Creazione di un Server di Posta Elettronica con Postfix, Courier, DSPAM e SquirrelMail

Scritto da ***Iarno Pagliani*** (iarno.pagliani@gmail.com) ed ***Alessandro Tani*** (alessandro.tani@gmail.com)

- Pubblicato il giorno 19 Gennaio 2009 -

Nel corso degli ultimi anni, la posta elettronica è diventata uno dei servizi più critici per le aziende. Da semplice veicolo di informazioni, la posta elettronica, è divenuta uno dei più importanti strumenti aziendali. Riunioni, conferme d'ordine, richieste di fatturazione, informazioni riservate; oggi tutte queste attività vengono svolte tramite l'utilizzo della posta elettronica. Risulta difficile pensare che una società, anche piccola, possa fare a meno della posta elettronica per più di due giorni lavorativi consecutivi! Ciò non di meno, non tutte le soluzioni di posta elettronica adottate dalle aziende, sono adeguate al livello di criticità che la posta elettronica ricopre per quelle aziende. Impreparazione da parte del personale direttivo, scarsa attenzione alla sicurezza, sottovalutazione dei rischi, sono tra le principali cause di questo stato di degrado. Questo articolo si propone di spiegare, nel modo più dettagliato possibile, come realizzare un semplice server di posta elettronica per piccole e medie imprese e come si possa garantire un adeguato livello di servizio al server di posta elettronica stesso. Per realizzare il server di posta elettronica, si ricorrerà ad alcuni dei migliori programmi scritti dalla comunità Open Source come Postfix e Courier per l'invio e la consultazione dei messaggi, SquirrelMail e IMAPProxy per accedere via web alla posta elettronica, ClamAV, ClamSMTP e DSPAM, per controllare la presenza di virus all'interno dei messaggi ricevuti ed inviati e per ridurre l'arrivo di messaggi indesiderati (SPAM).

Indice

Licenza

Lo scenario

Per facilitare la spiegazione, supporremo di dover realizzare il server di posta elettronica di una società, la Home Works S.p.A, la quale ha recentemente realizzato una propria infrastruttura PKI interna e si appresta a sostituire il proprio server di posta elettronica attuale.

Introduzione

La Home Works S.p.A. è una società dinamica in espansione. Al momento la sua unica sede è a Reggio Emilia, ma nel corso dei prossimi due anni dovrebbe aprire alcune sedi commerciali in Germania, Russia, India e Cina. In queste sedi commerciali sono previsti non più di dieci dipendenti, i quali avranno il compito di promuovere e supportare la vendita dei prodotti realizzati dalla Home Wors S.p.A. in questi paesi. Queste persone saranno dotate di un portatile aziendale e di un dispositivo palmare per poter operare al meglio in qualunque situazione. La sede principale della Home Works, ovvero la sede di Reggi Emilia, è composta da circa 450 persone, di cui solamente 200 hanno a disposzione un computer su cui operare stabilmente. Ciascuna di queste persone verrà dotata di un indirizzo email personale o di ufficio a seconda delle mansioni svolte, in ogni caso, a tutte le persone verrà dato un certificato digitale con cui firmare elettronicamente i propri messaggi di posta elettronica (questi stessi certificati digitali potranno venire utilizzati anche per *criptare* i messaggi di posta elettronica). Al momento la Home Works S.p.A. utilizza al suo interno un server di posta elettronica basato sulla vecchia versione di un noto programma commerciale per la posta elettronica. Compito del personale IT è quello di creare un nuovo server di posta elettronica che garantisca le seguenti funzionalità:

- il sistema di licenze del server di posta elettronica deve essere tale da poter creare quante caselle email (*mailbox*) la società desideri, senza costi aggiuntivi oltre a quelli di realizzazione della soluzione di posta elettronica;
- deve risultare possibile accedere alle caselle email (*mailbox*) anche via web, possibilmente in modo sicuro, tramite il protocollo HTTPS;
- l'interfaccia web per accedere alla posta elettronica deve supportare le lingue Tedesca, Russa, Inglese e Cinese;
- i messaggi di posta elettronica devono poter essere conservati in modo agevole sul server di posta elettronica stesso;
- l'accesso al server di posta elettronica, per la consultazione dei messaggi in arrivo e per l'invio dei messaggi in uscita, deve avvenire in modo sicuro, sia all'interno, sia all'esterno della rete aziendale;
- la soluzione di posta elettronica adottata deve garantire un buon livello di affidabilità e di scalabilità, garantendo un fermo massimo di servizio non superiore ai 30 minuti.

La soluzione di posta elettronica adottata

Dopo un'attenta analisi di quelle che erano le esigenze aziendali, il personale IT ha deciso di adottare una soluzione di posta elettronica originale e per certi versi coraggiosa. Da pochi mesi il personale IT della Home Works S.p.A. ha provveduto a virtualizzare l'intera sala server, utilizzando le soluzioni offerte dalla società VMWare. La virtualizzazione dell'intera sala server ha consentito al personale IT della Home Works di ridurre il carico energetico dell'intera sala server, aumentare il livello di servizio di ciascun server e di agevolare grandemente la realizzazione di nuove *postazioni server*, riducendo i tempi di passaggio dalla fase di test, o pilota, a quella di produzione.

La soluzione di posta elettronica proposta dal personale IT alla dirigenza, prevede l'utilizzo di solamente software Open Source, questo per ridurre da un lato i costi delle varie licenze e dall'altro per poter meglio controllare l'intera infrastruttura su cui verte la soluzione di posta elettronica. Come sistema operativo il personale IT ha scelto di utilizzare Debian, sebbene non supportata ufficialmente dalla VMWare (per maggiori informazioni si veda il documento Guest Operatin System Installation Guide). La distribuzione

Debian risulta ben documentata, ha un ottima gestione dei pacchetti d'installazione, una configurazione di base eccellente e soprattutto consente l'aggiornamento dell'intera distribuzione senza dover procedere con una nuova installazione.

Come demone SMTP, il personale IT della Home Works ha deciso di utilizzare il programma Postfix. Il programma Courier verrà invece utilizzato per consentire un accesso sicuro alle varie caselle email (*mailbox*), tramite i protocolli standard di Internet, POP3-SSL ed IMAP-SSL. Il programma SquirrelMail consentirà di accedere alle caselle email via Web in modo sicuro tramite il protocollo HTTPS, mentre come sistema antivirus per controllare le email in arrivo ed in uscita, verrà utilizzato il programma ClamAV. Per il controllo dei messaggi indesiderati verrà invece utilizzato il programma DSPAM. Come client di posta elettronica, il personale IT ha deciso di adottare il programma Thunderbird che verrà opportunamente installato su tutte le postazioni client dell'azienda.

La soluzione prevede la realizzazione di un unica macchina virtuale VMWare, la quale conterrà tutti i programmi citati e servirà come postazione di partenza (*base*) per la realizzazione dell'intera soluzione di posta elettronica. Una volta valutato il corretto funzionamento del server e le sue prestazione, si provvederà eventualmente a dimensionare e scalare adeguatamente la soluzione di posta elettronica.

La macchina virtuale realizzata avrà il nome pubblico **mail.homeworks.it**, si troverà in **DMZ** ed avrà come indirizzo IP il valore **192.168.1.8** La macchina verrà collocata in **DMZ** per consentire anche al personale che opera al difuori della rete aziendale della Home Works S.p.A. di raggiungere in modo semplice le propria caselle di posta elettronica (*mailbox*). Sul firewall che presidia la **DMZ** aziendale, verranno aperte solamente le porte necessarie al funzionamento del server di posta elettronica, in particolare:

- porta **TCP 25** per il protocollo **SMTP** per l'invio e la ricezione dei messaggi di posta elettronica;
- porte **TCP 80** e **TCP 443** per i protocolli **HTTP** e **HTTPS** relativie all'accesso via *webmail* alle caselle di posta elettronica;
- porte **TCP 110** e **TCP 995** per i protocolli **POP3** e **POP3-SSL**;
- porte **TCP 143** e **TCP 993** per i protocolli IMAP e **IMAP-SSL**;

L'alta disponibilità del servizio di posta elettronica realizzato, sarà garantita dall'infrastruttura VMWare stessa. Trattandosi di una macchina virtuale, al termine della sua installazione e più in generale una volta all'anno, verrà effettuata una copia, da tenere fuori linea in caso di emergenza, dell'intera macchina virtuale realizzata.

Con i soldi risparmiati dal costo delle licenze software, il personale IT ha deciso di organizzare dei corsi di formazione sull'utilizzo della posta elettronica e dei suoi programmi, per i vari dipendenti. Non potendo realizzare un numero adeguato di lezioni per tutti i dipendenti, in accordo con la direzione, il personale IT ha deciso di organizzare una serie di corsi di tre giorni per tutti i dipendenti che hanno un portatile aziendale e per tutti coloro che hanno necessità di conoscere bene l'utilizzo della posta elettronica e dei suoi programmi, nel corso delle proprie mansioni lavorative. Al termine di ciascun corso verrà svolto un test sul grado di apprendimento dei vari studenti, coloro che supereranno un punteggio minimo avranno il diritto a seguire altri corsi aziendali, per coloro invece che non supereranno questo punteggio minimo, la partecipazioni ad altri corsi interni verrà valutata di volta in volta.

Debian Etch

In questa sezione spiegheremo, a grandi linee, come installare il sistema operativo **Debian Etch**, demandando per i dettagli realizzativi ad appositi articoli dedicati. Il personale IT della Home Works, basandosi sull'esperienza maturata con l'attuale soluzione di posta elettronica, ha stimato che ogni *mailbox* possa avere una dimensione media massima di **5GB**, pertanto, essendo circa 200 le mailbox che dovranno venire create, lo spazio disco da assegnare alle mailbox dovrà essere di almeno **1TB**.

Installazione e configurazione del sistema operativo (Debian Etch)

Come traccia per l'installazione del sistema operativo Debian, si può utilizzare il documento, in lingua Inglese, The Perfect Setup - Debian Etch (Debian 4.0) che spiega in modo dettagliato come installare una distribuzione Debian Etch. Di seguito riportiamo alcune linee guida che conviene seguire quando s'installa una distribuzione Debian:

- l'installazione andrebbe fatta utilizzando la lingua **Inglese**;
- utilizzare il file system **ext3** per formattare la partizione **/home**;
- trattandosi di un server di posta elettronica pubblico (ubicato in **DMZ**), conviene assegnare al server lo stesso nome FQDN che avrà il **record A** che identificherà il server di posta elettronica in Internet. Nel nostro caso il server verrà chiamato col nome di **mail.homeworks.it**;
- non selezionare nessuna delle configurazioni riportate all'interno della procedura d'installazione, scegliendo di fatto d'installare i vari pacchetti che comporanno il server di posta elettronica manualmente;
- selezionare l'aggiornamento dei pacchetti via **HTTP** o FTP, specificando uno dei mirror riportati all'interno della procedura d'installazione (ad esempio si può scegliere http://ftp.it.debian.org/debian/). Più in generale, si può utilizzare il comando `netselect` per risalire ad un Mirror Debian con le migliori caratteristiche di connessione;
- creare come account amministrativo del server, l'utente **master** (per motivi di sicurezza, conviene evitare di utilizzare il nome utente **admin**);
- specificare come sorgente oraria del sistema i server NTP segnalati nel sito www.pool.ntp.org;

In base alla configurazione di Postfix che adotteremo, conviene creare le seguenti partizioni col seguente file system (per la scelta su quale file system utilizzare, invitiamo i lettori a leggere il capitolo quattro del libro The Book of IMAP):

Nome Mount Point	Dimensione	File System
/boot	100MB	ext3
/	20GB almeno	ext3
/home	1000GB almeno	ext3
/var	60GB almeno	ext3
/swap	pari a 1,5 volte la RAM	

Una volta installato il sistema operativo e verificato che questi non presenta problemi, si può procedere con la personalizzazione dell'installazione riportata nei paragrafi successivi.

Come installare i VMWare Tools

Trattandosi di un'installazione del sistema operativo **Debian Etch** all'interno di un'infrastruttura VMWare ed essendo il sistema operativo **Debian Etch** non ufficialmente supportato dalla società VMWare, facciamo vedere come installare i **VMWare Tools**, ovvero quei componenti del Kernel che consentono una migliore integrazione delle macchine virtuali all'interno dell'infrastruttura virtuale VMWare stessa.

Per installare i **VMWare Tools**, basta seguire le istruzioni seguenti. Prima di tutto, installiamo, qualora non lo fossero già presenti, i seguenti programmi:

```
apt-get install aptitude install autoconf automake binutils cpp gcc linux-headers-$(uname -r)
make psmisc
```

Individuiamo dove si trovano i *kernel headers*, utilizzando il comando:

```
ls -d /usr/src/linux-headers-$(uname -r)*/include
```

Prendere nota del percorso cartella in cui si trovano i *kernel headers*, in quanto durante l'installazione dei **VMWare Tools** ci verrà chiesto d'inserire questo percorso. Di solito i *kernel headers* si trovano nella cartella `/usr/src/linux-headers-<Versione Kernel Installato>-686/include` (ad esempio, nella cartella `/usr/src/linux-headers-2.6.18-5-686/include`).

A questo punto siamo pronti per installare i **VMWare Tools**:


L'installazione va svolta direttamente dalla *console* e non tramite una connessiore remota con SSH.

- montare il cdrom virtuale che contiene i **VMWare Tools**: dalla console VMWare, aprire il menù **VM** e selezionare la voce **Install VMWare Tools**
- eseguire in sequenza i seguenti comandi:

```
mount /media/cdrom
cd /media/cdrom
tar -C /tmp -zxvf VMwareTools-<Versione VMWare Tools>.tar.gz
cd /tmp/vmware-tools-distrib
./vmware-install.pl
```

  lasciare i valori di *default* che vengono man mano proposti;
- quando richiesto, eseguire il comando:

```
vmware-config-tools.pl
```

- lasciare i valori di *default* proposti, facendo attenzione al punto in vui verrà chiesto d'inserire il percorso dei *kernel headers*;
- ad un certo punto verrà chiesto d'inserire il percorso in cui si trovano i *kernel headers*, specificare il percorso che si è ottenuto eseguendo il comando `ls -d /usr/src/linux-headers-$(uname -r)*/include`
- al termine dell'installazione eseguire i seguenti comandi:

```
/etc/init.d/networking stop
depmod -a
modprobe vmxnet
/etc/init.d/networking start
```

- riavviare la macchina virtuale digitando il comando:

```
reboot
```

  Al successvio riavvio controllare che la scheda di rete virtuale venga regolarmente caricata.

Una volta riavviata la macchina e constatato il suo regolare funzionamento, si può procedere con la sua configurazione.

Configurazione delle impostazioni di Rete

Trattandosi dell'installazione di un server di posta elettronica, è bene che la macchina abbia un indirizzo IP fisso, ovvero non rilasciato da un server DHCP. Per scelta del personale IT della Home Works S.p.A, il server di posta elettronica verrà realizzato all'interno della **DMZ** (*DeMilitarized Zone*) aziendale. La rete della DMZ aziendale ha indirizzameto IP 192.168.1.0/24. Alla macchina verrà assegnato l'indirizzo IP **192.168.1.8**, mentre il Default Gateway avrà indirizzo IP **192.168.1.254** e il nome FQDN del server di posta sarà **mail.homeworks.it**. L'indirizzo IP pubblico a cui il server di posta verrà associato sarà **217.18.211.8**. Come server DNS verranno utilizzati i DNS pubblici del ISP (*Internet Service Provider*) che ospita la zona DNS *homeworks.it*, **208.67.222.222** e **217.18.208.130**.

Per impostare la configurazione di rete che abbiamo descritto, bisogna editare il file `/etc/network/interfaces` utilizzando il comando:

Per convenzione, tutte le istruzioni che verrà chiesto di eseguire, nel corso dell'articolo, dovranno essere intese come svolte dall'utente **root**, a meno che non venga esplicitamente indicato un altro utente. Pertanto, d'ora in avanti, supporemo che le operazioni che verranno indicate vengano svolte tutte dall'utente **root**.

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

Modificare il file `/etc/network/interfaces` come segue:

```
# 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
#allow-hotplug eth0
#iface eth0 inet dhcp
auto eth0
iface eth0 inet static
          address 192.168.1.8
          netmask 255.255.255.0
          network 192.168.1.0
          broadcast 192.168.1.255
          gateway 192.168.1.254
```

Riavviare l'interfaccia di rete col seguente comando:

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

Se si dovesse verificare una segnalazione d'errore del tipo **SIOCSIFADDR: No such device eth0**, vuol dire che si sono verificati dei problemi con la gestione del *MAC Address* della scheda di rete virtuale. Per ovviare a questo problema, basta rinominare il file `/etc/udev/rules.d/z25_persistent-net.rules` col comando: `mv /etc/udev/rules.d/z25_persistent-net.rules /etc/udev/rules.d/z25_persistent-net.rules.backup` e poi riavviare il sistema.

Modificare il file `/etc/hosts` aggiungendo la riga:

```
192.168.1.8     mail.homeworks.it       mail
```

Dopo la modifica, il file */etc/hosts* dovrebbe apparire come:

```
cat /etc/hosts
```

```
127.0.0.1       localhost.localdomain   localhost
192.168.1.8     mail.homeworks.it       mail

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Modificare infine il file */etc/resolv.conf* specificando i server DNS del ISP che ospita la zona DNS *homeworks.it*, ovvero i DNS pubblici **217.18.208.130** e **208.67.222.222**. Per modificare il file */etc/resolv.conf* eseguiamo il comando:

```
vi /etc/resolv.conf
```

Aggiungiamo le seguenti righe:

```
domain homeworks.it
nameserver 208.67.222.222
nameserver 217.18.208.130
```

Salviamo le modifiche. Con queste impostazioni, la configurazione di rete del server di posta elettronica risultano concluse. Passiamo adesso a migliorare la configurazione di base della distribuzione Debian.

Configurarazione di base del sistema operativo

A seguito della configurazione di Postfix che verrà adottata, tutte le *mailbox* verranno create all'interno della partizione **/home**, pertanto, per rendere più *reattivo* il server di posta elettronica, conviene adottare la seguente modifica al file */etc/fstab*:

```
cp /etc/fstab /etc/fstab.originale
vi /etc/fstab
```

aggiungere alla riga relativa alla partizione **/home** la voce `noatime`; ovvero se ad esempio la riga relativa alla partizione **/home** dovesse apparire come segue:

```
/dev/sda3  /home  ext3  defaults  0  2
```

allora la riga dovrebbe venire modificata come segue:

```
/dev/sda3  /home  ext3  defaults,noatime  0  2
```

in questo modo si renderebbe più rapido l'accesso alla partizione **/home** (per maggiori informazioni, invitiamo i lettori a leggere l'articolo A couple of minor ext3 performance tweaks ed il capitolo quattro del libro The Book of IMAP). Effettuata la modifica, non resta che smontare e rimontare la partizione **/home**:

```
umount /home
mount /home
```

Accertarsi infine che la formattazione della partizione **/home** goda delle seguenti cartatteristiche (per

semplicità continuamo a fare riferimento all'esempio utilizzato precedentemente):

```
tune2fs -l /dev/sda3 | grep features
Filesystem features: has_journal resize_inode dir_index filetype needs_recovery sparse_super
large_file
```

in particolare deve risultare presente la voce **dir_index**.

La Debian mette a disposizione dei siti ufficiali da cui scaricare sia le ultime versione dei programmi, sia gli aggiornamenti. Per comodità, conviene utilizzare esclusivamente dei repository ufficiali Debian (Mirror Debian) per eseguire l'installazione dei vari programmi, pertanto disabiliteremo l'utilizzo del cdrom come sorgente d'installazione. Per fare ciò, modificheremo il file */etc/apt/sources.list* utilizzando i comandi:

```
cp /etc/apt/sources.list /etc/apt/sources.list.originale
vi /etc/apt/sources.list
```

Commentiamo le righe che si riferiscono ai cdrom, ovvero la riga:

```
  deb cdrom:[Debian GNU/Linux 4.0 r0 _Etch_ - Official i386 CD Binary-1 20070407-
11:55]/ etch contrib main
```

diventa:

```
  # deb cdrom:[Debian GNU/Linux 4.0 r0 _Etch_ - Official i386 CD Binary-1 20070407-
11:55]/ etch contrib main
```

aggiungiamo poi le seguenti righe (Debian Volatile):

```
  # Installation from Debian Volatile
  deb http://volatile.debian.org/debian-volatile etch/volatile main contrib non-free
```

Dopo le modifiche apportate il file /etc/apt/sources.list dovrebbe apparire come segue:

```
cat /etc/apt/sources.list
```

```
  # /etc/apt/source.list
  #
  # Installation from cdrom
  # deb cdrom:[Debian GNU/Linux 4.0 r0 _Etch_ - Official i386 CD Binary-1 20070407-
11:55]/ etch contrib main

  # Installation from Official Debian Repository
  deb http://ftp.it.debian.org/debian/ etch main
  deb-src http://ftp.it.debian.org/debian/ etch main

  # Installation from Security Debian Repository
  deb http://security.debian.org/ etch/updates main contrib
  deb-src http://security.debian.org/ etch/updates main contrib

  # Installation from Debian Volatile
  deb http://volatile.debian.org/debian-volatile etch/volatile main contrib non-free
```

Aggiorniamo la lista del software ed installiamo gli ultimi aggiornamenti disponibili:

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

Per rendere la gestione del server di posta più agevole, conviene installare solamente i programmi che sono necessari al server di posta elettronica per il suo corretto funzionamento, pertanto eseguiamo l'installazione dei seguenti programmi:

```
apt-get install ssh openssh-server
apt-get install tree
apt-get install vim vim-common vim-doc vim-runtime vim-scripts vim-tiny
apt-get install fetchmail flex libarchive-zip-perl libc6-dev libcompress-zlib-perl libdb4.3-
dev libpcre3 libpopt-dev lynx m4 ncftp nmap openssl perl perl-modules unzip zip zlib1g-dev
libtool bison autotools-dev g++
```

Se non sono già stati installati in precedenza, installare anche i seguenti programmi:

```
apt-get install aptitude autoconf automake binutils cpp gcc linux-headers-$(uname -r) make
psmisc
```

L'amministrazione remota del server di posta sarà realizzata tramite connessioni SSH. Le impostazioni predefinite della Debian non impongono nessuna scadenza alle connessioni SSH, col risultato che una connessione SSH può rimanere attiva anche per diversi giorni o mesi. Per scongiurare queste situazioni, disdicevoli su di un server ad accesso pubblico, conviene impostare la variabile d'ambiente che impone un *Timeout* alle connessioni SSH inattive. Per poter attivare questa variabile d'ambiente, bisogna modifica il file */etc/profile*. Pertanto:

```
cp /etc/profile /etc/profile.originale
vi /etc/profile
```

aggiungiamo le seguenti righe per farsì che una connessione SSH non possa rimanere inattiva per più di dieci minuti:

```
# Enable timeout connection from shell console (seconds)
TMOUT=600
```

impostiamo l'editor `vim` come l'editor di default delle applicazioni:

```
# Default Editor vim
EDITOR=/usr/bin/vim
```

impostiamo il programma `less` per visualizzare i caratteri accentati:

```
# Enable foreign characters in "less"
LESSCHARSET=latin1
```

salviamo le modifiche effettuate al file /etc/profile. Dopo le modifiche apportate, il file */etc/profile* dovrebbe apparire come segue:

```
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).

if [ "`id -u`" -eq 0 ]; then
   PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
else
   PATH="/usr/local/bin:/usr/bin:/bin:/usr/games"
fi

# Default Editor vim
EDITOR=/usr/bin/vim

# Enable foreign characters in "less"
LESSCHARSET=latin1
```

```
# Enable timeout connection from shell console (minutes)
TMOUT=600

if [ "$PS1" ]; then
   if [ "$BASH" ]; then
      PS1='\u@\h:\w\$ '
   else
      if [ "`id -u`" -eq 0 ]; then
         PS1='#  '
      else
         PS1='$  '
      fi
   fi
fi

export PATH EDITOR LESSCHARSET
umask 022
```

Per comodità, decidiamo di attivare sia la *syntax highlighting* del editor `vim`, sia la modalità di ricerca avanzata dell'editor. Pertanto modifichiamo il file */etc/vim/vimrc* eseguendo i comandi:

```
cp /etc/vim/vimrc /etc/vim/vimrc.originale
vi /etc/vim/vimrc
```

Togliamo il segno di commento dalle seguenti righe:

```
...
" Vim5 and later versions support syntax highlighting. Uncommenting the next
" line enables syntax highlighting by default.
syntax on

" If using a dark background within the editing area and syntax highlighting
" turn on this option as well
set background=dark
...
set incsearch           " Incremental search
...
```

Salviamo le modifiche introdotte al file /etc/vim/vimrc. In questo modo l'utilizzo dell'editor `vim` sarà più semplice.

Miglioriamo la leggibilità dei messaggi di avvio introducendo le seguenti modifiche al file */boot/grub/menu.lst*:

```
vi /boot/grub/menu.lst
```

Modifichiamo le seguenti righe:

```
...
# Pretty colours
color cyan/blue white/blue
...
# defoptions
...
```

come segue (**788** se lo schermo ha risoluzione **800x600**, **791** se lo schermo ha risoluzione **1024x768**):

```
...
# Pretty colours
#color cyan/blue white/blue
```

```
color yellow/black light-green/black
...
# defoptions=vga=788
...
```

Salviamo le modifiche effettuate al file /boot/grub/menu.lst ed eseguiamo il comando:

```
update-grub
```

controllare che non compaino messaggi di errore. Introduciamo poi alcune personalizzazioni ed alcuni *alias* che hanno il compito di rendere più confortevole l'ambiente di lavoro. Pertanto modifichiamo il file /root/.bashrc con i seguenti comandi:

```
cp /root/.bashrc /root/.bashrc.originale
vi /root/.bashrc
```

Modifichiamo od aggiungiamo le seguenti righe:

```
...
# You may uncomment the following lines if you want `ls' to be colorized:
export LS_OPTIONS='--color=auto'
eval "`dircolors`"
alias ls='ls $LS_OPTIONS'
alias ll='ls $LS_OPTIONS -l'
alias l='ls $LS_OPTIONS -lA'

# Some more alias to avoid making mistakes:
alias rm='rm -iv'
alias cp='cp -iv'
alias mv='mv -iv'

# Some personal alias to live better
alias dir='ls -l'
alias ll='ls -l'
alias la='ls -la'
alias l='ls -alF'
alias ls-l='ls -l'
alias l.='ls -d .*'
alias ll.='ls -dl .*'
alias ,='cd -'
alias ..='cd ..'
alias ...='cd ../..'
alias rd=rmdir
alias md='mkdir -p'
alias which='type -p'
alias nslookup='nslookup -sil'
alias lping='ping -c 5 $1'
alias h=history

# Functions

# Manage resource
cdin()
{
      mount /media/cdrom0
      cd /media/cdrom0
      ls /media/cdrom0
}

cdout()
{
      cd ~
      umount /media/cdrom0
}
```

```
fdin()
{
	mount /media/floppy0
	cd /media/floppy0/
	ls /media/floppy0
}

fdout()
{
	cd ~
	umount /media/floppy0
}

# Change directory
cl()
{
	cd "$1" ; ls --color
}

# Manage configuration files
show()
{
	grep -v ^# "$1" | grep -v ^$
}

# Manage file tar.gz
inst()
{
	if [ $# = 1 ]; then
		tar xvzf $1
	else
		echo "Devi specificare un file .tar.gz da installare"
	fi
}

list()
{
	if [ $# = 1 ]; then
		tar tvzf $1
	else
		echo "Devi specificare un file .tar.gz da analizzare"
	fi
}
```

Salviamo le modifiche apportate al file *`/root/.bashrc`*. Eseguendo un *logout* ed un *login* come utente **root** e le modifiche introdotte risulteranno subito operative, in alternativa si può eseguire il comando:

```
source /root/.bashrc
```

Se si desidera rendere queste personalizzazioni valide per tutti gli utenti del server di posta, bisogna copiare il file *`/root/.bashrc`* nella cartella *`/etc/skel`*:

```
cp /root/.bashrc /etc/skel/.bashrc
```

Per semplicità, in questo articolo, ci riferiremo solamente all'utilizzo della lingua Italiana, sebbene, quanto affermeremo, può venire tranquillamente esteso anche alle altre lingue, in particolare al Tedesco, al Russo ed al Cinese tradizionale.

Per gestire il supporto della lingua Italiana e per evitare problemi di compatibilità col programma Putty, conviene modificare il file *`/etc/environment`* come segue:

```
cp /etc/environment /etc/environment.originale
rm /etc/environment
```

```
ln -s /etc/default/locale /etc/environment
dpkg-reconfigure locales
```

Aggiungiamo le seguenti selezioni oltre a quelle già presenti:

- Selezionare l'impostazione: **en_US ISO-8859-1**
- Selezionare l'impostazione: **it_IT ISO-8859-1**
- Selezionare l'impostazione: **it_IT.UTF-8 UTF-8**

Premiamo **OK** ed impostiamo come lingua predefinita per i pacchetti Debian la voce: **en_US**

Editare il file `/etc/environment` ed accertarsi che sia impostato come segue:

```
cat /etc/environment
```

```
LANG=en_US
```

In caso contrario procedere come indicato di seguito:

```
vi /etc/environment
```

modificare la riga:

```
LANG="en_US.UTF-8"
```

nel seguente modo:

```
LANG="en_US"
```

Salvare le modifiche e riavviare la macchina. In questo modo si potranno vedere in modo corretto i caratteri speciali all'interno di Putty (**Putty** è uno dei programmi più noti per accedere via SSH ad una postazione Linux in ambiente Windows).

Configurazione di Mutt per leggere le email firmate digitalmente

Conviene avere a disposizione, sul server di posta elettronica, un programma con cui leggere i vari messaggi email che il server di posta elettronica ospiterà. Un client di posta elettronica semplice ed allo stesso molto potente è Mutt. Poichè i messaggi email possono venire firmati digitalmente, sia dal personale della Home Works S.p.A, sia da altre persone, configuriamo il programma Mutt affinchè possa leggere le email firmate digitalmente. Per consentire a **Mutt** di leggere le email firmate digitalmente si deve procedere come segue (supporemo, nel corso della spiegazione seguente, di collegarci al server di posta elettronica con l'utente **master**):

```
su -
smime_keys init
md /etc/skel/.smime
ln -sf /etc/ssl/certs/ca-certificates.crt /etc/skel/.smime/ca-bundle.crt
exit
md /home/master/.smime
ln -sf /etc/ssl/certs/ca-certificates.crt ~/.smime/ca-bundle.crt
```

Grazie a questa modifica, il programma **Mutt** sarà in grado di leggere le firme digitali delle email che risultano essere firmate digitalmente.

Configurazione dell'accesso remoto via SSH al server

Come accennato in precedenza, l'amministrazione remota del server di posta elettronica sarà affidata al protcollo SSH. L'implementazione *Open Source* del protocollo SSH è affidata alle librerie OpenSSH. Per rendere l'accesso col protocollo SSH più sicuro, apportiamo, al file di configurazione delle librerie OpenSSH, */etc/ssh/sshd_config*, le seguenti modifiche:

```
cp /etc/ssh/sshd_config /etc/ssh/sshd_config.originale
vi /etc/ssh/sshd_config
```

Forziamo la porta di ascolto e la versione del protocollo SSH che dovranno venire utilizzati da `OpenSSH`:

```
Port 22
Protocol 2
```

Configuriamo il tempo di chiusura della connessione per gli utenti che non si sono autenticati (in secondi):

```
LoginGraceTime 20
```

Per evitare che gli utenti possano utilizzare l'interfaccia grafica, inseriamo le seguenti righe:

```
X11Forwarding no
X11DisplayOffset 10
```

Imponiamo che l'utente `root` non possa collegarsi tramite il protcollo SSH, questo forzerà l'autenticazione con un utente definito (nel corso dell'articolo, questo utente, sarà l'utente **master**):

```
PermitRootLogin no
```

Inseriamo infine un *messaggio di benvenuto* (*banner*) di modo da avvertire chi si collega al server di posta elettronica, che l'accesso al server è limitato alle sole persone autorizzate:

```
Banner /etc/issue.net
```

Salviamo le modifiche apportate al file */etc/ssh/sshd_config* Dopo le modifiche adottate, il file /etc/ssh/sshd_config dovrebbe apparire come segue:

```
# Package generated configuration file
# See the sshd(8) manpage for details

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

# Use these options to restrict which interfaces/protocols sshd will bind to
#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

#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

# Authentication:
LoginGraceTime 120
PermitRootLogin no
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 no
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
Banner /etc/issue.net

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

Subsystem sftp /usr/lib/openssh/sftp-server
UsePAM yes
```

Modifichiamo il contenuto del file */etc/issue.net*:

```
cp /etc/issue.net /etc/issue.net.originale
vi /etc/issue.net
```

aggiungendo le seguenti righe:

```
Welcome to mail.homeworks.it (Debian GNU/Linux 4.0)

* * * * * * * * * * * * * W A R N I N G * * * * * * * * * * * * *

THIS SYSTEM IS RESTRICTED TO AUTHORIZED USERS FOR AUTHORIZED USE
ONLY. UNAUTHORIZED ACCESS IS STRICTLY PROHIBITED AND MAY BE
PUNISHABLE UNDER THE COMPUTER FRAUD AND ABUSE ACT OF 1986 OR
OTHER APPLICABLE LAWS. IF NOT AUTHORIZED TO ACCESS THIS SYSTEM,
DISCONNECT NOW. BY CONTINUING, YOU CONSENT TO YOUR KEYSTROKES
AND DATA CONTENT BEING MONITORED. ALL PERSONS ARE HEREBY
NOTIFIED THAT THE USE OF THIS SYSTEM CONSTITUTES CONSENT TO
MONITORING AND AUDITING.

