ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Torino

INFN/TC-05/09
1 Luglio 2005

MANUALE DI INSTALLAZIONE DI UN SERVIZIO DI POSTA ELETTRONICA COMPLETO DI FILTRI ANTI-VIRUS E ANTI-SPAM

Giorgio Bar [1], Alberto D'Ambrosio [1], Franca De Giovanni [1, 2]

(1) INFN-Sezione di Torino, c/o Dip. di Fisica dell'Università
(2) Dipartimento di Fisica Generale dell'Università
Via Pietro Giuria 1, I-10125 Torino, Italy

Abstract

Con il completamento della ristrutturazione dei servizi di calcolo centrali della Sez. INFN di Torino e dei Dipartimenti di Fisica dell'Università (Rif. INFN/TC-02/23 del 16/09/2002, più successivo lavoro di aggiornamento), si è colta l'occasione per redigere un manuale dettagliato di installazione del più complesso di questi servizi, quello di Posta Elettronica. Le istruzioni qui contenute, pur facendo riferimento alla piattaforma Unix da noi utilizzata (Tru64-UNIX 5.1A for Alpha) ed alla configurazione locale, hanno comunque validità generale per qualunque altra piattaforma Unix, e sono state redatte avvalendosi della collaborazione del Gruppo di Lavoro *SEC-MAIL* del GARR.

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

0 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 il completamento della ristrutturazione dei servizi di calcolo centrali della Sez. INFN di Torino e dei Dipartimenti di Fisica dell'Università (Rif. INFN/TC-02/23 del 16/09/2002, più successivo lavoro di aggiornamento), si è colta l'occasione per redigere un manuale dettagliato di installazione del più complesso di questi servizi, quello di Posta Elettronica. Le istruzioni qui contenute, pur facendo riferimento alla piattaforma Unix da noi utilizzata (Tru64-UNIX 5.1A for Alpha) ed alla configurazione locale, hanno comunque validità generale per qualunque altra piattaforma Unix. Per questa implementazione ci siamo avvalsi della collaborazione del Gruppo di Lavoro *SEC-MAIL* del GARR.

1 PANORAMICA

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

- MTA
  - ✓ Sendmail 8.13.1
    - OpenSSL 0.9.7c
    - STARTTLS (TLSv1/SSLv3)
    - FEATURE (`greet_pause')
    - AMaViS (amavisd-new 2.1.1)
      - Perl 5.8.0
      - Sophos Anti-virus (Engine monthly updated)
      - SAVI 0.30
      - SpamAssassin 3.0.2
    - VbsFilter 1.7
- LDA
  - ✓ mail.local 8.11
  - ✓ SpamAssassin 3.0.2
    - Perl 5.8.0
    - Razor 2.36
    - Python 2.2.2
    - Pyzor 0.4.0
    - DCC 1.2.55
  - ✓ Procmail 3.22
- MUA
  - ✓ Pine 4.33
  - ✓ Netscape 7.2
  - ✓ SquirrelMail 1.4.3a
- IMAPS
  - ✓ Stunnel 4.04
  - ✓ OpenSSL 0.9.7c
  - ✓ Imapd 2002e
- Gestione di Mailing-List
  - ✓ MailMan 2.1.6
- Client per backup automatici
  - ✓ HP Data Protector Client A.05.10

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*).
- Filtro anti-virus abilitato per default via "milter" (*cfr. 3.1.1*), ma con possibilià di disabilitazione per gli utenti che lo richiedano.
- Filtro anti-spam utilizzabile facoltativamente:
  - a livello di LDA (*cfr. 4.1*): l'utente ha la facoltà di attivarlo mediante "procmail"; in questo modo le E-Mail vengono smistate in folder opportuni.
  - a livello di MTA (*cfr. 3.1.2*): attivabile via "milter" per gli utenti che lo richiedano, rigetta tutte le E-Mail identificate come "spam".
- Filtro per la rinomina dei files in attachment alle E-Mail nel caso la loro estensione (*.exe, *.bat, ..) sia di tipo potenzialmente pericoloso in termini di sicurezza (nel nostro caso con sostituzione del carattere "." con "_"). È abilitato per default via "milter", obbligatoriamente per tutti gli utenti.

