ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Torino

INFN/TC-09/09
25 Novembre 2009

MANUALE DI INSTALLAZIONE DI UN SERVIZIO DI POSTA ELETTRONICA COMPLETO DI FILTRI ANTI-VIRUS E ANTI-SPAM CON POLITICA DI IMPLEMENTAZIONE OPT-OUT

Alberto D'Ambrosio

INFN-Sezione di Torino, c/o Dip. di Fisica dell'Università

Abstract

Con la seconda ristrutturazione dei servizi di calcolo centrali della Sez. INFN di Torino e dei Dipartimenti di Fisica dell'Università, considerato il notevole aumento della frazione di spam sul totale di E-Mail consegnate agli utenti, a Settembre 2007 si è colta l'occasione per modificare la politica di implementazione dei filtri anti-spam/virus da OPT-IN ad OPT-OUT, con inasprimento di alcune funzionalità di default rispetto al progetto iniziale (INFN/TC-05/09 del 01/07/2005), per redigerne un manuale dettagliato di installazione. Le istruzioni qui contenute hanno validità generale per qualunque piattaforma Unix.

Published by ***SIS–Pubblicazioni***
Laboratori Nazionali di Frascati

INTRODUZIONE

Negli ultimi anni, tra i Servizi Informatici Centrali di una generica Sez./Lab. INFN, il Servizio di Posta Elettronica è sicuramente quello che ha assunto maggior importanza per lo svolgimento quotidiano del lavoro di Ricerca e/o Amministrazione del Personale INFN e dei Dipartimenti Universitari.

I vari Sw di gestione del flusso delle E-Mail hanno funzionalità sempre più sofisticate, e ciò sia per motivi di ottimizzazione delle prestazioni e dell'efficacia che di sicurezza dei mail-server.

Le dilaganti piaghe dei Virus e dello SPAM, poi, hanno costretto un po` tutti gli amministratori di sistema ad adottare delle contromisure per far sì che all'utente finale vengano consegnati, per quanto possibile, solo messaggi "buoni".

Inoltre, lo stesso concetto di E-Mail "buona" è divenuto così soggettivo da renderne complicata la gestione a livello di filtri.

Così, con la seconda ristrutturazione dei servizi di calcolo centrali della Sez. INFN di Torino e dei Dipartimenti di Fisica dell'Università, considerato il notevole aumento della frazione di spam sul totale di E-Mail consegnate agli utenti, a Settembre 2007 si è colta l'occasione per modificare la politica di implementazione dei filtri anti-spam/virus da OPT-IN ad OPT-OUT, con inasprimento di alcune funzionalità di default rispetto al progetto iniziale (INFN/TC-05/09 del 01/07/2005), per redigerne un manuale dettagliato di installazione. Le istruzioni qui contenute hanno validità generale per qualunque piattaforma Unix.

1 PANORAMICA

Il Servizio di Posta Elettronica che abbiamo implementato ha la seguente struttura:

- MTA
  - ✓ Sendmail 8.13.1
    - OpenSSL 0.9.7a
    - STARTTLS (TLSv1/SSLv3)
    - FEATURE (`greet_pause')
    - Milter Greylist 4.0
    - AMaViS (amavisd-new 2.4.5)
      - Perl 5.8.5
      - Python 2.2.2
      - ClamAV Anti-virus 0.91.2
      - SpamAssassin 3.2.4
      - Razor 2.36
      - Pyzor 0.4.0
      - DCC (dccifd) 1.3.57
      - MySQL (client + server)
- LDA
  - ✓ Procmail 3.22
- MUA
  - ✓ Alpine 2.00
  - ✓ Thunderbird 2.0.0.23
  - ✓ SeaMonkey 2.0
  - ✓ SquirrelMail
- IMAPS
  - ✓ Stunnel 4.04
  - ✓ OpenSSL 0.9.7a
  - ✓ Imapd 2007a1
- Client per backup automatici
  - ✓ HP Data Protector Client A.06.10

N.B.: In generale, l'approccio con le versioni dei vari Sw è di tipo "conservativo", legato alla politica del s.o. utilizzato (**RHEL 4.x**).

2 CARATTERISTICHE

Le caratteristiche principali di questa implementazione del Servizio di Posta Elettronica sono le seguenti:

- Possibilità di gestione di più domini (virtuali) di posta.
- Possibilità per gli utenti di poter scegliere in qualsiasi momento il dominio di appartenenza del mittente delle E-Mail spedite, e ciò indipendentemente da quello del calcolatore dal quale ha origine il messaggio.
- Su richiesta, relativamente al mittente delle E-Mail, possibilità per il singolo utente di essere stabilmente associato ad uno specifico dominio, ed eventualmente scegliere una forma particolare di "mailname". Questa possibilità è molto comoda, soprattutto per i possessori di username particolari o problematiche.
- Possibilità di far eseguire il Mail Transport Agent (MTA) come utente non privilegiato.
- Definizione di una black-list per il rifiuto di E-Mail provenienti da mittenti indesiderati.
- Definizione di una black-list per la disabilitazione della mailbox di utenti locali.
- Possibilità di inviare al mittente un messaggio standard con le informazioni sul nuovo indirizzo E-Mail di utenti rimossi e/o trasferiti presso altro ISP (Internet Service Provider).
- Possibilità di utilizzo del mail-server dall'esterno della LAN, permettendo il relay esclusivamente agli utenti interni muniti di Certificato Personale X.509 (STARTTLS).
- Rifiuto della connessione con gli host che non rispettano l'handshake iniziale del protocollo SMTP ["FEATURE (`greet_pause')"].
- Possibilità di definizione di uno o più filtri (anti-virus, anti-spam, ecc…), in modalità "milter" (*cfr. 3.1*).
- Greylisting abilitato per default via "milter" (*cfr. 3.1.1*), ma con ampie possibilità di disabilitazione multilivello.
- Filtro anti-virus abilitato per default via "milter" (*cfr. 3.1.2*), ma con possibilià di disabilitazione per gli utenti che lo richiedano.
- Filtro anti-spam abilitato per default via "milter" (*cfr. 3.1.3*), ma con possibilità di disabilitazione a diversi livelli per gli utenti che ne dovessero fare richiesta.

3 MTA (Mail Transport Agent)

Il compito di un MTA è quello di trasportare la posta elettronica dalla sorgente alla destinazione, fungendo eventualmente da gateway tra protocolli diversi di spedizione delle E-Mail, trasformando gli indirizzi di posta e instradando le E-Mail secondo opportuni criteri.

Tra gli MTA di pubblico dominio a disposizione, abbiamo optato per "BSD (Berkeley System Distribution) Sendmail", finora rivelatosi sempre affidabile e sicuramente aderente agli standard, e la cui versione 8.13.1 permette di implementare tutte le caratteristiche descritte.

Sendmail (almeno nella sua funzione di MTA) non è vincolato ad alcun protocollo di formato o di trasporto specifico, il suo compito è solamente quello di instradare i messaggi di posta, in base alle disposizioni date nel file di configurazione.

I dettagli tecnici relativi alla configurazione di questo servizio sono riportati nelle seguenti APPENDICI:

A. Istruzioni per l'installazione di Berkeley sendmail 8.13.1 su piattaforma Unix.
B. Il file site.config.m4 .
C. Il file sendmail.mc per l'host che funge da relay (mail-server) .
D. Il file sendmail.mc per l'host generico (client) .
E. Il file domain.m4 .
F. Il file aliases, nella sua configurazione minima .
G. Istruzioni per l'installazione di amavisd-new 2.4.5 + amavisd-milter 1.3.1.
H. File di configurazione per amavisd-new.
I. Istruzioni per l'installazione del Sw di Greylisting.
J. Istruzioni per l'installazione di SpamAssassin 3.2.4 su piattaforma Unix.
K. File di configurazione per SpamAssassin.
L. Istruzioni per la gestione del filtro anti-spam (SpamAssassin).
M. Script per la correzione statistica Bayesiana dei risultati dello SpamAssassin.

3.1 MILTER

Si tratta di una interfaccia che consente di utilizzare Sw esterni (filtri) agli MTA (ad es. Sendmail) per validare o modificare i messaggi mentre transitano attraverso lo stesso MTA.

Viene normalmente utilizzata come interfaccia efficiente (sicura, affidabile, ad alte prestazioni) con anti-virus, anti-spam e content-scanner.

All'inizio non risultava presente in tutti i MTA, e da prerogativa esclusiva del Sendmail (ciò fu una forte motivazione per la sua scelta) venne in seguito adottata anche dal "rivale" Postfix.

3.1.1 FILTRO PER GREYLISTING (a livello di MTA)

Oggigiorno oltre il 60% di spam e virus provengono da computer infetti, compromessi, e non da veri server. Le macchine infettate da questi virus cercano di emulare il comportamento di un lecito mail-server, ma questa imitazione fallisce nell'implementazione di alcune funzionalità. Questa mancanza di funzionalità può essere sfruttata per differenziare un vero mail-server da una macchina infetta.

La funzionalità utilizzata per differenziare veri server da macchine infette è la capacità di ritrasmissione, cioè la capacità di un server reale di poter ritrasmettere un messaggio nel caso il destinatario non potesse (o non volesse) ricevere E-Mail da un altro server (cioè, il server destinatario è sovraccarico, o utilizza il Greylisting).

3.1.2 FILTRO ANTI-VIRUS (a livello di MTA)

Nel nostro caso, come primigenio prodotto anti-virus si era utilizzato il Sw prodotto dalla Sophos, sostituito poi con Clamav (di pubblico dominio) al momento del passaggio su s.o. Linux a 64 bit in quanto il necessario modulo Perl **SAVI** risultava instabile nel nuovo ambiente. Anche per questo prodotto l'installazione è risultata semplice (vedi APPENDICE-J).

3.1.3 FILTRO ANTI-SPAM (a livello di MTA)

Come prodotto anti-spam si è optato per quello di pubblico dominio della ASF (Apache Software Foundation): SpamAssassin. La sua installazione risulta banale in quanto disponibile come modulo Perl (CPAN). Le istruzioni per l'installazione sono riportate nell'APPENDICE-J.

Il funzionamento del filtro è basato su una rete neurale addestrata con la retro propagazione dell' errore (*Perceptron*), a correzione automatica *Bayesiana*, che tende a definire in maniera statistica la natura "SPAM" di ogni singola E-Mail. Di conseguenza, per quanto finemente si possa effettuare il "tuning" dei parametri di configurazione (APPENDICE-K), ci sarà sempre un "fondo" di E-Mail "buone" erroneamente individuate come "SPAM" ("*Falsi Positivi*") e di messaggi di "SPAM" non rivelati come tali ("*Falsi Negativi*").

A partire dalla versione 2.50 di SpamAssassin, quest'ultimo implementa l'analisi *Bayesiana* delle E-Mail, utilizzando un algoritmo di "apprendimento" per mezzo del quale effettua poi una correzione statistica dei risultati. Una volta abilitato l'auto-apprendimento, è bene però effettuare periodiche correzioni in base al feedback degli utenti. Uno script che effettui periodicamente (ad es. ogni notte) tale correzione è riportato nell'APPENDICE-M.

4 LDA (Local Delivery Agent)

Sendmail non si occupa di effettuare la consegna finale delle E-Mail. Di questo si occupano i LDA, programmi tramite i quali le E-Mail passano dai MTA ad un'area di spool (INBOX).

Noi abbiamo preferito non sostituire il LDA fornito con il s.o. Linux (Procmail), utilizzato anche per il filtraggio, catalogazione, smistamento, ecc… dei messaggi al momento della consegna.

4.1 FILTRO ANTI-SPAM (a livello di LDA)

La definizione dei criteri per lo smistamento delle E-Mail in opportuni folder viene effettuata tramite Procmail. Le corrispondenti istruzioni si trovano nei primi due punti dell'APPENDICE-L.

5 MUA (Mail User Agent)

Gli MTA non vengono utilizzati direttamente dagli utenti finali, i quali usano invece i MUA, programmi che costituiscono l'interfaccia dell'utente a Sendmail (o ad altri sistemi di trasporto) tramite i quali si possono comporre e passare E-Mail ai MTA.

Questi programmi (ad esempio: Alpine, Thunderbird, SeaMonkey) formattano l'input dell'utente e lo passano a Sendmail (in spedizione) e prelevano le nuove E-Mail da un'area di spool o via IMAP (in ricezione).

Gli utenti della Sez. INFN di Torino e dei Dipartimenti di Fisica hanno a disposizione varie modalità di gestione della posta elettronica personale. Ci si può collegare via SSH su uno dei calcolatori centrali ed usare il programma Alpine, oppure configurare opportunamente un MUA sul proprio calcolatore (ad esempio, Thunderbird o SeaMonkey) configurandolo in modo da utilizzare il protocollo IMAPS (IMAP con SSL).