* * * * * * * * * * * * * W A R N I N G * * * * * * * * * * * * *
```

Una volta applicati i cambiamenti riavviamo il demone **ssh** eseguendo il comando:

```
/etc/init.d/ssh restart
```

Ora siamo pronti per collegarci, da remoto, in modo sicuro al server di posta elettronica.

Come non perdere una sessione SSH (Screen)

Dal momento che la maggior parte delle volte, l'amministrazione del server di posta elettronica verrà svolta da remoto, ovvero operando tramite una connessione **SSH**, diventa particolarmente critico evitare di perdere il controllo di una sessione SSH aperta. Per evitare di perdere la possibilità di ricollegarsi ad una sessione SSH precedentemente aperta, si deve ricorrere all'utilizzo di un opportuno comando, `screen` Pertanto una volta aperta la sessione SSH, per evitare di perderla, dovremo digitare il seguente comando:

```
screen
```

Le scorciatoie che il comando `screen` mette a disposizione sono:

- `[Ctrl]+a c`

  crea una nuova sessione SSH
- `[Ctrl]+a p`

  passa alla sessione SSH precedente, se si usano più sessioni
- `[Ctrl]+a n`

  passa alla sessione SSH successiva, se si usano più sessioni
- `[Ctrl]+a d`

  sconnette la sessione SSH corrette senza abortirla
- `screen -ls`

  elenca le sessioni esistenti sulla macchina
- `screen -r <Nome_Sessione>`

connette la sessione indicata nel campo <Nome_Sessione>

- `exit`

esce e chiude una sessione

Sincronizzazione dell'ora del mail server con una sorgente oraria

Per un server di posta elettronica, l'ora è molto importante, pertanto conviene impostare una sorgente oraria esterna (ad esempio in Internet) con cui sincronizzare l'ora di sistema in modo periodico. Per assolvere a questo compito, bisogna installare i componenti necessari:

```
apt-get install ntp ntpdate
```

Verificare che l'ora venga effettivamente presa da Internet. Lanciare il comando:

```
ntpq -np
```

Il risultato del comando dovrebbe essere simile a:

```
  remote           refid                st      t       when    poll    reach   delay
offset  jitter
  ==============================================================================
==================
  +192.135.48.21   192.43.244.18        2       u       288     512     377
179.769 -11.714 17.050
  +64.235.47.142   128.118.25.3         3       u       301     512     377
204.318 24.340  43.251
  64.182.117.175   192.12.19.20         2       u       263     512     373
364.621 78.281  579.788
  *192.87.36.4     .GPS.                1       u       335     512     377
61.028  -35.975 20.019
```

Se uno dei server elencati inzia col simbolo * allora vuol dire che l'ora viene presa da Internet, quindi la configurazione del NTP Client è corretta. Per controllare l'ora del sistema operativo, basta eseguire il comando:

```
date
```

Postfix

Postfix è uno dei più diffusi programmi per la gestione e la ricezione dei messaggi di posta elettronica. Testato da anni di sviluppo, è forse uno dei migliori programmi nel suo genere. La configurazione che adotteremo di Postfix prevede che le *Mailbox* siano associate direttamente agli utenti di sistema e che si possa poi modificare l'indirizzo email associato all'utente, utilizzando degli *alias*. Gli account utente che verranno creati non avranno però accesso al sistema, per ovvi motivi di sicurezza. Per scelta degli autori, non verrà adottata alcuna gestione delle quote disco sulle *Mailbox*. Il dominio di posta elettronica che provvederemo ad attivare sarà quello associato alla Home Works S.p.A, ovvero *homeworks.it*

Installazione e configurazione di Postfix

Per installare Postfix basta eseguire il seguente comando:

```
apt-get install postfix postfix-pcre libsasl2 sasl2-bin libsasl2-modules libdb3-util procmail
```

Configuriamo una prima volta Postfix:

```
General type of configuration? <-- Internet Site
Mail name? <-- mail.homeworks.it
```

Riconfiguriamo Postfix:

```
dpkg-reconfigure postfix
```

Rispondiamo alle domande proposte:

```
General type of configuration? <-- Internet Site
Where should mail for root go <-- master
Mail name? <-- mail.homeworks.it
Other destinations to accept mail for? (blank for none) <-- mail.homeworks.it,
localhost.homeworks.it, localhost.localdomain, localhost
Force synchronous updates on mail queue? <-- No
Local networks? <-- 127.0.0.0/8
Use procmail for local delivery? <-- Yes
Mailbox size limit <-- 0
Local address extension character? <-- +
Internet protocols to use? <-- all
```

Postfix ha due file di configurazione:

- `/etc/postfix/main.cf` che contiene le variabili per definire il comportamento generale di Postfix;
- `/etc/postfix/master.cf` che contiene la configurazione dei vari demoni che compongono l'*architettura* del programma Postfix.

Per il momento ci concentreremo solamente sul file `/etc/postfix/main.cf`, rimandando ad altri paragrafi la configurazione del file `/etc/postfix/master.cf`

Configuriamo Postfix impostando l'autenticazione SMTP-AUTH tramite il programma Cyrus-SASL (si osservi che il meccanismo di autenticazione di SMTP-AUTH fornito dal programma Cyrus-SASL non consente di utilizzare password con caratteri speciali come ad esempio i simboli: $, & ...).

```
postconf -e 'smtpd_sasl_local_domain ='
postconf -e 'smtpd_sasl_auth_enable = yes'
postconf -e 'smtpd_sasl_security_options = noanonymous'
postconf -e 'smtpd_sasl_tls_security_options = noanonymous'
postconf -e 'broken_sasl_auth_clients = yes'
postconf -e 'smtpd_recipient_restrictions =
permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
echo 'pwcheck_method: saslauthd' >> /etc/postfix/sasl/smtpd.conf
echo 'mech_list: plain login' >> /etc/postfix/sasl/smtpd.conf
```

Personalizziamo la configurazione di Postfix introducendo le seguenti modifiche:

Nella configurazione che segue, fissiamo la dimensione massima dei messaggi email, tenendo conto anche della dimensione degli allegati, a **7MB**, a seguito di quanto riportato nell'istruzione **message_size_limit**. Impostiamo inoltre il formato delle caselle di posta elettronica (*mailbox*) in modalità **Maildir** (per maggiori informazioni sulla modalità di archiviazione dei messaggi di posta elettronica denominata **Maildir**, invitiamo il lettore a leggere il capitolo ottavo del libro The Book of IMAP).

```
postconf -e 'anvil_rate_time_unit = 60s'
postconf -e 'smtpd_client_connection_rate_limit = 40'
postconf -e 'smtpd_client_connection_count_limit = 16'
postconf -e 'smtpd_client_message_rate_limit = 100'
postconf -e 'smtpd_client_recipient_rate_limit = 32'
postconf -e 'smtpd_client_event_limit_exceptions = $mynetworks'
postconf -e 'address_verify_sender = abuse@homeworks.it'
postconf -e 'address_verify_map = btree:/var/spool/postfix/verified_senders_cache'
```

```
postconf -e 'smtpd_helo_required = yes'
postconf -e 'smtpd_timeout = 60'
postconf -e 'smtpd_recipient_limit = 100'
postconf -e 'maximal_queue_lifetime = 1h'
postconf -e 'delay_warning_time = 30m'
postconf -e 'message_size_limit = 10240000'
postconf -e 'home_mailbox = Maildir/'
```

Il contenuto del file /etc/postfix/main.cf dopo le modifiche che abbiamo eseguito dovrebbe apparire come segue:

```
cat /etc/postfix/main.cf
```

```
  ...
  # SASL parameters
  smtpd_sasl_local_domain =
  smtpd_sasl_auth_enable = yes
  smtpd_sasl_security_options = noanonymous
  smtpd_sasl_tls_security_options = noanonymous
  broken_sasl_auth_clients = yes
  ...
  # Sender verification
  address_verify_sender = abuse@homeworks.it
  address_verify_map = btree:/var/spool/postfix/verified_senders_cache
  smtpd_helo_required = yes
  ...
  # Rate limit connecntions
  anvil_rate_time_unit = 60s
  smtpd_client_connection_rate_limit = 40
  smtpd_client_connection_count_limit = 16
  smtpd_client_message_rate_limit = 100
  smtpd_client_recipient_rate_limit = 32
  smtpd_client_event_limit_exceptions = $mynetworks
  smtpd_timeout = 60
  smtpd_recipient_limit = 100
  maximal_queue_lifetime = 1h
  delay_warning_time = 30m
  ...
  # Mailbox formats
  home_mailbox = Maildir/
  ...
  # SMTP restrictions (Localhost Only)
  smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated,
reject_unauth_destination
```

Controlliamo la sintassi del file di configurazione di Postfix, `/etc/postfix/main.cf` e riavviamo il demone di Postfix:

```
postfix check
/etc/init.d/postfix restart
```

Controlliamo che il demone di Postfix sia in ascolto sulla porta 25:

```
netstat -tln | grep 25
```

```
  tcp        0      0 127.0.0.1:10025         0.0.0.0:*               LISTEN
  tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
  tcp6       0      0 :::25080                :::*                    LISTEN
  tcp6       0      0 :::25                   :::*                    LISTEN
```

Avendo la Home Works S.p.A. provveduto a realizzare un propria infrastruttura PKI interna, sfruttiamo questa infrastruttura per generare i certificati digitali con cui criptare le comunicazioni col demone di Postfix. Seguendo le indicazioni riportate nell'articolo Creazione di un'infrastruttura PKI con OpenSSL

provvediamo a generare i certificati digitali da assegnare a Postfix:

- `/etc/postfix/certs/postfix_private_key.pem` è la *chiave privata* di Postfix.
- `/etc/postfix/ssl/postfix_public_cert.pem` è il *certificato digitale* di Postfix.
- `/etc/postfix/ssl/global_ca_public_cert.pem` rappresenta il *certificato globale* della **HomeWorks Root CA** e **HomeWorks Issuing CA**;

Nella configurazione che adotteremo, imporremo a Postfix di considerare *attendibile* solamente la HomeWorks Issuing CA, ovvero, di ritenere validi solamente i certificati generati dalla HomeWorks Issuing CA. Pertanto le modifiche da apportare al file di configurazione di Postfix, `/etc/postfix/main.cf`, sono, lato SMTP server (ovvero quando Postfix si comporta come un server SMTP):

```
postconf -e smtpd_tls_CAfile = /etc/postfix/certs/global_ca_public_cert.pem
postconf -e smtpd_tls_cert_file = /etc/postfix/certs/postfix_public_cert.pem
postconf -e smtpd_tls_key_file = /etc/postfix/certs/postfix_private_key.pem
postconf -e smtpd_use_tls = yes
postconf -e smtpd_tls_session_cache_timeout = 3600s
postconf -e smtpd_tls_auth_only = no
postconf -e smtpd_tls_loglevel = 1
postconf -e smtpd_tls_received_header = yes
postconf -e tls_random_source = dev:/dev/urandom
```

mentre lato SMTP client (ovvero quanto Postfix si comporta come un SMTP client) imporremo a Postfix di considerare attendibili sia i certificati digitali generati da CA pubbliche (l'elenco delle CA pubbliche da considerare attendibili si trova all'interno del file `/etc/ssl/certs/ca-certificates.crt`), sia i certificati digitali generati dalla HomeWorks Issuing CA. Concateniamo quindi il *certificato globale*, `/etc/postfix/ssl/global_ca_public_cert.pem` col file che contiene i certificati digitali delle CA pubbliche riconosciute dalla Debian, `/etc/ssl/certs/ca-certificates.crt`:

```
cp /etc/postfix/certs/global_ca_public_cert.pem /etc/ssl/certs/
cat /etc/ssl/certs/ca-certificates.crt /etc/ssl/certs/global_ca_public_cert.pem >
/etc/ssl/certs/ca-certificates.crt.tmp
mv /etc/ssl/certs/ca-certificates.crt.tmp /etc/ssl/certs/ca-certificates.crt
ln -s /etc/ssl/certs/ca-certificates.crt /etc/postfix/certs/ca-certificates.crt
```

dopo di che procediamo con la configurazione di Postfix:

```
postconf -e smtp_use_tls = yes
postconf -e smtp_tls_note_starttls_offer = yes
postconf -e smtp_tls_CAfile = /etc/postfix/certs/ca-certificates.crt
postconf -e smtp_tls_session_cache_timeout = 3600s
postconf -e smtp_tls_loglevel = 1
```

La configurazione relativa al protocollo Transport Layer Security (TLS) del file `/etc/postfix/main.cf` dovrebbe apparire come:

```
cat /etc/postfix/main.cf
```

```
...
# TLS parameters (Server Side, from this SMTP Server to Mail Client)
smtpd_tls_CAfile = /etc/postfix/certs/global_ca_public_cert.pem
smtpd_tls_cert_file = /etc/postfix/certs/postfix_public_cert.pem
smtpd_tls_key_file = /etc/postfix/certs/postfix_private_key.pem
smtpd_use_tls = yes
smtpd_tls_session_cache_database = btree:${queue_directory}/smtpd_scache
smtpd_tls_auth_only = no
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
```

```
# information on enabling SSL in the smtp client.

# TLS parameters (Client Side, from this SMTP Server to another SMTP Server)
smtp_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtp_tls_CAfile = /etc/postfix/certs/ca-certificates.crt
smtp_tls_session_cache_database = btree:${queue_directory}/smtp_scache
smtp_tls_session_cache_timeout = 3600s
smtp_tls_loglevel = 1
...
```

Poichè nel processo di autenticazione TLS fra due server SMTP si possono verificare dei problemi, conviene creare un apposito file che inibisca l'utilizzo del protocollo TLS verso certi server SMTP. Creiamo a tale scopo il file */etc/postfix/deny_tls_per_domains*:

```
vi /etc/postfix/deny_tls_per_domains
```

inseriamo, ad esempio, il seguente testo:

```
# File /etc/postfix/deny_tls_per_domains
#
# Insert the DNS domain should to be denied to use client-side TLS
#
# Example: mybusinessdomain.com       None
#
# DNS domain name                     Action (None)
#
gmail.com                             None
#  End File
```

Creiamo la mappa di Postfix del file */etc/postfix/deny_tls_per_domains*:

```
postmap hash:/etc/postfix/deny_tls_per_domains
```

Aggiungiamo la seguente riga al file di configurazione di Postfix, */etc/postfix/main.cf*:

```
postconf -e smtp_tls_per_site = hash:/etc/postfix/deny_tls_per_domains
```

Se si desidera verificare che non ci siano errori nella configurazione TLS di Postfix, si può decidere di aumentare momentaneamente il livello di logging a **2**, ovvero:

```
postconf -e 'smtpd_tls_loglevel = 2'
```

Verifichiamo se la configurazione di Postfix risulta corretta, simulando una connessione TLS:

```
openssl s_client -starttls smtp -CAfile /etc/postfix/certs/global_ca_public_cert.pem -connect
localhost:25

CONNECTED(00000003)
depth=2 /C=IT/ST=Italy/O=Home Works S.p.A./OU=HomeWorks IT Department/CN=HomeWorks Root
CA/emailAddress=support@homeworks.it
verify return:1
depth=1 /C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=HomeWorks Issuing CA/emailAddress=support@homeworks.it
verify return:1
depth=0 /C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=mail.homeworks.it/emailAddress=postmaster@homeworks.it
verify return:1
---
Certificate chain
0 s:/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=mail.homeworks.it/emailAddress=postmaster@homeworks.it
i:/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT Department/CN=HomeWorks
```

```
Issuing CA/emailAddress=support@homeworks.it
1 s:/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=HomeWorks Issuing CA/emailAddress=support@homeworks.it
i:/C=IT/ST=Italy/O=Home Works S.p.A./OU=HomeWorks IT Department/CN=HomeWorks Root
CA/emailAddress=support@homeworks.it
2 s:/C=IT/ST=Italy/O=Home Works S.p.A./OU=HomeWorks IT Department/CN=HomeWorks Root
CA/emailAddress=support@homeworks.it
i:/C=IT/ST=Italy/O=Home Works S.p.A./OU=HomeWorks IT Department/CN=HomeWorks Root
CA/emailAddress=support@homeworks.it
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIErzCCBBigAwIBAgIJANgUMb8Nfv2RMA0GCSqGSIb3DQEBBQUAMIG3MQswCQYD
VQQGEwJJVDEOMAwGA1UECBMFSXRhbHkxFjAUBgNVBAcTDVJlZ2dpbyBFbWlsaWEx
GjAYBgNVBAoTEUhvbWUgV29ya3MgUy5wLkEuMSAwHgYDVQQLExdIb21lV29ya3Mg
SVQgRGVwYXJ0bWVudDEdMBsGA1UEAxMUSG9tZVdvcmtzIElzc3VpbmcgQ0ExIzAh
BgkqhkiG9w0BCQEWFHN1cHBvcnRAaG9tZXdvcmtzLml0MB4XDTA4MDMyOTAyMDgy
M1oXDTEyMDMyODAyMDgyM1owgbcxCzAJBgNVBAYTAklUMQ4wDAYDVQQIEwVJdGFs
eTEWMBQGA1UEBxMNUmVnZ2lvIEVtaWxpYTEaMBgGA1UEChMRSG9tZSBXb3JrcyBT
LnAuQS4xIDAeBgNVBAsTF0hvbWVXb3JrcyBJVCBEZXBhcnRtZW50MRowGAYDVQQD
ExFtYWlsLmhvbWV3b3Jrcy5pdDEmMCQGCSqGSIb3DQEJARYXcG9zdG1hc3RlckBo
b21ld29ya3MuaXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALGJI5ZBWk5V
/14bTChuPh8f3R91UW1bEUJze7IxWIXaSqmS9W2CnPXZ03MQmp0uMA/p/BnzaqZk
KoVowPid99+S3l0EmYLv0tbZ2ckVtHbbi9wP3ZXRHZUfZoa7ALhDoBrWH5TjyN6Q
nZ07tiqlE8PHCY55lbMRkbZW378fQ7z1AgMBAAGjggG/MIIBuzAJBgNVHRMEAjAA
MBEGCWCGSAGG+EIBAQQEAwIGwDALBgNVHQ8EBAMCBPAwHQYDVR0lBBYwFAYIKwYB
BQUHAwEGCCsGAQUFBwMCMB0GA1UdDgQWBBRBtnfg2nht4wSKlMDF6uYzT12U6TCB
0QYDVR0jBIHJMIHGgBSsR7OnfSaM+wdWc7ZiHQ/raI6T16GBoqSBnzCBnDELMAkG
A1UEBhMCSVQxDjAMBgNVBAgTBUl0YWx5MRowGAYDVQQKExFIb21lIFdvcmtzIFMu
cC5BLjEgMB4GA1UECxMXSG9tZVdvcmtzIElUIERlcGFydG1lbnQxGjAYBgNVBAMT
EUhvbWVXb3JrcyBSb290IENBMSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGhvbWV3
b3Jrcy5pdIIJANgUMb8Nfv2KMD8GCCsGAQUFBwEBBDMwMTAvBggrBgEFBQcwAoYj
aHR0cDovL3d3dy5ob21ld29ya3MuaXQvY2FpbmZvLmh0bWwwOwYDVR0fBDQwMjAw
oC6gLIYqaHR0cDovL3d3dy5ob21ld29ya3MuaXQvY3JsL2lzc3VpbmdfY2EuY3Js
MA0GCSqGSIb3DQEBBQUAA4GBAEm7cTPDfILe6tbHIwDMH+tY8s3KM2wFxdE10iAu
mXINBE6t5AshDdghHw/vjmWGPnt2Wh6mcGlckdrtXhwtal6q2Wgbf/1Z7PDfGBA3
KOt1t+vxSL00Nm4FeO+MwRu7W4mbKqW0UaZzzDhOp80b1exSP5E/fZS1rD5Cx2PB
L7tG
-----END CERTIFICATE-----
subject=/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=mail.homeworks.it/emailAddress=postmaster@homeworks.it
issuer=/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=HomeWorks Issuing CA/emailAddress=support@homeworks.it
---
No client certificate CA names sent
---
SSL handshake has read 3899 bytes and written 326 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1
    Cipher : DHE-RSA-AES256-SHA
    Session-ID: 101D8C076F036B0AE5A8F9483BBB6009382228B280D648EC0F9853E24CE02EB8
    Session-ID-ctx:
    Master-
Key:CC5AACC3AC41023245CA2FAC724E08445A021CA53D5CCEAAC071FA936C723DF623CEDB72421AAC22CDC3D71FE
8E6CC58
    Key-Arg : None
    Start Time: 1207172342
    Timeout : 300 (sec)
    Verify return code: 0 (ok)
---
220 mail.homeworks.it ESMTP Postfix (Debian/GNU)
```

Chiudiamo la connessione di test aperta dal comando `openssl s_client -starttls smtp -CAfile /etc/postfix/certs/root_ca_private_key.pem -connect localhost:25`:

```
quit

221 2.0.0 Bye
```

```
read:errno=0
```

Se nel risultato della connessione TLS simulata compare il messaggio `Verify return code: 0 (ok)`, allora vuol dire che la configurazione di Postfix è corretta. A questo punto si possono configurare i client di posta elettronica di modo che possano collegarsi via TLS a Postfix, ovvero al server SMTP.

Postfix consente di eseguire alcuni controlli sui messaggi di posta elettronica in arrivo per poter meglio identificare i messaggi di *SPAM*. Affichè però questi controlli non compromettano il corretto funzionamento di Postfix, ovvero per evitare che alcuni messaggi in arrivo non vengano erroneamente persi, conviene creare alcuni file di controllo:

- `/etc/postfix/allow_special_role_accounts` per consentire di ricevere sempre messaggi indirizzati agli indirizzi email previsti dalla RFC2821.
- `/etc/postfix/deny_helo_parameters` per evitare che venga utilizzato come hostname nel comando HELO quello del server di posta elettronica.
- `/etc/postfix/allow_sender_domains` per consentire di ricevere comunque le email provenienti da certi mittenti.
- `/etc/postfix/check_sender_spam_domains` per controllare i mittenti di certi domini sospettati di inviare messaggi di SPAM.

Procediamo alla creazione dei file indicati di sopra:

```
touch /etc/postfix/allow_special_role_accounts
touch /etc/postfix/deny_helo_parameters
touch /etc/postfix/allow_sender_domains
touch /etc/postfix/check_sender_spam_domains
```

Il file `/etc/postfix/allow_special_role_accounts` va modificato come segue:

```
vi /etc/postfix/allow_special_role_accounts
```

inserire il testo:

```
# File /etc/postfix/allow_special_role_accounts
#
# RFC2821 Mail Address where you should always recive e-mail message
#
# Mailbox Name          Permission
postmaster@             OK
abuse@                  OK
webmaster@              OK
hostmaster@             OK
#  End File
```

Il file `/etc/postfix/deny_helo_parameters` va modificato come segue:

```
vi /etc/postfix/deny_helo_parameters
```

inserire il testo:

```
# File /etc/postfix/deny_helo_parameters
#
# Parameters not allowed to use in helo information
#
/^mail\.homeworks\.it$/         550 Don't use my public FQDN and my hostname
#  End File
```

Il file `/etc/postfix/allow_sender_domains` va modificato come segue:

```
vi /etc/postfix/allow_sender_domains
```

inserire, ad esempio, il testo:

```
# File /etc/postfix/allow_sender_domains
#
# Insert the DNS domain should allowed to send email from this server
#
# Example: mybusinessdomain.com        OK
#
# DNS domain name       Permission (OK)
#
homeworks.it            OK
#  End File
```

Fare molta attenzione ai domini di posta elettronica che si vogliono inserire in questa lista, in quanto su di essi non verrà fatto nessun controllo sullo SPAM.

Il file */etc/postfix/check_sender_spam_domains* va modificato come segue:

```
vi /etc/postfix/check_sender_spam_domains
```

inserire il testo (l'elenco di domini riportato, corrisponde, in base all'esperienza degli autori, ai principali domini da cui arriva la maggior parte dello SPAM):

```
# File /etc/postfix/check_sender_spam_domains
#
# SPAM domains to check the sender
#
# Example: spam.com     reject_unverified_sender
#
# SPAM DNS domain name          Action
#
sicurezza.it                    reject_unverified_sender
escortcorp.com                  reject_unverified_sender
yahoo.com                       reject_unverified_sender
faxsav.com                      reject_unverified_sender
hotmail.com                     reject_unverified_sender
compuserve.com                  reject_unverified_sender
#  End File
```

Una volta creati questi file procedere a creare le corrispondenti mappe di Postfix:

```
postmap hash:/etc/postfix/allow_special_role_accounts
postmap hash:/etc/postfix/allow_sender_domains
postmap hash:/etc/postfix/check_sender_spam_domains
```

Modifichiamo il file di configurazione di Postifx, */etc/postfix/main.cf* come segue:

```
vi /etc/postfix/main.cf
```

La riga:

```
  smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated,
reject_unauth_destination
```

diventa:

```
  # smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated,
```

```
reject_unauth_destination
```

Introduciamo le seguenti modifiche:

```
  # SMTP restrictions for business use (visit web site http://moensted.dk/spam/ for
SPAM checkers list)
  smtpd_recipient_restrictions =  reject_non_fqdn_recipient,
                                  reject_non_fqdn_sender,
                                  reject_unknown_sender_domain,
                                  reject_unknown_recipient_domain,
                                  reject_unauth_pipelining,
                                  permit_mynetworks,
                                  permit_sasl_authenticated,
                                  reject_unauth_destination,
                                  reject_multi_recipient_bounce,
                                  check_recipient_access
hash:/etc/postfix/allow_special_role_accounts
                                  reject_non_fqdn_hostname,
                                  reject_invalid_hostname,
                                  check_helo_access
pcre:/etc/postfix/deny_helo_parameters,
                                  check_sender_access
hash:/etc/postfix/allow_sender_domains,
                                  reject_rbl_client zen.spamhaus.org,
                                  reject_rbl_client black.uribl.com,
                                  reject_rbl_client grey.uribl.com,
                                  reject_rbl_client list.dsbl.org,
                                  reject_rbl_client rabl.nuclearelephant.com,
                                  reject_rbl_client dnsbl.sorbs.net,
                                  reject_unknown_client,
                                  reject_rhsbl_sender dsn.rfc-ignorant.org,
                                  check_sender_access
hash:/etc/postfix/check_sender_spam_domains,
                                  permit
```

Salviamo le modifiche. Verifichiamo eventuali errori e riavviamo postfix:

```
postfix check
/etc/init.d/postfix restart
```

Nel corso dell'ultima configurazione, abbiamo fatto uso della **DNSBLs** (*DNS Black Lists*) ZEN della Spamhaus, ovvero l'URL **zen.spamhaus.org**, è bene sapere che l'utilizzo del progetto ZEN è vincolato da quanto riportato nel documento Spamhaus DNSBL Usage.

Configuriamo il modulo **saslauthd** per l'autenticazione:

```
mkdir -p /var/spool/postfix/var/run/saslauthd
```

Editiamo il file */etc/default/saslauthd*:

```
vi /etc/default/saslauthd
```

Modifichiamo le variabili:

```
  START=yes
  OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd -r"
```

Ovvero il file /etc/default/saslauthd dovrebbe apparire come:

```
  #
```

```
# Settings for saslauthd daemon
#

# Should saslauthd run automatically on startup? (default: no)
START=yes

# Which authentication mechanisms should saslauthd use? (default: pam)
#
# Available options in this Debian package:
# getpwent  -- use the getpwent() library function
# kerberos5 -- use Kerberos 5
# pam       -- use PAM
# rimap     -- use a remote IMAP server
# shadow    -- use the local shadow password file
# sasldb    -- use the local sasldb database file
# ldap      -- use LDAP (configuration is in /etc/saslauthd.conf)
#
# Only one option may be used at a time. See the saslauthd man page
# for more information.
#
# Example: MECHANISMS="pam"
MECHANISMS="pam"

# Additional options for this mechanism. (default: none)
# See the saslauthd man page for information about mech-specific options.
MECH_OPTIONS=""

# How many saslauthd processes should we run? (default: 5)
# A value of 0 will fork a new process for each connection.
THREADS=5

# Other options (default: -c)
# See the saslauthd man page for information about these options.
#
# Example for postfix users: "-c -m /var/spool/postfix/var/run/saslauthd"
# Note: See /usr/share/doc/sasl2-bin/README.Debian
OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd -r"
```

Riavviamo il modulo **saslauthd**:

```
/etc/init.d/saslauthd start
```

Controlliamo che tutto funzioni:

```
telnet localhost 25
ehlo localhost
```

Risposta del demone Postfix:

```
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
220 mail.homeworks.it ESMTP Postfix (Debian/GNU)
ehlo localhost
250-mail.homeworks.it
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

Usiciamo dal collegamento via telnet con postfix:

```
quit
```

Se compaiono le sigle `250-AUTH PLAIN LOGIN` e `250-AUTH=PLAIN LOGIN` vuol dire che l'integrazione del modulo **saslauthd** con Postfix, è andata a buon fine, pertanto Postfix provvederà ad inviare solamente i messaggi di posta elettronica delle persone che sono *regolarmente autorizzate*. In altri termini, per poter inviare dei messaggi di posta elettronica col server **mail.homeworks.it** bisogna *prima autorevolmente registrarsi* sul server di posta elettronica **mail.homeworks.it** stesso.

Verifichiamo il corretto funzionamento della procedura di autenticazione SMTP-AUTH: per far ciò codifichiamo in **Base64** la password dell'utente da utilizzare come test. Ad esempio se si utilizza l'utente **master** con password *master* dobbiamo eseguire il comando seguente per codificare la password *master* in **Base64**:

```
perl -MMIME::Base64 -e 'print encode_base64("master\0master\0master");'
```

il risultato del comando è: **bWFzdGVyAG1hc3RlcgBtYXN0ZXI=**

Più in generale si può utilizzare il comando:

```
perl -MMIME::Base64 -e 'print encode_base64("<UserName>\0<UserName>\0<Password>");'
```

Eseguire una connessione telnet al demone di Postfix (porta 25) da una qualunque postazione (nel nostro esempio supporemo che questa postazione si chiami *sophie.homeworks.it*):

```
telnet 192.168.1.8 25
ehlo sophie.homeworks.it
auth plain bWFzdGVyAG1hc3RlcgBtYXN0ZXI=
```

Se compare un messaggio del tipo:

```
235 2.0.0 Authentication successful
```

vuol dire che la procedura di autenticazione è andata a buon fine.

In alternativa al metodo appena illustrato, si può utilizzare il comando:

```
testsaslauthd -s smtp -u master -p master -f /var/spool/postfix/var/run/saslauthd/mux
```

o più in generale:

```
testsaslauthd -s smtp -u <username> -p <Password> -f /var/spool/postfix/var/run/saslauthd/mux
```

In conformità con la RFC2821 è bene che esistano i seguenti alias all'interno del file `/etc/aliases`:

```
cat /etc/aliases
```

```
...
postmaster: root
abuse: root
root: master
...
```

Se questi *alias* non esistono, si deve editare il file `/etc/aliases`:

```
vi /etc/aliases
```

inserire le seguenti righe di testo:

```
postmaster: root
abuse: root
root: master
```

salvare le modifiche effettuate al file `/etc/aliases` ed eseguire i comandi:

```
postalias hash:/etc/aliases
newaliases
postfix reload
```

L'installazione e configurazione di Postfix è pertanto conclusa.

Manutenzione di Postfix

In questo paragrafo riporteremo alcuni dei comandi principali per poter amministrare Postfix. In particolare:

- Per vedere i valori di default di Postfix si deve usare il comando:

```
postfix -d
```

- Per conoscere la versione di Postfix basta digitare il comando:

```
postconf -d | grep mail_version
```

- Per vedere le porte in cui sono in ascolto i vari demoni:

```
netstat -tap
```

- Per vedere le mappe supportate da Postfix basta digitare il comando:

```
postconf -m
```

- Per vedere dove Postfix deposita le email in ingresso basta digitare il comando:

```
postconf mail_spool_directory
```

Come aggiungere o modificare un indirizzo di posta elettronica

Nella semplice installazione che abbiamo fatto, a ciascun utente di sistema, presente nel file `/etc/passwd`, resta associata una *Mailbox* (*casella di posta elettronica*). Pertanto, all'utente **master**, creato durante l'installazione della Debian, resterà associata la casella email **master@homeworks.it**. In generale, avremo che a ciascun *NomeUtente*, corrisponderà una Mailbox denominata *NomeUtente@homeworks.it*. Se si desidera assegnare ad un utente una Mailbox con un nome diverso, si deve provvedere a creare un *alias* della Mailbox *di default*. Supponiamo ad esempio che abbiamo creato l'utente **atani** associato alla persona di **Alessandro Tani**. In base alla nostra configurazione di Postfix avremo che ad **Alessandro Tani** corrisponderà l'indirizzo email **atani@homeworks.it**. Se volessimo associare ad Alessandro Tani, la casella email **alessandro_tani@homeworks.it** dovremo creare un opportuno *alias* della casella email **atani@homeworks.it** nel file `/etc/aliases`, ovvero inserire la seguente riga:

```
alessandro_tani: atani
```

In generale il file */etc/aliases* ha la seguente struttura:

```
Nome Mailbox: Nome Utente
```

Pertanto per aggiungere un nuovo *alias* ad una data Mailbox, basta editare il file */etc/aliases* ed aggiungere una nuova associazione *Nome Mailbox: Nome Utente*. L'unico vincolo di questa procedura è che il *Nome Utente* deve corrispondere ad un utente *reale* (di sistema) della macchina, ovvero *potenzialmente* in grado di effettuare la procedura di login sul nostro mail server. Per evitare che questi *utenti* possano *realmente* effettuare un login al mail server, basta creare questi utenti di sistema col seguente comando:

```
useradd -c "Nome Cognome" -d /home/<username> -s /usr/sbin/nologin -m <username>
passwd <username>
```

Una volta creato l'utente si può procedere ad assegnargli un eventuale *alias* della sua Mailbox seguendo lo schema *Nome Mailbox: Nome Utente*. Una volta modificato il file */etc/aliases* bisogna eseguire i comandi:

```
postalias hash:/etc/aliases
newaliases
postfix reload
```

per poter rendere disponibile a Postfix la versione aggiornata del file */etc/aliases*. In questo modo le modifiche apportate al file */etc/aliases* risulteranno operative. Un esempio di file */etc/aliases* potrebbe essere:

```
# /etc/aliases
# Mailbox Name: Username
mailer-daemon: postmaster
postmaster: root
nobody: root
hostmaster: root
usenet: root
news: root
webmaster: root
www: root
ftp: root
abuse: root
noc: root
security: root
support: root
root: master
```

Per verificare se gli utenti creati possano accedere correttamente alla loro Mailbox, si può utilizzare il comando:

```
testsaslauthd -s smtp -u <Username> -p <Password> -f /var/spool/postfix/var/run/saslauthd/mux
```

Se il processo di autenticazione va a buon fine vuol dire che la Mailbox è stata creata con successo.