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 .
E. Il file domain.m4 .
F. Il file aliases, nella sua configurazione minima .
G. Istruzioni per l'installazione di amavisd-new 2.1.1 su piattaforma Unix.
H. File di configurazione per amavisd-new.
I. Istruzioni per l'installazione di vbsfilter 1.7 su piattaforma Unix.
J. Istruzioni per l'installazione di SpamAssassin 3.0.2 su piattaforma Unix.
K. File di configurazione per SpamAssassin.
L. Istruzioni per l' (auto) attivazione 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.

Non risulta presente in tutti i MTA; ad esempio, lo è in Sendmail (e ciò è stata una forte motivazione per la sua scelta), ma non in Postfix.

3.1.1 FILTRO ANTI-VIRUS (a livello di MTA)

Nel nostro caso, come prodotto anti-virus si è utilizzato il Sw prodotto dalla Sophos, la cui installazione è semplice (vedi APPENDICE-J).

3.1.2 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 serie di test euristici con algoritmi genetici a correzione automatica *Bayesiana*, che tendono 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.

Nel caso di messaggi indirizzati a più destinatari, l'abilitazione del filtro a questo livello (MTA) diviene operativa (REJECT) solamente se richiesta da TUTTI i destinatari. Pertanto, se ne consiglia l'installazione anche a livello di LDA (*cfr. 4.1*), seguendo le istruzioni riportate nell'APPENDICE-L.

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 sostituire al LDA fornito con il s.o. quello distribuito nel pacchetto del Sendmail (mail.local).

Per quanto riguarda, invece, il filtraggio, catalogazione, smistamento, ecc… dei messaggi al momento della consegna, abbiamo utilizzato un secondo LDA, con funzionalità più ampie: Procmail.

Ovviamente, sarebbe stato possibile utilizzare quest'ultimo per entrambe le situazioni, sia di pre che post-consegna, ma per la prima abbiamo preferito utilizzarne uno che fosse sicuramente compatibile con Sendmail e rispondente agli standard.

4.1 FILTRO ANTI-SPAM (a livello di LDA)

Come già descritto (*cfr. 3.1.2*), quale prodotto anti-spam si è optato per quello di pubblico dominio della ASF (Apache Software Foundation): SpamAssassin.

L'attivazione del filtro anti-spam, nonché 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: Pine, Netscape, Mozilla) 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 Pine, oppure configurare opportunamente un MUA sul proprio calcolatore (ad esempio, Netscape Messenger) configurandolo in modo da utilizzare il protocollo IMAPS (IMAP con TLS/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/TLS 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, Netscape Navigator). 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 Netscape/Mozilla)

Per tutti gli utenti muniti di Certificato Personale X.509 rilasciato dalla "INFN Certification Authority" e che utilizzino Netscape o Mozilla come MUA, è possibile la ritrasmissione (*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/SSL 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.

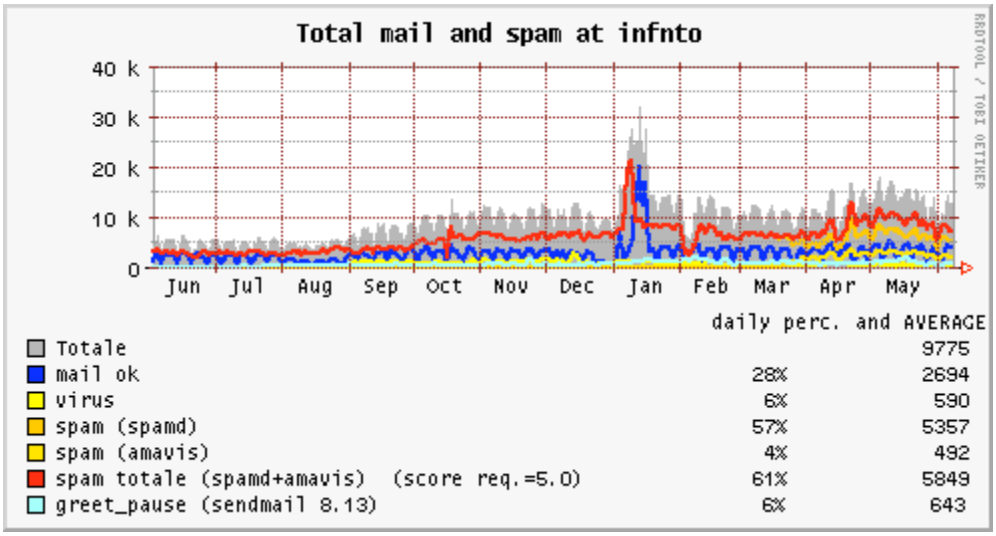
Limiti di STARTTLS:

- 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 finale del servizio implementato nella Sez. INFN di Torino, a Giugno 2005, è sicuramente positiva sia per quanto riguarda la funzionalità di MTA, che per l'efficienza dei filtri anti-virus e/o antispam.

