Antivirus en linux: F-prot+Amavis+Postfix

Por Paco Aldarias Raya

Impreso: 20 de septiembre de 2004

Email: pacolinux arroba inicia punto es
Web: `http://pagina.de/pacodebian`
Con Linux Debian. En Valencia (España)

Realizado con: LaTeX

Índice

1. Versiones **1**

2. Introducción **1**

3. El antivirus **2**

4. Uso de f-prot **2**

5. Instalación de amavis para debian sid **2**
5.1. Instalar amavis 2
5.2. Configurar para antivirus al correo 3
5.3. Cambiar el ficheros de configuracion de amavis 3

6. Estadisticas de amavis **3**

7. Instalación de amavis para debian woody **3**
7.1. Instalar amavis 4
7.2. Configurar para antivirus al correo 4
7.3. Cambiar el ficheros de configuracion de amavis: 4

8. Probando que funciona **4**

9. Antivirus clam **5**

10.Script para pasar antivirus al disco duro de windows **5**

11.Bibliografía **6**

1. Versiones

- 17.04.03 Primera version v.1.0
- 30.12.03 Amavis para debian woody v.1.1

2. Introducción

Vamos a ver la forma de como montar un antivirus para escanera ficheros. Y además veremos con comprobar si tiene virus el correo entrante y saliente.

Yo uso la combinación postfix + amavis + fprot, donde:

1. postfix es el servidor de correo (sé que pueden ser otros)
2. amavis es el programa que se encarga de pasar el antivirus y de tomar las acciones necesarias
3. fprot es el antivirus en sí, es gratuito para usuarios personales (y siempre que sea en Linux).

3. El antivirus

Previamente neceta instalar:
apt-get install wget

Bajarse el fichero:

```
fp-linux-sb.deb
```

Se encuentra en:
`http://www.f-prot.com/download/`
`ftp://ftp.f-prot.com/pub/linux/fp-linux-sb.deb`

Instalarlo ese paquete:

```
dpkg -i fp-linux-sb.deb
```

4. Uso de f-prot

Pasar el antivirus a una carpeta:

```
f-prot -append  -disinf -report=fprot.log /carpeta/
```

Para actualizar el antivirus:

```
/usr/local/f-prot/check-updates.sh
```

Pasar actualizar el antivirus, lo añadiremos en el cron:
#crontab -e

```
1 11 * * *      /usr/local/f-prot/check-updates.sh -cron
```

5. Instalación de amavis para debian sid

5.1. Instalar amavis

Para debian sid

```
apt-get install amavisd-new
```

5.2. Configurar para antivirus al correo

Requiere: rddtools, php4, apache, perl

```
apt-get install amavisd-new
```

nano /etc/postfix/main.cf

```
# Configuración Amavis - F-Prot
content_filter = smtp-amavis:[127.0.0.1]:10024
```

5.3. Cambiar el ficheros de configuracion de amavis

nano /etc/amavis/amavisd.conf
Descomentar la linea q aparece:

```
FRISK F-Prot Daemon
```

6. Estadisticas de amavis

Instalarlo con:

```
apt-get instal amavis-statsl
```

Versión:

```
amavis-stats                    0.1.12-2                        Virus statistics RRD
```

Hacer enlace simbolico:

```
ln -s  /usr/share/amavis-stats/ /var/www/amavis
```

Generar Estadisticas:

```
amavis-stats /var/log/mail.info
```

Probar que funciona:
`http://127.0.0.1/amavis/`

7. Instalación de amavis para debian woody

Aqui está el ayuda: `/usr/share/doc/amavis-postfix/`

7.1. Instalar amavis

Para debian woody:

```
apt-get install amavis-postfix
```

7.2. Configurar para antivirus al correo

Añadir al ficheros de configuracion de postfix:
Añadir las líneas: nano /etc/postfix/main.cf

```
content_filter = vscan:
soft_bounce = yes
```

Añadir la líneas: nano /etc/postfix/master.cf

```
vscan  unix  -  n  n  -  10  pipe flags=q \
user=amavis argv=/usr/sbin/amavis ${sender} ${recipient}

localhost:10025  inet  n  -  n  -  -   smtpd -o content_filter=
```

Reiniciar postfix:
/etc/init.d/postfix restart

7.3. Cambiar el ficheros de configuracion de amavis:

Modificar el fichero: nano /etc/amavis/amavisd.conf

```
# FRISK F-Prot
$fprot = "f-prot";
```

Reiniciar amavis:
/etc/init.d/amavis-postfix restart

8. Probando que funciona

```
Nos enviamos un correo:
echo "Mi texto" | mail -s "Mi Encabezado" paco


Este es el correo:
----------------------------
From paco@aldarias.dyndns.org  Tue Dec 30 15:27:11 2003
Return-Path: <paco@aldarias.dyndns.org>
Delivered-To: paco@aldarias.dyndns.org
Received: from localhost (localhost [127.0.0.1])
        by aldarias.dyndns.org (Postfix) with ESMTP id 4DB532C300
        for <paco@aldarias.dyndns.org>; Tue, 30 Dec 2003 15:27:11 +0100 (CET)
Received: by aldarias.dyndns.org (Postfix, from userid 1000)
        id ABF302C301; Tue, 30 Dec 2003 15:27:10 +0100 (CET)
To: paco@aldarias.dyndns.org
Subject: Mi Encabezado
Message-Id: <20031230142710.ABF302C301@aldarias.dyndns.org>
Date: Tue, 30 Dec 2003 15:27:10 +0100 (CET)
From: paco@aldarias.dyndns.org (Paco Aldarias)
X-Virus-Scanned: by AMaViS snapshot-20020222
X-Spam-Status: No, hits=0.0 required=6.0 tests= version=2.20
X-Spam-Level:

 Mi texto
----------------------------
X-Virus-Scanned: by AMaViS snapshot-20020222 <- Funciona.
```

9. Antivirus clam

Clam es un antivirus q se actualiza por internet y se puede poner tb en amavis.

Instalación:

```
apt-get install clam
```

Actualización de los virus

```
freshclam
```

Pasar el antivirus a la carpeta /winc

```
clamscan -i -r /winc -r clam.log
```

10. Script para pasar antivirus al disco duro de windows

```
echo pasando antivirus
/usr/sbin/update-f-prot
freshclam
f-prot -append -auto -disinf -report=fprot.log /winc
f-prot -append -auto -disinf -report=fprot.log /wind
clamscan -i -r /winc -r clam.log
clamscan -i -r /wind -r clam.log
```

11. Bibliografía

1. Ubicación de este documento:
   `http://pagina.de/pacolinux`
2. Página de linux :
   `http://inicia.es/de/pacolinux`