Per motivi di sicurezza, a tutti gli utenti di sistema a cui resta associata una Mailbox, è impedito l'accesso al server di posta elettronica, ovvero come *shell dei comandi* è stata impostata la shell */usr/sbin/nologin*

Come cancellare un indirizzo di posta elettronica

Per cancellare una Mailbox, bisogna cancellare l'utente di sistema a cui la Mailbox è associata. Ad esempio, se si vuole cancellare la casella di posta elettronica **atani@homeworks.it**, bisogna cancellare l'utente di sistema **atani**. Pertanto, la procedura da seguire per eliminare una Mailbox è la seguente:

- per prima cosa bisogna cancellare eventuali *alias* associati all'utente da cancellare. Per far ciò basta editare il file `/etc/aliases` e provvedere a cancellare tutte le riccorrenze che fanno riferimento al nome utente da cancellare. Ricordarsi che una volta modificato il file `/etc/aliases` bisogna eseguire i comandi:

```
postalias hash:/etc/aliases
newaliases
postfix reload
```

- una volta eliminati gli alias si può procedere a cancellare l'utente di sistema e la sua cartella `/home/<username>/Maildir` utilizzando il comando:

```
userdel -r <Username>
```

A questo punto Postfix non inoltrerà più email all'utente.

Courier

Come programma per accedere alle Mailbox (ovvero come *Mail Transport Agent*) i responsabili IT della Home Works S.p.A. hanno deciso di utilizzare il programma Courier, in quanto è ben supportato, la documentazione è di ottimo livello, la sua configurazione è relativamente semplice ed è un pacchetto ufficiale Debian.

Installazione e configurazione di Courier

L'installazione di Courier è molto semplice, per prima cosa installiamo i componeneti necessari:

```
apt-get install courier-authdaemon courier-base courier-imap courier-imap-ssl courier-pop
courier-pop-ssl courier-ssl gamin libgamin0 libglib2.0-0
```

alle domande che verranno poste durante l'installazione bisogna rispondere come indicato di seguito:

```
Create directories for web-based administration ? <-- No
SSL certificate required <-- Ok
```

I responsabili IT della Home Works, per consentire al personale che opera sulle postazioni portatili d'invivare i messaggi di posta elettronica direttamente dal loro client di posta elettronica (Thunderbird) anche quando la porta 25 (SMTP) è chiusa, ad esempio quando si trovano ad operare presso la sede di qualche cliente della HomeWorks S.p.A, hanno deciso di abilitare la possibilità d'inviare i messaggi di posta elettronica sfruttanto il protocollo IMAP, pertanto modifichiamo i file di configurazione di Courier come segue:

```
cp /etc/courier/imapd /etc/courier/imapd.originale
cp /etc/courier/pop3d /etc/courier/pop3d.originale
vi /etc/courier/imapd
```

assegnamo alla variabile `MAXPERIP` il valore `40` al posto del valore `20` e abilitiamo la possibilità d'inviare dei messaggi di posta elettronica tramite il protocollo IMAP, ovvero aggiungiamo le variabili:

```
  OUTBOX=.Outbox
  OUTBOX_MULTIPLE_SEND=1
```

dopo le modifiche effettuate, il file */etc/courier/imapd* dovrebbe apparire come (il comando `show` è un *alias* definito all'interno della sezione Configurarazione di base del sistema operativo):

```
show /etc/courier/imapd
```

```
  ADDRESS=0
  PORT=143
  MAXDAEMONS=40
  MAXPERIP=40
  PIDFILE=/var/run/courier/imapd.pid
  TCPDOPTS="-nodnslookup -noidentlookup"
  LOGGEROPTS="-name=imapd"
  IMAP_CAPABILITY="IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT
THREAD=REFERENCES SORT QUOTA IDLE"
  IMAP_KEYWORDS=1
  IMAP_ACL=1
  IMAP_CAPABILITY_ORIG="IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT
THREAD=REFERENCES SORT QUOTA AUTH=CRAM-MD5 AUTH=CRAM-SHA1 AUTH=CRAM-SHA256 IDLE"
  IMAP_PROXY=0
  IMAP_PROXY_FOREIGN=0
  IMAP_IDLE_TIMEOUT=60
  IMAP_CAPABILITY_TLS="$IMAP_CAPABILITY AUTH=PLAIN"
  IMAP_CAPABILITY_TLS_ORIG="$IMAP_CAPABILITY_ORIG AUTH=PLAIN"
  IMAP_DISABLETHREADSORT=0
  IMAP_CHECK_ALL_FOLDERS=0
  IMAP_OBSOLETE_CLIENT=0
  IMAP_UMASK=022
  IMAP_ULIMITD=65536
  IMAP_USELOCKS=1
  IMAP_SHAREDINDEXFILE=/etc/courier/shared/index
  IMAP_ENHANCEDIDLE=0
  IMAP_TRASHFOLDERNAME=Trash
  IMAP_EMPTYTRASH=Trash:7
  IMAP_MOVE_EXPUNGE_TO_TRASH=0
  OUTBOX=.Outbox
  SENDMAIL=/usr/sbin/sendmail
  HEADERFROM=X-IMAP-Sender
  OUTBOX_MULTIPLE_SEND=1
  IMAPDSTART=YES
  MAILDIRPATH=Maildir
```

Per inviare un messaggio di posta elettronica tramite il protocollo IMAP, sarà sufficiente copiare il messaggio da inviare all'interno della cartella **Outbox** (si osservi che i messaggi di posta elettronica inviati tramite la cartella **Outbox**, non verranno copiati, in seguito al meccanismo d'invio dei messaggi stessi, nella cartella **Sent**).

Analogamente, modifichiamo il file di configurazione del protocollo POP3 di Courier, */etc/courier/pop3d*:

```
vi /etc/courier/pop3d
```

assegnamo alla variabile `MAXPERIP` il valore `20` al posto del valore `4`. Dopo le modifiche il file */etc/courier/pop3d* dovrebbe apparire come (il comando `show` è un *alias* definito all'interno della sezione Configurarazione di base del sistema operativo) segue:

```
show /etc/courier/pop3d
```

```
  PIDFILE=/var/run/courier/pop3d.pid
```

```
MAXDAEMONS=40
MAXPERIP=20
POP3AUTH=""
POP3AUTH_ORIG="PLAIN LOGIN CRAM-MD5 CRAM-SHA1 CRAM-SHA256"
POP3AUTH_TLS=""
POP3AUTH_TLS_ORIG="LOGIN PLAIN"
POP3_PROXY=0
PORT=110
ADDRESS=0
TCPDOPTS="-nodnslookup -noidentlookup"
LOGGEROPTS="-name=pop3d"
POP3DSTART=YES
MAILDIRPATH=Maildir
```

Per adottare dei meccanismi di accesso sicuro (via TLS) alle Mailbox, sfruttiamo l'infrastruttura PKI della Home Works S.p.A per generare i certificati digitali da assegnare a Courier, pertanto procediamo come indicato nell'articolo Creazione di un'infrastruttura PKI con OpenSSL. Una volta ottenuti i certificati:

- */etc/courier/imapd.pem* per la connessione IMAP-SSL;
- */etc/courier/pop3d.pem* per la connessione POP3-SSL;

riavviamo i demoni di Courier relativi ai protocolli IMAP-SSL e POP3-SSL:

```
/etc/init.d/courier-imap-ssl restart
/etc/init.d/courier-pop-ssl restart
```

Verifichiamo che il collegamento tramite i protocolli IMAP-SSL ed POP3-SSL venga eseguito correttamente. Per controllare il protocollo POP3-SSL digitiamo:

```
openssl s_client -CAfile /etc/postfix/certs/global_ca_public_cert.pem -connect
mail.homeworks.it:995

CONNECTED(00000003)
depth=2 /C=IT/ST=Italy/O=Home Works S.p.A./OU=HomeWorks IT Department/CN=HomeWorks Root
CA/emailAddress=support@homeworks.it
verify return:1
depth=1 /C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=HomeWorks Issuing CA/emailAddress=support@homeworks.it
verify return:1
depth=0 /C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=mail.homeworks.it/emailAddress=postmaster@homeworks.it
verify return:1
---
Certificate chain
0 s:/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=mail.homeworks.it/emailAddress=postmaster@homeworks.it
i:/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT Department/CN=HomeWorks
Issuing CA/emailAddress=support@homeworks.it
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIF1DCCBLygAwIBAgIJAITSw4sZn+qIMA0GCSqGSIb3DQEBBQUAMIG3MQswCQYD
VQQGEwJJVDEOMAwGA1UECBMFSXRhbHkxFjAUBgNVBAcTDVJlZ2dpbyBFbWlsaWEx
GjAYBgNVBAoTEUhvbWUgV29ya3MgUy5wLkEuMSAwHgYDVQQLExdIb21lV29ya3Mg
SVQgRGVwYXJ0bWVudDEdMBsGA1UEAxMUSG9tZVdvcmtzIElzc3VpbmcgQ0ExIzAh
BgkqhkiG9w0BCQEWFHN1cHBvcnRAaG9tZXdvcmtzLml0MB4XDTA4MDUwMzE0MjEw
N1oXDTEyMDUwMjE0MjEwN1owgbcxCzAJBgNVBAYTAklUMQ4wDAYDVQQIEwVJdGFs
eTEWMBQGA1UEBxMNUmVnZ2lvIEVtaWxpYTEaMBgGA1UEChMRSG9tZSBXb3JrcyBT
LnAuQS4xIDAeBgNVBAsTF0hvbWVXb3JrcyBJVCBEZXBhcnRtZW50MRowGAYDVQQD
ExFtYWlsLmhvbWV3b3Jrcy5pdDEmMCQGCSqGSIb3DQEJARYXcG9zdG1hc3RlckBo
b21ld29ya3MuaXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALWZkmHfE0TF
pTdhUJsvbXFaty9CCUaVjHdSR/NPAGJslxC6pamh2FfBNchVjelrxR5TiRpKneUI
Ncl2qSuqXjdXt+N5LtJ8RYi9pamwTyvZU02GW8qd/JhMla/ff7ZadrhRf2lrs7QI
7///6Xdl/v9IB4eYlOlQrvV6MJ03jY99AgMBAAGjggJjMIICXzAJBgNVHRMEAjAA
MBEGCWCGSAGG+EIBAQQEAwIGwDALBgNVHQ8EBAMCBPAwHQYDVR0lBBYwFAYIKwYB
BQUHAwEGCCsGAQUFBwMCMB0GA1UdDgQWBBQRPiCzc32TqWZfPQDtfVGbEQCeODCB
0QYDVR0jBIHJMIHGgBSLG4DX0xig6QVQHP36Q2GQ/3+tRaGBoqSBnzCBnDELMAkG
A1UEBhMCSVQxDjAMBgNVBAgTBUl0YWx5MRowGAYDVQQKExFIb21lIFdvcmtzIFMu
```

```
cC5BLjEgMB4GA1UECxMXSG9tZVdvcmtzIElUIERlcGFydG1lbnQxGjAYBgNVBAMT
EUhvbWVXb3JrcyBSb290IENBMSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGhvbWV3
b3Jrcy5pdIIJAIp0ryKAjVmbMD8GCCsGAQUFBwEBBDMwMTAvBggrBgEFBQcwAoYj
aHR0cDovL3d3dy5ob21ld29ya3MuaXQvY2FpbmZvLmh0bWwwOwYDVR0fBDQwMjAw
oC6gLIYqaHR0cDovL3d3dy5ob21ld29ya3MuaXQvY3JsL2lzc3VpbmdfY2EuY3Js
MIGhBgNVHSAEgZkwgZYwgZMGDCsGAQQBgc9Sg30BATCBgjA7BggrBgEFBQcCARYv
aHR0cDovL3d3dy5ob21ld29ya3MuaXQvY2EvaXNzdWluZ19jYV9jcHMuaHRtbDsw
QwYIKwYBBQUHAgIwNxo1SG9tZVdvcmtzIElzc3VpbmcgQ0EgQ2VydGlmaWNhdGlv
biBQcmFjdGljZSBTdGF0ZW1lbnQwDQYJKoZIhvcNAQEFBQADggEBAH/h8+uQp+KX
0JvurS+4iIyJhMS60X4Hz/snbuTEnZJmbVRNM+OaZdV1G9enGLJ8iwhghyjVmJ0I
JrYlWmcxd5SYYGmrAiGSSSvbpVg7M+g1I/AEa4gJraiOoiybBfWz5p18eIfveBNt
G+OA7WOGlYeFDd6G+INTbtIRXsqCe3L63D/bl4oV5rgKKYOC+jnZW8TTCwLgOJ2p
buYql+5nmqwdtw49weoXaLui0gQYxVFkg8Dq2KmDZkDB3guXbD9J4f3y8bZc1AHS
laTE7L80s9Ba/Vxv/u02eXXCh2MpfDyCoQdNLOrQi+lYSiFIRaYJPM3qIBHeBYHy
+NoEpjlSaqs=
-----END CERTIFICATE-----
subject=/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=mail.homeworks.it/emailAddress=postmaster@homeworks.it
issuer=/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=HomeWorks Issuing CA/emailAddress=support@homeworks.it
---
No client certificate CA names sent
---
SSL handshake has read 1658 bytes and written 316 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
  Protocol : TLSv1
  Cipher : AES256-SHA
  Session-ID: ACE31A085ACDFADB6505B6C1CCB0B5754CF812D908A875F6BE1B403838E7BAA6
  Session-ID-ctx:
  Master-Key:
AD7FDC44B7F107F42807100F6BD64D7B9D73CF837CE614DD66E50FD79465B0B08110137894564BD5B390D2AB06491
9F5
  Key-Arg : None
  Start Time: 1209826648
  Timeout : 300 (sec)
  Verify return code: 0 (ok)
---
+OK Hello there.
```

Se compare la sigla `Verify return code: 0 (ok)` vuol dire che il collegamento è andato a buon fine. Interrompiamo la connessione di prova:

```
quit
+OK Better luck next time.
closed
```

Per controllare l'accesso tramite il protocollo IMAP-SSL invece digitiamo:

```
openssl s_client -CAfile /etc/postfix/certs/global_ca_public_cert.pem -connect
mail.homeworks.it:993

CONNECTED(00000003)
depth=2 /C=IT/ST=Italy/O=Home Works S.p.A./OU=HomeWorks IT Department/CN=HomeWorks Root
CA/emailAddress=support@homeworks.it
verify return:1
depth=1 /C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=HomeWorks Issuing CA/emailAddress=support@homeworks.it
verify return:1
depth=0 /C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=mail.homeworks.it/emailAddress=postmaster@homeworks.it
verify return:1
---
Certificate chain
0 s:/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=mail.homeworks.it/emailAddress=postmaster@homeworks.it
i:/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT Department/CN=HomeWorks
Issuing CA/emailAddress=support@homeworks.it
---
```

```
Server certificate
-----BEGIN CERTIFICATE-----
MIIF1DCCBLygAwIBAgIJAITSw4sZn+qIMA0GCSqGSIb3DQEBBQUAMIG3MQswCQYD
VQQGEwJJVDEOMAwGA1UECBMFSXRhbHkxFjAUBgNVBAcTDVJlZ2dpbyBFbWlsaWEx
GjAYBgNVBAoTEUhvbWUgV29ya3MgUy5wLkEuMSAwHgYDVQQLExdIb21lV29ya3Mg
SVQgRGVwYXJ0bWVudDEdMBsGA1UEAxMUSG9tZVdvcmtzIEl2c3VpbmcgQ0ExIzAh
BgkqhkiG9w0BCQEWFHN1cHBvcnRAaG9tZXdvcmtzLml0MB4XDTA4MDUwMzE0MjEw
N1oXDTEyMDUwMjE0MjEwN1owgbcxCzAJBgNVBAYTAklUMQ4wDAYDVQQIEwVJdGFs
eTEWMBQGA1UEBxMNUmVnZ2lvIEVtaWxpYTEaMBgGA1UEChMRSG9tZSBXb3JrcyBT
LnAuQS4xIDAeBgNVBAsTF0hvbWVXb3JrcyBJVCBEZXBhcnRtZW50MRowGAYDVQQD
ExFtYWlsLmhvbWV3b3Jrcy5pdDEmMCQGCSqGSIb3DQEJARYXcG9zdG1hc3RlckBo
b21ld29ya3MuaXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALWZkmHfE0TF
pTdhUJsvbXFaty9CCUaVjHdSR/NPAGJslxC6pamh2FfBNchVjelrxR5TiRpKneUI
Ncl2qSuqXjdXt+N5LtJ8RYi9pamwTyvZU02GW8qd/JhMla/ff7ZadrhRf2lrs7QI
7///6Xdl/v9IB4eYlOlQrvV6MJ03jY99AgMBAAGjggJjMIICXzAJBgNVHRMEAjAA
MBEGCWCGSAGG+EIBAQQEAwIGwDALBgNVHQ8EBAMCBPAwHQYDVR0lBBYwFAYIKwYB
BQUHAwEGCCsGAQUFBwMCMB0GA1UdDgQWBBQRPiCzc32TqWZfPQDtfVGbEQCeODCB
0QYDVR0jBIHJMIHGgBSLG4DX0xig6QVQHP36Q2GQ/3+tRaGBoqSBnzCBnDELMAkG
A1UEBhMCSVQxDjAMBgNVBAgTBUl0YWx5MRowGAYDVQQKExFIb21lIFdvcmtzIFMu
cC5BLjEgMB4GA1UECxMXSG9tZVdvcmtzIElUIERlcGFydG1lbnQxGjAYBgNVBAMT
EUhvbWVXb3JrcyBSb290IENBMSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGhvbWV3
b3Jrcy5pdIIJAIp0ryKAjVmbMD8GCCsGAQUFBwEBBDMwMTAvBggrBgEFBQcwAoYj
aHR0cDovL3d3dy5ob21ld29ya3MuaXQvY2FpbmZvLmh0bWwwOwYDVR0fBDQwMjAw
oC6gLIYqaHR0cDovL3d3dy5ob21ld29ya3MuaXQvY3JsL2lzc3VpbmdfY2EuY3Js
MIGhBgNVHSAEgZkwgZYwgZMGDCsGAQQBgc9Sg30BATCBgjA7BggrBgEFBQcCARYv
aHR0cDovL3d3dy5ob21ld29ya3MuaXQvY2EvaXNzdWluZ19jYV9jcHMuaHRtbDsw
QwYIKwYBBQUHAgIwNxo1SG9tZVdvcmtzIElzc3VpbmcgQ0EgQ2VydGlmaWNhdGlv
biBQcmFjdGljZSBTdGF0ZW1lbnQwDQYJKoZIhvcNAQEFBQADggEBAH/h8+uQp+KX
0JvurS+4iIyJhMS60X4Hz/snbuTEnZJmbVRNM+OaZdV1G9enGLJ8iwhghyjVmJ0I
JrYlWmcxd5SYYGmrAiGSSSvbpVg7M+g1I/AEa4gJraiOoiybBfWz5p18eIfveBNt
G+OA7WOGlYeFDd6G+INTbtIRXsqCe3L63D/bl4oV5rgKKYOC+jnZW8TTCwLgOJ2p
buYql+5nmqwdtw49weoXaLui0gQYxVFkg8Dq2KmDZkDB3guXbD9J4f3y8bZc1AHS
laTE7L80s9Ba/Vxv/u02eXXCh2MpfDyCoQdNLOrQi+lYSiFIRaYJPM3qIBHeBYHy
+NoEpjlSaqs=
-----END CERTIFICATE-----
subject=/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=mail.homeworks.it/emailAddress=postmaster@homeworks.it
issuer=/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=HomeWorks Issuing CA/emailAddress=support@homeworks.it
---
No client certificate CA names sent
---
SSL handshake has read 1658 bytes and written 316 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
  Protocol : TLSv1
  Cipher : AES256-SHA
  Session-ID: ACE31A085ACDFADB6505B6C1CCB0B5754CF812D908A875F6BE1B403838E7BAA6
  Session-ID-ctx:
  Master-Key:
AD7FDC44B7F107F42807100F6BD64D7B9D73CF837CE614DD66E50FD79465B0B08110137894564BD5B390D2AB06491
9F5
  Key-Arg : None
  Start Time: 1209826648
  Timeout : 300 (sec)
  Verify return code: 0 (ok)
---
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES
SORT QUOTA IDLE AUTH=PLAIN ACL ACL2=UNION XCOURIEROUTBOX=INBOX.Outbox] Courier-IMAP ready.
Copyright 1998-2005 Double Precision, Inc. See COPYING for distribution information.
```

Se compare la sigla `Verify return code: 0 (ok)` vuol dire che il collegamento è andato a buon fine. Interrompiamo la connessione:

```
1 logout
* BYE Courier-IMAP server shutting down
1 OK LOGOUT completed
closed
```

A questo punto possiamo collegarci al server che ospita il programma Courier (ovvero,

mail.homeworks.it) utilizzando i protocolli IMAP-SSL ed POP3-SSL.

Sebbene non verranno utilizzate, per il momento, le Courier Shared Folder, conviene lo stesso creare il file vuoto `/etc/courier/shared/index` (per maggiori informazioni sulle **Courier Shared Folder**, invitiamo i lettori a leggere il capitolo dieci del libro The Book of IMAP):

```
md /etc/courier/shared
touch /etc/courier/shared/index
```

Una volta creato il file `/etc/courier/shared/index`, provvedere a riavviare i demoni **imapd-ssl** e **pop3d-ssl**:

```
/etc/init.d/courier-pop-ssl restart
/etc/init.d/courier-imap-ssl restart
```

Per migliorare la gestione degli utenti, creiamo la cartella `Maildir`, le varie cartelle utilizzate da Thunderbird e la cartella `Maildir/.SPAM` per tutti gli utenti, in questo modo non saranno necessarie ulteriori operazioni oltre a quella di creare l'utente di sistema a cui associare una data *Mailbox*:

```
maildirmake /etc/skel/Maildir
maildirmake /etc/skel/Maildir/.Drafts
maildirmake /etc/skel/Maildir/.Outbox
maildirmake /etc/skel/Maildir/.Sent
maildirmake /etc/skel/Maildir/.SPAM
maildirmake /etc/skel/Maildir/.Templates
maildirmake /etc/skel/Maildir/.Trash
```

Abilitiamo infine la capacità di Courier di avvisare, in tempo reale, i client di posta elettronica dell'arrivo di un nuovo messaggio email (questa operazione corrisponde al comando IDLE del protocollo IMAP). Modifichiamo quindi il file `/etc/courier/imapd`:

```
vi /etc/courier/imapd
```

assegnamo alla variabile `IMAP_ENHANCEDIDLE` il valore `1` al posto del valore `0`. Una volta salvate le modifiche, il file `/etc/courier/imapd` dovrebbe apparire come segue (il comando `show` è un *alias* definito all'interno della sezione Configurarazione di base del sistema operativo):

```
show /etc/courier/imapd
```

```
  ADDRESS=0
  PORT=143
  MAXDAEMONS=40
  MAXPERIP=40
  PIDFILE=/var/run/courier/imapd.pid
  TCPDOPTS="-nodnslookup -noidentlookup"
  LOGGEROPTS="-name=imapd"
  IMAP_CAPABILITY="IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT
THREAD=REFERENCES SORT QUOTA IDLE"
  IMAP_KEYWORDS=1
  IMAP_ACL=1
  IMAP_CAPABILITY_ORIG="IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT
THREAD=REFERENCES SORT QUOTA AUTH=CRAM-MD5 AUTH=CRAM-SHA1 AUTH=CRAM-SHA256 IDLE"
  IMAP_PROXY=0
  IMAP_PROXY_FOREIGN=0
  IMAP_IDLE_TIMEOUT=60
  IMAP_CAPABILITY_TLS="$IMAP_CAPABILITY AUTH=PLAIN"
  IMAP_CAPABILITY_TLS_ORIG="$IMAP_CAPABILITY_ORIG AUTH=PLAIN"
  IMAP_DISABLETHREADSORT=0
  IMAP_CHECK_ALL_FOLDERS=0
  IMAP_OBSOLETE_CLIENT=0
  IMAP_UMASK=022
  IMAP_ULIMITD=65536
  IMAP_USELOCKS=1
```

```
IMAP_SHAREDINDEXFILE=/etc/courier/shared/index
IMAP_ENHANCEDIDLE=1
IMAP_TRASHFOLDERNAME=Trash
IMAP_EMPTYTRASH=Trash:7
IMAP_MOVE_EXPUNGE_TO_TRASH=0
OUTBOX=.Outbox
SENDMAIL=/usr/sbin/sendmail
HEADERFROM=X-IMAP-Sender
OUTBOX_MULTIPLE_SEND=1
IMAPDSTART=YES
MAILDIRPATH=Maildir
```

Verifichiamo che il demone **gam_server** sia in esecuzione:

```
ps ax | grep gam
1444 ? S< 0:00 [kgameportd]
3183 ? S 0:00 /usr/lib/gamin/gam_server
3185 ? S 0:00 /usr/lib/gamin/gam_server
3191 ? S 0:00 /usr/lib/gamin/gam_server
3248 pts/0 R+ 0:00 grep gam
```

Riavviamo i demoni **courier-imap** e **courier-imap-ssl**:

```
/etc/init.d/courier-imap restart
/etc/init.d/courier-imap-ssl restart
```

Ci accertiamo che non si siano verificati degli errori:

```
tail -n 30 /var/log/mail.err
tail -n 30 /var/log/mail.log
```

Creazione di un messaggio di benvenuto

Per meglio venire incontro alle esigenze del personale della Home Works, i responsabili IT della Home Works S.p.A hanno deciso d'inserire un messaggio di benvenuto in tutte le nuove *Mailbox*. Scopo di questo messaggio di benvenuto, è quello di aiutare le persone dell'azienda che ancora non hanno avuto modo di utilizzare il sistema di posta elettronica aziendale, su come iniziare ad utilizzarlo in modo profittevole.

Per creare un messaggio di benvenuto basta utilizzare un qualunque client di posta elettronica, collegarsi possibilmente come **postmaster@homeworks.it** (ma in generale va bene un qualunque utente presente sulla macchina a cui far corrispondere il messaggio email di benvenuto), scrivere il messaggio di benvenuto che si desidera creare e poi inviarlo ad una qualunque casella email presente sul server, ad esempio **postmaster@homeworks.it**. Se si suppone di aver inviato l'email all'indirizzo **postmaster@homeworks.it** i passi da seguire sono (per semplicità supponiamo che il **Message ID** del messaggio sia **1193494764.V802I5f7b0M898756.mail.homeworks.it:2,S**):

```
cp /home/master/Maildir/cur/1193494764.V802I5f7b0M898756.mail.homeworks.it:2,S
/etc/skel/Maildir/cur
```

D'ora in avanti, quando si creerà un nuovo utente per Postfix, questi avrà di default all'interno della sua Mailbox il messaggio di benvenuto creato (ovvero quello corrispondente al **Message ID**:**1193494764.V802I5f7b0M898756.mail.homeworks.it:2,S**). Un possibile messaggio di benvenuto protrebbe essere:

```
Ciao,

questo è un messaggo di benvenuto generato automaticamente, ti invitiamo
pertanto a non rispondere a questa email. Cogliamo l'occasione per informarti
```

che tutti i messaggi di posta elettronica che invierai o che riceverai verranno controllati dal programma antivirus ClamAV (http://www.clamav.org/).
Tutti i messaggi di posta elettronica che riceverai saranno opportunamente analizzati
dal programma DSPAM (http://dspam.nuclearelephant.com/) allo scopo di ridurre i messaggi di SPAM.
Tutte le email considerate SPAM, ti verranno inviate con l'oggetto modificato con la sigla **[SPAM]**.

Per accedere alla posta aziendale puoi utilizzare uno dei seguenti servizi:

IMAP Non Sicuro

IMAP Server: *mail.homeworks.it*
Porta IMAP Server: *143*
Autenticazione Non Criptata: *Supportata*
Autenticazione Criptata (TLS): *Supportata, previa installazione dei certificati* ***root_ca_public_cert_windows_format.der*** *e* ***issuing_ca_public_cert_windows_format.der*** *reperibili sul sito* http://www.homeworks.it/ca/cainfo.html.

IMAP Sicuro (SSL)

IMAP Server: *mail.homeworks.it*
Porta IMAP Server: *993*
Per sfruttare questa modalità bisogna installare i certificati ***root_ca_public_cert_windows_format.der*** *e* ***issuing_ca_public_cert_windows_format.der*** *reperibili sul sito* http://www.homeworks.it/ca/cainfo.html.

Mentre per inviare i messaggi di posta elettronica tramite il server aziendale, puoi utilizzare
la modalità di accesso seguente:

SMTP Non Sicuro

SMTP Server: *mail.homeworks.it*
Porta SMTP Server: *25*
Autenticazione Non Criptata: *Supportata*
Autenticazione Criptata (TLS): *Supportata, previa installazione dei certificati* ***root_ca_public_cert_windows_format.der*** *e* ***issuing_ca_public_cert_windows_format.der*** *reperibili sul sito* http://www.homeworks.it/ca/cainfo.html.

Puoi accedere alla tua Mailbox anche direttamente da Internet utilizzando la webmail aziendale,
inserendo le tue credenziali di accesso all'interno del URL http://mail.homeworks.it
Il collegamento verrà automaticamente inoltrato ad un collegamento sicuro (**HTTPS**),
previa eventuale accettazione del certificato di firma digitale.
In allegato puoi trovare i certificati digitali (**root_ca_public_cert_windows_format.der**
e **issuing_ca_public_cert_windows_format.der**) per accedere al servizio di posta elettronica via Internet
direttamente, senza confermare l'accettazione del certificato digitale della webmail.

Ti invitiamo a non cancellare questo messaggio in quanto ti può tornare utile in futuro.
Per qualsiasi problema, puoi inviare un email all'indirizzo postmaster@homeworks.it

Cordialmente,

Supporto Tecnico della Home Works

In allegato andrebbe inserito un file ZIP contenente i due certificati citati: **root_ca_public_cert_windows_format.der** e **issuing_ca_public_cert_windows_format.der**. Conviene poi specificare, eventualmente, un luogo (magari l'Intranet aziendale) dove reperire le guide necessarie alla configurazione di Thunderbird.

Come configurare Thunderbird per farlo funzionare con Courier

Il client di posta elettronica Thunderbird, è il client di posta elettronica adottato dai responsabili IT della Home Works S.p.A. In questo paragrafo faremo vedere come configurare Thunderbird per farlo funzionare col programma Courier. Se si è appena installato il programma Thunderbird, si avvierà un comodo *wizard* con cui creare la prima casella email in Thunderbird, in alternativa, si può procedere come segue (la spiegazione che riportiamo si riferisce alla *versione 2.0.0.14 in lingua Inglese di Thunderbird*):

- avviare il programma Thunderbird;
- aprire il menù **Tools** e selezionare la voce **Account Settings ...**;
- premere il pulsante **Add Account ...**;
- nella sezione **New Account Setup** selezionare la voce **Email Account**. Premere il pulsante **Next** per andare avanti;
- nella sezione **Identity** inserire nel campo **Your Name** il nome e cognome del titolare della casella email, ad esempio *Alessandro Tani*. Inserire nel campo **Email Address** l'indirizzo email associato alla Mailbox che si sta configurando, ad esempio *atani@homeworks.it*. Premere il pulsante **Next** per andare avanti;
- nella sezione **Server Information**, selezionare la voce **IMAP**. Nel campo **Incoming Server** inserire il nome FQDN del server di posta elettronica, nel nostro caso *mail.homeworks.it* Premere il pulsante **Next** per andare avanti;
- nella sezione **User Names** inserire nel campo **Incoming User Name** il nome utente di sistema a cui resta associata la Mailbox che stiamo configurando, ad esempio *atani* Premere il pulsante **Next** per andare avanti;
- nella sezione **Account Name** inserire nel campo **Account Name** il nome della Mailbox, ad esempio *Alessandro Tani - HomeWorks* Premere il pulsante **Next** per andare avanti;
- nella sezione **Congratulations** controllare che i dati riportati siano corretti e poi premere il pulsante **Finish**;
- nella finestra dal titolo **Account Settings** individuare l'**Account Name** appena creato;
- andare nella sezione **Server Settings** e selezionare la voce **TLS** all'interno della sottosezione **Use Secure Connection**. Selezionare poi la voce **Check for new messagge every** ed impostare il tempo a **10 minuti**, selezionare infine la voce **Empty Trash on Exit**;
- premere il pulsante **Advanced ...**;
- nella finestra dal titolo **Advanced Account Settings** inserire nel campo **IMAP Server Directory** la voce **INBOX.**, selezionare le voci **Server Supports Folder That Contain sub-Folder and Messagges** e **User IDLE Command if the Server Supports it**. Nel campo **Personal Namespace** inserire la voce **"INBOX."**, nel campo **Public (Shared)** la voce **"shared.","#shared."** Selezionare infine la voce **Allow Server to Overrride These Namespace**. Premere **OK** per confermare le impostazioni adottate;
- nella finestra dal titolo **Account Settings** individuare la voce **Outgoing Server (SMTP)**. Premere il pulsante **Add**;
- nella finestra dal titolo **SMTP Server** inserire le seguenti voci:
    - **Description**: inserire una descrizione che identifica il server SMTP che si sta configurando, ad esempio: *HomeWorks - mail.homeworks.it*;
    - **Server Name**: inserire il nome FQDN del server SMTP, nel nostro caso: *mail.homeworks.it*
    - **Port**: lasciare il vaolore predefinitio di **25**;
    - **Username**: inserire il nome dell'utente di sistema a cui resta associata la Mailbox appena configurata, ad esempio: *atani*

selezionare infine le voce **Use Name and Password** e **TLS**. Premere **OK** per confermare;
- nella finestra dal titolo **Account Settings** individuare l'**Account Name** creato in precedenza;
- controllare nel campo **Outgoing Server SMTP** sia riportato il corretto server SMTP da utilizzare;

Prima però di portare a termine la configurazione di Thunderbird, bisogna ricordarsi d'importare i certificati digitali **root_ca_public_cert_windows_format.der** e **issuing_ca_public_cert_windows_format.der** reperibili sul sito http://www.homeworks.it/ca/cainfo.html come indicato nel paragrafo Installazione dei certificati digitali in Firefox e Thunderbird

A questo punto Thunderbird è pronto per leggere ed inviare i messaggi di posta elettronica tramite il server di posta (*mail.homeworks.it*) che abbiamo realizzato. Se si desdiera associare all'account di posta elettronica un certificato digitale tramite l'infrastruttura PKI della Home Works S.p.A, si può leggere il paragrafo Installazione dei certificati PKCS#12 in Thunderbird

Verifica di base delle prestazioni del server di posta elettronica

Adesso che abbiamo terminato l'installazione di Courier possiamo procedere con la creazione di un account di test per effettuare tutta una serie di prove sul server di posta elettronica. La presenza di questo account di test tornerà molto utile quando il server di posta elettronica sarà in produzione. Pertanto, eseguiamo i seguenti comandi:

```
useradd -c "Utente di Test" -d /home/test -s /usr/sbin/nologin -m test
passwd test
```

Si provi a mandare un email di prova all'indirizzo **test@homeworks.it** per verificare che la *Mailbox* sia attiva. Una volta certi che l'indirizzo **test@homeworks.it** è operativo, possiamo procedere con una prima verifica delle prestazioni di base del server di posta elettronica. Svolgere delle verifiche sulle prestazioni del server di posta elettronica, ci è utile per comprendere quale sarà il comportamento del server di posta quando questi sarà in produzione. Pertanto eseguiamo (conviene eseguire il test sfruttando due sessioni SSH, in una si potranno eseguire i comandi del test, quelli che riporteremo di seguito, nell'altra si potrà tenere monitorato il file di log di Postfix, col comando `tail -f /var/log/mail.info` per verificare se effettivamente i messaggi di prova vengono correttamente inoltrati) i seguenti comandi:

```
time smtp-source -s 20 -l 5120 -m 100 -c -f master@homeworks.it -t test@homeworks.it
localhost:25
```

Dove:

- `-s 20` sta ad indicare che veranno utilizzate 20 connessioni simultanee;
- `-l 5120` sta ad indicare che verranno inviati messaggi da 5120 bytes;
- `-m 100` sta ad indicare che verranno inviati 100 messaggi di prova;
- `-c` sta indicare che verrà mostrato un contatore dei messaggi inviati;
- `-f master@homeworks.it` indica l'indirizzo email del mittente;
- `-t test@homeworks.it` indica l'indirizzo email del destinatario.

