate with Amavis for anti-virus/spam checks.
amavis      unix    -       -       -       -       3       smtp
  -o smtp_data_done_timeout=1200
  -o smtp_send_xforward_command=yes
  -o disable_dns_lookups=yes
  -o max_use=20
```

```
127.0.0.1:10025 inet    n       -       -       -       -       smtpd
  -o content_filter=
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_delay_reject=no
  -o smtpd_client_restrictions=permit_mynetworks,reject
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o smtpd_data_restrictions=reject_unauth_pipelining
  -o smtpd_end_of_data_restrictions=
  -o mynetworks=127.0.0.0/8
  -o smtpd_error_sleep_time=0
  -o smtpd_soft_error_limit=1001
  -o smtpd_hard_error_limit=1000
  -o smtpd_client_connection_count_limit=0
  -o smtpd_client_connection_rate_limit=0
  -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks

# Integration with Dovecot - hand mail over to it for local delivery, and
# run the process under the vmail user and mail group.
dovecot      unix   -        n      n       -       -   pipe
  flags=DRhu user=vmail:mail argv=/usr/lib/dovecot/dovecot-lda -d $(recipient)
```

De mentionat ca Amavis este restrictionat la doua procese ceea ce poate fi bine pentru cele mai multe utilizari medii.
Procesele sunt memory-heavy, astfel incat pornesc incet, si adauga mai mult daca avem nevoie, in cazul unui volum mai
mare de mailuri.

Restart totul si testati serverul

Restartati toate procesele necesare pentru a incarca noile configurari:

```
service postfix restart
service spamassassin restart
service clamav-daemon restart
service amavis restart
service dovecot restart
```

Acum incepeti sa testati! Uitati-va de fiecare data in fisierele cu mesaje de eroare, /var/log/mail.err si
/var/log/mail.log si incercati sa va logati cu POP si IMAP, sa trimiteti mailuri catre un cont creat pe server, si
sa trimiteti mailuri de la server. Daca intalniti probleme, atunci Google poate fi un bun prieten, pentru a gasi subiecte
referitoare la un mesaj specifica de eroare in vederea identificarii a ceea ce este

gresit.

Restrictiile AWS Mail si interogarile DNS inverse (Reverse)

Odata serverul configurat, cu adresa de IP setata, precum si inregistrarile DNS configurate, va trebui sa faceti o cautare
DNS inversa cu privire la serverul de mail, precum si sa ridicati restrictiile de iesire AWS. Puteti face acest lucru,
completand formularul standard de servicii pentru clienti. Aceasta nu ia mult timp, si poate avea loc, daca este necesar,
înainte de finalizarea serverului.

Trebuie sa modific ceva pentru Postgrey in fisierul /etc/default/postgrey pentru a arata precum:

POSTGREY_OPTS="--inet=127.0.0.1:10023"

o alta varianta in care schimb si intarzierea implicita care este de 300 de secunde (5 minute), este:

POSTGREY_OPTS="--inet=127.0.0.1:10023 --delay=60"

Odata ce Postgrey ruleaza, intrarile vor incepe sa apara in /var/log/mail.log. Pentru a le vedea putem rula:
sudo grep -i greylisted /var/log/mail.log

Intrarile vor trebui sa arate asemanator cu ceea ce prezentam mai jos:

Sep 14 10:44:57 mailserver postfix/smtpd[17049]: NOQUEUE: reject: RCPT from mail.server.com[1.2.3.4]: 450
<someone@somedomain.com>: Recipient address rejected: Greylisted for 300 seconds (see
http://isg.ee.ethz.ch/tools/postgrey/help/somedomain.com.html);
from=<someone.else@anotherdomain.com> to=<someone@somedomain.com> proto=ESMTP helo=<mail.server.com>

In plus, e-mailurile care au fost greylisted vor avea un antet X-Greylist, de exemplu:

X-Greylist: delayed 1201 seconds by postgrey-1.24 at mail.server.com; Fri, 14 Sep 2007 11:04:58 BST

Instalare SquirrelMail ca si aplicatie pentru WebMail

Instalare:
apt-get update
apt-get upgrade
apt-get install squirrelmail squirrelmail-locales php-pear php5-cli
apt-get clean

Puteti utiliza si https://help.ubuntu.com/community/Squirrelmail pentru mai multe informatii.

Veti avea nevoie sa permiteti accesul web in firewall Verificati configuratia acestuia daca este necesar.

Va trebui sa copiati configuratia fisierului pentru SquirrelMail in cadrul Apache:
sudo cp /etc/squirrelmail/apache.conf /etc/apache2/sites-available/squirrelmail

si sa o activati cu:
sudo ln -s /etc/apache2/sites-available/squirrelmail
/etc/apache2/sites-enabled/500-squirrelmail

sau si mai bine cu:
sudo a2ensite squirrelmail

Puteti accepta configuratia Apache implicita, unde squirrelmail este un folder in cadrul fiecarui site.
Dar, eu prefer configuratia pentru hosturi virtuale.
sudo vi /etc/apache2/sites-available/squirrelmail

Comment out the alias.
alias /squirrelmail /usr/share/squirrelmail

Decomentati setarea virtual settings., si inserati numele serverului

users will prefer a simple URL like http://webmail.example.com
DocumentRoot /usr/share/squirrelmail
ServerName webmail.example.com

Daca aveti activat modulul SSL, atunci puteti deasemenea decomenta si sectiunea mod_rewrite section pentru securitate
suplimentara.

Restartati apache pentru a activa modificarile. Mai intat testati daca totul este OK.
sudo apache2ctl -t

Apoi restartati:
sudo /etc/init.d/apache2 reload

Mergeti apoi la yourdomain.com/squirrelmail/ sau mail.yourdomain.com daca ati ales hosturile virtuale. Aceasta
va va duce pe pagina web a squirrel. Logati-va Log si incepeti configurarea.

sudo squirrelmail-configure

La inceput nu schimbati nimic. Veti customiza mai multe mai tarziu. Puteti naviga si iesi din submeniuri tastand R.
Tastati 2 pentru a edita setarile serverului Tastati A pentru setari IMAP.
Tastati 8 pentru a edita software-ul de server - Courier / Dovecot, etc

Acum cei ce spun ca utilizarea TLS peste localhost este pierdere de vreme. Dar o vom face oricum.
Tastati 7 pentru a edita IMAP securizat. Tastati Y pentru a activa asta.
Tastati 5 pentru a edita portul IMAP. Introduceti 993.
Tastati S pentru salvare, si apoi ENTER.
Tastati Q pentru iesire.

Puteti merge acum la yourdomain.com/squirrelmail/ sau mail.yourdomain.com daca ati ales configurarea ca si host virtual.
Asta va va duce pe pagina web a squirrel. Logarea va functiona acum (exceptie facand cazul in care nu ati setat inca
userii de mail).

Alta descriere:

Instalare SquirrelMail:
apt-get update
apt-get upgrade
apt-get install squirrelmail squirrelmail-locales php-pear php5-cli
apt-get clean

Apoi configuram SquirrelMail:
sudo squirrelmail-configure

Trebuie sa-i spunem lui SquirrelMail ce anume utilizam Dovecot-IMAP/-POP3:

SquirrelMail Configuration : Read: config.php (1.4.0)

Main Menu --
1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

D. Set pre-defined settings for specific IMAP servers

```
C   Turn color on
S   Save data
Q   Quit

Command >> <-- D

SquirrelMail Configuration : Read: config.php
---------------------------------------------------------
While we have been building SquirrelMail, we have discovered some
preferences that work better with some servers that don't work so
well with others.  If you select your IMAP server, this option will
set some pre-defined settings for that server.

Please note that you will still need to go through and make sure
everything is correct.  This does not change everything.  There are
only a few settings that this will change.

Please select your IMAP server:
    bincimap    = Binc IMAP server
    courier     = Courier IMAP server
    cyrus       = Cyrus IMAP server
    dovecot     = Dovecot Secure IMAP server
    exchange    = Microsoft Exchange IMAP server
    hmailserver = hMailServer
    macosx      = Mac OS X Mailserver
    mercury32   = Mercury/32
    uw          = University of Washington's IMAP server
    gmail       = IMAP access to Google mail (Gmail) accounts

    quit        = Do not change anything
Command >> <-- dovecot

SquirrelMail Configuration : Read: config.php
---------------------------------------------------------
While we have been building SquirrelMail, we have discovered some
preferences that work better with some servers that don't work so
well with others.  If you select your IMAP server, this option will
set some pre-defined settings for that server.

Please note that you will still need to go through and make sure
everything is correct.  This does not change everything.  There are
only a few settings that this will change.

Please select your IMAP server:
    bincimap    = Binc IMAP server
    courier     = Courier IMAP server
    cyrus       = Cyrus IMAP server
    dovecot     = Dovecot Secure IMAP server
    exchange    = Microsoft Exchange IMAP server
```

```
    hmailserver = hMailServer
    macosx      = Mac OS X Mailserver
    mercury32   = Mercury/32
    uw          = University of Washington's IMAP server
    gmail       = IMAP access to Google mail (Gmail) accounts

    quit        = Do not change anything
Command >> dovecot

              imap_server_type = dovecot
         default_folder_prefix = <none>
                  trash_folder = Trash
                   sent_folder = Sent
                  draft_folder = Drafts
            show_prefix_option = false
          default_sub_of_inbox = false
show_contain_subfolders_option = false
             optional_delimiter = detect
                  delete_folder = false

Press any key to continue... <-- press a key

SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> <-- S

Tastati 2 pentru a edita setarile serverului Tastati A pentru setari IMAP.
Tastati 8 pentru a edita software-ul de server - Courier / Dovecot, etc

Acum cei ce spun ca utilizarea TLS peste localhost este pierdere de vreme. Dar o vom
face oricum.
Tastati 7 pentru a edita IMAP securizat. Tastati Y pentru a activa asta.
```

Tastati 5 pentru a edita portul IMAP. Introduceti 993.
Tastati S pentru salvare, si apoi ENTER.

SquirrelMail Configuration : Read: config.php (1.4.0)

Main Menu --
1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

D. Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> <-- Q

Tot la aceste configurari, intrand in 8. Plugins, pot sa activez vizualizarea si utilizarea Calendarului.

Acum vom configura SquirrelMail astfel incat sa-l utilizam in cadrul site-ului nostru web utilizand /squirrelmail
sau /webmail aliases. De exemplu daca site-ul web este www.example.com, veti fi capabil sa accesati SquirrelMail
utilizand www.example.com/squirrelmail sau www.example.com/webmail.

Configuratia apache pentru SquirrelMail se gaseste in fisierul /etc/squirrelmail/apache.conf, dar acest fisier nu este
incarcat de Apache deoarece el nu este in directorul /etc/apache2/conf.d/. Vom crea un symlink numit squirrelmail.conf in
directorul /etc/apache2/conf.d/ care indica catre /etc/squirrelmail/apache.conf apoi restartam Apache.

```
cd /etc/apache2/conf.d/
ln -s ../../squirrelmail/apache.conf squirrelmail.conf
/etc/init.d/apache2 reload
```

Deschidem: /etc/apache2/conf.d/squirrelmail.conf

vi /etc/apache2/conf.d/squirrelmail.conf

... si adaugam urmatoarele linii in <Directory /usr/share/squirrelmail></Directory>
care ne asigura ca mod_php este
utilizat pentru accesarea SquirrelMail, privitor la ce mod PHP am selectat pentru
site-ul web:

```
[...]
<Directory /usr/share/squirrelmail>
  Options FollowSymLinks
  <IfModule mod_php5.c>
    AddType application/x-httpd-php .php
    php_flag magic_quotes_gpc Off
    php_flag track_vars On
    php_flag register_globals off
    php_value include_path .
    php_admin_flag allow_url_fopen Off
    php_admin_value upload_tmp_dir /var/lib/squirrelmail/tmp
    php_admin_value open_basedir
/usr/share/squirrelmail:/etc/squirrelmail:/var/lib/squirrelmail:/etc/hostname:/etc/m
ailname:/var/spool/squirrelmail
  </IfModule>
  <IfModule mod_dir.c>
    DirectoryIndex index.php
  </IfModule>
  # access to configtest is limited by default to prevent information leak
  <Files configtest.php>
    order deny,allow
    deny from all
    allow from 127.0.0.1
  </Files>
</Directory>
[...]
```

Creem folderul: /var/lib/squirrelmail/tmp

```
mkdir /var/lib/squirrelmail/tmp
```

... asi-l facem sa fie detinut de www-data:

```
chown www-data /var/lib/squirrelmail/tmp
```

Restartam Apache:

```
/etc/init.d/apache2 reload
```

E deja gata" - /etc/apache2/conf.d/squirrelmail.conf defineste un alias numit
/squirrelmail care indica catre folderul de
instalare al SquirrelMail si anume /usr/share/squirrelmail.

Daca la incercarea de a trimite mailuri,daca la receptionarea lor, acestea nu ajung
in casuta, iar daca ma uit la
loguri (/var/log/email.info) vad ca imi da eroare de conectare la POSTGREY la

127.0.0.1:10023, atunci ar trebui si
sa restartez serverul cu totul...
Apoi ar trebui sa mearga. Oricum la receptionarea mailurilor pentru prima data
acestea vor fi rejectate, urmand ca
apoi sa fie acceptate.

Putem sa accesam astfel:
http://192.168.0.100/squirrelmail
http://www.example.com/squirrelmail

Daca dorim sa utilizam aliasul /webmail in loc de /squirrelmail, deschidem
/etc/apache2/conf.d/squirrelmail.conf...
vi /etc/apache2/conf.d/squirrelmail.conf

... si adaugam linia: Alias /webmail /usr/share/squirrelmail:

```
Alias /squirrelmail /usr/share/squirrelmail
Alias /webmail /usr/share/squirrelmail
[...]
```

Apoi restartam Apache:
/etc/init.d/apache2 reload

Acum putem accesa Squirrelmail:
http://192.168.0.100/webmail
http://www.example.com/webmail

Daca dorim sa definim un virtual host precum webmail.example.com trebuie sa adaugam
urmatoarele in fisierul:
/etc/apache2/conf.d/squirrelmail.conf:

vi /etc/apache2/conf.d/squirrelmail.conf

```
[...]
<VirtualHost 1.2.3.4:80>
  DocumentRoot /usr/share/squirrelmail
  ServerName webmail.example.com
</VirtualHost>
```

Asigurati-va ca inlocuiti 1.2.3.4 cu IP-ul corect al serverului. Bineintelesva
trebui sa existe o inregistrare DNS pentru
webmail.example.com care sa indice catreconfiguratia virtual host.

Reincarcati Apache...

/etc/init.d/apache2 reload

... si accesati SquirrelMail la:
http://webmail.example.com

Eu am creat fisierul /etc/apache2/sites-available/squirrel-ssl care arata astfel (acesta l-am avut prima data,
pentru ca apoi sa modific folosind varianta 2 - vezi-o mai jos!)

```
## Virtual Host for SquirrelMail
<VirtualHost *:443>
        ServerName cladwmsx.cursuriladistanta.ro
        ServerAdmin sysadmin@cursuriladistanta.ro
        DocumentRoot /usr/share/squirrelmail

        RewriteEngine On
        RewriteCond %{HTTP_HOST} !cladwmsx.cursuriladistanta.ro
        RewriteRule (.*) [L]

        <Directory /usr/share/squirrelmail/>
                Options +FollowSymLinks -Indexes
                DirectoryIndex index.php
                AllowOverride None
                <IfModule mod_php5.c>
                        AddType application/x-httpd-php .php
                        php_flag magic_quotes_gpc Off
                        php_flag track_vars On
                        php_flag register_globals Off
                        php_value include_path .
                </IfModule>
        </Directory>

        # access to configtest is limited by default to prevent information leak
        <Files configtest.php>
                order deny,allow
                deny from all
                allow from 127.0.0.1
        </Files>

        # SSL Engine Switch: Enable/Disable SSL for this virtual host.
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/webcert.crt
        SSLCertificateKeyFile /etc/apache2/ssl/webcert.key

        ErrorLog ${APACHE_LOG_DIR}/error.log
        # Possible values include: debug, info, notice, warn, error, crit, alert,
emerg.
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined
</VirtualHost>
```

Varianta 2 (Acum pe aceasta o am configurata:)

```
## Virtual Host for SquirrelMail
<VirtualHost *:443>
        ServerName cladwmsx.cursuriladistanta.ro
        ServerAdmin sysadmin@cursuriladistanta.ro
        DocumentRoot /usr/share/squirrelmail

        RewriteEngine On
        RewriteCond %{HTTP_HOST} !cladwmsx.cursuriladistanta.ro
        RewriteRule (.*) [L]

        <Directory /usr/share/squirrelmail/>
                Options +FollowSymLinks -Indexes
                DirectoryIndex index.php
                AllowOverride None
                <IfModule mod_php5.c>
                        AddType application/x-httpd-php .php
                        php_flag magic_quotes_gpc Off
                        php_flag track_vars On
                        php_flag register_globals Off
                        php_value include_path .
                        php_admin_flag allow_url_fopen Off
                        php_admin_value upload_tmp_dir /var/lib/squirrelmail/tmp
                        php_admin_value open_basedir
/usr/share/squirrelmail:/etc/squirrelmail:/var/lib/squirrelmail:/etc/hostname:/etc/m
ailname:/var/spool/squirrelmail
                </IfModule>

                <IfModule mod_dir.c>
                        DirectoryIndex index.php
                </IfModule>

                # access to configtest is limited by default to prevent information
leak
                <Files configtest.php>
                        order deny,allow
                        deny from all
                        allow from 127.0.0.1
                </Files>
        </Directory>

        # SSL Engine Switch: Enable/Disable SSL for this virtual host.
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/webcert.crt
        SSLCertificateKeyFile /etc/apache2/ssl/webcert.key

        ErrorLog ${APACHE_LOG_DIR}/error.log
        # Possible values include: debug, info, notice, warn, error, crit, alert,
emerg.
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined
```

</VirtualHost>

Pentru a mari dimensiunea fisierului care se ataseaza la mailuri:

AttachmentSize
DocumentationHome | RecentChanges | Preferences
Uploading the attachment to the server

Limitations in PHP

PHP sets limits on the maximum files size when uploading files to the server. To change this limit, you need to edit the php.ini configuration file. The values you will need to increase or decrease are:

```
    [memory_limit]                              <--- Am setat 256M  ... Default era 128M
    [post_max_size]                             <--- Am setat 30M
    [upload_max_filesize]               <--- Am setat 28M   ... Aceasta este suma fisierelor ce pot fi atasate in squirrelmail
```

The values can be set in bytes (1,048,576 per MB) or they can be set by MB by appending the value with an "M", i.e. 8M.

To upload large files, post_max_size must be larger than upload_max_filesize. If memory limit is enabled by configure script, memory_limit also affects file uploading. Generally speaking, memory_limit should be larger than post_max_size. [1]

There is also more information to be found in the PHP documentation about [handling file uploads].

Limitations in the web server

The HTTP server may add further restrictions on the file upload size:

    Apache: You can restrict maximum file size using [LimitRequestBody] directive. Search for /etc/httpd/conf.d/php.conf and comment out LimitRequestBody. Restart Apache after editing the configuration and you will be able to attach file with sizes over 0,5 MB again.

```
<Files *.php>
    SetOutputFilter PHP
    SetInputFilter PHP
#    LimitRequestBody 524288
</Files>
```

Limitation in web proxies

Pay attention if you use any proxy server like Squid. In Squid, you need to change

the request_body_max_size (the default is 1 MB), e.g: request_body_max_size 10 MB

In some versions of Squid this is called request_size rather than
request_body_max_size.
Sending the mail with the attachment

You should also take into account limits for your MTA software:

Courier-MTA: showconfig or /etc/courier/sizelimit - default 10MBytes
Postfix: a configuration parameter called message_size_limit in the file
/etc/postfix/main.cf sets the maximum size (in bytes) of the entire message -
default: 10240000 - i.e. approximately 10MBytes
Qmail-MTA: a file in /var/qmail/control called databytes. The file contains one line
that represents the max size of attachments in bytes.
Sendmail: option MaxMessageSize, usually unset; can be changed in mc file
define(`confMAX_MESSAGE_SIZE',`5242880')dnl
hMail: !Max message size (KB) in Settings > Protocols > SMTP

Reguli IPTABLES pentru a permite e-mailing:

```
iptables -A INPUT -i eth0 -p tcp -s 192.168.100.0/24 --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
```

sau:

```
iptables -A INPUT -p tcp -s 127.0.0.1 --dport 10023 -j ACCEPT
```

Postgrey foloseste portul 10023, insa nu e nevoie sa introduc o astfel de regula.

Am nevoie, in schimb de urmatoarele:

```
iptables -A INPUT -p tcp --dport 25 -j ACCEPT                          <-- SMTP
iptables -A INPUT -p tcp --dport 465 -j ACCEPT                         <-- SMTPS
iptables -A INPUT -p tcp --dport 143 -j ACCEPT                         <-- IMAP
iptables -A INPUT -p tcp --dport 993 -j ACCEPT                         <-- IMAPS
iptables -A INPUT -p tcp --dport 110 -j ACCEPT                         <-- POP3
iptables -A INPUT -p tcp --dport 995 -j ACCEPT                         <-- POP3S
```

sau:

```
iptables -A OUTPUT -o eth0 -p tcp --sport 25 -m state --state ESTABLISHED -j ACCEPT
```

sau

```
iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -m multiport --sports 22,80,443 -m state --state
ESTABLISHED -j ACCEPT
```

sau:

```
iptables -A INPUT -p tcp -m multiport --dports 25,143,993,110,995 -j ACCEPT
     <--- Asta am aplicat-o
iptables -A OUTPUT -o eth0 -p tcp -m multiport --sports 22,80,443 -m state --state
ESTABLISHED -j ACCEPT

21. Allow IMAP and IMAPS
The following rules allow IMAP/IMAP2 traffic.
iptables -A INPUT -i eth0 -p tcp --dport 143 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 143 -m state --state ESTABLISHED -j ACCEPT
The following rules allow IMAPS traffic.
iptables -A INPUT -i eth0 -p tcp --dport 993 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 993 -m state --state ESTABLISHED -j ACCEPT

22. Allow POP3 and POP3S
The following rules allow POP3 access.
iptables -A INPUT -i eth0 -p tcp --dport 110 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 110 -m state --state ESTABLISHED -j ACCEPT
The following rules allow POP3S access.
iptables -A INPUT -i eth0 -p tcp --dport 995 -m state --state NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 995 -m state --state ESTABLISHED -j ACCEPT

-----------------------------------------------

Setari clienti mail:

- Thunderbird:
Pentru a citi mailurile - prin IMAP:
In cadrul Server Settings:
Server Name: Adresa FQDN a serverului de mail
Port: 143
User Name: florin.dena@inovatop.ro    <----- Atentie ca aici Thunderbird nu pune
domeniul - Il completez eu si
il corelez cu Account name si email address
Connection Security: STARTTLS
Authentication method: Normal password
------
Pentru a citi mailurile - prin IMAPS:
In cadrul Server Settings:
Server Name: Adresa FQDN a serverului de mail
Port: 993
User Name: florin.dena@inovatop.ro    <----- Atentie ca aici Thunderbird nu pune
domeniul - Il completez eu si
il corelez cu Account name si email address
Connection Security: SSL/TLS
Authentication method: Normal password
------
```

Pentru a citi mailurile - prin POP3:
In cadrul Server Settings:
Server Name: Adresa FQDN a serverului de mail
Port: 110
User Name: florin.dena@inovatop.ro   <----- Atentie ca aici Thunderbird nu pune domeniul - Il completez eu si
il corelez cu Account name si email address
Connection Security: STARTTLS
Authentication method: Normal password

Pentru a citi mailurile - prin POP3S:
In cadrul Server Settings:
Server Name: Adresa FQDN a serverului de mail
Port: 995
User Name: florin.dena@inovatop.ro   <----- Atentie ca aici Thunderbird nu pune domeniul - Il completez eu si
il corelez cu Account name si email address
Connection Security: SSL/TLS
Authentication method: Normal password

Pentru setarea serverului SMTP - se creeaza datele de conectare pentru fiecare cont.
La Accont Settings:
User Name: florin.dena@inovatop.ro
Server Name: invtmtax.inovatop.ro
Port: 465
Connection Scurity: SSL/TLS
Normal password.

Pentru a seta un cont sa mearga in Outlook, trebuie sa urmezi pasii:
- Tools --> Options --> Mail Setup --> E-Mail Accounts
1. Aici daca contul nu exista, alegi New... sau daca contul exista, il selectezi si alegi Change...
Daca ai ales sa creezi un cont nou (New...), ajungi in fereastra Add New E-mail Account, bifezi Microsoft Exchange, POP3, IMAP, or HTTP, apoi Next >
In fereastra urmatoare bifezi jos Mannually configure server settings or additional server types, si apoi Next >
In fereastra urmatoare alegi Internet E-mail, apoi Next >
Si ajungi la aceeasi fereastra la care ai fi ajuns la pasul 1 daca in loc de New... ai fi ales Change...
2. Exemplu de setare in aceasta fereastra:
Your Name: SysAdmin
E-Mail Address: sysadmin@druckfarben.ro
Account Type: POP3
Incoming Mail Server: dkfbmtax.druckfarben.ro
Outgoing Mail Server (SMTP): dkfbmtax.druckfarben.ro
User name: sysadmin@druckfarben.ro
Password: bla,bla
Bifezi Remember Password (Asta face ca omuletul sa nu introduca parola de fiecare data dimineata cand porneste Outlook-ul)

Bifezi Require logon using Secure Password Authentication (SPA) - Asta face ca parola intre client si server sa plece criptat.
Apesi apoi butonul More Settings, si in fereastra Internet E-Mail Settings, faci urmatoarele setari:
In tabul General:
Numele contului: sysadmin@druckfarben.ro
Organization: Druckfarben Romania
Reply E-Mail: sysadmin@druckfarben.ro
In tabul Outgoing Server:
Bifezi My outgoing server (SMTP) requires authentication (Asta face ca nimeni sa nu poata sa trimita mail prin server fara sa fie autentificat prin user si parola).
Bifezi Use same settings as my incoming mail server
In tabul Connection:
Connect using my local area network (LAN)
In tabul Advanced:
Bifezi This server requires an encripted connection (SSL) <--- Asta va schimba automat deasupra porul din 110 in 995, prin urmare toate mesajele intre client si server vor circula criptat si nu in clar.
La Outgoing server port, setezi 25
La Use the following type of encrypted connection, alegi TLS
Bifezi: Leave a copy of mesages on the server
Bifezi: Remove from server after: si alegi 60 zile (sau poate mai putin la unii dintre ei)
Apoi apesi OK, si revii la fereastra anterioara si acolo testezi apasand butonul: Test Account Settings ...
Si totul ar trebui sa fie OK.
Acestea ar fi setarile pentru Outlook in cazul POP3S (POP3 securizat). Ele ofera o securitate foarte buna atat pentru mailuri cat si pentru server.
De asemenea, pot exista si alte combinatii, gen POP3 nesecurizat, IMAP sau IMAPS.
Insa, e bine sa mergi pe cele descrise mai sus.

Iata aici si setarile pentru Thunderbird. Eu am setat acasa pe calculatorul meu un Thunderbird pe POP3 si a mers foarte bine.
Pentru setarea serverului SMTP - se creeaza datele de conectare pentru fiecare cont.
La Accont Settings:
User Name: denumire_user@druckfarben.ro
Server Name: dkfbmtax.druckfarben.ro
Port: 465
Connection Security: SSL/TLS
Normal password.

SETARI Thunderbird:
Din meniul de sus: TOOLS --> Account Settings...
Pentru Server:
In stanga la Outgoing Server (SMTP):
Aleg in dreapta: Add..., si in fereastra SMTP Server:
Description: Druckfarben New Mail Server

Server Name: dkfbmtax.druckfarben.ro
Port: 465 (465 este pentru SMTPS, altfel 25)
Connection Security: SSL/TLS
Authentication method: Normal Password
User Name: florin.dena@druckfarben.ro
Apoi OK
Pentru setarea contului de e-mail:
Din meniul de sus: TOOLS --> Account Settings...
In stanga la Account Actions aleg Add Mail Account...
Se deschide fereastra Mail Account Setup... si acolo completez:
Your name: Florin Dena
E-mail address: florin.dena@druckfarben.ro
Password: bla,bla
Bifez Remember password, apoi apas Continue si incearca sa se conecteze...
si esueaza urmand sa afiseze mai multe detalii:
De exemplu:
Pentru a citi mailurile - prin IMAP:
In cadrul Server Settings:
Server Name: Adresa FQDN a serverului de mail (dkfbmtax.druckfarben.ro)
Port: 143
User Name: (dkfbmtax.druckfarben.ro)   <----- Atentie ca aici Thunderbird nu pune domeniul - Il completez eu si il corelez cu Account name si email address
Connection Security: STARTTLS
Authentication method: Normal password

Pentru a citi mailurile - prin IMAPS:
In cadrul Server Settings:
Server Name: Adresa FQDN a serverului de mail (dkfbmtax.druckfarben.ro)
Port: 993
User Name: denumire_user@druckfarben.ro   <----- Atentie ca aici Thunderbird nu pune domeniul - Il completez eu si il corelez cu Account name si email address
Connection Security: SSL/TLS
Authentication method: Normal password

Pentru a citi mailurile - prin POP3:
In cadrul Server Settings:
Server Name: Adresa FQDN a serverului de mail (dkfbmtax.druckfarben.ro)
Port: 110
User Name: denumire_user@druckfarben.ro   <----- Atentie ca aici Thunderbird nu pune domeniul - Il completez eu si il corelez cu Account name si email address
Connection Security: STARTTLS
Authentication method: Normal password

Pentru a citi mailurile - prin POP3S:
In cadrul Server Settings:
Server Name: Adresa FQDN a serverului de mail (dkfbmtax.druckfarben.ro)
Port: 995

User Name: denumire_user@druckfarben.ro   <----- Atentie ca aici
Thunderbird nu pune domeniul - Il completez eu si
il corelez cu Account name si email address
Connection Security: SSL/TLS
Authentication method: Normal password

Inainte de a incepe sa faceti orice modificare aveti nevoie sa urmati cativa pasi in cateva fisiere externe.
(Sau cel putin inainte de a incepe sa facem testele).

Numele de domeniu:

Avem nevoie de un nume de domeniu pe care sa-l utilizam cu serverul nostru de e-mail. Acesta poate fi unul cumparat
sau un subdomeniu la unul existent sau unul dinamic, de exemplu, dyndns.org.

DNS

Avem nevoie de asemenea sa configuram inregistrarea MX a DNS-ului pentru acest server. Providerul tau poate sa te lase
sa faci asta prin intermediul unui GUI dar in acest caz cum ar arata asta:
domain.tld   IN   MX   10   yourmailserver.domain.tld

(Inlocuiti domain.tld cu numele tau de domeniu si yourmailserver.domain.tld cu numele complet al serverului de mail.
Repetati asta pentru fiecare domeniu pe care serverul il va administra.

Este posibil ca intrarile mx sa fie in acelasi fisier, daca exista subdomenii. Si totodata puteti sa aveti servere MX
de backup.

Nota: Alte sisteme de mail, vor verifica dupa reverse DNS pentru potrivire intre adresa de IP si numele de domeniu al
serverului de mail, ca si parte a scorului in ceea ce priveste evaluarea spam-urilor.

INSTALARE Roundcube for Webmail

Roundcube is a straightforward PHP webmail package: if all you need is simply to send and receive mail via a web interface then this is for you. There are other, more complex, extensible, and full-featured options out there but you pay the price for that in the time taken to install and configure the package. Roundcube is a much less onerous experience, but unfortunately the installation instructions you'll find online on how to install Roundcube are, shall we say, somewhat confused. They will largely lead you down the wrong path if working from a package install on Ubuntu. Here instead is the quick and easy way to manage things.

apt-get update
apt-get install php5-ldap

```
apt-get install php5-intl
service apache2 restart
apt-get clean
php -m
```

Mai intai creez o baza de date in mysql pentru roundcube, cu un user si o parola. Altfel in cazul in care am schimbat numele root-ului la instalare automata a acestei baze de date de catre kitul de instalare, va da eroare.

RoundCube Webmail is a free and open source Webmail with browser-based multilingual IMAP client packed with plenty of AJAX goodness. RoundCube Webmail comes with an application-like user interface and provides full functionality you expect from an email client, address book, folder manipulation, including MIME support, message searching and spell checking.

The Roundcube application is a Webmail application so you need an email account to log in to it.

The objective of this article is to provide you with an understanding of installation and configuration of the RoundCube Webmail.
Install RoundCube Webmail on Ubuntu
Step 1 :Install Prerequisites

Before get started install RoundCube Webmail, you need to install a web server on Ubuntu (Apache, PHP, MySQL) called LAMP server, open terminal then running following commands:

```
sudo apt-get install lamp-server^
```

After installing LAMP Server on ubuntu/Linux mint, you can now follow these instructions to install Roundcube Webmail on Ubuntu:
Step 2 : Creating A MySQL Database & User

Open the terminal and run this command to log in to MySQL server (use the MySQL password you have entered during the installation of the LAMP Server):

```
mysql -u root -p
```

Create a database for Roundcube Webmail.

```
create database roundcubedb;
```

Create MySQL user adminstrator of Roundcube Webmail.

```
create user adminmail;
```

Now Give user: admim123 a password

```
set password for 'adminmail' = password('admin123');
```

set privileges usercube to access database roundcubedb using this command:

grant all privileges on roundcubedb.* to adminmail@localhost

Now, Exit from MySQL server,by typing command:

FLUSH PRIVILEGES;
exit

Step 3: Installing Roundcube Webmail

In this case Roundcube Webmail will be installed in the directory /var/www/webmail. Download and extract archieve Roundcube Webmail to directory /var/www/webmail

cd /tmp && wget
http://sourceforge.net/projects/roundcubemail/files/roundcubemail/1.0.5/roundcubemail-1.0.5.tar.gz/download
sudo tar -xzvf roundcubemail-1.0.5.tar.gz -C /var/www
sudo mv /var/www/roundcubemail-1.0.5/ /var/www/webmail

change ownership directory /var/www/webmail/ to user and group www-data (www-data is user and group web server)

sudo chown -R www-data:www-data /var/www/webmail/*
sudo chown -R www-data:www-data /var/www/webmail/

Import database RoundCube to mysql server, login to mysql server then typing these command

mysql -u root -p roundcubedb < /var/www/webmail/SQL/mysql.initial.sql

To start the installation of Roundcube, open chrome or firefox browser, on address bar type :

http://server-ipaddress/webmail/installer/

This is screenshot page installer Roundcube Webmail

If all required modules and extensions are installed, press Continue and go to the next step

Enter your own configuration you want to use (SMTP & IMAP settings, etc.). If you want to log into your Gmail account with Roundcube Webmail, you can check this page for Gmail SMTP & IMAP settings. Don’t forget to fill your MySQL database details you have already created:

After Installation Roundcube Webmail complete, remove the directory /var/www/webmail/installer:

sudo rm -rf /var/www/webmail/installer

Roundcube Webmail ready to use, Access Roundcube Webmail via browser (http://localhost/webmail/) then sign in using your email (Gmail, Yahoo, etc.)

Done. RoundCube Webmail with browser-based now available on your ubuntu server.

Enjoy !

==========

Exemplu de fisier: /etc/apache2/sites-available/roundcube-ssl

```
## Virtual Host for RoundCube
# Those aliases do not work properly with several hosts on your apache server
# Uncomment them to use it or adapt them to your configuration
#    Alias /roundcube/program/js/tiny_mce/ /usr/share/tinymce/www/
#    Alias /roundcube /var/lib/roundcube

<VirtualHost *:443>
        ServerName anpmwmsx.anpmr.ro
        ServerAdmin sysadmin@anpmr.ro
        DocumentRoot /var/www/roundcube

        RewriteEngine On
        RewriteCond %{HTTP_HOST} !anpmwmsx.anpmr.ro
        RewriteRule (.*) [L]

        <Directory /var/www/roundcube/>
                Options +FollowSymLinks -Indexes
                DirectoryIndex index.php
                # This is needed to parse /var/www/roundcube/.htaccess. See its
                # content before setting AllowOverride to None.
                AllowOverride All
                <IfVersion >= 2.3>
                        Require all granted
                </IfVersion>
                <IfVersion < 2.3>
                        Order allow,deny
                        Allow from all
                </IfVersion>
        </Directory>

        # Access to tinymce files
        <Directory /var/www/roundcube/program/js/tinymce/>
                Options Indexes MultiViews FollowSymLinks
                AllowOverride None
                DirectoryIndex index.php
                <IfVersion >= 2.3>
                        Require all granted
                </IfVersion>
```

```
                <IfVersion < 2.3>
                        Order allow,deny
                        Allow from all
                </IfVersion>
        </Directory>

        # Protecting basic directories:
        <Directory /var/www/roundcube/config>
                Options -FollowSymLinks -Indexes
                AllowOverride None
        </Directory>

        <Directory /var/www/roundcube/temp>
                Options -FollowSymLinks -Indexes
                AllowOverride None
                <IfVersion >= 2.3>
                        Require all denied
                </IfVersion>
                <IfVersion < 2.3>
                        Order allow,deny
                        Deny from all
                </IfVersion>
        </Directory>

        <Directory /var/www/roundcube/logs>
                Options -FollowSymLinks -Indexes
                AllowOverride None
                <IfVersion >= 2.3>
                        Require all denied
                </IfVersion>
                <IfVersion < 2.3>
                        Order allow,deny
                       Deny from all
                </IfVersion>
        </Directory>

    # SSL Engine Switch: Enable/Disable SSL for this virtual host.
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/webcert.crt
        SSLCertificateKeyFile /etc/apache2/ssl/webcert.key

        ErrorLog ${APACHE_LOG_DIR}/error.log
        # Possible values include: debug, info, notice, warn, error, crit, alert,
emerg.
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined
</VirtualHost>

=====================================================
```

Start by installing the necessary packages. The plugin packages aren't essential, but it doesn't hurt to look them over to see what is available. The additional PHP packages are needed to read some types of mail you might receive:

```
apt-get update
apt-get install roundcube roundcube-mysql roundcube-plugins roundcube-plugins-extra
php-mail php-mail-mimedecode php-mime-type php-mail-mime
apt-get clean
```

sau:

```
apt-get install --assume-yes \
  roundcube \
  roundcube-plugins \
  roundcube-plugins-extra \
  php-mail \
  php-mail-mimedecode \
  php-mime-type \
  php-mail-mime
```

In the package installation process you will be asked whether the installer should configure the database. Answer "Yes", then choose "mysql" as the database type. You'll be asked for the MySQL root user password, so enter it. Then you will be asked to enter and confirm a password for a new "roundcube" database user that will be created for you. The same comments on passwords apply here as for those you created earlier for the "root" and "mail" user.

Set the following lines in /etc/roundcube/main.inc.php to tell Roundcube that the mail server applications are running on the same machine as it is, force it to redirect non-secure HTTP connections to HTTPS, and enable the use of Memcache for caching:

```
// The mail host chosen to perform the log-in.
// Leave blank to show a textbox at login, give a list of hosts
// to display a pulldown menu or set one host as string.
// To use SSL/TLS connection, enter hostname with prefix ssl:// or tls://
// Supported replacement variables:
// %n - hostname ($_SERVER['SERVER_NAME'])
// %t - hostname without the first part
// %d - domain (http hostname $_SERVER['HTTP_HOST'] without the first part)
// %s - domain name after the '@' from e-mail address provided at login screen
// For example %n = mail.domain.tld, %t = domain.tld
// WARNING: After hostname change update of mail_host column in users table is
//          required to match old user data records with the new host.
$rcmail_config['default_host'] = 'localhost';

// enforce connections over https
// with this option enabled, all non-secure connections will be redirected.
// set the port for the ssl connection as value of this option if it differs from
the default 443
```

```
$rcmail_config['force_https'] = true;

// Type of IMAP indexes cache. Supported values: 'db', 'apc' and 'memcache'.
$rcmail_config['imap_cache'] = 'memcache';

// Backend to use for session storage. Can either be 'db' (default) or 'memcache'
// If set to memcache, a list of servers need to be specified in 'memcache_hosts'
// Make sure the Memcache extension (http://pecl.php.net/package/memcache) version
>= 2.0.0 is inst$
$rcmail_config['session_storage'] = 'memcache';

// Use these hosts for accessing memcached
// Define any number of hosts in the form of hostname:port or
unix:///path/to/socket.file
$rcmail_config['memcache_hosts'] = array( 'localhost:11211' );
```

At this point Roundcube is now installed and minimally configured, but it isn't accessible from the server webroot. The Roundcube webroot containing PHP files and various symlinks is sitting in /var/lib/roundcube, and the next step is to make that available to visitors. This is easily accomplished by creating a symlink in the webroot:

```
1

ln -s /var/lib/roundcube /var/www/html/roundcube
```

Now redirect the default landing page for visitors to Roundcube, which first requires moving the default index page out of the way:

```
1

mv /var/www/html/index.html /var/www/html/index.bak.html
```

Then expand /var/www/html/.htaccess to include a rule to redirect just the landing page to Roundcube. Being this selective leaves the open the option of adding other files and subdirectories under /var/www/html for whatever you might want to use them for, and preserves access to Postfix Admin.

```
RewriteEngine On

# Redirect all HTTP traffic to HTTPS.
RewriteCond %{HTTPS} !=on
RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]

# Send / to /roundcube.
RewriteRule ^/?$ /roundcube [L]
```

You can now test Roundcube by visiting http://mail.example.com and logging in as a user.

```
============================================================
************************************************************
```

==========
OpenDKIM si Postfix pe Ubuntu Server 12.04LTS

Instalarea functioneaza pentru Postfix 2.3.3 sau mai nou. Verificam versiunea cu:
postconf -d mail_version

Daca rulam Postfix, Sendmail trebuie sa fie oprit. Verificam cu:
service sendmail status

DomainKeys Identified Mail (DKIM) permite unei organizatii sa-si asume responsabilitatea pentru un mesaj care este in
tranzit. Organizatia este un detinator al mesajului, atat ca si initiator sau ca si intermediar. Reputatia lor este baza
evaluarii daca mesajul este de incredere pentru viitoare operatii, precum si pentru livrari. Tehnic, DKIM asigura o
metoda de validare a identitatii numelui de domeniu care este asociat cu mesajul prin autentificare criptografica.

DKIM ataseaza un nou identificator al numelui de domeniu la un mesaj si utilizeaza tehnicile criptografice pentru
validarea autorizarii pentru prezenta sa. Identificatorul este independent de orice alt identificator in cadrul
mesajului, precum in campul From.

Prima versiune a DKIM sintetizeaza si extinde specificatiile Yahoo!'s DomainKeys si Cisco's Identified Internet Mail.
Este rezultatul unui an intreg de colaborari dintre numerosi jucatori din industrie, de-a lungul anului 2005, pentru
dezvoltarea unei specificatii de autentificare a e-mail-urilor de tip standard deschis.

DomainKeys Identified Mail (DKIM) este o metoda de asociere a numelui de domeniu la un mesaj de e-mail, alocand o persoana,
rol, sau organizatie sa-si asume responsabilitatea pentru mesaj. Asocierea este setata, insemnand o semnatura digitala
care poate fi validata de recipient. Responsabilitatea este asumata de un semnatar - independent de autorul actual al
mesajului – adaugand o semnatura DKIM: camp la antetul mesajului. Verificatorul utilizeaza o cheie publica pentru semnare
utilizand DNS-ul, si apoi verifica ca semnatura se potriveste cu continutul mesajului actual.

Semnatura DKIM poate acoperi si alte campuri ale antetului de mesaj, precum From: si Subject: si corpul mesajului (sau
partea sa initiala). Campul semnaturii DKIM insusi este intotdeauna implicit acoperit si, semnatura potrivita, contine alte
date identificabile prin etichete, precum numele de domeniu, lista campurilor acoperite, algoritmii de semnare, si metoda
prin care text snippets este simplificat in scopul semnarii (canonicalization). Puterea semnaturii DKIM poate fi ajustata

astfel incat sa permita acelor mesaje modificari care sunt considerate normale. DKIM nu a fost proiectat pentru a asigura
integritatea end-to-end.

Dintre furnizorii importanti de servicii e-mail care au implementat DKIM, amintim: Yahoo, Gmail, si AOL. Orice e-mail care
vine de la aceste organizatii, trebuie sa contina o semnatura DKIM.

Cateva referinte despre subiect:
    man opendkim-testkey
    man opendkim.conf
    http://www.serveridol.com/2012/02/17/opendkim-configuring-dkim-keys-on-postfix/

http://stevejenkins.com/blog/2010/09/how-to-get-dkim-domainkeys-identified-mail-working-on-centos-5-5-and-postfix-using-opendkim/
    http://blog.example.com/tag/opendkim/

http://blog.tjitjing.com/index.php/2012/03/guide-to-install-opendkim-for-multiple-domains-with-postfix-and-debian.html
si Wikipedia are o buna documentare a acestui subiect.

La nivel minim, veti avea nevoie de:
- Acces root la serverul de mail
- Acces la modificarea inregistrarilor DNS pentru domeniul respectiv.

Instalati opendkim din repozitorii:
sudo apt-get install opendkim opendkim-tools

Trebuie sa decideti care “selector” doriti sa-l utilizati. Selectorul este pur si simplu un cuvant care descrie cheia
pe care doriti sa o utilizati. In exemplul acesta vom utiliza selectorul 201205 ca si cheie care devine valida in Mai
2012. Vom da doua exemple pentru varietate, care vor fi de ajutor pentru clarificare. Veti avea nevoie de generarea
doar a unei singure chei. In orice caz am dat ambele exemple, pentru a putea sa le comparati:

201205 (prima cheie)
my_selector (a 2-a cheie)

Domeniul nostru va fi example.com, dar vom utiliza un subdomeniu pentru cel de-al 2-lea exemplu:

example.com (pentru prima cheie)
mail.example.com (pentru a 2-a cheie)

Am decis sa lucram in urmatorul director:
mkdir /etc/opendkim/

Generam cheile in directorul curent, utlizand selectorul ales si domeniul:

```
cd /etc/opendkim/
opendkim-genkey -s 201205 -d example.com
```

Al 2-lea exemplu de generare a cheii se va face tot pentru "example.com" chiar daca cheia va fi utilizata pentru
"mail.example.com". Daca am genera pentru "mail.example.com" nu ar merge.

