Полезности Clamav + Amavisd

Проверка на спамлисты и корректность настройки сервера:

https://spamtest.smtp.bz https://www.mail-tester.com

Настройки хранятся тут

Фильтрация

```
/etc/amavis/conf.d/15-content_filter_mode
```

Дополнительные настройки

```
/etc/amavis/conf.d/50-user
```

Обучение антиспама и антивируса

```
sa-learn --spam /mail/fellk.ru/*/{.\&BCEEPwQwBDw-,.Spam,.Junk\ E-mail,.Junk}/cur
```

```
~# sa-learn --ham /mail/fellk.ru/spam\@fellk.ru/.Ham/cur
```

Статистика по обучению

```
sa-learn --dump magic
```

Обновление антивирусных баз ClamAV

Останавливаем службу

```
systemctl stop clamav-daemon.service
```

Удаляем логи (иногда он блокируется, поэтому удаляем) <xode> rm /var/log/clamav/freshclam.log </code> Запускаем службу

```
systemctl start clamav-daemon.service
```

Проверяем статус службы

```
systemctl status clamav-daemon.service
```

Пример

Обновляем базы

```
freshclam
```

Не запускается clamav-daemon

Если видите такую ошибку как на скрине

То для решения нужно скачать пару файлов **daily.cvd** и **main.cvd** и поместить их в папку **/var/lib/clamav** Теперь перезапустить сервис

```
systemctl restart clamav-daemon
```

Файлы можно найти вот здесь БД доступны по ссылке. Пароль: 1d7Yir/E*@\$D

Не корректно работает amavis

Если видите подобную ошибку Для исправления нужно создать файл

```
nano /etc/amavis/conf.d/99-warden
```

с содержимым

```
$inet_socket_bind = '127.0.0.1';
```

Затем перезапустить сервис

```
systemctl restart amavis
```

Не хватает кодеров для работы

Если вы видите такую ошибку

То нужно выполнить следующее

```
sudo apt install arj bzip2 cabextract cpio rpm2cpio file gzip lhasa nomarch
pax rar unrar p7zip-full unzip zip lrzip lzip liblz4-tool lzop unrar-free
```

Редактирование блокировок расширений файлов во вложениях

Открываем файл

```
/etc/amavis/conf.d/20-debian_defaults
```

Находим там строку

```
qr'\.[^./]*\.(apk|exe|vbs|pif|scr|bat|cmd|com|cpl|dll)\.?$'i
```

и теперь в этот список добавляем еще расширения, которые хотите заблокировать

Так же делаем и в этой строке

```
qr'.\.(apk|exe|vbs|pif|scr|bat|cmd|com|cpl)$'i, # banned extension - basic
```

Сохраняемся и перезапускаем сервис

```
systemctl restart amavis
```

Проверяем отправив какой либо файл с запрещенным расширением и в логах увидим подобное сообщение

```
amavis[1465344]: (1465344-05) Blocked BANNED
(application/vnd.android.package-
archive,.zip,apkpure_3203537_494_1109.apk,=?UTF-8?B?YXBrcHVyZV8zMjAzNTM3XzQ5
NF8xMTA5LmFwaw==?=) {DiscardedOpenRelay,Quarantined}
```