Un possibile risultato potrebbe essere:

```
real    0m4.473s
user    0m0.020s
sys     0m0.136s
```

Questo significa che per inviare 100 messaggi da 5120 bytes con 20 sessioni parallele, ci sono voluti circa 4.473 secondi. Questo ha richiesto un tempo in *System Space* di circa 0.136 secondi. Ripetiamo il test

precedente con altri parametri per confrontare poi i risultati fra di loro:

```
time smtp-source -s 20 -l 5120 -m 500 -c -f master@homeworks.it -t test@homeworks.it
localhost:25
```

Un possibile risultato potrebbe essere:

```
real    0m26.888s
user    0m0.056s
sys     0m0.556s
```

Come si evince, in questo caso ci sono voluti circa 27 secondi per inviare 500 messaggi di posta elettronica da 5120 bytes ciascuno. L'invio di questi messaggi ha richiesto circa 0.556 secondi di lavoro in *System Space* da parte del sistema operativo. Ripetiamo il primo test inviando però messaggi di dimensioni pari a circa 10kb:

```
time smtp-source -s 20 -l 10240 -m 100 -c -f master@homeworks.it -t test@homeworks.it
localhost:25
```

Un possibile risultato potrebbe essere:

```
real    0m2.772s
user    0m0.008s
sys     0m0.080s
```

Come si vede, il tempo d'invio si è notevolmente abbassato, in quanto con messaggi di 10kb le prestazioni del disco della macchina sono nettamente migliori che non con messaggi di 5kb.

Una volta valutate le prestazioni complessive del server di posta elettronica, possiamo dedicarci alle singole prestazioni del programma Postfix, ovvero valutare la sua capacità di gestire le email in ingresso. Per far questo dobbiamo aprire due sessioni terminal, oppure effettuare due connessioni SSH. Nella *prima connessione* digitiamo il comando:

```
smtp-sink localhost:2500 1000
```

mentre nella *seconda sessione* eseguiamo il comando:

```
time smtp-source -s 20 -l 5120 -m 100 -c -f master@homeworks.it -t test@homeworks.it
localhost:2500
```

Un possibile risultato potrebbe essere:

```
real    0m0.381s
user    0m0.028s
sys     0m0.068s
```

Se confrontiamo il valore **0.381** con quello ottenuto in precedenza **4.473**, ci accorgiamo che il server di posta elettronica è circa *dodici volte più lento* di quello che dovrebbe essere! Compito di un buon amministratore di sistemi, è quello di cercare di rendere *più piccola possibile*, la differenza fra il valore prestazionale relativo a Postfix e quello dell'intero server di posta elettronica.

SquirrelMail

Per accedere via Web alle *Mailbox*, i responsabili IT della Home Works S.p.A. hanno deciso di utilizzare il programma SquirrelMail. Il programma SquirrelMail utilizza Apache HTTP Server come motore HTTP

ed il linguaggio PHP per definire l'accesso via Web alle Mailbox. Per rendere più veloce l'accesso via Web alle Mailbox, i sistemisti della Home Works hanno deciso di porre fra il programma SquirrelMail ed il programma Courier, il programma up-imapproxy che ha il compito di agevolare il dialogo fra SquirrelMail e Courier. Il programma SquirrelMail è relativamente semplice da installare e gode di un numero considerevole di Plugins che ne estendono le funzionalità.

Per prima cosa mostriamo come installare e configurare il programma Apache HTTP Server, successivamente faremo vedere come installare le librerie del linguaggio PHP, il programma up-imapproxy ed infine mostreremo come installare e configurare il programma SquirrelMail ed alcuni dei suoi innumerevoli Plugins.

Installazione e configurazione base di Apache

Apache è forse il progetto Open Source più noto al mondo. Il programma Apache HTTP Server è senza dubbio il più diffuso programma per la gestione delle connessioni HTTP e HTTPS al mondo. Se si desidera quindi attivare l'accesso HTTP o HTTPS alle *Mailbox* non si può presciendere dall'installazione del programma Apache2:

```
apt-get install apache2 apache2-mpm-prefork apache2-utils libexpat1 ssl-cert
```

Modifichiamo la configurazione di Apache editando il file di configurazione `/etc/apache2/mods-available/dir.conf` aggiungendo come possibile *home page*, anche le pagine che hanno nome `index.htm`, per cui:

```
vi /etc/apache2/mods-available/dir.conf
```

ed inseriamo la voce `index.htm`:

```
<IfModule mod_dir.c>
  DirectoryIndex index.html index.htm index.cgi index.pl index.php index.xhtml
</IfModule>
```

dopo di che salviamo le modifiche effettuate al file `/etc/apache2/mods-available/dir.conf`

Mettiamo in ascolto Apache sulla porta **443** per poter accedere in modalità HTTPS alle Mailbox:

```
vi /etc/apache2/ports.conf
```

Aggiungiamo la voce `Listen 443`:

```
Listen 80
Listen 443
```

Modifichiamo le impostazioni di default:

```
cp /etc/apache2/sites-available/default to /etc/apache2/sites-available/default-ssl
vi /etc/apache2/sites-available/default
```

trasformando le righe:

```
NameVirtualHost *
<VirtualHost *>
...
</VirtualHost>
```

nel seguente modo:

```
NameVirtualHost *:80
<VirtualHost *:80>
...
</VirtualHost>
```

salviamo le modifiche apportate al file */etc/apache2/sites-available/default* Dal momento che vogliamo implementare un accesso sicuro, via HTTPS, alle Mailbox, sfruttiamo l'infrastruttura PKI della Home Works S.p.A. provvedendo a generare i certificati digitali di Apache come indicato nell'articolo Creazione di un'infrastruttura PKI con OpenSSL. Una volta generati i certificati da assegnare al programma Apache:

- */etc/apache2/ssl/mail_private_key.pem* è la *chiave privata* di Apache;
- */etc/apache2/ssl/mail_public_cert.pem* è il *certificato digitale* di Apache;

modifichiamo il file */etc/apache2/sites-available/default-ssl* come segue:

```
vi /etc/apache2/sites-available/default-ssl
```

aggiungiamo le seguenti voci:

```
NameVirtualHost *:443
<VirtualHost *:443>
...
      ServerAdmin webmaster@localhost
      SSLEngine on
      SSLCertificateFile /etc/apache2/ssl/mail_public_cert.pem
          SSLCertificateKeyFile /etc/apache2/ssl/mail_private_key.pem
      DocumentRoot /var/www/
...
</VirtualHost>
```

Salviamo le modifiche realizzate. Dopo le modifiche il file */etc/apache2/sites-available/default-ssl* dovrebbe apparire come:

```
cat /etc/apache2/sites-available/default-ssl
```

```
NameVirtualHost *:443
<VirtualHost *:443>
      ServerAdmin webmaster@localhost
      SSLEngine on
      SSLCertificateFile /etc/apache2/ssl/mail_public_cert.pem
          SSLCertificateKeyFile /etc/apache2/ssl/mail_private_key.pem
      DocumentRoot /var/www/
      <Directory />
              Options FollowSymLinks
              AllowOverride None
      </Directory>
      <Directory /var/www/>
              Options Indexes FollowSymLinks MultiViews
              AllowOverride None
              Order allow,deny
              allow from all
              # This directive allows us to have apache2's default start page
              # in /apache2-default/, but still have / go to the right place
              RedirectMatch ^/$ /apache2-default/
      </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 /var/log/apache2/error.log

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

        CustomLog /var/log/apache2/access.log combined
        ServerSignature On

    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>
```

Definiamo il seguente collegamento simbolico:

```
ln -s /etc/apache2/sites-available/default-ssl /etc/apache2/sites-enabled/000-default-ssl
```

Abilitiamo infine i seguenti moduli di Apache:

```
a2enmod ssl
a2enmod rewrite
```

Disabilitiamo i siti di default:

```
a2dissite
Which site would you like to disable?
Your choices are: 000-default 000-default-ssl
Site name? 000-default
Site 000-default disabled; run /etc/init.d/apache2 reload to fully disable.

a2dissite
Which site would you like to disable?
Your choices are: 000-default 000-default-ssl
Site name? 000-default-ssl
Site 000-default-ssl disabled; run /etc/init.d/apache2 reload to fully disable.
```

Forziamo la riesecuzione di del demone **apache2**:

```
/etc/init.d/apache2 force-reload
```

Installazione e configurazione del programma up-imapproxy

Un *IMAP Proxy* è un programma che consente di velocizzare le Webmail e snellire il carico di lavoro sul server di posta, questo perchè di solito le Webmail, come SquirrelMail, per ogni operazione svolta, eseguono un'operazione di autenticazione nei confronti del server di posta elettronica. Per ridurre il numero di queste operazioni di autenticazione, viene utilizzato un *IMAP Proxy*. Il programma up-imapproxy è una possibile implementazione di un *IMAP Proxy*.

Per prima cosa installiamo il programma up-imapproxy:

```
apt-get install imapproxy
```

Una volta installato il programma, passiamo alla sua configurazione. La configurazione del programma up-imapproxy è piuttosto semplice. Per prima cosa editiamo il suo file di configurazione, */etc/imapproxy.conf*:

```
cp /etc/imapproxy.conf /etc/imapproxy.conf.originale
vi /etc/imapproxy.conf
```

Modificare le seguenti voci (il testo a lato non va riportato nelle modifiche, serve solo a spiegare il significato di ciascuna riga):

```
  server_hostname localhost  <-- Nome del server IMAP
  listen_port 343            <-- Porta in cui resta in ascolto il programma up-
imapproxy
  server_port 143            <-- Porta in cui resta in ascolto il demone IMAP di
Courier
```

Le restanti impostazioni di default possono andare bene. Salviamo quindi le modifiche apportate al file di configurazione. Con queste impostazioni la SquirrelMail deve essere configurata per connettersi alla **porta 343** in luogo di quella di default 143.

Installazione e configurazione di base del programma SquirrelMail

Il programma SquirrelMail è uno dei più diffusi programmi per realizzare una Webmail. Ricco di numerosi Plugins che ne estendono la funzionalità, è in grado di soddisfare le più moderne esigenze di Webmail che un azienda potrebbe richiedere. La sua interfaccia, semplice e leggera, rende la SquirrelMail facile da utilizzare, anche per le persone meno smaliziate.

Per prima cosa, procediamo con l'installazione dei componenti PHP e della SquirrelMail:

> In conformità con la scelta fatta all'inizio dell'articolo, installeremo solamente i componenti linguistici relativi alla sola lingua Italiana.

```
apt-get install php5 libapache2-mod-php5 php5-cgi php5-common php5-recode
apt-get install squirrelmail squirrelmail-locales squirrelmail-decode ispell
apt-get install witalian vacation
```

A causa dell'installazione del programma **ispell**, verrà chiesto di selezionare il **Dictionaries-common: Wordlist dictionary**. Selezionare come Wordlist dictionary il dizionario **american (American English)**. Per configurare in futuro **ispell** si potrà utilizzare il comando:

```
select-default-wordlist
```

Appena l'installazione dei componenti PHP si è conclusa, editiamo il file */etc/php5/apache2/php.ini*:

```
cp /etc/php5/apache2/php.ini /etc/php5/apache2/php.ini.originale
vi /etc/php5/apache2/php.ini
```

controllare che le seguenti variabili siano impostate come di seguito (per scelta del personale IT della Home Works, non sarà possibile inviare file allegati dalla Webmail con dimensione superiore ai 7MB):

```
  expose_php = Off
  file_uploads = On
  upload_max_filesize = 10M
```

con le impostazioni di seguito, non verrà mostrata la versione del linguaggio PHP installata (`expose_php = Off`) e potranno venire caricati nella Webmail al più file di dimensione pari a circa 8MB (`upload_max_filesize`), in seguito alla codifica a 7 bits dei messaggi di posta elettronica.

A questo punto possiamo passare alla configurazione del programma SquirrelMail. Per prima cosa, controlliamo che i permessi della cartella */var/spool/squirrelmail/attach/* siano impostati correttamente:

```
ll /var/spool/squirrelmail
```

assicurarsi che i permessi della cartella siano come quelli riportati di seguito:

```
drwx-wx--- 2 root www-data 4096 2007-05-11 14:11 attach
```

Attiviamo la SquirrelMail, avendo cura di trasformare, per ovvi motivi di sicurezza, i collegamenti HTTP verso la Webmail, in collegamenti HTTPS. Dal momento che il nome FQDN pubblico del server di posta elettronica è **mail.homeworks.it**, attiveremo su questo URL il collegamento alla Webamil. Pertanto:

```
cp /etc/squirrelmail/apache.conf /etc/squirrelmail/apache.conf.originale
vi /etc/squirrelmail/apache.conf
```

modifichiamo il file */etc/squirrelmail/apache.conf* come segue (dove la rete **172.16.4.0/24** è la VLAN del personale IT della Home Works S.p.A):

```
  Alias /squirrelmail /usr/share/squirrelmail

          <Directory /usr/share/squirrelmail>
                Options Indexes FollowSymLinks
          <IfModule mod_php4.c>
                php_flag register_globals off
          </IfModule>
          <IfModule mod_php5.c>
                php_flag register_globals off
          </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 127.0.0.1 192.168.1.0/24 172.16.4.0/24
          </Files>
        </Directory>

        # users will prefer a simple URL like http://mail.example.com
        # will be redirected to URL like https://mail.example.com
        <VirtualHost 192.168.1.8:80>
          DocumentRoot /usr/share/squirrelmail
          ServerAdmin  webmaster@homeworks.it
          ServerName mail.homeworks.it
          RewriteEngine   on
          RewriteCond     %{SERVER_PORT} ^80$
          RewriteRule     ^(.*)$ https://%{SERVER_NAME}$1 [L,R]
          RewriteLog      "/var/log/apache2/rewrite.log"
          RewriteLogLevel 2
        </VirtualHost>

        # users will prefer a simple URL like https://mail.example.com
        <VirtualHost 192.168.1.8:443>
          DocumentRoot /usr/share/squirrelmail
          ServerAdmin  webmaster@homeworks.it
          ServerName mail.homeworks.it
```

```
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/mail_public_cert.pem
        SSLCertificateKeyFile /etc/apache2/ssl/mail_private_key.pem
      </VirtualHost>
```

Impostiamo Apache affinchè possa gestire il sito relativo alla SquirrelMail:

```
ln -s /etc/squirrelmail/apache.conf /etc/apache2/conf.d/squirrelmail.conf
```

Forziamo la riesecuzione del demone **apache2**:

```
/etc/init.d/apache2 force-reload
```

Controlliamo che tutto funzioni correttamente:

```
openssl s_client -CAfile /etc/postfix/certs/global_ca_public_cert.pem -connect
mail.homeworks.it:443

CONNECTED(00000003)
depth=2 /C=IT/ST=Italy/O=Home Works S.p.A./OU=HomeWorks IT Department/CN=HomeWorks Root
CA/emailAddress=support@homeworks.it
verify return:1
depth=1 /C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=HomeWorks Issuing CA/emailAddress=support@homeworks.it
verify return:1
depth=0 /C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=mail.homeworks.it/emailAddress=webmaster@homeworks.it
verify return:1
---
Certificate chain
  0 s:/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=mail.homeworks.it/emailAddress=webmaster@homeworks.it
   i:/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=HomeWorks Issuing CA/emailAddress=support@homeworks.it
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIE5zCCBFCgAwIBAgIJANgUMb8Nfv2UMA0GCSqGSIb3DQEBBQUAMIG3MQswCQYD
VQQGEwJJVDEOMAwGA1UECBMFSXRhbHkxFjAUBgNVBAcTDVJlZ2dpbyBFbWlsaWEx
GjAYBgNVBAoTEUhvbWUgV29ya3MgUy5wLkEuMSAwHgYDVQQLExdIb211V29ya3Mg
SVQgRGVwYXJ0bWVudDEdMBsGA1UEAxMUSG9tZVdvcmtzIEl1zc3VpbmcgQ0ExIzAh
BgkqhkiG9w0BCQEWFHN1cHBvcnRAaG9tZXdvcmtzLml0MB4XDTA4MDQwNzAwMTA0
MloXDTEyMDQwNjAwMTA0MlowgbYxCzAJBgNVBAYTAklUMQ4wDAYDVQQIEwVJdGFs
eTEWMBQGA1UEBxMNUmVnZ2lvIEVtaWxpYTEaMBgGA1UEChMRSG9tZSBXb3JrcyBT
LnAuQS4xIDAeBgNVBAsTF0hvbWVXb3JrcyBJVCBEZXBhcnRtZW50MRowGAYDVQQD
ExFtYWlsLmhvbWV3b3Jrcy5pdDElMCMGCSqGSIb3DQEJARYWd2VibWFzdGVyQGhv
bWV3b3Jrcy5pdDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAviI4YjyMdfmv
uPN9PCix76ip3xGzyAOtvIHTiGk7m+Zwn4wi2MGm4/iTQB8k6pgRZxWibj3/imei
I9kptc9MELKhwRdQkAe8Fp2Nsmek6e3gkZfvFWYp9lNqrE0Jkoq8kIir1r/ukvL9
T96622lDTvruHNYRHhf1bn1EJcL2GVcCAwEAAaOCAfgwggH0MAkGA1UdEwQCMAAw
EQYJYIZIAYb4QgEBBAQDAgZAMAsGA1UdDwQEAwIE8DAoBgNVHSUEITAfBggrBgEF
BQcDAQYIKwYBBQUHAwIGCWCGSAGG+EIEATAdBgNVHQ4EFgQUdu/VgFhHDDxGEUG2
YhNCu6KvMp0wgdEGA1UdIwSByTCBxoAUrEezp30mjPsHVnO2Yh0P62iOk9ehgaKk
gZ8wgZwxCzAJBgNVBAYTAklUMQ4wDAYDVQQIEwVJdGFseTEaMBgGA1UEChMRSG9t
ZSBXb3JrcyBTLnAuQS4xIDAeBgNVBAsTF0hvbWVXb3JrcyBJVCBEZXBhcnRtZW50
MRowGAYDVQQDExFIb211V29ya3MgUm9vdCBDQTEjMCEGCSqGSIb3DQEJARYUc3Vw
cG9ydEBob211ld29ya3MuaXSCCQDYFDG/DX79ijA/BggrBgEFBQcBAQQzMDEwLwYI
KwYBBQUHMAKGI2h0dHA6Ly93d3cuaG9tZXdvcmtzLml0L2NhaW5mby5odG1sMDsG
A1UdHwQ0MDIwMKAuoCyGKmh0dHA6Ly93d3cuaG9tZXdvcmtzLml0L2NybC9pc3N1
aW5nX2NhLmNybDAsBgNVHREEJTAjpCEwHzEdMBsGA1UEAxMUd2VibWFpbC5ob21l
d29ya3MuaXQwDQYJKoZIhvcNAQEFBQADgYEAqGqEREGNX7bpMS1sX6Obt5v2j0pE
TFz06XquTEyBYdvnyJuFIF5h/gMcmX0qT7Ho/sGCu4l4qYYZhGzBYojk8dWVxHmg
B6zIx1lwuojUD+xgan/VvUEspKMPjwOgSwx5FRc7o0Glqlyvyxsr VLVqS+yZp6I6
0r2+a5uD5g6Uykg=
-----END CERTIFICATE-----
subject=/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=mail.homeworks.it/emailAddress=webmaster@homeworks.it
issuer=/C=IT/ST=Italy/L=Reggio Emilia/O=Home Works S.p.A./OU=HomeWorks IT
Department/CN=HomeWorks Issuing CA/emailAddress=support@homeworks.it
---
No client certificate CA names sent
```

```
---
SSL handshake has read 1823 bytes and written 316 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
  Protocol : TLSv1
  Cipher : DHE-RSA-AES256-SHA
  Session-ID: 0E39A40FD14A7BA11381059930D5A8EB2737AF24F7EB19B04AD502B8E2E36C27
  Session-ID-ctx:
  Master-Key:
729274FA1DAA1FC9EC5E80D61648E197975D30ED6EF9FB201DFED0C123DD7E8D3800CB3B1E66F5F3E267EC116B6A5
9FF
  Key-Arg : None
  Start Time: 1208012232
  Timeout : 300 (sec)
  Verify return code: 0 (ok)
---
```

Se compare la sigla `Verify return code: 0 (ok)` vuol dire che tutto è andato bene. Possiamo quindi interrompere il collegamento:

```
quit
closed
```

Verifichiamo che i permessi della cartella */etc/squirrelmail* siano come quelli riportati di seguito:

```
ll /etc/squirrelmail/
```

```
  -rw-r--r-- 1 root root  1328 2007-07-01 01:09 apache.conf
  -rw-r--r-- 1 root root  1230 2007-06-30 01:26 apache.conf.originale
  -rw-r--r-- 1 root root 30482 2007-05-10 11:59 config_default.php
  -rw-r--r-- 1 root root   473 2007-05-10 11:59 config_local.php
  -rw-r--r-- 1 root root  8733 2007-08-07 00:43 config.php
  lrwxrwxrwx 1 root root    32 2007-06-30 00:49 conf.pl -> /usr/sbin/squirrelmail-
configure
  -rw-r--r-- 1 root root    48 2007-05-10 11:59 default_pref
  -rw-r--r-- 1 root root  6589 2007-05-10 11:59 filters_setup.php
  -rw-r--r-- 1 root root   492 2007-05-10 11:59 index.php
  -rw-r--r-- 1 root root  1901 2007-05-10 11:59 sqspell_config.php
```

Per abilitare il modulo di amministrazione (plugin **Administrator**) modifichiamo i permessi del file */etc/squirrelmail/config.php* come segue:

```
chown master:www-data /etc/squirrelmail/config.php
ll /etc/squirrelmail/config.php
```

```
-rw-rw---- 1 master www-data  7924 2007-08-07 01:28 config.php
```

In questo modo, l'utente di sistema denominato **master** godrà dei privilegi amministrativi sulla SquirrelMail.

Verifichiamo i permessi della cartella */usr/share/squirrelmail/src/* per controllare che siano come quelli riportati di seguito:

```
  -rw-r--r-- 1 root root  1204 2007-05-10 11:59 addrbook_popup.php
  -rw-r--r-- 1 root root 10750 2007-05-10 11:59 addrbook_search_html.php
  -rw-r--r-- 1 root root 10232 2007-05-10 11:59 addrbook_search.php
  -rw-r--r-- 1 root root 21453 2007-05-10 11:59 addressbook.php
  -rw-r--r-- 1 root root 65413 2007-05-11 14:09 compose.php
  -rw-r--r-- 1 root root 16014 2007-05-10 11:59 configtest.php
  -rw-r--r-- 1 root root  2292 2007-05-10 11:59 delete_message.php
```

```
-rw-r--r-- 1 root root  5075 2007-05-10 11:59 download.php
-rw-r--r-- 1 root root  2487 2007-05-10 11:59 empty_trash.php
-rw-r--r-- 1 root root  2514 2007-05-10 11:59 folders_create.php
-rw-r--r-- 1 root root  4604 2007-05-10 11:59 folders_delete.php
-rw-r--r-- 1 root root 10584 2007-05-10 11:59 folders.php
-rw-r--r-- 1 root root  2468 2007-05-10 11:59 folders_rename_do.php
-rw-r--r-- 1 root root  2591 2007-05-10 11:59 folders_rename_getname.php
-rw-r--r-- 1 root root  2208 2007-05-10 11:59 folders_subscribe.php
-rw-r--r-- 1 root root  9215 2007-05-10 11:59 help.php
-rw-r--r-- 1 root root  1974 2007-05-10 11:59 image.php
-rw-r--r-- 1 root root   492 2007-05-10 11:59 index.php
-rw-r--r-- 1 root root 16345 2007-05-10 11:59 left_main.php
-rw-r--r-- 1 root root  7031 2007-05-10 11:59 login.php
-rw-r--r-- 1 root root  2560 2007-05-10 11:59 mailto.php
-rw-r--r-- 1 root root  9028 2007-05-10 11:59 move_messages.php
-rw-r--r-- 1 root root 16298 2007-05-10 11:59 options_highlight.php
-rw-r--r-- 1 root root  6382 2007-05-10 11:59 options_identities.php
-rw-r--r-- 1 root root  5571 2007-05-10 11:59 options_order.php
-rw-r--r-- 1 root root 17949 2007-05-10 11:59 options.php
-rw-r--r-- 1 root root  9859 2007-05-10 11:59 printer_friendly_bottom.php
-rw-r--r-- 1 root root  1465 2007-05-10 11:59 printer_friendly_main.php
-rw-r--r-- 1 root root  1371 2007-05-10 11:59 printer_friendly_top.php
-rw-r--r-- 1 root root 33851 2007-05-10 11:59 read_body.php
-rw-r--r-- 1 root root  6587 2007-05-10 11:59 redirect.php
-rw-r--r-- 1 root root  7700 2007-05-10 11:59 right_main.php
-rw-r--r-- 1 root root 19638 2007-05-10 11:59 search.php
-rw-r--r-- 1 root root  2948 2007-05-10 11:59 signout.php
-rw-r--r-- 1 root root  8071 2007-05-10 11:59 vcard.php
-rw-r--r-- 1 root root  4450 2007-05-10 11:59 view_header.php
-rw-r--r-- 1 root root  3779 2007-05-11 14:09 view_text.php
-rw-r--r-- 1 root root  5336 2007-05-10 11:59 webmail.php
```

A questo punto siamo pronti per eseguire la configurazione di base della SquirredMail. Pertanto eseguiamo il comando:

```
squirrelmail-configure
```

procediamo come segue:

- al prompt, scrivere `D` (**Set pre-defined settings for specific IMAP servers**) e poi premere **invio**;
- dal menù:

```
    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
```

  scegliere `courier`, ovvero scrivere al prompt la parola `courier` e poi premere **invio**;
- al prompt, scrivere `2` (**Server Settings**) e poi premere **invio**;
- al prompt, scrivere `A` (**Update IMAP Settings**) e poi premere **invio**;
- compilare i vari campi della sezione **Update IMAP Settings** come segue:

```
IMAP Settings
--------------
4.  IMAP Server            : localhost
5.  IMAP Port              : 343
```

```
6.  Authentication type    : login
7.  Secure IMAP (TLS)      : FALSE
8.  Server software        : courier
9.  Delimiter              : .
```

- al prompt scrivere il numero del parametro da modificare e poi premere **invio**. Inserire la modifica desiderata e confermare premendo **invio**;
- compilati tutti i campi, al prompt scrivere **S** (**Save data**) e poi premere due volte **invio**;
- al prompt scrivere `H` e poi premere **invio**;
- al prompt, scrivere `R` (**Return to Main Menu**) e poi premere **invio**;
- al prompt, scrivere `4` (**General Options**) e poi premere **invio**;
- configurare le **General Options** come segue:

```
General Options
1.  Data Directory              : /var/lib/squirrelmail/data/
2.  Attachment Directory        : /var/spool/squirrelmail/attach/
3.  Directory Hash Level        : 0
4.  Default Left Size           : 100
5.  Usernames in Lowercase      : FALSE
6.  Allow use of priority       : TRUE
7.  Hide SM attributions        : FALSE
8.  Allow use of receipts       : TRUE
9.  Allow editing of identity   : TRUE
    Allow editing of name       : TRUE
    Remove username from header : FALSE
10. Allow server thread sort    : FALSE
11. Allow server-side sorting   : TRUE
12. Allow server charset search : TRUE
13. Enable UID support          : TRUE
14. PHP session name            : SQMSESSID
15. Location base               :
```

- al prompt scrivere il numero del parametro da modificare e poi premere **invio**. Inserire la modifica desiderata e confermare premendo **invio**;
- compilati tutti i campi, al prompt scrivere **S** e poi premere due volte **invio**;
- al prompt, scrivere `R` (**Return to Main Menu**) e poi premere **invio**;
- al prompt, scrivere `1` (**Organization Preferences**) e poi premere **invio**;
- configurare le **Organization Preferences** come segue:

```
Organization Preferences
1.  Organization Name      : Home Works
2.  Organization Logo      : ../images/sm_logo.png
3.  Org. Logo Width/Height : (308/111)
4.  Organization Title     : Webmail Home Works ($version)
5.  Signout Page           :
6.  Top Frame              : _top
7.  Provider link          : http://www.homeworks.it/
8.  Provider name          : Home Works
```

- al prompt scrivere il numero del parametro da modificare e poi premere **invio**. Inserire la modifica desiderata e confermare premendo **invio**;
- compilati tutti i campi, al prompt scrivere **S** (**Save data**) e poi premere due volte **invio**;
- al prompt, scrivere `R` (**Return to Main Menu**) e poi premere **invio**;
- al prompt, scrivere `5` (**Themes**) e poi premere **invio**;
- al prompt, scrivere `1` (**Change Themes**) e poi premere **invio**;
- al prompt, scrivere `?` e poi premere **invio**. In questo modo si ha una lista dei comandi che si hanno a disposizione;

- al prompt, scrivere `l` e poi premere **invio**;
- al prompt, scrivere `m 48` e poi premere **invio**, per selezionare il tema **Classic Blue 2** come tema predefinito;
- al prompt, scrivere `l` e poi premere **invio**, per verificare che accanto al numero **48** compaia un asterisco, *****, che sta ad indicare qual'è il tema predefinito;
- al prompt, scrivere `d` e poi premere **invio**, per confermare le modifiche;
- al prompt, scrivere `S` (**Save data**) e poi premere due volte **invio**;
- al prompt, scrivere `R` (**Return to Main Menu**) e poi premere **invio**;
- al prompt, scrivere `7` (**Message of the Day (MOTD)**) e poi premere **invio**;
- al prompt, scrivere `1` (**Edit the MOTD**) e poi premere **invio**;
- al nuovo prompt, scrivere **Webmail di Home Works S.p.A.** e poi premere **invio**;
- al nuovo prompt, scrivere `@` e poi premere **invio**;
- verificare che la schermata appaia come riportato di seguito:

```
Message of the Day (MOTD)
Webmail di Home Works S.p.A.
```

- al prompt, scrivere `S` (**Save data**) e poi premere due volte **invio**;
- al prompt, scrivere `R` (**Return to Main Menu**) e poi premere **invio**;
- al prompt, scrivere `10` (**Languages**) e poi premere **invio**;
- assicurarsi che i campi siano compilati come riportato di seguito:

```
Language preferences
1.  Default Language       : en_US
2.  Default Charset        : iso-8859-1
3.  Enable lossy encoding  : FALSE
```

- al prompt scrivere il numero del parametro da modificare e poi premere **invio**. Inserire la modifica desiderata e confermare premendo **invio**;
- al prompt, scrivere `S` (**Save data**) e poi premere due volte **invio**;
- al prompt, scrivere `R` (**Return to Main Menu**) e poi premere **invio**;
- al prompt, scrivere `S` (**Save data**) e poi premere due volte **invio**;
- al prompt, scrivere `Q` (**Quit**) e poi premere **invio** per uscire dalla procedura di configurazione della SquirrelMail.

Per verificare che tutto sia andato bene, aprire il proprio browser predefinito ed aprire il seguente URL **https://mail.homeworks.it/src/configtest.php** Non preoccuparsi se compare la seguente segnalazione di errore:

ERROR: *OUTBOX setting is enabled in your Courier imapd configuration. SquirrelMail uses standard SMTP protocol or sendmail binary to send emails. Courier IMAP delivery method is not supported and can create duplicate email messages.*

Verificare alla fine della pagina che compaia la seguente indicazione: **Congratulations, your SquirrelMail setup looks fine to me!** A questo punto la configurazione di base della SquirrelMail è conlcusa.

Come abilitare il supporto alla lingua Italiana nella SquirrelMail

La SquirrelMail supporta diversi tipi di lignue, tra cui l'Italiano, il Tedesco ed il Russo. Per venire incontro alle esigenze aziendali, la lingua base della Webmail sarà l'Inglese, a ciascun dipendente della Home Works verrà poi spiegato come passare dalla lingua Inglese alla sua lingua madre. Di seguito

faremo vedere come consentire il passaggio dalla lingua Inglese a quella Italiana. Quanto detto per la lingua Italiana, varrà anche per le lignue Tedesca e Russa.

Per impostazione predefinta, la distribuzione Debian supporta solamente la lingua Inglese, pertanto, il supporto alle altre lingua va esplicitamente abilitato (per sapere come abilitare la distribuzione Debian al supporto di altre lingue oltre all'Inglese, si può consultare quanto riportato nel paragrafo Configurarazione di base del sistema operativo). Per prima cosa andiamo a verificare se la SquirrelMail è in grado di supportare le lingue aggiuntive, per cui apriamo il nostro browser preferito e torniamo a far visita al URL **https://mail.homeworks.it/src/configtest.php** e controlliamo che compaia la frase: **gettext - Gettext functions are available. You must have appropriate system locales compiled**. Se la frase compare vuol dire che la SquirrelMail è in grado di supportare le lingue aggiuntive.

