RHX Studio Associato
Piazza Resistenza, 5/1
31053 Pieve di Soligo (TV)
e-mail: info@rhx.it
Tel. +39 0437 3730899
FAX +39 0437 3731180
www.rhx.it

Phamm HOWTO

Indice

Introduzione

Convenzioni

Le seguenti convenzioni sono state utilizzate per la stesura della presente documentazione:

1) Parti di testo estrapolate da file [1] e path assoluti o relativi di directory sono riportate come:

```
testo a lunghezza costante
```

2) I link di riferimento (URLs) vegono riportati come mostrato nel seguente esempio:

[*http://www.debian.org/*]

3) I comandi da eseguire a bash si suddividono in:

- comandi da eseguire con **privilegi di root** preceduti dal carattere "#"
- comandi da eseguire a **livello utente** preceduti dal carattere "$"

4) I comandi da eseguire a bash vengono riportati come nell'esempio di seguito:

```
# apt-get update
```

5) Tutti gli **screenshot** mostrati di seguito evidenziano in rosso la risposta data nel nostro caso.

[1] che indicano esempi di codice o di configurazioni

Capitolo 1

Analisi della struttura

Si prevede nella redazione delle access control list [1] (ACL) di LDAP, la gestione di tre ruoli di accesso:

1. admin (root dn)
2. postmaster (accesso a tutto il proprio dominio)
3. utente finale (accesso unicamente ai propri dati).

In Figura 1.1 la struttura che sarà realizzata seguendo questa documentazione.

[1] file che stabilisce i diritti di accesso a file e directory per ciascuna tipologia di utente

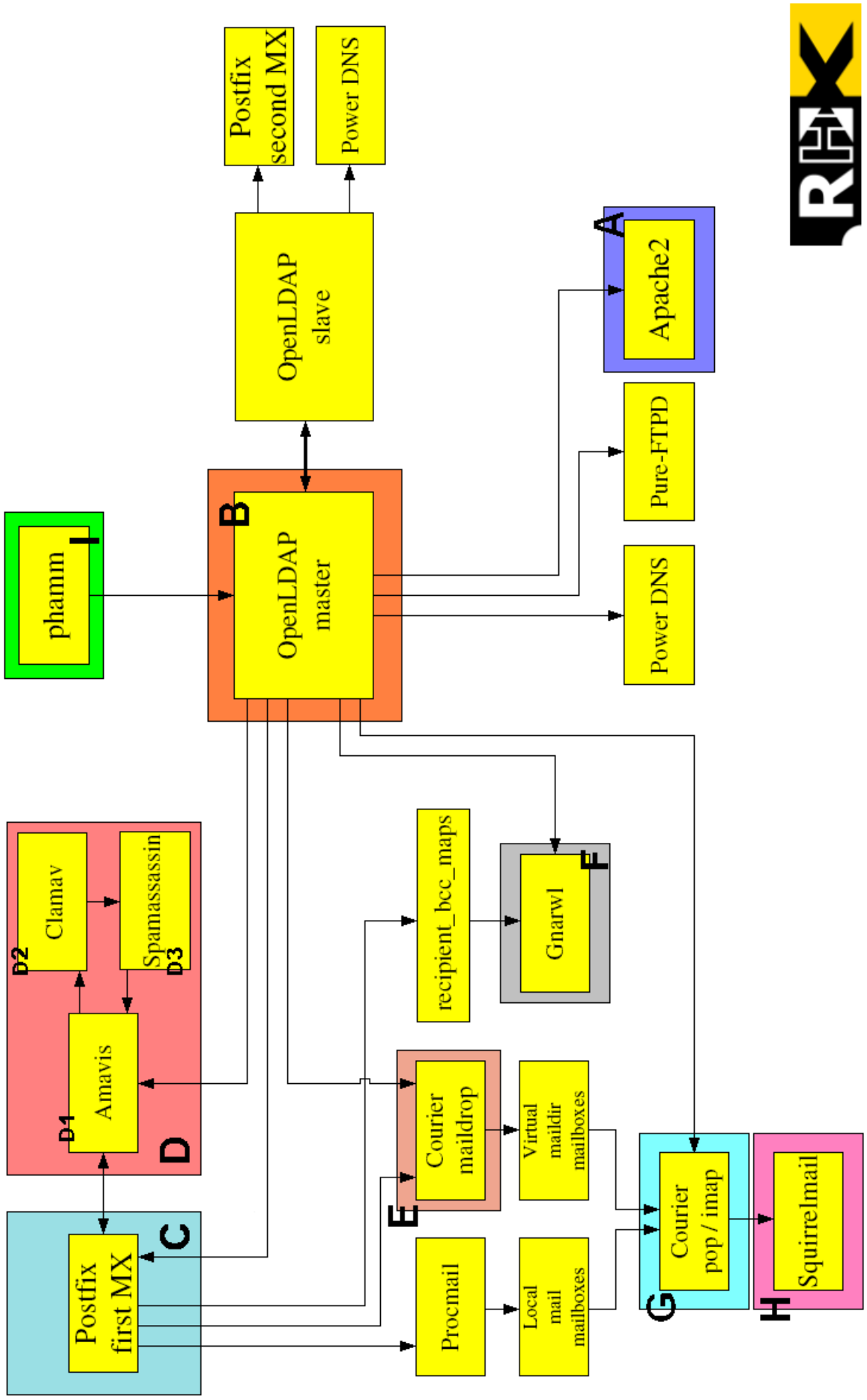

Figura 1.1: Schema Struttura

Capitolo 2

Sistema Operativo di partenza

Per l'implementazione di tale sistema vengono utilizzati esclusivamente strumenti opensource, basati sulla distribuzione DEBIAN LENNY del sistema operativo GNU/LINUX.