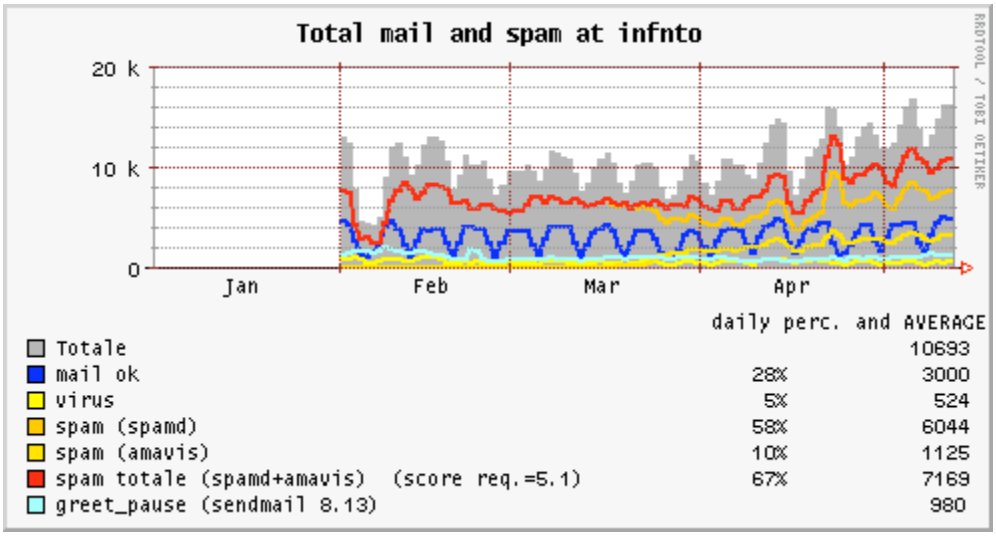
Nel grafico seguente sono riportate tutte le funzionalità illustrate in questo documento ed implementate nel corso dell'ultimo anno.



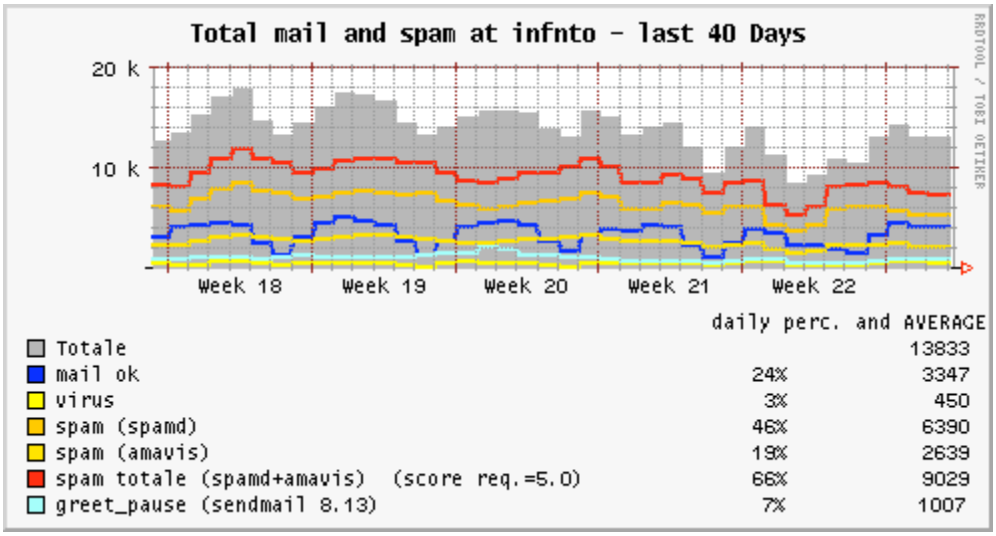
La cosa che più salta agli occhi è l'aumento della quantità di posta complessivamente gestita dal mail-server che è triplicata nel corso dell'ultimo anno, e di come le varie funzionalità gradualmente implementate abbiano contribuito ad eliminare la mole sempre maggiore di E-Mail indesiderate, mantenendo sempre "pulito" il flusso dei messaggi "buoni":