Procediamo pertanto con l'impostazione della lingua Italiana nella SquirrelMail:

- ci colleghiamo alla SquirrelMail col utente a cui vogliamo impostare la lingua Italiana (per fare una prova si può utilizzare l'utente **Test**);
- una volta collegati andiamo nella sezione **Options** -> **Display Preferences**. Dal menù a tendiano del campo **Language**, scegliamo come lingua la voce **Italian**. Confermiamo la nostra selezione premendo il pulsante **Submit**, che si trova in fondo alla pagina;
- ricarichiamo la pagina (in Firefox ed Internet Explorer è sufficiente premere il tasto **F5**) e dopo qualche istante la pagina ci dovrebbe riapparire in Italiano.


Si osservi infine che non tutti i Plugins prevedono una traduzione in Italiano, quindi in alcune pagine della SquirrelMail potrebbero comparire sia voci in Italiano sia voci in Inglese. Per ovviare a questo, bisogna provvedere in autonomia ad eseguire la traduzione di queste parti di testo, contribuendo direttamente al progetto SquirrelMail.

Installazione e configurazione dei principali Plugins della SquirrelMail

La SquirrelMail ha diversi Plugins che ne estendono le funzionalità. Per installare un Plugin basta seguire la seguente procedura:

- scaricare il Plugin che interessa installare in una cartella temporanea (ad esempio */home/master/sm_new_plugins*):

```
md /home/master/sm_new_plugins
cd /home/master/sm_new_plugins
wget http://squirrelmail.org/countdl.php?fileurl=http%3A%2F%2Fwww.squirrelmail.org
%2Fplugins%2F<Nome_Plugin>.tar.gz
```

- estarre il plugin nella cartella temporanea e controllare che i permessi dei file siano assegnati sia all'utente, sia al gruppo **root**:

```
tar -zxvf /home/master/sm_new_plugins/<Nome_Plugin>.tar.gz
ll /home/master/sm_new_plugins/<Nome_Plugin>.tar.gz
```

- per sapere come installare il plugin, conviene leggere il file *INSTALL* che di solito si trova nella cartella in cui è stato estratto il plugin. Nella maggior parte dei casi, però, è sufficiente copiare il contenuto della cartella che contiene il plugin nella cartella */usr/share/squirrelmail/plugins* Per leggere il file *INSTALL* si può utilizzare il comando:

```
less /home/master/sm_new_plugins/<Nome_Plugin>/INSTALL
```

  Per copiare il contenuto della cartella */home/master/sm_new_plugins/<Nome_Plugin>* nella cartella */usr/share/squirrelmail/plugins*, si può eseguire il comando:

```
cp -R /home/master/sm_new_plugins/<Nome_Plugin> /usr/share/squirrelmail/plugins
```

Una volta che la cartella contenente il plugin è stata copiata nella cartella `/usr/share/squirrelmail/plugins`, si può procedere all'abilitazione del plugin. Per abilitare uno o più plugin si può procedere come segue:

- eseguire, sfruttando i permessi dell'utente **root**, il comando

```
squirrelmail-configure
```

- al prompt, scrivere `8` (**Plugins**) e poi premere **invio**;
- osservando la lista degli **Available Plugins** individuare il nome del plugin da abilitare. Prendere nota del numero che sta a fianco al nome del plugin da abilitare;
- al prompt, scrivere il numero relativo al plugin da abilitare e poi premere **invio**;
- verificare che il nome del plugin da abilitare compaia nell'elenco **Installed Plugins**. Se il nome del plugin da abilitare compare all'interno dell'elenco **Installed Plugins** vuol dire che il plugin è stato correttamente abilitato;
- al prompt, scrivere `S` (**Save data**) e poi premere due volte **invio**;
- al prompt, scrivere `R` (**Return to Main Menu**) e poi premere **invio**;
- al prompt, scrivere `S` (**Save data**) e poi premere due volte **invio**;
- al prompt, scrivere `Q` (**Quit**) e poi premere **invio** per uscire dalla procedura di configurazione della SquirrelMail. Se necessario, alla domanda che chiede si salvare o meno la configurazione della SquirrelMail, ripondere scrivendo `y` e poi premere **invio**.

Risulta conveniente abilitare i seguenti plugin (i plugin senza collegamento URL fanno già parte della versione base della SquirrelMail):

- Add Address;
- Addressbook Import-Export;
- Administrator;
- Compatibility;
- Compose Extras;
- Delete Move Next;
- Empty Folders;
- Folder Sizes;
- Forced Preferences;
- Left CSS;
- Local User Autoresponder;
- Message_Details;
- Reply Buttons;
- Shared Calendars;
- Show User and IP;
- Spam Buttons;

Configurazione del plugin Local User Autoresponder

Il plugin Local User Autoresponder consente di impostare un messaggio email di risposta automatica e di inoltrare i messaggi in arrivo ad una o più mailbox (in questo modo, anche in assenza di una o più persone della Home Works, i messaggi di posta elettronica a loro indirizzati possono venire consultati dai colleghi). Questo plugin per funzionare richiede che gli utenti del servizio di posta elettronica siano anche utenti del sistema ed abbiamo quindi una propria *home directory* e che il plugin Compatibility sia installato.

Per attivare i messaggi di risposta automatica verranno creati i seguenti file all'interno delle *home directory* degli utenti (in questo esempio è riportato ciò che compare nella home directory dell'utente **test**):

```
-rw------- 1 test test    32 2007-11-24 16:11 .forward
-rw------- 1 test test     0 2007-11-24 16:11 .forward.fwd
-rw------- 1 test test 12288 2007-11-24 16:29 .vacation.db
-rw------- 1 test test   120 2007-11-24 16:11 .vacation.msg
-rw------- 1 test test    90 2007-11-24 16:11 .vacation.pref
-rw------- 1 test test    54 2007-11-24 16:11 .vacation.sq
-rw------- 1 test test    12 2007-11-24 16:11 .vacation.subj
```

Per poter installare il plugin Local User Autoresponder bisogna procedere come segue (eseguire le operazioni riportate utilizzando l'utente **root**):

```
cd /home/master/sm_new_plugins
wget http://www.squirrelmail.org/countdl.php?fileurl=http%3A%2F%2Fwww.squirrelmail.org
%2Fplugins%2Flocal_autorespond_forward-3.0-1.4.0.tar.gz
cp /home/master/sm_new_plugins/local_autorespond_forward-3.0-1.4.0.tar.gz
/usr/share/squirrelmail/plugins
cd /usr/share/squirrelmail/plugins
tar -zxvf /usr/share/squirrelmail/plugins/local_autorespond_forward-3.0-1.4.0.tar.gz
cd /usr/share/squirrelmail/plugins/local_autorespond_forward/suid_backend/
./configure --enable-auth=shadow --enable-webuser=www-data
make
make install
cd ..
cp /usr/share/squirrelmail/plugins/local_autorespond_forward/config.sample.php
/usr/share/squirrelmail/plugins/local_autorespond_forward/config.php
```

Modificare il file `/usr/share/squirrelmail/plugins/local_autorespond_forward/config.php` come segue:

```
vi /usr/share/squirrelmail/plugins/local_autorespond_forward/config.php
```

modificare la riga: `$laf_backend = 'ftp';` in

```
$laf_backend = 'suid';
```

Salvare il file.

A questo punto si può aggiungere il plugin Local User Autoresponder tra quelli della SquirrelMail. Per attivare il messaggio di risposta automatica, bisogna andare nella sezione **Options** (**Opzioni**), poi in **Autoresponder / Mail Forwarding** e compilare in modo opportuno gli appositi campi. Per abilitare il messaggio di risposta automatica, selezionare la voce **Enable auto-reply to sender**. Una volta compilato gli appositi campi in modo opportuno premere il pulsante **Submit** per confermare le impostazioni adottate.

Come creare un profilo predefinito per tutti gli utenti della SquirrelMail

Risulta particolarmente comodo creare un profilo predefinito per i nuovi accessi alla Webmail, in questo modo molte delle impostazioni più utilizzate possono venire attivate sin dal primo accesso, senza che la persona che accede alla Webmail debba provvedere ad attivarle.

I vari profili degli utenti vengono archiviati in un unico file (estensione `.pref`) che si trova nella cartella (*Data Directory*): `/var/lib/squirrelmail/data/`

Per creare un profilo predefinito, ovvero per impostare una configurazione di default per tutti gli utenti, si può procedere come segue (le operazioni che riportiamo vanno eseguite prima che la webmail diventi operativa, ovvero prima che inizi ad essere utilizzata dal personale della Home Works S.p.A):

- utilizzare uno degli accessi alla SquirrelMail già esistenti, per impostare le impostazioni di default che si desidera attivare (allo scopo si può utilizzare ad esempio l'utente **master** creato in precedenza);
- una volta terminato di configurare il profilo di default (nel nostro esempio quello dell'utente **master**), uscire dalla SquirrelMail;
- copiare il file relativo al profilo dell'utente utilizzato come modello (ad esempio, qualora si avesse utilizzato l'utilizzato l'utente **master**, il file in questione sarebbe */var/lib/squirrelmail/data/master.pref*) col nome */var/lib/squirrelmail/data/default_pref*. Ad esempio:

```
cp /var/lib/squirrelmail/data/master.pref /var/lib/squirrelmail/data/default_pref
```

- assicurarsi che il file */var/lib/squirrelmail/data/default_pref* abbia i seguenti permessi:

```
-r-------- 1 www-data www-data  817 2007-08-14 17:58 default_pref
```

  Se ciò non fosse, eseguire il comando:

```
chown www-data:www-data /var/lib/squirrelmail/data/default_pref
```

- editare il file */var/lib/squirrelmail/data/default_pref*:

```
vi /var/lib/squirrelmail/data/default_pref
```

- togliere tutti i riferimenti relativi all'utente che è stato utilizzato come modello (nel nostro esempio, togliere tutti i riferimenti all'utente **master**). Salvare le modifiche.

A questo punto il profilo predefinito è operativo. Per controllare che tutto funzioni correttamente, provare ad accedere alla Webmail con un utente diverso da quello utilizzato per creare il profilo predefinito (nel nostro esempio, questo possibile utente, potrebbe essere l'utente **test**) e verificare che tutto funzioni correttamente.

Un possibile esempio di file */var/lib/squirrelmail/data/default_pref* potrebbe essere:

```
  adm_Group2=on
  adm_Group3=on
  adm_Group4=off
  adm_Group6=on
  adm_Group7=on
  adm_Group8=on
  adm_Group9=on
  chosen_theme=../themes/classic_blue2.php
  compose_height=678
  compose_new_win=1
  compose_width=728
  delete_move_next_b=on
  delete_move_next_formATbottom=on
  delete_move_next_formATtop=off
  delete_move_next_t=off
  empty_folders_link_behavior=moveToTrash
  empty_folders_show_link=INBOX.Drafts###INBOX.Sent###
  fix_compose_tabs=2
  folder_sizes_link_button=1
  folder_sizes_subtotals=1
  hililist=a:1:{i:0;a:4:{s:4:"name";s:23:"Postmaster -
HomeWorks";s:5:"color";s:6:"ff99ff";s:5:"value";s:25:"postmaster@homeworks.it";s:10:"
match_type";s:4:"from";}}
  hour_format=1
  insert_lines_in_reply_body=0
  javascript_on=1
  language=en_US
```

```
left_refresh=300
left_size=190
pp_refresh_message_list=1
prefix_sig=1
previewPane_vertical_split=0
reply_citation_style=date_time_author
reply_focus=focus
sb_move_after_report_not_spam=0
sb_move_after_report_spam=INBOX.Trash
sb_suppress_not_spam_button_folder=0
sb_suppress_spam_button_folder=0
show_host_on_left_pane=0
show_html_default=0
show_ip_on_left_pane=1
show_reply_all_button_on_message_list=1
show_reply_button_on_message_list=1
show_user_on_left_pane=0
smallcal_bottom=0
smallcal_calendar=Personal
smallcal_event=#FFFF00
smallcal_header=#c95d02
smallcal_separator=0
smallcal_show=1
smallcal_today=#00CC00
sort=0
use_previewPane=1
use_signature=1
```

ClamAV

L'antivirus ClamAV, sebbene gratuito, è sia particolarmente efficace, sia piuttosto efficiente. Non di rado capita che alcuni virus individuati dal ClamAV risultino sconosciuti ai principali prodotti antivirus commerciali (per maggiori informazioni su questo tipo di statistiche, si può consultare il sito web Virustotal).

Installazione e configurazione dell'antivirus ClamAV

A causa della frequenza con cui viene aggiornato il programma antivirus ClamAV, la versione disponibile nel repository ufficiale Debian, relativo alla versioni stabili dei programmi, risulta datata. Pertanto la distribuzione Debian ha provveduto a realizzare un apposito repository per i programmi, come ClamAV, che hanno bisogno di aggiornamenti frequenti, questo repository prende il nome di Debian Volatile. Aggiungere, qualora non lo si fosse già fatto in precedenza, il repository Debian Volatile alla lista dei repository ufficiali Debian (per sapere come aggiungere il repository Debian Volatile si può consultare il paragrafo Configurarazione di base del sistema operativo)

Una volta reso disponibile il repository Debian Volatile, possiamo procedere con l'installazione dei componenti dell'antivirus ClamAV (al momento in cui questa articolo è stato scritto, la versione stabile del antivirus ClamAV disponibile era la **0.90.1-3etch3**):

```
apt-get install clamav clamav-freshclam clamav-testfiles clamsmtp
```

Controllare che durante l'installazione, vengano svolte con successo le seguenti operazioni:

```
Setting up clamav-base (0.90.1-3etch3) ...
Adding system user `clamav' (UID 107) ...
Adding new group `clamav' (GID 108) ...
Adding new user `clamav' (UID 107) with group `clamav' ...
Not creating home directory `/var/lib/clamav'.
```

```
Setting up clamsmtp (1.8-5) ...
Warning: The home dir you specified does not exist.
Adding system user `clamsmtp' (UID 108) ...
Adding new group `clamsmtp' (GID 109) ...
Adding new user `clamsmtp' (UID 108) with group `clamsmtp' ...
Not creating home directory `/var/spool/clamsmtp'.
Adding user `clamav' to group `clamsmtp' ...
Done.
```

Per poter interfacciare il programma antivirus ClamAV con Postfix, i responsabili IT della Home Works hanno deciso di utilizzare il programma ClamSMTP. Per scelta da parte dei manutentori del pacchetto Debian del programma ClamSMTP, il programma ClamSMTP utilizza, di default, le seguenti porte:

- **127.0.0.1:10025** per inviare le email controllate dall'antivirus
- **127.0.0.1:10026** per ricevere le email che devono essere controllate

pertanto la configurazione di Postfix va modificata nel seguente modo. Per prima cosa editiamo il file di configurazione */etc/postfix/main.cf*:

```
vi /etc/postfix/main.cf
```

aggiungiamo le righe seguenti:

```
content_filter = scan:[127.0.0.1]:10026
receive_override_options = no_address_mappings
```

Salviamo le modifiche apportate al file */etc/postfix/main.cf* e passiamo a cambiare il contenuto del file */etc/postfix/master.cf*:

```
vi /etc/postfix/master.cf
```

aggiungere la seguente porzione di codice:

```
# AV scan filter (used by content_filter)
scan      unix  -       -       n       -       16      smtp
        -o smtp_send_xforward_command=yes
        -o disable_dns_lookups=yes

# For injecting mail back into postfix from the filter
127.0.0.1:10025 inet  n -       n       -       16      smtpd
        -o content_filter=
        -o
receive_override_options=no_unknown_recipient_checks,no_header_body_checks
        -o smtpd_helo_restrictions=
        -o smtpd_client_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o mynetworks_style=host
        -o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

Riavviamo il demone di Posftix:

```
postfix check
/etc/init.d/postfix restart
```

A questo punto siamo pronti per eseguire i primi test sul funzionamento dell'antivirus ClamAV.

Controllo del corretto funzionamento dell'antivirus ClamAV

In questo paragrafo riporteremo una serie di test che conviene svolgere per controllare il corretto funzionamento dell'antivirus ClamAV. Per prima cosa mettiamo in esecuzione il programma ClamSMTP:

```
clamsmtpd -f /etc/clamsmtpd.conf
```

Eseguiamo il primo test sfruttando i file di prova dell'antivirus ClamAV:

```
cd /usr/share/clamav-testfiles
clamscan -i -r
```

se compaiono i seguenti messaggi a video, vuol dire che il motore funziona correttamente:

```
/usr/share/clamav-testfiles/clam.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-v2.rar: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.exe.bz2: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-v3.rar: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.zip: ClamAV-Test-File FOUND

----------- SCAN SUMMARY -----------
Known viruses: 139558
Engine version: 0.90.1
Scanned directories: 1
Scanned files: 7
Infected files: 5
Data scanned: 0.00 MB
Time: 30.460 sec (0 m 30 s)
```

Eseguiamo una scansione manuale del sistema:

```
cd /usr/share/clamav-testfiles
clamdscan
```

se compaiono i seguenti messaggi vuol dire che il demone funziona correttamente:

```
/usr/share/clamav-testfiles/clam.exe: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-v2.rar: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.exe.bz2: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam-v3.rar: ClamAV-Test-File FOUND
/usr/share/clamav-testfiles/clam.zip: ClamAV-Test-File FOUND

----------- SCAN SUMMARY -----------
Infected files: 5
Time: 0.534 sec (0 m 0 s)
```

Una volta certi che il programma antivirus ClamAV funzioni correttamente, si può procedere a testare il funzionamento del programma ClamSMTP. Scopo di questa prova è quello d'inviare al nostro server di posta elettronica delle email infette con virus di prova e verficare che queste email infette siano effettivamente intercettate dal programma antivirus ClamAV. La società GFI mette a disposizione in maniera gratuita delle email con virus di prova. Per poter utilizzare queste email, bisogna prima registrarsi sul sito web http://www.gfi.com/emailsecuritytest/. Una volta acceduti al sito http://www.gfi.com/emailsecuritytest/ bisogna compilare i campi di accesso come segue (nel corso dei nostri test utilizzeremo la mailbox **postmaster@homeworks.it**):

- **Name**: Postmaster Home Works
- **Email**: postmaster@homeworks.it

Togliamo il segno di selezione dalla voce **Check here to receive GFI's security newsletter, containing**

Email Security Testing Zone updates and other security-related news e premiamo il pulsante **Test my email system**. A questo punto verrà inviata un email di conferma di invio dei file di test. Leggere questa email inviata dalla società GFI e seguire le istruzioni riportate nella sezione:

```
If you have any problems with the above link, please visit:
http://www.gfi.com/emailsecuritytest/manual.htm
Then enter the following:
465373706350174 and click on 'Submit'.
```

Visitiamo pertanto il sito http://www.gfi.com/emailsecuritytest/manual.htm, inseriamo il codice che ci è stato fornito, `465373706350174` e premiamo il pulsante **Submit** come richiesto. Alla pressione del tasto **Submit** verranno inviate tutte le email di test. Attendere qualche minuto e poi andare controllare il file di log dell'antivirus ClamAV:

```
tail -n 50 /var/log/clamav/clamav.log
```

se compaiono i seguenti messaggi:

```
  Sat Jul 21 17:09:10 2007 -> /var/spool/clamsmtp/clamsmtpd.mor1Mk: GFI.VBS.Test
FOUND
  Sat Jul 21 17:09:11 2007 -> /var/spool/clamsmtp/clamsmtpd.bdPy6s: GFI.VBS.Test
FOUND
  Sat Jul 21 17:09:11 2007 -> /var/spool/clamsmtp/clamsmtpd.Lm6NIC: GFI.VBS.Test
FOUND
  Sat Jul 21 17:09:12 2007 -> /var/spool/clamsmtp/clamsmtpd.6usOiY: GFI.VBS.Test
FOUND
  Sat Jul 21 17:09:13 2007 -> /var/spool/clamsmtp/clamsmtpd.y4LUia: GFI.VBS.Test
FOUND
  Sat Jul 21 17:09:14 2007 -> /var/spool/clamsmtp/clamsmtpd.moqPkB:
Exploit.ObjCodebase.Calc FOUND
  Sat Jul 21 17:09:15 2007 -> /var/spool/clamsmtp/clamsmtpd.Bu7Se6: Eicar-Test-
Signature FOUND
  Sat Jul 21 17:09:19 2007 -> /var/spool/clamsmtp/clamsmtpd.74zJ8M: Eicar-Test-
Signature FOUND
  Sat Jul 21 17:09:21 2007 -> /var/spool/clamsmtp/clamsmtpd.7r6VpQ: GFI.VBS.Test
FOUND
  Sat Jul 21 17:09:22 2007 -> /var/spool/clamsmtp/clamsmtpd.fZcQDj: GFI.VBS.Test
FOUND
  Sat Jul 21 17:09:23 2007 -> /var/spool/clamsmtp/clamsmtpd.znXLOO:
Exploit.ObjCodebase.Calc FOUND
  Sat Jul 21 17:09:23 2007 -> /var/spool/clamsmtp/clamsmtpd.YXU0Zj: GFI.VBS.Test
FOUND
```

Vuol dire che il motore antivirus di ClamAV è in grado di controllare le email in ingresso.

Non resta adesso che accertarsi che l'antivirus ClamAV sia in grado di aggiornare sia le impronte antivirus, sia il motore di scansione, sia se stesso. Andiamo quindi a controllare i file di log del programma Freshclam:

```
less /var/log/clamav/freshclam.log
```

se compaiono dei messaggi del tipo:

```
Received signal: wake up
ClamAV update process started at Sat Jul 21 16:20:40 2007
WARNING: Your ClamAV installation is OUTDATED!
WARNING: Local version: 0.90.1 Recommended version: 0.91.1
DON'T PANIC! Read http://www.clamav.net/support/faq
main.inc is up to date (version: 44, sigs: 133163, f-level: 20, builder: sven)
daily.cvd is up to date (version: 3715, sigs: 6395, f-level: 16, builder: ccordes)
```

Vuol dire che i file di ClamAV sono aggiornati ma c'è una nuova versione di ClamAV, precisamente la versione 0.91.1 che sostituisce la versione 0.90.1. Per passare alla nuova versione di ClamAV bisogna eseguire il comando:

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

Si osservi che di solito la distribuzione Debian impiega un po' di tempo a rendere disponibili questo tipo di aggiornamenti, di solito ci vuole qualche settimana, dal momento dell'uscita della nuova versione *stable release* (*versione stabile*) sul sito dell'antivirus ClamAV, prima che questa venga resa disponibile nel repository Debian Volatile.

Abilitazione dei controlli Antispam dell'antivirus ClamAV

Il programma antivirus ClamAV è anche in grado di valutare i seguenti messaggi di SPAM:

- **PDF Message SPAM**, ovvero messagi email con in allegato documenti in formato PDF che contengono testo classificabile come SPAM;
- **XLS Message SPAM**, ovvero messagi email con in allegato documenti in formato XLS che contengono testo classificabile come SPAM;
- **Image Message SPAM**, ovvero messagi email con in allegato immagini che contengono testo classificabile come SPAM;

Per individurare questo tipo di messaggi di SPAM bisogna scaricare un opportuno script bash che si trova sul sito http://sanesecurity.co.uk/ Per poter eseguire questo script bisogna che vengano installati i seguenti programmi:

```
apt-get install gzip curl rsync
```

Scarichiamo ed impostiamo lo script da eseguire come segue:

```
cd /usr/bin
wget http://sanesecurity.co.uk/clamav/scamp.txt
mv scamp.txt UpdateSaneSecurity
chmod +x UpdateSaneSecurity
```

Editiamo lo script `/usr/bin/UpdateSaneSecurity` per poter impostare la variabile **SIG_DB** in cui viene specificato dove si trovano i database dell'antivirus ClamAV:

```
vi UpdateSaneSecurity
```

togliamo il segno di commento dalla riga:

```
SIG_DB="/var/lib/clamav"
```

Salviamo le modifiche. Se lo si desidera si può inserire il comando `date` di modo da visualizzare la data e l'ora in cui viene eseguito lo script:

```
...
# For tcsh or csh shells you may need to use this instead. Comment out above
# and uncomment this. Modify as required.

# set PATH = (/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin)

# Show date and time execution script
date

## ********************************************************************** ##
```

```
# Uncomment this on to enable logging. It is off by default.
...
```

Salviamo dinuovo le modifiche.

A questo punto non resta che testare il corretto funzionamento dello script /usr/bin/UpdateSaneSecurity. Pertanto eseguiamo il comando:

```
./UpdateSaneSecurity
```

L'esecuzione dello script potrebbe richiedere diversi minuti. Un possibile risultato dello script potrebbe essere:

```
Logging has been disabled
Using Rsync to download the MSRBL files.
Using curl to download Sanesecurity, Securiteinfo and Malware files

No update available MSRBL-SPAM.ndb


********** WARNING **********
Unable to install: phish.ndb
Clamscan exited with error code 50
Try downloading and installing the file again.


No update available scam.ndb
Installed:    ........ honeynet.hdb
No update available MSRBL-Images.hdb
Installed:    ........ securiteinfo.hdb
Installed:    ........ vx.hdb
Installed:    ........ mbl.db

Database Reloaded

Files saved to: /var/lib/clamav

Installed:   4
Not Updated: 3
Failed:      1
```

Eseguire poi un test del motore antivirus ClamAV:

```
cd /usr/share/clamav-testfiles
clamscan -i -r
clamdscan
```

Una volta eseguito lo script e verificato che l'antivirus ClamAV funziona correttamente, possiamo controllare se l'antivirus ClamAV è effettivamente in grado di controllare eventuali email con in allegato dei documenti di SPAM. Per poter svolgere questa verifica, bisogna prima creare due opportuni file da mettere in allegato alle email di prova. I nomi dei due file da creare sono (per comodità gli autori dell'articolo hanno messo a disposizione questi documenti HTML all'interno del file ClamAV_HomeWorks_Test_SPAM.zip):

- *phish_sigtest.html*
- *scam_sigtest.html*

Il file *phish_sigtest.html* deve contenere il seguente testo:

```
  <html>
    <SaneSecurity>dr1aYlariaDiax!_!
leBr_aWOEWIehi5s1oapro8yL#chlAC7iUtOezoUqluviUd</SaneSecurity>
  </html>
```

mentre il file *scam_sigtest.html* deve contenere il testo seguente:

```
  <html>
    <SaneSecurity>xr1aYlariaDiax!_!
leBr_aWOEWIehi5s1oapro8yL#chlAC7iUtOezoUqluviUx</SaneSecurity>
  </html>
```

Una volta creati i due file, si deve procedere a creare due messaggi di posta elettronica, ciascun messaggio deve avere in allegato una copia di uno dei file *phish_sigtest.html* e *scam_sigtest.html* Questi due messaggi email dovranno venire poi inviati ad una mailbox del server di posta elettronica **mail.homeworks.it**; a puro titolo di esempio, si potrebbe utilizzare la mailbox **test@homeworks.it** Una volta inviati i messaggi email, si devono controllare i file di log di Postfix per accertarsi che i messaggi siano stati effettivamente intercettati dall'antivirus ClamAV ed identificati come SPAM. Pertanto eseguiamo il comando:

```
tail -n 70 /var/log/mail.log | grep clamsmtpd
```

se compaiono dei messaggi simili a quelli riportati di seguito:

```
  Sep  1 18:53:51 mail clamsmtpd: 10000B: accepted connection from: 127.0.0.1
  Sep  1 18:53:51 mail clamsmtpd: 10000B: from=atani@homeworks.it,
to=test@homeworks.it, status=VIRUS:Html.Phishing.Sanesecurity.TestSig
  Sep  1 18:54:47 mail clamsmtpd: 10000C: accepted connection from: 127.0.0.1
  Sep  1 18:54:47 mail clamsmtpd: 10000C: from=atani@homeworks.it,
to=test@homeworks.it, status=VIRUS:Html.Phishing.Sanesecurity.TestSig
  Sep  1 18:59:43 mail clamsmtpd: 10000D: accepted connection from: 127.0.0.1
  Sep  1 18:59:43 mail clamsmtpd: 10000D: from=atani@homeworks.it,
to=test@homeworks.it, status=VIRUS:Html.Phishing.Sanesecurity.TestSig
  Sep  1 19:00:27 mail clamsmtpd: 10000E: accepted connection from: 127.0.0.1
  Sep  1 19:00:27 mail clamsmtpd: 10000E: from=atani@homeworks.it,
to=test@homeworks.it, status=VIRUS:Html.Scam.Sanesecurity.TestSig
```

vuol dire che tutto è andato bene. In base all'esperienza degli autori di questo articolo, questo tipo di controlli sono abbastanza efficaci e di solito l'antivirus ClamAV è in grado di individuare la maggior parte dei messaggi email che hanno in allegato o documenti HTML fraudolenti o documenti PDF contenenti testo classificabile come SPAM. Osservando i file di log di Postfix potrebbero comparire di tanto in tanto, messaggi come quello che riportiamo di seguito:

```
tail -n 70 /var/log/mail.log | grep clamsmtpd
```

```
  Sep  3 22:20:51 mail clamsmtpd: 100001: accepted connection from: 127.0.0.1
  Sep  3 22:20:51 mail clamsmtpd: 100001: from=atani@homeworks.it,
to=test@homeworks.it, status=CLEAN
  Sep  3 22:33:03 mail clamsmtpd: 100002: accepted connection from: 127.0.0.1
  Sep  3 22:33:04 mail clamsmtpd: 100002: from=atani@homeworks.it,
to=test@homeworks.it, status=VIRUS:Email.Stk.Gen606.Sanesecurity.07080101.pdf
```

Questo significa che l'antivirus ClamAV ha individuato un email *pulita* (**status=CLEAN**) ed un email *infetta* (**status=VIRUS:Email.Stk.Gen606.Sanesecurity.07080101.pdf**).

A questo punto si può procedere alla pianficazione dell'esecuzione dello script */usr/bin/UpdateSaneSecurity*. Scheduliamo lo script per essere eseguito ogni quattro ore (per evitare di appensantire il server da cui vengono scaricati gli aggiornamenti, si sono impostati i minuti di esecuzione

in modo insuale):

```
crontab -e
37 */4 * * * /usr/bin/UpdateSaneSecurity > /var/log/UpdateSaneSecurity
```

Controlliamo che la pianificazione dell'esecuzione dello script `/usr/bin/UpdateSaneSecurity` sia attiva:

```
crontab -l
```

se compare un risultato simile al seguente:

```
# m h  dom mon dow   command
# m => minute (0->59)
# h => hour (0->23)
# dom => day of month
# mon => month (1->12)
# dow => day of week (0 = Sunday)
37 */4 * * * /usr/bin/UpdateSaneSecurity > /var/log/UpdateSaneSecurity
```

vuol dire che tutto è stato impostate correttamente. A regime, si potrà verificare il corretto funzionamento dell script `/usr/bin/UpdateSaneSecurity`, andando a controllare il file di log `/var/log/UpdateSaneSecurity`:

```
cat /var/log/UpdateSaneSecurity
```

DSPAM

Lo SPAM è una delle maggiori piaghe che affligono sia gli amministratori di sistema, sia i dipendenti di un azienda. Purtroppo l'Italia è tra le maggiori nazioni colpite dalla piaga dello SPAM (stando ad un rapporto della McAfee, il nostro paese occupa il terzo posto in questa abominevole classifica). In media, sette messaggi di posta elettronica su dieci sono SPAM, questo comporta da un lato un sovraccarico indesiderato sui server di posta elettronica, dall'altro l'impossibilità di fruire in modo gradevole e profittevole del servizio posta elettronica da parte di un dipendente di una società.

L'unico modo per risolvere la piaga dello SPAM, è quello di dotare l'azienda di un filtro AntiSPAM e di invitare i dipendenti ad avere un comportamento più accorto nei confronti di Internet. Per essere vittime dello SPAM, infatti, non è sufficiente avere un indirizzo email pubblico, ovvero disponibile su un sito web, come potrebbe essere quello aziendale, ma bisogna o fare un uso improprio dell'indirizzo email aziendale, oppure essere vittima di opportuni malware denominati *Mass Mailer*. Per avere un'idea di quali potrebbero essere i comportamenti innoportuni che un dipendente dovrebbe evitare, riportiamo alcune citazioni estratte dal blog delle persone che hanno svolto, per conto dell'Italia, l'esperimento della MacAfee sullo SPAM:

> *" Passando alla navigazione sul Web, ho passato in rassegna i siti che ci sono stati indicati a proposito di presunti regali. Dei quasi 30 indirizzi segnalati, una buona parte non erano più attivi, indice che in effetti si tratta di atività poco affidabili. In quelli ancora attivi, non ho esitato a inserire i miei dati per ricevere una serie di importanti premi che mi sono guadagnato: un notebook, un iPod, un telefono cellulare, due console per videogame e altro ancora che non ricordo."* [**Giuseppe 2**]
>
> *" Ho iniziato inoltre una seconda attività, quella di rimuovere le sottoscrizioni, con l'obiettivo opposto, di confermare la presenza concreta della mia e-mail."* [**Giuseppe 2**]
>
> *" Puntavo anche a un'altra forma di spam molto diffusa, che sconfina nel Phishing: il furto di identità di eBay. Proprio mentre scrivevo però, questa è arrivata e non ho resistito a fare*

quello che in situazioni abituali non avrei mai osato: seguire il link." [**Giuseppe 2**]

" L'impressione e' che la maggior parte dei siti italiani che ho visitato per una ragione o per l'altra sembrano essere "puliti" dallo spam." [**Ingrid**]

" Oggi ho tentato un'altra interazione con lo spam provando a disiscrivermi da una mailing - list. La risposta è stata che ci vorranno minimo 10 gg per cancellarmi.....! mentre ne era bastato 1 solo per ricevere quotidianamente un sacco di spam!!!" [**Ingrid**]

Ciò che un dipendente aziendale **dovrebbe evitare di fare é**:

- evitare di rendere disponibile ad un *social newtork* (come Facebook o MySpace) il proprio indirizzo email aziendale;
- non utilizzare l'indirizzo email aziendale per iscriversi o partecipare alle comunità virtuali;
- evitare di lasciare incautamente il proprio indirizzo email aziendale in siti web poco attinenti con l'attività aziendale (vedi siti pornografici, siti di viaggi, siti per l'acquisto o la vendita di prodotti ...);

Ciò che un buon amministratore di sistemi invece **dovrebbe fare** per ridurre il rischio di far finire la propria azienda tra i bersagli degli *SPAMers* (ovvero quelle persone che inviano grosse quantità di messaggi di SPAM) è:

- evitare di fornire privilegi amministrativi ai vari dipendenti aziendali sulle loro postazioni di lavoro;
- dotare le postazioni Windows aziendali di un buon programma antivirus ed antispyware;
- assicurarsi che il programma antivirus ed antispywere delle varie postazioni Windows si aggiorni regolarmente;
- dotare la propria azienda di un buon sistema firewall perimetrale opportunamente configurato;
- chiudere in modo selettivo la porta TCP 25 sul firewall aziendale (in altri termini, dalle postazioni di lavoro dei dipendenti non dovrebbe essere possibile inviare email sfruttando server SMTP *esterni* alla rete aziendale);
- dotare l'azienda di una soluzione per il controllo della navigazione Internet da parte dei dipendenti aziendali;
- installare l'ultima versione diponibile di Internet Explorer;
- aggiornare regolarmente le postazioni di lavoro con le ultime fix di sicurezza.

Si ricordi che una volta che gli indirizzi email di un azienda sono rientrati tra i bersagli degli SPAMers, non è più possibile uscierne, se non cambiando dominio di posta elettronica! Pertanto, conviene svolgere le attività indicate *prima* che il problema dello SPAM si verifichi e non dopo che si è verificato, perchè ormai sarebbe troppo tardi!

Introduzione a DSPAM

Sia nel mondo Open Source, sia nel mondo commerciale, ci sono molti prodotti per cercare di arginare la piaga dello SPAM. Sebbene la soluzione migliore sia quella di dotare la propria azienda di un dispositivo dedicato a contrastare l'arrivo dei messaggi di SPAM, i responsabili IT della Home Works S.p.A. hanno deciso di adottare il programma DSPAM come sistema per cercare di individuare i messaggi di SPAM in arrivo. DSPAM è un flitro AntiSPAM che si basa sull'analisi statistiche dei testi dei messaggi di posta elettronica. Scritto qualche anno fa da Jonathan A. Zdziarski, è unanimemente riconosciuto come uno dei migliori filtri statistici per combattere lo SPAM. I suoi maggiori punti di forza sono la sua parsimonia nell'utilizzo delle risorse fisiche (hardware) del sistema e la sua efficacia nel combattere lo SPAM. In questa e nelle prossime sezioni, verrà spiegato come integrare DSPAM con i programmi Postfix, ClamAV e SquirrelMail.

Al momento il flusso delle email, sia in ingresso (provenienti da Internet), sia in uscita (provenienti dalle postazioni aziendali verso Internet), è il seguente (*NomeDemone*:*PortaInAscolto*):

