

## Integrando o Amavisd-new, SpamAssassin e ClamAV com o Postfix no SUSE 9.3

### Termos de Uso

#### Nota de Copyright

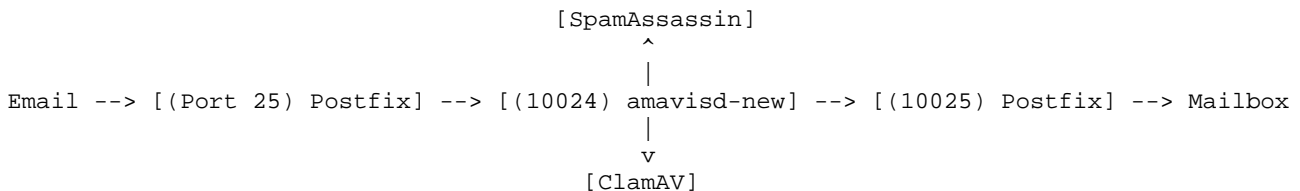
```
Copyright (c) 2007 Linux2Business.  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the GNU Free Documentation License, Version 1.2 or  
any later version published by the Free Software Foundation; with no  
Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A  
copy of the license is included in the section entitled "GNU Free  
Documentation License".
```

O conteúdo textual deste documento está disponível sob a licença GNU FDL. Para maiores informações acesse <http://www.gnu.org/copyleft/fdl.html>. Os logotipos, marcas registradas e símbolos usados neste livro são de propriedade de seus respectivos proprietários.

### Introdução

Neste artigo veremos como instalar, configurar e integrar o Amavisd-new, com o SpamAssassin e ClamAV, ao Postfix no SUSE 9.3, porém estes mesmos procedimentos podem ser utilizados em outras distribuições.

Em uma breve explicação da integração, temos que as mensagens recebidas pelo Postfix na porta 25/tcp serão enviadas ao Amavisd-new pela porta 10024/tcp, que irá invocar o ClamAV e o SpamAssassin para analisar a mensagem e caso a mesma esteja livre de Vírus e não seja SPAM, será devolvida ao Postfix, através da porta 10025/tcp, e assim entregue na caixa postal do destinatário. Abaixo temos um esquema de toda comunicação:



### Instalação

Para instalação dos pacotes, utilizaremos o YaST, através do comando apresentado abaixo:

```
# yast sw_single
```

Os pacotes que devem ser instalados são: `amavisd-new`, `spamassassin` e `clamav`.

**Obs.:** Para instalação dos pacotes será preciso os CDs ou DVD de instalação do SUSE Linux 9.3. Se foram configuradas outras fontes de instalação que utilizem a internet, é necessário que o acesso a internet esteja disponível.

## Configuração

O arquivo de configuração do Amavisd-new é `/etc/amavisd.conf`, onde é sempre importante manter uma cópia do arquivo original de instalação para eventuais problemas.

```
# cd /etc
# cp -p amavisd.conf amavisd.conf.default
```

A partir do arquivo original, vamos inserir alguns parâmetros e alterar outros. Abaixo estão apresentadas somente as diferenças entre o arquivo padrão e o novo arquivo:

```
$mydomain = 'linux2business.net.br';
$sa_tag_level_deflt = undef; # add spam info headers if at, or above that
level
$sa_tag2_level_deflt = 5.0;
$sa_kill_level_deflt = 10.0; # triggers spam evasive actions
$sa_dsn_cutoff_level = 5.0; # spam level beyond which a DSN is not sent
$sa_spam_subject_tag = undef;
$final_virus_destiny = D_DISCARD;
$final_banned_destiny = D_DISCARD;
$final_spam_destiny = D_DISCARD;
$final_bad_header_destiny = D_PASS;
### http://www.clamav.net/
['ClamAV-clamd',
 \&ask_daemon, ["CONTSCAN {}\n", "/var/lib/clamav/clamd-socket"],
 qr/\bOK$/, qr/\bFOUND$/,
 qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
# NOTE: the easiest is to run clamd under the same user as amavisd; match
the
# socket name (LocalSocket) in clamav.conf to the socket name in this entry
# When running chrooted one may prefer: ["CONTSCAN {}\n", "$MYHOME/clamd"]
```

**Obs.:** Na configuração dos anti-vírus, somente deixar descomentadas as opções para o ClamAV, comentando todas as outras se necessário.

Com a configuração proposta para o Amavisd-new, todas as mensagens que forem identificadas como um Vírus ou que contenham Vírus, serão armazenadas no diretório `/var/spool/amavis/virusmails` e uma mensagem de alerta será enviada para o usuário `virusalert`, onde estes parâmetros podem ser alterados no arquivo `/etc/amavisd.conf` através das variáveis `$QUARANTINEDIR` e `$virus_admin`.