- Ottobre 2002: attachment renaming
- Gennaio 2003: anti-spam (spamd)
- Gennaio 2004: Bayesian filtering
- Febbraio 2004: Bayesian learning
- Luglio 2004: greet_pause
- Settembre 2004: anti-virus
- Marzo 2005: anti-spam con REJECT (amavis)

Per quanto riguarda l'ultima funzionalità abilitata, il prossimo grafico (riportato nella pagina seguente) ne mostra meglio la finestra di attivazione.



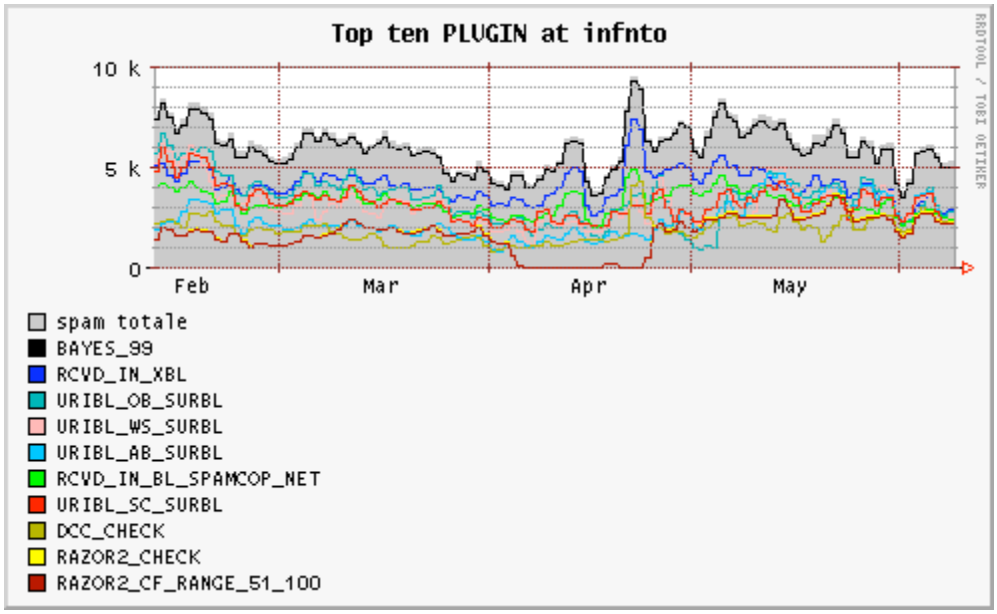
Valori numerici che rispecchino l'attuale realtà si possono ottenere graficando un periodo che contenga tutte le funzionalità implementate; come, ad esempio, nel seguente grafico degli ultimi 40 giorni.



Dai valori medi reali si evince che, tra spam *rejected* (amavis) e *greet_pause*, ben un quarto delle E-Mail vengono rifiutate, con ovvie (benefiche) ripercussioni sul carico di CPU dei calcolatori che compongono il TruCluster del mail-server.