Editiamo il file `/etc/apt/sources.list` aggiungendo le clausole "contrib" e "non-free" affinchè risulti come riportato di seguito:

```
deb http://debian.fastweb.it/debian/ lenny main contrib non-free
deb-src http://debian.fastweb.it/debian/ lenny main contrib non-free

deb http://security.debian.org/ lenny/updates main contrib non-free
deb-src http://security.debian.org/ lenny/updates main contrib non-free
```

Salvare il file e aggiornare il sistema con:

```
# apt-get update
```

Aggiornare eventualmente il sistema con:

```
# apt-get upgrade
```

e a questo punto dovremmo essere pronti per iniziare con l'implementazione della struttura di Figura 1.1.

Capitolo 3

Analisi ed installazione dei pacchetti

Si tiene unicamente conto dei pacchetti minimi ed indispansabili allo scopo di ottenere il funzionamento del software **Phamm**. Analizziamo ora di seguito i vari blocchi evidenziati in Figura 1.1 riportando per ognuno una breve descrizione dalla loro funzionalità e dei PACKAGE da installare per ottenere la loro implementazione con eventuale analisi delle scelte di configurazione.

3.1 Blocco A: Apache2

[*http://www.apache.org/*]

La piattaforma server Web dove gireranno le applicazioni web della struttura ovvero l'interfaccia grafica di PHAMM e di SQUIRRELMAIL analizzate in seguito. Oltre ad APACHE2 viene installato anche il modulo PHP5 ovvero il linguaggio con il quale sono scritte le stesse pagine web.
Installare:

```
# apt-get install apache2 libapache2-mod-php5 php5
```

3.2 Blocco B: OpenLdap

[*http://www.openldap.org/*]

OpenLDAP è il blocco che contiene tutte le informazioni relative ad ogni singolo utente organizzate in forma gerarchica. Oltre a ciò fornisce al sistema le "informazioni di lavoro", ovvero tutti i parametri di settaggio[1] dei blocchi ai quali è collegato.
Installare:

```
# apt-get install slapd ldap-utils
```

Prima di terminare l'installazione vengono richiesti dei parametri all'utente. In particolare compare una schermata che richiede la "`password di amministrazione`" con successiva conferma e completare le schermate che compaiono come di seguito:

[1] di ogni singolo utente o gruppi di essi

Figura 3.1: configurazione di slapd

Figura 3.2: configurazione di slapd

3.3 Blocco C: Postfix

[*http://www.postfix.org/*]

Postfix è un MTA (Mail Transfer Agent) ovvero un software che si occupa dello smistamento della posta elettronica basato su protocollo STMP.
Installare:

```
# apt-get install postfix postfix-ldap
```

Prima di terminare l'installazione vengo richiesti dei parametri di configurazione: completare come mostrato nelle figure 3.3 e analizzeremo una configurazione più approfondita nel prossimo capitolo.