```
Internet -> Postfix:25 -> ClamSMTP:10026 -> Postfix:10025 -> Mailbox
```

per le email in ingresso; per per le email in uscita (*NomeDemone*:*PortaInAscolto*):

```
Mail Client -> Postfix:25 -> ClamSMTP:10026 -> Postfix:10025 -> Internet
```

Per poter controllare l'arrivo di eventuali messaggi di SPAM, i responsabili IT della Home Worsk S.p.A, hanno deciso di modificare i flussi di email appena riportati come segue:

```
Internet -> Postfix:25 -> Clamsmtp:10026 -> Postfix:10025 -> DSPAM -> Postfix:10024 -
> Mailbox
```

```
Mail Client -> Postfix:25 -> Clamsmtp:10026 -> Postfix:10025 -> DSPAM ->
Postfix:10024 -> Internet
```

In questo modo, verranno svolti, nell'ordine, i seguenti controlli:

1. verrà controllato che l'email non abbia virus o simili (ClamAV);
2. verrà conttrollato che l'email non abbia in allegato messaggi di SPAM (ClamAV);
3. verrà controllato che l'email non sia SPAM (DSPAM).

Questa scelta, è dettata dal fatto che in Internet circolano molte più email di SPAM che non email con virus. In questo modo, DSPAM eviterà di controllare delle email infette da virus o simili.

Il programma DSPAM fa uso, per questioni di efficienza, di MySQL come motore di database. Pertanto, prima di procedere con l'installazione del programma DSPAM, procediamo con l'installazione del motore di database MySQL.

Installazione e configurazione di MySQL e PHPMyAdmin

Il motore per database MySQL, è uno dei motori più diffusi all'interno della comunità Open Source. Grazie all'ausilio del programma PHPMyAdmin, risulta possibile amministrare (con una comoda interfaccia web) i database di MySQL in modo semplice e agevole.

Per installare MySQL e il programma PHPMyAdmin si può procedere come riportato di seguito:

```
apt-get install mysql-client mysql-server phpmyadmin php5-mysql libpam-mysql
```

Al termine della procedura d'installazione, impostiamo la password dell'utente **root** che amministrerà il programma MySQL (per semplicità, imporremo come password la parla *mysqladmin*):

```
mysqladmin -u root password mysqladmin
```

Per comodità semplifichiamo la sintassi del file `/etc/mysql/my.cnf`. Per prima cosa facciamo una copia del file `/etc/mysql/my.cnf`:

```
cp /etc/mysql/my.cnf /etc/mysql/my.cnf.originale
```

poi creiamo il *master*, ovvero il modello base, per le modifiche:

```
cp /etc/mysql/my.cnf /etc/mysql/my.master.cnf
```

riscriviamo il file `/etc/mysql/my.cnf` (il comando `show` è un *alias* definito all'interno della sezione

Configurarazione di base del sistema operativo):

```
show /etc/mysql/my.master.cnf > /etc/mysql/my.cnf
```

A questo punto possiamo procedere con la configurazione di Apache per consentire l'accesso al programma PHPMyAdmin. Dal momento che le porte **80** (protocollo HTTP) e **443** (protocollo HTTPS) sono già utilizzate dalla SquirrelMail, configureremo il sito PHPMyAdmin di modo che stia in ascolto sulle porte **20080** (protocollo HTTP) e **20443** (protocollo HTTPS). Per far ciò, editiamo il file di configurazione */etc/phpmyadmin/apache.conf*:

```
cp /etc/phpmyadmin/apache.conf /etc/phpmyadmin/apache.conf.originale
vi /etc/phpmyadmin/apache.conf
```

introduciamo le seguenti righe all'interno del file */etc/phpmyadmin/apache.conf*:

```
Alias phpmyadmin /var/www/phpmyadmin/

# Enable access to phpmyadmin fron Internet
# User who prefer to a simple URL like http://mail.example.com:20080
# will be redirected to URL like https://mail.example.com:20443
<VirtualHost 192.168.1.8:20080>
        DocumentRoot /var/www/phpmyadmin/
        ServerAdmin  webmaster@homeworks.it
        ServerName mail.homeworks.it
        RewriteEngine   on
        RewriteCond     %{SERVER_PORT} ^20080$
        RewriteRule     ^(.*)$ https://%{SERVER_NAME}:20443$1 [L,R]
        RewriteLog      "/var/log/apache2/rewrite.log"
        RewriteLogLevel 2
</VirtualHost>

# Secure access to phpmyadmin https://mail.example.com:20443
<VirtualHost 192.168.1.8:20443>
        DocumentRoot  /var/www/phpmyadmin/
        ServerAdmin  webmaster@homeworks.it
        ServerName mail.homeworks.it
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/mail_public_cert.pem
        SSLCertificateKeyFile /etc/apache2/ssl/mail_private_key.pempem
</VirtualHost>
```

Creiamo un link simbolico all'interno della cartella */etc/apache2/conf.d/*

```
ln -s /etc/apache2/conf.d/phpmysqladmin.conf /etc/phpmyadmin/apache.conf
```

Modifichiamo il file */etc/apache2/ports.conf*:

```
vi /etc/apache2/ports.conf
```

aggiungendo le seguenti porte:

```
Listen 20080
Listen 20443
```

dopo la modifica il file */etc/apache2/ports.conf* dovrebbe apparire come segue:

```
cat /etc/apache2/ports.conf
```

```
Listen 80
Listen 443
```

```
Listen 20080
Listen 20443
```

Riavviamo il demone **Apache2**:

```
/etc/init.d/apache2 restart
```

A questo punto si può accedere al programma PHPMyAdmin digitando uno dei seguenti URL:

- **http://mail.homeworks.it:20080**
- **https://mail.homeworks.it:20443**

A seguito della configurazione adottata, se ci si collega al URL **http://mail.homeworks.it:20080**, si verrà reindirizzati al URL **https://mail.homeworks.it:20443**, per ovvi motivi di sicurezza.

L'utilizzo del programma PHPMyAdmin consente di vedere con semplicità il contenuto delle tabelle e dei database di DSPAM.

Installazione e configurazione del programma DSPAM

Una volta installati i programmi MySQL e PHPMyAdmin si può procedere con l'installazione del programma DSPAM:

```
apt-get install dspam dspam-doc libdspam7-drv-mysql
```

Dopo aver installato i pacchetti verranno poste le seguenti domande (impostiamo la password dell'utente amministratore del database di DSPAM uguale a *mysqladmin* e assegniamo la password *libdspam* all'utente **libdspam7-drv-mysql**):

```
Configure database for libdspam7-drv-mysql with dbconfig-common? <-- Yes
Password of your database's administrative user: <-- mysqladmin
MySQL application password for libdspam7-drv-mysql: <-- libdspam
Password confirmation: <-- libdspam
```

se compaino messaggi simili a questi:

```
  dbconfig-common: writing config to /etc/dbconfig-common/libdspam7-drv-mysql.conf
  Creating config file /etc/dbconfig-common/libdspam7-drv-mysql.conf with new version
  Creating config file /etc/dspam/dspam.d/mysql.conf with new version
  granting access to database libdspam7drvmysql for libdspam7-drv-my@localhost:
success.
  verifying access for libdspam7-drv-my@localhost: success.
  creating database libdspam7drvmysql: success.
  verifying database libdspam7drvmysql exists: success.
  populating database via sql...  done.
  dbconfig-common: flushing administrative password
```

vuol dire che la procedura d'installazione è andata a buon fine. In alternativa, si può procedere alla creazione del database di DSPAM in modo manuale (questo secondo metodo è da preferire al primo, ovvero quello automatico, in quanto consente di scegliere il nome del database da assegnare a DSPAM e quindi di rendere più facile la sua identificazione all'interno del programma di amministrazione PHPMyAdmin). Per comodità chiameremo il database di DSPAM col nome di *db_dspam*, all'utente amministratore del database di DSPAM assegneremo il nome di *db_dspam_admin* e password *dspamadmin*:

```
mysql -u root -p
mysql> create database db_dspam;
```

```
mysql> exit
mysql -u root -p db_dspam < mysql_objects-speed.sql
mysql -u root -p db_dspam < virtual_users.sql
mysql -u root -p
mysql> grant all on db_dspam.* to db_dspam_admin@localhost identified by 'dspamadmin';
mysql> exit
```

Se si decide di utilizzare il database creato manualmente, nel nostro caso il database **db_dspam**, bisognerà provvedere a cancellare il database **libdspam7drvmysql** o manualmente o tramite il programma PHPMyAdmin.

Il database di DSPAM è composto dalle seguenti tabelle:

- **dspam_preferences**: contiene le modifiche alle impostazioi predefinite degli utenti;
- **dspam_signature_data**: contiene le varie *firme* che DSPAM associa a ciascun messaggio di posta elettronica analizzato;
- **dspam_stats**: contiene i dati statistici relativi a ciascun utente;
- **dspam_token_data**: contiene i vari *token* di ciascun messaggio di posta elettronica analizzato;
- **dspam_virtual_uids**: contiene gli indirizzi email (*utenti*) che DSPAM ha analizzato o che analizzerà.

Creiamo infine le cartelle `opt-out` e `opt-in` che consentono di descriminare il comportamento di DSPAM:

```
md /var/spool/dspam/opt-out
md /var/spool/dspam/opt-in
chown dspam:dspam /var/spool/dspam/opt-out
chown dspam:dspam /var/spool/dspam/opt-in
```

Per rendere più leggibile il contenuto del file di configurazione di DSPAM, `/etc/dspam/dspam.conf`, creiamo un file *master* che conterrà tutte le modifiche al file di configurazione, dopo di che, provvederemo a riportare le modifiche effettuate al file *master* nel file di configurazione `/etc/dspam/dspam.conf`, pertanto:

```
cp /etc/dspam/dspam.conf /etc/dspam/dspam.conf.originale
cp /etc/dspam/dspam.conf /etc/dspam/dspam.master.conf
```

Impostazione del comportamento generale di DSPAM

DSPAM ha due modalità di funzionamento che ne caratterizzano il comportamento generale. Per specificare in quale modalità deve operare DSPAM, bisogna modificare il parametro **Opt**, più precisamente:

- **Opt out**: *tutte le email che passano attraverso DSPAM vengono analizzate*. Questo significa che DSPAM crea un account, nel suo database, per ogni destinatario di posta elettronica (corrispondente, nel *header* del messaggio, al campo **To**). In questa modalità, gli alias di un destinatario vengono considerati come tanti destinatari distinti e quindi verranno creati tanti account (in DSPAM) quanti sono gli alias del destinatario. Se si vuole che le email indirizzate ad un dato destinatario non vengano analizzate, bisogna configurare esplicitamente DSPAM di modo che escluda il tal indirizzo di posta elettronica dai suoi controlli. In questa modalità, possono venire controllati sia i messaggi in arrivo (provenienti da Internet), sia quelli in uscita (provenienti dal personale della Home Works S.p.A). Pertanto, se si controllano anche i messaggi in uscita, verranno creati tanti account in DSPAM quanti sono i vari destinatari dei messaggi in uscita. Questo comportamento può provocare dei problemi qualora si abilitassero le notifiche di DSPAM, in quanto persone esterne all'azienda Home Works, potrebbero ricevere le notifiche di DSPAM, mettendo in un certo imbarazzo la direzione della Home Works.
- **Opt in**: *nessuna email che passa attraverso DSPAM viene analizzata*, se si vuole che un dato indirizzo email venga analizzato, bisogna configurare DSPAM esplicitamente. In questo modo,

nel database di DSPAM vengono inserite solamente gli account di posta elettronica (corrispondenti, nel *header* del messaggio, al campo **To**) che si è deciso di analizzare.

Più precisamente, un indirizzo di posta elettronica è composto, per convenzione, da due parti, tutto ciò che precede il simbolo **@**, che per semplicità chiameremo *Nome_Mailbox* e tutto ciò che segue il simbolo **@**, che per semplicità chiameremo *Nome_Dominio_di_Posta_Elettronica*, ovvero: **<Nome_Mailbox>@<Nome_Dominio_di_Posta_Elettronica>**. Per esempio, nell'indirizzo email **atani@homeworks.it**, stando alla nostra convenzione avremo:

- **Nome_Mailbox**: atani
- **Nome_Dominio_di_Posta_Elettronica**: homeworks.it

Nella modalità **Opt out** se si vuole escludere un indirizzo di posta elettronica dall'essere analizzato da DSPAM, bisogna creare un file *.nodspam* nella cartella */var/spool/dspam/opt-out/<Nome_Dominio_di_Posta_Elettronica>/<Nome_Mailbox>.nodspam* Per cui se si desidera escludere dall'analisi di DSPAM l'indirizzo email **atani@homeworks.it** bisognerà creare la cartella */var/spool/dspam/opt-out/homeworks.it/atani.nodspam* ed il file */var/spool/dspam/opt-out/homeworks.it/atani.nodspam/.nodspam*, assegnare poi sia al file, sia alla cartella il proprietario e il gruppo `dspam` (il comando `ll` è un *alias* definito all'intero della sezione Configurarazione di base del sistema operativo):

```
md /var/spool/dspam/opt-out/homeworks.it/atani.nodspam
touch /var/spool/dspam/opt-out/homeworks.it/atani.nodspam/.nodspam
chwon -R dspam:dspam /var/spool/dspam/opt-out/homeworks.it/atani.nodspam
ll /var/spool/dspam/opt-out/homeworks.it
```

```
drwxr-xr-x 3 dspam dspam 4096 2007-11-02 00:23 homeworks.it
drwxr-xr-x 2 dspam dspam 4096 2007-11-02 00:20 homeworks.it/atani.nodspam
```

Dal momento della creazione del file */var/spool/dspam/opt-out/homeworks.it/atani.nodspam/.nodspam*, DSPAM non analizzerà più le email indirizzate ad **atani@homeworks.it**. Ciò non di meno, le email che provengono dall'indirizzo email **atani@homeworks.it** continueranno ad essere analizzate da DSPAM, a meno che non vengano inoltrare ad un destinatario che è stato escluso dalle analisi di DSPAM.

Analogamente, ma in modo duale, se viene utilizzata la modalità **Opt in**, solamente gli account che vengono abilitati in DSPAM per essere analizzati, verranno effettivamente analizzati, altrimenti non saranno elaborati da DSPAM. Per istruire DSPAM ad analizzare un indirizzo email si deve procedere in modo simile a quello per escludere un indirizzo email nella modalità **Opt out**. Per far sì che DSPAM analizzi l'indirizzo email **<Nome_Mailbox>@<Nome_Dominio_di_Posta_Elettronica>** bisognerà:

1. creare la cartella */var/spool/dspam/opt-in/<Nome_Dominio_di_Posta_Elettronica>/<Nome_Mailbox>.dspam*:

```
md /var/spool/dspam/opt-in/<Nome_Dominio_di_Posta_Elettronica>/<Nome_Mailbox>.dspam
chown dspam:dspam /var/spool/dspam/opt-in/<Nome_Dominio_di_Posta_Elettronica>/<Nome_Mailbox>.dspam
```

   Ad esempio, se l'indirizzo da analizzare è **ipagliani@homeworks.it**, bisognerà creare la cartella: */var/spool/dspam/opt-in/homeworks.it/ipagliani.dspam*

```
md /var/spool/dspam/opt-in/homeworks.it/ipagliani.dspam
chown dspam:dspam /var/spool/dspam/opt-in/homeworks.it/ipagliani.dspam
```

2. una volta creata la cartella */var/spool/dspam/opt-in/<Nome_Dominio_di_Posta_Elettronica>/<Nome_Mailbox>.dspam*, creare il file */var/spool/dspam/opt-in/<Nome_Dominio_di_Posta_Elettronica>/<Nome_Mailbox>.dspam/.dspam*:

```
touch /var/spool/dspam/opt-
in/<Nome_Dominio_di_Posta_Elettronica>/<Nome_Mailbox>.dspam/.dspam
chown dspam:dspam /var/spool/dspam/opt-
in/<Nome_Dominio_di_Posta_Elettronica>/<Nome_Mailbox>/.dspam
```

facendo riferimento all'esempio precedente:

```
touch /var/spool/dspam/opt-in/homeworks.it/ipagliani.dspam/.dspam
chown dspam:dspam /var/spool/dspam/opt-in/homeworks.it/ipagliani.dspam/.dspam
```

Dal momento della creazione del file */var/spool/dspam/opt-in/<Nome_Dominio_di_Posta_Elettronica>/<Nome_Mailbox>.dspam/.dspam*, DSPAM inzierà ad analizzare tutte le email che verranno indirizzate all'indirizzo di posta elettronica **<Nome_Mailbox>@<Nome_Dominio_di_Posta_Elettronica>**; mentre tutte le email che hanno come mittente **<Nome_Mailbox>@<Nome_Dominio_di_Posta_Elettronica>** non verranno analizzate da DSPAM.

Considerazioni sulle modalità "Opt in" ed "Opt out" di DSPAM

La scelta fra la modalità **Opt in** ed **Opt out** ha diverse conseguenze operative a seconda di quale scelta viene effettuata. Tendenzialmente, se un server di posta elettronica è di uso aziendale, si vorrebbe evitare che le email non aziendali (cioè quelle email che non sono indirizzate ad un indirizzo di posta elettronica aziendale) vengano analizzate da DSPAM, soprattutto se le notifiche sono attive, in quanto ci potrebbe essere il rischio che ad alcune persone esterne all'azienda, possano arrivare parte delle notifiche di DSPAM, mettendo in tal modo in imbarazzo l'azienda stessa. Per cui, per un server di posta elettronica aziendale, la scelta **Opt in** è quella più opportuna.

> Si osservi che sebbene DSPAM possa non controllare alcune email in uscita, l'antivirus ClamAV continua lo stesso ad analizzare tutte le email in uscita.

Viceversa, se si vuole aumentare la sicurezza del server di posta elettronica, allora conviene che tutte le email che vi transitino attraverso siano analizzate da DSPAM, in questo modo, le persone che utilizzano il server di posta elettronica, hanno la garanzia che tutte le email che inviano o che ricevono saranno analizzate da DSPAM. Pertanto, i vari destinatari, siano esse persone dell'azienda o meno, avrebbero la garanzia che le email provenienti dal server di posta elettronica non dovrebbero mai essere messaggi di SPAM, in quanto analizzati dal programma DSPAM; in altri termini, tutte le persone che riceveranno messaggi email provenienti dal server di posta elettronica in questione, dovrebbero sentirsi più garantite, in quanto, potenzialmente, da questo server di posta elettronica non dovrebbe essere possibile inviare messaggi di SPAM. In questo caso la scelta **Opt out** è quella più opportuna.

Qualora si decida di adottare la scelta **Opt in**, bisogna seguire la seguente procedura operativa ogni qual volta si crea o si modifica una mailbox di posta elettronica:

- se si modifica una mailbox, bisgona modificare di conseguenza anche il contenuto della cartella */var/spool/dspam/opt-in/*
- se si crea una nuova mailbox, bisogna creare il corrispondente account anche nella cartella */var/spool/dspam/opt-in/*
- se si aggiunge o si modifica un alias di una mailbox, allora bisogna o creare o modificare l'apposita mailbox presente nella cartella */var/spool/dspam/opt-in/*

Ne consegue che dal punto di vista operativo, la scelta **Opt in** è sicuramente la più onerosa. Per cercare di ridurre il carico di lavoro di coloro che devono gestire il server di posta elettronica, conviene creare un apposito script in grado di automatizzare al massimo le operazioni di creazione e modifica delle mailbox.

> Per scelta del personale IT della Home Works S.p.A, DSPAM verrà configurato per funzionare in modalità **Opt in**. Pertanto d'ora in avanti daremo per scontato che DSPAM operi in modalità **Opt**

in.

Configurazione delle notifiche sullo stato dei controlli di DSPAM

DSPAM consente di inviare delle notifiche alle varie persone che lo utilizzano, per avvertirle delle seguenti situazioni:

- la prima volta che un persona accede ad una Mailbox monitoarata da DSPAM (file */etc/dspam/txt/firstrun.txt*);
- la prima volta che una persona riceve un messaggio email di SPAM (file */etc/dspam/txt/firstspam.txt*);
- quando la *quarantena* supera i 2MB di dimensione (nella configurazione adottata, questa situazione non si potrà mai verificare, in quanto la *quarantena* non viene utilizzata);

Queste notifiche possono essere un utile occasione per fornire ai dipendenti della Home Works, dei messaggi informativi sulla gestione dei messaggi di SPAM e su come si devono comportare, ad esempio, quando un messaggio email viene erroneamente classificato.

Per abilitare le notifiche da parte del programma DSPAM, bisogna accertarsi che la variabile `Notifications` sia impostata su `on`, ovvero, osservando il contenuto del file */etc/dspam/dspam.master.conf* deve risultare:

```
Notifications on
```

Una volta che le notifiche sono attive, si deve procedere a creare la cartella */etc/dspam/txt* ed i rispettivi messaggi da inviare alle persone:

```
md /etc/dspam/txt
touch /etc/dspam/txt/firstrun.txt
touch /etc/dspam/txt/firstspam.txt
touch /etc/dspam/txt/quarantinefull.txt
chmod 770 /etc/dspam/txt
chmod 640 /etc/dspam/txt/*
chown -R dspam:dspam txt
ln -s /etc/dspam/txt /var/spool/dspam/txt
ll /etc/dspam/txt
```

```
  -rw-r----- 1 dspam dspam 2257 2007-10-03 01:15 firstrun.txt
  -rw-r----- 1 dspam dspam 1315 2007-10-03 01:17 firstspam.txt
  -rw-r----- 1 dspam dspam 1283 2007-10-03 01:20 quarantinefull.txt
```

Modificare i file firstrun.txt e firstspam.txt di modo che siano coerenti con l'ambiente di lavoro. Esempi di file */firstrun.txt* e */firstspam.txt* potrebbero essere:

firstrun.txt:

```
  To: $u
  From: Technical Support
  Subject: Spam Filtering is Active - Filtro Antispam Attivo

  Dear Colleague,

  this email is to inform you that spam filtering has been activated on this account
and provide
  you with some basic instructions to assist in filtering spam from your email. The
filtering software
  we are using is called DSPAM and is capable of dynamically learning your specific
email behavior.
  We have started you off with a pre-configured spam dictionary which will help
```

filter a limited amount
of spam immediately for you. As you continue to receive email, your specific email patterns will be learned
by the spam software, which will result in increasing accuracy in catching spam. For this reason, it is
important that you forward any spam you receive for this email account into the filtering software.
By forwarding your spam, the software is capable of learning from its mistakes and will improve itself
to do better next time.

To forward a spam into the system, please use the link 'Spam' in the Home Works webmail
(https://mail.homeworks.it), to send the spam to spam@homeworks.it It is not necessary to provide an
explanation of the message, as it will not be opened by a human, but processed by the software.

For your convenience, all messages classified as spam will have the abbreviation [SPAM] in the
subject and will be stored in the SPAM folder of your email program.

Thank you, and please feel free to contact us if you have any questions.

Technical Support
postmaster@homeworks.com

Caro Collega,

questo messaggio è per informarti che il filtraggio dello spam è stato attivato su questa casella
e-mail e per fornirti alcuni elementi di base per aiutarti nel filtraggio dello spam della tua e-mail.
Il software di filtraggio che stiamo utilizzando è chiamato DSPAM, è dinamico ed è in grado di imparare
il comportamento specifico della la tua e-mail. Ti abbiamo fornito un dizionario pre-configurato dello
spam che contribuirà a filtrati una quantità di spam immediatamente per te. Il programma DSPAM, è in grado
d'imparare a riconoscere lo spam dalle tue e-mail. Per questo motivo, è importante che si inoltri ogni spam
che ricevi che non sia stato riconosciuto dal software di filtraggio. Con la tua trasmissione dello spam,
il software è in grado di imparare dai suoi errori e di migliorare se stesso per fare meglio la prossima volta.

Per inoltrare un spam nel sistema, puoi utilizzare il link 'Spam' nella webmail della Home Works
(https://mail.homeworks.it), per inviare spam a spam@homeworks.it Non è necessario fornire una spiegazione
del messaggio, in quanto non sarà aperto da qualcuno, ma trasferito direttamente al software.

Per tua comodità, tutti i messaggi classificati come spam avranno la sigla [SPAM] nell'oggetto del
messaggio e verranno archiviati nella cartella SPAM del tuo programma di posta elettronica.

Ti ringrazio, e non esitate a contattarci se hai domande.

Supporto tecnico
postmaster@homeworks.com

firstspam.txt:

```
To: $u
```

```
  From: Technical Support
  Subject: Your first spam has been caught - Il primo messaggio di spam è stato
catturato

  Dear Colleague,

  This email is to inform you that our spam filtering software, DSPAM, has caught its
first spam
  for your account.  This message will only be sent once.

  For your convenience, all messages classified as spam will have the abbreviation
[SPAM] in the
  subject and will be stored in the SPAM folder of your email program.

  Thank you, and please feel free to contact us if you have any questions.

  Technical Support
  postmaster@homeworks.it


  Caro Collega,

  questa e-mail è per informarti che il nostro programma di filtraggio dello spam,
DSPAM, ha individuato
  il primo messaggio di spam indirizzato alla tua casella e-mail. Questo messaggio ti
verrà inviato
  solamente una volta.

  Per tua comodità, tutti i messaggi classificati come spam avranno la sigla [SPAM]
nell'oggetto del
  messaggio e verranno archiviati nella cartella SPAM del tuo programma di posta
elettronica.

  Ti ringrazio, e non esitate a contattarci se hai domande.

  Supporto tecnico
  postmaster@homeworks.com
```

Configurazione dell'accesso a MySQL da parte di DSPAM

DSPAM, come abbiamo visto, utilizza un database su MySQL per archiviare le informazioni fondamentali per il suo corretto funzionamento. Per specificare a DSPAM come accedere al suo database in MySQL, bisogna modificare in modo opportuno il file */etc/dspam/dspam.d/mysql.conf*:

```
mv /etc/dspam/dspam.d/mysql.conf /etc/dspam/mysql.conf.originale
cp /etc/dspam/mysql.conf.originale /etc/dspam/mysql.master.conf
vi /etc/dspam/mysql.master.conf
```

introduciamo le seguenti modifiche (per scelta degli autori di questo articolo, d'ora in avanti faremo riferimento al database di DSPAM creato manualmente):

```
  MySQLServer       /var/run/mysqld/mysqld.sock
  MySQLUser         db_dspam_admin
  MySQLPass         dspamadmin
  MySQLDb           db_dspam
  MySQLConnectionCache    10
  MySQLUIDInSignature    on
```

salviamo la nuova configurazione sul file */etc/dspam/dspam.d/mysql.conf*:

```
show /etc/dspam/mysql.master.conf > /etc/dspam/dspam.d/mysql.conf
chown dspam /etc/dspam/dspam.d/mysql.conf
```

Configurazione di base di DSPAM

Una volta stabilito come si deve comportare DSPAM, si può procedere alla sua configurazione di base. Per scelta del personale IT della Home Works S.p.A, DSPAM dovrà avere il seguente comportamento generale:

- il funzionamento di base di DSPAM dovrà essere in modalità **Opt In**;
- le notifiche di DSPAM dovranno essere abilitate;
- i messaggi classificati come SPAM dovranno avere la sigla **[SPAM]** nell'oggetto del messaggio;
- i messaggi classificati come SPAM dovranno venire inoltrati comunque al destinatario;
- i messaggi classificati come SPAM dovranno venire archiviati in una cartella denominata **SPAM** (per sapere come creare la cartella SPAM, si può consultare il paragrafo Installazione e configurazione di Courier);
- le *firme di DSPAM* dovranno venire inserite nel *header* dei messaggi di posta elettronica (per maggiori informazioni su cosa s'intenda per *firme di DSPAM* si consulti il paragrafo Come gestire i messaggi erroneamente classificati);
- dovrà essere possibile cambiare il valore della variabile d'ambiente di DSPAM denominata **localStore**;
- la modalità di apprendimento predefinita di DSPAM sarà la **TUM** (*Train-until-Mature*);

Modifichiamo il file di configurazione di DSPAM `/etc/dspam/dspam.master.conf` di modo che le richieste appena citate, relative alla configurazione di DSPAM, siano soddisfatte:

```
vi /etc/dspam/dspam.master.conf
```

introduciamo le seguenti personalizzazioni al file /etc/dspam/dspam.master.conf (i commenti inseriti a lato, servono solamente per spiegare meglio il significato di alcune variabili o parti del file di configurazione e non vanno riportate all'interno del file di configurazione stesso):

```
  Home /var/spool/dspam
  StorageDriver /usr/lib/dspam/libmysql_drv.so
  TrustedDeliveryAgent "/usr/bin/procmail"
  DeliveryHost        127.0.0.1
  DeliveryPort        10024
  DeliveryIdent       localhost
  DeliveryProto       SMTP
  OnFail error
  Trust root
  Trust dspam
  Trust mail
  Trust mailnull
  Trust smmsp
  Trust daemon
  Trust nobody <-- Questo utente va messo in Trust solamente se si installa il
pacchetto dspam-webfrontend
  TrainingMode tum
  TestConditionalTraining on
  Feature noise
  Feature chained
  Feature whitelist
  Algorithm graham burton
  PValue graham
  Preference "spamAction=tag"
  Preference "signatureLocation=headers" <-- "message" qualora si volesse mettere la
firma di DSPAM in fondo ai messaggi email
  Preference "showFactors=off" <-- Durante i test di funzionamento di DSPAM, conviene
impostarla nel seguente modo: showFactors=on
  Preference "spamSubject=[SPAM]"
  Preference "enableWhitelist=on"
  AllowOverride trainingMode
  AllowOverride spamAction spamSubject
```

```
  AllowOverride statisticalSedation
  AllowOverride enableBNR
  AllowOverride enableWhitelist
  AllowOverride signatureLocation
  AllowOverride showFactors
  AllowOverride optIn optOut
  AllowOverride whitelistThreshold
  AllowOverride localStore
  HashRecMax              98317
  HashAutoExtend          on
  HashMaxExtents          0
  HashExtentSize          49157
  HashMaxSeek             100
  HashConnectionCache     10
  Notifications   on
  PurgeSignatures 14          # Stale signatures
  PurgeNeutral    90          # Tokens with neutralish probabilities
  PurgeUnused     90          # Unused tokens
  PurgeHapaxes    30          # Tokens with less than 5 hits (hapaxes)
  PurgeHits1S     15          # Tokens with only 1 spam hit
  PurgeHits1I     15          # Tokens with only 1 innocent hit
  LocalMX 127.0.0.1
  SystemLog off <-- Se non si utilizza la componente Web di DSPAM possono venire
disabilitati
  UserLog   off <-- Se non si utilizza la componente Web di DSPAM possono venire
disabilitati
  Opt in <-- Solamente le email in ingresso verranno analizzate da DSPAM
  TrackSources spam nonspam
  ParseToHeaders on
  ChangeModeOnParse on
  ChangeUserOnParse off
  MaxMessageSize 12582912
  ServerPID             /var/run/dspam/dspam.pid
  ServerMode auto
  ServerPass.Relay1       "secret"
  ServerParameters        "--deliver=innocent"
  ServerIdent             "localhost.localdomain"
  ServerDomainSocketPath  "/var/spool/postfix/var/run/dspam.sock"
  ClientHost      /var/spool/postfix/var/run/dspam.sock
  ClientIdent     "secret@Relay1"
  ProcessorBias on
  Include /etc/dspam/dspam.d/ <-- Importante per gestire la connessione a MySQL
```

Una volta modificato il file *`/etc/dspam/dspam.conf.master`* riportiamo le modifiche sul file *`/etc/dspam/dspam.conf`* (il comando `show` è un *alias* definito all'intero della sezione Configurarazione di base del sistema operativo):