Al fine di facilitare l'utilizzo del sistema di posta elettronica anche quando ci si trova fuori sede e non si ha la possibilità di configurare un MUA per la lettura della posta con IMAP/SSL o di accedere alle macchine centrali tramite SSH, abbiamo attivato un Servizio di WebMail ed implementato STARTTLS nel MTA.

5.1 WEBMAIL

Tale Servizio, basato su *SquirrelMail*, permette di leggere ed inviare E-Mail tramite un browser web (ad esempio, Firefox). Con questo strumento è possibile accedere alla INBOX ed ai folders personali ed effettuare operazioni di lettura, archiviazione, spedizione, cancellazione e ricerca.

Questo servizio utilizza una connessione cifrata (HTTPS) tra il browser ed il server di posta (cifratura a chiave pubblica). In questo modo viene garantita la riservatezza dei dati contenuti nei messaggi, oltre che di Username & Password. L'identità del server è garantita da un certificato rilasciato dalla Certification Authority dell'INFN (INFN-CA).

5.2 STARTTLS (con Thunderbird/SeaMonkey)

Per tutti gli utenti muniti di Certificato Personale X.509 rilasciato dalla "INFN Certification Authority" e che utilizzino Thunderbird o SeaMonkey come MUA, è possibile il reinstradamento (*relaying*) della posta in ingresso verso la rete esterna (WAN). In altre parole, l'utente che si trovi con il proprio PC portatile al di fuori della nostra LAN (ad es.: wi-fi spot aeroportuale) può utilizzare il mail-server di Sezione per spedire posta sia all'interno (LAN) che all'esterno (WAN); operazione, quest'ultima, generalmente non permessa su un mail-server configurato correttamente. Essenzialmente, rispetto ad una configurazione standard, la differenza sta nell'utilizzare sempre TLS sulla porta 587 del server di uscita.

Vantaggi di STARTTLS:

- Autenticazione del client e del server che consente il RELAY sicuro attraverso l'utilizzo di certificati.
- Privacy: la trasmissione di informazioni non può essere letta e ritradotta in plaintext, il canale di comunicazione è criptato.
- Integrita` dei dati che transitano nel canale di comunicazione, dal momento che il plaintext non puo` essere modificato in transito.

Limiti di STARTTLS:

- Non puo` garantire una encryption end-to-end (multiple hops).
- Non puo` fornire in assoluto un'autenticazione del messaggio a meno che la E-Mail sia inviata dal MUA direttamente al MTA del destinatario (ma potrebbe a sua volta venire modificata localmente).

6 CONCLUSIONE

La valutazione del servizio implementato nella Sez. INFN di Torino, a Novembre 2009, è sicuramente positiva sia per quanto riguarda la funzionalità di MTA, che per l'efficienza dei filtri anti-virus e/o antispam, coadiuvati dal meccanismo di greylisting.

Le varie funzionalità gradualmente implementate hanno contribuito ad eliminare la mole sempre maggiore di E-Mail indesiderate, mantenendo sempre "pulito" il flusso dei messaggi "buoni":

- Ottobre 2002: attachment renaming
- Gennaio 2003: anti-spam (opt-in)
- Gennaio 2004: Bayesian filtering
- Febbraio 2004: Bayesian learning
- Luglio 2004: greet_pause
- Settembre 2004: anti-virus (opt-out)
- Marzo 2005: anti-spam con REJECT (amavis)
- Settembre 2007: politica opt-out per anti-spam + anti-virus
- Maggio 2008: greylisting

7 RINGRAZIAMENTI

- Al Prof. Silio d'Angelo, dell'Università di Roma II (Torvergata/Roma), per la disponibilità dimostrata e per i consigli ricevuti, relativamente agli ambienti di cluster.

APPENDICE-A
Istruzioni per l'installazione di Berkeley sendmail 8.13.1 su piattaforma Unix

Le istruzioni che seguono, pur rimanendo generiche per la piattaforma Unix, fanno comunque riferimento a quella da noi utilizzata: **RHEL 4.x**.

Spacchettare il tar-file in una directory locale:

```
# cd /usr/local++
# gzip -dc sendmail.8.13.1.tar.gz | tar -xvf -
# chown -R root:root ./sendmail-8.13.1
```

Se attivo, fermare il processo **sendmail**. Nel nostro caso:

```
# service sendmail stop
```

Con la versione 8.13.1 è stata razionalizzata la dislocazione dei vari files di configurazione, ora tutti localizzati in **`/etc/mail`**. Quindi, se questa directory non esiste, va creata, con delle opportune protezioni ed ownership:

```
# mkdir /etc/mail
# chmod go-w / /etc /etc/mail /usr /var /var/spool /var/spool/mqueue
# chown root / /etc /etc/mail /usr /var /var/spool /var/spool/mqueue
```

Prima della compilazione, è necessario creare il file **site.config.m4,** contenente i riferimenti alla configurazione locale. Considerate le funzionalità richieste (STARTTLS e MILTER), si può utilizzare il file riportato nell'APPENDICE B. Il supporto per i MILTER dovrebbe essere già incluso di default a partire dalla versione 8.13.0, ma lo si riporta comunque (linee 4 e 5) per completezza:

```
# cd /usr/local++/sendmail-8.13.1/devtools/Site/
# cp /APPENDICE-B/site.config.m4 ./
```

Eventualmente, salvare il preesistente binario ed i corrispondenti files di configurazione (`*.mc`, `*.cf`), quindi lanciare la compilazione del nuovo codice:

```
# cd /usr/local++/sendmail-8.13.1/sendmail/
# sh Build
# cd ../libmilter/
# sh Build
```

Normalmente è possibile utilizzare **mail.local** come LDA, anche se ciò non è sempre fattibile a causa della sua eventuale incompatibilità con il sistema di locking del s.o. Dove tale incompatibilità non sussista, l'installazione di questo applicativo (distribuito con il **sendmail**) è banale:

```
# cd /usr/local++/sendmail-8.13.1/mail.local/
# sh Build force-install
```

Se, come nel nostro caso, l'installazione di **mail.local** non avviene in **`/usr/libexec`**, creare questa directory e copiarvi il binario:

```
# mkdir /usr/libexec
# cp /usr/lbin/mail.local /usr/libexec
```

Diversamente, quale LDA andrà utilizzato quello fornito con il s.o.; nel nostro caso: **`/usr/bin/procmail`** .

Esistono altri due applicativi, sempre distribuiti con il **sendmail**, che è possibile installare: **smrsh**, **makemap**. Rispettivamente:

```
# cd /usr/local++/sendmail-8.13.1/smrsh/
# sh Build install
# cp /usr/lbin/smrsh /usr/libexec

# cd /usr/local++/sendmail-8.13.1/makemap/
# sh Build
```

Noi abbiamo preferito installare **makemap**, diverso da quello del s.o., in **`/etc/mail`**:

```
# cp /usr/local++/sendmail-8.13.1/build-dir/makemap/makemap \
     /etc/mail/
```

L'utilizzo di **smrsh** fà sì che l'invocazione di eseguibili da parte di **sendmail** debba essere esplicitamente autorizzata tramite la creazione di un link simbolico, da porsi nella directory **`/etc/smrsh/`** . Ad esempio, per gli usuali **vacation** e **procmail**:

```
# cd /etc/smrsh/
# ln -s /usr/bin/vacation vacation
# ln -s /usr/local/bin/procmail procmail
```

A questo punto è possibile generare il file di configurazione **sendmail.cf**, utilizzando uno dei files **sendmail.mc** riportati nelle APPENDICI C o D (a seconda si stia configurando un mail-server o un host generico), ed il file **domain.m4** riportato nell'APPENDICE-E:

```
# cd /usr/local++/sendmail-8.13.1/cf/cf/
# cp /APPENDICE-CoD/sendmail.mc ./
# cd /usr/local++/sendmail-8.13.1/cf/domain/
# cp /APPENDICE-E/domain.m4 ./to.infn.it.m4
# sh Build sendmail.cf
# sh Build install-cf
```

Creare il Gruppo:

```
smmsp:*:51:
```

e l'utente:

```
smmsp:*:51:51:SendMail MessageSubmissionProgram:/var/spool/clientmqueue:/bin/sh
```

ed installare il binario di **sendmail**:

```
# cd /usr/local++/sendmail-8.13.1/sendmail
# sh Build install
```

A questo punto si può procedere con l'installazione dei MILTER definiti nel file **sendmail.mc** (APPENDICE-C). Nell'ordine, si tratta di **milter-greylist** ed **AMaViS**, le cui istruzioni di installazione si trovano rispettivamente nelle APPENDICI I e G.

Il file degli aliases deve avere una configurazione minima obbligatoria, come riportato nell'APPENDICE-F:

```
# cp /APPENDICE-F/aliases /etc/mail/aliases
# newaliases
```

Se dopo quest'ultimo comando si ottiene un errore come il seguente:

```
/etc/mail/sendmail.cf: line 55: unknown configuration line "
```

cancellare in **`/etc/mail/sendmail.cf`** la riga indicata (in questo caso la 55).

Verificare le seguenti protezioni ed ownership:

```
-r-xr-sr-x   1 root   smmsp   951264 Aug 29 15:48 /usr/sbin/sendmail
drwxrwx---   2 smmsp  smmsp      512 Aug 29 15:48 /var/spool/clientmqueue
drwx------   2 root   root       512 Aug  1  2001 /var/spool/mqueue/
-r--r--r--   1 root   root     40187 Aug 29 16:03 /etc/mail/sendmail.cf
-r--r--r--   1 root   root     38724 Aug 29 15:33 /etc/mail/submit.cf
```

Inserire in **`/etc/mail/local-host-names`** i nomi per i quali si vuole che la macchina possa ricevere E-Mail. Nel nostro caso, per il mail-server:

```
acufene.to.infn.it
smtp.to.infn.it
lama01.to.infn.it
lama02.infn.it
lama04.to.infn.it
clusterfloat01.infn.it
clusterfloat02.infn.it
clusterfloat04.infn.it
torino.infn.it
to.infn.it
cosmot.to.infn.it
ph.unito.it
cifs-spazio.it
```

dove: *acufene* è il nostro MX, e *lama0x* i tre membri del cluster.

Per il solo mail-server, in **`/etc/mail/access`** vanno elencati i domini (o i MATCH, nel caso di STARTTLS) per i quali la macchina accetta di ricevere posta o fare da relay-host; ma può contenere anche domini remoti e/o utenti locali da filtrare; inoltre, a partire dalla versione 8.13.0, contiene anche i time-out da assegnare alla feature '*greet_pause*'. Nel caso del nostro mail-server:

```
CERTIssuer:/C=IT/O=INFN/CN=INFN+20Certification+20Authority     SUBJECT
CERTSubject:MATCH       RELAY
to.infn.it              RELAY
torino.infn.it          RELAY
ph.unito.it             RELAY
GreetPause:to.infn.it   0
```

```
GreetPause:ph.unito.it  0
GreetPause:127.0.0.1    0
GreetPause:10.0.0       0
GreetPause:10.1.0       0
spam.domain.xx          REJECT
veryspam.domain.xx      DISCARD
Bill.Gates@             ERROR:550  Mailbox disabled for this User
```

dove, il `GreetPause` è stato disabilitato (=0) per domini e sottoreti locali., mentre sull'ultima riga c'è da dire che il blocco vale oltre che per l'utente locale anche per gli omonimi remoti.
Per rendere attive le modifiche di questo file e ricostruire il corrispondente DB:

```
# /etc/mail/makemap hash /etc/mail/access.db < /etc/mail/access
```

Relativamente alla posta in ingresso, i files **`/etc/mail/virtusertable`** ed **`/etc/mail/virtuser-domains`** permettono di gestire ulteriori domini (virtuali e non) oltre quello (reale) di appartenenza del mail-server. Nel caso del nostro mail-server, considerato che il DB utenti è lo stesso per tutti i domini gestiti, i due files assumono rispettivamente la forma seguente:

```
@ph.unito.it            %1@to.infn.it
@torino.infn.it         %1@to.infn.it
@cosmot.to.infn.it      %1@to.infn.it
@cifs-spazio.it         %1@to.infn.it
```

e

```
ph.unito.it
torino.infn.it
cosmot.to.infn.it
cifs-spazio.it
```

Per rendere attive le modifiche del primo file e ricostruire il corrispondente DB:

```
# /etc/mail/makemap hash /etc/mail/virtusertable.db < /etc/mail/virtusertable
```