```
opendkim-genkey -s my_selector -d example.com                          (2nd key)
```

In momentul acesta s-au generat 2 fisiere: unul my_selector.private si altul, my_selector.txt

Veti avea sau nu veti avea nevoie sa schimbati proprietarul. Vedeti detaliile pentru cel de-al 2-lea exemplu cu cea
de-a 2-a cheie pentru care proprietar si permisiuni, care trebuie sa fie.

Verificam proprietarul si permisiunile pentru cheia privata:

```
root@localhost:/etc/opendkim# ls -la
-rw------- 1 opendkim opendkim 891 May 10 07:44 my_selector.private
```

Mai intai trebuie sa verificam urmatoarele:

```
# cat /etc/passwd | grep opendkim
```

Ar trebui sa arate asemanator cu:

```
opendkim:x:108:117::/var/run/opendkim:/bin/false
```

Si probabil e nevoie sa facem asta:

```
chmod 700 /var/run/opendkim
```

Observatie: Aceste doua noi comenzi nu sunt necesare in Ubuntu 12.04. Dar daca comanda de mai sus nu arata ca userul
opendkim nu a fost setat corespunzator, faceti ceva similar cu urmatoarea:

```
useradd -r -g opendkim -G mail -s /sbin/nologin -d /var/run/opendkim -c "OpenDKIM" opendkim
chown opendkim:opendkim 201205.private
cat 201205.private

-----BEGIN RSA PRIVATE KEY-----
ABCCXQ...[long strong]...SdQaZw9
-----END RSA PRIVATE KEY-----
```

Acum verificati cheia publica (fisierul my_selector.txt) si retineti ca exista un bug (in openDKIM 2.5.2 pe Ubuntu 12.04)! unde este continutul:
";=rsa;", it should contain ";k=rsa;".
Caracterul "k" lipseste. Trebuie sa-l inserati.

```
# cat 201205.txt

201205._domainkey IN TXT "v=DKIM1;=rsa; p=WIGfM..[snip]..QIDIAB" ; ----- DKIM 201205 pentru example.com
```

Dupa ce ati modificat, va arata astfel:
201205._domainkey IN TXT "v=DKIM1;k=rsa; p=WIGfM..[snip]..QIDIAB" ; ----- DKIM
201205 for example.com

Suplimentar, probabil vreti sa inlaturati comentariile. Daca nu doriti sa terminati cu comentarii, pur si simplu le
stergem. De asemenea, retineti ca trebuie sa adaugati flagul t=y pentru a indica catre serverele destinatie ca testam
DKIM, dar deocamdata nu il utilizam. Am ramas cu o inregistrare viabila:
201205._domainkey IN TXT "v=DKIM1\;k=rsa\;t=y\;p=WIGfM..[snip]..QIDIAB"

Trebuie sa publicam continutul acestei chei publice a serverului DNS autoritar. Recomandam utilizarea unei inregistrari
TXT. Se pare ca exista o controversa daca sa utilizam o inregistrare SPF sau ambele tipuri de inregistrari. Am ales sa
marcam cu o inregistare TXT exclusiv.

Puteti utiliza o scurta eticheta TTL (time to live) astfel incat puteti schimba cheia fara sa asteptam termenul pentru care
sa se propage prin dns. Am utilizat 180 de secunde.

Exemplu general de inregistrare DKIM TXT in cadrul fisierului DNS:
(Selector)._domainkey.(YourDomain). IN TXT "v=DKIM1;
p=MIGfMA0GCSqGSIb4DQ(.....)z2nJSPOxvGGznkcY25w5lIYpxpVwZ/IwIDAQAB;"

Inregistrarea DNS in cadrul fisierului DNS ar putea sa arate astfel:
201205._domainkey.example.com. 180 IN TXT "v=DKIM1;
p=MIGfMA0GCSqGSIb4DQ(.....)z2nJSPOxvGGznkcY25w5lIYpxpVwZ/IwIDAQAB;"

Dupa ce facem modificarea in fisierul de zona al DNS, trebuie apoi sa restartam serverul DNS:

Apoi verificam cu dig. Ar trebui sa returneze exact ceea ce am introdus in resource record (RR).
$ dig 201205._domainkey.example.com txt +short

"v=DKIM1\;k=rsa\;t=y\;p=WIGfM..[snip]..QIDIAB"

Acum, testam cheia. Comenzile de mai jos ne asigura ca suntem in folderul unde cheia exista (/etc/opendkim pentru noi).
opendkim-testkey -d example.com -s 201205 -k 201205.private -vvv

opendkim-testkey: key loaded from /etc/opendkim/201205.private
opendkim-testkey: checking key '201205._domainkey.example.com'
opendkim-testkey: key not secure
opendkim-testkey: key OK

Aceste rezultate sunt cele asteptate. "key not secure" nu indica o eroare. Este o consecinta asteptata a neutilizarii

DNSSSEC. DNSSEC va veni ca si tehnologie viitoare.

Exemplul cu a 2-a cheie:
root@localhost:/etc/opendkim# opendkim-testkey -d example.com -s my_selector -k /etc/opendkim/my_selector.private -vvvv

opendkim-testkey: key loaded from /etc/opendkim/my_selector.private
opendkim-testkey: checking key 'my_selector._domainkey.example.com'
opendkim-testkey: key not secure
opendkim-testkey: key OK

Observati ca opendkim raporteaza ca cheia nu este sigura. Asta datorita faptului ca DNSSEC nu este implementat
in DNS serverul meu si teoretic, cineva poate intercepta DNS lookup-ul si sa-l inlocuiasca cu propria cheie.

Editam fisierul de configurare al OpenDKIM:
nano /etc/opendkim.conf

root@localhost:/etc/opendkim# cat /etc/opendkim.conf

```
# This is a basic configuration that can easily be adapted to suit a standard
# installation. For more advanced options, see opendkim.conf(5) and/or
# /usr/share/doc/opendkim/examples/opendkim.conf.sample.
#
Domain                  example.com
KeyFile                 /etc/opendkim/201205.private
Selector                201205
#
# Commonly-used options
Canonicalization        relaxed/simple
Mode                    sv
SubDomains              yes
# Log to syslog
Syslog                  yes
LogWhy                  yes
# Required to use local socket with MTAs that access the socket as a non-
# privileged user (e.g. Postfix)
UMask                   022
UserID                  opendkim:opendkim
#
KeyTable                refile:/etc/opendkim/KeyTable
SigningTable            refile:/etc/opendkim/SigningTable
ExternalIgnoreList      refile:/etc/opendkim/TrustedHosts
InternalHosts           refile:/etc/opendkim/TrustedHosts
#
Socket                  inet:8891@localhost
#EOF
```

Daca utilizam al 2-lea exemplu cu domeniul "mail.example.com" intrarea ar trebui sa

indice doar domeniul principal:

```
Domain                  example.com
KeyFile                 /etc/dkim/my_selector.private
Selector                my_selector
-----
```

Daca rulam instante multiple ale Postfix, avem nevoie sa adaugam asta in opendkim.conf pentru fiecare instanta (sau
pentru acelea pentru care vrem sa utilizam opendkim).

Editam /etc/opendkim/TrustedHosts:
nano /etc/opendkim/TrustedHosts

Adaugam domenii, nume de host si / sau IP-uri care trebuie sa fie detinute de OpenDKIM. Nu uitati de localhost.

```
127.0.0.1
localhost
example.com
mail.example.com
192.168.1.100 #(Adresa IP a serverului dumneavoastra, daca este cazul)

-----------
```

Eu in /etc/opendkim/TrustedHosts am editat ceva de genul:

```
127.0.0.1
localhost
cursuriladistanta.ro
cladmtax.cursuriladistanta.ro
86.107.58.227

------------------
```

Ultima linie de mai sus probabil ca nu este necesara. Daca avem un IP sa adaugam, trebuie sa-l utilizam pe acela propriu.

The TrustedHosts file tells OpenDKIM who to let use your keys. Because it’s referenced by the ExternalIgnoreList
directive in your conf file, OpenDKIM will ignore this list of hosts when verifying incoming mail. And, because it’s
also referenced by the InternalHosts directive, this same list of hosts will be considered “internal,” and OpenDKIM
will sign their outgoing mail.

Editam /etc/default/opendkim. Uncomment acest rand sa utilizam portul 8891:

```
SOCKET="inet:8891@localhost" # listen on loopback on port 8891
```

Asigurati-va ca firewall-ul (iptables) permite loopback pe localhost:
sudo iptables -A INPUT -i lo -j ACCEPT

Apoi, editam /etc/opendkim/KeyTable si adaugam domeniul la KeyTable.
nano /etc/opendkim/KeyTable

Adaugam linia:
#EXAMPLE showing my 2nd key:
my_selector._domainkey.example.com
example.com:my_selector:/etc/opendkim/my_selector.private

If you're going to use multiple keys (to sign mail for virtual domains with different keys, for example),
you'll need to create a separate line in the KeyTable file for each domain, like this:
default._domainkey.example.com
example.com:default:/etc/opendkim/keys/example.com/default
default._domainkey.example2.com
example2.com:default:/etc/opendkim/keys/example2.com/default

Apoi editam /etc/opendkim/SigningTable:
nano /etc/opendkim/SigningTable

Adaugam domeniul la SigningTable

Aratam ambele exemple. Notam ca pentru a 2-a cheie, trebuie sa utilizam acum numele complet al domeniului "mail.example.com":

example.com 201205._domainkey.example.com
mail.example.com my_selector._domainkey.example.com

La mine nu a functionat asa, ci astfel, prin urmare continutul lui /etc/opendkim/SigningTable va fi:
*@example.com my_selector._domainkey.example.com

Again, for multiple domains and/or users, you'll need multiple lines, like this:
*@example.com default._domainkey.example.com
bob@example2.com default._domainkey.example2.com
doug@example2.com default._domainkey.example2.com

Notam ca in OpenDKIM 2.0.1 numele de domenii sunt case sensitive. In acest exemplu, utilizam o noua versiune a OpenDKIM
si asta nu apare a fi o problema.

Configuram Postfix. Editam /etc/postfix/main.cf si adaugam liniile urmatoare la final:

milter_default_action = accept
milter_protocol = 2
smtpd_milters=inet:localhost:8891

```
non_smtpd_milters=inet:localhost:8891
```

La mine nu a functionat asa, ci astfel, prin urmare adaugam la sfarsitul lui /etc/postfix/main.cf, urmatoarele linii:

```
milter_default_action = accept
milter_protocol = 2
smtpd_milters=inet:127.0.0.1:8891
non_smtpd_milters=$smtpd_milters
```

De fapt am setat astfel:

```
# Setari referitoare la DKIM:
# -------------------------------------
milter_default_action = accept
milter_protocol = 2

# smtpd_milters=inet:localhost:8891
smtpd_milters=inet:127.0.0.1:8891,inet:127.0.0.1:8892

# non_smtpd_milters=inet:localhost:8891
non_smtpd_milters=$smtpd_milters,inet:127.0.0.1:8892
```

De asemenea schimbam numele de domeniu:

```
#myhostname = localhost         #original
myhostname = mail.example.com
```

Trebuie de asemenea sa schimbam intrarea corespondenta in /etc/hosts. Aceste schimbari sunt efective dupa restartare
(sau puteti sa setati imediat cu comanda: hostname NEW_NAME).

Restartam Postfix si opendkim, daca nu rebootam. Prima data restartam opendkim, apoi postfix:

```
root@localhost:/etc# sudo service opendkim restart
Restarting OpenDKIM: opendkim.
root@localhost:/etc# sudo service postfix restart

* Stopping Postfix Mail Transport Agent postfix   [ OK ]
* Starting Postfix Mail Transport Agent postfix   [ OK ]
```

DKIM Author Domain Signing Practices

You should also add another TXT Record to your zone file that reads:

```
_adsp._domainkey.example.com    IN    TXT    "dkim=unknown"
```

This record publishes your Author Domain Signing Practices. “Unknown” is the least strict setting, and the best place
to start. You can learn more and tinker with other options later, but most people just use “Unknown” for now, since
ADSP is relatively new (as of the writing of this post).

A DKIM Author Domain Signing Practice lookup is done by the verifier to determine whether it should expect email with
the From: address to be signed. The Author Domain Signing Practice is published with a DNS TXT record as follows:
_adsp._domainkey.example.com. IN TXT "dkim=unknown"

The dkim tag denotes the outbound signing Practice. unknown means that the example.com domain may sign some emails.

Testam:

tail -f /var/log/mail.log

When OpenDKIM starts (or restarts), you should see lines like:
opendkim[4397]: OpenDKIM Filter: mi_stop=1
opendkim[4397]: OpenDKIM Filter v2.4.2 terminating with status 0, errno = 0
opendkim[27444]: OpenDKIM Filter v2.4.2 starting (args: -x /etc/opendkim.conf)

When you send a mail that gets successfully signed, you should see:
opendkim[22254]: 53D0314803B: DKIM-Signature header added

Cea mai buna cale de verificare daca mailul semnat este autentificat si daca inregistrarile DNS sunt corect setate
este sa utilizam unul dintre serviciile free. Am utilizat acestea:

Brandon Checketts Email Validator - http://www.brandonchecketts.com/emailtest.php (preferatul nostru)

Trimitem un e-mail semnat la: check-auth@verifier.port25.com (preferatul nostru)

Trimitem un e-mail semnat la: sa-test@sendmail.net (putem pune toate adresele de e-mail de test in cadrul campului To:
pentru un singur mesaj de test)

Trimitem un e-mail semnat la: autorespond+dkim@dk.elandsys.com <--- BROKEN!!! Nu-l mai utilizam.

Fiecare dintre acestea ne va spune daca lucrurile merg cum trebuiesi ne vor da indicii despre ceea ce nu merge daca
e cazul.

Daca avem un cont Gmail, putem de asemenea trimite acolo un mesaj semnat, pentru un test rapid si simplu.

Odata ce toate lucrurile merg bine, putem inlatura flagul de test in inregistrarea DNS TXT, si sa crestem TTL-ul.

Adaugam inregistrari TXT la zona DNS pentru SPF si DKIM.

Fisierul meu /etc/opendkim.conf este urmatorul:

```
# This is a basic configuration that can easily be adapted to suit a standard
# installation. For more advanced options, see opendkim.conf(5) and/or
# /usr/share/doc/opendkim/examples/opendkim.conf.sample.

# Log to syslog. Log activity to the system log.
Syslog                  yes

# Log additional entries indicating successful signing or verification of messages.
SyslogSuccess           yes

# If logging is enabled, include detailed logging about why or why not a message was
# signed or verified. This causes a large increase in the amount of log data
generated
# for each message, so it should be limited to debugging use only.
LogWhy                  yes

# Required to use local socket with MTAs that access the socket as a non-
# privileged user (e.g. Postfix)
UMask                   022

# Attempt to become the specified user before starting operations.
UserID                  opendkim:opendkim

# Sign for example.com with key in /etc/mail/dkim.key using
# selector '2007' (e.g. 2007._domainkey.example.com)
# Domain(s) whose mail should be signed by this filter. Mail from other domains will
# be verified rather than being signed. Uncomment and use your domain name.
# This parameter is not required if a SigningTable is in use.
Domain                  inovatop.ro

# Gives the location of a private key to be used for signing ALL messages.
KeyFile                 /etc/opendkim/InovaSep2012.private

# Defines the name of the selector to be used when signing messages.
Selector                InovaSep2012

# Commonly-used options; the commented-out versions show the defaults.
# Selects the canonicalization method(s) to be used when signing messages.
Canonicalization        relaxed/simple
```

```
# Selects operating modes. Valid modes are s (signer) and v (verifier). Default is
v.
Mode                    sv
SubDomains              yes

# ADSPDiscard (Boolean) If "true", requests rejection of messages which are
determined
# to be suspicious according to the author domain's published signing practises
(ADSP)
# record if that record also recommends discard of such messages.
# ADSPDiscard           no

#
KeyTable                refile:/etc/opendkim/KeyTable

# Defines a table used to select one or more signatures to apply to a message based
# on the address found in the From: header field. In simple terms, this tells
# OpenDKIM how to use your keys.
SigningTable            refile:/etc/opendkim/SigningTable

# Identifies a set of "external" hosts that may send mail through the server as one
# of the signing domains without credentials as such.
ExternalIgnoreList      refile:/etc/opendkim/TrustedHosts

# Identifies a set internal hosts whose mail should be signed rather than verified.
InternalHosts           refile:/etc/opendkim/TrustedHosts

# Create a socket through which your MTA can communicate.
Socket                  inet:8891@localhost

#EOF

------------------------------------------------

Inregistrarile mele DKIM si SPF din fisierul de zona DNS sunt urmatoarele:

; BIND data file for INOVATOP.RO zon;
;
$TTL    172800                                          ; (2 days) Conform
RIPE.NET
;(name) (ttl)   Class   SOA     Origin                  Postmaster      Comments
;-------------------------------------------------------------------------------
---------
@               IN      SOA     ns.inovatop.ro.         sysadmin.inovatop.ro. (
                                     2012102201                 ; Serial no. - based
on date
                                          86400                 ; Refresh after 1
day
                                           7200                 ; Retry after 2
hours
```

```
                                        3542400                 ; Expire after 41
days
                                         172800 )               ; Negative Cache TTL
(2 days)
;---------------------------------------------------------------------------------
---------
;(name) (ttl)   Class   NS      Nameserver      Name
;---------------------------------------------------------------------------------
---------
; Nameservers definition
@               IN      NS      ns.inovatop.ro.                 ; Inet address of
name server
;---------------------------------------------------------------------------------
---------
; Mail exchanger definition
@               IN      MX 10   invtmtax.inovatop.ro.           ; Primary Mail
Exchanger
;---------------------------------------------------------------------------------
---------
; A Records definition
@                       IN      A       86.107.58.226           ; Main Domain
Address
ns                      IN      A       86.107.58.226           ; Name Server
www                     IN      A       86.107.58.226           ; Web Server
invtmtax                IN      A       86.107.58.226           ; Mail Server
invtwmsx                IN      A       86.107.58.226           ; Web Mail
invtftpx                IN      A       86.107.58.226           ; ftp server
invtpmax                IN      A       86.107.58.226           ; PhpMyAdmin
invtpadx                IN      A       86.107.58.226           ; Postfix Web Admin
invtcacx                IN      A       86.107.58.226           ; Web Monitoring
invtphlx                IN      A       86.107.58.226           ; Newsletter
;---------------------------------------------------------------------------------
---------
; SPF (Sender Policy Framework) Records
; version 1 of SPF and servers which are allowed to send e-mail from @inovatop.ro
email
; address are the one listed in the a records, mx records and also xxx.xxx.xxx.xxx
address.
; inovatop.ro.          IN      TXT     "v=spf1 a mx ~all"
; inovatop.ro.          IN      SPF     "v=spf1 a mx ~all"
inovatop.ro.            IN      TXT     "v=spf1 a mx a:inovatop.ro ip4:86.107.58.226
mx:invtmtax.inovatop.ro ~all"
inovatop.ro.            IN      SPF     "v=spf1 a mx a:inovatop.ro ip4:86.107.58.226
mx:invtmtax.inovatop.ro ~all"
;---------------------------------------------------------------------------------
---------
; DKIM Records  InovaSep2012 for inovatop.ro
/etc/opendkim/InovaSep2012.txt
; Public key records:
InovaSep2012._domainkey.inovatop.ro.            IN      TXT
```

```
"k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC4oEFybiCV...kjhkhk"
; DKIM Author Domain Signing Practices
_adsp._domainkey.inovatop.ro                    IN      TXT     "dkim=unknown"
;----------------------------------------------------------------------------------
---------
; Domainkeys Records    InovaDKSep2012 for inovatop.ro
/etc/dk-filter/public.key
; Create the policy sub-domain:
_domainkey.inovatop.ro.                         IN      TXT     "o=~;
r=sysadmin@inovatop.ro"
; Public key records:
InovaDKSep2012._domainkey.inovatop.ro.          IN      TXT
"k=rsa;p=MFwwDQYJKoZIhvcNAQEBBQADSwAwS......AJBAK74+N3D79K9l8Yt"
;----------------------------------------------------------------------------------
---------
-------------------------------------------
```

The maximum size for all txt records in a DNS cannot exceed 512 bytes. This means that you cannot use 1024
bit for both Domainkeys and DKIM.

If you need to use both Domainkeys and DKIM, you will have to choose one 512 bit and the other one 1024 bit,
so that it can fit in the 512 bytes

From the RFC:
3.1.4. Record Size

> The published SPF record for a given domain name SHOULD remain small enough that the results of a query for it will fit within 512 octets. This will keep even older DNS implementations from falling over to TCP. Since the answer size is dependent on many things outside the scope of this document, it is only possible to give this guideline: If the combined length of the DNS name and the text of all the records of a given type (TXT or SPF) is under 450 characters, then DNS answers should fit in UDP packets. Note that when computing the sizes for queries of the TXT format, one must take into account any other TXT records published at the domain name. Records that are too long to fit in a single UDP packet MAY be silently ignored by SPF clients.

DomainKeys with Postfix in Ubuntu

Introduction

DomainKeys is an e-mail authentication system designed to verify the DNS domain of an e-mail sender and the message integrity. DomainKeys was originally developed by Yahoo! and has since been superseded by a newer protocol called DomainKeys Identified Mail Postfix/DKIM. DomainKeys has been deprecated and should no longer be

used. dk-milter is unmaintained and it's author recommends it no longer be used due to significant bugs.

DomainKeys is very similar in most respects to Postfix/DKIM's operation.

dk-filter implements a Sendmail Mail Filter (Milter) for the DomainKeys standard. DomainKeys provides a way for senders to confirm their identity when sending email by adding a cryptographic signature to the headers of the message.

The dk-milter implements both DomainKeys signing and verification.

Installation

We assume you already successfully installed Postfix MTA, if not, please read the Postfix dedicated page.

To install dk-filter, you need Universe repositories added, if so, use your favorite package manager and install the package. For example:

```
apt-get update
apt-get upgrade
sudo aptitude install dk-filter
```

Simply accept the defaults if the installation process asks questions. The configuration will be done in greater detail in the next stage.