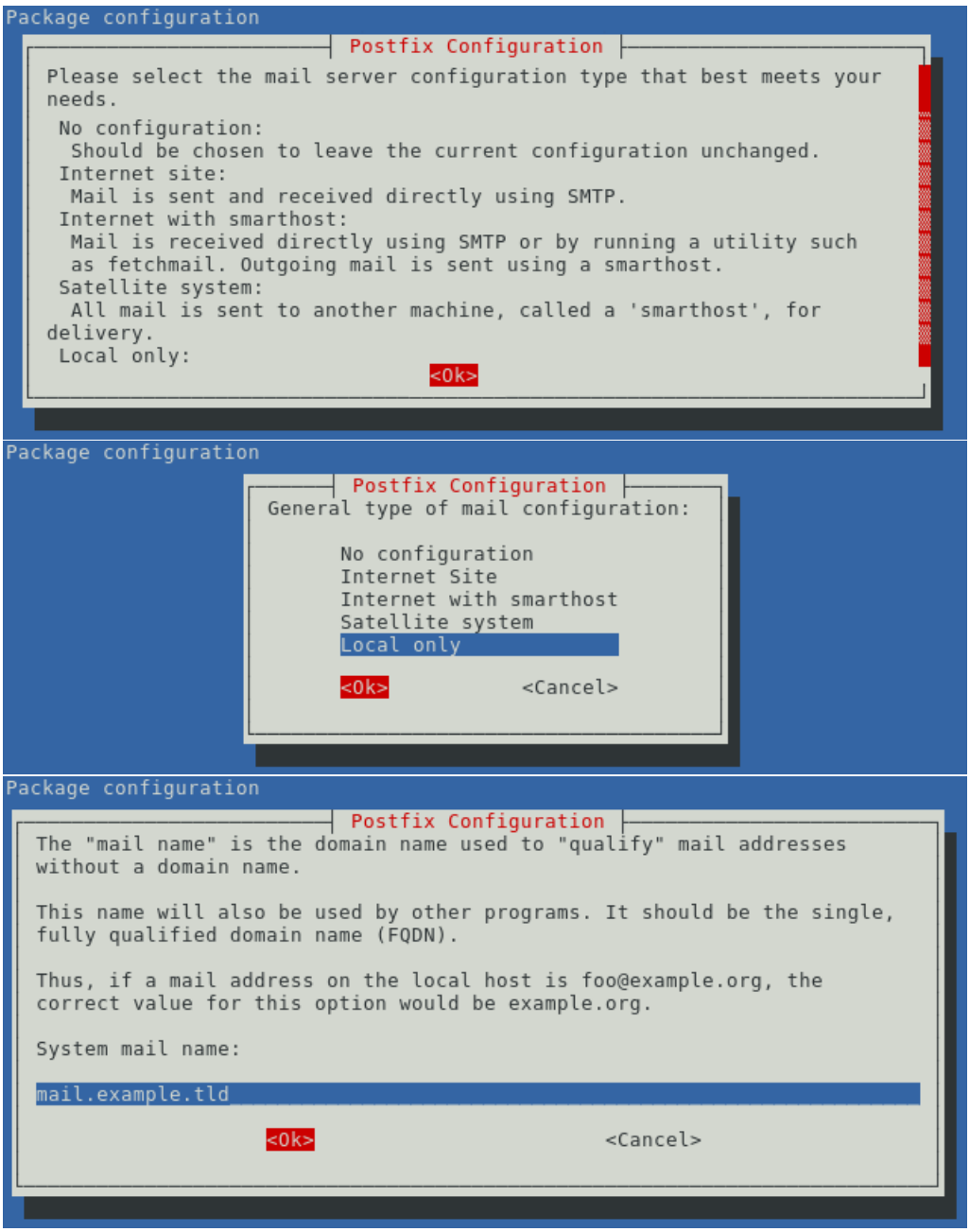

Figura 3.3: configurazione di postfix

3.4 Blocco D:

Sostanzialmente il blocco si occupa di riconoscere e scartare tutte le mail indesiderate a partire dalle mail *spam* per arrivare ai *virus*. Se una mail supera tutto il controllo a catena, che vedremo in dettaglio tra poco, significa che tornerà ”nelle mani” di Postfix che si occuperà poi di andarla a consegnare al/ai destinatario/i.

3.4.1 Blocco D1: Amavis

[*http://www.amavis.org/*]

Pacchetto che funge da interfaccia tra il servizio MTA (blocco C), clamav e spamassassin (blocchi D2 e D3). Installare:

```
# apt-get install amavisd-new libnet-ldap-perl
```

Analizzando i pacchetti si può notarne una sequenza di consigliati che nel nostro caso sono invece necessari: si tratta di algoritmi di compressione necessari ad Amavis per scompattare gli allegati delle mail che dovrà poi far analizzare ai blocchi successivi:

```
# apt-get install lha unrar zoo nomarch lzop cabextract rpm pax rar p7zip p7zip-rar
```

3.4.2 Blocco D2: Clamav

[*http://www.clamav.net/*]

Clam Antivirus è un toolkit anti-virus open source (GPL) per sistemi UNIX.
Lo scopo principale di questo software è l'integrazione con i software server di posta elettronica (in particolare per la scansione degli allegati).
In pratica prende le mail e ne fa un controllo antivirus che comprende anche un'analisi del *Phishing* [2].
Se la mail non viene scartata nemmeno in questo passaggio significa che è "buona" e viene rispedita ad Amavis.
Installare:

```
# apt-get install clamav-daemon clamav-freshclam
```

- Daemon è un programma eseguito in background, senza che sia sotto il controllo diretto dell'utente
- Freshclam è il software che si occupa di aggiornare automaticamente il database delle firme dei virus scaricandone una lista aggiornata da web.

3.4.3 Blocco D3: Spamassassin

[*http://spamassassin.apache.org/*]

Blocco che si occupa di analizzare la mail che gli viene passata da amavis e cerca di capire se è una mail spam, analizzando il suo contenuto. La sua funzione è tipicamente da "filtro".
Installare:

```
# apt-get install spamassassin
```

3.5 Blocco E: Courier maildrop

[*http://www.courier-mta.org/maildrop/*]

Questo blocco rappresenta un Mail Delivery Agent (MDA) ovvero un software che accetta in entrata messaggi e-mail e li distribuisce alle mailbox destinatarie.
Oltre a cio, effettua anche un controllo di **quota** [3] segnalando al destinatario un'eventuale **superamento di quota**.
Installare:

```
# apt-get install courier-maildrop courier-authlib-ldap courier-authdaemon
```

Prima di terminare l'installazione viene richiesto se si desidera creare directories per l'amministrazione web-based come mostrato in Figura 3.4.

[2] mail utilizzate per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità.
[3] il blocco "Virtual maildir mailboxes" ovvero il supporto fisico (HDD) dove la mail verrà salvata