Relativamente alla posta in uscita, i files **`/etc/mail/genericstable`** ed **`/etc/mail/generics-domains`** permettono di associare a ciascuna username un mailname ed un dominio virtuali. Nel caso del nostro mail-server i due files assumono rispettiva-

mente la forma seguente:

```
gandalf         Alberto.DAmbrosio@to.infn.it
```

e

```
ph.unito.it
to.infn.it
torino.infn.it
cosmot.to.infn.it
cifs-spazio.it
```

Per rendere attive le modifiche del primo file e ricostruire il corrispondente DB:

```
# /etc/mail/makemap hash /etc/mail/genericstable.db < /etc/mail/genericstable
```

Terminata la configurazione, far ripartire il processo **sendmail**:

```
# /path/to/sendmail –bd –q30m
```

da inserire nell'opportuno file di startup, che nel nostro caso è **`/etc/init.d/sendmail`**

N.B.:

Affinché STARTTLS funzioni correttamente, nel caso in cui il s.o. non metta a disposizione **`/dev/urandom`**, è necessario specificare un file contenente "random data" , il cui contenuto venga aggiornato ad intervalli minori di 10 minuti. La corrispondente istruzione da utilizzare all'interno del file **sendmail.mc** (APPENDICE-C) è la seguente:

```
define(`confRAND_FILE', `file:/etc/mail/randfile')dnl
```

APPENDICE-B
File site.config.m4 per STARTTLS + MILTER

```
define(`confSTDIO_TYPE', `portable')
APPENDDEF(`confINCDIRS', `-I/usr/local+/openssl-0.9.7a/include')
APPENDDEF(`confLIBDIRS', `-L/usr/local+/openssl-0.9.7a/lib')
APPENDDEF(`conf_libmilter_ENVDEF', `-DMILTER')
APPENDDEF(`conf_sendmail_ENVDEF', `-DMILTER')
APPENDDEF(`conf_sendmail_ENVDEF', `-DSTARTTLS')
APPENDDEF(`conf_sendmail_LIBS', `-lssl -lcrypto')
```

APPENDICE-C
File sendmail.mc per mail-server (relay-host)

```
divert(-1)dnl
dnl #
dnl # This is the sendmail macro config file for m4. If you make changes
dnl # to /etc/mail/sendmail.mc, you will need to regenerate the
dnl # /etc/mail/sendmail.cf file by confirming that the sendmail-cf
dnl # package is installed and then performing a
dnl #
dnl #     make -C /etc/mail
dnl #
include(`/usr/share/sendmail-cf/m4/cf.m4')dnl
VERSIONID(`setup for Red Hat Linux')dnl
OSTYPE(`linux')dnl
dnl #
define(`confSMTP_LOGIN_MSG', `Unknown Hidden Identity')dnl
define(`confCF_VERSION', `[Gnorri: ON]')dnl
dnl #
dnl # default logging level is 9, you might want to set it higher to
dnl # debug the configuration
dnl #
dnl define(`confLOG_LEVEL', `9')dnl
dnl #
dnl # Uncomment and edit the following line if your outgoing mail needs
dnl # to be sent out through an external mail server:
dnl #
define(`confMAIL_HUB',`acufene.to.infn.it.')dnl
dnl define(`LUSER_RELAY',confMAIL_HUB)dnl
dnl define(`SMART_HOST',smtp:confMAIL_HUB)dnl
dnl #
define(`confDEF_USER_ID',``8:12'')dnl
dnl define(`confAUTO_REBUILD')dnl
define(`confTO_CONNECT', `1m')dnl
dnl define(`confTRY_NULL_MX_LIST',true)dnl
dnl define(`confDONT_PROBE_INTERFACES',true)dnl
dnl #
define(`PROCMAIL_MAILER_PATH',`/usr/bin/procmail')dnl
define(`LOCAL_SHELL_PATH', `/usr/sbin/smrsh')dnl
define(`ALIAS_FILE', `/etc/aliases')dnl
define(`STATUS_FILE', `/var/log/mail/statistics')dnl
dnl define(`UUCP_MAILER_MAX', `2000000')dnl
define(`confUSERDB_SPEC', `/etc/mail/userdb.db')dnl
dnl #
dnl define(`confPRIVACY_FLAGS',
     `authwarnings,novrfy,noexpn,restrictqrun')dnl
define(`confPRIVACY_FLAGS', `noexpn,needmailhelo,novrfy')dnl
define(`confMESSAGE_TIMEOUT', `5d/24h')dnl
dnl define(`confAUTH_OPTIONS', `A')dnl
define(`confMAX_MESSAGE_SIZE', `100000000')dnl
define(`confMAX_HEADERS_LENGTH', `32768')dnl
dnl #
dnl # The following allows relaying if the user authenticates, and
dnl # disallows plaintext authentication (PLAIN/LOGIN) on non-TLS links
dnl #
```

```
dnl define(`confAUTH_OPTIONS', `A p')dnl
dnl #
dnl # PLAIN is the preferred plaintext authentication method and used by
dnl # Mozilla Mail and Evolution, though Outlook Express and other MUAs
dnl # do use LOGIN. Other mechanisms should be used if the connection is
dnl # not guaranteed secure.
dnl # Please remember that saslauthd needs to be running for AUTH.
dnl #
dnl TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl define(`confAUTH_MECHANISMS',
     `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl #
dnl # Rudimentary information on creating certificates for sendmail TLS:
dnl #     cd /usr/share/ssl/certs; make sendmail.pem
dnl # Complete usage:
dnl #     make -C /usr/share/ssl/certs usage
dnl #
dnl define(`confCACERT_PATH',`/usr/share/ssl/certs')
dnl define(`confCACERT',`/usr/share/ssl/certs/ca-bundle.crt')
dnl define(`confSERVER_CERT',`/usr/share/ssl/certs/sendmail.pem')
dnl define(`confSERVER_KEY',`/usr/share/ssl/certs/sendmail.pem')
dnl #
define(`CERT_DIR', `/usr/local+/etc/stunnel/certs')dnl
define(`CACERT_DIR', `/usr/local+/etc/stunnel/certs')dnl
define(`confCACERT_PATH',`CACERT_DIR')dnl
define(`confCACERT',`CACERT_DIR/INFN-CA-Cert.pem')dnl
define(`confSERVER_CERT',`CERT_DIR/sendmail-cert.pem')dnl
define(`confSERVER_KEY',`CERT_DIR/sendmail-key.pem')dnl
define(`confCLIENT_CERT',`CERT_DIR/sendmail-cert.pem')dnl
define(`confCLIENT_KEY',`CERT_DIR/sendmail-key.pem')dnl
define(`_CERT_REGEX_SUBJECT_',
     `-aMATCH /C=IT/O=INFN/OU=Personal\+20Certificate/L=Torino')dnl
dnl #
INPUT_MAIL_FILTER(`greylist',
     `S=local:/var/run/milter-greylist/milter-greylist.sock',
     F=T, T=C:5m;S:5m;R:5m;E:5m')dnl
define(`confMILTER_MACROS_CONNECT', `j, {if_addr}')dnl
define(`confMILTER_MACROS_HELO', `{verify}, {cert_subject}')dnl
define(`confMILTER_MACROS_ENVFROM', `i, {auth_authen}')dnl
dnl define(`confMILTER_MACROS_ENVRCPT', `{greylist}')dnl
dnl #
INPUT_MAIL_FILTER(`amavis-milter',
     `S=local:/var/run/amavis/amavis-milter.sock,
     F=T, T=S:10m;R:10m;E:10m')dnl
dnl INPUT_MAIL_FILTER(`vbsfilter',
     `S=unix:/var/run/vbsfilter-milter.sock,
     F=T, T=S:10s;R:10s;E:5m')dnl
define(`confINPUT_MAIL_FILTERS', `greylist, amavis-milter')dnl
dnl define(`confINPUT_MAIL_FILTERS', `greylist')dnl
dnl define(`confINPUT_MAIL_FILTERS', `amavis-milter, vbsfilter')dnl
define(`confMILTER_MACROS_ENVFROM', confMILTER_MACROS_ENVFROM``,
     {b}'')dnl
dnl #
dnl # This allows sendmail to use a keyfile that is shared with
dnl # OpenLDAP's slapd, which requires the file to be readble by group
dnl # ldap
```

```
dnl #
dnl define(`confDONT_BLAME_SENDMAIL',`groupreadablekeyfile')dnl
dnl #
define(`confTO_QUEUEWARN', `24h')dnl
define(`confTO_QUEUERETURN', `5d')dnl
define(`confDELAY_LA', `12')dnl
define(`confQUEUE_LA', `24')dnl
define(`confREFUSE_LA', `36')dnl
dnl define(`confTO_IDENT', `0')dnl
dnl #
dnl FEATURE(delay_checks)dnl
FEATURE(`no_default_msa',`dnl')dnl
FEATURE(`smrsh',`/usr/sbin/smrsh')dnl
FEATURE(`mailertable',`hash -o /etc/mail/mailertable.db')dnl
FEATURE(`virtusertable',`hash -o /etc/mail/virtusertable.db')dnl
VIRTUSER_DOMAIN_FILE(`/etc/mail/virtuser-domains')dnl
FEATURE(`genericstable',`hash -o /etc/mail/genericstable.db')dnl
GENERICS_DOMAIN_FILE(`/etc/mail/generics-domains')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
dnl #
dnl # The following limits the number of processes sendmail can fork to
dnl # accept incoming messages or process its message queues to 12.)
dnl # sendmail refuses to accept connections once it has reached its
dnl # quota of child processes.
dnl #
dnl define(`confMAX_DAEMON_CHILDREN', 12)dnl
dnl #
dnl # Limits the number of new connections per second. This caps the
dnl # overhead incurred due to forking new sendmail processes. May be
dnl # useful against DoS attacks or barrages of spam. (As mentioned
dnl # below, a per-IP address limit would be useful but is not available
dnl # as an option at this writing.)
dnl #
define(`confCONNECTION_RATE_THROTTLE', 3)dnl
dnl #
dnl # The -t option will retry delivery if e.g. the user runs over his
dnl # quota.
dnl #
FEATURE(local_procmail,`',`procmail -t -Y -a $h -d $u')dnl
FEATURE(`access_db',`hash -T<TMPF> -o /etc/mail/access.db')dnl
FEATURE(`greet_pause', `5000')dnl
FEATURE(`blacklist_recipients')dnl
FEATURE(`nouucp', `reject')dnl
dnl #
dnl # The following causes sendmail to only listen on the IPv4 loopback
dnl # address 127.0.0.1 and not on any other network devices. Remove the
dnl # loopback address restriction to accept email from the internet or
dnl # intranet.
dnl #
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl
dnl #
```

```
dnl # The following causes sendmail to additionally listen to port 587
for
dnl # mail from MUAs that authenticate. Roaming users who can't reach
dnl # their preferred sendmail daemon due to port 25 being blocked or
dnl # redirected find this useful.
dnl #
dnl DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl
DAEMON_OPTIONS(`Port=submission, Name=MSA, M=E')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 465,
dnl # but starting immediately in TLS mode upon connecting. Port 25 or
dnl # 587 followed by STARTTLS is preferred, but roaming clients using
dnl # Outlook Express can't do STARTTLS on ports other than 25. Mozilla
dnl # Mail can ONLY use STARTTLS and doesn't support the deprecated
dnl # smtps; Evolution <1.1.1 uses smtps when SSL is enabled—STARTTLS
dnl # support is available in version 1.1.1.
dnl #
dnl # For this to work your OpenSSL certificates must be configured.
dnl #
dnl DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl
dnl #
dnl # The following causes sendmail to additionally listen on the IPv6
dnl # loopback device. Remove the loopback address restriction listen to
dnl # the network.
dnl #
dnl DAEMON_OPTIONS(`port=smtp,Addr=::1, Name=MTA-v6, Family=inet6')dnl
dnl #
dnl # enable both ipv6 and ipv4 in sendmail:
dnl #
dnl DAEMON_OPTIONS(`Name=MTA-v4, Family=inet, Name=MTA-v6,
     Family=inet6')
dnl #
dnl # We strongly recommend not accepting unresolvable domains if you
dnl # want to protect yourself from spam. However, the laptop and users
dnl # on computers that do not have 24x7 DNS do need this.
dnl #
dnl FEATURE(`accept_unresolvable_domains')dnl
dnl #
dnl FEATURE(`relay_based_on_MX')dnl
dnl #
dnl # Also accept email sent to "localhost.localdomain" as local email.
dnl #
LOCAL_DOMAIN(`localhost.localdomain')dnl
dnl #
dnl # The following example makes mail from this host and any additional
dnl # specified domains appear to be sent from mydomain.com
dnl #
dnl DOMAIN(`to.infn.it')dnl
MASQUERADE_AS(`to.infn.it')dnl
dnl #
dnl # masquerade not just the headers, but the envelope as well
dnl #
dnl FEATURE(masquerade_envelope)dnl
dnl #
dnl # masquerade not just @mydomainalias.com, but @*.mydomainalias.com
dnl # as well
```

```
dnl #
dnl FEATURE(masquerade_entire_domain)dnl
FEATURE(allmasquerade)
FEATURE(limited_masquerade)
dnl #
EXPOSED_USER(`root')dnl
EXPOSED_USER(postmaster)dnl
dnl #
dnl MASQUERADE_DOMAIN(localhost)dnl
dnl MASQUERADE_DOMAIN(localhost.localdomain)dnl
dnl MASQUERADE_DOMAIN(mydomainalias.com)dnl
dnl MASQUERADE_DOMAIN(mydomain.lan)dnl
MAILER(smtp)dnl
MAILER(procmail)dnl
```