```
--------
Building dependency tree
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@invtmtax:/home/inotanaka96# aptitude install dk-filter
The following NEW packages will be installed:
  dk-filter
0 packages upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 53.0 kB of archives. After unpacking 171 kB will be used.
Get: 1 http://archive.ubuntu.com/ubuntu/ precise/universe dk-filter amd64
1.0.0.dfsg-1.2 [53.0 kB]
Fetched 53.0 kB in 0s (236 kB/s)
Selecting previously unselected package dk-filter.
(Reading database ... 36195 files and directories currently installed.)
Unpacking dk-filter (from .../dk-filter_1.0.0.dfsg-1.2_amd64.deb) ...
Processing triggers for man-db ...
Setting up dk-filter (1.0.0.dfsg-1.2) ...
adduser: Warning: The home directory `/var/run/dk-filter' does not belong to the
user you are currently creating.
Starting DomainKeys Filter: dk-filter.
--------
```

Generating signing keys

You can generate a public and private key pair which will be used in signing and verifying mail using the following:

Se vor genera in folderul in care ne aflam cand executam comenzile:

De exemplu construiesc un folder nou:
mkdir /etc/domainkeys/
cd /etc/domainkeys
openssl genrsa -out private.key 1024 <------- Am generat de 512
openssl rsa -in private.key -out public.key -pubout -outform PEM

You can then move it to a more secure location:
cp private.key /etc/mail/domainkey.key

Configuration

dk-filter configuration consists of a single file: /etc/default/dk-filter

In this example configuration, we'll assume your domain is domain.tld and your selector is mail:

```
# Sane defaults: log to syslog
DAEMON_OPTS="-l"
# Sign for domain.tld with key in /etc/mail/domainkey.key using
# selector '2007' (e.g. 2007._domainkey.domain.tld)
DAEMON_OPTS="$DAEMON_OPTS -d domain.tld -s /etc/mail/domainkey.key -S mail"
# See dk-filter(8) for a complete list of options
#
# Uncomment to specify an alternate socket
#SOCKET="/var/run/dk-filter/dk-filter.sock" # default
#SOCKET="inet:54321" # listen on all interfaces on port 54321
SOCKET="inet:8892@localhost" # listen on loopback on port 8892
#SOCKET="inet:12345@192.0.2.1" # listen on 192.0.2.1 on port 12345
```

Eu l-am editat astfel:

```
# Sane defaults: log to syslog
DAEMON_OPTS="-l"
# Sign for example.com with key in /etc/mail/domainkey.key using
# selector '2007' (e.g. 2007._domainkey.example.com)
DAEMON_OPTS="$DAEMON_OPTS -d cursuriladistanta.ro -s /etc/mail/domainkey.key -S
CladDKOct2012"
# See dk-filter(8) for a complete list of options
#
# Uncomment to specify an alternate socket
# SOCKET="/var/run/dk-filter/dk-filter.sock" # default
# SOCKET="inet:54321" # listen on all interfaces on port 54321
```

```
# SOCKET="inet:12345@localhost" # listen on loopback on port 12345
#
SOCKET="inet:8892@localhost" # listen on loopback on port 8892
#
# SOCKET="inet:12345@192.0.2.1" # listen on 192.0.2.1 on port 12345
```

The DAEMON_OPTS is the most important setting. For a full list of optional arguments you can pass to the dk-filter:

```
dk-filter --help
```

For instance, if you are configuring a 'smarthost' and need to allow other servers to connect to it to send mail, you can create a file with each allowed IP address per line. You then tell dk-filter about this list by passing it the '-i' argument. For example, if you create a file '/etc/default/ilist' with the following contents:

```
192.168.0.1
192.168.0.2
```

the DAEMON_OPTS setting would then become:

```
DAEMON_OPTS="$DAEMON_OPTS -d domain.tld -s /etc/mail/domainkey.key -S mail -i
/etc/default/ilist"
```

This will allow mail sent by those IP addresses to be signed by the smarthost you are configuring.

Configuring DNS

You will need to create two TXT records in order for mail recipients to verify your signed mail. The DNS record should look like this:

```
_domainkey.domain.tld. IN TXT "t=y; o=~;"
```

Where the "t=y" means that the domain is in test mode, actually that it is activated, and the "o=~;" means that only some mail is being signed from this domain. If you want to indicate that all mail is signed, use "o=-;".

```
mail._domainkey.domain.tld. IN TXT "k=rsa; t=y; p=PpYHdE2tevfEpvL1Tk2dDYv0pF28/f
5MxU83x/0bsn4R4p7waPaz1IbOGs/6bm5QIDAQAB"
```

The t=y value pair means that the domain is using this key in test mode, also that is activate. Everything after p= is actually the content of the public key we generated above, public.key. Be sure to only copy the key string itself, leaving out these comments:

```
-----BEGIN PUBLIC KEY-----
```

and:

-----END PUBLIC KEY-------

Startup and testing

Now that dk-filter is configured, you need to restart the daemon:

/etc/init.d/dk-filter restart
sau:
service dk-filter restart

If for some reason the daemon is not already running, you can simply start it:
/etc/init.d/dk-filter start

You can check the log file if everything is ok:
sudo grep -i dk /var/log/mail.log

Now, to tell the Postfix about the existing milter, and where to connect with it, edit your Postfix main.cf file /etc/postfix/main.cf, and append the following data:

milter_default_action = accept
milter_protocol = 2
smtpd_milters = inet:localhost:8892
non_smtpd_milters = inet:localhost:8892

If you are already using another milter (for example Postfix/DKIM), you can append additional settings using a comma as a separator:

milter_default_action = accept
milter_protocol = 2
smtpd_milters = inet:localhost:8891,inet:localhost:8892
non_smtpd_milters = inet:localhost:8891,inet:localhost:8892

La mine fisierul contine ceva de genul:

milter_default_action = accept
milter_protocol = 2
smtpd_milters=inet:127.0.0.1:8891,127.0.0.1:8892
non_smtpd_milters=$smtpd_milters,127.0.0.1:8892

Now restart Postfix:
sudo /etc/init.d/postfix restart

For testing purposes, I recommend you tools like:
http://domainkeys.sourceforge.net/#interop

Sender ID & SPF

Alte caracteristici de securitate utilizeaza Microsoft's Sender ID sau Pobox's SPF. Utilizam SPF.

spf.pobox.com
www.microsoft.com/mscorp/safety/technologies/senderid/

Generare SPF la Microsoft:
http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/

SPF trebuie sa limiteze cine poate sa trimita mailuri in numele domeniului tau, si este in continua dezvoltare.
Recomandam SPF cu cateva rezerve, detaliate mai jos.

Microsoft nu este intotdeauna un lucru rau, si cateodata mai fac si lucruri bune, si fac unele software-uri utile,
eu prefer sa nu fiu blocat in tehnologia lor Sender ID.

Configurarea SPF

Site-ul pobox are cateva instrumente de generare a SPF pentru setarea configurarii SPF. Probabil cel mai bine sa le
utilizam pe ale lor.

Dar, modalitatea prin care vom face setarea este in general - un domeniu cu SPF-ul detaliat - apoi toate celelalte
domenii cu un alias SPF catre acesta. Exemplu:

Campul DNS TXT al domeniului principal:
"v=spf1 a mx a:myserver.example.com include:aspmx.googlemail.com include:gmail.com ~all"

Exemplu de setare a SPF-ului la cursuri-web-design.ro si care este acceptat de Microsoft:
v=spf1 a mx a:cursuri-web-design.ro ip4:89.35.233.243 mx:mail.cursuri-web-design.ro ~all

Cele mai importante elemente sunt:
- Am listat serverele de mail si site-urile web asociate cu acest domaniu (inregistrarile a si mx).
- Specificam apoi lista numelor serverelor prin care trimit mailuri de la aplicatii automate utilizand adrese in cadrul
acestui domeniu.
- Dupa cum vedeti, deasemenea utilizam Google Apps cu acest domeniu, spunand astfel SPF sa permita toate serverele de
mail asociate cu google mail.

Apoi, pentru cele mai multe dintre celelalte domenii, ne-ar folosi aceasta inregistare DNS TXT:
"v=spf1 a mx include:example.com ~all"

Cele mai importante elemente sunt:
- Am listat serverele de mail si site-urile web asociate cu acest domeniu.
- Apoi spunem SPF-ului sa permita, de asemenea, toate serverele de mail asociate cu domeniul nostru principal (example.com).
- Si pentru toate acestea utilizam ~all!

Observatie: Unele domenii pe care le-am adaugat avand un SPF strict, sunt domenii care niciodata nu trimit mailuri.

Probleme SPF:

Este de remarcat cu privire la SPF, ca ar trebui sa lase decizia de a respinge sau daca sa permita e-mail-uri la
serverele de mail. Prin urmare, folosind pe -all in loc de ~all, nu este deloc o alegere buna. Sa-l lasam sa se
ocupe de mail pe SPAM scoring al serverului de primire, asa cum o face SpamAssasin. Ai minimiza atunci riscul de
fals pozitive.

Unul dintre aceste motive pentru care descurajam utilizarea -all, este ca SPF are o problema distincta: Nu-i place
redirectionarea de e-mail-uri sau utilizarea MX back-ul.

Considerati asta: Adresa ta, lulu@hoopa.com trimite un mail cu bancuri la cativa prieteni. Unul dintre acestia este
trixie@bellbell.org. Adresa de e-mail a lui Trixie este in prezent un alias si forwardeaza emailul catre contul sau
privat de webmail la hotmailnot.com.

Acum, daca domeniul tau, hoopa.com, are setat un SPF strict, care permite doar email-uri sa fie trimise de catre
propriul mail server. Si tu / admin-ul mail serverului ai adaugat -all la SPF, care spune altor servere sa rejecteze
e-mail-urile ce nu sunt de la serverul tau. Asta, crezi ca face sens, spammerii nu vor putea utiliza domeniul tau
pentru a face spoof emails.

Dar ce se intampla: bellbell.org receptioneaza e-mail-ul de la lulu, si posibil, verifica SPF-ul, care este OK, si
il forwardeaza catre hotmailnot.com.

Acum, daca hotmailnot.com deasemenea verifica SPF, el va receptiona e-mail-ul de la bellbell.org, verifica SPF-ul
pentru a vedea daca mail serverul bellbell.org este permis sa trimita e-mail-uri in numele hoopa.com. SPF va spune NU!,
si cu -all, serverul de mail al hotmailnot.com va rejecta e-mail-ul!

Al 2-lea scenariu: daca lulu transmite e-mail-ul catre trixie direct la hotmailnot.com, dar serverul de mail al

hotmailnot.com este cazut, si mailul a fost apoi trimis catre serverul de backup mx. Cand serverul principal revine din
nou online, si serverul de backup trimite mailul catre el, SPF-ul va esua din nou cu hoopa.com. SPF nu mentioneaza
hotmailnot.com backup mx ca si mail server permis.

Solutie:
Desigur, nu puteti lista toate situatiile posibile de forwarding / backup mx email server pe care domeniul poate sa le
intalneasca! Prin urmare, doar utilizam optiunea ~all. Care pur si simplu, spune ca nu e serverul acceptat, dar ca
probabil este OK. Si daca asta conteaza la un scor la destinatar, atunci scorul de spam acumulat, poate fi suficient
sa rejecteze email-urile necorespunzatoare.

---

http://spfwizard.com/

Blackberry SPF Records

Google Sync: InstalledIf you use Blackberry Internet Service and have seen delivery issues related to SPF records when using your own domain name or company domain name you should consider the following suggestions:

SPF for the BlackBerry BIS and Google For Your Domain

About 6 weeks ago I moved one of my email domains from a self-hosted server to Google Apps for Your Domain (né GMail for Your Domain). I think now it's just called Google Apps, but what's in a name anyways? I'm using the Standard (free) edition, but the instructions are the same for all versions.

My domain is configured with a catch-all, so any email sent to *@mydomain.tld ends up in my inbox. Aside from scripts that send spam to a thousand names at my domain, the other big problem is with sender forging. If a spammer sets their reply to address to alsdjflk@mydomain.tld and sends out a pile of messages, I end up with the bounces for those.

One way of combating this is to use an SPF record. Put simply, an SPF record which tells servers (that are looking for it) "here is a list of servers that can send email using this domain." It's very effective, but for some reason RIM hasn't seen fit to publish their SMTP servers. Google does, and the information can be found in the Google Apps help section.
Finding RIM's SMTP Servers

After a few Google searches and checking the headers of a dozen or so emails I have a fairly good sized list of RIM owned netblocks. Some employee desktops might be included in this, but it's a start.

193.109.81.0 - 193.109.81.255
204.92.70.0 - 204.92.70.255
206.51.26.0 - 206.51.26.255
206.53.144.0 - 206.53.159.255
216.9.240.0 - 216.9.255.255
213.161.84.32 - 213.161.84.63
67.69.150.144 - 67.69.150.159

That's a lot of IP addresses, but I've only found mail in the US coming from 206.51.26.0-206.51.26.255 and 216.9.240.0-216.9.255.25. Users in Europe or Asia (see Derek Tom's comment) will want to try the range 193.109.81.0-193.109.81.255.

Using those IP addresses our SPF record will look like this:

```
mydomain.tld. IN TXT "v=spf1 ip4:216.9.240.0/20 ip4:206.51.26.0/24
include:aspmx.googlemail.com ~all"
```

Breaking that down:

v=spf1 – This identifies the TXT record as an SPF string.
ip4::206.51.26.0/24 – Every host in the range 206.51.26.0-206.51.26.255 is allowed to send mail from mydomain.tld.
ip4:216.9.240.0/20 – Every host in the range 216.9.240.0-216.9.255.255 is allowed to send mail from mydomain.tld.
include:aspmx.googlemail.com – Any server allowed to send mail from aspmx.googlemail.com is also allowed to send mail from mydomain.tld.
~all – SPF queries that do not match any other mechanism will return "softfail".

Messages that are not sent from an approved server should still be accepted but may be subjected to greater scrutiny.

Testing and Deployment

The Sender Policy Framework site has a wizard that will help you generate a SPF record for your domain and Scott Kitterman has tools available to validate your newly published SPF record. If you've got anything resembling a Linux box available you can also use dig.

```
$ dig txt mydomain.tld; <<>> DiG 9.4.1-P1 <<>> txt mydomain.tld
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14302
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;mydomain.tld.                          IN      TXT
;; ANSWER SECTION:
mydomain.tld. 1788  IN  TXT "v=spf1 ip4:216.9.248.0/20 ip4:216.9.240.0/0
include:aspmx.googlemail.com ~all"
```

Notice the numbers after your domain in the answer section – this is the remainder of the TTL for your domain, and tells you how much time you have before the cached record expires. If you control your DNS and make frequent changes to your zone file you may want to set to something lower like 1800 or 3600. Dynamic DNS servers usually keep the TTL set to 60 seconds.

I am reading thru the SPF syntax and it seems that instead of hardcoding IP adresses registered with RIM – we can also use the PTR syntax. this is inefficient as it causes larger number of DNS queries but is probably a more fool-proof way.

so, I suggest to use something like:
v=spf1 include:aspmx.googlemail.com ptr:blackberry.com ~all

(I have brought googlemail as the first check and blackberry as second assuming that more mails are sent from google than from blackberry and this order of checks will cause lesser strain on mx servers)

Mail : SPF Record for Blackberry SMTP servers
Posted by kgagnon@itechlounge.net on November 22, 2010

Using SPF record restrict the hosts allowed to send message on your behalf. If you are using Blackberry device, all your e-mail are relayed through RIM servers. So to make delivery successful, you need to allow their servers.

Add the following to your DNS text string to allow RIM servers to send out e-mails with your domain:

"v=spf1 a include:srs.bis.na.blackberry.com include:srs.bis.eu.blackberry.com ~all"

SPF Records for Blackberry Users

If you use a Blackberry and are considering implementing SPF (good) then you will need to add the following parts to your SPF record. This is to allow the Blackberry smtp servers to send mail on your behalf when you send mail from your handheld device.

ip4:206.51.26.0/24 ip4:193.109.81.0/24 ip4:216.9.240.0/20 ip4:204.187.87.0/24

So, a sample SPF record would be:

mydomain.com IN TXT v=spf1 a mx ip4:206.51.26.0/24 ip4:193.109.81.0/24
ip4:216.9.240.0/20 ip4:204.187.87.0/24 ~all

I’ve only really started really digging in to SPF the past day or two but from various things I’ve read, it seems like it would be better to add:
include include:srs.bis.eu.blackberry.com
and/or include include:srs.bis.eu.blackberry.com
so that you would have to be less concerned about the ip addresses of the Blackberry service’s mail servers. The na (North America) one includes the ip addresses in our post. I didn’t check the eu (Europe) one.

SPF Record for BIS (Blackberry Internet Service)

If you have set up your blackberry to send via your carrier's BIS portal (Blackberry Internet Service) and some of your messages are bouncing back to you from some servers as spam it is likely because your domain has an SPF record but you have not included Blackberry's servers in your SPF record.

What does this do? - If you have an SPF record it is important that you include all possible sending servers in your syntax otherwise receiving SMTP servers that do an SPF check will generate a "FAIL" condition on check.

Most SMTP servers reject mail from an SPF check that generates an explicit SPF fail.

For North American Blackberry's add the following to your SPF record:
include:srs.bis.na.blackberry.com

For European Blackberry's add the following to your SPF record:
include:srs.bis.eu.blackberry.com

Because it is RIM's responsibility to maintain the list of IP addresses that send mail, by using the include statement you are creating a dynamic list of records maintained by RIM.

Originally Posted by phrider
I'd like to set up a SPF record for this domain. I know what out-going servers to specify for mail sent by me from the domain's shared server.
Does this help you? This is the SPF entry I found after doing whois/nslookup for tmo.blackberry.net.

v=spf1 ip4:206.51.26.0/24 ip4:193.109.81.0/24 ip4:204.187.87.0/24 ip4:216.9.240.0/20 ip4:206.53.144.0/20 -all

Thank you.

Now to see if I can narrow that to the *.bis.na.blackberry.com servers....

Two options:

Option 1
ip4:216.9.248.0/24

Option 2
a:smtp01.bis.na.blackberry.com
a:smtp02.bis.na.blackberry.com
a:smtp03.bis.na.blackberry.com
a:smtp04.bis.na.blackberry.com
a:smtp05.bis.na.blackberry.com

I just noticed this in the mail authentication section for SPF records for cpanel;

Include List (INCLUDE):

The SPF settings for all hosts your specify in this list will be included with your SPF settings. This is useful if you will be sending mail though another service (ex. mac.com, comcast.com, etc).

Would it solve my problem if I simply included srs.bis.ap.blackberry.com ?

Yes, since they're publishing an SPF record too.

Brilliant! :)

Just tested it by sending mail to;
check-auth@verifier.port25.com

it works!

My spf record looks like this;

v=spf1 a mx ip4:122.100.10.xxx include:srs.bis.ap.blackberry.com -all

Looks fine to me, the include will be best overall because if blackberry mess with anything you dont need to change your record (unlike my original IP block suggestion)

Making a big SPF record

by Andrew Macpherson on Dec.03, 2009, under SPF the Sender Policy Framework

“Ok so how do I make a big SPF record? I’ve run over the size of a DNS TXT record.”

Well as I commented elsewhere you can’t simply have a bunch of records as only the first one received will be applied, and if the software notices there’s more than one it’ll throw a wobbly. You can however split your spf record up like this:

```
    $ORIGIN X.com.
    @           IN      TXT     "v=spf1 a mx include:part1.x.com include:part2.x.com
include:part3.x.com -all"
    part1       IN      TXT     "v=spf1 ip4:192.168.128.0/20 -all"
    part2       IN      TXT     "v=spf1 ip4:192.168.64.0/22 -all"
    part3       IN      TXT     "v=spf1 ip4:192.168.192.0/18 -all"
```

Of course if you're setting up for a large multinational, then it's sensible to make the included parts correspond to your national gateways so you can use the a and mx tags, and avoid having to set up separate SPF records for national presentation.

What are SPF and SRS?

Article ID: KB12718

Type: Support Content

Last Modified: 01-26-2012
PrintEmail Document Bookmark

Product(s) Affected:

    BlackBerry Internet Service

Search the knowledge base:

    Visit BlackBerry Community Support Forums

    Follow us on Twitter® @BlackBerryHelp

Collapse all | Expand all
Jump to: Environment | Overview | Additional Information
CollapseEnvironment

    BlackBerry® Internet Service

    Back to top

CollapseOverview

Sender Policy Framework (SPF) and Sender Rewrite Scheme (SRS) are two proposed standards to reduce spam-type email messages. These methods prevent spam email message senders from falsifying the From address in email messages.

SPF is a set of methods that messaging servers can implement and use to decide which email messages should be accepted and which should be denied. A high-level example of SPF is as follows:

An email message is sent from <userA>@<CompanyA>.<xyz> to <userB>@<CompanyB>.<xyz>.

Company B receives the email message to its messaging server and performs an SPF record lookup on the From address (<userA>@<CompanyA>.<xyz>).

Based on the SPF record information retrieved by the lookup, Company B's messaging server verifies that the messaging server that sent the email message to Company B is authorized by Company A to do so.

The email message is then processed as accepted or denied, based on the configuration of Company B's SPF rules and the results of the SPF lookup.

SRS was created as another proposed standard to address issues created with SPF in situations such as email message forwarding. SRS alters the Mail from address to include a unique key (to prevent forging), the sender's From address, and an email address where error messages can be returned. SRS is implemented on the BlackBerry® Internet Service messaging servers.

Due to these proposed standards, there could be situations where email messages sent from a BlackBerry Internet Service email address are not accepted by the destination messaging server. The following is an example of a configuration scenario where BlackBerry Internet Service email message delivery might be affected:

User A integrates an email address with a BlackBerry Internet Service account (<userA>@<domain>.<xyz>)

User A configures the Sent from setting for the integrated account address (<userA>@<domain>.<xyz>) to an alternate email address (<userA>@<alternatedomain>.<abc>)

Note: For instructions on configuring the Sent from address, see KB02204.

User A sends an email message from the BlackBerry smartphone intended for <userB>@<anotherdomain>.<xyz>

The messaging server at <anotherdomain>.<xyz> receives this email message and notes the following:

From: = <examplesmtp>.blackberry.com (the messaging server that is actually sending the email message data)

To: = <userB>@<anotherdomian>.<xyz> (the email address where User A intends the email message to arrive)

Mail From: = <userA>@<alternatedomain>.<abc> (the reconfigured Sent from address of User A's integrated email address)

The messaging server at <anotherdomain>.<xyz> then performs the SPF check on the MAIL FROM domain (<userA>@<alternatedomain>.<abc>) to see if <anotherdomain>.<xyz> has authorized email messages from the blackberry.com domain.

In this example scenario, <anotherdomain>.<xyz> has not authorized the domain blackberry.com as a verified sender in their SPF records.

The messaging server configuration for <anotherdomain>.<xyz> is configured to reject email messages that do not have a valid SPF response.

The message is denied delivery by <anotherdomain>.<xyz> due to the SPF record result and does not arrive to <userB>@<anotherdomain>.<xyz>.

Back to top

CollapseAdditional Information

The email message is sent from the BlackBerry smartphone user's integrated account to a third-party email address. The email message is rejected by the receiving messaging server and an error message is received by the BlackBerry Internet Service. This error generates a bounce-back email message which is sent to the BlackBerry smartphone from which the email message originated. The following is an example of the bounce-back email message:

-----Original Message-----

From: "Mail Delivery System" < MAILER-DAEMON@smtp05.bis.na.blackberry.com
Date: 19 Jul 2007 18:47:24

To:SRS0=HqZoNe=MR=aol.com=sender@srs.bis.na.blackberry.com

Subject: Delivery Status Notification (Failure)

The following message to receipient@somedomain.com was undeliverable. The reason for the problem:

5.1.0 - Unknown address
SRS0=HqZoNe=MR=aol.com=sender@srs.bis.na.blackberry.com">
550-'Ne=MR=aol.com=sender@srs.bis.na.blackberry.com">SRS0=HqZoNe=MR=aol.com=sender@srs.bis.na.blackberry.com > ...Relaying denied The receiving mail server is unable to properly read the Mail From: field and therefore rejects the email message.

Direct affected BlackBerry device users to follow up with their IT departments to investigate why their mail servers have rejected the email message.

For more detailed information on SPF and SRS, see the following:

For SRS, http://www.openspf.net/Introduction
For SPF, http://www.openspf.net/SRS
For SPF Record Check, http://www.openspf.net/

Change the Sent From Address for email messages

Article ID: KB02204

Type: Support Content

Last Modified: 12-15-2011

PrintEmail Document Bookmark

Product(s) Affected:

BlackBerry Internet Service

Search the knowledge base:

Visit BlackBerry Community Support Forums

Follow us on Twitter® @BlackBerryHelp

Collapse all | Expand all
Jump to: Environment | Overview | Additional Information
CollapseEnvironment

BlackBerry® Internet Service

Back to top

CollapseOverview

To change the Sent From Address for email messages, complete the following steps:

Log in to the wireless service provider's BlackBerry Internet Service web site.
Click the Edit icon beside the email account.
In the Reply to field, type the email address to use as the Sent From Address.
Click Save to confirm the changes.
Click OK to return to the BlackBerry Internet Service account main page.

Back to top

CollapseAdditional Information

The Sent From Address is the email address that appears in the From field of email messages sent from a BlackBerry smartphone.

When forwarding an email message, the Sent From Address field can be changed on the BlackBerry smartphone. For instructions, see KB10871.

How to send an email message using a specific email address with BlackBerry Internet Service

If you have more than one email address integrated on your BlackBerry smartphone, you can set the default email address by completing the following steps:

Go to Options > Advanced Options > Default Services.

Change Messaging (CMIME) to the email address you would like to use as your default.
Press the Menu key and click Save.

To send email messages from a email address other than the one currently set as default, complete the following steps:

Compose a new email message on your BlackBerry smartphone.
Before sending it, scroll to the very top and change Send Using to the email address you would like to use.
Press the Menu key and click Send.

The BlackBerry smartphone recalls the last email address that was used as the Send Using email address for each contact in your contact list.

How To Implement SPF In Postfix

This tutorial shows how to implement SPF (Sender Policy Framework) in a Postfix 2.x installation. The Sender Policy Framework is an open standard specifying a technical method to prevent sender address forgery (see http://www.openspf.org/Introduction). There are lots of SPF extensions and patches available for Postfix, but most require that you recompile Postfix. Therefore we will install the postfix-policyd-spf-perl package from openspf.org which is a Perl package and can be implemented in existing Postfix installations (no Postfix compilation required).

I want to say first that this is not the only way of setting up such a system. There are many ways of achieving this goal but this is the way I take. I do not issue any guarantee that this will work for you!

1 Preliminary Note

I assume that you have already set up a working Postfix mail server.

The following procedure is distribution-independent, i.e., it should work on any Linux distribution (however, I tested this on Debian Etch).

2 Install Required Perl Modules

The postfix-policyd-spf-perl package depends on the Mail::SPF and the NetAddr::IP Perl modules. Therefore we are going to install them now using the Perl shell. Start the Perl shell like this:

```
perl -MCPAN -e shell
```

If you run the Perl shell for the first time, you will be asked a few questions. You can accept all default values. You will also be asked about the CPAN repositories to use. Select repositories that are close to you.

After the initial Perl shell configuration, we can start to install the needed modules. To install Mail::SPF, simply run

```
install Mail::SPF
```

In my case, it tried to install Module::Build (which is a dependency), but then it failed. If this happens to you, simply quit the Perl shell by typing

```
q
```

Then start the Perl shell again:

```
perl -MCPAN -e shell
```

and try to install Mail::SPF again:

```
install Mail::SPF
```

This time it should succeed, and you should see that it also installs the modules Net::DNS::Resolver::Programmable and NetAddr::IP on which Mail::SPF depends.

A successful installation of Mail:SPF should end like this:

```
Installing /usr/local/bin/spfquery
Writing /usr/local/lib/perl/5.8.8/auto/Mail/SPF/.packlist
  /usr/bin/make install  -- OK
```

Because NetAddr::IP has already been installed, we can now leave the Perl shell:

```
q
```

3 Install postfix-policyd-spf-perl

Next we download postfix-policyd-spf-perl from http://www.openspf.org/Software to the /usr/src/ directory and install it to the /usr/lib/postfix/ directory like this:

```
cd /usr/src
wget http://www.openspf.org/blobs/postfix-policyd-spf-perl-2.001.tar.gz
tar xvfz postfix-policyd-spf-perl-2.001.tar.gz
cd postfix-policyd-spf-perl-2.001
cp postfix-policyd-spf-perl /usr/lib/postfix/policyd-spf-perl
```

Then we edit /etc/postfix/master.cf and add the following stanza at the end:

```
vi /etc/postfix/master.cf
```

```
[...]
policy  unix  -       n       n       -       -       spawn
        user=nobody argv=/usr/bin/perl /usr/lib/postfix/policyd-spf-perl
```

(The leading spaces before user=nobody are important so that Postfix knows that this line belongs to the previous one!)

Then open /etc/postfix/main.cf and search for the smtpd_recipient_restrictions directive. You should have reject_unauth_destination in that directive, and right after reject_unauth_destination you add check_policy_service unix:private/policy like this:

```
vi /etc/postfix/main.cf

[...]
smtpd_recipient_restrictions =
permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination,check_policy_s
ervice unix:private/policy
[...]
```

or like this:

```
[...]
smtpd_recipient_restrictions =
            [...]
            reject_unauth_destination
            check_policy_service unix:private/policy
            [...]
[...]
```

It is important that you specify check_policy_service AFTER reject_unauth_destination or else your system can become an open relay!

Then restart Postfix:

```
/etc/init.d/postfix restart
```

That's it already. You should check the README file that comes with the postfix-policyd-spf-perl package, it contains some important details about how postfix-policyd-spf-perl processes emails, e.g. like this part from the postfix-policyd-spf-perl-2.0001 README:

This version of the policy server always checks HELO before Mail From (older versions just checked HELO if Mail From was null). It will reject mail that fails either Mail From or HELO SPF checks. It will defer mail if there is a temporary SPF error and the message would othersise be permitted (DEFER_IF_PERMIT). If the HELO check produces a REJECT/DEFER result, Mail From will not be checked.

If the message is not rejected or deferred, the policy server will PREPEND the appropriate SPF Received header. In the case of multi-recipient mail, multiple headers will get appended. If Mail From is anything other than completely empty (i.e.) then the Mail From result will be used for SPF Received (e.g. Mail From None even if HELO is Pass).

The policy server skips SPF checks for connections from the localhost (127.) and instead prepends and logs 'SPF skipped - localhost is always allowed.'

4 Test policyd-spf-perl

We can test policyd-spf-perl by running

```
perl /usr/lib/postfix/policyd-spf-perl
```

The cursor will then wait on the policyd-spf-perl shell. We can now act as if we tried to send an email from a certain domain and a certain server to another email address. policyd-spf-perl will then check if that certain server is allowed to send emails for the sender domain and show us the result.

So let's see what happens if we try to send a mail from info@h****forge.com from the server h****.server*********.net (IP address 81.169.1**.**). The h****forge.com has an SPF record that allows 81.169.1**.** to send emails from h****forge.com.

So on the policyd-spf-perl shell we type:

```
request=smtpd_access_policy
protocol_state=RCPT
protocol_name=SMTP
helo_name=h****forge.com
queue_id=8045F2AB23
sender=info@h****forge.com
recipient=falko.timme@*******.de
client_address=81.169.1**.**
client_name=h****.server*********.net
[empty line]
```

The output should look like this:

```
action=PREPEND Received-SPF: pass (h****forge.com: 81.169.1**.** is authorized to
use 'info@h****forge.com' in 'mfrom' identity (mechanism 'ip4:81.169.1**.**'
matched)) receiver=server1.example.com; identity=mfrom;
envelope-from="info@h****forge.com"; helo=h****forge.com; client-ip=81.169.1**.**
```

which means we passed the test.

Let's run another test, this time we will send from the client 1.2.3.4 (www.example.com) which is not allowed to send emails from h****forge.com:

```
request=smtpd_access_policy
protocol_state=RCPT
protocol_name=SMTP
helo_name=h****forge.com
queue_id=8045F2AB23
```

```
sender=info@h****forge.com
recipient=falko.timme@*******.de
client_address=1.2.3.4
client_name=www.example.com
[empty line]
```

This is the output, the test failed as expected:

```
action=PREPEND Received-SPF: softfail (h****forge.com: Sender is not authorized by
default to use 'info@h****forge.com' in 'mfrom' identity, however domain is not
currently prepared for false failures (mechanism '~all' matched))
receiver=server1.example.com; identity=mfrom; envelope-from="info@h****forge.com";
helo=h****forge.com; client-ip=1.2.3.4
```

We can now even try to leave the sender field empty, as many spammers do. Still, policyd-spf-perl should be able to complete its tests:

```
request=smtpd_access_policy
protocol_state=RCPT
protocol_name=SMTP
helo_name=h****forge.com
queue_id=8045F2AB23
sender=
recipient=falko.timme@*******.de
client_address=81.169.1**.**
client_name=h****.server*********.net
[empty line]
```

This is the output, we are still allowed to send from h****forge.com:

```
action=PREPEND Received-SPF: pass (h****forge.com: 81.169.1**.** is authorized to
use 'h****forge.com' in 'helo' identity (mechanism 'ip4:81.169.1**.**' matched))
receiver=server1.example.com; identity=helo; helo=h****forge.com;
client-ip=81.169.1**.**
```

Let's try the same test with an invalid client:

```
request=smtpd_access_policy
protocol_state=RCPT
protocol_name=SMTP
helo_name=h****forge.com
queue_id=8045F2AB23
sender=
recipient=falko.timme@*******.de
client_address=1.2.3.4
client_name=www.example.com
[empty line]
```

As expected, this is the output:

action=PREPEND Received-SPF: softfail (h****forge.com: Sender is not authorized by default to use 'h****forge.com' in 'helo' identity, however domain is not currently prepared for false failures (mechanism '~all' matched)) receiver=server1.example.com; identity=helo; helo=h****forge.com; client-ip=1.2.3.4

To leave the policyd-spf-perl shell, type

[CTRL+C]

SPF
If you use SPF for your domain, consider that both your server and google will receive and send mail on behalf of that domin. Adding include:_spf.google.com should cover it.

Google internally
Be aware Google think they host you domain. So if others inside google, or using google hosted apps or GMail, if they email you, the email may not go via your email server, but directly to the Google Apps for your domain. That could be an issue if not all aliases you have use Google Apps. This needs to be tested more though. Especially as it may only be an issue if Google's servers are part of you domains MXs. It may be worth adding aliases in your Google Apps admin for the non google apps adresses to some user whom can handle these?

Acum este momentul sa inseram date, si sa testam cum functioneaza.

Cum sa sarim peste verificarea Spam si Virus pentru mailurile transmise local

Daca trebuie sa trasnsmitem in afara newslettere, de la serverul local unde avem controlul total al continutului acestor
e-mail-uri, atunci probabil ca nu mai vrem sa rulam verificarea anti-spam si anti-virus pentru fiecare dintre acestea.
Verificarile ar utiliza inutil ciclii de procesare ai serverului iar rularea newsletterului ar supraincarca serverul in
cazul in care el proceseaza verificari pentru fiecare dintre aceste e-mail-uri.

Pentru a face amavisd-new sa sara peste toate aceste verificari ale mailurilor generate de la un set cunoscut de adrese IP
(Exemplu: localhost, de la aplicatii web sau un alt server, etc), editati fisierul /etc/amavis/conf.d/50-user astfel:
nano /etc/amavis/conf.d/50-user

```
use strict;

#
# Place your configuration directives here.  They will override those in
# earlier files.
#
```

```
# See /usr/share/doc/amavisd-new/ for documentation and examples of
# the directives you can use in this file
#

# Replace 111.111.111.111/32 with your desired list of client IP address  <-- De
aici am introdus eu
# ranges which will bypass checks.
@mynetworks = qw( 127.0.0.0/8 [::1] 111.111.111.111/32 );

# Rules for clients defined in @mynetworks
$policy_bank{'MYNETS'} = {
  bypass_spam_checks_maps   => [1],  # don't spam-check internal mail
  bypass_banned_checks_maps => [1],  # don't banned-check internal mail
  bypass_header_checks_maps => [1],  # don't header-check internal mail
};                                                                      <--
Pana aici

#------------ Do not modify anything below this line -------------
1;  # ensure a defined return
```

Inlocuiti 111.111.111.111/32 cu orice set de adrese IP de la care doriti sa bypass-ati verificarea amavisd-new.
Toate mailurile ce sosesc de la acele surse vor ajunge in MYNETS pentru amavisd-new si totodata bypass-eaza verificarile.
Daca bypass-area dupa IP nu indelineste nevoile noastre, atunci puteti gasi modalitati prin care sa sariti peste
verificari pentru unii useri, destinatii sau surse.

Comenzi monitorizare:

```
vmstat 3
vmstat -m
vmstat -a
w username    <-- Cine este conectat
w vivek    <-- Ce procese ruleaza
------
top
Hot Key Usage:
t       Displays summary information off and on.
m       Displays memory information off and on.
A       Sorts the display by top consumers of various system resources. Useful for
quick identification of performance-hungry tasks on a system.
f       Enters an interactive configuration screen for top. Helpful for setting up
top for a specific task.
o       Enables you to interactively select the ordering within top.
r       Issues renice command.
k       Issues kill command.
z       Turn on or off color/mono
```

---
uptime
---
ps -A
Show Long Format Output:
ps -Al
To turn on extra full mode (it will show command line arguments passed to process):
ps -AlF
To See Threads (LWP and NLWP):
ps -AlFH
To See Threads After Processes:
ps -AlLm
Print All Process On The Server:
ps ax
ps axu
Print A Process Tree:
ps -ejH
ps axjf
pstree
Print Security Information:
ps -eo euser,ruser,suser,fuser,f,comm,label
ps axZ
ps -eM
See Every Process Running As User Vivek:
ps -U vivek -u vivek u
Set Output In a User-Defined Format:
ps -eo pid,tid,class,rtprio,ni,pri,psr,pcpu,stat,wchan:14,comm
ps axo stat,euid,ruid,tty,tpgid,sess,pgrp,ppid,pid,pcpu,comm
ps -eopid,tt,user,fname,tmout,f,wchan
Display Only The Process IDs of Lighttpd
ps -C lighttpd -o pid=
OR
pgrep lighttpd
OR
pgrep -u vivek php-cgi
Display The Name of PID 55977:
ps -p 55977 -o comm=
Find Out The Top 10 Memory Consuming Process:
ps -auxf | sort -nr -k 4 | head -10
Find Out top 10 CPU Consuming Process:
ps -auxf | sort -nr -k 3 | head -10
---
free
---
sar - Collect and Report System Activity
The sar command is used to collect, report, and save system activity information. To see network counter, enter:
sar -n DEV | more
To display the network counters from the 24th:
sar -n DEV -f /var/log/sa/sa24 | more

You can also display real time usage using sar:
sar 4 5
---
mpstat - Multiprocessor Usage
The mpstat command displays activities for each available processor, processor 0 being the first one. mpstat -P ALL to display average CPU utilization per processor:
mpstat -P ALL
---
pmap - Process Memory Usage
The command pmap report memory map of a process. Use this command to find out causes of memory bottlenecks.
pmap -d PID
To display process memory information for pid # 47394, enter:
pmap -d 47394
---
netstat and ss - Network Statistics
The command netstat displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. ss command is used to dump socket statistics. It allows showing information similar to netstat. See the following resources about ss and netstat commands:
---
iptraf - Real-time Network Statistics
The iptraf command is interactive colorful IP LAN monitor. It is an ncurses-based IP LAN monitor that generates various network statistics including TCP info, UDP counts, ICMP and OSPF information, Ethernet load info, node stats, IP checksum errors, and others. It can provide the following info in easy to read format:
    Network traffic statistics by TCP connection
    IP traffic statistics by network interface
    Network traffic statistics by protocol
    Network traffic statistics by TCP/UDP port and by packet size
    Network traffic statistics by Layer2 address
---
tcpdump - Detailed Network Traffic Analysis
The tcpdump is simple command that dump traffic on a network. However, you need good understanding of TCP/IP protocol to utilize this tool. For.e.g to display traffic info about DNS, enter:
tcpdump -i eth1 'udp port 53'
To display all IPv4 HTTP packets to and from port 80, i.e. print only packets that contain data, not, for example, SYN and FIN packets and ACK-only packets, enter:
tcpdump 'tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<<2)) - ((tcp[12]&0xf0)>>2)) != 0)'
To display all FTP session to 202.54.1.5, enter:
tcpdump -i eth1 'dst 202.54.1.5 and (port 21 or 20'
To display all HTTP session to 192.168.1.5:
tcpdump -ni eth0 'dst 192.168.1.5 and tcp and port http'
Use wireshark to view detailed information about files, enter:
tcpdump -n -i eth1 -s 0 -w output.txt src or dst port 80

/Proc file system - Various Kernel Statistics
/proc file system provides detailed information about various hardware devices and

other Linux kernel information. See Linux kernel /proc documentations for further details. Common /proc examples:

```
# cat /proc/cpuinfo
# cat /proc/meminfo
# cat /proc/zoneinfo
# cat /proc/mounts
```

Nagios - Server And Network Monitoring

Nagios is a popular open source computer system and network monitoring application software. You can easily monitor all your hosts, network equipment and services. It can send alert when things go wrong and again when they get better. FAN is "Fully Automated Nagios". FAN goals are to provide a Nagios installation including most tools provided by the Nagios Community. FAN provides a CDRom image in the standard ISO format, making it easy to easilly install a Nagios server. Added to this, a wide bunch of tools are including to the distribution, in order to improve the user experience around Nagios.

Cacti - Web-based Monitoring Tool

Cacti is a complete network graphing solution designed to harness the power of RRDTool's data storage and graphing functionality. Cacti provides a fast poller, advanced graph templating, multiple data acquisition methods, and user management features out of the box. All of this is wrapped in an intuitive, easy to use interface that makes sense for LAN-sized installations up to complex networks with hundreds of devices. It can provide data about network, CPU, memory, logged in users, Apache, DNS servers and much more. See how to install and configure Cacti network graphing tool under CentOS / RHEL.

A few more tools:

nmap - scan your server for open ports.

lsof - list open files, network connections and much more.

ntop web based tool - ntop is the best tool to see network usage in a way similar to what top command does for processes i.e. it is network traffic monitoring software. You can see network status, protocol wise distribution of traffic for UDP, TCP, DNS, HTTP and other protocols.

Conky - Another good monitoring tool for the X Window System. It is highly configurable and is able to monitor many system variables including the status of the CPU, memory, swap space, disk storage, temperatures, processes, network interfaces, battery power, system messages, e-mail inboxes etc.

GKrellM - It can be used to monitor the status of CPUs, main memory, hard disks, network interfaces, local and remote mailboxes, and many other things.

vnstat - vnStat is a console-based network traffic monitor. It keeps a log of hourly, daily and monthly network traffic for the selected interface(s).

htop - htop is an enhanced version of top, the interactive process viewer, which can display the list of processes in a tree form.

mtr - mtr combines the functionality of the traceroute and ping programs in a single network diagnostic tool.

---

22) Install and Set up Monit for Monitoring

Monit is a very useful monitoring tool that helps rescue your server from failed processes. Install it through apt-get:

```
apt-get install monit
```

The following are a set of fairly trivial instructions that set monit to watch over the important server processes - but without issuing notifications or doing much more than restarting on failure. Create the following files in the Monit configuration directory.