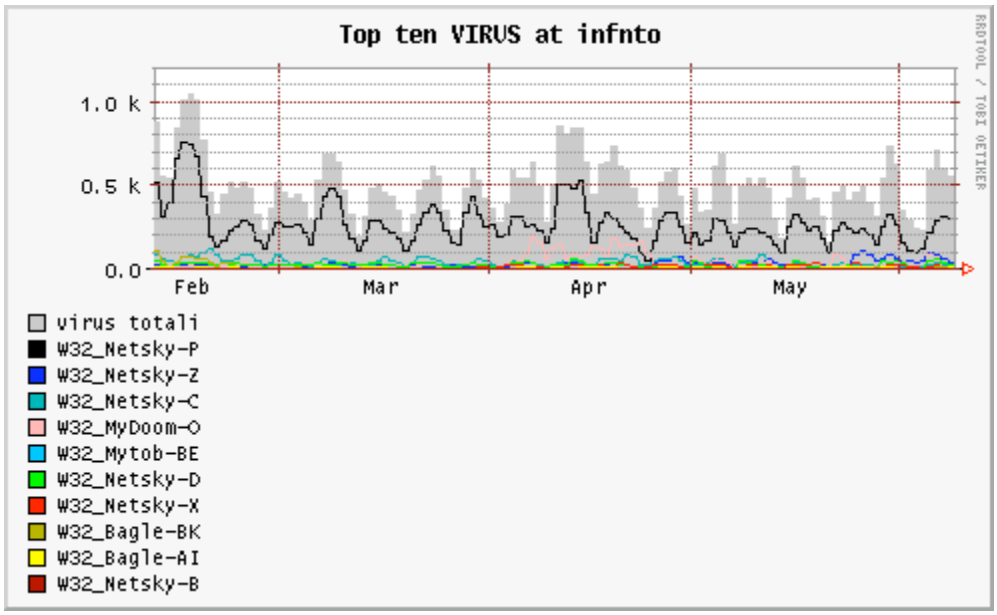
È anche da notare come, oramai, la posta "buona" sia arrivata ad essere addirittura meno di un quarto di quella complessivamente transitata sul mail-server.

Per quanto riguarda, invece, l'efficacia dei filtri Bayesiani, si consideri il grafico dei principali plugin utilizzati da SpamAssassin.



Si vede chiaramente come il classificatore statistico Bayesiano utilizzato all'interno di SpamAssassin sia fondamentale nell'individuazione dello spam.

Per completezza, si riporta anche il grafico dei principali Virus intercettati dal corrispondente filtro.



7 RINGRAZIAMENTI

- Ai membri del Gruppo di Lavoro *SEC-MAIL* (GARR), sia per le direttive implementate che per la disponibilità dimostrata in alcune fasi critiche della (ri)configurazione del Servizio; ed in particolare alla Dott.ssa Ombretta Pinazza per i grafici
- Al Prof. Silio d'Angelo, dell'Università di Roma II (Torvergata/Roma), per la disponibilità dimostrata e per i consigli ricevuti, relativamente all'ambiente TruCluster.

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: **Tru64-UNIX 5.1A for Alpha**.

Spacchettare il tar-file in una directory locale:

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

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

```
# /sbin/init.d/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 bene utilizzare **mail.local** come LDA, anche se ciò non è sempre possibile 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/binmail`** .

Esistono altri due applicativi, sempre distribuiti con il **sendmail**, che è necessario 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/obj.OSF1.V5.1.alpha/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 **`/usr/adm/sm.bin/`** . Ad esempio, per gli usuali **vacation** e **procmail**:

```
# cd /usr/adm/sm.bin/
# 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:*:25:
```

e l'utente:

```
smmsp:*:25:25: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 **AMaViS** e **vbsfilter**, le cui istruzioni di installazione si trovano rispettivamente nelle APPENDICI G ed I.

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   system     512 Aug  1  2001 /var/spool/mqueue/
-r--r--r--   1 root   system   40187 Aug 29 16:03 /etc/mail/sendmail.cf
-r--r--r--   1 root   system   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:

```
magda.to.infn.it
scilla.to.infn.it
cariddi.to.infn.it
torino.infn.it
to.infn.it
ph.unito.it
```

dove: *magda* è il cluster-alias, e *scilla* e *cariddi* i due 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 i sinonimi 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
```

e

```
ph.unito.it
torino.infn.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 rispettivamente la forma seguente:

```
gandalf         Alberto.DAmbrosio@to.infn.it
bar             Giorgio.Bar@to.infn.it
degiovan        Franca.DeGiovanni@ph.unito.it
```