APPENDICE-D
File sendmail.mc per host generico (non-relay)

```
divert(-1)
#
# Copyright (c) 1998-2000 Sendmail, Inc. and its suppliers.
#    All rights reserved.
# Copyright (c) 1983 Eric P. Allman.  All rights reserved.
# Copyright (c) 1988, 1993
#    The Regents of the University of California.  All rights reserved.
#
# By using this file, you agree to the terms and conditions set
# forth in the LICENSE file which can be found at the top level of
# the sendmail distribution.
#
#

divert(0)dnl
include(`../m4/cf.m4')
VERSIONID(`$Id: host.mc,v 8.14 2002/04/22 09:30:00 ca Exp $')
OSTYPE(osf1)dnl

define(confDOMAIN_ONLY, `to.infn.it')
define(`confMAIL_HUB',`smtp.to.infn.it.')
define(confMAX_MESSAGE_SIZE, `20000000')

define(`ALIAS_FILE', `/etc/mail/aliases')
define(`LOCAL_MAILER_PATH', `/usr/libexec/mail.local')
define(`LOCAL_SHELL_PATH', `/usr/libexec/smrsh')

define(`LUSER_RELAY',confMAIL_HUB)dnl
define(`SMART_HOST',smtp:confMAIL_HUB)dnl
define(`MAIL_HUB',confMAIL_HUB)dnl

DOMAIN(confDOMAIN_ONLY)dnl
MASQUERADE_AS(confDOMAIN_ONLY)dnl

FEATURE(smrsh)
FEATURE(use_cw_file)dnl
FEATURE(allmasquerade)
FEATURE(limited_masquerade)
EXPOSED_USER(postmaster)

MAILER(`local')dnl
MAILER(`smtp')dnl
```

APPENDICE-E
File domain.m4 (to.infn.it.m4)

```
divert(0)
VERSIONID(`@(#)to.infn.it.m4,v 8.15 2002/04/22 09:30:00 ca Exp $')
define(`confFORWARD_PATH',
`$z/.forward.$w+$h:$z/.forward+$h:$z/.forward.$w:$z/.forward')dnl
define(`confMAX_HEADERS_LENGTH', `32768')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)
define(`confPRIVACY_FLAGS', `noexpn,needmailhelo,novrfy')
define(`confMESSAGE_TIMEOUT', `5d/24h')
```

APPENDICE-F
File /etc/mail/aliases (configurazione minima obbligatoria)

```
##
#    >>>>>>>>>>    The command "sendmail -bi" must be run after
#    >> NOTE >>    this file is updated for any changes to
#    >>>>>>>>>>    affect sendmail operation.
##

# Alias for mailer daemon
MAILER-DAEMON:root

# Following alias is required by the new mail protocol, RFC 822
postmaster:root

# Alias for abuse@to.infn.it
abuse:root

# Aliases to handle mail to msgs and news
nobody: /dev/null
```

APPENDICE-G
Istruzioni per l'installazione di amavisd-new 2.4.5 + amavisd-milter 1.3.1

Prima dell'installazione vera e propria è necessario effettuare qualche operazione preliminare. Iniziamo con la configurazione riguardante il **sendmail**:

```
# cd /usr/local/sendmail-8.13.1/cf/cf
```

Inserire le seguenti istruzioni nel file **sendmail.mc** (già presenti nell'APPENDICE-C):

```
define(`_FFR_MILTER',`1')dnl
INPUT_MAIL_FILTER(`amavis-milter',
`S=local:/var/run/amavis/amavis-milter.sock, F=T, T=S:10m;R:10m;E:10m')
define(`confINPUT_MAIL_FILTERS', `amavis-milter')
```

Rigenerare il file **sendmail.cf** (operazione già inclusa nell'APPENDICE-A):

```
# ./Build sendmail.cf
# ./Build install-cf
```

Prima della ricompilazione del **sendmail** è necessario inserire nel file **site.config.m4** i riferimenti per l'attivazione del supporto per i MILTER. Quest'ultimo dovrebbe essere già incluso di default a partire dalla versione 8.13.0, ma lo si riporta comunque per completezza:

```
# cd /usr/local++/sendmail-8.13.1/devtools/Site
```

Inserire nel file **site.config.m4** le due seguenti linee:

```
APPENDDEF(`conf_sendmail_ENVDEF', `-DMILTER')
APPENDDEF(`conf_libmilter_ENVDEF', `-DMILTER')
```

A questo punto è possibile procedere con la (ri)compilazione e la (re)installazione del **sendmail**:

```
# cd /usr/local/sendmail-8.13.1/sendmail/
# ./Build -c
# ./Build install
```

e di alcune necessarie librerie:

```
# cd ../libmilter/
# ./Build -c

# cd ../libsm/
# ./Build -c

# cd ../libsmutil/
# ./Build -c
```

```
# cd ../
```

Copiare tutte queste ultime in una stessa area comune:

```
# cp -p build-dir/libmilter/*.a  /usr/local+/lib/
# cp -p build-dir/libsm/*.a      /usr/local+/lib/
# cp -p build-dir/libsmutil/*.a  /usr/local+/lib/
```

Con il s.o. **RHEL 4.x**, in presenza del pacchetto *RPM* **"sendmail-devel"**, queste librerie risultano già installate in **`/usr/lib64`**.

Nel caso non esistano già, creare il gruppo e l'utente seguenti:

```
vscan:*:52:
```

```
vscan:NoLogin:52:52:AMaViS:/usr/local+/amavis:/sbin/nologin
```

per il quale occorre configurare una opportuna home-directory:

```
# mkdir /usr/local+/amavis/tmp
# mkdir /usr/local+/amavis/var
# mkdir /usr/local+/amavis/db
# chmod -R 750 /usr/local+/amavis
# chown -R vscan:vscan /usr/local+/amavis
```

È anche necessaria la creazione di un`area di quarantena per le E-Mail infette:

```
# mkdir /usr/local+/virusmails
# chmod -R 750 /usr/local+/virusmails
# chown -R vscan:vscan /usr/local+/virusmails
```

A questo punto è possibile procedere con l'installazione vera e propria del Sw. Spacchettare il tar-file all'interno della directory di installazione del **sendmail**:

```
# cd /usr/local++/sendmail-8.13.1/
# gzip -dc amavisd-new-2.4.5.tar.gz | tar -xvf -
# chown -R root:system ./amavisd-new-2.4.5/
```

Nel file **`/usr/local++/sendmail-8.13.1/amavisd-new-2.4.5/INSTALL`** esiste un elenco di moduli Perl e programmi esterni che devono essere preliminarmente installati. Verificati tutti i requisiti finora elencati, si può continuare con l'installazione:

```
# cd /usr/local++/sendmail-8.13.1/amavisd-new-2.4.5/helper-progs
# setenv CFLAGS "-pthread"

# ./configure --prefix=/usr/local+                          \
              --enable-milter=yes                           \
              --with-milterinc=../../include                \
              --with-milterlib=/usr/lib64                   \
              --with-runtime-dir=/usr/local+/amavis/tmp     \
```

```
              --with-sockname=/var/run/amavis/amavisd.sock    \
              --with-user=vscan                               \
              --with-x-header-tag="X-Scanned"                 \
              --with-x-header-val="by amavisd-new"


# make
# make install

# cp amavis /usr/local+/sbin/
# cp amavis-milter /usr/local+/sbin/
# cp ../amavisd /usr/local+/sbin/
# chmod 755 /usr/local+/sbin/amavis*
```

Il milter incluso nel pacchetto di **amavisd-new** (**amavis-milter**) non è in grado di modificare l'header delle E-Mail analizzate e di conseguenza non permetterebbe l'implementazione della policy *opt-out*. Per realizzare ciò si è quindi utilizzato un diverso milter, l'**amavisd-milter** di *Petr Rehor*, che utilizzando lo speciale protocollo **AM.PDP** è in grado di modificare l'header delle E-Mail analizzate. La sua installazione è abbastanza semplice:

```
# cd /usr/local++/amavisd-milter-1.3.1/
# setenv LDFLAGS -L/usr/lib64
# setenv CFLAGS "-pthread"
# setenv CPPFLAGS -I../../include

# ./configure -prefix=/usr/local+/ --enable-milter=yes
# make
# make install
```

Nel nostro caso come prodotto anti-virus si è utilizzato **ClamAV**, di pubblico dominio, la cui installazione è banale:

```
# cd /usr/local++/clamav-0.91.2/
# ./install.sh --with-user=vscan
               --with-group=vscan
               --sysconfdir=/usr/local+/etc/clamav
               --with-db-dir=/usr/local+/lib/clamav
# make
# make install
```

Come prodotto anti-spam, invece, si è optato per quello di pubblico dominio della ASF (Apache Software Foundation): **SpamAssassin**. La sua installazione risulta banale in quanto disponibile come modulo Perl (CPAN). In ogni caso, delle linee-guida sono disponibili nella APPENDICE-J.

Nella APPENDICE-H è riportato un esempio di file di configurazione per **AMaViS**, dove:

- L'anti-virus è abilitato di default per tutti gli utenti. Gli indirizzi E-Mail da disabilitare vanno inseriti nelle variabili **`bypass_virus_checks_maps`** e **`virus_lovers_maps`**.

- L'anti-spam è abilitato di default per tutti gli utenti. Gli indirizzi E-Mail da disabilitare vanno inseriti nelle variabili **`bypass_spam_checks_maps`** (disabilitazione totale del filtro) e **`spam_lovers_maps`** (disabilitazione del **`REJECT`** del filtro).
- La notifica al mittente delle E-Mail intercettate è disabilitata.

Il tutto va poi lanciato (prima del **sendmail**) nel modo seguente:

```
# setenv LD_LIBRARY_PATH
         /usr/lib:/usr/local/lib:/usr/local+/lib:/usr/local++/lib

# rm -f /var/run/amavis/amavis-milter.sock
# rm -f /var/run/amavis/amavisd.lock
# rm -f /var/run/amavis/amavisd.sock
# rm -f /var/run/amavis/amavisd.pid

# su - vscan -c '/usr/local+/sbin/amavisd-milter              \
             -s /var/run/amavis/amavis-milter.sock'           \
             -S /var/run/amavis/amavisd.sock                  \
             -p /var/run/amavis/amavisd-milter.pid            \
             -w /usr/local+/amavis/tmp                        \
             -m 10 -M 1800 -t 1800 -T 1800

# /usr/local+/sbin/amavisd -u vscan -c /usr/local+/etc/amavisd.conf
```

N.B.:

Affinché il modulo Perl **Mail::SpamAssassin** venga correttamente rilevato, è necessario inserire la seguente istruzione all'interno (ad es., come seconda riga) del daemon **`/usr/local+/sbin/amavisd`** :

```
use lib '/usr/local+/lib64/perl5/site_perl';
```