```
nano /etc/monit/conf.d/amavis
```

```
Editam urmatoarele:
check process amavisd with pidfile /var/run/amavis/amavisd.pid
# every 5 cycles
  group mail
  start program = "/etc/init.d/amavis start"
  stop  program = "/etc/init.d/amavis stop"
  if failed port 10024 protocol smtp then restart
  if 5 restarts within 25 cycles then timeout
```

```
nano /etc/monit/conf.d/apache2
```

```
Editam urmatoarele:
check process apache2 with pidfile /var/run/apache2/apache2.pid
  group www
  start program = "/etc/init.d/apache2 start"
  stop program = "/etc/init.d/apache2 stop"
  if failed host localhost port 80 protocol http
    with timeout 10 seconds
    then restart
  if 5 restarts within 5 cycles then timeout
```

```
nano /etc/monit/conf.d/dovecot
```

```
Editam urmatoarele:
check process dovecot with pidfile /var/run/dovecot/master.pid
  group mail
  start program = "/sbin/start dovecot"
  stop program = "/sbin/stop dovecot"
  group mail
  # We'd like to use this line, but see:
  #
http://serverfault.com/questions/610976/monit-failing-to-connect-to-dovecot-over-ssl
-imap
  #if failed port 993 type tcpssl sslauto protocol imap for 5 cycles then restart
  if failed port 993 for 5 cycles then restart
  if 5 restarts within 25 cycles then timeout
```

```
nano /etc/monit/conf.d/mysql

Editam urmatoarele:
check process mysqld with pidfile /var/run/mysqld/mysqld.pid
  group database
  start program = "/etc/init.d/mysql start"
  stop program = "/etc/init.d/mysql stop"
  if failed host localhost port 3306 protocol mysql then restart
  if 5 restarts within 5 cycles then timeout

nano /etc/monit/conf.d/memcached

Editam urmatoarele:
check process memcached with pidfile /var/run/memcached.pid
  group www
  start program = "/etc/init.d/memcached start"
  stop program = "/etc/init.d/memcached stop"
  if failed host localhost port 11211 then restart
  if 5 restarts within 5 cycles then timeout

nano /etc/monit/conf.d/postfix

Editam urmatoarele:
check process postfix with pidfile /var/spool/postfix/pid/master.pid
  group mail
  start program = "/etc/init.d/postfix start"
  stop  program = "/etc/init.d/postfix stop"
  if failed port 25 protocol smtp then restart
  if 5 restarts within 5 cycles then timeout

nano /etc/monit/conf.d/spamassassin

Editam urmatoarele:
check process spamassassin with pidfile /var/run/spamd.pid
  group mail
  start program = "/etc/init.d/spamassassin start"
  stop  program = "/etc/init.d/spamassassin stop"
  if 5 restarts within 5 cycles then timeout

nano /etc/monit/conf.d/sshd

Editam urmatoarele:
check process sshd with pidfile /var/run/sshd.pid
  start program "/etc/init.d/ssh start"
  stop program "/etc/init.d/ssh stop"
  if failed host 127.0.0.1 port 22 protocol ssh then restart
   if 5 restarts within 5 cycles then timeout

nano /etc/monit/conf.d/bind9
```

Editam urmatoarele:

```
## bind
check process named with pidfile /var/run/named/named.pid
 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
```

Then restart Monit to pick up the new orders:

```
service monit restart
```

Monit offers options for notifications, a web console, restarting on high load, logging activity, and many other amenities, so you may want to add more to this very basic configuration.

```
iptables -I INPUT 6 -p tcp --dport 2812 -j ACCEPT
sau:
iptables -I INPUT 6 -p tcp -m multiport --dports 80,443,38826 -j ACCEPT
```

Configurarea MONIT se face in fisierul: /etc/monit/monitrc:

```
nano /etc/monit/monitrc
```

Editam urmatoarele:

```
 set daemon  60
 set logfile syslog facility log_daemon
 set mailserver localhost
 set mail-format { from: monit@serveurdev.example.com }
 set alert root@localhost
 set httpd port 2812 and
 allow admin:monit
 set httpd port 2812 and
    SSL ENABLE
    PEMFILE  /var/certs/monit.pem
    allow admin:test
    allow xxx.xxx.xxx.xxx                    # Retea XXX
    allow yyy.yyy.yyy.yyy                    # Retea yyy
    signature disable
```

Pentru conectarea prin https, trebuie sa generam certificatul.

```
$ mkdir /var/certs
$ cd /var/certs
```

Editam optiunile de generare a certificatului:

```
nano /var/certs/monit.cnf
```

```
# create RSA certs - Server
RANDFILE = ./openssl.rnd
[ req ]
default_bits = 1024
encrypt_key = yes
distinguished_name = req_dn
x509_extensions = cert_type
[ req_dn ]
countryName = Country Name (2 letter code)
countryName_default = MO
stateOrProvinceName    = Ile de France
stateOrProvinceName_default     = Monitoria
localityName                    = Paris
localityName_default            = Monittown
organizationName                = the_company
organizationName_default        = Monit Inc.
organizationalUnitName          = Organizational Unit Name
organizationalUnitName_default  = Dept. of Monitoring Technologies
commonName                      = Common Name (FQDN of your server)
commonName_default              = server.monit.mo
emailAddress                    = Email Address
emailAddress_default            = root@monit.mo
[ cert_type ]
nsCertType = server
```

Eu am creat acest fisier in cadrul /etc/monit/certs/ iar el arata astfel:

```
# create RSA certs - Server
RANDFILE = ./openssl.rnd
[ req ]
default_bits = 1024
encrypt_key = yes
distinguished_name = req_dn
x509_extensions = cert_type
[ req_dn ]
countryName = Country Name (2 letter code)
countryName_default = MO
stateOrProvinceName    = State Or Province Name
stateOrProvinceName_default     = Monitoria
localityName                    = Locality Name
localityName_default            = Monittown
organizationName                = The Company Name
organizationName_default        = Monit Inc.
organizationalUnitName          = Organizational Unit Name
organizationalUnitName_default  = Dept. of Monitoring Technologies
commonName                      = Common Name (FQDN of your server)
commonName_default              = server.monit.mo
emailAddress                    = Email Address
```

```
emailAddress_default            = root@monit.mo
[ cert_type ]
nsCertType = server

----------
Apoi generam certificatul:

openssl req -new -x509 -days 365 -nodes -config ./monit.cnf -out
/var/certs/monit.pem -keyout /var/certs/monit.pem
openssl gendh 1024 >> /var/certs/monit.pem
openssl x509 -subject -dates -fingerprint -noout -in /var/certs/monit.pem
chmod 700 /var/certs/monit.pem

In fisierul /etc/default/monit, editam:
   startup=1
   CHECK_INTERVALS=60

Restartam serviciul monit:
$ /etc/init.d/monit start

Vérificam ca *daemonul* este activ, la adresa:
   https://exemple.com:2812/

Alte  editari in /etc/monit/monitrc:

check system invtmtax.inovatop.ro
     if loadavg (1min) > 4 then alert
     if loadavg (5min) > 3 then alert
     if memory usage > 75% then alert
     if swap usage > 25% then alert
     if cpu usage (user) > 70% then alert
     if cpu usage (system) > 30% then alert
     if cpu usage (wait) > 20% then alert


############################################################################
#REMOTE GOOGLE CHECKS
############################################################################
check host google-test with address google.com
  if failed port 80 proto http then alert
group server
#

Alte configurari de monitorizare:

nano /etc/monit/conf.d/cron

# cron
check process cron with pidfile /var/run/crond.pid
group system
```

```
start program = "/etc/init.d/cron start"
stop  program = "/etc/init.d/cron stop"
if 5 restarts within 5 cycles then timeout
depends on cron_rc

check file cron_rc with path /etc/init.d/cron
group system
if failed checksum then unmonitor
if failed permission 755 then unmonitor
if failed uid root then unmonitor
if failed gid root then unmonitor

nano /etc/monit/conf.d/apache

check process apache2 with pidfile /var/run/apache2.pid
  group www
  start program = "/etc/init.d/apache2 start"
  stop program = "/etc/init.d/apache2 stop"
     if cpu > 60% for 2 cycles then alert
     if cpu > 80% for 5 cycles then restart
     if totalmem > 200.0 MB for 5 cycles then restart                    <--- Aici
pot sa maresc memoria sau sa elimin !!!
     if children > 250 then restart
     if loadavg(5min) greater than 10 for 8 cycles then stop
  if failed host www.inovatop.ro port 80 protocol http
    with timeout 15 seconds
    then restart
  if failed host invtwmsx.inovatop.ro port 443 type tcpssl protocol http
    with timeout 15 seconds
    then restart
  if 5 restarts within 5 cycles then timeout
#    depends on apache_bin
#    group server


nano /etc/monit/conf.d/ntp

# ntp
check process ntpd with pidfile /var/run/ntpd.pid
  start program = "/etc/init.d/ntp start"
  stop  program = "/etc/init.d/ntp stop"
  if failed host 127.0.0.1 port 123 type udp then alert
  if 5 restarts within 5 cycles then timeout


nano /etc/monit/conf.d/syslogd

check process syslogd with pidfile /var/run/syslogd.pid
   start program = "/etc/init.d/sysklogd start"
   stop program = "/etc/init.d/sysklogd stop"
```

```
   if 5 restarts within 5 cycles then timeout

check file syslogd_file with path /var/log/syslog
   if timestamp > 65 minutes then alert # Have you seen "-- MARK --"?


nano /etc/monit/conf.d/filesystem

check filesystem rootfs with path /
if space usage > 90% 5 times within 15 cycles
then alert


nano /etc/monit/conf.d/rsyslogd

## rsyslogd
check process rsyslogd
      with pidfile "/var/run/rsyslogd.pid"
      start program = "/etc/init.d/rsyslog start"
      stop program = "/etc/init.d/rsyslog stop"
      if 3 restarts within 3 cycles then timeout

nano /etc/monit/conf.d/clamav
####
# ClamAV
#
check process clamavd with pidfile /var/run/clamav/clamd.pid
   start program = "/etc/init.d/clamav-daemon start"
   stop  program = "/etc/init.d/clamav-daemon stop"
#  if failed unixsocket /var/run/clamav/clamd.sock then restart
   if 5 restarts within 5 cycles then timeout


nano /etc/monit/conf.d/pure-ftpd
####
# Pure-FTPd
check process pure-ftpd with pidfile /var/run/pure-ftpd/pure-ftpd.pid
    start program = "/etc/init.d/pure-ftpd-mysql start"
    stop program  = "/etc/init.d/pure-ftpd-mysql stop"
    if failed port 21 protocol ftp then restart
    if 5 restarts within 5 cycles then timeout


Verificare sintaxa:
monit -t
monit -h
-------------------------------------------------

CACTI - Aplicatie monitorizare - Instalarea manuala
```

Trebuie sa rulez comenzile ca si user root:
sudo su

Instalare:
apt-get update
apt-get upgrade
apt-get clean

Merg pe site-ul http://www.cacti.net/ si sus la link-uri in stanga am kiturile de instalare pentru Windows si Linux.
Prin urmare downloadez chitul pentru Linux / Unix. In cazul meu: cacti-0.8.8a.tar.gz
Fac in asa fel incat sa ajunga intr-un folder pe server (il uploadez prin FTP sau SFTP).

De exemplu il incarc in /home/florin/kituri/
Ma deplasez in respectivul folder:
cd /home/florin/kituri/

si apoi dezarhivez:
tar -xf cacti-0.8.8a.tar.gz

In urma dezarhivarii a rezultat un folder numit: cacti-0.8.8a

Mai departe, vreau sa copiez acest folder in folderul radacina al serverului web, adica la locatia /var/www.
Prin urmare:
cp -R cacti-0.8.8a /var/www/

Voi redenumi acest folder:
cd /var/www/
mv cacti-0.8.8a cacti

Daca incerc sa accesez acum pagina web:
http://localhost/cacti
nu voi vedea nimic! Mai am de facut si alte setari:

Daca ma duc acum in folderul /var/www/cacti/
cd /var/www/cacti/
voi vedea mai multe foldere si fisiere.

Ma intereseaza /var/www/cacti/cacti.sql care include interogarile pentru crearea bazei de date, si un alt fisier
aflat in folderul /include, fisierul: /var/www/cacti/include/config.php
cd include
nano config.php

Aici putem seta parametri de conectare pentru baza de date pe care o vom crea:

```
/* make sure these values refect your actual database/host/user/password */
$database_type = "mysql";
```

```
$database_default = "cacti";            <--- Numele bazei de date
$database_hostname = "localhost";
$database_username = "cactiuser";
$database_password = "cactiuser";
$database_port = "3306";
$database_ssl = false;
```

Tot in acest fisier exista o variabila care imi seteaza calea de referinta. In cazul in care vreau sa creez un subdomeniu,
de genul: https://ceva.example.com/altceva/... atunci setez valoarea variabilei de cale la
$url_path ="/altceva/";
sau, daca vreau subdomeniu de genul: https://ceva.example.com/, atunci am:
$url_path ="/";

Dupa care in apache creez subdomeniul virtual. De exemplu:

nano /etc/apache2/sites-available/cacti-ssl, in care, de exemplu editez:

```
------------
## Virtual Host for CACTI
<VirtualHost *:443>
        ServerName invtcacx.inovatop.ro
        ServerAdmin sysadmin@inovatop.ro

        DocumentRoot /var/www/cacti

        RewriteEngine On
        RewriteCond %{HTTP_HOST} !invtcacx.inovatop.ro
        RewriteRule (.*) [L]

        <Directory /var/www/cacti/>
                Options +FollowSymLinks -Indexes
                DirectoryIndex index.php
                AllowOverride None
                Order Deny,Allow
                Deny from ALL
                Allow from 89.35.233.244                # TQM LAN
                Allow from 86.125.50.152                # SER LAN
                # Allow from 89.35.233.245              # Sala INFO

                <IfModule mod_php5.c>
                        AddType application/x-httpd-php .php
                        php_flag magic_quotes_gpc Off
                        php_flag track_vars On
                        php_flag register_globals Off
                        php_value include_path .
                </IfModule>
        </Directory>

        # SSL Engine Switch: Enable/Disable SSL for this virtual host.
```

```
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/webcert.crt
        SSLCertificateKeyFile /etc/apache2/ssl/webcert.key

        ErrorLog ${APACHE_LOG_DIR}/error.log
        # Possible values include: debug, info, notice, warn, error, crit, alert,
emerg.
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined
</VirtualHost>
```

La final:
a2ensite cacti-ssl
service apache2 restart

Voi crea baza de date si voi defini userul care o poate administra si drepturile pentru el.
Pot in linie de comanda sau altfel, din phpMyAdmin.

Aici ma duc la Databases ---> Create new database: ---> cacti
Dupa ce s-a creat ma duc pe ea si merg la Privileges, si vad ca nu exista un user care sa lucreze cu ea. Il voi crea!

Add a new User ---> si la Login Information:
User name: Use text field: cactiuser
Host: Local: localhost
User password: Use text field: cactiuser
Bifez Grant all privileges on database "cacti"
Apoi Go!

Alta metoda, in linie de comanda:

```
mysql -u root -p
Introduc parola, apoi:
show databases;
create database cacti;
show databases;
use cacti;
CREATE USER 'nume_user'@'localhost' IDENTIFIED BY 'parola_user';
GRANT USAGE ON * . * TO 'nume_user'@'localhost' IDENTIFIED BY 'parola_user' WITH
MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0
MAX_USER_CONNECTIONS 0;
GRANT ALL PRIVILEGES ON `nume_baza_de_date` . * TO 'nume_user'@'localhost';
```

Daca incerc sa accesez acum pagina web:
http://localhost/cacti
nu voi vedea nimic! Mai am de facut si alte setari:

Ma duc la fisierul /var/www/cacti/cacti.sql
cd ..
ls -l
nano cacti.sql

```
CREATE TABLE cdef (
  id mediumint(8) unsigned NOT NULL auto_increment,
  hash varchar(32) NOT NULL default '',
  name varchar(255) NOT NULL default '',
  PRIMARY KEY  (id)
) ENGINE=MyISAM;   <---- Verifica ca la fiecare tabel sa am asa, si nu TYPE=MyISAM;
```

Daca gasesc cu TYPE, modific!

Daca incerc sa accesez acum pagina web:
http://localhost/cacti
nu voi vedea nimic! Mai am de facut si alte setari:

daca ma uit in loguri:
updatedb
locate apache | grep log
Gasesc ca fisierul de loguri de erori este: /var/log/apache2/error.log
cat /var/log/apache2/error.log | more

Si o sa gasesc ceva afisat despre adodb... acesta lipseste si il instalez:
apt-get install php5-adodb

Retartez Apache:
service apache2 restart

Daca incerc sa accesez acum pagina web:
http://localhost/cacti
nu voi vedea nimic! Mai am de facut si alte setari:

Daca merg din nou in phpMyAdmin si dau click pe baza de date, o sa vad ca ea e goala. Nu exista nici un tabel, nimic. Va
trebui sa o populez, importand fisierul cacti.sql (va trebui sa-l am disponibil in calculatorul meu).

Click pe Import, Dupa care, Browse, aleg fisierul cacti.sql, dupa care Go si apare mesajul:
Import has been successfully finished, 1686 queries executed. (cacti.sql)

Daca incerc sa accesez acum pagina web:
http://localhost/cacti
Va trebui sa vad pagina de inceput a setarilor.

In cazul meu, doresc sa creez un subdomeniu la domeniul principal.

Voi ajunge in final in pagina de inceput al instalarii --> Next, apoi aleg New install,

si apoi intr-o pagina in care diverse lucruri vor fi semnalate cu rosu, de exemplu ca nu am instalat rrdtool si ca lipseste
snmp, etc...

apt-get install rrdtool

Dupa instalare, ma duc din nou in pagina si dau refresh... si posibil sa scap de mesajele rosii, sau altfel va trebui
sa mai intalez ce lipseste. De exemplu, snmp:

apt-get install snmp
respectiv,
apt-get install php5-snmp

Dupa care, toate ar trebui sa fie bune (cu verde)!

Apas Finish si ajung in pagina de logare:
User: admin
Parola: admin
si o sa-mi ceara sa introduc o noua parola.

*** Forced Password Change ***
Please enter a new password for cacti:
Password:
Confirm:

Iar acum ar trebui sa intre in aplicatie.

Acum ar trebui sa instalam plugin-urile necesare arhitecturii CACTI. Pentru aceasta mergem pe site-ul CACTI la:
http://www.cacti.net/
Accesez tab-ul de sus: Documentation, iar apoi din stanga aleg link-ul Plugins

De aici accesez link-ul de sus de la Plugin Architecture Installation documentation is locate "here" <------
Primul lucru este sa downloadez chitul de instalare: The first step is to "download" the Plugin Architecture.
Voi primi, astfel o arhiva. Prin urmaree voi downloada cea mai recenta varianta din lista. De exemplu:
cacti-plugin-0.8.7g-PA-v2.9.tar.gz 17-Oct-2010 20:18 2.2M

Il downloadez in calculator, dupa care il incarc pe server prin sftp.
Sa presupunem ca l-am incarcat in /home/florin/kituri/

Navighez in acest folder si de acolo, dezarhivez fisierul arhivat:
cd /home/florin/kituri/
tar -zvxf cacti-plugin-0.8.7g-PA-v2.9.tar.gz

Iar acum daca dau un ls -l, observ ca a aparut un folder numit: cacti-plugin-arch

Acum voi trece la instalarea plugin architecture. Inainte de toate, insa, ar fi recomandat sa fac un Back-up la toata
instalarea din cadrul /var/www/cacti:

```
cd /var/www/
mkdir cacti-BAK
ls -l
```

dupa care voi copia continutul lui cacti in interiorul lui cacti-BAK:

```
cp -r cacti cacti-BAK
```

Pe site-ul oficial se gasesc patch-urile oficiale. Pentru asta accesam in stinga link-ul Oficial patches
Patch-urile corecteaza orice bug descoperit in versiunea curenta de Cacti.
Instalarea se face astfel (conform instructiunilor
de la respectiva pagina):

De exemplu:
Daca eu acum am Cacti versiunea 0.8.8a.

```
cd /var/www/cacti/
apt-get update
apt-get upgrade
apt-get clean
apt-get install patch
apt-get clean
wget http://www.cacti.net/downloads/patches/0.8.8a/snmpv3_priv_proto_none.patch
patch -p1 -N < snmpv3_priv_proto_none.patch
```

List of Patches
SNMPv3 Privilege Protocol None 2012/06/03
Fix SNMPv3 privilege protocol to allow NONE

Incepand cu versiunea 0.8.8a, The Plugin Architecture face parte acum din releas-ul oficial (adica este gata instalat).
Partea de Plugin Architecture permite aparitia in meniul din stanga al aplicatiei a functionalitatii de Plugin Management.

Mai departe, trebuie sa instalez plugins-uri. Instalarea se face de pe site-ul oficial CACTI --> documentation -->Plugins
Aici exista un tabel cu plugins-uri disponibile... Se da click pe unul dintre ele si ajung intr-o alta pagina
unde sunt prezentate toate versiunile acelui plugin. O downloadez pe cea mai recenta, o iploadez pe server, dupa care,
din folderul in care am salvat arhiva, o dezarhivez cu

```
tar -xf nume_arhiva
```

dupa care copiez folderul dezarhivat in cadrul /var/www/cacti/plugins/, astfel:

```
cp -r nume_folder_dezarhivat /var/www/cacti/plugins/
```

Dupa care din pagina web a aplicatiei, la sectiunea Plugins Management, incarc

respectivul plugin.

Instalare PHPList

Downloadez ultima versiune de pe site-ul PHPList, de la pagina:
http://www.phplist.com/download

De exemplu: phplist-2.10.19.tgz

Dupa care o urc pe server printr-un program gen: FTP sau SSH.

De exemplu il incarc in /home/florin/kituri/
Ma deplasez in respectivul folder:
cd /home/florin/kituri/

si apoi dezarhivez:
tar -xf phplist-2.10.19.tgz

In urma dezarhivarii a rezultat un folder numit: phplist-2.10.19

In interiorul acestuia exista un folder /public_html/lists. Va trebui sa uploadez folderul /lists in /var/www/
Prin urmare:
cd phplist-2.10.19
cd public_html
cp -R lists /var/www/

Daca vreau sa instalez phplist ca si subdomeniu, voi crea un alt folder in cadrul lui /var/www/lists/ si in acel folder
voi muta tot continutul de acum al lui lists.

de exemplu:
cd /var/www/lists/
mkdir cldgoldmail

In final trebuie sa am in /var/lists/cldgoldmail/ tot continutul care il aveam inainte in /lists/
Iar acum in /lists/ voi avea doar /cldgoldmail/ si favicon.ico

Mai departe trebuie sa creez baza de date necesara aplicatiei phpList.

