Installing a SpamAssassin, ClamAV and Amavisd-new on EnGarde Secure Linux HOWTO

Installing a SpamAssassin, ClamAV and Amavisd-new on EnGarde Secure Linux HOWTO

Revision History

Revision $Revision: 1.2 $ $Date: 2006/01/19 20:46:27 $

Table of Contents

Chapter 1. Introduction

This document outlines how to install and configure the latest stable versions (as of this writing) of SpamAssassin, ClamAV and Amavisd-new on EnGarde Secure Linux 3.0. It assumes that you have already performed an installation of EnGarde Secure LInux 3.0.X and have configured Postfix and it is successfully sending and receiving mail. If this is not the case you must do so by following the procedures outlined in the EnGarde Secure Linux 3.0 -- Quick Start Guide Section 6.6. Setting up a Mail Server (http://www.engardelinux.org/doc/guides/engarde-quick-start-guide-3.0/engarde-quick-start-guide-3.0/webtool-mail.shtml) before proceeding the steps outlined in this document. You will need to have a shell session as the "root" user to perform the following procedures. You will also need to change your SELinux role to "sysadm_r" by running the command "newrole -r sysadm_r". You will be prompted for a password. Enter the "root" user's password.

Chapter 2. Installation

Here is how to install the necessary packages.

2.1. Download the Packages

Here is the list of packages that you will need to install. The version and release numbers are the earliest ones that will be required for this operation.

- amavisd-new-2.3.3-1.i686.rpm
- clamav-0.88-1.i686.rpm
- perl-Archive-Tar-1.26-1.i686.rpm
- perl-Archive-Zip-1.16-1.i686.rpm
- perl-BerkeleyDB-0.27-1.i686.rpm
- perl-Compress-Zlib-1.41-1.i686.rpm
- perl-Convert-BinHex-1.119-1.i686.rpm
- perl-Convert-TNEF-0.17-1.i686.rpm
- perl-Convert-UUlib-1.06-1.i686.rpm
- perl-Digest-SHA1-2.10-1.i686.rpm
- perl-IO-stringy-2.110-1.i686.rpm
- perl-MIME-Base64-3.07-1.i686.rpm
- perl-MIME-tools-5.419-1.i686.rpm
- perl-MailTools-1.71-1.i686.rpm
- perl-Net-DNS-0.48-1.i686.rpm
- perl-Net-Server-0.90-1.i686.rpm
- perl-Unix-Syslog-0.100-1.i686.rpm
- spamassassin-3.1.0-1.i686.rpm

To download these packages to your server follow the instructions found at http://wiki.engardelinux.org/index.php/Extra_Packages .Use the "apt-get install PACKAGENAME" to do the actual download.

2.2. Installing the Packages

To install the packages you will first have to disable SELinux. Refer to SELinux Quick Start Guide section 3.1. Disabling SELinux (http://www.engardelinux.org/doc/guides/selinux-quick-start-guide/selinux-quick-start-guide/c81.shtml#AEN84) on how to do this. Once SELinux is disabled go to the directory that the packages have been downloaded into.

```
[root@salle1 rpms]# cd /tmp/rpms/
[root@salle1 rpms]# ls -l
total 6260
-rw-r--r--  1 root root  455457 Jan 17 16:42 amavisd-new-2.3.3-1.i686.rpm
-rw-r--r--  1 root root 3620054 Jan 17 16:42 clamav-0.88-1.i686.rpm
-rw-r--r--  1 root root   37347 Jan 17 16:28 perl-Archive-Tar-1.26-1.i686.rpm
```

```
-rw-r--r--  1 root root   73951 Jan 17 16:28 perl-Archive-Zip-1.16-1.i686.rpm
-rw-r--r--  1 root root  190444 Jan 17 16:28 perl-BerkeleyDB-0.27-1.i686.rpm
-rw-r--r--  1 root root  133330 Jan 17 16:28 perl-Compress-Zlib-1.41-1.i686.rpm
-rw-r--r--  1 root root   27144 Jan 17 16:28 perl-Convert-BinHex-1.119-1.i686.rpm
-rw-r--r--  1 root root   14808 Jan 17 16:28 perl-Convert-TNEF-0.17-1.i686.rpm
-rw-r--r--  1 root root  153971 Jan 17 16:28 perl-Convert-UUlib-1.06-1.i686.rpm
-rw-r--r--  1 root root   38030 Jan 17 16:28 perl-Digest-SHA1-2.10-1.i686.rpm
-rw-r--r--  1 root root   63119 Jan 17 16:28 perl-IO-stringy-2.110-1.i686.rpm
-rw-r--r--  1 root root   38311 Jan 17 16:28 perl-MIME-Base64-3.07-1.i686.rpm
-rw-r--r--  1 root root  242802 Jan 17 16:28 perl-MIME-tools-5.419-1.i686.rpm
-rw-r--r--  1 root root   73636 Jan 17 16:28 perl-MailTools-1.71-1.i686.rpm
-rw-r--r--  1 root root    1614 Jan 17 16:28 perl-Net-DNS-0.48-1.i686.rpm
-rw-r--r--  1 root root  111469 Jan 17 16:28 perl-Net-Server-0.90-1.i686.rpm
-rw-r--r--  1 root root   40540 Jan 17 16:28 perl-Unix-Syslog-0.100-1.i686.rpm
-rw-r--r--  1 root root  935141 Jan 17 16:28 spamassassin-3.1.0-1.i686.rpm
[root@salle1 rpms]#
```