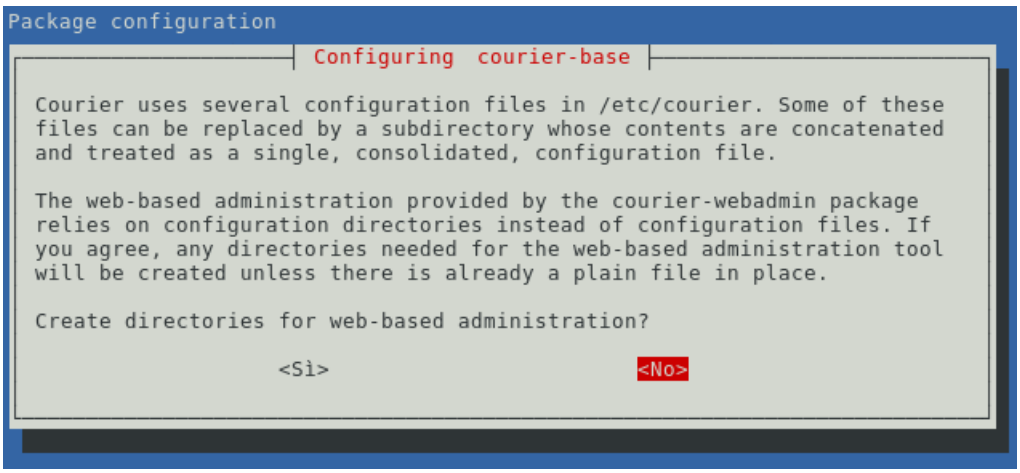

Figura 3.4: web-based administration

Dare il comando:

```
# maildrop -v
```

e controllare che le voci `Courier Authentication Library extension` e `Maildir quota extension` siano abilitate come mostrato di seguito:

```
maildrop 2.0.4 Copyright 1998-2005 Double Precision, Inc.
GDBM extensions enabled.

Courier Authentication Library extension enabled.
Maildir quota extension enabled.

This program is distributed under the terms of the GNU General Public
License. See COPYING for additional information
```

3.6 Blocco F: Gnarwl

[*http://www.home.unix-ag.org/patrick/index.php?gnarwl*]

Si tratta di un servizio E-MAIL AUTORESPONDER basato su LDAP. Questo servizio prende il nome di *vacation* nello schema LDAP.
Installare:

```
# apt-get install gnarwl
```

3.7 Blocco G: Courier pop / imap

[*http://www.courier-mta.org/*]

Aggiungiamo ora al nostro sistema i protocolli rispettivamente di consegna (POP) o di visualizzazione (IMAP) delle mail. Installare:

```
# apt-get install courier-pop courier-imap
```

Qualora lo si ritenga necessario si possono integrare i precedenti con il protocollo Secure Socket Layer [4] (SSL). Installare:

```
# apt-get install courier-pop-ssl courier-imap-ssl
```

Prima di terminare l'installazione appare un messaggio in Figura 3.5.

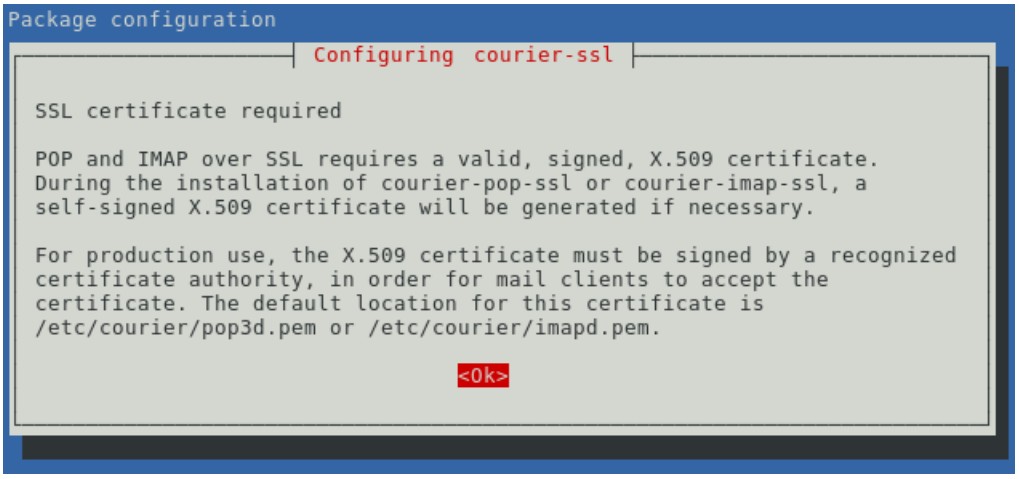

Figura 3.5: SSL

3.8 Blocco H: Squirrelmail

[*http://www.squirrelmail.org/*]

SquirrelMail consente di accedere ad un account di posta elettronica utilizzando un comune browser HTML. Installare:

```
# apt-get install squirrelmail
```

3.9 Blocco I: Phamm

[*http://www.phamm.org/*]

```
# apt-get install phamm
```

Prima di terminare l'installazione completare la schermate che appaiono come mostrato in Figura 3.6.

[4] protocollo per realizzare comunicazioni cifrate su Internet: questo per garantire affidabilità e riservatezza delle comunicazioni web

