

Re: [SLE] RE: [suse-sles-e] Configuring Spamassassin and amavisd-new

Source: <http://linux.derkeiler.com/Mailing-Lists/SuSE/2005-04/0195.html>

From: Carlos E. R. (*robin1.listas_at_fiscal.es*)

Date: 04/02/05

Date: Sat, 2 Apr 2005 02:20:59 +0200 (CEST)

To: SLE <suse-linux-e@suse.com>

The Friday 2005-04-01 at 21:33 +0200, I wrote:

> *I don't see this clear, and I know no documentation. :-/*

I said that amavis-new has no documentation. I'll qualify that statement: there is no manual under "/usr/share/doc/packages/amavisd-new", and "man amavis-new" produces nothing, not found (nor info nor perldoc). Some say that the documentation is included as comments in "/etc/amavis.conf", but while that is true, it is a "documentation" that only programmers can really understand. There is no user documentation, or, at least, it was not included with SuSE 9.1.

So... reading that file, I have some more info on the problem at hand, after an hour or more studying it – but before, check this two vars:

```
# @bypass_virus_checks_acl = qw( . ); # uncomment to DISABLE anti-virus code
# @bypass_spam_checks_acl = qw( . ); # uncomment to DISABLE anti-spam code
```

I would write that as "comment to enable whatever" – that explanation above is in "programmers parlance". You need both commented, then, as I suppose you need to check both spam and viruses.

This setting, around 1/3 of the file, defines what action it takes for spam:

```
$final_spam_destiny = D_PASS;
```

The possible actions are:

```
# Alternatives to consider for spam:
# – use D_PASS if clients will do filtering based on inserted mail headers;
# – use D_DISCARD, if kill_level is set safely high;
# – use D_BOUNCE instead of D_REJECT if not using milter;
...
# The separation of *_destiny values into D_BOUNCE, D_REJECT, D_DISCARD
```

and D_PASS made settings \$warnvirusender and \$warnspamsender only still
useful with D_PASS.

Notify spam sender?
\$warnspamsender = 0; # (defaults to false (undef))

The possible actions we can use are:

The following symbolic constants can be used in *destiny settings:

D_PASS mail will pass to recipients, regardless of bad contents;

D_DISCARD mail will not be delivered to its recipients, sender will NOT be
notified. Effectively we lose mail (but will be quarantined
unless disabled). Losing mail is not decent for a mailer,
but might be desired.

D_BOUNCE mail will not be delivered to its recipients, a non-delivery
notification (bounce) will be sent to the sender by amavisd-new;
Exception: bounce (DSN) will not be sent if a virus name matches
\$viruses_that_fake_sender_re, or to messages from mailing lists
(Precedence: bulk|list|junk);

D_REJECT mail will not be delivered to its recipients, sender should
preferably get a reject, e.g. SMTP permanent reject response
(e.g. with milter), or non-delivery notification from MTA
(e.g. Postfix). If this is not possible (e.g. different recipients
have different tolerances to bad mail contents and not using LMTP)
amavisd-new sends a bounce by itself (same as D_BOUNCE).
#

So D_PASS should be the correct action for spam, so that the user can
decide. Those actions are taken when?

tag_level <= tag2_level <= kill_level < \$sa_dsn_cutoff_level

tag_level = 3.0

 Adds the X-Spam-Status and X-Spam-Level headers

tag2_level = 5.0

 Adds 'X-Spam-Flag: YES', and allows editing Subject.

kill_level = 5.0

 Does whatever action was defined, and we should have D_PASS

sa_dsn_cutoff_level = 10.0

 Discard email – undef to disable (default, but not for SuSE).

Ie, although we defined that action as "D_PASS", above this level it does a "D_DISCARD". This means that it would be quarantined unless disabled, probably in "/var/spool/amavis/virusmails", in almost maildir format.