```
mysql -u root -p
...
show databases;
create database nume_baza_De_date;
grant all on nume_baza_De_date.* to nume_user@localhost identified by "parola";
flush privileges;
```

Mai departe trebuie sa editam fisierul de configurare al aplicatiei:
nano /var/www/lists/cldgoldmail/config/config.php

De exemplu, pentru inovatop.ro, fisierul config.php este urmatorul:

```
<?php

/*

========================================================================

General settings for language and database

========================================================================

*/

# select the language module to use
# Look for <country>.inc files in the texts directory
# to find your language
# this is the language for the frontend pages. In the admin pages you can
# choose your language by using the dropdown in the pages.
# $language_module = "english.inc";
$language_module = "romanian.inc";

# what is your Mysql database server
$database_host = "localhost";

# what is the name of the database we are using
$database_name = "phplist691";

# who do we log in as?
$database_user = "phplist4news";

# and what password do we use
$database_password = 'smart4newsletter24';

# if you use multiple installations of PHPlist you can set this to
# something to identify this one. it will be prepended to email report
# subjects
$installation_name = 'PHPlist';

# if you want a prefix to all your tables, specify it here,
$table_prefix = "phplist_";

# if you want to use a different prefix to user tables, specify it here.
# read README.usertables for more information
$usertable_prefix = "phplist_user_";
```

```
# if you change the path to the PHPlist system, make the change here as well
# path should be relative to the root directory of your webserver (document root)
# you cannot actually change the "admin", but you can change the "lists"
# DO NOT include the file eg "index.php" because that is added when required. If you
do
# it is likely to break the tracking, see
http://mantis.phplist.com/view.php?id=15542
$pageroot = '/lists/goldmail';
$adminpages = '/goldmail/admin';

/*

=========================================================================

Settings for handling bounces

=========================================================================

*/

# Message envelope. This is the email that system messages come from
# it is useful to make this one where you can process the bounces on
# you will probably get a X-Authentication-Warning in your message
# when using this with sendmail
# NOTE: this is *very* different from the From: line in a message
# to use this feature, uncomment the following line, and change the email address
# to some existing account on your system
# requires PHP version > "4.0.5" and "4.3.1+" without safe_mode
# $message_envelope = 'listbounces@yourdomain';

# Handling bounces. Check README.bounces for more info
# This can be 'pop' or 'mbox'
$bounce_protocol = 'pop';

# set this to 0, if you set up a cron to download bounces regularly by using the
# commandline option. If this is 0, users cannot run the page from the web
# frontend. Read README.commandline to find out how to set it up on the
# commandline
define ("MANUALLY_PROCESS_BOUNCES",1);

# when the protocol is pop, specify these three
$bounce_mailbox_host = 'invtmtax.inovatop.ro';
#$bounce_mailbox_user = 'marketing@inovatop.ro';
$bounce_mailbox_user = 'bounce@inovatop.ro';
#$bounce_mailbox_password = 'definitiv24mkt';
$bounce_mailbox_password = 'definitiv24bounce';

# the "port" is the remote port of the connection to retrieve the emails
# the default should be fine but if it doesn't work, you can try the second
```

```
# one. To do that, add a # before the first line and take off the one before the
# second line

$bounce_mailbox_port = "110/pop3/notls";
#$bounce_mailbox_port = "110/pop3";

# when the protocol is mbox specify this one
# it needs to be a local file in mbox format, accessible to your webserver user
$bounce_mailbox = '/var/spool/mail/listbounces';

# set this to 0 if you want to keep your messages in the mailbox. this is
potentially
# a problem, because bounces will be counted multiple times, so only do this if you
are
# testing things.
$bounce_mailbox_purge = 1;

# set this to 0 if you want to keep unprocessed messages in the mailbox. Unprocessed
# messages are messages that could not be matched with a user in the system
# messages are still downloaded into PHPlist, so it is safe to delete them from
# the mailbox and view them in PHPlist
$bounce_mailbox_purge_unprocessed = 1;

# how many bounces in a row need to have occurred for a user to be marked
unconfirmed
$bounce_unsubscribe_threshold = 5;

/*

========================================================================

Security related settings

========================================================================

*/

# set this to 1 if you want PHPlist to deal with login for the administrative
# section of the system
# you will be able to add administrators who control their own lists
# default login is "admin" with password "phplist"
#
$require_login = 1;

# if you use login, how many lists can be created per administrator
define("MAXLIST",1);

# if you use commandline, you will need to identify the users who are allowed to run
# the script. See README.commandline for more info
$commandline_users = array("admin");
```

```
# or you can use the following to disable the check (take off the # in front of the
line)
# $commandline_users = array();

# as of version 2.4.1, you can have your users define a password for themselves as
well
# this will cause some public pages to ask for an email and a password when the
password is
# set for the user. If you want to activate this functionality, set the following
# to 1. See README.passwords for more information
define("ASKFORPASSWORD",0);

# if you also want to force people who unsubscribe to provide a password before
# processing their unsubscription, set this to 1. You need to have the above one set
# to 1 for this to have an effect
define("UNSUBSCRIBE_REQUIRES_PASSWORD",0);

# if a user should immediately be unsubscribed, when using their personal URL,
instead of
# the default way, which will ask them for a reason, set this to 1
define("UNSUBSCRIBE_JUMPOFF",0);

# when a user unsubscribes they are sent one final email informing them of
# their unsubscription. In order for that email to actually go out, a gracetime
# needs to be set otherwise it will never go out. The default of 5 minutes should
# be fine, but you can increase it if you experience problems
$blacklist_gracetime = 5;

# to increase security the session of a user is checked for the IP address
# this needs to be the same for every request. This may not work with
# network situations where you connect via multiple proxies, so you can
# switch off the checking by setting this to 0
define("CHECK_SESSIONIP",1);

# if you use passwords, you can store them encrypted or in plain text
# if you want to encrypt them, set this one to 1
# if you use encrypted passwords, users can only request you as an administrator to
# reset the password. They will not be able to request the password from
# the system
define("ENCRYPTPASSWORD",0);

# Check for host of email entered for subscription
# Do not use it if your server is not 24hr online
# make the 0 a 1, if you want to use it
$check_for_host = 0;

/*

========================================================================
```

```
Debugging and informational

==========================================================================

*/


# if test is true (not 0) it will not actually send ANY messages,
# but display what it would have sent
define ("TEST",0);

# if you set verbose to 1, it will show the messages that will be sent. Do not do
this
# if you have a lot of users, because it is likely to crash your browser
# (it does mine, Mozilla 0.9.2, well 1.6 now, but I would still keep it off :-)
define ("VERBOSE",0);

# some warnings may show up about your PHP settings. If you want to get rid of them
# set this value to 0
define ("WARN_ABOUT_PHP_SETTINGS",1);

# If you set up your system to send the message automatically, you can set this
value
# to 0, so "Process Queue" will disappear from the site
# this will also stop users from loading the page on the web frontend, so you will
# have to make sure that you run the queue from the commandline
# check README.commandline how to do this
define ("MANUALLY_PROCESS_QUEUE",1);

# after every run of the queue to send out messages, phpList will send a summary to
the
# admin address. If you want to stop this, set this to false or 0
define('SEND_QUEUE_PROCESSING_REPORT',true);

# if you want to use \r\n for formatting messages set the 0 to 1
# see also http://www.securityfocus.com/archive/1/255910
# this is likely to break things for other mailreaders, so you should
# only use it if all your users have Outlook (not Express)
define("WORKAROUND_OUTLOOK_BUG",0);

# user history system info.
# when logging the history of a user, you can specify which system variables you
# want to log. These are the ones that are found in the $_SERVER and the $_ENV
# variables of PHP. check
http://www.php.net/manual/en/language.variables.predefined.php
# the values are different per system, but these ones are quite common.
$userhistory_systeminfo = array(
  'HTTP_USER_AGENT',
  'HTTP_REFERER',
  'REMOTE_ADDR'
```

```
);

# add spamblock
# if you set this to 1, phplist will try to check if the subscribe attempt is a
spambot trying to send
# nonsense. If you think this doesn't work, set this to 0
# this is currently only implemented on the subscribe pages
define('USE_SPAM_BLOCK',1);

# notify spam
# when phplist detects a possible spam attack, it can send you a notification about
it
# you can check for a while to see if the spam check was correct and if so, set this
value
# to 0, if you think the check does it's job correctly.
# it will only send you emails if you have "Does the admin get copies of subscribe,
update and unsubscribe messages"
# in the configuration set to true
define('NOTIFY_SPAM',1);

/*

============================================================================

Feedback to developers

============================================================================

*/

# use Register to "register" to PHPlist.com. Once you set TEST to 0, the system will
then
# request the "Powered By" image from www.phplist.com, instead of locally. This will
give me
# a little bit of an indication of how much it is used, which will encourage me to
continue
# developing PHPlist. If you do not like this, set Register to 0.
define ("REGISTER",0);

# CREDITS
# We request you retain some form of credits on the public elements of
# PHPlist. These are the subscribe pages and the emails.
# This not only gives respect to the large amount of time given freely
# by the developers but also helps build interest, traffic and use of
# PHPlist, which is beneficial to future developments.
# By default the webpages and the HTML emails will include an image and
# the text emails will include a powered by line

# If you want to remove the image from the HTML emails, set this constant
# to be 1, the HTML emails will then only add a line of text as signature
```

```
define("EMAILTEXTCREDITS",0);

# if you want to also remove the image from your public webpages
# set the next one to 1, and the pages will only include a line of text
define("PAGETEXTCREDITS",0);

# in order to get some feedback about performance, PHPlist can send statistics to a
central
# email address. To de-activate this set the following value to 1
define ("NOSTATSCOLLECTION",0);

# this is the email it will be sent to. You can leave the default, or you can set it
to send
# to your self. If you use the default you will give me some feedback about
performance
# which is useful for me for future developments
# $stats_collection_address = 'phplist-stats@phplist.com';
$stats_collection_address = 'florin.dena@inovatop.ro';

/*

========================================================================

Miscellaneous

========================================================================

*/


# the number of criterias you want to be able to select when sending a message.
# Useful is to make it the same as the number of selectable attributes you enter in
the
# system, but that is up to you (selectable = select, radio or checkbox)
define ("NUMCRITERIAS",2);

# if you do not require users to actually sign up to lists, but only want to
# use the subscribe page as a kind of registration system, you can set this to 1 and
# users will not receive an error when they do not check a list to subscribe to
define("ALLOW_NON_LIST_SUBSCRIBE",0);

# batch processing
# if you are on a shared host, it will probably be appreciated if you don't send
# out loads of emails in one go. To do this, you can configure batch processing.
# Please note, the following two values can be overridden by your ISP by using
# a server wide configuration. So if you notice these values to be different
# in reality, that may be the case

## if you send the queue using your browser, you may want to consider settings like
this
```

```
## which will send 10 messages and then reload the browser to send the next 10.
However, this
## will not restrict the sending to any limits, so there's a good chance you will
## go over the limits of your ISP
# define("MAILQUEUE_BATCH_SIZE",10);
# define("MAILQUEUE_BATCH_PERIOD",1);

## if you send the queue using commandline, you can set it to something that
complies with the
## limits of your ISP, eg 300 messages an hour would be
# define("MAILQUEUE_BATCH_SIZE",300);
# define("MAILQUEUE_BATCH_PERIOD",3600);
# and then you need to set the cron to run every 5 minutes

# define the amount of emails you want to send per period. If 0, batch processing
# is disabled and messages are sent out as fast as possible

##-------------------------------------------------
# Pentru YAHOO! merge bine cu 18, 180, 5.
# Pentru DOMENII merge bine cu 20, 60, 1.
##-------------------------------------------------

define("MAILQUEUE_BATCH_SIZE",20);

# define the length of one batch processing period, in seconds (3600 is an hour)
# Please note: this setting has two consequences:
# 1. it will enforce that the amount of emails sent in the period identified here
does not exceed the amount
#  set in MAILQUEUE_BATCH_SIZE
# 2. there will be a delay of MAILQUEUE_BATCH_PERIOD when running the queue.
#
# number 1 is mostly when using commandline queue processing (strongly recommended)
# number 2 is when using browser queue processing. The browser will reload to send
the next
# batch after the amount of seconds set here

define("MAILQUEUE_BATCH_PERIOD",60);

# to avoid overloading the server that sends your email, you can add a little delay
# between messages that will spread the load of sending
# you will need to find a good value for your own server
# value is in seconds, and you can use fractions, eg "0.5" is half a second
# (or you can play with the autothrottle below)
define('MAILQUEUE_THROTTLE',1);

# year ranges. If you use dates, by default the drop down for year will be from
# three years before until 10 years after this the current value for year. If there
# is no current value the current year will be used.
# if you want to use a bigger range you can set the start and end year here
# be aware that the drop down may become very large.
```

```
# if set to 0 they will use the default behaviour. So I'm afraid you can't start
with
# year 0. Also be aware not to set the end year to something relatively soon in the
# future, or it will stop working when you reach that year.
define('DATE_START_YEAR',0);
define('DATE_END_YEAR',0);

# empty value prefix. This can be used to identify values in select attributes
# that are not allowed to be selected and cause an error "Please enter your ..."
# by using a top value that starts with this string, you can make sure that the
# selects do not have a default value, that may be accidentally selected
# eg. "-- choose your country"
define('EMPTY_VALUE_PREFIX','--');

# admin details for messages
# if this is enabled phplist will initialise the From in new messages to be the
# details of the logged in administrator who is sending the message
# otherwise it will default to the values set in the configure page that identify
# the From for system messages
define('USE_ADMIN_DETAILS_FOR_MESSAGES',1);

# test emails
# if you send a test email, phplist will by default send you two emails, one in HTML
format
# and the other in Text format. If you set this to 1, you can override this
behaviour
# and only have a test email sent to you that matches the user record of the user
that the
# test emails are sent to
define('SEND_ONE_TESTMAIL',0);

/*

============================================================================

Experimental Features

============================================================================

*/

# list exclude will add the option to send a message to users who are on a list
# except when they are on another list.
# this is currently marked experimental

define("USE_LIST_EXCLUDE",0);

# admin authentication module.
# to validate the login for an administrator, you can define your own authentication
module
```

```
# this is not finished yet, so don't use it unless you're happy to play around with
it
# if you have modules to contribute, open a tracker issue on
http://mantis.phplist.com
# the default module is phplist_auth.inc, which you can find in the "auth"
subdirectory of the
# admin directory. It will tell you the functions that need to be defined for
phplist to
# retrieve it's information.
# phplist will look for a file in that directory, or you can enter the full path to
the file

# eg
#$admin_auth_module = 'phplist_auth.inc';

# or
#$admin_auth_module = '/usr/local/etc/auth.inc';

# stacked attribute selection
# this is a new method of making a selection of attributes to send your messages to
# to start with, it doesn't seem to work very well in Internet Explorer, but it
works fine
# using Mozilla, Firefox, Opera (haven't tried any other browsers)
# so if you use IE, you may not want to try this.

# stacked attribute selection allows you to continuously add a selection of
attributes
# to your message. This is quite a bit more powerful than the old method, but it can
also
# cause very complex queries to be constructed that may take too long to calculate
# If you want to try this, set the value to 1, and give us feedback on how it's
going

# if you want to use dates for attribute selections, you need to use this one

define("STACKED_ATTRIBUTE_SELECTION",0);


# send a webpage. You can send the contents of a webpage, by adding
# [URL:http://website/file.html] as the content of a message. This can also be
personalised
# for users by using eg
# [URL:http://website/file.html?email=[email]]
# the timeout for refetching a URL can be defined here. When the last time a URL has
been
# fetched exceeds this time, the URL will be refetched. This is in seconds, 3600 is
an hour
# this only affects sending within the same "process queue". If a new process queue
is started
# the URL will be fetched the first time anyway. Therefore this is only useful is
```

```
processing
# your queue takes longer than the time identified here.
define('REMOTE_URL_REFETCH_TIMEOUT',3600);

# Mailqueue autothrottle. This will try to automatically change the delay
# between messages to make sure that the MAILQUEUE_BATCH_SIZE (above) is spread
evently over
# MAILQUEUE_BATCH_PERIOD, instead of firing the Batch in the first few minutes of
the period
# and then waiting for the next period. This only works with mailqueue_throttle off
# it still needs tweaking, so send your feedback to http://mantis.phplist.com if you
find
# any issues with it
define('MAILQUEUE_AUTOTHROTTLE',0);

# Click tracking
# If you set this to 1, all links in your emails will be converted to links that
# go via phplist. This will make sure that clicks are tracked. This is experimental
and
# all your findings when using this feature should be reported to mantis
# for now it's off by default until we think it works correctly
define('CLICKTRACK',0);

# Click track, list detail
# if you enable this, you will get some extra statistics about unique users who have
clicked the
# links in your messages, and the breakdown between clicks from text or html
messages.
# However, this will slow down the process to view the statistics, so it is
# recommended to leave it off, but if you're very curious, you can enable it
define('CLICKTRACK_SHOWDETAIL',0);

# Domain Throttling
# You can activate domain throttling, by setting USE_DOMAIN_THROTTLE to 1
# define the maximum amount of emails you want to allow sending to any domain and
the number
# of seconds for that amount. This will make sure you don't send too many emails to
one domain
# which may cause blacklisting. Particularly the big ones are tricky about this.
# it may cause a dramatic increase in the amount of time to send a message,
depending on how
# many users you have that have the same domain (eg hotmail.com)
# if too many failures for throttling occur, the send process will automatically add
an extra
# delay to try to improve that. The example sends 1 message every 2 minutes.

define('USE_DOMAIN_THROTTLE',0);
define('DOMAIN_BATCH_SIZE',1);
define('DOMAIN_BATCH_PERIOD',120);
```

```
# if you have very large numbers of users on the same domains, this may result in
the need
# to run processqueue many times, when you use domain throttling. You can also tell
phplist
# to simply delay a bit between messages to increase the number of messages sent per
queue run
# if you want to use that set this to 1, otherwise simply run the queue many times.
A cron
# process every 10 or 15 minutes is recommended.
define('DOMAIN_AUTO_THROTTLE',0);

# admin language
# if you want to disable the language switch for the admin interface (and run all in
english)
# set this one to 0
define('LANGUAGE_SWITCH',1);

# advanced bounce processing
# with advanced bounce handling you are able to define regular expressions that
match bounces and the
# action that needs to be taken when an expression matches. This will improve
getting rid of bad emails in
# your system, which will be a good thing for making sure you are not being
blacklisted by other
# mail systems
# if you use this, you will need to teach your system regularly about patterns in
new bounces
define('USE_ADVANCED_BOUNCEHANDLING',0);

/*
=============================================================================

Security

=============================================================================

*/

# CHECK REFERRER. Set this to "true" to activate a check on each request to make
sure that
# the "referrer" in the request is from ourselves. This is not failsafe, as the
referrer may
# not exist, or can be spoofed, but it will help a little
# it is also possible that it doesn't work with Webservers that are not Apache, we
haven't tested that.
define('CHECK_REFERRER',false);

# if you activate the check above, you can add domain names in this array for those
domains
# that you trust and that can be allowed as well
```

```
# only mention the domain for each.
# for example: $allowed_referrers =
array('mydomain.com','msn.com','yahoo.com','google.com');
$allowed_referrers = array();

/*

========================================================================

Advanced Features, HTML editor, RSS, Attachments, Plugins. PDF creation

========================================================================

*/

# you can specify the encoding for HTML and plaintext messages here. This only
# works if you do not use the phpmailer (see below)
# the default should be fine. Valid options are 7bit, quoted-printable and base64
define("HTMLEMAIL_ENCODING","quoted-printable");
define("TEXTEMAIL_ENCODING",'7bit');


# PHPlist can send RSS feeds to users. Feeds can be sent daily, weekly or
# monthly. To use the feature you need XML support in your PHP installation, and you
# need to set this constant to 1
define("ENABLE_RSS",0);

# if you have set up a cron to download the RSS entries, you can set this to be 0
define("MANUALLY_PROCESS_RSS",1);

# the FCKeditor is now included in PHPlist, but the use of it is experimental
# if it's not working for you, set this to 0
# NOTE: If you enable TinyMCE please disable FCKeditor and vice-versa.
define("USEFCK",1);

# If you want to upload images to the FCKeditor, you need to specify the location
# of the directory where the images go. This needs to be writable by the webserver,
# and it needs to be in your public document (website) area
# the directory is relative to the root of PHPlist as set above
# This is a potential security risk, so read README.security for more information
define("FCKIMAGES_DIR","uploadimages");

# TinyMCE Support (http://tinymce.moxiecode.com/)
# It is suggested to copy the tinymce/jscripts/tiny_mce directory from the
# standard TinyMCE distribution into the public_html/lists/admin/plugins
# directory in order to keep the install clean.
# NOTE: If you enable TinyMCE please disable FCKeditor and vice-versa.
# Set this to 1 to turn on TinyMCE for writing messages:
define("USETINYMCEMESG", 0);
# Set this to 1 to turn on TinyMCE for editing templates:
```

```
define("USETINYMCETEMPL", 0);
# Set this to path of the TinyMCE script, relative to the admin directory:
define("TINYMCEPATH", "plugins/tiny_mce/tiny_mce.js");
# Set this to the language you wish to use for TinyMCE:
define("TINYMCELANG", "en");
# Set this to the theme you wish to use.  Default options are: simple, default and
advanced.
define("TINYMCETHEME", "advanced");
# Set this to any additional options you wish.  Please be careful with this as you
can
# inadvertantly break TinyMCE.  Rever to the TinyMCE documentation for full details.
# Should be in the format: ',option1:"value",option2:"value"'   <--- note comma at
beginning
define("TINYMCEOPTS", "");

# Manual text part, will give you an input box for the text version of the message
# instead of trying to create it by parsing the HTML version into plain text
define("USE_MANUAL_TEXT_PART",0);

# attachments is a new feature and is currently still experimental
# set this to 1 if you want to try it
# caution, message may become very large. it is generally more
# acceptable to send a URL for download to users
# if you try it, it will be appreciated to give feedback to the
# users mailinglist, so we can learn whether it is working ok
# using attachments requires PHP 4.1.0 and up
define("ALLOW_ATTACHMENTS",0);

# if you use the above, how many would you want to add per message (max)
# You can leave this 1, even if you want to attach more files, because
# you will be able to add them sequentially
define("NUMATTACHMENTS",1);

# when using attachments you can upload them to the server
# if you want to use attachments from the local filesystem (server) set this to 1
# filesystem attachments are attached at real send time of the message, not at
# the time of creating the message
define("FILESYSTEM_ATTACHMENTS",0);

# if you add filesystem attachments, you will need to tell PHPlist where your
# mime.types file is.
define("MIMETYPES_FILE","/etc/mime.types");

# if a mimetype cannot be determined for a file, specify the default mimetype here:
define("DEFAULT_MIMETYPE","application/octet-stream");

# you can create your own pages to slot into PHPlist and do certain things
# that are more specific to your situation (plugins)
# if you do this, you can specify the directory where your plugins are. It is
# useful to keep this outside the PHPlist system, so they are retained after
```

```
# upgrading
# there are some example plugins in the "plugins" directory inside the
# admin directory
# this directory needs to be absolute, or relative to the admin directory

define("PLUGIN_ROOTDIR","/home/me/phplistplugins");

# uncomment this one to see the examples in the system (and then comment the
# one above)
#define("PLUGIN_ROOTDIR","plugins");


# the attachment repository is the place where the files are stored (if you use
# ALLOW_ATTACHMENTS)
# this needs to be writable to your webserver user
# it also needs to be a full path, not a relative one
# for secutiry reasons it is best if this directory is not public (ie below
# your website document root)
$attachment_repository = '/tmp';

# if you want to be able to send your messages as PDF attachments, you need to
install
# FPDF (http://www.fpdf.org) and set these variables accordingly

# define('FPDF_FONTPATH','/home/pdf/font/');
# require('fpdf.php');
# define("USE_PDF",1);
# $pdf_font = 'Times';
# $pdf_fontstyle = '';
# $pdf_fontsize = 14;