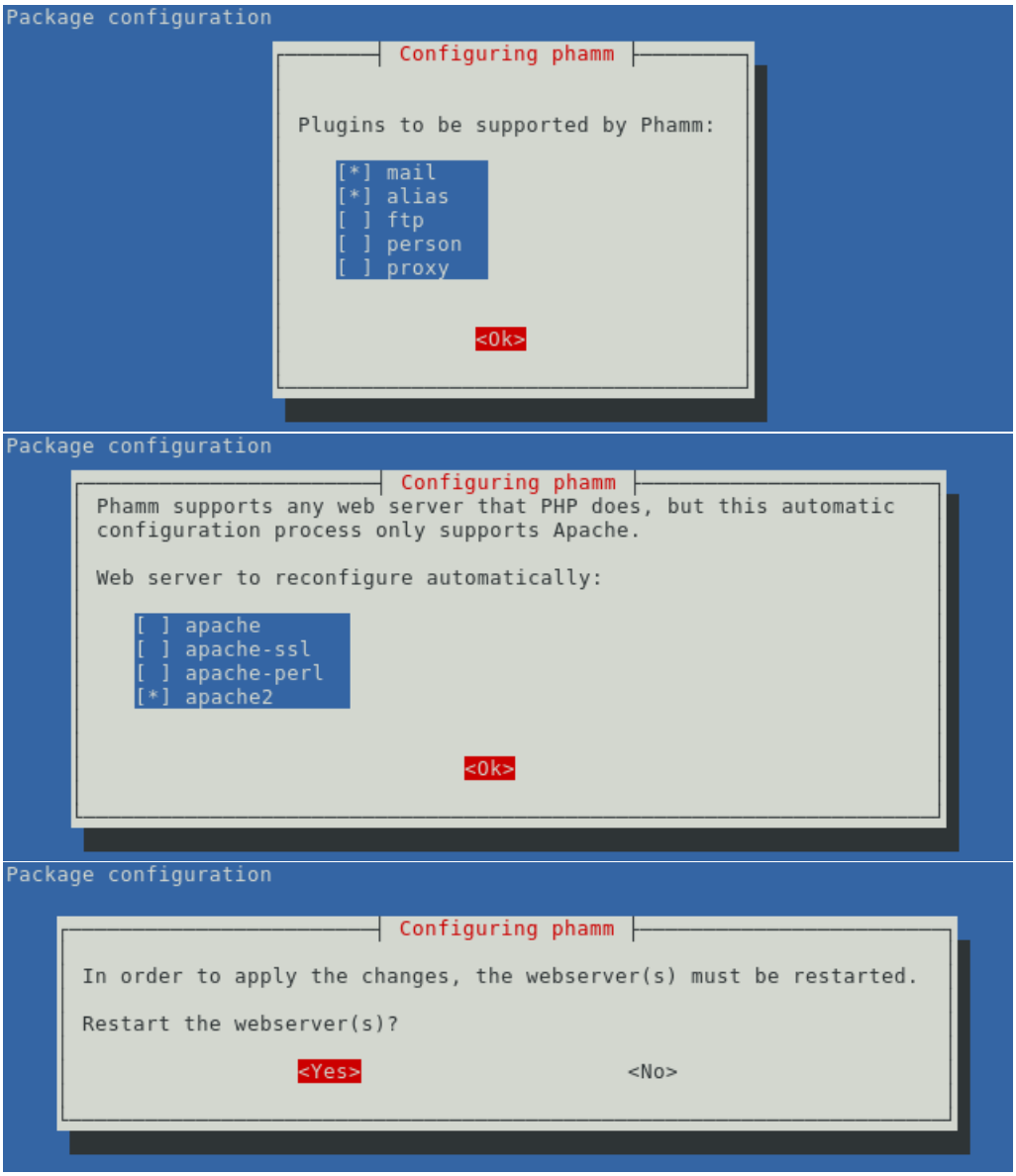

Figura 3.6: configurazione di phamm

Capitolo 4

Configurazioni

Si consiglia di creare una copia di backup di tutti i file che andranno modificati in seguito utilizzando il comando:

cp *[path_assoluto]/[nome_file] [path_assoluto]/[nome_file].orig*

Tutte le modifiche riportate di seguito, relative ai file di configurazione, vengono analizzate in ordine; ovvero per ogni singolo file sono descritte la modifiche da apportare scorrendo il listato dalla prima riga in poi.

4.1 Creazione "Utente Vmail"

» Creare l'utente vmail

adduser –disabled-password –disabled-login vmail

id vmail

dovrebbe comparire una cosa simile

```
uid=1002(vmail) gid=1002(vmail) gruppi=1002(vmail)
```

(tenere nota dell'UID 1002, in questo caso, che servirà come parametro nella configurazione del file `/etc/postfix/main.cf`)....

» Divenire utente vmail con il comando:

su - vmail

» Creare le tre directory seguenti:

$ mkdir bin tmp domains

» Al momento non sono disponibili tutti i pacchetti .deb quindi i 2 passaggi seguenti richiedono l'utilizzo del tar.gz

- scaricare con il seguente comando il sorgente
  $ wget -c http://open.rhx.it/phamm/daily/phamm05-current.tar.gz

- decomprimere il file scaricato
  $ tar xzvf phamm05-current.tar.gz

- copiare il file cleaner.sh e il file make-mail.sh in ∼/bin
  $ cp phamm05-`date +%F`/tools/cleaner.sh ∼/bin
  $ cp phamm05-`date +%F`/tools/make-mail.sh ∼/bin

  Il file cleaner.sh ci consente di cancellare il dominio o la mail con il parametro di LDAP `delete=TRUE` sia dalla base dati LDAP che dal file system.
  Tale operazione può essere impostata in cron agli intervalli desiderati.