APPENDICE-H
File di configurazione per amavisd-new

```
use strict;

# a minimalistic configuration file for amavisd-new with all necessary
settings
#
#   (see amavisd.conf-default for a list of all variables with their de-
faults)
#   (see amavisd.conf-sample for a traditional-style commented file)


# COMMONLY ADJUSTED SETTINGS:

# @bypass_virus_checks_maps = (1);  # uncomment to DISABLE anti-virus
code
# @bypass_spam_checks_maps  = (1);   # uncomment to DISABLE anti-spam
code

@bypass_virus_checks_maps = (
 { 'username@' => 1,
   'nome.cognome@' => 1,
 },
);

@virus_lovers_maps = (
 { 'username@' => 1,
   'nome.cognome@' => 1,
 },
);

########################################################
### DISABILITAZIONE *TOTALE* DEL FILTRO ANTI-SPAM ###
########################################################

@bypass_spam_checks_maps = (
 { 'username@' => 1,
   'nome.cognome@' => 1,
},
 0,
);

########################################################
### DISABILITAZIONE *REJECT* DEL FILTRO ANTI-SPAM ###
########################################################

@spam_lovers_maps = (
 { 'username@' => 1,
   'nome.cognome@' => 1,
},
 0,
);
```

```
$max_servers   = 10;         # number of pre-forked children (2..15 is
common)
$max_requests  = 10;         # retire a child after that many accepts
$child_timeout =10*60;       # abort child if it does not complete each
task in
                             # approximately n sec (default: 8*60 sec-
onds)
$daemon_user   = 'vscan';    # (no default;  customary: vscan or amavis)
$daemon_group  = 'vscan';    # (no default;  customary: vscan or amavis)

$mydomain   = 'to.infn.it';       # a convenient default for other set-
tings
$myhostname = 'mail.to.infn.it';  # must be a fully-qualified domain
name!

$MYHOME   = '/usr/local+/amavis'; # a convenient default for other set-
tings
$TEMPBASE = "$MYHOME/tmp";    # working directory, needs to be created
manually
$ENV{TMPDIR} = '/usr/local+/amavis/tmp';   # environment variable TMPDIR
$QUARANTINEDIR = '/usr/local+/virusmails';
$quarantine_subdir_levels = 1;    # add level of subdirs to disperse
quarantine

# $daemon_chroot_dir = $MYHOME;   # chroot directory or undef

$db_home   = "$MYHOME/db";
$helpers_home = "$MYHOME/var";    # prefer $MYHOME clean and owned by
root?
$pid_file  = "/var/run/amavis/amavisd.pid";
$lock_file = "/var/run/amavis/amavisd.lock";

@local_domains_maps = ( [".$mydomain", 'torino.infn.it', 'ph.unito.it',
'con-scienze.it', 'cifs-spazio.it'] );
# @mynetworks = qw( 127.0.0.0/8 ::1 10.0.0.0/8 172.16.0.0/12
192.168.0.0/16 );
#$policy_bank{'MYNETS'} = {
#  bypass_spam_checks_maps => [1],
#};

$log_level = 2;              # verbosity 0..5
$sa_debug  = 0;
$DO_SYSLOG = 1;              # log via syslogd (preferred)
#$SYSLOG_LEVEL='mail.debug'; # Obsolete variable (from 2.4.0)
$syslog_ident = 'amavis';    # Syslog ident string (defaults to
'amavis')
$syslog_facility = 'mail';   # Syslog facility as a string
                             # e.g.: mail, daemon, user, local0, ... lo-
cal7
$syslog_priority = 'debug';  # Syslog base (minimal) priority as a
string,
                             # choose from: emerg, alert, crit, err,
warning,
                             #              notice, info, debug
```

```
$enable_db = 0;              # enable use of BerkeleyDB/libdb (SNMP and
nanny)
$enable_global_cache = 0;    # enable use of libdb-based cache if $en-
able_db=1

@additional_perl_modules = qw(
 Mail/SpamAssassin/Plugin/AntiVirus.pm
);

$protocol = "AM.PDP";        # Use AM.PDP protocol
#$inet_socket_port = 10024;   # listen on this local TCP port(s) (see
$protocol)
$unix_socketname = "/var/run/amavis/amavisd.sock"; # when using sendmail
milter

$sa_tag_level_deflt  = -999; # add spam info headers if at, or above
that level
$sa_tag2_level_deflt = 3.7;  # add 'spam detected' headers at that level
$sa_kill_level_deflt = 15;   # triggers spam evasive actions
$sa_dsn_cutoff_level = -999; # spam level beyond which a DSN is not sent
$sa_quarantine_cutoff_level = -999; # spam level beyond which quarantine
is off

$sa_mail_body_size_limit = 256*1024; # don't waste time on SA if mail is
larger
$sa_local_tests_only = 0;    # only tests which do not require internet
access?
$sa_auto_whitelist = 1;      # turn on AWL in SA 2.63 or older (irrele-
vant
                             # for SA 3.0, cf option is
'use_auto_whitelist')
$sa_spam_report_header = 1;
$sa_spam_subject_tag = '***SPAM*** ';
$remove_existing_spam_headers = 1;

# @lookup_sql_dsn =
#   ( ['DBI:mysql:database=mail;host=127.0.0.1;port=3306', 'user1',
'passwd1'],
#     ['DBI:mysql:database=mail;host=host2', 'username2', 'password2']
);

$virus_admin = undef;  # notifications recip.

#@virus_admin_maps = (                          # by-recipient maps
#  { 'to.infn.it'        => 'request@to.infn.it', # default for our vi-
rus senders
#    'torino.infn.it'    => 'request@to.infn.it',
#    'ph.unito.it'       => 'request@to.infn.it',
#    'con-scienze.it'    => 'request@to.infn.it',
#    'cifs-spazio.it'    => 'request@to.infn.it',
#    'cosmot.to.infn.it' => 'request@to.infn.it',
#  },
#  '',  # catchall for the rest (don't send admin notifications)
#);
```

```
$notify_virus_recips_templ =
read_text("$MYHOME/notify_virus_recips.txt");
$warn_offsite = 0;     # (defaults to false (undef), i.e. only notify
locals)

###$mailfrom_notify_recip     = "\"Central Antivirus at $myhostname\"
<postmaster\@$mydomain>";
###$hdrfrom_notify_recip      = "\"Central Antivirus at $myhostname\"
<postmaster\@$mydomain>";
###$mailfrom_to_quarantine    = "\"Central Antivirus at $myhostname\"
<postmaster\@$mydomain>";

$warnvirussender = 0;  # (defaults to false (undef))
$warnspamsender = 0;   # (defaults to false (undef))
$warnbannedsender = 0; # (defaults to false (undef))
$warnbadhsender = 0;   # (defaults to false (undef))

$warnvirusrecip = 0;   # (defaults to false (undef))
$warnbannedrecip = 0;  # (defaults to false (undef))
$warnbadhrecip = 0;    # (defaults to false (undef))

@addr_extension_virus_maps      = ('virus');
@addr_extension_spam_maps       = ('spam');
@addr_extension_banned_maps     = ('banned');
@addr_extension_bad_header_maps = ('badh');

$path =
'/usr/local++/sbin:/usr/local++/bin:/usr/local+/sbin:/usr/local+/bin:/us
r/local/sbin:/usr/local/bin:/usr/sbin:/sbin:/usr/bin:/bin';

$file   = 'file';   # file(1) utility; use recent versions

#$gzip   = 'gzip';
#$bzip2  = 'bzip2';
#$lzop   = 'lzop';
#$rpm2cpio   = ['rpm2cpio.pl','rpm2cpio'];
#$cabextract = 'cabextract';
#$uncompress = ['uncompress', 'gzip -d', 'zcat'];
#$unfreeze   = ['unfreeze', 'freeze -d', 'melt', 'fcat'];
#$arc        = ['nomarch', 'arc'];
#$unarj      = ['arj', 'unarj'];
#$unrar      = ['rar', 'unrar'];
#$zoo    = 'zoo';
#$lha    = 'lha';
#$cpio   = ['gcpio','cpio'];
#$dspam  = 'dspam';

$append_header_fields_to_bottom=0;

###$X_HEADER_TAG  = 'X-Virus-Scanned';
###$X_HEADER_LINE = "by amavisd-new at $mydomain [Gnorri: ON]";
$X_HEADER_TAG  = 'X-INFNTO-Scanned';
$X_HEADER_LINE = "by amavisd-new [2.4.5] at $mydomain [Opossum: ON]";

$MAXLEVELS = 14;
$MAXFILES = 1500;
```

```
$MIN_EXPANSION_QUOTA =      100*1024;  # bytes  (default undef, not en-
forced)
$MAX_EXPANSION_QUOTA = 300*1024*1024;  # bytes  (default undef, not en-
forced)

$defang_virus          = 1;  # MIME-wrap passed infected mail
$defang_banned         = 0;  # MIME-wrap passed mail containing banned
name
$defang_bad_header     = 0;
$defang_undecipherable = 0;
$defang_spam           = 0;

# OTHER MORE COMMON SETTINGS (defaults may suffice):

# $notify_method  = 'smtp:[127.0.0.1]:10025';
$notify_method = 'pipe:flags=q argv=/usr/sbin/sendmail -Ac -odd -i -f
${sender} -- ${recipient}';
# $forward_method = 'smtp:[127.0.0.1]:10025';  # set to undef with
milter!
$forward_method = undef;

$final_virus_destiny      = D_DISCARD;
$final_banned_destiny     = D_PASS;
$final_spam_destiny       = D_REJECT;
$final_bad_header_destiny = D_PASS;

# SOME OTHER VARIABLES WORTH CONSIDERING (see amavisd.conf-default for
all)

# $warnbadhsender,
# $warnvirusrecip, $warnbannedrecip, $warnbadhrecip, (or
@warn*recip_maps)
#
# @bypass_virus_checks_maps, @bypass_spam_checks_maps,
# @bypass_banned_checks_maps, @bypass_header_checks_maps,
#
# @virus_lovers_maps, @spam_lovers_maps,
# @banned_files_lovers_maps, @bad_header_lovers_maps,
#
# @blacklist_sender_maps, @score_sender_maps,
#
# $virus_quarantine_to, $banned_quarantine_to,
# $bad_header_quarantine_to, $spam_quarantine_to,
#
# $defang_bad_header, $defang_undecipherable, $defang_spam


# REMAINING IMPORTANT VARIABLES ARE LISTED HERE BECAUSE OF LONGER
ASSIGNMENTS

@viruses_that_fake_sender_maps = (new_RE(
  [qr'\bEICAR\b'i => 0],            # av test pattern name
  [qr'^(WM97|OF97|Joke\.)'i => 0],  # adjust names to match your AV
scanner
  [qr/.*/ => 1],  # true for everything else
));
```

```
$bypass_decode_parts = 0;

@keep_decoded_original_maps = (new_RE(
# qr'^MAIL$',   # retain full original message for virus checking (can
be slow)
  qr'^MAIL-UNDECIPHERABLE$', # recheck full mail if it contains undeci-
pherables
  qr'^(ASCII(?! cpio)|text|uuencoded|xxencoded|binhex)'i,
));


$banned_namepath_re = undef;  # disable new-style

$banned_filename_re = new_RE(
# qr'^UNDECIPHERABLE$',  # is or contains any undecipherable components

  # block certain double extensions anywhere in the base name
# qr'\.[^./]*\.(exe|vbs|pif|scr|bat|cmd|com|dll)\.?$'i,

# qr'[{}]',      # curly braces in names (serve as Class ID extensions -
CLSID)

# qr'^application/x-msdownload$'i,                  # block these MIME
types
# qr'^application/x-msdos-program$'i,
# qr'^application/hta$'i,

# qr'^message/partial$'i, qr'^message/external-body$'i, # rfc2046 MIME
types

# [ qr'^\.(Z|gz|bz2)$'           => 0 ],  # allow any type in Unix-
compressed
# [ qr'^\.(rpm|cpio|tar)$'       => 0 ],  # allow any type in Unix ar-
chives
# [ qr'^\.(zip|rar|arc|arj|zoo)$'=> 0 ],  # allow any type within such
archives

# qr'.\.(exe|vbs|pif|scr|bat|cmd|com)$'i, # banned extension - basic
# qr'.\.(ade|adp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|
#        jse|lnk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|vb|
#        vbe|vbs|wsc|wsf|wsh|
#        app|fxp|prg|mdw|mdt|ops)$'ix,    # banned extension - long

# qr'.\.(mim|b64|bhx|hqx|xxe|uu|uue)$'i,  # banned extension - WinZip
vulnerab.

# qr'^\.(exe-ms)$',                       # banned file(1) types
# qr'^\.(exe|lha|tnef|cab)$',             # banned file(1) types
);
# See http://support.microsoft.com/default.aspx?scid=kb;EN-US;q262631
# and http://www.cknow.com/vtutor/vtextensions.htm


# ENVELOPE SENDER SOFT-WHITELISTING / SOFT-BLACKLISTING
```

```
@score_sender_maps = ({ # a by-recipient hash lookup table,
                        # results from all matching recipient tables are
summed

# ## per-recipient personal tables  (NOTE: positive: black, negative:
white)
# 'user1@example.com'  => [{'bla-mobile.press@example.com' => 10.0}],
# 'user3@example.com'  => [{'.ebay.com'                => -3.0}],
# 'user4@example.com'  => [{'cleargreen@cleargreen.com' => -7.0,
#                           '.cleargreen.com'          => -5.0}],

 'Alberto.DAmbrosio@to.infn.it'  => [{' Another.User@dmn.it' => -50.0}],
 ' Another.User@dmn.it'  => [{'Alberto.DAmbrosio@to.infn.it' => -50.0}],

  ## site-wide opinions about senders (the '.' matches any recipient)
  '.' => [  # the _first_ matching sender determines the score boost

   new_RE(  # regexp-type lookup table, just happens to be all soft-
blacklist
    [qr'^(bulkmail|offers|cheapbenefits|earnmoney|foryou)@'i         =>
5.0],
    [qr'^(greatcasino|investments|lose_weight_today|market\.alert)@'i=>
5.0],
    [qr'^(money2you|MyGreenCard|new\.tld\.registry|opt-out|opt-in)@'i=>
5.0],
    [qr'^(optin|saveonlsmoking2002k|specialoffer|specialoffers)@'i   =>
5.0],
    [qr'^(stockalert|stopsnoring|wantsome|workathome|yesitsfree)@'i  =>
5.0],
    [qr'^(your_friend|greatoffers)@'i                                =>
5.0],
    [qr'^(inkjetplanet|marketopt|MakeMoney)\d*@'i                    =>
5.0],
   ),

   { # a hash-type lookup table (associative array)
     'nobody@cert.org'                       => -3.0,
     'cert-advisory@us-cert.gov'             => -3.0,
     'owner-alert@iss.net'                   => -3.0,
     'slashdot@slashdot.org'                 => -3.0,
     'bugtraq@securityfocus.com'             => -3.0,
     'ntbugtraq@listserv.ntbugtraq.com'      => -3.0,
     'security-alerts@linuxsecurity.com'     => -3.0,
     'mailman-announce-admin@python.org'     => -3.0,
     'amavis-user-admin@lists.sourceforge.net'=> -3.0,
     'notification-return@lists.sophos.com'  => -3.0,
     'owner-postfix-users@postfix.org'       => -3.0,
     'owner-postfix-announce@postfix.org'    => -3.0,
     'owner-sendmail-announce@lists.sendmail.org'   => -3.0,
     'sendmail-announce-request@lists.sendmail.org' => -3.0,
     'donotreply@sendmail.org'               => -3.0,
     'ca+envelope@sendmail.org'              => -3.0,
     'noreply@freshmeat.net'                 => -3.0,
     'owner-technews@postel.acm.org'         => -3.0,
     'ietf-123-owner@loki.ietf.org'          => -3.0,
     'cvs-commits-list-admin@gnome.org'      => -3.0,
```

```
    'rt-users-admin@lists.fsck.com'          => -3.0,
    'clp-request@comp.nus.edu.sg'            => -3.0,
    'surveys-errors@lists.nua.ie'            => -3.0,
    'emailnews@genomeweb.com'                => -5.0,
    'yahoo-dev-null@yahoo-inc.com'           => -3.0,
    'returns.groups.yahoo.com'               => -3.0,
    'clusternews@linuxnetworx.com'           => -3.0,
    lc('lvs-users-admin@LinuxVirtualServer.org')    => -3.0,
    lc('owner-textbreakingnews@CNNIMAIL12.CNN.COM') => -5.0,

    # soft-blacklisting (positive score)
    'sender@example.net'                     =>  3.0,
    '.example.net'                           =>  1.0,

  },
 ],  # end of site-wide tables