# the mime type for the export files. You can try changing this to
# application/vnd.ms-excel to make it open automatically in excel
$export_mimetype = 'application/csv';

# if you want to use export format optimized for Excel, set this one to 1
define("EXPORT_EXCEL",1);

# Repetition. This adds the option to repeat the same message in the future.
# After the message has been sent, this option will cause the system to
automatically
# create a new message with the same content. Be careful with it, because you may
# send the same message to your users
# the embargo of the message will be increased with the repetition interval you
choose
# also read the README.repetition for more info
define("USE_REPETITION",0);

# Prepare a message. This system allows you to create messages as a super admin
# that can then be reviewed and selected by sub admins to send to their own lists
```

```
# it is old functionality that is quite confusing, and therefore by default it
# is now off. If you used to use it, you can switch it on here. If you did not
# use it, or are a new user, it is better to leave it off. It has nothing to
# do with being able to edit messages.
define("USE_PREPARE",0);

#0011857: forward to friend, retain attributes
# When forwarding ('to a friend') the message will be using the attributes of the
destination email by default.
# This often means the message gets stripped of al its attributes.
# When setting this constant to 1, the message will use the attributes of the
forwarding user. It can be used
# to connect the destinatory to the forwarder and/or reward the forwarder.
define("KEEPFORWARDERATTRIBUTES",0);

#0011860: forward to friend, multiple emails
# This setting defines howmany email addresses you can enter in the forward page.
# Default is 1 to not change behaviour from previous version.
define("FORWARD_EMAIL_COUNT",1);

#0011996: forward to friend - personal message
# Allow user to add a personal note when forwarding 'to a friend'
# 0 will turn this option off. default is 0 to not change behaviour from previous
version.
# 500 is recommended as a sound value to write a little introductory note to a
friend
#The note is prepeded to both text and html messages and will be stripped of all
html
define("FORWARD_PERSONAL_NOTE_SIZE",500);

#0013076: different content when forwarding 'to a friend'
# Allow admin to enter a different message that will be sent when forwarding 'to a
friend'
# This will show an extra tab in the message dialog.
define("FORWARD_ALTERNATIVE_CONTENT",0);

#0013845 Lead Ref Scheme
# When this setting has a value <> '' all succesfull handovers to the MTA will be
counted
# and saved in the attribute with the name of this setting.
#define('FORWARD_FRIEND_COUNT_ATTRIBUTE', 'FriendCount');

# If you want to use the PHPMailer class from phpmailer.sourceforge.net, set the
following
# to 1. If you tend to send out html emails, it is recommended to do so.
define("PHPMAILER",1);

# To use a SMTP please give your server hostname here, leave it blank to use the
standard
# PHP mail() command.
```

```
# define("PHPMAILERHOST",'');

define("PHPMAILERHOST",'invtmtax.inovatop.ro');

# if you want to use smtp authentication when sending the email uncomment the
following
# two lines and set the username and password to be the correct ones
# $phpmailer_smtpuser = 'smtpuser';
# $phpmailer_smtppassword = 'smtppassword';

$phpmailer_smtpuser = 'marketing@inovatop.ro';
$phpmailer_smtppassword = 'definitiv24mkt';

# tmpdir. A location where phplist can write some temporary files if necessary
# Make sure it is writable by your webserver user, and also check that you have
# open_basedir set to allow access to this directory. Linux users can leave it as it
is.
# this directory is used for all kinds of things, mostly uploading of files (like in
# import), creating PDFs and more
$tmpdir = '/tmp';

# if you are on Windoze, and/or you are not using apache, in effect when you are
getting
# "Method not allowed" errors you will want to uncomment this
# ie take off the #-character in the next line
# using this is not guaranteed to work, sorry. Easier to use Apache instead :-)
# $form_action = 'index.php';

# select the database module to use
# anyone wanting to submit other database modules is
# very welcome!
$database_module = "mysql.inc";

# you can store sessions in the database instead of the default place by assigning
# a tablename to this value. The table will be created and will not use any prefixes
# this only works when using mysql and only for administrator sessions
# $SessionTableName = "phplistsessions";

# there is now support for the use of ADOdb http://php.weblogs.com/ADODB
# this is still experimental, and any findings should be reported in the
# bugtracker
# in order to use it, define the following settings:
#$database_module = 'adodb.inc';
#$adodb_inc_file = '/path/to/adodb_inc.php';
#$adodb_driver = 'mysql';

# if you want more trouble, make this 63 (very unlikely you will like the result)
$error_level = error_reporting(0);

?>
```

Trebuie apoi sa pregatesc setarea subdomeniului in fisierul de configurare apache

nano /etc/apache2/sites-available/phplist

si editez in el urmatoarele:

```
## Virtual Host for PHPLIST

<VirtualHost *:80>
        ServerName invtphlx.inovatop.ro
        ServerAdmin sysadmin@inovatop.ro

        DocumentRoot /var/www/lists
        Options -Indexes

        RewriteEngine On
        RewriteCond %{HTTP_HOST} !invtphlx.inovatop.ro
        RewriteRule (.*) [L]

        Redirect /goldmail/admin/ https://invtphlx.inovatop.ro/goldmail/admin/

        <Directory /var/www/lists/goldmail/>
                Options +FollowSymLinks -Indexes
                DirectoryIndex index.php
                AllowOverride None
                Order Allow,Deny
                Allow from ALL
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log
        # Possible values include: debug, info, notice, warn, error, crit, alert,
emerg.
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<VirtualHost *:443>
        ServerName invtphlx.inovatop.ro
        ServerAdmin sysadmin@inovatop.ro

        DocumentRoot /var/www/lists
        Options -Indexes

        RewriteEngine On
        RewriteCond %{HTTP_HOST} !invtphlx.inovatop.ro
```

```
        RewriteRule (.*) [L]

        # All other pages have to be on http
        RewriteCond %{SERVER_PORT} ^443$ [OR]
        RewriteCond %{HTTPS} on
        RewriteCond %{REQUEST_URI} !^/goldmail/admin/ [NC]
        RewriteRule ^(.*)$ http://invtphlx.inovatop.ro$1 [L,R=301]

        <Directory /var/www/lists/goldmail/admin/>
                Options +FollowSymLinks -Indexes
                DirectoryIndex index.php
                AllowOverride None

                Order Deny,Allow
                Deny from ALL
                Allow from 89.35.233.244                # TQM LAN
                Allow from 86.125.50.152                # SER LAN
                # Allow from 89.35.233.245              # Sala INFO

                <IfModule mod_php5.c>
                        AddType application/x-httpd-php .php
                        php_flag magic_quotes_gpc Off
                        php_flag track_vars On
                        php_flag register_globals Off
                        php_value include_path .
                </IfModule>
        </Directory>

        # SSL Engine Switch: Enable/Disable SSL for this virtual host.
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/webcert.crt
        SSLCertificateKeyFile /etc/apache2/ssl/webcert.key

        ErrorLog ${APACHE_LOG_DIR}/error.log
        # Possible values include: debug, info, notice, warn, error, crit, alert,
emerg.
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined
</VirtualHost>

----------------------------------------

Activez site-ul:
a2ensite phplist
service apache2 restart

Apoi merg la adresa:
https://cladphlx.cursuriladistanta.ro/cldgoldmail/admin

si incep instalare - va trebui sa initializez baza de date...
```

Continui cu setarea introducand userul predefinit: admin, cu parola phplist

Merg la link-ul setup si schimb datele de conectare - user si parola:

1. Schimb parola userului admin in altceva si apoi salvez.
2. Ies cu logout si verific conectarea userului admin cu noua parola.
3. Creez un alt user cu o noua parola si il definesc ca Superadmin punand un "1" in campul corespunzator,
iar unde ma intreaba daca este desabled, nu pun nimic, apoi salvez.
4. Ies cu logout si ma loghez din nou cu noul user creat si verific ca totul este OK.
5. Merg si dezactivez userul admin, punand un "1" in campul unde intreaba daca este disabled, apoi salvez.
6. Ies cu logout si verific din nou totul.

Dupa ce fac toate setarile. in cazul in care daca am in lista mailuri care nu sunt valide phplist incearca sa trimita
catre ele la nesfarsit, atunci trebuie sa corectez acest bug.
Merg in /var/www/goldmail/lists/admin/processqueue.php si ii fac copie sub forma processqueue.php.original
Dupa care modific fisierul processqueue.php, dezactivand liniile: 673 si 677, respectiv:

```
//           if (!$throttled && !validateEmail($useremail)) {
               logEvent("invalid email $useremail user marked unconfirmed");
               Sql_Query(sprintf('update %s set confirmed = 0 where email = "%s"',
                 $GLOBALS['tables']['user'],$useremail));
//           }
```

Dupa aceea verific daca s-a corectat, trimitand un nou mesaj.

phpList e setat sa trimita e-mailuri din partea adresei listmaster@domeniu.tld. Pentru a seta astfel incat sa vina de la
o adresa bine stabilita (exemplu: marketng@domeniu.tld), atunci modifica urmatoarele 2 fisiere:

E vorba despre:
/admin/sendmaillib.php   <--- linia 51

si despre:
/admin/help/en/from.php   <--- liniile 6 si 7

Dupa toate acestea, mailurile vor veni din partea marketing@domeniu.tld.

Some Final Notes on Security

You'll note that there are a fair number of configuration files that contain database passwords for the mail and Horde data in this server, and that includes PHP

files sitting in the webroot. This is not really the dominant security concern: the mail users are virtual and only the server administrator should be logging in as a system user. On AWS the default setup is for SSH login to use keys rather than passwords, and only the ubuntu user has a key setup to allow login. You can also easily lock down the SSH port to selected IP addresses via the security group applied to the server. Further, you can set .htaccess directives to ensure that no web visitor can directly view configuration files - and thus they are only used as includes, which covers the rare case where some error causes PHP files to be served by Apache as plain text. MySQL access is from localhost only, in any case.

All in all the lowest bar from a security perspective is probably that the mail server built here runs a couple of complicated PHP web applications with database access. A serious breach there would involve a way to upload and execute an arbitrary PHP script or shell command with the www-data user's permissions, or various other XSS attacks allowing for session hijacking of administrators - either way, or just by getting into the mail and Horde databases, compromise of the webroot is compromise of all of the important functions of the server. Horde has had multiple vulnerabilities in past years, but at some point you have to pick your software. On the whole which given the choice I'd rather go with the output of established development communities whose members have a demonstrated track record of vulnerabilities found and fixed, and where there are a large number of eyes directed at the codebase.

These are all good reasons for setting up your webmail on a different server from the one running Postfix and Dovecot - something to bear in mind.

Of course being on AWS - or indeed pretty much any sort of easily available hosting in the US wherein the server is not in your front room - means that the US government has free access to your data any time they particularly feel up to the task, and you may never know a copy was taken. One of the welcome forthcoming evolutions in virtual hosting services will be some form of turn-key encrypted server operations such that you can have the convenience of an AWS-style service but without the transparency it affords the present day panopticon-in-the-making.

==========

Sender ID / SPF
Reverse DNS
upgrade apache2
Verificare de ce apare header aiurea la accesare http://www.inovatop.ro:443
Reguli iptables de securitate
Verificare procese pornite degeaba. Vezi: service sendmail status
Erorile din loguri !!!

1.3 RDNS_NONE Delivered to internal network by a host with no rDNS
0.1 DKIM_SIGNED Message has a DKIM or DK signature, not necessarily valid
DomainKeys Signature validation: not available
DomainKeys Policy: query failed
DKIM Author Domain Signing Practices: no DNS record for _adsp._domainkey.inovatop.ro

ADSP is not required for DKIM signature validation.
Note: The authentication results are not available as
there was no signature header or the signature could
not be verified

What is "reverse DNS" and do I need it?

Reverse DNS is IP address to domain name mapping - the opposite of forward (normal) DNS which maps domain names to IP addresses.

Reverse DNS is separate from forward DNS.
Forward DNS for "abc.com" pointing to IP address "1.2.3.4", does not necessarily mean that reverse DNS for IP "1.2.3.4" also points to "abc.com".
This comes from two separate sets of data.

A special PTR-record type is used to store reverse DNS entries. The name of the PTR-record is the IP address with the segments reversed + ".in-addr.arpa".
For example the reverse DNS entry for IP 1.2.3.4 would be stored as a PTR-record for "4.3.2.1.in-addr.arpa".

Reverse DNS is also different from forward DNS in who points the zone (domain name) to your DNS server.
With forward DNS, you point the zone to your DNS server by registering that domain name with a registrar.
With reverse DNS, your Internet connection provider (ISP) must point (or "sub-delegate") the zone ("....in-addr.arpa") to your DNS server.
Without this sub-delegation from your ISP, your reverse zone will not work.

Reverse DNS is mostly used by humans for such things as tracking where a web-site visitor came from, or where an e-mail message originated etc.
It is typically not as critical in as forward DNS - visitors will still reach your web-site just fine without any reverse DNS for your web-server IP or the visitor's IP.

However reverse DNS is important for one particular application.
Many e-mail servers on the Internet are configured to reject incoming e-mails from any IP address which does not have reverse DNS.
So if you run your own e-mail server, reverse DNS must exist for the IP address that outgoing e-mail is sent from.
It does not matter what the reverse DNS record for your IP address points to as long as it is there. If you host multiple domains on one e-mail server, just setup reverse DNS to point to whichever domain name you consider primary.
(e-mail servers checking for reverse DNS do recognize that it is normal to host many domains on a single IP address and it would be impossible to list all those domains in reverse DNS for the IP).

Special note about AOL:
It appears that AOL has recently restricted this even further:
They also require that reverse DNS points to a "fully qualified domain name" (we assume they mean a name with 3 or more segments, such as "mail.jhsoft.com"), and

that this name does not contain the segments "in-addr.arpa" and is not just an IP address.
If you want to be able to send e-mail to AOL users, the reverse DNS record for your e-mail server IP address must adhere to this as well.
For details, please see http://postmaster.aol.com/Postmaster.Errors.php#whatisrdns

REFERENCES:
For more information, please see the following knowledge base articles:

==========

Configuring Reverse DNS in BIND 9

Reverse DNS is the process of using DNS to translate IP addresses to hostnames. Reverse DNS is the opposite of Forward DNS, which is used to translate hostnames to IP addresses.

One way to see reverse DNS at work is to use nslookup a tool on most OS’s.

Let’s use `nslookup` to do a forward and reverse DNS lookup on redhat.com:

##FORWARD LOOKUP

```
[phil@ns1 ~]$ nslookup redhat.com
Server:         206.71.175.XX
Address:        206.71.175.XX#53

Non-authoritative answer:
Name:   redhat.com
Address: 209.132.177.50
```

##REVERSE LOOKUP

```
[phil@ns1 ~]$ nslookup 209.132.177.50
Server:         206.71.175.XX
Address:        206.71.175.XX#53

Non-authoritative answer:
50.177.132.209.in-addr.arpa     name = www.redhat.com.

Authoritative answers can be found from:
177.132.209.in-addr.arpa        nameserver = ns3.redhat.com.
177.132.209.in-addr.arpa        nameserver = ns2.redhat.com.
177.132.209.in-addr.arpa        nameserver = ns1.redhat.com.
```

Reverse DNS is setup by configuring PTR records (Pointer Records) on your DNS server.

This is in different to Forward DNS, which are configured with A records (Address

Records).

Typically you or a DNS provider is in charge of Forward DNS. In the case of Reverse DNS most likely your ISP supplying your IP information will have responsibility. You would simply send them what Hostname resolves to what IP, and they would setup the PTR records. You can setup Reverse DNS on your own name servers if you choose which we will cover in this article.

Your ISP or hosting provider may delegate your own range of IP addresses, or you may have NAT setup for Private IP space you control, in this case you must configure Reverse DNS thru PTR records on your DNS server.

A lot of Systems Administrators configure Forward DNS but not Reverse DNS. In most cases when you do this things will work fine, however some applications require doing Reverse DNS lookups in which case you could run into latency issues and a whole slew of other issues.

Common applications and protocols such as IRC, SMTP, Backup utilities, and Databases sometimes use Reverse DNS.

It is best practice to configure Reverse DNS from the get go, to avoid troubleshooting headaches.

Below is a quick example how-to.

Say you NAT Private IP’s in your network 192.168.0.1-192.168.0.255

STEP 1 create a zone file and place it where you store your zone files named

0.168.192.in-addr.arpa

(Notate your address space backwards missing last octect with .in-addr.arpa appended)

Your zone file will look like this: (between ##)

#######

```
@       IN      SOA     ns1.yournameserver.com. root.domain.com.     (
2007040301      ;serial
14400                ;refresh
3600                 ;retry
604800              ;expire
10800                ;minimum
)

0.168.192.in-addr.arpa.                IN      NS      ns1.yournameserver.com.
0.168.192.in-addr.arpa.                IN      NS      ns2.yournameserver.com.

2               IN      PTR     blah1.domain.com.
```

```
3               IN      PTR     blah2.domain.com.
4               IN      PTR     blah3.domain.com.
5               IN      PTR     blah4.domain.com.
6               IN      PTR     blah5.domain.com.

########
```

The example zone file above stipulates the below:

```
192.168.0.2 blah1.domain.com
192.168.0.3 blah2.domain.com
192.168.0.4 blah3.domain.com
192.168.0.5 blah4.domain.com
192.168.0.6 blah5.domain.com
```

The number 2-6 are the last octect of 192.168.0. and PTR is the pointer.

STEP 2 Enter the zone into your named.conf or named.boot as you would a regular zone.

This would go into your Master DNS server or Primary DNS server

```
zone "0.168.192.in-addr.arpa" IN {
type master;
file "0.168.192.in-addr.arpa";
allow-update { none; };
};
```

This would go into your Slave DNS server or Secondary DNS server

```
zone "0.168.192.in-addr.arpa" IN {
type slave;
file "0.168.192.in-addr.arpa";
masters { whateveryourmasteripis; };
};
```

STEP 3

Wholla if configured right you should be up and running. Make sure to tail your log file when you restart DNS for any errors in syntax.

Ensuring Your rDNS Configuration is Working

You can make sure you rDNS configuration is working by issuing a simple command:

```
    host 192.168.0.1
```

In the example above, 192.168.0.1 is meant to represent the IP address that corresponds to the domain, subdomain, or addon domain name for which

you have configured rDNS.

If rDNS is properly configured, you will see a message similar to the
following:

    1.0.192.168.in-addr.arpa domain name pointer example.com

If rDNS is not properly configured, you will see the following message:

    Host 1.0.192.168.in-addr.arpa. not found: 3(NXDOMAIN)

==========
==========

SuexecUserGroup "#1022" "#1017"

ServerName cursuri-web-design.ro
ServerAlias www.cursuri-web-design.ro
ServerAlias webmail.cursuri-web-design.ro
ServerAlias admin.cursuri-web-design.ro

DocumentRoot /home/cursuriwebdesign/public_html
ErrorLog /var/log/virtualmin/cursuri-web-design.ro_error_log
CustomLog /var/log/virtualmin/cursuri-web-design.ro_access_log combined
ScriptAlias /cgi-bin/ /home/cursuriwebdesign/cgi-bin/
DirectoryIndex index.html index.htm index.php index.php4 index.php5

<Directory /home/cursuriwebdesign/public_html>
        Options -Indexes +IncludesNOEXEC +FollowSymLinks
        allow from all
        AllowOverride All
</Directory>

<Directory /home/cursuriwebdesign/cgi-bin>
        allow from all
</Directory>

RewriteEngine on
RewriteCond %{HTTP_HOST} =webmail.cursuri-web-design.ro
RewriteRule ^(.*) https://cursuri-web-design.ro:20000 [R]
RewriteCond %{HTTP_HOST} =admin.cursuri-web-design.ro
RewriteRule ^(.*) https://cursuri-web-design.ro:10000/ [R]

How to: Purge, Flush or Delete Postfix Queue, or a Single Email

To flush or purge the postfix mail queue, just enter this command
postfix -f

But if you need to delete an individual email from the queue, you'll first need to see the queue. Traditionally you use mailq this time we'll use:
postqueue -p

And the output should show all messages in queue:
5642B4D8647* 1683500 Tue Jun 3 08:37:27 xxxxxx@xxxxxxx.com
                                          rrrrrrrrr@hotmail.com

9359B4D82B1* 1635730 Tue Jun 3 08:36:53 xxxxxx@xxxxxxx.com
                                          yyyyyyyy@hotmail.com

The first number is the message ID, if you only want to delete one of them, enter:
postsuper -d 5642B4D8647

That will only delete one email for the queue, that specific email you want to delete from it.

If you want to delete all deferred mails, you can use:
postsuper -d deferred
sau
postsuper -d ALL

==========
==========

Am instalat Aplicatia de facturare Server - Client numita:
icefact-srv_0.9-1_amd64.deb

S-a instalat cu:
dpkg -i icefact-srv_0.9-1_amd64.deb   <--- Comanda se ruleaza de orisiunde

Verific daca a pornit serverul cu comanda:
service icefact-srv status

La instalare a dat urmatoarele mesaje:
Setting up icefact-srv (0.9-1) ...
 Adding system startup for /etc/init.d/icefact-srv ...
   /etc/rc0.d/K20icefact-srv -> ../init.d/icefact-srv
   /etc/rc1.d/K20icefact-srv -> ../init.d/icefact-srv
   /etc/rc6.d/K20icefact-srv -> ../init.d/icefact-srv
   /etc/rc2.d/S20icefact-srv -> ../init.d/icefact-srv
   /etc/rc3.d/S20icefact-srv -> ../init.d/icefact-srv
   /etc/rc4.d/S20icefact-srv -> ../init.d/icefact-srv
   /etc/rc5.d/S20icefact-srv -> ../init.d/icefact-srv
 * Starting IceFact Server icefact-srv   [OK]
root@invtmtax:/home/inotanaka96/kiturile-mele# service icefact-srv status
 * icefact-srv is running

Dezinstalarea se poate face cu:

dpkg -r PACKAGE_NAME

S-a instalat in /opt/icefact/icefact-srv

Note:
1) daca rulati procedura de instalare ca superuser (root), IceFact se va instala in /opt/icefact si va crea un symlink in /usr/bin (poate ar fi fost mai bine in /usr/local/bin, dar unele distro-uri nu il au in PATH)
2) daca rulati procedura de instalare ca user obisnuit, IceFact se va instala in $HOME/icefact si va pune si un shortcut pe desktop
3) baza de date se afla in $HOME/icefact.db

Serverul asculta pe portul 4000, prin urmare acesta trebuie sa-l permit in iptables.
iptables -I INPUT 10 -p tcp --dport 4000 -j ACCEPT

In client, dupa instalarea in windows, dau click dreapta pe iconita de start, aleg Properties si la Target, modific in:
"C:\Program Files (x86)\IceFact\icefact.exe" InovaTop@86.107.58.226

==========
==========