  Il file make-mail.sh ci consente di creare la struttura della mail se usiamo come transport `maildrop` all'invio della prima mail.
  Tale operazione può essere impostata in cron con una frequenza abbastanza elevata (non sappiamo quando vengano create delle mail)

4.2 Blocco B: Configurazione OpenLdap

» Modificare il file `/etc/ldap/slapd.conf`

- aggiungere sotto la sezione `# Schema and objectClass definitions`

```
include         /etc/ldap/schema/amavis.schema
include         /etc/ldap/schema/phamm.schema
include         /etc/ldap/schema/ISPEnv2.schema
include         /etc/ldap/phamm.acl
```

- commentare (###) le righe successive a

```
# admin entry below
# These access lines apply to database #1 only


###access to attrs=userPassword,shadowLastChange
###        by dn="cn=admin,dc=example,dc=tld" write
###        by anonymous auth
###        by self write
###        by * none
```

- commentare (###) la riga successiva a

```
# want SASL (and possible other things) to work
# happily.


###access to dn.base="" by * read
```

- commentare (###) le righe successive a

```
# The admin dn has full write access, everyone else
# can read everything.


###access to *
###        by dn="cn=admin,dc=example,dc=tld" write
###        by * read
```

4.3 Blocco C: Configurazione Postfix

» Qualora postfix fosse già installato nel vostro sistema si consiglia di dare il comando:
dpkg-reconfigure postfix
e settare ”No configuration”

» Modificare il file `# etc/postfix/master.cf`:

- sostituire alla riga 9

```
smtp inet n - - - - smtpd
```

con

```
smtp inet n - n - - smtpd
```

- sostituire alla riga 59

```
flags=DRhu user=vmail argv=/usr/bin/maildrop -d $recipient
```

con

```
flags=Rhu user=daemon argv=/usr/bin/maildrop -w 91 -d $recipient
```

- aggiungere alla riga 78

```
# for autoresponder
gnarwl    unix  -       n       n       -       -       pipe
   flags=F  user=vmail argv=/usr/bin/gnarwl -a ${user}@${nexthop} \
   -s ${sender}
# only if you use amavisd-new for content filtering
smtp-amavis   unix - - n - 3 smtp
   -o smtp_data_done_timeout=1200
   -o disable_dns_lookups=yes
127.0.0.1:10025 inet n - n - - smtpd
   -o content_filter=
   -o local_recipient_maps=
   -o relay_recipient_maps=
```

» Modificare il file `# etc/postfix/main.cf`:

- commentare (###)le righe successive ad
  `# TLS parameters`

```
###smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
###smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
###smtpd_use_tls=yes
###smtpd_tls_session_cache_database = btree:${queue_directory}/ \
 smtpd_scache
###smtp_tls_session_cache_database = btree:${queue_directory}/ \
 smtp_scache
```

- sostituire alla riga 30
  `myhostname = [hostname server]`

  ovvero il nome del vostro server con l'FQDN del nostro caso

```
myhostname = mail.example.tld
```

- aggiungere alla riga 41

```
# main.cf specific for phamm

#  Copyright (c) 2005 Alessandro De Zorzi, Mirko Grava
#   <phamm@rhx.it> http://phamm.rhx.it/
#
#  Permission is granted to copy, distribute and/or modify this document
#  under the terms of the GNU Free Documentation License, Version 1.2
#  or any later version published by the Free Software Foundation;
#  A copy of the license in DOCS.LICENSE file.

ldap_bind_dn = cn=phamm,o=hosting,dc=example,dc=tld
ldap_bind_pw = rhx
ldap_search_base = o=hosting,dc=example,dc=tld
ldap_domain = dc=example,dc=tld
ldap_server_host = localhost
ldap_server_port = 389

# transports
transport_server_host = $ldap_server_host
transport_search_base = $ldap_search_base
transport_query_filter = (&(&(vd=%s)(objectClass=VirtualDomain)) \
(accountActive=TRUE)(delete=FALSE))
transport_result_attribute = postfixTransport
transport_cache = no
transport_bind = yes
transport_scope = one
transport_bind_dn = $ldap_bind_dn
transport_bind_pw = $ldap_bind_pw
```

```
# aliases
aliases_server_host = $ldap_server_host
aliases_search_base = $ldap_search_base
aliases_query_filter=(&(&(objectClass=VirtualMailAlias)(mail=%s)) \
(accountActive=TRUE))
aliases_result_attribute = maildrop
aliases_bind = yes
aliases_cache = no
aliases_bind_dn = $ldap_bind_dn
aliases_bind_pw = $ldap_bind_pw

# VirtualForward
virtualforward_server_host = $ldap_server_host
virtualforward_search_base = $ldap_search_base
virtualforward_query_filter = (&(&(objectClass=VirtualMailAccount) \
(mail=%s))(vacationActive=FALSE)(forwardActive=TRUE) \
(accountActive=TRUE)(delete=FALSE))
virtualforward_result_attribute = maildrop
virtualforward_bind = yes
virtualforward_cache = no
virtualforward_bind_dn = $ldap_bind_dn
virtualforward_bind_pw = $ldap_bind_pw

# Accounts
accounts_server_host = $ldap_server_host
accounts_search_base = $ldap_search_base
accounts_query_filter = (&(&(objectClass=VirtualMailAccount) \
(mail=%s))(forwardActive=FALSE)(accountActive=TRUE)(delete=FALSE))
accounts_result_attribute = mailbox
accounts_cache = no
accounts_bind = yes
accounts_bind_dn = $ldap_bind_dn
accounts_bind_pw = $ldap_bind_pw

accountsmap_server_host = $ldap_server_host
accountsmap_search_base = $ldap_search_base
accountsmap_query_filter = (&(&(objectClass=VirtualMailAccount) \
(mail=%s))(forwardActive=FALSE)(accountActive=TRUE)(delete=FALSE))
accountsmap_result_attribute = mail
accountsmap_cache = no
accountsmap_bind = yes
accountsmap_bind_dn = $ldap_bind_dn
accountsmap_bind_pw = $ldap_bind_pw

# virtual quota
quota_server_host = $ldap_server_host
quota_search_base = $ldap_search_base
quota_query_filter = (&(&(objectClass=VirtualMailAccount) \
(mail=%s))(accountActive=TRUE)(delete=FALSE))
quota_result_attribute = quota
quota_cache = no
quota_bind = yes
quota_bind_dn = $ldap_bind_dn
```

```
quota_bind_pw = $ldap_bind_pw

# Mail to reply for gnarwl and mail to forward during vacation
recipient_bcc_maps = ldap:vfm
vfm_server_host = $ldap_server_host
vfm_search_base = $ldap_search_base
vfm_query_filter = (&(&(objectClass=VirtualMailAccount) \
(mail=%s))(vacationActive=TRUE)(forwardActive=FALSE) \
(accountActive=TRUE)(delete=FALSE))
vfm_result_attribute = mailAutoreply
vfm_cache = no
vfm_bind = yes
vfm_bind_dn = $ldap_bind_dn
vfm_bind_pw = $ldap_bind_pw

# transport_maps
maildrop_destination_concurrency_limit = 2
maildrop_destination_recipient_limit = 1
gnarwl_destination_concurrency_limit = 1
gnarwl_destination_recipient_limit = 1
transport_maps = hash:/etc/postfix/transport, ldap:transport
mydestination = $transport_maps, localhost, $myhostname, \
localhost.$mydomain, $mydomain
virtual_alias_maps = hash:/etc/postfix/virtual, \
ldap:virtualforward, ldap:aliases, ldap:accountsmap

# virtual accounts for delivery
virtual_mailbox_base = /home/vmail/domains
virtual_mailbox_maps = ldap:accounts
virtual_minimum_uid = 1002
virtual_uid_maps = static:1002
virtual_gid_maps = static:1002

local_recipient_maps = proxy:unix:passwd.byname, $alias_maps, \
$virtual_mailbox_maps
```