});

@decoders = (
  ['mail', \&do_mime_decode],
  ['asc',  \&do_ascii],
  ['uue',  \&do_ascii],
  ['hqx',  \&do_ascii],
  ['ync',  \&do_ascii],
  ['F',    \&do_uncompress, ['unfreeze','freeze -d','melt','fcat'] ],
  ['Z',    \&do_uncompress, ['uncompress','gzip -d','zcat'] ],
  ['gz',   \&do_gunzip],
  ['gz',   \&do_uncompress,  'gzip -d'],
  ['bz2',  \&do_uncompress,  'bzip2 -d'],
  ['lzo',  \&do_uncompress,  'lzop -d'],
  ['rpm',  \&do_uncompress, ['rpm2cpio.pl','rpm2cpio'] ],
  ['cpio', \&do_pax_cpio,   ['pax','gcpio','cpio'] ],
  ['tar',  \&do_pax_cpio,   ['pax','gcpio','cpio'] ],
  ['tar',  \&do_tar],
  ['deb',  \&do_ar,          'ar'],
# ['a',    \&do_ar,          'ar'],  # unpacking .a seems an overkill
  ['zip',  \&do_unzip],
  ['rar',  \&do_unrar,      ['rar','unrar'] ],
  ['arj',  \&do_unarj,      ['arj','unarj'] ],
  ['arc',  \&do_arc,        ['nomarch','arc'] ],
  ['zoo',  \&do_zoo,         'zoo'],
  ['lha',  \&do_lha,         'lha'],
# ['doc',  \&do_ole,         'ripole'],
  ['cab',  \&do_cabextract,  'cabextract'],
  ['tnef', \&do_tnef_ext,    'tnef'],
  ['tnef', \&do_tnef],
  ['exe',  \&do_executable, ['rar','unrar'], 'lha', ['arj','unarj'] ],
);


@av_scanners = (

# ### http://www.vanja.com/tools/sophie/
# ['Sophie',
#   \&ask_daemon, ["{}/\n", '/var/run/sophie'],
```

```
#   qr/(?x)^ 0+ ( : | [\000\r\n]* $)/,  qr/(?x)^ 1 ( : | [\000\r\n]*
$)/,
#   qr/(?x)^ [-+]? \d+ : (.*?) [\000\r\n]* $/ ],

### http://www.csupomona.edu/~henson/www/projects/SAVI-Perl/
#['Sophos SAVI', \&sophos_savi ],

# Commented out because the name 'sweep' clashes with Debian and FreeBSD
# package/port of an audio editor. Make sure the correct 'sweep' is
found
# in the path when enabling.
#
 ### http://www.sophos.com/   - backs up Sophie or SAVI-Perl
# ['Sophos Anti Virus (sweep)', 'sweep',
#   '-nb -f -all -rec -ss -sc -archive -cab -tnef --no-reset-atime {}',
#   [0,2], qr/Virus .*? found/,
#   qr/^>>> Virus(?: fragment)? '?(.*?)'? found/,
# ],
# other options to consider: -mime -oe -idedir=/usr/local/sav

# ### http://www.clamav.net/
# ['ClamAV-clamd',
#   \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd"],
#   qr/\bOK$/, qr/\bFOUND$/,
#   qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
# # NOTE: run clamd under the same user as amavisd;  match the socket
# # name (LocalSocket) in clamav.conf to the socket name in this entry
# # When running chrooted one may prefer: ["CONTSCAN
{}\n","$MYHOME/clamd"],

# ### http://www.clamav.net/ and CPAN  (memory-hungry! clamd is pre-
ferred)
['Mail::ClamAV', \&ask_clamav, "*", [0], [1], qr/^INFECTED: (.+)/],

# ### http://www.openantivirus.org/
# ['OpenAntiVirus ScannerDaemon (OAV)',
#   \&ask_daemon, ["SCAN {}\n", '127.0.0.1:8127'],
#   qr/^OK/, qr/^FOUND: /, qr/^FOUND: (.+)/ ],

# ### http://www.vanja.com/tools/trophie/
# ['Trophie',
#   \&ask_daemon, ["{}/\n", '/var/run/trophie'],
#   qr/(?x)^ 0+ ( : | [\000\r\n]* $)/,  qr/(?x)^ 1 ( : | [\000\r\n]*
$)/,
#   qr/(?x)^ [-+]? \d+ : (.*?) [\000\r\n]* $/ ],

# ### http://www.grisoft.com/
# ['AVG Anti-Virus',
#   \&ask_daemon, ["SCAN {}\n", '127.0.0.1:55555'],
#   qr/^200/, qr/^403/, qr/^403 .*?: ([^\r\n]+)/ ],

# ### http://www.f-prot.com/
# ['FRISK F-Prot Daemon',
#   \&ask_daemon,
#   ["GET {}/*?-dumb%20-archive%20-packed HTTP/1.0\r\n\r\n",
#     ['127.0.0.1:10200','127.0.0.1:10201','127.0.0.1:10202',
```

```
#      '127.0.0.1:10203','127.0.0.1:10204'] ],
#   qr/(?i)<summary[^>]*>clean<\/summary>/,
#   qr/(?i)<summary[^>]*>infected<\/summary>/,
#   qr/(?i)<name>(.+)<\/name>/ ],

# ### http://www.sald.com/, http://www.dials.ru/english/,
http://www.drweb.ru/
# ['DrWebD', \&ask_daemon,   # DrWebD 4.31 or later
#   [pack('N',1).  # DRWEBD_SCAN_CMD
#    pack('N',0x00280001).   # DONT_CHANGEMAIL, IS_MAIL, RETURN_VIRUSES
#    pack('N',     # path length
#      length("$TEMPBASE/amavis-yyyymmddTHHMMSS-xxxxx/parts/pxxx")).
#    '{}/*'.       # path
#    pack('N',0).  # content size
#    pack('N',0),
#    '/var/drweb/run/drwebd.sock',
#  # '/var/amavis/var/run/drwebd.sock',   # suitable for chroot
#  # '/usr/local/drweb/run/drwebd.sock',  # FreeBSD drweb ports default
#  # '127.0.0.1:3000',                    # or over an inet socket
#   ],
#   qr/\A\x00(\x10|\x11)\x00\x00/s,              # IS_CLEAN, EVAL_KEY
#   qr/\A\x00(\x00|\x01)\x00(\x20|\x40|\x80)/s,  # KNOWN_V, UNKNOWN_V,
V._MODIF
#   qr/\A.{12}(?:infected with )?([^\x00]+)\x00/s,
# ],
# # NOTE: If using amavis-milter, change length to:
# # length("$TEMPBASE/amavis-milter-xxxxxxxxxxxxxx/parts/pxxx").

# ### http://www.kaspersky.com/  (in the 'file server version')
# ['KasperskyLab AVP - aveclient',
#
['/usr/local/kav/bin/aveclient','/usr/local/share/kav/bin/aveclient',
#    '/opt/kav/bin/aveclient','aveclient'],
#   '-p /var/run/aveserver -s {}/*', [0,3,6,8],
qr/\b(INFECTED|SUSPICION)\b/,
#   qr/(?:INFECTED|SUSPICION) (.+)/,
# ],

# ### http://www.kaspersky.com/
# ['KasperskyLab AntiViral Toolkit Pro (AVP)', ['avp'],
#   '-* -P -B -Y -O- {}', [0,3,6,8], [2,4],    # any use for -A -K   ?
#   qr/infected: (.+)/,
#   sub {chdir('/opt/AVP') or die "Can't chdir to AVP: $!"},
#   sub {chdir($TEMPBASE) or die "Can't chdir back to $TEMPBASE $!"},
# ],

# ### The kavdaemon and AVPDaemonClient have been removed from Kasperky
# ### products and replaced by aveserver and aveclient
# ['KasperskyLab AVPDaemonClient',
#   [ '/opt/AVP/kavdaemon',       'kavdaemon',
#     '/opt/AVP/AvpDaemonClient', 'AvpDaemonClient',
#     '/opt/AVP/AvpTeamDream',    'AvpTeamDream',
#     '/opt/AVP/avpdc', 'avpdc' ],
#   "-f=$TEMPBASE {}", [0,8], [3,4,5,6], qr/infected: ([^\r\n]+)/ ],
#   # change the startup-script in /etc/init.d/kavd to:
#   #   DPARMS="-* -Y -dl -f=/var/amavis /var/amavis"
```

```
#   #   (or perhaps:   DPARMS="-I0 -Y -* /var/amavis" )
#   # adjusting /var/amavis above to match your $TEMPBASE.
#   # The '-f=/var/amavis' is needed if not running it as root, so it
#   # can find, read, and write its pid file, etc., see 'man kavdaemon'.
#   # defUnix.prf: there must be an entry "*/var/amavis" (or whatever
#   #   directory $TEMPBASE specifies) in the 'Names=' section.
#   # cd /opt/AVP/DaemonClients; configure; cd Sample; make
#   # cp AvpDaemonClient /opt/AVP/
#   # su - vscan -c "${PREFIX}/kavdaemon ${DPARMS}"

# ### http://www.hbedv.com/ or http://www.centralcommand.com/
# ['H+BEDV AntiVir or CentralCommand Vexira Antivirus',
#   ['antivir','vexira'],
#   '--allfiles -noboot -nombr -rs -s -z {}', [0], qr/ALERT:|VIRUS:/,
#   qr/(?x)^\s* (?: ALERT: \s* (?: \[ | [^']* ' ) |
#        (?i) VIRUS:\ .*?\ virus\ '?) ( [^\]\s']+ )/ ],
#   # NOTE: if you only have a demo version, remove -z and add 214, as
in:
#   #  '--allfiles -noboot -nombr -rs -s {}', [0,214],
qr/ALERT:|VIRUS:/,

# ### http://www.commandsoftware.com/
# ['Command AntiVirus for Linux', 'csav',
#   '-all -archive -packed {}', [50], [51,52,53],
#   qr/Infection: (.+)/ ],

# ### http://www.symantec.com/
# ['Symantec CarrierScan via Symantec CommandLineScanner',
#   'cscmdline', '-a scan -i 1 -v -s 127.0.0.1:7777 {}',
#   qr/^Files Infected:\s+0$/, qr/^Infected\b/,
#   qr/^(?:Info|Virus Name):\s+(.+)/ ],

# ### http://www.symantec.com/
# ['Symantec AntiVirus Scan Engine',
#   'savsecls', '-server 127.0.0.1:7777 -mode scanrepair -details -
verbose {}',
#   [0], qr/^Infected\b/,
#   qr/^(?:Info|Virus Name):\s+(.+)/ ],
#   # NOTE: check options and patterns to see which entry better applies

# ### http://www.f-secure.com/products/anti-virus/
# ['F-Secure Antivirus', 'fsav',
#   '--dumb --mime --archive {}', [0], [3,8],
#   qr/(?:infection|Infected|Suspected): (.+)/ ],

# ['CAI InoculateIT', 'inocucmd',  # retired product
#   '-sec -nex {}', [0], [100],
#   qr/was infected by virus (.+)/ ],
# # see: http://www.flatmtn.com/computer/Linux-Antivirus_CAI.html

# ### http://www3.ca.com/Solutions/Product.asp?ID=156  (ex InoculateIT)
# ['CAI eTrust Antivirus', 'etrust-wrapper',
#   '-arc -nex -spm h {}', [0], [101],
#   qr/is infected by virus: (.+)/ ],
#   # NOTE: requires suid wrapper around inocmd32; consider flag: -mod
reviewer
```

```
#   # see http://marc.theaimsgroup.com/?l=amavis-user&m=109229779912783

# ### http://mks.com.pl/english.html
# ['MkS_Vir for Linux (beta)', ['mks32','mks'],
#   '-s {}/*', [0], [1,2],
#   qr/--[ \t]*(.+)/ ],

# ### http://mks.com.pl/english.html
# ['MkS_Vir daemon', 'mksscan',
#   '-s -q {}', [0], [1..7],
#   qr/^... (\S+)/ ],

# ### http://www.nod32.com/
# ['ESET Software NOD32', 'nod32',
#   '-all -subdir+ {}', [0], [1,2],
#   qr/^.+? - (.+?)\s*(?:backdoor|joke|trojan|virus|worm)/ ],

# ### http://www.nod32.com/
# ['ESET Software NOD32 - Client/Server Version', 'nod32cli',
#   '-a -r -d recurse --heur standard {}', [0], [10,11],
#   qr/^\S+\s+infected:\s+(.+)/ ],

# Experimental, based on posting from Rado Dibarbora (Dibo) on 2002-05-
31
# ['ESET Software NOD32 Client/Server (NOD32SS)',
#   \&ask_daemon2,    # greets with 200, persistent, terminate with QUIT
#   ["SCAN {}/*\r\n", '127.0.0.1:8448' ],
#   qr/^200 File OK/, qr/^201 /, qr/^201 (.+)/ ],

# ### http://www.norman.com/products_nvc.shtml
# ['Norman Virus Control v5 / Linux', 'nvcc',
#   '-c -l:0 -s -u {}', [0], [1],
#   qr/(?i).* virus in .* -> \'(.+)\'/ ],

# ### http://www.pandasoftware.com/
# ['Panda Antivirus for Linux', ['pavcl'],
#   '-aut -aex -heu -cmp -nbr -nor -nso -eng {}',
#   qr/Number of files infected[ .]*: 0+(?!\d)/,
#   qr/Number of files infected[ .]*: 0*[1-9]/,
#   qr/Found virus :\s*(\S+)/ ],

# ### http://www.pandasoftware.com/
# ['Panda Antivirus for Linux', ['pavcl'],
#   '-TSR -aut -aex -heu -cmp -nbr -nor -nso -eng {}',
#   [0], [0x10, 0x30, 0x50, 0x70, 0x90, 0xB0, 0xD0, 0xF0],
#   qr/Found virus :\s*(\S+)/ ],

# GeCAD AV technology is acquired by Microsoft; RAV has been discontin-
ued.
# Check your RAV license terms before fiddling with the following two
lines!
# ['GeCAD RAV AntiVirus 8', 'ravav',
#   '--all --archive --mail {}', [1], [2,3,4,5], qr/Infected: (.+)/ ],
# # NOTE: the command line switches changed with scan engine 8.5 !
# # (btw, assigning stdin to /dev/null causes RAV to fail)
```

```
# ### http://www.nai.com/
# ['NAI McAfee AntiVirus (uvscan)', 'uvscan',
#   '--secure -rv --mime --summary --noboot - {}', [0], [13],
#   qr/(?x) Found (?:
#       \ the\ (.+)\ (?:virus|trojan)  |
#       \ (?:virus|trojan)\ or\ variant\ ([^ ]+)  |
#       :\ (.+)\ NOT\ a\ virus)/,
# # sub {$ENV{LD_PRELOAD}='/lib/libc.so.6'},
# # sub {delete $ENV{LD_PRELOAD}},
# ],
# # NOTE1: with RH9: force the dynamic linker to look at /lib/libc.so.6
before
# # anything else by setting environment variable
LD_PRELOAD=/lib/libc.so.6
# # and then clear it when finished to avoid confusing anything else.
# # NOTE2: to treat encrypted files as viruses replace the [13] with:
# #  qr/^\s{5,}(Found|is password-protected|.*(virus|trojan))/

# ### http://www.virusbuster.hu/en/
# ['VirusBuster', ['vbuster', 'vbengcl'],
#   # VirusBuster Ltd. does not support the daemon version for the work-
station
#   # engine (vbuster-eng-1.12-linux-i386-libc6.tgz) any longer. The
names of
#   # binaries, some parameters AND return codes have changed (from 3 to
1).
#   "{} -ss -i '*' -log=$MYHOME/vbuster.log", [0], [1],
#   qr/: '(.*)' - Virus/ ],

# ### http://www.virusbuster.hu/en/
# ['VirusBuster (Client + Daemon)', 'vbengd',
#   # HINT: for an infected file it always returns 3,
#   # although the man-page tells a different story
#   '-f -log scandir {}', [0], [3],
#   qr/Virus found = (.*);/ ],

# ### http://www.cyber.com/
# ['CyberSoft VFind', 'vfind',
#   '--vexit {}/*', [0], [23], qr/##==>>>> VIRUS ID: CVDL (.+)/,
# # sub {$ENV{VSTK_HOME}='/usr/lib/vstk'},
# ],

# ### http://www.ikarus-software.com/
# ['Ikarus AntiVirus for Linux', 'ikarus',
#   '{}', [0], [40], qr/Signature (.+) found/ ],

# ### http://www.bitdefender.com/
# ['BitDefender', 'bdc',
#   '--all --arc --mail {}', qr/^Infected files *:0+(?!\d)/,
#   qr/^(?:Infected files|Identified viruses|Suspect files) *:0*[1-9]/,
#   qr/(?:suspected|infected): (.*)(?:\033|$)/ ],

);


@av_scanners_backup = (
```

```
  ### http://www.clamav.net/   - backs up clamd or Mail::ClamAV
  ['ClamAV-clamscan', 'clamscan',
    "--stdout --disable-summary -r --tempdir=$TEMPBASE {}", [0], [1],
    qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],

# ### http://www.f-prot.com/   - backs up F-Prot Daemon
# ['FRISK F-Prot Antivirus', ['f-prot','f-prot.sh'],
#   '-dumb -archive -packed {}', [0,8], [3,6],
#   qr/Infection: (.+)/ ],

# ### http://www.trendmicro.com/   - backs up Trophie
# ['Trend Micro FileScanner', ['/etc/iscan/vscan','vscan'],
#   '-za -a {}', [0], qr/Found virus/, qr/Found virus (.+) in/ ],

# ### http://www.sald.com/, http://drweb.imshop.de/   - backs up DrWebD
# ['drweb - DrWeb Antivirus',
#   ['/usr/local/drweb/drweb', '/opt/drweb/drweb', 'drweb'],
#   '-path={} -al -go -ot -cn -upn -ok-',
#   [0,32], [1,9,33], qr' infected (?:with|by)(?: virus)? (.*)$'],

# ['KasperskyLab kavscanner', ['/opt/kav/bin/kavscanner','kavscanner'],
#   '-i1 -xp {}', [0,10,15], [5,20,21,25],
#   qr/(?:CURED|INFECTED|CUREFAILED|WARNING|SUSPICION) (.*)/ ,
#   sub {chdir('/opt/kav/bin') or die "Can't chdir to kav: $!"},
#   sub {chdir($TEMPBASE) or die "Can't chdir back to $TEMPBASE $!"},
# ],

# Commented out because the name 'sweep' clashes with Debian and FreeBSD
# package/port of an audio editor. Make sure the correct 'sweep' is
found
# in the path when enabling.
#
# ### http://www.sophos.com/   - backs up Sophie or SAVI-Perl
# ['Sophos Anti Virus (sweep)', 'sweep',
#   '-nb -f -all -rec -ss -sc -archive -cab -tnef --no-reset-atime {}',
#   [0,2], qr/Virus .*? found/,
#   qr/^>>> Virus(?: fragment)? '?(.*?)'? found/,
# ],
# other options to consider: -mime -oe -idedir=/usr/local/sav

# always succeeds (uncomment to consider mail clean if all other scan-
ners fail)
['always-clean', sub {0}],

);


1;  # insure a defined return
```