e

```
ph.unito.it
to.infn.it
torino.infn.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 **`/sbin/init.d/sendmail`**

N.B.:

Affinché STARTTLS funzioni correttamente, nel caso (come il nostro) 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-0.9.7c/include')
APPENDDEF(`confLIBDIRS', `-L/usr/local+/openssl-0.9.7c/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)
#
# 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: relay.mc,v 8.14 2004/04/22 09:30:00 ca Exp $')
OSTYPE(osf1)dnl

define(`confSMTP_LOGIN_MSG', `Testo con messaggio di benvenuto')dnl
define(`confCF_VERSION', `Stringa con personalizz. della versione')dnl

define(confDOMAIN_ONLY, `to.infn.it')
define(confUSERDB_SPEC, `/etc/mail/userdb.db')
define(confMAX_MESSAGE_SIZE, `10000000')

define(`confMAIL_HUB', `magda.to.infn.it.')
define(`ALIAS_FILE', `/etc/mail/aliases')
define(`STATUS_FILE', `/etc/mail/statistics')
define(`LOCAL_MAILER_PATH', `/usr/libexec/mail.local')
define(`LOCAL_SHELL_PATH', `/usr/libexec/smrsh')

define(`confRAND_FILE', `file:/etc/mail/randfile')dnl
define(`CERT_DIR', `/usr/local+/stunnel/certs')dnl
define(`CACERT_DIR', `/usr/local+/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

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')
INPUT_MAIL_FILTER(`vbsfilter',
`S=unix:/var/run/vbsfilter-milter.sock, F=T, T=S:10s;R:10s;E:5m')
define(`confINPUT_MAIL_FILTERS', `amavis-milter, vbsfilter')
define(`confMILTER_MACROS_ENVFROM', confMILTER_MACROS_ENVFROM``,
{b}'')dnl
```

```
DOMAIN(confDOMAIN_ONLY)dnl
MASQUERADE_AS(confDOMAIN_ONLY)dnl

FEATURE(`virtusertable', `hash /etc/mail/virtusertable.db')dnl
VIRTUSER_DOMAIN_FILE(`/etc/mail/virtuser-domains')dnl

FEATURE(`genericstable', `hash /etc/mail/genericstable.db')dnl
GENERICS_DOMAIN_FILE(`/etc/mail/generics-domains')dnl

FEATURE(smrsh)dnl
FEATURE(use_cw_file)dnl
FEATURE(access_db)dnl
FEATURE(`greet_pause', `5000')dnl
FEATURE(`blacklist_recipients')dnl
FEATURE(`nouucp', `reject')dnl

FEATURE(allmasquerade)
FEATURE(limited_masquerade)

EXPOSED_USER(postmaster)

MAILER(`local')dnl
MAILER(`smtp')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',`magda.to.infn.it.')
define(confMAX_MESSAGE_SIZE, `10000000')

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

define(`LUSER_RELAY',confMAIL_HUB)dnl
define(`SMART_HOST',smtp: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 2.1.1 su piattaforma Unix

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 obj.OSF1.V5.1.alpha/libmilter/*.a  /usr/local+/lib/
# cp -p obj.OSF1.V5.1.alpha/libsm/*.a      /usr/local+/lib/
# cp -p obj.OSF1.V5.1.alpha/libsmutil/*.a  /usr/local+/lib/
```

Creare il gruppo:

```
vscan:*:26:
```

e l'utente:

```
vscan:NoLogin:26:26:AMaViS:/usr/local+/amavis:/bin/false
```

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-2.1.1.tar.gz | tar -xvf -
# chown -R root:system ./amavisd-new-2.1.1/
```

Nel file **`/usr/local++/sendmail-8.13.1/amavisd-new-2.1.1/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-2.1.1/helper-progs
# setenv CFLAGS "-pthread"

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

```
              --with-sockname=/var/run/amavis/amavisd.sock    \
              --with-user=vscan

# 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*
```

Nel nostro caso, come prodotto anti-virus si è utilizzato quello (commerciale) della **Sophos**, la cui installazione è banale:

```
# cd /usr/local++/sav-install
# ./install.sh -v -d /usr/local+ -ni -nssi -nidc
```

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 disabilitato di default per tutti gli utenti. Gli indirizzi E-Mail da abilitare vanno inseriti nelle variabili **`bypass_spam_checks_maps`** e **`spam_lovers_maps`**.
- La notifica al mittente delle E-Mail intercettate è disabilitata.

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

```
# 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/amavis-milter              \
           -p local:/var/run/amavis/amavis-milter.sock'

# /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+/lib/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 = (
 { 'latina@' => 1,
   'andrea.latina@' => 1,
 },
);

@virus_lovers_maps = (
 { 'latina@' => 1,
   'andrea.latina@' => 1,
 },
);

@bypass_spam_checks_maps = (
 { 'gandalf@' => 0,
   'dambrosio@' => 0,
   'alberto.dambrosio@' => 0,
 },
 1,
);

@spam_lovers_maps = (
 { 'gandalf@' => 0,
   'dambrosio@' => 0,
   'alberto.dambrosio@' => 0,
 },
 1,
);

$max_servers   = 3;          # 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 se-
conds)
$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 na-
me!