- verificare inoltre che l'ultima parte da inserire del punto precedente, sotto la voce `# virtual accounts for delivery` contenga lo stesso **id** del risultato ottenuto dal comando **# id vmail** dato nel primo punto della configurazione dell'utente vmail:

```
virtual_minimum_uid = 1002
virtual_uid_maps = static:1002
virtual_gid_maps = static:1002
```

» Creare un file di nome `transport` in `/etc/postfix/` con il seguente comando:

 # echo ".autoreply gnarwl:" » /etc/postfix/transport

» Creare il `transport.db` nella stessa directory con il comando:

```
# postmap transport
```

» Riavviare postfix con il comando:

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

4.4 Blocco D1: Configurazione Amavis

» Inserire nel file `/etc/hostname`

```
mail.example.tld
```

» Inserire nella seconda riga del file `/etc/hosts`

```
127.0.1.1   mail.example.tld
```

» Modificare il file `/etc/amavis/conf.d/01-debian`[1]:

- togliere il commento (#) alla riga 36
  `$unrar = ['rar', 'unrar']; #disabled (non-free, no security support)`

- mettere il commento (#) alla riga 37
  `#$unrar = undef;`

- togliere il commento (#) alla riga 39
  `$lha = 'lha'; #disabled (non-free, no security support)`

- mettere il commento (#) alla riga 40
  `#$lha = undef;`

» Modificare il file `/etc/amavis/conf.d/15-content_filter_mode`[2]:

- togliere il commento (#) alle righe 11 e 12
  ```
  @bypass_virus_checks_maps = (
  \%bypass_virus_checks,\@bypass_virus_checks_acl,\$bypass_virus_checks_re);
  ```

- togliere il commento (#) alle righe 20 e 21
  ```
  @bypass_spam_checks_maps = (
  \%bypass_spam_checks,\@bypass_spam_checks_acl,\$bypass_spam_checks_re);
  ```

[1] le modifiche apportate attivano il supporto di amavis per i file compressi con *rar* e *lha*
[2] le modifiche apportate attivano il controllo *antivirus* e *antispam*

» Modificare il file `/etc/amavis/conf.d/50-user`:

- dopo le righe commentate

```
# See /usr/share/doc/amavisd-new/ for documentation and examples of
# the directives you can use in this file
#
```

- aggiungere

```
$warnvirusrecip = 1;

@bypass_virus_checks_acl = qw("localhost.$mydomain");
#
$enable_ldap = 1;
$default_ldap = {
        hostname => [ 'localhost' ],
        port => 389,
        version => 3,
        timeout => 120,
        tls => 0,
        scope => 'sub',
        base => 'o=hosting,dc=example,dc=tld',
        bind_dn => 'cn=admin,dc=example,dc=tld',
        bind_password => 'rhx',
        query_filter => '(&(objectClass=amavisAccount)(mail=%m))'
};
```

» Riavviare amavis con il comando:

/etc/init.d/amavis restart

e controllare nei log di sistema se sono stati caricati i codici di LDAP, dell'antispam e dell'antivirus, aprendo il file `/var/log/syslog` e controllando la presenza delle seguenti righe:

```
amavis[6202]:  Lookup::LDAP code loaded
amavis[6202]:  ANTI-VIRUS code loaded
amavis[6202]:  ANTI-SPAM code loaded
amavis[6202]:  ANTI-SPAM-SA code loaded
amavis[6202]:  Unpackers code loaded
```

