

# Come montare un antivirus su Postfix

Antonio "AGX" Gallo

## Sommario

- 1. Introduzione ..... ??
- 2. Componenti fondamentali ..... ??
  - 2.1. Postfix ..... ??
  - 2.2. Sophos ..... ??
  - 2.3. Amavis ..... ??
- 3. Installazione e configurazione ..... ??
- 4. Principio di funzionamento ..... ??
- 5. Licenza D'Uso ..... ??
- 6. DISCLAIMER ..... ??

# 1. Introduzione

In questa documento parlo di come configurare postfix per effettuare lo scanning di tutte le mail in entrata ed in uscita dal vostro postoffice. Ovviamente nelle mail cerchiamo virus principalmente per Windows non per Unix!

Un ringraziamento particolare ad Andrea Fanfani: c'è l'ho fatta ma è stata dura.

Il documento è mantenuto da Antonio Gallo (<http://www.antoniogallo.it>). Il sorgente SGML per poter mandare le proprie patch è disponibile su [www.badpenguin.org](http://www.badpenguin.org) (<http://www.badpenguin.org/docs/lug-howto/lug-howto.sgml>).

## 2. Componenti fondamentali

Il sistema prevede i seguenti componenti:

- postfix
- amavisd (snapshot da CVS)
- sophos

### 2.1. Postfix

Postfix lo conosciamo tutti è il miglior, a mio giudizio, server di posta attualmente in circolazione.

### 2.2. Sophos

Sophos è un'antivirus che esiste anche per Unix: si paga. Ti da a disposizione tre cose:

- un file .dat contenente tutti i pattern dei virus;
- una libreria per poter crearti e/o personalizzarti un antivirus ad hoc;
- un file 'sweep' per lo scanning di file o directory che è in pratica un esempio delle sue librerie di programmazione (SAVI).

### 2.3. Amavis

Amavis è GPL. Bisogna usare 'amavisd' da CVS non la versione amavis-perl e ne la versione amavis-smtp danno problemi... il problema è che sul loro sito non ci sono informazioni adeguate. Io ho usato un .tgz dalla loro directory contrib dove ho trovato una snapshot recente.

L'installazione di amavid ha dato molti problemi, ho dovuto ricorrere varie volte a 'strace' per vedere dov'era il problema. In particolare i permessi su file e directory. Bisogna creare un utente per questo programma, io ho creato anche un gruppo. Bisogna quindi lanciare amavisd non da 'root' ma usando questo utente ad hoc.

### 3. Installazione e configurazione

Postfix lo conosciamo tutti e va configurato nel seguente modo.

in `master.cf` aggiungere:

```
vscan unix - n n - 10 pipe user=amavis argv=/usr/sbin/amavis $sender $recipient
localhost:10025 inet n - n - - smtpd -o content_filter=
```

in `main.cf` aggiungere:

```
content_filter = vscan:
```

inoltre la variabile `mailbox_command` deve essere commentata.

### 4. Principio di funzionamento

Postfix riceve le mail che vengono passate ad amavis attraverso il transport 'vscan'. In pratica il programma 'pipe' di postfix provvede a lanciare il client di amavis con l'utente amavis.

Il client amavis si connette attraverso la socket su file ad amavisd, decomprime gli attachment e vengono controllati tramite 'sweep'. In caso di virus trovati si comporta secondo il file di configurazione `/etc/amavisd.conf` (manda mail, rimuove allegati, etc).

Le mail pulite vengono rimandate al Postfix.

### 5. Licenza D'Uso

Il seguente documento può essere riprodotto in parte o totalmente appatto che compaia il mio nome (Antonio Gallo) e un link al mio sito ([www.badpenguin.org](http://www.badpenguin.org)). Grazie anticipate.

### 6. DISCLAIMER

Md correggimi se sbaglio!!!

Spero sia utile, Antonio