Clamav - антивирусная защита сервера

Опубликовано muff в Втр, 2010-08-24 16:37

Всем уже давно известно, что пользователю без антивирусной защиты сегодня не обойтись. И если раньше компьютерные вирусы писались в одиночку, то на данный момент это уже серьезный бизнес, и написанием вредоносного ПО занимаются профессионалы. Но, если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет. Поэтому при настройке серверов не будем забывать о антивирусном пакете с подальшей интеграцией его в Exim, Sendmail, Squid, Samba и тд...

Итак, пришла пора познакомиться с ClamAV. Главной целью Clam AntiVirus является интеграция с серверами электронной почты для проверки файлов, прикреплённых к сообщениям. В пакет входит масштабируемый многопоточный демон **clamd**, управляемый из командной строки сканер **clamscan**, а также модуль обновления сигнатур по Интернету - **freshclam**. Возможности Clam AntiVirus:

- управление из командной строки;
- возможность использования с большинством почтовых серверов, включая реализацию milter-интерфейса для Sendmail;
- сканер в виде библиотеки Си;
- сканирование файлов и почты «на лету»;
- определение свыше 700 000 вирусов, червей, троянов, сообщений фишинга;
- анализ сжатых файлов RAR (2.0, 3.0), Zip, Gzip, Bzip2, MS OLE2, MS Cabinet, MS CHM (сжатый HTML) и MS SZDD;
- поддержка сканирования mbox, Maildir и «сырых» почтовых файлов;
- анализ файлов формата Portable Executable, упакованных UPX, FSG или Petite.

Приступаем к установке пакета из системы портов:

```
# cd /usr/ports/security/clamav/ && make install clean && rehash
```

Дистрибутив "весит" немало - 38 мегабайт, так что если канал в интернет не очеть быстрый, придется немного подождать.

После инсталяции добавляем в **rc.conf** опции загрузки:

```
# echo '# ClamAV Antivirus' >> /etc/rc.conf

# echo 'clamav_clamd_enable="YES"' >> /etc/rc.conf

# echo 'clamav_freshclam_enable="YES"' >> /etc/rc.conf
```

Запускаем clamav:

```
# sh /usr/local/etc/rc.d/clamav-clamd start
Starting clamav_clamd.LibClamAV Warning: ******************************************
*******LibClamAV Warning: ***  The virus database is older than 7 days!  ***LibClamA
```

```
V Warning: ***   Please update it as soon as possible.    ***LibClamAV Warning: ****
*********************************************
```

После запуска наблюдаем сообщение системы, что антивирусные базы устарели, и их необходимо обновить... Не вопрос. Запускаем модуль обновления **freshclam**.

```
# sh /usr/local/etc/rc.d/clamav-freshclam start
```

Теперь еще немного подождать, и антивирусные базы будуть в актуальном состоянии.

Дальнейшее использование ClamAV будет зависеть только от вашей фантазии. Интеграцию с ClamAv поддерживает довольно много разнообразного софта.

Источник (получено *2025-08-07 09:30*):
http://muff.kiev.ua/content/clamav-antivirusnaya-zashchita-servera