$MYHOME   = '/usr/local+/amavis'; # a convenient default for other set-
tings
$TEMPBASE = "$MYHOME/tmp";        # working directory, needs to be crea-
ted manually
$ENV{TMPDIR} = $TEMPBASE;         # environment variable TMPDIR
$QUARANTINEDIR = '/usr/local+/virusmails';

# $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 );

$log_level = 0;              # verbosity 0..5
# $log_recip_templ = undef;  # disable by-recipient level-0 log entries
$DO_SYSLOG = 1;              # log via syslogd (preferred)
$SYSLOG_LEVEL = 'mail.debug';

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

$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 = 4.5;  # add 'spam detected' headers at that level
$sa_kill_level_deflt = 4.5;  # triggers spam evasive actions
$sa_dsn_cutoff_level = -999; # spam level beyond which a DSN is not sent

$sa_mail_body_size_limit = 200*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 'u-
se_auto_whitelist')

# @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)
#);

$notify_virus_recips_templ = re-
ad_text("$MYHOME/notify_virus_recips.txt");

###$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 = 1;   # (defaults to false (undef))
$warnbannedrecip = 1;  # (defaults to false (undef))
$warnbadhrecip = 1;    # (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';

$X_HEADER_TAG  = 'X-Virus-Scanned';
$X_HEADER_LINE = "by amavisd-new at $mydomain [Gnorri: 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)

$sa_spam_subject_tag = '***SPAM*** ';

$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 mil-
ter!
$forward_method = undef;

$final_virus_destiny      = D_BOUNCE;
$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
));

@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}],

  ## 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
});


@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 ],

# ### 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 prefer-
red)
# ['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 discontinued.
# 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 workstation
#   # 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 vbsfilter 1.7 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. Spacchettare il tar-file all'interno della directory di installazione del **sendmail**:

```
# cd /usr/local++/sendmail-8.13.1/
# gzip -dc vbsfilter-1.7.INFN.tar.gz | tar -xvf -
# chown -R root:system ./vbsfilter-1.7.INFN/
```

e procedere con la compilazione del sorgente:

```
# cd ../vbsfilter-1.7.INFN/
# cc -std0 -O1 -I../include -o vbsfilter_INFN vbsfilter_INFN.c  \
     -L/usr/local/lib                                          \
     -L../obj.OSF1.V5.1.alpha/libmilter                        \
     -L../obj.OSF1.V5.1.alpha/libsmutil                        \
     -L../obj.OSF1.V5.1.alpha/libsm                            \
     -lmilter -lsm -lsmutil -pthread

# cp vbsfilter_INFN /usr/sbin/
# chgrp smmsp /usr/sbin/vbsfilter_INFN
```

Lanciare (prima del **sendmail**) con:

```
# /usr/sbin/vbsfilter_INFN -p unix:/var/run/vbsfilter-milter.sock
```

APPENDICE-J
Istruzioni per l'installazione di SpamAssassin 3.0.2 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:

```
# /usr/local+/perl5.8.0/bin/perl -MCPAN -e shell
cpan> o conf prerequisites_policy ask
cpan> install Mail::SpamAssassin
cpan> quit
```

Nel nostro caso, però, si è preferito procedere in maniera tradizionale. Quindi, innanzitutto spacchettare il tar-file in una directory locale:

```
# cd /usr/local++/
# gzip -dc Mail-SpamAssassin-3.0.2.tar.gz | tar -xvf -
# chown -R root:system ./Mail-SpamAssassin-3.0.2
```

Nel file **`/usr/local++/Mail-SpamAssassin-3.0.2/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-3.0.2/
# /usr/local+/perl5.8.0/bin/perl Makefile.PL PREFIX=/usr/local+
# make
# make test
# make install
```

Va attivato (preferibilmente prima del **sendmail**) con:

```
# /usr/local+/bin/spamd -m 5 -c -d 2> /dev/null &
```

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 SpamAssassin
# See 'perldoc Mail::SpamAssassin::Conf' for details of what can be
# tweaked.
#
###########################################################################
###
#

required_score              4.2

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

rewrite_header Subject      ***SPAM?***
```

```
report_safe                 0
report_header               1
use_terse_report            1

use_bayes                   1
use_bayes_rules             1
bayes_auto_learn            1
bayes_learn_to_journal      1
bayes_learn_during_report   1
bayes_path                 /usr/local+/etc/mail/spamassassin/bayes/bayes
bayes_file_mode             777
bayes_journal_max_size      204800
bayes_expiry_max_db_size    300000
lock_method                 nfssafe

whitelist_from              angelo.maggiora@to.infn.it
whitelist_from              maggiora@to.infn.it
whitelist_from              @to.infn.it @ph.unito.it *.garr.it
use_auto_whitelist          1
auto_whitelist_file_mode    777
auto_whitelist_path
          /usr/local+/etc/mail/spamassassin/auto-whitelist/auto-whitelist

defang_mime                 0

use_razor2                  1
use_dcc                     1
use_pyzor                   1

dcc_path                    /usr/local+/bin/dccproc
pyzor_path                  /usr/local+/bin/pyzor

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

APPENDICE-L
Istruzioni per l' (auto) attivazione del filtro anti-spam (SpamAssassin)

Una volta attivato il filtro, le E-Mail etichettate come "SPAM" verranno smistate verso due folder chiamati di default **Probably-Spam** e **Almost-Certainly-Spam**, in maniera tale da poter poi verificare manualmente l'assenza di "*Falsi Positivi*".

L'attivazione del filtro è facoltativa, a discrezione dell'utente, e si può effettuare secondo i passi seguenti (i primi due operano a livello di LDA, il terzo di MTA):

1. 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

:0fw: spamc.lock
* < 256000
| /usr/local+/bin/spamc

: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 (Pine, Netscape, ecc..). Inoltre, è possibile modificare il nome dei folder nei quali vengono spostate le E-Mail etichettate come "SPAM": **Probably-Spam** e **Almost-Certainly-Spam**.

   In quest'ultimo folder (che è possibile non utilizzare eliminando le corrispondenti tre righe di istruzioni nel file **`.procmailrc`**) finiscono le E-Mail con "punteggio" (vedi parametro **`required_score`**) maggiore o uguale a 15, cioè con una probabilità dello 0.005% di "*Falsi Positivi*". Di conseguenza, il suo controllo può essere effettuato con meno frequenza.

2. Creare nella propria home-directory il file:

   .forward

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

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

3. REJECT (anti-spam a livello di MTA)

   Per chi ha già attivato il filtro anti-spam secondo i due punti precedenti, esiste la possibilità di far rifiutare (REJECT) immediatamente i messaggi identificati come "SPAM", senza effettuarne la consegna nella INBOX, o lo smistamento nei folder **Probably-Spam** e **Almost-Certainly-Spam**.

   Tale funzionalità è attivabile dietro esplicita richiesta degli utenti (vedi APPENDICE-G ed APPENDICE-H), i quali devono però tenerne ben presente i pro ed i contro:

   PRO:

   - ✓ Nei due folder sopra riportati verranno smistate solo una minima parte delle E-Mail identificate come "SPAM"; la maggior parte verrà rigettata.
   - ✓ 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 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 l'attivazione 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!).
   - Nel caso di messaggi indirizzati a più destinatari, l'abilitazione del REJECT diviene operativa solamente se richiesta da TUTTI i destinatari. In altre parole, una E-Mail identificata come "SPAM" è comunque NON rigettata da parte dell'anti-spam se almeno uno dei destinatari è non-abilitato. In tal caso il sistema effettuerà la consegna del messaggio nella INBOX, o lo smistamento nei due folder **Probably-Spam** e **Almost-Certainly-Spam**.
   - Occorre comunque continuare a verificare manualmente che nei due 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-Virus-Scanned: by amavisd-new

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

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

- **Giorgio Bar**
  Perito Industriale con specializzazione Informatica, dal 2000 System Administrator c/o Servizio Calcolo della Sez. INFN di Torino, in precedenza System Administrator presso aziende private.
- **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.
- **Franca De Giovanni**
  Ragioniere Programmatore, dal 1999 Assistente di Elaborazione Dati presso il Dipartimento di Fisica Generale dell'Università di Torino (in collaborazione con il Servizio Calcolo dell'INFN di Torino, al quale è associata, gestisce il patrimonio informatico del comprensorio di Fisica); in precedenza, prima programmatore, poi tecnico informatico presso aziende private.