```
show /etc/dspam/dspam.master.conf > /etc/dspam/dspam.conf
/etc/inet.d/dspam restart
```

Creazione degli alias di DSPAM per la gestione dei messaggi

DSPAM, come tutti i filtri statistici, fonda le sue capacità predittive relative ai messaggi di SPAM sull'apprendimento, talvolta, però, capita di commettere qualche errore, per ovviare a questo, DSPAM mette a disposizione una procedura per rimediare a questi sbagli. La procedura consiste nell'inviare i messaggi erroneamente classificati come SPAM o come HAM (ovvero non SPAM), a degli opportuni indirizzi email, a **spam@homeworks.it** tutti i messaggi erroneamente classificati come HAM, a **notspam@homeworks.it** tutti i messaggi email erroneamente classificati come SPAM. Più precisamente:

- se un messaggio di SPAM non viene correttamente riconosciuto, lo si può inoltrare all'indirizzo email **spam@homeworks.it**, per fare in modo che in futuro DSPAM lo riconosca;
- se un messaggio valido viene erroneamente classificato come SPAM, lo si può inoltrare

all'indirizzo email **notspam@homeworks.it**, per fare in modo che DSPAM non commetta più lo stesso errore;

Le operazioni di inoltro dei messaggi erroneamente classificati, è di gran lunga più agevole se si utilizza l'accesso alla webmail, **http://mail.homeworks.it** (per maggiori informazioni su l'utilizzo della webmail per la gestione dei messaggi erroneamente classificati, si può consultare il paragrafo Configurazione ed installazione del plugin Spam Buttons).

Editiamo pertanto il file */etc/aliases*:

```
vi /etc/aliases
```

introduciamo le seguenti righe:

```
spam:"|/usr/bin/dspam  --client --user root --class=spam --source=error"
notspam:"|/usr/bin/dspam --client --user root --class=innocent --source=error"
```

salviamo le modifiche e ricarichiamo la mappa relativa agli alias:

```
cd /etc
postalias /etc/aliases
newaliases
postfix reload
```

Per poter abilitare l'invio agli indirizzi **spam@homeworks.it** e **notspam@homeworks.it** bisogna provvedere a creare questi due account all'interno della tabella: **dspam_virtual_uids** Per creare questi account si può utilizzare il programma **phpMyAdmin** disponibile al URL: **http://mail.homeworks.it:20080**:

- **Username**: spam@homeworks.it
- **UID**: 1

- **Username**: notspam@homeworks.it
- **UID**: 2

In alternativa si possono utilizzare i comandi di MySQL:

```
mysql -u root -p
mysql> use db_dspam;
mysql> insert into dspam_virtual_uids (uid, username) values ('1', 'spam@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('2', 'notspam@homeworks.it');
mysql> quit;
```

Creiamo le cartelle necessarie per la configurazione **Opt In**:

```
md /var/spool/dspam/opt-in/homeworks.it/spam.dspam
touch /var/spool/dspam/opt-in/homeworks.it/spam.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/spam.dspam
md /var/spool/dspam/opt-in/homeworks.it/notspam.dspam
touch /var/spool/dspam/opt-in/homeworks.it/notspam.dspam/.dspam
```

In questo modo DSPAM analizzerà le email indirizzata sia a **spam@homeworks.it**, sia a **notspam@homeworks.it**

Configurazione ed installazione del plugin Spam Buttons in SquirrelMail

Il plugin Spam Buttons consente di specificare se un messaggio email è da considerare *SPAM* o *HAM*

(ovvero un messaggio valido, non indesiderato). Questo plugin può essere configurato per convivere con DSPAM. Per installare questo plugin si possono eseguire i comandi seguenti, le operazioni riportate prevedono l'utilizzo dell'utente **root** (nel corso dell'esempio faremo riferimento alla versione *2.2-1.4.0* del plugin Spam Buttons):

```
cd /home/master/sm_new_plugins
wget http://www.squirrelmail.org/countdl.php?fileurl=http%3A%2F%2Fwww.squirrelmail.org
%2Fplugins%2Fspam_buttons-2.2-1.4.0.tar.gz
cp /home/master/sm_new_plugins/spam_buttons-2.2-1.4.0.tar.gz /usr/share/squirrelmail/plugins
cd /usr/share/squirrelmail/plugins
tar -zxvf /usr/share/squirrelmail/plugins/spam_buttons-2.2-1.4.0.tar.gz
```

Modifichiamo il file */usr/share/squirrelmail/plugins/spam_buttons/config.php* come segue:

```
vi /usr/share/squirrelmail/plugins/spam_buttons/config.php
```

introduciamo le seguenti modifiche:

```
  $spam_button_text = 'Spam';
  $not_spam_button_text = 'Not Spam';
  $is_spam_resend_destination = 'spam';
  $is_not_spam_resend_destination = 'notspam';
  $spam_report_email_method = 'attachment';
```

A questo punto si può abilitare il plugin Spam Buttons tra quelli abilitati della SquirrelMail.

Integrazione di DSPAM con Postfix

Siamo finalmente pronti per configurare Postfix di modo che inoltri i messaggi di posta elettronica a DSPAM per essere analizzati. Modifichiamo quindi il file */etc/postfix/master.cf* come segue:

```
vi /etc/postfix/master.cf
```

inseriamo le seguenti righe di testo (fare attenzione a non lasciare degli spazi sia intorno al simbolo di uguale, sia ad inizio riga):

```
  # DSPAM filter (used by SPAM filtering with content_filter)
  dspam     unix  -       -       -       -       2       lmtp
                        -o lmtp_data_done_timeout=1200s
  #
  #
  # For injecting mail back into postfix from the antivirus filter (clamsmtp) and
goes to spam checking (dspam)
  127.0.0.1:10025 inet  n         -       n       -       16      smtpd
                -o content_filter=dspam:unix:/var/run/dspam.sock
                -o
receive_override_options=no_unknown_recipient_checks,no_header_body_checks
                -o smtpd_helo_restrictions=
                -o smtpd_client_restrictions=
                -o smtpd_sender_restrictions=
                -o smtpd_recipient_restrictions=permit_mynetworks,reject
                -o mynetworks_style=host
                -o smtpd_authorized_xforward_hosts=127.0.0.0/8
  #
  # For injecting mail back into postfix from the spam filter (dspam)
  127.0.0.1:10024 inet    n       -       -       -       10       smtpd
                -o content_filter=
                -o
receive_override_options=no_unknown_recipient_checks,no_header_body_checks
                -o smtpd_helo_restrictions=
                -o smtpd_client_restrictions=
```

```
                -o smtpd_sender_restrictions=
                -o smtpd_recipient_restrictions=permit_mynetworks,reject
                -o mynetworks=127.0.0.0/8
                -o smtpd_authorized_xforward_hosts=127.0.0.0/8
  #
```

In questo modo, una volta che un messaggio email è stato controllato dal ClamAV (vedi sezione Installazione e configurazione dell'antivirus ClamAV), verrà poi controllato da DSPAM. Terminato il controllo da parte di DSPAM, il messaggio email verrà di nuovo inoltrato a Postfix. Riavviamo il demone di Postfix:

```
/etc/init.d/postfix restart
```

Creazione degli utenti di Postfix in DSPAM

A seguito della scelta di utilizzare la modalità **Opt In**, provvediamo ad impostare il controllo delle Mailbox sinora realizzate (oltre alle Mailbox già operative, creiamo anche l'utente **globaluser@homeworks.it** che ci tornerà utile quando realizzeremo la prima fase di apprendimento di DSPAM):

```
mysql -u root -p
mysql> use db_dspam;
mysql> insert into dspam_virtual_uids (uid, username) values ('3',
'globaluser@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('4',
'postmaster@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('5', 'nobody@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('6',
'hostmaster@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('7', 'usenet@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('8', 'news@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('9', 'webmaster@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('10', 'www@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('11', 'ftp@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('12', 'abuse@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('13', 'noc@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('14', 'security@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('15', 'clamav@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('16', 'mailer-
daemon@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('17', 'support@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('18', 'root@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('19', 'master@homeworks.it');
mysql> quit;
```

Creiamo le cartelle necessarie alla configurazione **Opt In**:

```
md /var/spool/dspam/opt-in/homeworks.it/globaluser.dspam
touch /var/spool/dspam/opt-in/homeworks.it/globaluser.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/globaluser.dspam
md /var/spool/dspam/opt-in/homeworks.it/mailer-daemon.dspam
touch /var/spool/dspam/opt-in/homeworks.it/mailer-daemon.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/mailer-daemon.dspam
md /var/spool/dspam/opt-in/homeworks.it/postmaster.dspam
touch /var/spool/dspam/opt-in/homeworks.it/postmaster.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/postmaster.dspam
md /var/spool/dspam/opt-in/homeworks.it/nobody.dspam
touch /var/spool/dspam/opt-in/homeworks.it/nobody.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/nobody.dspam
md /var/spool/dspam/opt-in/homeworks.it/hostmaster.dspam
touch /var/spool/dspam/opt-in/homeworks.it/hostmaster.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/hostmaster.dspam
md /var/spool/dspam/opt-in/homeworks.it/usenet.dspam
touch /var/spool/dspam/opt-in/homeworks.it/usenet.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/usenet.dspam
md /var/spool/dspam/opt-in/homeworks.it/news.dspam
```

```
touch /var/spool/dspam/opt-in/homeworks.it/news.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/news.dspam
md /var/spool/dspam/opt-in/homeworks.it/webmaster.dspam
touch /var/spool/dspam/opt-in/homeworks.it/webmaster.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/webmaster.dspam
md /var/spool/dspam/opt-in/homeworks.it/www.dspam
touch /var/spool/dspam/opt-in/homeworks.it/www.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/www.dspam
md /var/spool/dspam/opt-in/homeworks.it/www.dspam
touch /var/spool/dspam/opt-in/homeworks.it/www.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/www.dspam
md /var/spool/dspam/opt-in/homeworks.it/ftp.dspam
touch /var/spool/dspam/opt-in/homeworks.it/ftp.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/ftp.dspam
md /var/spool/dspam/opt-in/homeworks.it/abuse.dspam
touch /var/spool/dspam/opt-in/homeworks.it/abuse.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/abuse.dspam
md /var/spool/dspam/opt-in/homeworks.it/noc.dspam
touch /var/spool/dspam/opt-in/homeworks.it/noc.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/noc.dspam
md /var/spool/dspam/opt-in/homeworks.it/security.dspam
touch /var/spool/dspam/opt-in/homeworks.it/security.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/security.dspam
md /var/spool/dspam/opt-in/homeworks.it/clamav.dspam
touch /var/spool/dspam/opt-in/homeworks.it/clamav.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/clamav.dspam
md /var/spool/dspam/opt-in/homeworks.it/support.dspam
touch /var/spool/dspam/opt-in/homeworks.it/support.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/support.dspam
md /var/spool/dspam/opt-in/homeworks.it/root.dspam
touch /var/spool/dspam/opt-in/homeworks.it/root.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/root.dspam
md /var/spool/dspam/opt-in/homeworks.it/master.dspam
touch /var/spool/dspam/opt-in/homeworks.it/master.dspam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/master.dspam
```

Modifichiamo i *localStore* dei vari alias di modo che corrispondano alla loro Mailbox principale, *master*.

L'operazione di modifica del *localStore* andrebbe svolta **prima che gli alias di posta elettronica diventino operativi**, o in altri termini, prima che il server di posta elettronica che si sta realizzando venga messo in produzione.

```
dspam_admin change preference postmaster@homeworks.it localStore master
dspam_admin change preference nobody@homeworks.it localStore master
dspam_admin change preference hostmaster@homeworks.it localStore master
dspam_admin change preference usenet@homeworks.it localStore master
dspam_admin change preference news@homeworks.it localStore master
dspam_admin change preference webmaster@homeworks.it localStore master
dspam_admin change preference www@homeworks.it localStore master
dspam_admin change preference ftp@homeworks.it localStore master
dspam_admin change preference abuse@homeworks.it localStore master
dspam_admin change preference noc@homeworks.it localStore master
dspam_admin change preference security@homeworks.it localStore master
dspam_admin change preference clamav@homeworks.it localStore master
dspam_admin change preference support@homeworks.it localStore master
dspam_admin change preference mailer-daemon@homeworks.it localStore master
dspam_admin change preference root@homeworks.it localStore master
dspam_admin change preference master@homeworks.it localStore master
```

In questo modo il *localStore* degli alias dell'utente **master** sarà la cartella `/var/spool/dspam/data/local/master` mentre di solito per un utente di DSPAM il *localStore*, è la cartella `/var/spool/dspam/data/homeworks.it/<NomeMailbox>`

Ottimizzazzione del database di DSPAM

Per migliorerare l'efficienza di DSPAM, provvediamo ad ottimizzare l'accesso al database di DSPAM. Per poter ottimizzare l'accesso al database di DSPAM, bisogna introdurre degli indici che semplifichino la fase di ricerca dei record. Per introdurre questi indici si può procedere come segue (come in

precedenza, faremo riferimento al database di DSPAM creato manualmente):

```
mysql -u root -p
mysql> use db_dspam;
mysql> alter table dspam_token_data add index(spam_hits);
mysql> alter table dspam_token_data add index(innocent_hits);
mysql> alter table dspam_token_data add index(last_hit);
mysql> quit;
```

A questo punto bisogna modificare lo script */usr/share/doc/libdspam7-drv-mysql/purge-4.1.sql* in quanto questo script non utilizza gli indici che sono stati appena introdotti. Pertanto modifichiamo questo script come segue:

```
cp /usr/share/doc/libdspam7-drv-mysql/purge-4.1.sql /usr/share/doc/libdspam7-drv-mysql/purge-4.1.sql.originale
vi /usr/share/doc/libdspam7-drv-mysql/purge-4.1.sql
```

Modifichiamo la seguente query:

```
delete from dspam_token_data
where (innocent_hits*2) + spam_hits < 5
and @a-to_days(last_hit) > 60;
```

facendola diventare come segue:

```
delete from dspam_token_data
where (innocent_hits*2) + spam_hits < 5
and from_days(@a-60) > last_hit;
```

La query:

```
delete from dspam_token_data
where innocent_hits = 1 and spam_hits = 0
and @a-to_days(last_hit) > 15;
```

diventa:

```
delete from dspam_token_data
where innocent_hits = 1 and spam_hits = 0
and from_days(@a-15) > last_hit;
```

La query:

```
delete from dspam_token_data
where innocent_hits = 0 and spam_hits = 1
and @a-to_days(last_hit) > 15;
```

diventa:

```
delete from dspam_token_data
where innocent_hits = 0 and spam_hits = 1
and from_days(@a-15) > last_hit;
```

La query:

```
delete from dspam_token_data
USING
```

```
dspam_token_data LEFT JOIN dspam_preferences
ON dspam_token_data.uid = dspam_preferences.uid
AND dspam_preferences.preference = 'trainingMode'
AND dspam_preferences.value in('TOE','TUM','NOTRAIN')
WHERE @a-to_days(dspam_token_data.last_hit) > 90
AND dspam_preferences.uid IS NULL;
```

diventa:

```
delete from dspam_token_data
USING
dspam_token_data LEFT JOIN dspam_preferences
ON dspam_token_data.uid = dspam_preferences.uid
AND dspam_preferences.preference = 'trainingMode'
AND dspam_preferences.value in('TOE','TUM','NOTRAIN')
WHERE from_days(@a-90) > dspam_token_data.last_hit
AND dspam_preferences.uid IS NULL;
```

La query:

```
delete from dspam_token_data
USING
dspam_token_data LEFT JOIN dspam_preferences
ON dspam_token_data.uid = dspam_preferences.uid
AND dspam_preferences.preference = 'trainingMode'
AND dspam_preferences.value = 'TUM'
WHERE @a-to_days(dspam_token_data.last_hit) > 90
AND innocent_hits + spam_hits < 50
AND dspam_preferences.uid IS NOT NULL;
```

diventa:

```
delete from dspam_token_data
USING
dspam_token_data LEFT JOIN dspam_preferences
ON dspam_token_data.uid = dspam_preferences.uid
AND dspam_preferences.preference = 'trainingMode'
AND dspam_preferences.value = 'TUM'
WHERE from_days(@a-90) > dspam_token_data.last_hit
AND innocent_hits + spam_hits < 50
AND dspam_preferences.uid IS NOT NULL;
```

La query:

```
delete from dspam_signature_data
where @a-14 > to_days(created_on);
```

diventa:

```
delete from dspam_signature_data
where from_days(@a-14) > created_on;
```

Salviamo le modifiche ed eseguiamo una copia di salvataggio dello script appena modificato:

```
cp /usr/share/doc/libdspam7-drv-mysql/purge-4.1.sql /usr/share/doc/libdspam7-drv-mysql/purge-4.1.sql.index.use
```

A questo punto si può provare ad eseguire lo script /usr/share/doc/libdspam7-drv-mysql/purge-4.1.sql

appena modificato (per eseguire questo script utilizziamo l'utente *db_dspam_admin* con password *dspamadmin*):

```
mysql -udb_dspam_admin -pdspamadmin db_dspam < /usr/share/doc/libdspam7-drv-mysql/purge-4.1.sql
```

Per tenere il database di DSPAM pulito e snello, conviene pianificare l'esecuzione dello script `/usr/share/doc/libdspam7-drv-mysql/purge-4.1.sql` almeno una volta al mese; ad esempio per pianificare un ciclo di puliza alle 23:30 del primo giorno di ogni mese si può procedere come segue (ricordarsi di modoficare la configurazione di *crontab*, se si decide di cambiare la password dell'utente **db_dspam_admin**):

```
crontab -e
30 23 1 * * /usr/bin/mysql -udb_dspam_admin -pdspamadmin db_dspam < /usr/share/doc/libdspam7-drv-mysql/purge-4.1.sql
```

Dopo la modifica il file crontab dovrebbe contenere:

```
crontab -l
```

```
  # m h  dom mon dow   command
  # m => minute (0->59)
  # h => hour (0->23)
  # dom => day of month
  # mon => month (1->12)
  # dow => day of week (0 = Sunday)
  37 */4 * * * /usr/bin/UpdateSaneSecurity > /var/log/UpdateSaneSecurity
  30 23 1 * * /usr/bin/mysql -udb_dspam_admin -pdspamadmin db_dspam < /usr/share/doc/libdspam7-drv-mysql/purge-4.1.sql
```

Creazione del Global Merge Group di DSPAM

Essendo DSPAM un filtro statistico, conviene, prima che venga messo in produzione, eseguire una fase di addestramento di modo che possa individuare, sin dal suo primo utilizzo operativo, la maggior parte dello SPAM che verrà inoltrato al server di posta elettronica (stando all'esperienza degli autori, dopo questa fase DSPAM dovrebbe essere in grado di individuare circa il settanta percento dei messaggi di SPAM in arrivo). Per svolgere questa prima fase di apprendimento, bisogna utilizzare un elenco di messaggi di posta elettronica il cui contenuto è già stato *correttamente* classificato come SPAM o come HAM (ovvero messaggi legittimi). Un possibile elenco di questi messaggi di posta elettronica può essere reperito sul sito di SpamAssassin. Per prima cosa, quindi, iniziamo a scaricare questi elenchi di messaggi di posta elettronica:

```
cd /etc/dspam
md /etc/dspam/spamtest
cd /etc/dspam/spamtest
wget http://spamassassin.apache.org/publiccorpus/20021010_easy_ham.tar.bz2
wget http://spamassassin.apache.org/publiccorpus/20021010_hard_ham.tar.bz2
wget http://spamassassin.apache.org/publiccorpus/20030228_easy_ham.tar.bz2
wget http://spamassassin.apache.org/publiccorpus/20030228_easy_ham_2.tar.bz2
wget http://spamassassin.apache.org/publiccorpus/20030228_hard_ham.tar.bz2
wget http://spamassassin.apache.org/publiccorpus/20021010_spam.tar.bz2
wget http://spamassassin.apache.org/publiccorpus/20030228_spam.tar.bz2
wget http://spamassassin.apache.org/publiccorpus/20030228_spam_2.tar.bz2
wget http://spamassassin.apache.org/publiccorpus/20050311_spam_2.tar.bz2
tar xvfj 20021010_easy_ham.tar.bz2
mv easy_ham easy_ham_1
tar xvfj 20021010_hard_ham.tar.bz2
mv hard_ham hard_ham_1
tar xvfj 20030228_easy_ham.tar.bz2
mv easy_ham easy_ham_3
tar xvfj 20030228_easy_ham_2.tar.bz2
tar xvfj 20030228_hard_ham.tar.bz2
```

```
mv hard_ham hard_ham_2
tar xvfj 20021010_spam.tar.bz2
mv spam spam_1
tar xvfj 20030228_spam_2.tar.bz2
mv spam_2 spam_3
tar xvfj 20050311_spam_2.tar.bz2
tar xvfj 20030228_spam.tar.bz2
mv spam spam_4
chown -R dspam:dspam /etc/dspam/spamtest/easy_ham_1
chown -R dspam:dspam /etc/dspam/spamtest/easy_ham_2
chown -R dspam:dspam /etc/dspam/spamtest/easy_ham_3
chown -R dspam:dspam /etc/dspam/spamtest/hard_ham_1
chown -R dspam:dspam /etc/dspam/spamtest/hard_ham_2
chown -R dspam:dspam /etc/dspam/spamtest/spam_1
chown -R dspam:dspam /etc/dspam/spamtest/spam_2
chown -R dspam:dspam /etc/dspam/spamtest/spam_3
chown -R dspam:dspam /etc/dspam/spamtest/spam_4
```

la cartella `/etc/dspam/spamtest` dovrebbe apparire come:

```
ll /etc/dspam/spamtest/
```

```
-rw-r--r-- 1 root  root  1677144 2004-06-29 05:28 20021010_easy_ham.tar.bz2
-rw-r--r-- 1 root  root  1021126 2004-12-16 20:56 20021010_hard_ham.tar.bz2
-rw-r--r-- 1 root  root  1192582 2004-06-29 05:27 20021010_spam.tar.bz2
-rw-r--r-- 1 root  root  1077892 2004-06-29 05:27 20030228_easy_ham_2.tar.bz2
-rw-r--r-- 1 root  root  1612216 2004-06-29 05:27 20030228_easy_ham.tar.bz2
-rw-r--r-- 1 root  root  1029898 2004-12-16 20:56 20030228_hard_ham.tar.bz2
-rw-r--r-- 1 root  root  2059563 2004-06-29 05:27 20030228_spam_2.tar.bz2
-rw-r--r-- 1 root  root  1183768 2004-06-29 05:27 20030228_spam.tar.bz2
-rw-r--r-- 1 root  root  2059029 2005-06-03 02:23 20050311_spam_2.tar.bz2
drwx--x--x 2 dspam dspam  180224 2002-10-10 22:56 easy_ham_1
drwx--x--x 2 dspam dspam  106496 2003-02-28 12:04 easy_ham_2
drwx--x--x 2 dspam dspam  176128 2003-02-28 12:04 easy_ham_3
drwx--x--x 2 dspam dspam   20480 2004-12-16 20:36 hard_ham_1
drwx--x--x 2 dspam dspam   20480 2004-12-16 20:38 hard_ham_2
drwxr-xr-x 2 dspam dspam   36864 2003-02-28 12:05 spam_1
drwxrwxr-x 2 dspam dspam   98304 2005-03-12 00:46 spam_2
drwxrwxr-x 2 dspam dspam   98304 2003-04-24 09:13 spam_3
drwxr-xr-x 2 dspam dspam   36864 2003-02-28 12:05 spam_4
```

Per creare una base statistica comune a tutte le persone che utilizzeranno il programma DSPAM, creiamo il seguente *merged global group* (ovvero un singolo *merged group* valido per tutte le persone):

```
touch /var/spool/dspam/group
chown dspam:dspam /var/spool/dspam/group
vi /var/spool/dspam/group
```

inseriamo la sigla:

```
globaluser@homeworks.it:merged:*
```

I *merged group* consentono di essere utilizzati come base statistica *integrata*, ovvero i risultati statistici di ciascuna persona vengono *integrati*, al momento dell'analisi statistica di DSPAM, con la base statistica del *merged group*. In questo modo, anche persone che hanno una base statistica limitata, possono ottenere dei buoni risultati contro lo SPAM.

Per creare questa base statistica comune, utilizzeremo l'account **globaluser@homeworks.it**, già introdotto in precedenza. Questo account dovrà venire opportunamente creato, per cui:

```
useradd -c "Global Merged DSPAM User" -d /home/globaluser -s /usr/sbin/nologin -m globaluser
passwd globaluser
Enter new UNIX password: SharedGroup
Retype new UNIX password: SharedGroup
```

```
passwd: password updated successfully
```

Modifichiamo la fase di apprendimento dell'utente **globaluser@homeworks.it**:

```
dspam_admin change preference globaluser@homeworks.it trainingMode teft
dspam_admin list preference globaluser@homeworks.it
```

dovrebbe comparire la sigla:

```
trainingMode=teft
```

Una volta preparata la mailbox **globaluser@homeworks.it** possiamo iniziare la fase di apprendimento (le operazioni riportate possono richiedere diverse decine di minuti):

```
dspam_train globaluser@homeworks.it /etc/dspam/spamtest/spam_1 /etc/dspam/spamtest/easy_ham_1
dspam_train globaluser@homeworks.it /etc/dspam/spamtest/spam_2 /etc/dspam/spamtest/easy_ham_2
dspam_train globaluser@homeworks.it /etc/dspam/spamtest/spam_3 /etc/dspam/spamtest/hard_ham_1
dspam_train globaluser@homeworks.it /etc/dspam/spamtest/spam_4 /etc/dspam/spamtest/hard_ham_2
```

Al termine del processo di appendimento, conviene controllare le statistiche relative all'utente **globaluser@homeworks.it**:

```
dspam_stats -H globaluser@homeworks.it
```

dovrebbe comparire un risultato simile a questo:

```
globaluser@homeworks.it:
              TP True Positives:           3622
              TN True Negatives:           4581
              FP False Positives:            39
              FN False Negatives:           214
              SC Spam Corpusfed:             20
              NC Nonspam Corpusfed:           0
              TL Training Left:               0
              SHR Spam Hit Rate          94.42%
              HSR Ham Strike Rate:        0.84%
              OCA Overall Accuracy:      97.01%
```

Modifichiamo la fase di apprendimento dell'utente **globaluser** da **teft** a **toe**:

```
dspam_admin change preference globaluser@homeworks.it trainingMode toe
dspam_admin list preference globaluser@homeworks.it
```

dovrebbe comparire la sigla:

```
trainingMode=toe
```

A questo punto la prima fase di apprendimento di DSPAM è conclusa. Di tanto in tanto, dipende dai risultati che DSPAM ottiene nei confronti dello SPAM, bisognerà eseguire una fase di *aggiornamento statistico* nei confronti dell'account **globaluser@homeworks.it**, in questo modo si potrà tenere *aggiornata* la base statistica comune.

Verifica del funzionamento di DSPAM

Una volta creata la base statistica comune, si può procedere a verificare il corretto funzionamento di DSPAM. Per controllare il corretto funzionamento di DSPAM, utilizzeremo l'indirizzo email

test@homeworks.it già utilizzato in precedenza. Avendo adottato nel corso dell'articolo la modalità di funzionamento **Opt in**, per DSPAM, prima di procedere con i test dobbiamo accertarci che la seguente cartella ed il seguente file esistano:

```
  drwxr-xr-x 2 dspam dspam 4096 2007-11-08 03:55 /var/spool/dspam/opt-
in/homeworks.it/test.dspam
  -rw-r--r-- 1 dspam dspam    0 2007-11-08 03:56 /var/spool/dspam/opt-
in/homeworks.it/test.dspam/.dspam
```

In caso contrario si dovrà procedere alla loro creazione, altimenti DSPAM non provvederà a controllare le email indirizzate all'indirizzo **test@homeworks.it**. Pertanto:

```
md /var/spool/dspam/opt-in/homeworks.it/test.dpsam
touch /var/spool/dspam/opt-in/homeworks.it/test.dpsam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/test.dpsam
```

Creaimo, qualora ciò non fosse già stato fatto in precedenza, l'utente di DSPAM relativo all'indirizzo email **test@homeworks.it** (questa stessa operazione può venire svolta utilizzando il programma **PHPMyAdmin**):

```
mysql -u root -p
mysql> use db_dspam;
mysql> insert into dspam_virtual_uids (uid, username) values ('20', 'test@homeworks.it');
mysql> quit;
```

Per svolgere i test per valutare il corretto funzionamento di DSPAM utilizzeremo la seguente procedura:

1. inviamo un breve messaggio di email all'indirizzo **test@homeworks.it**;
2. dalla console dei comandi, lanciamo il comando:

   ```
   dspam_stats test@homeworks.it
   ```

   se tutto è andato bene si dovrebbe vedere un risultato simile a quello riportato di seguito (**TN: 1**):

   ```
           test@homeworks.it  TP:      0 TN:      1 FP:      0 FN:      0 SC:      0
   NC:      0
   ```

   dove:

   - **TP** = *Total Positive* (Il messaggio è classificato come *SPAM*)
   - **TN** = *Total Negative* (Il messaggio è classificato come *INNOCENT*)
   - **FN** = *False Negative* (Il messaggio precedentemente classificato come *SPAM* era invece un messaggio *INNOCENT*)
   - **FP** = *False Positive* (Il messaggio precedentemente classificato come *INNOCENT* era invece un messaggio *SPAM*)

3. eseguiamo poi il comando:

   ```
   dspam_dump test@homeworks.it
   ```

   se tutto è andato bene dovrebbe comparire un risultato simile al seguente (il numero di righe dipende dal numero di parole contenute nell'email inivata in precedenza all'indirizzo **test@homeworks.it**):

   ```
           18405170340785537991 S: 00001  I: 00001  P: 0.4000 LH: Sun Sep 16
   00:00:00 2007
           18405514230328945959 S: 00001  I: 00000  P: 0.4000 LH: Mon Sep 17
   ```

```
00:00:00 2007
        18420787804149786117 S: 00001  I: 00000  P: 0.4000 LH: Sun Sep 16
00:00:00 2007
        18423737673249977587 S: 00000  I: 00004  P: 0.4000 LH: Sat Sep 15
00:00:00 2007
        18431276009438829505 S: 00001  I: 00000  P: 0.4000 LH: Mon Sep 17
00:00:00 2007
```

4. apriamo l'intestazione (*header*) del messaggio ricevuto da **test@homeworks.it** e controllare che compaia la vode **X-DSPAM-SID**. Si dovrebbe vedere una sigla di numeri e lettere simile a **20,46ed597b26671343920161**. Dove la cifra prima della *virgola* indica lo **UID** (*User Identifier*) dell'utente DSPAM (nel nostro esempio, **20** corrisponde all'utente **test@homeworks.it**). Il codice che segue il simbolo della *virgola*, è un identificativo con cui DSPAM individua un dato messaggio email. Questa sequenza di numeri e lettere, composta dallo **UID** e dal codice *identificativo*, è la *firma di DSPAM*. Prendere nota di questa sequenza di numeri e lettere ed eseguire il comando:

```
dspam --client --user test@homeworks.it --class=spam --source=error
--signature='<Firma_DSPAM>'
```

   ad esempio:

```
dspam --client --user test@homeworks.it --class=spam --source=error
--signature='20,46ed597b26671343920161'
```

5. eseguiamo poi il comando:

```
dspam_stats test@homeworks.it
```

   se tutto è andato bene dovrebbe comparire il messaggio (**FN: 1**):

```
        test@homeworks.it  TP:     0 TN:     1 FP:     0 FN:     1 SC:     0
NC:     0
```

6. Inviamo diversi messaggi email all'indirizzo **test@homeworks.it** e controlliamo l'intestazione (*header*) di ciascun messaggio inviato e verifichiamo che compaia il campo **X-DSPAM-SID**.

Se i test hanno dato esito positivo, si può pensare di mettere DSPAM in produzione.

Come gestire i messaggi erroneamente classificati

Come tutti gli strumenti informatici realizzati per combattere lo SPAM, anche DSPAM non è immune da errori di valutazione, può succedere pertanto che DSPAM classifichi un messaggio *buono* come SPAM e viceversa, un messaggio *cattivo* come HAM. In questi casi bisogno provvedere a segnalare a DSPAM l'errore commesso. Il metodo più semplice per fare questa segnalazione è quello di utilizzare la webmail, sfruttando il plug-in Spam Buttons illustrato nel paragrafo Configurazione ed installazione del plugin Spam Buttons in SquirrelMail. In alternativa si può ricorrere alla seguente procedura:

- visualizzare l'intestazione (*header*) del messaggio erroneamente classificato;
- prendere nota della *firma di DSAPM* prendendo nota del testo che segue la voce **X-DSPAM-SID** (qualcosa di simile a **20,46ed597b26671343920161**);
- editare il messaggio email erroneamente classificato come *nuovo*; specificare come destinatario l'indirizzo email:
    - **spam@homeworks.it**: se il messaggio era *cattivo* ed è stato classficato come HAM;
    - **notspam@homeworks.it**: se il messaggio era *buono* ed è stato classificato come SPAM;

- inserire in fondo al corpo dell'email, il seguente testo:

```
!DSPAM:<Firma_DSPAM>!
```

  Dove **<Firma_DSPAM>** corrisponde alla sigla contenuta nell'intestazione del messaggio. Facendo riferimento all'esempio citato in precedenza, dovremmo scrivere:

```
!DSPAM:20,46ed597b26671343920161!
```

  nel nostro esempio la sigla **20,46ed597b26671343920161** corrisponde alla voce **<Firma_DSPAM>**;
- inviare l'email e verificare nei file di log (*/var/log/mail.info*) di Postfix che il messaggio sia stato correttamente inviato.

La notifica degli errori comessi è estremamente importate per poter *tarare* al meglio il funzionamento di DSPAM.

Come attivare la funzione di debug di DSPAM

Se si vuole comprendere come funziona DSPAM, si può attivare la funzione di *debug* di DSPAM. Per attivare questa funzione bisogna modificare in modo opportuno il file di configurazione di DSPAM, */etc/dspam/dspam.master.conf*:

```
vi /etc/dspam/dspam.master.conf
```

togliere il segno di commento alla riga:

```
#Debug *
```

facendola diventare:

```
Debug *
```

salvare le modifiche ed eseguire i comandi:

