

AMaViSd-new

Интерфейс между MTA и сканером вирусов/фильтром содержания

AMaViSd-new — сценарий, осуществляющий взаимодействие агента пересылки почты (MTA) со сканерами вирусов и [SpamAssassin](#).

Он поддерживает все распространённые сканеры вирусов (более 20), в том числе на уровне прямого взаимодействия со службами антивирусов [ClamAV](#), OpenAntiVirus, Trophie, AVG, f-prot и Sophos.

AMaViSd-new поддерживает все MTA по средствам фильтрования SMTP/LMTP. Использование режима фильтрования SMTP/LMTP быстрее и безопаснее, чем использование передачи через канал в клиенте AMaViS.

<https://www.ijs.si/software/amavisd/>

Установка

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

Настройка

| | |
|-----------------|----------------------------|
| Файлы настройки | /etc/amavis/conf.d |
| Документация | /usr/share/doc/amavisd-new |
| Карантин | /var/lib/amavis/virusmails |

Управление:

```
service amavis
```

[Настройка Postfix](#)

05-node_id

Нужно указать правильное имя сервера в формате FQDN (вместе с доменом) в переменной `$myhostname`

15-content_filter_mode

Антивирусы

Для работы с антивирусами нужно убрать комментарии в файле `/etc/amavis/conf.d/15-content_filter_mode` с строк:

```
@bypass_virus_checks_maps = (  
  \bypass_virus_checks, \bypass_virus_checks_acl, \bypass_virus_checks_re);
```

ClamAV

Для работы с [ClamAV](#) нужно:

1. Добавить пользователя clamav в группу amavis:

```
groupadd -a clamav amavis
```

2. Убрать комментарии в файле `/etc/amavis/conf.d/15-av_scanners` с строк относящихся к ClamAV

3. Добавить в файл:

[/etc/clamav/clamd.conf](#)

```
AllowSupplementaryGroups true
```

Антиспам

Для работы с антиспамом, например с [SpamAssassin](#) нужно убрать комментарии в файле `/etc/amavis/conf.d/15-content_filter_mode` с строк:

```
@bypass_spam_checks_maps = (  
  \%bypass_spam_checks, \@bypass_spam_checks_acl, \%bypass_spam_checks_re);
```

20-debian_defaults

Для переменных:

- `$final_virus_destiny`
- `$final_banned_destiny`
- `$final_spam_destiny`
- `$final_bad_header_destiny`

Предусмотрены следующие значения:

| | |
|------------------|---|
| D_DISCARD | блокировать, никаких уведомлений не отсылать |
| D_BOUNCE | блокировать, отправить уведомление отправителю письма |
| D_REJECT | почта не проходит к получателям, отправитель должен получить reject |
| D_PASS | пропустить письмо |

Настройка папки карантина:

| | |
|---|--|
| <code>\$quarantine_subdir_levels</code> | Создание структуры из 62 папок (0-9, A-Z, a-z) 0= Нет 1 = Да |
|---|--|

[20-debian_defaults](#)

```
$quarantine_subdir_levels = 0
```

Доставка SPAM с изменённой темой письма



Для того, чтобы доставлять SPAM с изменённой темой письма нужно:

[/etc/amavis/conf.d/20-debian_defaults](#)

```
$sa_spam_subject_tag = '***SPAM***';  
$final_spam_destiny = D_PASS;
```

[/etc/amavis/conf.d/50-user](#)

```
@local_domains_acl = ( "domain.ru", "domain2.ru" );
```

Доставка вирусов с изменённой темой письма

Для того, чтобы доставлять заражённые письма с изменённой темой письма нужно:

[/etc/amavis/conf.d/20-debian_defaults](#)

```
$final_virus_destiny = D_PASS; ***INFECTED***
```

Белый список

[/etc/amavis/conf.d/20-debian_defaults](#)

```
read_hash(\%whitelist_sender, '/etc/amavis/whitelist');  
@whitelist_sender_maps = (\%whitelist_sender);
```

SpamAssassin

Настройки для работы с [SpamAssassin](#).

Исправление прав на папку с правилами:

[amavis_spamassassin_rights.sh](#)

```
#!/bin/bash  
  
path=/var/lib/amavis/.spamassassin  
chmod -R 644 $path  
chgrp -R amavis $path  
chown -R amavis $path  
chmod 700 $path
```

Извлечение из карантина

Отправка письма из карантина получателю.

[amavis_reslease.sh](#)

```
#!/bin/sh  
  
VIRUSMAILS_DIR="/var/lib/amavis/virusmails"  
  
if [ -d $VIRUSMAILS_DIR ]; then  
  cd $VIRUSMAILS_DIR  
  amavisd-release $1
```

```
fi
```

Пример использования:

```
amavis_reslease.sh spam-xNYUd-gWtWDk.gz
```

Очистка карантина

Для периодической очистки карантина можно создать задание для периодического выполнения с помощью [Cron](#) следующего скрипта:

[amavis_clean_virusmails.sh](#)

```
#!/bin/bash

VIRUSMAILS_DIR="/var/lib/amavis/virusmails"

if [ -d $VIRUSMAILS_DIR ]; then
  cd $VIRUSMAILS_DIR
  find $VIRUSMAILS_DIR -type d -mtime +30 -exec rm -r {} \;
  find $VIRUSMAILS_DIR -type f -mtime +30 -exec rm -r {} \;
fi
```

Отладка

```
/etc/init.d/amavis debug
```

Ссылки

<https://help.ubuntu.com/community/PostfixAmavisNew>

[Руководство по Ubuntu Server » Почтовые сервисы: Фильтрация почты](#)

[iRedMail → iRedMail Support → \[SOLVED\] How to bypass amavisd for some senders?](#)

[How to fix amvavis reporting "permission denied" for clamav](#)

<http://sysadminmosaic.ru/amavisd-new/amavisd-new>

2020-09-18 09:11