O usuário `virusalert` é um alias para o usuário `root`, que DEVE ser também um alias para outro usuário, como por exemplo: `sysadmin`. Este procedimento é uma questão de segurança, pois nada deve ser feito utilizando o usuário `root`.

O controle das mensagens identificadas como SPAM também pode ser configurado da mesma maneira que é realizado para mensagens com Vírus, bastando adicionar ou alterar os parâmetros `$spam_admin` e `$spam_quarantine_to`.

Uma vez realizada a configuração do Amavisd-new, devemos configurar o ClamAV, através do arquivo `/etc/clamd.conf`. Abaixo temos as alterações realizadas a partir da configuração padrão:

```
LogFileMaxSize 2M
LocalSocket /var/lib/clamav/clamd-socket
#TCPSocket 3310
#TCPAddr 127.0.0.1
```

Em seguida, devemos configurar o serviço FreshClam, responsável pela atualização da base de vírus do ClamAV. O arquivo de configuração é `/etc/freshclam.conf`, onde a partir do arquivo padrão, devemos realizar as seguintes alterações:

```
UpdateLogFile /var/log/freshclam.log
DatabaseMirror db.BR.clamav.net
DatabaseMirror database.clamav.net
```

Com a configuração terminada, devemos primeiro carregar a base de dados do ClamAV, através do comando:

```
# freshclam --verbose
```

**Obs.:** O comando acima deve finalizar corretamente sua operação.

Devemos também criar o arquivo `/var/log/freshclam.log` configurando as permissões corretas para seu funcionamento:

```
# touch /var/log/freshclam.log
# chown vsan.vscan /var/log/freshclam.log
```

Por último, devemos iniciar os serviços `freshclam`, `clamd` e `amavis`:

```
# rcfreshclam start
# rcclamd start
# rcamavis start
```

As atividades dos serviços acima, podem ser monitoradas através do arquivo `/var/log/mail` e para o serviço Amavisd-new devemos verificar se a porta 10024/tcp foi iniciada.

```
# netstat -ntl | grep ":10024"
tcp        0      0 127.0.0.1:10024          0.0.0.0:*               LISTEN
```

Finalizando a integração, devemos alterar os arquivos `/etc/postfix/main.cf` e `/etc/postfix/master.cf` adicionando os seguintes parâmetros em cada um deles.

No arquivo `/etc/postfix/master.cf`:

```
smtp-amavis unix - - n - 2 smtp
-o smtp_data_done_timeout=1200
-o smtp_send_xforward_command=yes
-o disable_dns_lookups=yes
```

```
localhost:10025 inet n - n - - smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000
-o smtpd_client_connection_count_limit=0
-o smtpd_client_connection_rate_limit=0
-o receive_override_options=no_header_body_checks
```

No arquivo `/etc/postfix/main.cf`:

```
content_filter=smtp-amavis:[localhost]:10024
```

**Obs.:** Este procedimento de integração entre o Amavisd-new e o Postfix está descrito no arquivo `/usr/share/doc/packages/amavisd-new/README_FILES/README.protocol`.

Com as alterações realizadas é necessário reiniciar o Postfix.

```
# rcpostfix restart
```

Com o comando `netstat` devemos verificar a porta 10025/tcp iniciada:

```
# netstat -ntl | grep ":10025"
tcp        0      0 127.0.0.1:10025        0.0.0.0:*               LISTEN
tcp        0      0 :::1:10025            :::*                    LISTEN
```

Os testes de integração podem ser realizados com o comando `telnet`, simplesmente enviando mensagens de um usuário para o outro e observando os registros no arquivo `/var/log/mail`.

A princípio, nenhuma alteração precisa ser realizada para o funcionamento do SpamAssassin, porém é importante sempre melhorar as regras de verificação de SPAM, adicionando novas regras ao arquivo de configuração: `/etc/mail/spamassassin/local.cf`.

## Referências

- ✓ Amavisd-new Home Page  
<http://www.ijs.si/software/amavisd>
- ✓ How To Install Postfix, Amavis, ClamAV, and Spamassassin on Debian Linux  
<http://www.fatofthelan.com/articles/articles.php?pid=22>

- ✓ Integrating amavisd-new Into Postfix For Spam- And Virus-Scanning  
[http://www.howtoforge.com/amavisd\\_postfix\\_debian\\_ubuntu](http://www.howtoforge.com/amavisd_postfix_debian_ubuntu)
- ✓ Montando um servidor de e-mail completo com Postfix  
<http://www.vivaolinux.com.br/artigos/verArtigo.php?codigo=526>