APPENDICE-I
Istruzioni per l'installazione di milter-greylist 4.0 su piattaforma Unix

Prima dell'installazione vera e propria è necessario effettuare qualche operazione preliminare, riguardanti la (ri)compilazione e la (re)installazione del **sendmail**.

Tali passi, già riportati nell'APPENDICE-G, comprendono la rigenerazione del file **sendmail.cf** (operazione già inclusa nell'APPENDICE-A), dopo aver opportunamente modificato il file **sendmail.mc** (modifiche già presenti nell'APPENDICE-C).
A questo punto è possibile procedere con l'installazione vera e propria del Sw. Solo per questo caso specifico si è deciso di utilizzare la tecnologia **RPM** di Red Hat.

Pacchetti **RPM** necessari:

```
geoip-1.4.0-1.el4.rf.i386.rpm
GeoIP.dat
libspf2-1.2.5-3.i386.rpm
libspf2-progs-1.2.5-3.i386.rpm
milter-greylist-4.0-4.jkf.el4.i386.rpm
```

Procedere con la loro installazione:

```
# rpm -Uvh geoip-1.4.0-1.el4.rf.i386.rpm
# cp GeoIP.dat /usr/share/GeoIP/

# rpm -Uvh libspf2-1.2.5-3.i386.rpm \
           libspf2-progs-1.2.5-3.i386.rpm

# rpm -Uvh milter-greylist-4.0-4.jkf.el4.i386.rpm
```

Adattare lo script di startup al proprio ambiente:

```
# emacs /etc/rc.d/init.d/milter-greylist

# mv /var/milter-greylist /var/run/milter-greylist
# chown -R smmsp:smmsp /var/run/milter-greylist
# chmod 750 /var/run/milter-greylist
```

Adattare il file di configurazione secondo le proprie necessità:

```
# emacs /usr/local+/etc/greylist.conf
```

Abilitare lo script di startup ed avviare il corrispondente servizio:

```
# chkconfig --add milter-greylist
# chkconfig milter-greylist on
# service milter-greylist start
```

Abilitare il milter in **`sendmail.mc`**:

```
INPUT_MAIL_FILTER(`greylist',`S=local:/var/run/milter-greylist/milter-
greylist.sock', F=T, T=C:5m;S:5m;R:5m;E:5m')dnl
define(`confMILTER_MACROS_CONNECT', `j, {if_addr}')dnl
define(`confMILTER_MACROS_HELO', `{verify}, {cert_subject}')dnl
define(`confMILTER_MACROS_ENVFROM', `i, {auth_authen}')dnl

# make -C /etc/mail
```

Riavviare il **sendmail**:

```
service sendmail stop
service sendmail start
```

Non è escluso possa rendersi necessario un watcher:

```
#!/bin/sh
RETVAL=0
/sbin/service milter-greylist status
RETVAL=$?
if [ $RETVAL –ne 0 ];
then /sbin/service milter-greylist restart
else echo “diag-message”
fi
```

APPENDICE-J
Istruzioni per l'installazione di SpamAssassin 3.2.4 su piattaforma Unix

L'installazione può avvenire in due modi diversi: via CPAN (Comprehensive Perl Archive Network, http://www.cpan.org/), o in maniera tradizionale partendo dal tar-file.