```
show /etc/dspam/dspam.master.conf > /etc/dspam/dspam.conf
/etc/inet.d/dspam restart
```

La informazioni di *debug* verranno scritte all'interno del file: */var/log/dspam/dspam.debug*

Come abilitare Thunderbird a controllare i messaggi di SPAM

A seguito della configurazione di DSPAM che è stata adottata, per consentire al programma Thunderbird di individuare i messaggi classificati come SPAM ed inserirli all'interno della cartella SPAM creata appositamente in precedenza, dobbiamo creare un'apposita regola di filtro:

- avviamo il programma **Thunderbird**;
- apriamo il menù **Tools** e selezioniamo la voce **Messagge Filters ...**;
- premiamo il pulsante **New**;
- nel campo di testo denominato *Filter Name* inseriamo il testo **Filtro AntiSPAM**;
- selezioniamo l'opzione **Match any of the following**;
- impostiamo la seguente regola: **Subject**, **Contains**, **[SPAM]**;
- nella sezione *Perform this actions* inseriamo la seguente azione: **Move messagge to**, **SPAM on**

<Nome_Mailbox>. Dove **<Nome_Mailbox>** corrisponde al nome della Mailbox che è stato impostato;
- confermiamo i dati inseriti premendo il pulsante **OK**;
- controlliamo che la regola appena inserita sia abilitata, ovvero compaia il simbolo di selezione nel campo **Enable**. Se non compare, provvederemo ad inserirlo;
- chiudiamo la finestra dal titolo *Message Filters*.

Una volta creata la regola, Thunderbird provvederà a mettere i messaggi che contengono la voce **[SPAM]** nell'oggetto nella cartella SPAM creata appositamente in precedenza.


In futuro, si potrà automatizzare questa operazione, riccorendo al comando `maildrop` che si trova a corredo del programma Courier.

Per evitare che i messaggi di SPAM archiviati nella cartella **SPAM** di Thunderbird arrivino ad occupare troppo spazio disco, conviene abilitare una procedura di cancellazione automatica dei messaggi di SPAM più vecchi di una certa data, ad esempio *60 giorni*:

- avviamo il programma **Thunderbird**;
- evidenziamo col mouse la cartella **SPAM**;
- apriamo il menù **Edit** e selezioniamo la voce **Folder Properties**;
- andiamo nella sezione **Retention Policy**;
- selezioniamo la voce **Delete Messagge More Than** ed impostiamo come periodo, nella casella di testo, il valore di **60** giorni (*days old*);
- confermiamo i dati inseriti premendo il pulsante **OK**.

In questo modo, Thunderbird provvederà a cancellare i messaggi di SPAM più vecchi di *60 giorni*, evitando in questa maniera di far crescere troppo in dimensioni la cartella **SPAM**.

Come inserire un Disclaimer nei messaggi email in uscita

La direzione della Home Works S.p.A ha chiesto al personale IT di aggiungere un messaggio di assunzione di responsabilità (*Disclaimer*) in fondo ad ogni email inviata dai dipendenti della Home Works S.p.A. Per assolvere a questo compito il personale IT ha deciso di utilizzare il programma alterMIME.


Quanto esposto in questa sezione è liberamente ispirato all'articolo How To Automatically Add A Disclaimer To Outgoing Emails With alterMIME

Iniziamo quindi con l'installare il programma alterMIME:

```
apt-get install altermime
```

Creiamo poi l'utente `filter`, utilizzato dal programma alterMIME, avente come *home directory* la cartella */var/spool/filter*:

```
useradd -r -c "Postfix Filters" -d /var/spool/filter filter
mkdir /var/spool/filter
chown filter:filter /var/spool/filter
chmod 750 /var/spool/filter
```

Modifichiamo lo script d'esempio per la configurazione del programma alterMIME, */usr/share/doc/altermime/examples/postfix_filter.sh*, in base alla configurazione del server di posta elettronica esposta in questo articolo. Per semplicità, applicheremo il Disclaimer a tutti gli indirizzi email presenti nel database di DSPAM denominato **dspam_virtual_uids**. Pertanto:

```
cp /usr/share/doc/altermime/examples/postfix_filter.sh /etc/postfix/disclaimer
chgrp filter /etc/postfix/disclaimer
chmod 750 /etc/postfix/disclaimer
```

Per ovvi motivi di sicurezza, dal momento che nello script dovremo specificare la password di accesso a MySQL in chiaro, creiamo un utente di MySQL che abbia solamente i diritti di *lettura* (*SELECT*) nei confronti del database **db_dspam** (questo utente avrà il nome di **db_dspam_reader** e password **dspamreader**):

```
mysql -u root -p
mysql> create user 'db_dspam_reader'@'localhost' identified by 'dspamreader';
mysql> use mysql;
mysql> select user from user;
```

```
+------------------+
| user             |
+------------------+
| root             |
| db_dspam_admin   |
| db_dspam_reader  |
| debian-sys-maint |
| dspam            |
| libdspam7-drv-my |
| root             |
+------------------+
7 rows in set (0.01 sec)
```

assegnamo all'utente di MySQL **db_dspam_reader** i permessi di lettura (*select*) al database **db_dspam**:

```
mysql> grant select on db_dspam.* to db_dspam_reader@localhost;
mysql> exit
```

Per conoscere quali sono i comandi amministrativi del programma MySQL si può consultare il sito web www.techotopia.com

Editiamo il file */etc/postfix/disclaimer*:

```
vi /etc/postfix/disclaimer
```

ed aggiungiamo le seguenti modifiche:

```
#!/bin/sh
# Localize these.
INSPECT_DIR=/var/spool/filter
SENDMAIL=/usr/sbin/sendmail

# Exit codes from <sysexits.h>
EX_TEMPFAIL=75
EX_UNAVAILABLE=69

# Clean up when done or when aborting.
trap "rm -f in.$$" 0 1 2 3 15

# Start processing.
cd $INSPECT_DIR || { echo $INSPECT_DIR does not exist; exit
$EX_TEMPFAIL; }

cat >in.$$ || { echo Cannot save mail to file; exit $EX_TEMPFAIL; }

####### Changed From Original Script #######
# Obtain the email address (from_address) of the sender
from_address=`grep -m 1 "From:" in.$$ | cut -d "<" -f 2 | cut -d ">" -f 1`
result=`mysql -u db_dspam_reader --password=dspamreader -e \
```

```
                "use db_dspam; select uid from db_dspam.dspam_virtual_uids where
username='$from_address';"`

  # We check if the email address is in the table dspam_virtual_uids
  if [ "$result" ]; then
        /usr/bin/altermime --input=in.$$ \
                           --disclaimer=/etc/postfix/disclaimer.txt \
                           --disclaimer-html=/etc/postfix/disclaimer.html \
                           --xheader="X-Copyrighted-Material: Please visit
http://www.homeworks.it/Html/Privacy.html" || \
                           { echo Message content rejected; exit $EX_UNAVAILABLE; }
  fi
  ####### Changed From Original Script END #######

  $SENDMAIL "$@" <in.$$

  exit $?
```

Una volta modificato lo script di configurazione del programma alterMIME, creiamo i file in cui inserire il messaggio di Disclaimer:

Per avere un'idea di quali messaggi si possono utilizzare come Disclaimer, si può consultare il sito web www.emaildisclaimers.com

```
touch /etc/postfix/disclaimer.txt
touch /etc/postfix/disclaimer.html
```

Aggiungiamo il seguente testo all'interno dei file */etc/postfix/disclaimer.txt* e */etc/postfix/disclaimer.html*:

```
vi /etc/postfix/disclaimer.txt
```

il file */etc/postfix/disclaimer.txt* diventa:

```
  Versione Italiana:

  La Home Works S.p.A ha un limite, per le email, compresi i file allegati,
  di 10MB. Se i tuoi messaggi di posta elettronica superano questo limite,
  non sarà possibile inoltrarli al personale della Home Works S.p.A.
  Elimina qualche allegato o rendi più piccolo di 10MB il tuo messaggio
  di posta elettronica, se non sai come fare, fa rimerifemento al tuo
  supporto tecnico.

  Informativa della Privacy ai sensi del art. 13 D.lgs. 196/2003
  (http://www.homeworks.it/Html/Privacy.html)

  English Version:

  Home Works S.p.A limits all e-mail, including attachments, to 10MB.
  Your message will not be delivered if it exceeds this limit. Please create a
  shorter message, remove attachments, or consult your technician
  if your message exceeds the 10MB limit.

  Notice of Privacy under Art. D.lgs 13. 196/2003
  (http://www.homeworks.it/Html/Privacy.html)
```

salviamo le modifiche effettuate al file */etc/postfix/disclaimer.txt* ed editiamo il file */etc/postfix/disclaimer.html*:

```
vi /etc/postfix/disclaimer.html
```

aggiungiamo il seguente testo al file */etc/postfix/disclaimer.html*:

```
  <b>Versione Italiana:</b><br><br>
  <i>La Home Works S.p.A ha un limite per le email, compresi i file allegati,
  di 10MB</i>. Se i tuoi messaggi di posta elettronica superano questo limite,
  non sarà possibile inoltrarli al personale della Home Works S.p.A.
  Elimina qualche allegato o rendi più piccolo di 10MB il tuo messaggio
  di posta elettronica, se non sai come fare, fa rimerifemento al tuo
  supporto tecnico.<br>
  Informativa della Privacy ai sensi del <b>art. 13 D.lgs. 196/2003</b><br>
  (<a
href="http://www.homeworks.it/Html/Privacy.html">http://www.homeworks.it/Html/Privacy
.html</a>)
  <br><br>
  <b>English Version:</b><br><br>
  <i>Home Works S.p.A limits all e-mail, including attachments, to 10MB</i>.
  Your message will not be delivered if it exceeds this limit. Please create a
  shorter message, remove attachments, or consult your technician
  if your message exceeds the 10MB limit.<br>
  Notice of Privacy under <b>art. 13 D.lgs. 196/2003</b><br>
  (<a
href="http://www.homeworks.it/Html/Privacy.html">http://www.homeworks.it/Html/Privacy
.html</a>)
```

salviamo le modifiche effettuate al file */etc/postfix/disclaimer.html* A questo punto possiamo modificare la configurazione di Postfix; editiamo quindi il file /etc/postfix/master.cf:

```
vi /etc/postfix/master.cf
```

aggiungiamo all'inizio del file */etc/postfix/master.cf* la riga:

```
  smtp      inet  n       -       -       -       -       smtpd
    -o content_filter=dfilt:
  ...
```

mentre in fondo al file */etc/postfix/master.cf* aggiungiamo la riga:

```
  ...
  dfilt     unix    -       n       n       -       -       pipe
    flags=Rq user=filter argv=/etc/postfix/disclaimer -f ${sender} -- ${recipient}
```

salviamo le modifiche effettuate al file */etc/postfix/master.cf* e riavviamo Postfix:

```
/etc/init.d/postfix restart
```

Si osservi che se un email è firmata digitalmente, il contenuto del testo del Disclaimer non verrà aggiunto all'email. In questi casi, l'unica soluzione, è quella di chiedere alla persona di provvedere a creare una propria firma aziendale, all'interno della quale inserire il testo del messaggio di riservatezza. Allo stesso modo, se un messaggio di posta elettronica viene inviato tramite il protocollo IMAP utilizzando la cartella **Outbox**, non verrà aggiunto, in fondo al messaggio, il contenuto del testo del Disclaimer.

Gestione delle Mailbox

In questa sezione cerchiamo di spiegare come creare, modificare e cancellare una Mailbox all'interno del server di posta elettronica che abbiamo realizzato.

Tutte le operazioni che andremo a svolgere, possono venire eseguite in modo più semplice e agevole, ricorrendo a degli opportuni script che consentano di automatizzare le varie operazioni descritte.

Per creare una nuova Mailbox si può procedere come segue (tanto per fissare le idee, supporemo che la nuova Mailbox abbia indirizzo email *ipagliani@homeworks.it*, come alias di posta elettronica l'indirizzo email *iarno_pagliani@homeworks.it* e sia associata all'utente di sistema *ipagliani*):

```
useradd -c "Iarno Pagliani" -d /home/ipagliani -s /usr/sbin/nologin -m ipagliani
passwd ipagliani
```

Una volta creato l'utente si può procedere ad assegnargli un eventuale *alias* della sua Mailbox (seguendo lo schema *Nome Mailbox: Nome Utente*) modificando opportunamente il file `/etc/aliases` (nel nostro esempio ciò equivale ad aggiungere la riga: `iarno_pagliani: ipagliani`). Una volta modificato il file `/etc/aliases` bisogna eseguire i comandi:

```
postalias hash:/etc/aliases
newaliases
postfix reload
```

A questo punto bisogna abilitare il controllo antispam agli indirizzi email *ipagliani@homeworks.it* e *iarno_pagliani@homeworks.it*, avendo l'accortezza di unificare il *localstore* dei due indirizzi email (per semplicità supporemo che gli *uid* di questi due indirizzi email siano, rispettivamente, *19* e *20*):

```
md /var/spool/dspam/opt-in/homeworks.it/ipagliani.dpsam
touch /var/spool/dspam/opt-in/homeworks.it/ipagliani.dpsam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/ipagliani.dpsam
md /var/spool/dspam/opt-in/homeworks.it/iarno_pagliani.dpsam
touch /var/spool/dspam/opt-in/homeworks.it/iarno_pagliani.dpsam/.dspam
chown -R dspam:dspam /var/spool/dspam/opt-in/homeworks.it/iarno_pagliani.dpsam
mysql -u db_dspam_admin -p
mysql> use db_dspam;
mysql> select * from dspam_virtual_uids;
mysql> insert into dspam_virtual_uids (uid, username) values ('21',
'ipagliani@homeworks.it');
mysql> insert into dspam_virtual_uids (uid, username) values ('22',
'iarno_pagliani@homeworks.it');
mysql> quit;
dspam_admin change preference ipagliani@homeworks.it localStore ipagliani
dspam_admin change preference iarno_pagliani@homeworks.it localStore ipagliani
```

Una volta creata la Mailbox, si può procedere con la configurazione di Thunderbird. Se previsto, si può assegnare alla persona titolare della Mailbox (nel nostro esempio *Iarno Pagliani*) un certificato digitale con cui firmare digitalmente i messaggi di posta elettronica inviati.

Se si decide di modificare l'alias di posta elettronica da *iarno_pagliani@homeworks.it* a *iarno.pagliani@homeworks.it*, si deve prima modificare opportunamente il file `/etc/aliases` modificando la riga `iarno_pagliani: ipagliani` in `iarno.pagliani: ipagliani` Una volta modificato il file `/etc/aliases` bisogna ricreare la mappa degli alias associata a Postfix:

```
postalias hash:/etc/aliases
newaliases
postfix reload
```

Dopo di che si deve sostituire dal controllo antispam l'indirizzo email *iarno_pagliani@homeworks.it*, coll'indirizzo email *iarno.pagliani@homeworks.it*:

```
mv /var/spool/dspam/opt-in/homeworks.it/iarno_pagliani.dpsam /var/spool/dspam/opt-
in/homeworks.it/iarno.pagliani.dpsam
mysql -u db_dspam_admin -p
mysql> use db_dspam;
mysql> select * from dspam_virtual_uids;
mysql> update dspam_virtual_uids set username='iarno.pagliani@homeworks.it' where uid=21;
```

```
mysql> quit;
```

Se si vuole invece cancellare una Mailbox, si deve per prima cosa cancellare eventuali alias della Mailbox dal file */etc/aliases* (facendo riferimento al nostro esempio, si dovrà procedere con la cancellazione della riga `iarno.pagliani: ipagliani`). Una volta cancellati questi alias bisognerà ricaricare in Postfix la nuova versione del file */etc/aliases*:

```
postalias hash:/etc/aliases
newaliases
postfix reload
```

Successivamente, si deve da prima cancellare l'account di sistema associalto alla Mailbox da eliminare e poi cancellare i controlli antispam associati agli indirizzi email che fanno riferimento alla Mailbox (per comodità, continuiamo a fare riferimento all'esempio sin qui utilizzato):

```
userdel -r ipagliani
rm -rf /var/spool/dspam/opt-in/homeworks.it/ipagliani.dpsam
rm -rf /var/spool/dspam/opt-in/homeworks.it/iarno.pagliani.dpsam
mysql> use db_dspam;
mysql> select * from dspam_virtual_uids;
mysql> delete from dspam_virtual_uids where uid=21;
mysql> delete from dspam_virtual_uids where uid=22;
mysql> quit;
```

Se si desdiera creare una *lista di distribuzione*, bisognerà modificare opportunamente il file */etc/aliases* Ad esempio, se si vuole assegnare agli indirizzi email *atani@homeworks.it*, *ipagliani@homeworks.it* e *mrossi@homeworks.it* (associati, rispettivamente, agli account di sistema *atani*, *ipagliani* e *mrossi*), la lista di distribuzione *info@homeworks.it*, si dovrà aggiungere, al file */etc/aliases*, la riga `info: atani, ipagliani, mrossi` e procedere con l'aggiornamento della mappa associata a Postfix:

```
postalias hash:/etc/aliases
newaliases
postfix reload
```

Installazione e configurazione di Mailgraph

Installiamo il programma Mailgraph per poter accedere alle statistiche di Postfix via Internet, attraverso un comune browser. Per prima cosa installiamo il programma Mailgraph:

```
apt-get install rrdtool mailgraph
```

Riconfiguriamo il programma Mailgraph:

```
dpkg-reconfigure mailgraph
```

alle varie domande dovremo rispondere nel modo seguente:

```
Should Mailgraph start on boot? <-- Yes
Logfile used by mailgraph: <-- /var/log/mail.log
Count incoming mail as outgoing mail? <-- No
```

Configuriamo il programma Mailgraph affinchè i suoi risultati siano consultabili via Internet (in particolare, integriamo l'esecuzione di Mailgraph all'interno della SquirrelMail):

```
md /usr/share/squirrelmail/cgi-bin
ln -s /usr/lib/cgi-bin/mailgraph.cgi /usr/share/squirrelmail/cgi-bin/mailgraph.cgi
```

Modifichiamo il file di configurazione della SquirrelMail, */etc/squirrelmail/apache.conf*:

```
vi /etc/squirrelmail/apache.conf
```

aggiungiamo le seguenti righe:

```
...

      AllowOverride All
      Options ExecCGI FollowSymLinks
      AddHandler cgi-script .cgi

...
```

A questo punto i risultati del programma Mailgraph sono visualizzabili tramite lo URL **http://mail.homeworks.it/cgi-bin/mailgraph.cgi**. Possiamo quindi procedere col raccogliere i dati statistici già presenti nel file */var/log/mail.log* Se ad esempio il server di posta elettronica è operativo dall'anno precedente (nel nostro caso dall'anno *2007*), allora per raccogliere i dati statistici basterà eseguire i comandi:

```
/etc/init.d/mailgraph stop
mailgraph -v -c -l /var/log/mail.log --daemon_rrd=/var/lib/mailgraph -y 2007
```

Viceversa, se il server di posta elettronica è operativo da quest'anno, basterà eseguire i comandi seguenti per raccogliere i dati statistici contenuti nel file */var/log/mail.log*:

```
/etc/init.d/mailgraph stop
mailgraph -v -c -l /var/log/mail.log --daemon_rrd=/var/lib/mailgraph
```

I comandi `mailgraph -v -c -l /var/log/mail.log --daemon_rrd=/var/lib/mailgraph -y 2007` e `mailgraph -v -c -l /var/log/mail.log --daemon_rrd=/var/lib/mailgraph` possono richiedere diverso tempo (anche qualche decina di minuti) prima di poter terminare. Da questo momento in poi il programma Mailgraph sarà in grado di raccogliere i dati statistici relativi al server di posta elettronica in tempo reale.

Più in generale avremo:

```
mailgraph -v -c -l /var/log/mail.log --daemon_rrd=/var/lib/mailgraph -y <Anno_Più_Vecchio>
```

Dove `<Anno_Più_Vecchio>` indica l'anno più vecchio riportato nel file */var/log/mail.log*, ovvero se nel file */var/log/mail.log* sono presenti dati sin dall'anno 2005, dovremo eseguire il comando:

```
mailgraph -v -c -l /var/log/mail.log --daemon_rrd=/var/lib/mailgraph -y 2005
```

Prima di poter riavviare il demone */etc/init.d/mailgraph* bisogna modificare il file */etc/init.d/mailgraph* affinchè venga tenuto conto, qualora fosse necessario, del parametro `-y <Anno_Più_Vecchio>`. Per cui, se il server di posta elettronica è operativo da qualche anno, editiamo il file */etc/init.d/mailgraph*:

```
vi /etc/init.d/mailgraph
```

modifichiamo la riga:

```
IGNORE_OPTION=""
```

in:

```
IGNORE_OPTION="-y <Anno_Più_Vecchio>"
```

ad esempio:

```
IGNORE_OPTION="-y 2007"
```

A questo punto si può salvare il file */etc/init.d/mailgraph* ed avviare il demone */etc/init.d/mailgraph* e riavviare quello di Apache2:

```
/etc/init.d/mailgraph start
/etc/init.d/apache2 restart
```

Per verificare se i parametri di esecuzione del demone */etc/init.d/mailgraph* sono corretti, si può utilizzare il comando seguente:

```
ps aux | grep mailgraph
root 3229 0.2 0.7 8156 3784 ? Ss 17:21 0:02 /usr/bin/perl -w /usr/sbin/mailgraph -l /var/log/
mail.log -d --daemon_rrd=/var/lib/mailgraph -y 2007
root 3426 0.0 0.1 3056 632 pts/0 R+ 17:40 0:00 grep mailgraph
```

Per vedere le statistiche relative al nostro server di posta elettronica, basterà collegarsi al sito **http://mail.homeworks.it/cgi-bin/mailgraph.cgi** Rinfrescando la pagina web **http://mail.homeworks.it/cgi-bin/mailgraph.cgi** si potranno vedere le statistiche aggiornarsi ogni cinque minuti.

Per vedere il contenuto del database in cui Mailgraph inserisce i suoi dati, si possono utilizzare i comandi:

```
rrdtool dump /var/lib/mailgraph/mailgraph.rrd | less
```

e

```
rrdtool dump /var/lib/mailgraph/mailgraph_virus.rrd | less
```

Modifiche al pacchetto Debian di Mailgraph

Purtroppo il pacchetto Debian relativo al programma Mailgraph non è aggiornato con le nuove pagine web del programma RRDTool e dell'autore David Schweikert. Pertanto, se si vuole che i collegamenti a questi siti siano corretti, bisogna modificare il file */usr/lib/cgi-bin/mailgraph.cgi* manualmente:

```
vi /usr/lib/cgi-bin/mailgraph.cgi
```

modifichiamo le righe:

```
  ...
  <A href="http://people.ee.ethz.ch/~dws/software/mailgraph">Mailgraph</A> $VERSION
  by <A href="http://people.ee.ethz.ch/~dws/">David Schweikert</A></td>
  <td ALIGN="right">
  <a HREF="http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/">
        <img border="0"
src="http://people.ethz.ch/~oetiker/webtools/rrdtool/.pics/rrdtool.gif" alt=""
width="120" height="34">
  </a>
  ...
```

come segue:

```
  ...
  <A href="http://mailgraph.schweikert.ch/">Mailgraph</A> $VERSION
```

```
  by <A href="http://david.schweikert.ch/">David Schweikert</A></td>
  <td ALIGN="right">
  <a HREF="http://oss.oetiker.ch/rrdtool/">
    <img border="0" src="http://oss.oetiker.ch/rrdtool/.pics/rrdtool.gif"
alt="RRDTool Logo" width="120" height="34">
  </a>
  ...
```

una volta effettuate le modifiche si può salvare il file */usr/lib/cgi-bin/mailgraph.cgi*

Osservazioni su Mailgraph

Si osservi che in seguito alla configurazione adottata, i messaggi di posta elettronica in arrivo vengono contati tre volte, come messaggi in ingresso (*Received*) e due volte come inviati (*Sent*), a causa dei meccanismi di controllo dei virus (*ClamSMTPD*) e dello SPAM (*DSPAM*). I messaggi di posta elettronica inviati dal server di posta, invece, vengono contati come due messaggi inviati (*Sent*) e come tre messaggi in arrivo (*Received*), sempre a causa dei controlli sui virus (*ClamSMTPD*) e dello SPAM (*DSPAM*), sebbene, in base alla nostra configurazione i messaggi inviati non vengano controllati dal motore AntiSPAM (*DSPAM*). Pertanto i valori riportati nei campi **Received** e **Sent** non corrispondono esattamente al numero dei messaggi inviati da un client di posta elettronica da un server SMTP verso il nostro server di posta, o dal nostro server di posta ad un altro server SMTP, ma al numero complessivo di messaggi che il nostro server di posta elettronica gestisce in ingresso (da un server SMTP esterno verso il nostro server di posta elettronica) ed in uscita (dal nostro server di posta elettronica ad un altro server SMTP esterno).

Installazione e configurazione di CourierGraph

Analogamente al programma Mailgraph si può installare il programma CourierGraph, ovvero un programma in grado di visualizzare le statiche di accesso ai programmi Courier-POP, Courier-POP-SSL e Courier-IMAP, Courier-IMAP-SSL. Per prima cosa procediamo con l'installazione del programma CourierGraph:

```
apt-get install couriergraph
```

Fermiamo il demone associato al programma CourierGraph:

```
/etc/init.d/couriergraph stop
```

Creiamo il primo database del programma CourierGraph (questa operazione può richiedere diversi minuti). Esattamente come per Mailgraph, anche per CourierGraph bisogna gestire i dati degli anni passati contenuti, eventualmente, nel file */var/log/mail.log* Ad esempio se il file */var/log/mail.log* contiene dei dati risalenti all'anno 2007, dovremo utilizzare il seguente comando per raccogliere i dati statistici:

```
couriergraph.pl -v -c -l /var/log/mail.log --daemon-rrd=/var/lib/couriergraph -y 2007
```

Viceversa, se il file */var/log/mail.log* contiene solamente i dati di quest'anno, dovremo eseguire il comando:

```
couriergraph.pl -v -c -l /var/log/mail.log --daemon-rrd=/var/lib/couriergraph
```

Una volta raccolti i dati statistici, possiamo rendere disponibili i risultati via Internet:

```
ln -s /usr/lib/cgi-bin/couriergraph.cgi /usr/share/squirrelmail/cgi-bin/couriergraph.cgi
```

Modifichiamo il file */etc/init.d/couriergraph* per poter gestire i dati degli anni precedenti (nel esempio che riportiamo facciamo riferimento per comodità all'anno 2007):

Le modifiche relative alla gestione degli anni precedenti, vanno effettuate solamente se nel file */var/log/mail.log* sono presenti dati statistici risalenti agli anni passati, altrimenti queste modifiche non sono necessarie.

```
vi /etc/init.d/couriergraph
```

modifichiamo il file da:

```
  ...
  RRD_NAME=couriergraph

  test -x $DAEMON || exit 0

  if [ -f $CONFIG ]; then
        . $CONFIG
  fi

  case "$1" in
    start)
        echo -n "Starting $DESC: "
        start-stop-daemon --start --quiet --pidfile $PIDFILE \
                --exec $DAEMON -N 15 -c daemon:adm -- \
                -l $MAIL_LOG -d --daemon_rrd=$RRD_DIR --rrd_name=$RRD_NAME
        echo "$NAME."
  ...
```

in:

```
  ...
  RRD_NAME=couriergraph
  IGNORE_OPTION="-y 2007"

  test -x $DAEMON || exit 0

  if [ -f $CONFIG ]; then
        . $CONFIG
  fi

  case "$1" in
    start)
        echo -n "Starting $DESC: "
        start-stop-daemon --start --quiet --pidfile $PIDFILE \
                --exec $DAEMON -N 15 -c daemon:adm -- \
                -l $MAIL_LOG -d --daemon_rrd=$RRD_DIR --rrd_name=$RRD_NAME
$IGNORE_OPTION
        echo "$NAME."
  ...
```

Aggiorniamo poi il file */usr/lib/cgi-bin/couriergraph.cgi* con i collegamenti corretti alle varie pagine web riportate (esattamente come fatto nel paragrafo Modifiche al pacchetto Debian di Mailgraph):

```
vi /usr/lib/cgi-bin/couriergraph.cgi
```

modifichiamo le righe:

```
  ...
  <A href="http://people.ee.ethz.ch/~dws/software/mailgraph"<Mailgraph</A> $VERSION
  by <A href="http://people.ee.ethz.ch/~dws/">David Schweikert</A></td>
```

```
  <td ALIGN="right">
  <a HREF="http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/">
    <img border="0"
src="http://people.ethz.ch/~oetiker/webtools/rrdtool/.pics/rrdtool.gif" alt=""
width="120" height="34">
  </a>
  ...
```

come segue:

```
  ...
  <A href="http://mailgraph.schweikert.ch/">Mailgraph</A> $VERSION
  by <A href="http://david.schweikert.ch/">David Schweikert</A></td>
  <td ALIGN="right">
  <a HREF="http://oss.oetiker.ch/rrdtool/">
    <img border="0" src="http://oss.oetiker.ch/rrdtool/.pics/rrdtool.gif"
alt="RRDTool Logo" width="120" height="34">
  </a>
  ...
```

Una volta effettuate le modifiche si può salvare il file */usr/lib/cgi-bin/couriergraph.cgi* A questo punto possiamo avviare il demone del programma CourierGraph:

```
/etc/init.d/couriergraph start
```

Per accedere alle statistiche messe a disposizione dal programma CourierGraph, basta collegarsi alla pagina web: **https://mail.homeworks.it/cgi-bin/couriergraph.cgi**

Considerazioni Finali

Oggigiorno è difficile pensare che una società si affidi ad una soluzione Open Source, simile ad esempio a quella proposta in questo articolo, per la gestione delle proprie Mailbox aziendali. Questa difficoltà è più culturale che tecnica. La soluzione di posta elettronica proposta in questo articolo non solo è perfettamente funzionante, ma cerca anche di venire incontro alle normali esigenze che una piccola o media impresa possono avere. Per fare un esempio, l'idea di ricorrere al protocollo IMAP, consente di accedere alle Mailbox aziendali, da parte del personale che opera sulle postazioni mobili, come ad esempio i laptop aziendali, sia quando queste persone operano all'interno della rete aziendale, sia quando queste persone si trovano a lavorare al di fuori della rete aziendale. Questo accesso alle Mailbox avviene, nella configurazione proposta in questo articolo, in modo sicuro, senza alcuna necessità di creare preventivamente una connessione VPN (un'operazione che talvolta mette in difficoltà il personale meno esperto).

La soluzione proposta, è inoltre perfettamente scalabile (per maggiori informazioni su come rendere la soluzione di posta elettronica esposta in questo articolo *scalabile*, invitiamo i lettori a leggere il capitolo terzo del libro The Book of IMAP), alcuni componenti di controllo, come ad esempio DSPAM o ClamAV possono venire *esternalizzati*, ovvero messi su postazioni server dedicate, di modo da *scaricare* il server di posta elettronica stesso.

Considerazioni sulla configurazione di Postfix

Per semplicità, in questo articolo, abbiamo adottato le mappe *hash* di Postfix. Questo per rendere da un lato più semplice la configurazione di Postfix, dall'altro per poterci concentrare su alcuni argomenti di solito trascurati dalla letteratura, come ad esempio la SquirrelMail o DSPAM. Vale la pena sottolineare, che fra tutte le mappe che può utilizzare Postfix, come ad esempio OpenLDAP o MySQL, le mappe *hash* risultano di gran lunga quelle con le migliori prestazioni, anche se hanno il difetto di richiedere il

caricamento della configurazione di Postfix ogni qual volta si apportano delle modifiche alle mappe stesse. Sarà premura degli autori, approfondire l'integrazione di Postfix con MySQL ed OpenLDAP in un apposito articolo dedicato a questo argomento.

Considerazioni sulle quote disco delle Mailbox

Nel corso della configurazione di Postfix che è stata proposta in questo articolo, non abbiamo abilitato la gestione delle quote disco. L'utilizzo delle quote disco delle Mailbox, ovvero la possibilità di limitare la dimensione massima, in byte o in numero di messaggi, che una Mailbox può raggiungere, può essere effettuato in quattro modi distinti. Il primo consiste nell'applicare una patch alla versione installata di Postfix e quindi escludere, di fatto, questo pacchetto dalle normali procedure di aggiornamento della distribuzione Debian (per sapere che ovviare a questo problema, consigliamo la lettura del libro The Book of IMAP); la patch è disponibile sul sito Postfix VDA

Il secondo metodo consiste nello sfruttare il comando `maildrop` che si trova a corredo del programma Courier. Il comando `maildrop` permette di impostare quote sia sul numero massimo di messaggi archiviabili all'interno di una Mailbox, sia sul numero massimo di byte che una Mailbox può occupare su di un disco. Il comando `maildrop` è poi in grado di inviare un messaggio di posta al proprietario della Mailbox per informarlo che il limite imposto dalla quota è prossimo all'essere raggiunto. In questo secondo caso non è necessario attivare alcuna configurazione particolare e pertanto tutte le procedure di aggiornamento dei programmi possono essere mantenute all'interno dei normali cicli di aggiornamento della distribuzione Debian.

Il terzo metodo, più semplice, ma limitato è utilizzare in Postfix l'opzione `mailbox_size_limit`. Questo permette di specificare la dimensione massima individuale di una mailbox o di un singolo file se si utilizza il formato maildir. Un messaggio destinato ad una mailbox che ha superato la dimensione massima, viene rimandato al mittente con un errore generico di *write error*. Non viene notificato nulla al destinatario del messaggio. Di default il valore è impostato a *51200000 bytes*.

Il quarto metodo consiste nell'utilizzare il comando `deliverquta`. Questo comando consente di impostare gli stessi limiti che si possono realizzare col comando `maildrop`.

Bisogna sottolineare, però, che tutti i metodi di quota citati, fanno utilizzo delle capacità di quota espresse dal formato Maildir. Quando si utilizzano le quote, bisogna stare poi attenti a non imporre quote troppo piccole, in quanto si espone il proprietario della Mailbox ad eventuali attacchi di servizio (*Denial-Of-Service*), soprattutto, quando, come nel articolo esposto, i messaggi di SPAM vengono comunque inviati alla Mailbox.

Accanto ai metodi di quota citati, andrebbe messo in piedi un sistema per limitare le capacità d'invio di una persona quando supera un dato limite di spazio disco. Questa soluzione, è di norma ben più persuasiva di un qualunque limite sullo spazio disco utilizzato.

Bibliografia

Nella stesura di questo articolo, gli autori hanno fatto riferimento ai seguenti testi:

- *Ralf Hildebrandt*, *Patrick Koetter*,
  The book of Postfix State-Of-The-Art Message Transport
  (No Starch Press, `ISBN: 1-59327-001-1`);
-
- *Magnus Bäck*, *Patrick Ben Koetter*, *Ralf Hilderbrandt ed altri*,
  Linux Email, Set up and Run a Small Office Email Server
  (PACKT Publishing, `ISBN: 1-904811-37-X`);

-
- *Jonathan A. Zdziarski*,
  Ending SPAM, Bayesian Content Filtering and The Art Of Statistical Language Classification
  (No Starch Press, ISBN: 1-59327-052-6);
-
- *Peer Heinlein*, *Peer Hartleben*
  The Book of IMAP
  (No Starch Press, ISBN: 978-3-937514-11-6);