4.5 Blocco D2: Configurazione Clamav

» In questo blocco si deve solamente verificare che l'utente clamav sia facente parte del gruppo di amavis con la seguente procedura:

id clamav

ed il risultato dovrebbe essere il seguente (mancante del gruppo amavis):

```
uid=111(clamav) gid=121(clamav) gruppi=121(clamav)
```

diamo quindi il comando

```
# usermode -a -G amavis clamav
```

e ora con

```
# id clamav
```

dovremmo ottenere

```
uid=111(clamav) gid=121(clamav) gruppi=121(clamav),120(amavis)
```

» Riavviare clamav:

```
# /etc/init.d/clamav-daemon restart
# /etc/init.d/clamav-freshclam restart
```

4.6 Blocco D3: Configurazione Spamassassin

» Modificare il file `/etc/default/spamassassin`:

- modificare la voce ENABLED alla riga 8 sotto la sezione

```
# Change to one to enable spamd

ENABLED=1
```

» Riavviare spamassassin:

```
# /etc/init.d/clamav-daemon restart
```

4.7 Blocco E, G: Configurazione Courier

» Modificare il file `/etc/courier/authdaemonrc`:

- sostituire alla riga 27

  `authmodulelist="authpam"`

  con

  `authmodulelist="authldap"`

» Modificare il file `/etc/courier/authldaprc`:

- creare una copia di backup del file originale con il comando:

  # cp /etc/courier/authldaprc /etc/courier/authldaprc.orig

- inserire ora le seguenti righe nel file `authldaprc`

```
LDAP_URI    ldap://localhost
LDAP_PORT                389
LDAP_PROTOCOL_VERSION    3
LDAP_BASEDN              o=hosting,dc=example,dc=tld
LDAP_BINDDN              cn=phamm,o=hosting,dc=example,dc=tld
LDAP_BINDPW              rhx
LDAP_TIMEOUT             5
LDAP_AUTHBIND            1
LDAP_MAIL                mail
LDAP_FILTER              (accountActive=TRUE)
LDAP_GLOB_UID            vmail
LDAP_GLOB_GID            vmail
LDAP_HOMEDIR             vdHome
LDAP_MAILDIR             mailbox
LDAP_MAILDIRQUOTA        quota
LDAP_FULLNAME            cn
LDAP_CRYPTPW             userPassword
LDAP_DEREF               never
LDAP_TLS                 0
```

» Riavviare courier:

/etc/init.d/courier-authdaemon restart

4.8 Blocco F: Configurazione Gnarwl

» Modificare il file `/etc/gnarwl.cfg`:

- creare una copia di backup del file originale con il comando:

  # cp /etc/gnarwl.cfg /etc/gnarwl.cfg.orig

- inserire ora le seguenti righe nel file `gnarwl.cfg`

```
map_sender $sender
map_receiver $recepient
map_subject $subject
map_field $begin vacationStart
map_field $end vacationEnd
map_field $fullname cn
map_field $deputy vacationForward
map_field $reply mail
server localhost
port 389
scope sub
login cn=phamm,o=hosting,dc=example,dc=tld
password rhx
protocol 0
base dc=example,dc=tld
queryfilter (&(mailAutoreply=$recepient)(vacationActive=TRUE))
result vacationInfo
blockfiles /var/lib/gnarwl/block/
umask 0644
blockexpire 48
mta /usr/sbin/sendmail -F $recepient -t $sender
maxreceivers 64
maxheader 512
charset ISO8859-1
badheaders /var/lib/gnarwl/badheaders.db
blacklist /var/lib/gnarwl/blacklist.db
forceheader /var/lib/gnarwl/header.txt
forcefooter /var/lib/gnarwl/footer.txt
recvheader To Cc
loglevel 3
```

» Dare i seguenti comandi:

```
# chmod 600 /etc/gnarwl.cfg
# chown vmail:vmail /etc/gnarwl.cfg
# chown vmail:vmail /var/lib/gnarwl/block/
```

» Modificare il file `/var/lib/gnarwl/footer.txt`:

- sostituire alla riga 3

  ```
  $fullname <$recepient>
  ```

con

```
$fullname <$reply>
```

» Modificare il file `/var/lib/gnarwl/header.txt`:

- sostituire alla riga 1

  ```
  From:  $fullname <$recepient>
  ```

  con

  ```
  From:  $fullname <$reply>
  ```

4.9 Blocco I: Configurazione Phamm

Si ricorda che sarebbe opportuno cambiare la password del cn PHAMM [3].

» Popoliamo la base dati dando il comando:

```
# ldapadd -v -x -D "cn=admin,dc=example,dc=tld" -W -h localhost -f \
/usr/share/doc/phamm-ldap/ldif/sample-hosting.ldif
```

» Modificare il file `/etc/phamm/config.inc.php`:

- mettere alla riga 43 sotto il commento

  ```
  // The container
  define ('SUFFIX','dc=example,dc=tld');
  ```

- mettere alla riga 46 sotto il commento

  ```
  // The admin bind dn (could be rootdn)
  define ('BINDDN','cn=admin,dc=example,dc=tld');
  ```

[3] per i ns. esempi si utilizza "rhx" che sarebbe quella definita di default

Capitolo 5

Test finale

Bene arrivati a questo punto potete digitare sul vostro browser il seguente URL:

```
http://ipserver/phamm
```

dove ipserver deve essere sostituito dall'indirizzo IP del server che ospita Phamm.

Enjoy