Now install the packages using the "rpm" utility.

```
[root@salle1 rpms]# rpm -Uhv *.rpm
Preparing...                ########################################### [100%]
   1:perl-IO-stringy        ########################################### [  6%]
   2:perl-MailTools         ########################################### [ 11%]
   3:perl-MIME-Base64       ########################################### [ 17%]
   4:perl-Compress-Zlib     ########################################### [ 22%]
   5:perl-Archive-Zip       ########################################### [ 28%]
   6:perl-Unix-Syslog       ########################################### [ 33%]
   7:perl-Net-Server        ########################################### [ 39%]
   8:perl-Net-DNS           ########################################### [ 44%]
   9:perl-Digest-SHA1       ########################################### [ 50%]
  10:perl-Convert-UUlib     ########################################### [ 56%]
  11:perl-Convert-BinHex    ########################################### [ 61%]
  12:perl-MIME-tools        ########################################### [ 67%]
  13:perl-Convert-TNEF      ########################################### [ 72%]
  14:perl-Archive-Tar       ########################################### [ 78%]
  15:amavisd-new            ########################################### [ 83%]
  16:clamav                 ########################################### [ 89%]
  17:perl-BerkeleyDB        ########################################### [ 94%]
  18:spamassassin           ########################################### [100%]
[root@salle1 rpms]#
```

Unless any errors were reported you now have all of the required packages and can proceed to configuration.

Chapter 3. Setup

This document assumes that you already have Postfix successfully sending and retrieving mail. If not then refer to SELinux Quick Start Guide section 6.6 Setting up a Mail Server (http://www.engardelinux.org/doc/guides/engarde-quick-start-guide-3.0/engarde-quick-start-guide-3.0/webtool-mail.shtml) .

3.1. ClamAV

The first component of mail filtering that we will look at is the virus scanner ClamAV. The "clamd" daemon will not start until virus identities are downloaded for the first time. You will need to do this manually once. After that the virus identities will be downloaded via the cron service once every three hours. The actual file that defines this is /etc/cron.d/clamav_update. To download manually you will have to change your uid to the "vscan" user and then run the program "freshclam".

```
[root@salle1 tmp]# su - vscan
[vscan@salle1 ~]$
[vscan@salle1 tmp]# freshclam
ClamAV update process started at Thu Jan 19 13:28:35 2006
Downloading main.cvd [*]
main.cvd updated (version: 35, sigs: 41649, f-level: 6, builder: tkojm)
Downloading daily.cvd [*]
daily.cvd updated (version: 1245, sigs: 843, f-level: 6, builder: sven)
Database updated (42492 signatures) from db.us.clamav.net (IP: 216.24.174.245)
ERROR: Clamd was NOT notified: Can’t find or parse configuration file /etc/clamd.conf
[vscan@salle1 tmp]#
[vscan@salle1 ~]$ ls -l /usr/share/clamav
total 2800
-rw-r--r--  1 vscan vscan   97597 Jan 19 13:35 daily.cvd
-rw-r--r--  1 vscan root  2750061 Jan 19 13:33 main.cvd
[vscan@salle1 ~]$
```

As you can see from the listing of /usr/share/clamav there are two files (the ones that have just been downloaded from freshclam) that makeup the virus identity database. The reported ERROR is OK. Clamd couldn’t be notified of the download because it wasn’t running but now that there is virus data clamd can now be started. You will need to change your uid back to the "root" user by typing in exit and then you can start clamd. Follow this with a process listing to verify that clamd is running.

```
[vscan@salle1 ~]$ exit
logout
[root@salle1 tmp]# /etc/init.d/clamd start
[ SUCCESSFUL ] Starting clamd
[root@salle1 tmp]#
[root@salle1 tmp]# ps auxwwww| grep clamd
vscan     2571  0.0  3.7  10912  9440 ?        Ss   13:45   0:00 /usr/sbin/clamd
root      2575  0.0  0.2   1800   552 ttyp2    R+   13:48   0:00 grep clamd
[root@salle1 tmp]#
```

3.2. SpamAssassin

Now on to the spam filter SpamAssassin.The local configuration file for SpamAssassin is /etc/mail/spamassassin/local.cf. There are other configuration files in /usr/share/spamassassin but you don't want to edit those as they will be overwritten anytime you update the SpamAssassin package. All configuration is done in /etc/mail/spamassassin/local.cf. For most situations the default local.cf will suffice. Typically the settings that you will want to change are the point the point thresholds and the actions to be take at these thresholds which is done in the amavisd-new configuration. For more in depth information on SpamAssassin can be found at http://spamassassin.apache.org .