Via CPAN è banalissima:

```
# perl -MCPAN -e shell
cpan> o conf prerequisites_policy ask
cpan> install Mail::SpamAssassin
cpan> quit
```

Volendo procedere in maniera tradizionale, innanzitutto spacchettare il tar-file in una directory locale:

```
# cd /usr/local++/
# gzip –dc Mail-SpamAssassin-3.2.4.tar.gz | tar –xvf –
# chown –R root:system ./Mail-SpamAssassin-3.2.4
```

Nel file **`/usr/local++/Mail-SpamAssassin-3.2.4/INSTALL`** esiste un elenco di moduli Perl e programmi esterni che devono essere preliminarmente installati. Inoltre, in caso di upgrade da precedenti versioni, è bene rimuovere totalmente i files relativi ai database (nel nostro caso centralizzati) del classificatore bayesiano & dell'auto_whitelist, in quanto sovente incompatibili tra versioni diverse del Sw. Verificati tutti i requisiti finora elencati, si può continuare con l'installazione:

```
# cd /usr/local++/Mail-SpamAssassin-3.2.4/
# perl Makefile.PL PREFIX=/usr/local+
# make
# make test
# make install
```

N.B.: Non va attivato alcun tipo di daemon (**spamd**) e/o servizio.

Il file di configurazione **`/usr/local+/etc/mail/spamassassin/local.cf`** è riportato nell'APPENDICE-K.

APPENDICE-K
File di configurazione per SpamAssassin (local.cf)

```
# This is the right place to customize your installation of SA.
# See 'perldoc Mail::SpamAssassin::Conf' for details of what can be
# tweaked.
#
###########################################################################
###
#

required_score              3.5

skip_rbl_checks             0

score RCVD_IN_MAPS_RBL      3.5
score RCVD_IN_MAPS_RSS      3.5
score RCVD_IN_MAPS_DUL      1
score RCVD_IN_MAPS_NML      2
score RCVD_IN_MAPS_OPS      2

score RCVD_IN_RBL           3.5
score RCVD_IN_RSS           3.5
score RCVD_IN_DUL           1
score RCVD_IN_DUL_FH        1
score RCVD_IN_BL_SPAMCOP_NET 3.5

score RCVD_IN_OSIRUSOFT_COM  0
score X_OSIRU_DUL           0
score X_OSIRU_DUL_FH        0
score X_OSIRU_OPEN_RELAY    0
score X_OSIRU_SPAM_SRC      0
score X_OSIRU_SPAMWARE_SITE  0

score HABEAS_SWE            0

#score  SPF_PASS            0
#score  SPF_FAIL            0
#score  SPF_SOFTFAIL        0
#score  SPF_HELO_PASS       0
#score  SPF_HELO_FAIL       0
#score  SPF_HELO_SOFTFAIL   0

score BAYES_00              -1.665
score BAYES_05              -0.925
score BAYES_20              -0.730
score BAYES_40              -0.276
score BAYES_50              1.567
score BAYES_60              3.515
score BAYES_80              3.608
score BAYES_95              3.514
score BAYES_99              4.070

score DCC_CHECK             3.5
```

```
score DATE_IN_FUTURE_96_XX  0.001

header LOCAL_CERT_GNORRI_ON Received =~ /\[Gnorri\: ON\].+verify=OK\)/
score  LOCAL_CERT_GNORRI_ON -15

rewrite_header Subject      ***SPAM?***

report_safe                 0

### Obsolete ###
#report_header              1
#use_terse_report           1
#defang_mime                0

use_bayes                   1
use_bayes_rules             1
bayes_auto_learn            1
bayes_learn_to_journal      1
bayes_learn_during_report   1
bayes_auto_expire           0

bayes_sql_override_username vscan
bayes_store_module          Mail::SpamAssassin::BayesStore::MySQL
bayes_sql_dsn               DBI:mysql:mailserver-
sa:titicaca.to.infn.it:3306
bayes_sql_username          US3RN4M3
bayes_sql_password          P4SSW0RD

whitelist_from              events@news.taborcommunications.com
whitelist_from              DS4700@to.infn.it

use_auto_whitelist          1

auto_whitelist_factory  Mail::SpamAssassin::SQLBasedAddrList
user_awl_dsn            DBI:mysql:mailserver-sa:titicaca.to.infn.it:3306
user_awl_sql_username   US3RN4M3
user_awl_sql_password   P4SSW0RD

use_razor2              1

use_pyzor               1
pyzor_path              /usr/local+/bin/pyzor

use_dcc                 1
dcc_dccifd_path         /var/run/dccifd.sock
dcc_home                /usr/local+/dcc

dns_available test: to.infn.it ph.unito.it unito.it
```

APPENDICE-L
Istruzioni per la gestione del filtro anti-spam (SpamAssassin)

Con il filtro abilitato, le E-Mail etichettate come "SPAM" a bassa probabilità vengono consegnate nella **INBOX**, o smistate verso un folder chiamato di default **Probably-Spam**, in maniera tale da poter poi verificare manualmente l'assenza dei "*Falsi Positivi*" di cui sopra. Quelle con alta probabilità, invece, vengono immediatamente rifiutate o, a scelta dell'utente, spostate nel folder **Almost-Certainly-Spam**.

Nell'header completo di ciascuna E-Mail sono riportate delle informazioni riguardanti il risultato dei test effettuati dallo SpamAssassin su quel particolare messaggio (vedi campi "*X-Spam-*").

Per default, il filtro è già attivo per tutti gli utenti. Per l'utente che eventualmente non dovesse gradire questa modalità di funzionamento, sono disponibili vari livelli di personalizzazione e/o disabilitazione delle varie funzionalità (*opt-out*):

1. ***REJECT***

   Il rifiuto (REJECT) immediato dei messaggi identificati come "SPAM" ad alta probabilità è caratterizzato dai seguenti pro e contro:

   PRO:

   - Assenza di messaggi da controllare nel folder **`Almost-Certainly-Spam`**
   - Risparmio di spazio-disco in conseguenza del minor numero di messaggi smistati in tali folder.

   CONTRO:

   - Data la natura statistica del filtro, ci sarà sempre un fondo (probabilità dello 0.005%) di "*Falsi Positivi*" che, quindi, verranno rigettati. In tal caso, comunque, il mittente viene informato del motivo del rifiuto.

   Gli utenti che lo desiderino, possono richiedere la disattivazione di questa funzionalità per la loro posta, tenendo però ben presente che:

   - La NON abilitazione del REJECT sulla posta indirizzata ad una certa username/casella postale non si traduce nel non transito attraverso il filtro anti-spam (è disabilitato il controllo, non il transito!).
   - I messaggi non rifiutati verranno consegnati nella INBOX, o smistati nel folder **`Almost-Certainly-Spam`**.
   - Occorrerà verificare manualmente che nel folder di cui sopra non siano presenti dei "*Falsi Positivi*".

   Il semplice passaggio attraverso il filtro (con o senza abilitazione del REJECT) è segnalata nell'header completo delle E-Mail dalla riga seguente:

   ```
   X-INFNTO-Scanned: by amavisd-new [2.X.Y] at to.infn.it [Opossum: ON]
   ```

2. ***SMISTAMENTO***

Per default, le E-Mail ritenute SPAM, quando non rifiutate, vengono etichettate inserendo la stringa *****SPAM?***** nel *Subject*. Gli utenti che lo desiderino, possono smistare tali messaggi nel/i folder **Probably-Spam** e/o **Almost-Certainly-Spam** seguendo le seguenti istruzioni:

- Creare nella propria home-directory un file chiamato:

  .procmailrc

  contenente le seguenti istruzioni (se il file esiste già, inserirle all'inizio):

```
DROPPRIVS=yes
MAILDIR=$HOME/mail

:0:
* ^X-Spam-Level: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
Almost-Certainly-Spam

:0:
* ^X-Spam-Status: Yes
Probably-Spam
```

  Eventualmente, controllare che la variabile **MAILDIR** sia correttamente definita, in accordo con il MUA utilizzato (Alpine, Thunderbird, ecc..). Inoltre, è possibile modificare il nome dei folder ove vengono spostate le E-Mail etichettate come "SPAM": **Probably-Spam** e **Almost-Certainly-Spam**.

  In quest'ultimo folder (che è possibile non utilizzare eliminando la corrispondente parte di codice nel file **.procmailrc**) finiscono le E-Mail con una probabilità dello 0.005% di *"Falsi Positivi"*. Di conseguenza, il suo controllo può essere effettuato con meno frequenza.

- Creare nella propria home-directory il file:

  .forward

  contenente la seguente riga (doppi apici compresi!), nella quale è necessario sostituire a **UserName** la propria username Unix:

```
"|exec /usr/local/bin/procmail -f- || exit 75 #UserName"
```

- **N.B.:** Assicurarsi che le protezioni dei due file **.procmailrc** e **.forward** siano: **-rw-r--r--**

3. ***DISABILITAZIONE***

Gli utenti che lo desiderino, possono richiedere la disattivazione globale del filtro anti-spam per la loro posta, tenendo però ben presente che:

- La disabilitazione non si traduce nel non transito attraverso il filtro anti-spam (è disabilitato il controllo, non il transito!).

- Il semplice passaggio attraverso il filtro è segnalato nell'header completo delle E-Mail dalla riga seguente:

```
X-INFNTO-Scanned: by amavisd-new [2.X.Y] at to.infn.it [Opossum: ON]
```

Informazioni riguardanti il risultato dei test effettuati dallo **SpamAssassin** sono riportate nell'header completo di ciascuna E-Mail (vedi campi "*X-Spam-*").

Affinché il meccanismo statistico di correzione Bayesiano funzioni al meglio, ciascun utente può raccogliere i "*Falsi Negativi*" (messaggi erroneamente ritenuti non-spam) in uno specifico folder di posta chiamato **BAYES-Spam**, mentre i "*Falsi Positivi*" (messaggi erroneamente ritenuti spam) in un'altro folder chiamato **BAYES-Ham**.

Onde evitare erronei funzionamenti del filtro Bayesiano, è necessario che in tali folder vengano raccolti solamente quei messaggi che siano evidentemente dei "*Falsi Negativi*" o "*Falsi Positivi*".

In questi folder è opportuno che, periodicamente, vengano cancellate le E-Mail ivi presenti da più di un mese.

Un apposito script (APPENDICE-M) provvederà periodicamente (cron) a scandire questi folder e ad effettuare la correzione statistica dei risultati in base al feedback degli utenti.

APPENDICE-M
Script per la correzione statistica Bayesiana dei risultati dello SpamAssassin

```
#!/bin/sh

ELENCO="/tmp/sa$$.txt"
ypcat passwd > $ELENCO

while read LINEA; do
   UTENTE=`echo $LINEA | awk -F: '{print $1}'`
   HOMEDIR=`echo $LINEA | awk -F: '{print $6}'`
   SPAM="$HOMEDIR/mail/BAYES-Spam"
   HAM="$HOMEDIR/mail/BAYES-Ham"

   if [ -f "$SPAM" -o -f "$HAM" ]; then
#  echo "."
   echo ">>> Scanning username: $UTENTE"
   fi

   if [ -f "$SPAM" ]; then
#  echo "SPAM: \c"
   echo -n "SPAM: "
   /usr/local+/bin/sa-learn --mbox --spam   \
                -C /usr/local+/etc/mail/spamassassin/bayes/bayes $SPAM
   fi

   if [ -f "$HAM" ]; then
#  echo "HAM:  \c"
   echo -n "HAM:  "
   /usr/local+/bin/sa-learn --mbox --ham    \
                -C /usr/local+/etc/mail/spamassassin/bayes/bayes $HAM
   fi

done < $ELENCO

exit 0
```

APPENDICE-N
Biografie degli Autori

- **Alberto D'Ambrosio**

  Perito Elettronico Industriale, System Administrator c/o Servizio Calcolo INFN (dal 2000 della Sez. INFN di Torino, dal 1992 al 2000 dei Laboratori Nazionali del Gran Sasso), in precedenza analista/programmatore nel campo dell'automazione industriale presso aziende private.