But it is disabled:

```
$spam_quarantine_to = undef;
```

Lets see what I can learn about this.

```
$QUARANTINEDIR = '/var/spool/amavis/virusmails'; # a directory
```

```
#$virus_quarantine_method = "local:virus-%i-%n"; # default
```

```
#$spam_quarantine_method = "local:spam-%b-%i-%n"; # default
```

I think this means that virus mails are filed with names like "virus-date-hour-numbers". For example: "virus-20040628-013731-13574-10". Spam mails would be similar... perhaps.

The "/etc/amavis.conf" continues saying this:

```
# When using the 'local:' quarantine method (default), the following applies:
```

```
#
```

```
# A finer control of quarantining is available through variable
```

```
# $virus_quarantine_to/$spam_quarantine_to. It may be a simple scalar string,
```

```
# or a ref to a hash lookup table, or a regexp lookup table object,
```

```
# which makes possible to set up per-recipient quarantine addresses.
```

There are four variants – and notice that, as I don't know perl, I don't really understand the jargon:

```
# VARIANT 1:
```

```
# empty or undef disables quarantine;
```

And we have:

```
$virus_quarantine_to = 'virus-quarantine'; # traditional local quarantine
```

```
$spam_quarantine_to = undef;
```

Ie, spam above level 10 is not quarantined. What if we want to? Well... the file continues:

```
#$spam_quarantine_to = "spam-quarantine\@$mydomain";
```

```
#$spam_quarantine_to = new_RE( # per-recipient multiple quarantines
```

```
# [qr'^(.*)@example\.com$i => 'spam-${1}@example.com'],
```

```
# [qr/.*i => 'spam-quarantine' ] );
```

My mind simply refuses to understand that. Somebody, please? I think we could simply write 'spam-quarantine' (single quotes). That would be "VARIANT 2":

SuSE: Re: [SLE] RE: [suse-sles-e] Configuring Spamassassin and amavisd-new

```
# VARIANT 2:
# a string NOT containing an '@';
# amavisd will behave as a local delivery agent (LDA) and will quarantine
# viruses to local files according to hash %local_delivery_aliases (pseudo
# aliases map) – see subroutine mail_to_local_mailbox() for details.
```

See? we have to be programmers to read documentation: "see subroutine..."
:-/

```
# Some of the predefined aliases are 'virus-quarantine' and 'spam-quarantine'.
# Setting $virus_quarantine_to ($spam_quarantine_to) to this string will:
#
# * if $QUARANTINEDIR is a directory, each quarantined virus will go
# to a separate file in the $QUARANTINEDIR directory (traditional
# amavis style, similar to maildir mailbox format);
#
```

What I deduce is that if we set

```
$spam_quarantine_to = 'spam-quarantine'
```

it will go to \$QUARANTINEDIR in almost maildir format. But I don't know what other "predefined aliases" are there, even though I tried looking at the source. Possibly: virus-quarantine, spam-quarantine, user-quarantine, ham-quarantine, outgoing-quarantine, and incoming-quarantine.

This one looks promising also:

```
$spam_quarantine_to = new_RE( # per-recv multiple quarantines
  [qr'^(*)@example\.com$i => 'spam-${1}@example.com'],
  [qr/.*/ => 'spam-quarantine' ] );
```

but it is not documented, as always...

Or, if we simply want spam above 10 to go the final recipients, so they can apply their own filters (that's what I would do), we can do

```
#$sa_dsn_cutoff_level = 10;
```

or perhaps:

```
$sa_dsn_cutoff_level = undef;
```

And I'm tired of this (study). Hope you can make use of this :-)

--

Cheers,

Carlos Robinson

--

Check the headers for your unsubscription address

For additional commands send e-mail to suse-linux-e-help@suse.com

Also check the archives at <http://lists.suse.com>

SuSE: Re: [SLE] RE: [suse-sles-e] Configuring Spamassassin and amavisd-new

Please read the FAQs: suse-linux-e-faq@suse.com