3.3. Amavisd-new

Now we'll configure amavisd-new, the actual content filter. Postfix will pass email to amavisd-new which will then redirect the mail to a virus scanner and a spam scanner based on the default configuration found in the file /etc/amavisd.conf. There are several parameters that you will need to modify in this file. "$myhostname" must be the fully qualified domain name of the server and "$mydomain" should be one of the domains that the server will be processing mail for. In most cases it will be the same domain that the server is in. Here I show the lines that I have added for the server salle1.test.com.

- $myhostname
- $mydomain
- $sa_tag_level_deflt - the spam point level at which amavisd will add a header to the email that displays spam scoring.
- $sa_tag2_level_deflt - the spam point level at which amavisd will tag the "Subject:" with a "***SPAM***" marking.
- $sa_kill_level_deflt - the spam point level at which amavisd will incur the action describe by $final_spam_destiny.
- $final_spam_destiny - the action taken upon mail that is determined to be spam. There are one of four actions: REJECT, BOUNCE, DISCARD or PASS.
- $final_virus_destiny - the action taken upon mail that is determined to be a virus. These actions are the same as above.

"$myhostname" must be the fully qualified domain name of the server and "$mydomain" should be one of the domains that the server will be processing mail for. In most cases it will be the same domain that the server is in. Here I show the lines that I have added for the server salle1.test.com.

```
$myhostname = 'salle1.test.com';
$mydomain = 'test.com';
```

The $sa_tag_level_deflt, $sa_tag_level_defl, $sa_kill_level_deflt and $final_spam_destiny parameters in amavisd.conf are SpamAssassin related.

- $sa_tag_level_deflt - The default value is 0.0. Any mail with a spam score higher that this will cause a score header to be added to the mail (transparent to a browser that displays the normal headers).
- $sa_tag2_level_deflt - The default value is 5.0 which is the standard. If you find that too much spam is still getting undetected you may want to lower this value but do so in small increments, especially if your spam destiny is DISCARD as you may start getting valid mail being determined to be spam.
- $sa_kill_level_deflt - The default value is 5.0. This is because most admins want to take action upon a mail that has been determined to be spam which means it is usually the same value as $sa_tag2_level_deflt.
- $final_spam_destiny - The default value is PASS. This will pass the mail to the recipient with the "Subject:" header tagged with "***SPAM***". This is the safest setting due to the fact that any spam filter will at some point determine that a valid mail is spam, especially right after an initial install as familiarity with the site's spam patterns is not yet established.

- $final_virus_destiny - The default value is DISCARD.

Should you want to make changes to the configuration you would edit /etc/amavisd.conf and then restart amavisd by running the command "/etc/init.d/amavisd start".

```
[root@salle1 ~]# /etc/init.d/amavisd start
[ SUCCESSFUL ] Starting amavisd
[root@salle1 ~]#
```

You can verify that the amavisd daemon is running by doing a process listing that looks for amavisd.

```
[root@salle1 ~]# ps auxwww| grep amavisd
vscan    2286  0.9 16.5  46876 41988 ?       Ss   13:13   0:00 amavisd (master)
vscan    2289  0.0 16.5  47612 42076 ?       S    13:13   0:00 amavisd (virgin child)
vscan    2290  0.0 16.5  47612 42076 ?       S    13:13   0:00 amavisd (virgin child)
root     2312  0.0  0.2   1800   560 ttyp2    S+   13:15   0:00 grep amavisd
[root@salle1 ~]#
```

3.4. Postfix

OK, we have the virus scanner, spam scanner and amavisd set up and running. Now we have to tell postfix to send incoming mail to amavisd and where to get the results back from amavisd. To do this we will have to edit two files in /etc/postfix, master.cf and main.cf.

3.4.1. master.cf

You will need to add the following lines to the end of /etc/postfix/master.cf.

Warning

t is very IMPORTANT that the lines with "-o" have at least one space at the begging of the line. Also lines other than those with "-o" must have NO SPACE at the begging of the line.

```
smtp-amavis unix - - n - 2 smtp -o smtp_data_done_timeout=1200 -o smtp_send_xforward_command=yes -o disable_dns_lookups=yes -o max_use=20

127.0.0.1:10025 inet n - y - - smtpd -o content_filter= -o local_recipient_maps= -o relay_recipient_maps= -o smtpd_restriction_classes= -o smtpd_delay_reject=no -o smtpd_client_restrictions=permit_mynetworks,reject -o smtpd_helo_restrictions= -o smtpd_sender_restrictions= -o smtpd_recipient_restrictions=permit_mynetworks,reject -o mynetworks_style=host -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_unknown_recipient_checks
```

3.4.2. main.cf

You will need to add the following two lines to /etc/postfix/main.cf. These lines should not start with any white space.

content_filter = smtp-amavis:localhost:10024 receive_override_options = no_address_mappings

Now restart postfix by running the command "/etc/init.d/postfix restart". Your server should now discard any viruses detected by ClamAV and tag the subject of mail that has accumulated 5.0 or more spam points as determined by SpamAssassin.

3.5. Bootup

Now that we have added two new daemons (clamd and amavisd) we will want these services to start up automatically at bootup. To do this go to the server's WebTool "Service Configuration" page and turn enable the "Boot state" for clamd and amavisd. This procedure is now complete.