IRAM-COMP-015

Revision: 0
2005-03-08

Contact Author

Institut de RadioAstronomie Millimétrique

Introduction to Postfix

Owner Sebastien Blanchet

Keywords: postfix, sendmail, smtp, imss, spamassassin

Approved by:	Date:	Signature:
A.Perrigouard	March 2005	

Change Record

REVISION	DATE	AUTHOR	ECTION/PAGE AFFECTED	REMARKS

Content

1 Introduction 3

2 Computer and Operating system 3

3 Postfix installation 3

4 Postfix Configuration 4

4.1 Files 4
4.2 Settings 4
4.3 Commands 5

5 Postfix maintenance 6

5.1 Commands 6

6 Interscan Messaging Security Suite 6

6.1 Installation 6

7 Spamassassin 10

7.1 Installation 10
7.2 Configuration 10
7.3 Advanced spamassassin 11

8 Compare with current Sendmail configuration 12

This document introduces Postfix, a mail transfer agent, and its integration with InterScan Messaging Security Suite and Spamassassin on Linux, to be used on IRAM servers.

1 Introduction

In December of 1998, IBM released Secure Mailer as open source software providing a new, freely available alternative to the nearly universal Sendmail program. The program, more commonly known in open-source circles as Postfix, attempts to be fast, easy to administer, and secure. One of the primary goals of Postfix is to be widely implemented in order to make the most significant impact on the performance and security of Internet email overall.

Postfix attempts to be fast, easy to administer, and secure, while at the same time being sendmail compatible enough to not upset existing users. Thus, the outside has a sendmail-ish flavor, but the inside is completely different.

Postfix is widely used on the Internet, for example by:

- free.fr
- wanadoo.fr
- club-internet.fr
- java.sun.com
- samba.org
- freebsd.org

2 Computer and Operating system

To do the test, I have installed a standard Linux RedHat 9.0 on a VMware computer: gre44.iram.fr
After the installation I have apply the security patches and configure iptables.
I have also installed nmap, nedit and imap

To send and receive email, I have used Thunderbird-1.0 from pctcp72.iram.fr. It will be useful for testing.

3 Postfix installation

Download the last version of postfix from www.postfix.org
Note: it is better if sendmail is not installed on the computer

```
# cd /tmp
# tar xfz ~/postfix-2.1.5.tar.gz
# cd postfix-2.1
# make
# adduser postfix -s /sbin/nologin
# groupadd postdrop

# make install
```

```
   Warning: you still need to edit myorigin/mydestination/mynetworks
    parameter settings in /etc/postfix/main.cf.

    See also http://www.postfix.org/faq.html for information about
dialup sites or about sites inside a firewalled network.
```

```
    BTW: Check your /etc/aliases file and be sure to set up aliases
    that send mail for root and postmaster to a real person, then run
    /usr/bin/newaliases.
```

To start automatically postfix at the startup, you need a init.d script.
Get it from a postfix rpm package for Redhat:

```
# mkdir /tmp/postfix
# cd !$
# rpm2cpio postfix-1.11.i386.rpm | cpio -id
# cp etc/rc.d/init.d/postfix  /etc/rc.d/init.d/postfix

# ln -s /etc/init.d/postfix /etc/rc3.d/S81postfix
# ln -s /etc/init.d/postfix /etc/rc5.d/S81postfix
# ln -s /etc/init.d/postfix /etc/rc6.d/K29postfix
# ln -s /etc/init.d/postfix /etc/rc0.d/K29postfix
```

4 Postfix Configuration

4.1 Files

All the configuration files are located in /etc/postfix.

```
[root@gre44 root]# ls -1 /etc/postfix/
access
aliases
aliases.db
canonical
header_checks
LICENSE
main.cf
main.cf.default
makedefs.out
master.cf
postfix-files
postfix-script
post-install
relocated
transport
virtual
```

In fact, only `/etc/postfix/main.cf` and `/etc/postfix/master.cf` are real configuration files. The others files (access, aliases, canonical, relocated, virtual) are data files, and can be replaced by a database.

4.2 Settings

The configuration files are very well documented, with numerous examples
`# man -S 5 postconf`

For example, this is the settings for an operational postfix on gre44.iram.fr
/etc/postfix/main.cf

```
alias_maps = hash:/etc/postfix/aliases
command_directory = /usr/sbin
```

```
config_directory = /etc/postfix
content_filter = imss:localhost:10025
daemon_directory = /usr/libexec/postfix
debug_peer_level = 2
default_process_limit = 200
html_directory = no
mail_owner = postfix
mailbox_command = /usr/bin/procmail -f- -a "$USER"
mailq_path = /usr/bin/mailq
manpage_directory = /usr/local/man
mydomain = gre44.iram.fr
myhostname = gre44.iram.fr
mynetworks = 127.0.0.0/8, 193.48.252.0/24
newaliases_path = /usr/bin/newaliases
queue_directory = /var/spool/postfix
readme_directory = no
sample_directory = /etc/postfix
sendmail_path = /usr/sbin/sendmail
setgid_group = postdrop
unknown_local_recipient_reject_code = 550
```

The settings are easy to understand: for example to control the anti-relay, just defined *mynetwork,* and postfix will relay only the mail **from** *mynetwork* or **to** *mynetwork*.

4.3 Commands

You may use sendmail-like commands with Postfix (mailq, sendmail, newaliases, etc), it is useful for legacy scripts. But for manual operation, native postfix command are more convenient.

This a summary of the configuration commands:

postfix reload
This command re-read configuration files. Running processes terminate at their earliest convenience.

postconf
This command prints the actual value of a parameter (all known parameters by default). With the –n option, it displays only the parameter settings that are not left at their built-in default value.

postalias
This command creates or queries one or more Postfix alias databases, or updates an existing one. The input and output file formats are expected to be compatible with Sendmail version 8, and are expected to be suitable for the use as NIS alias maps.

5 Postfix maintenance

5.1 Commands

postqueue
This command manages the queue

- flush the queue: `postqueue -f`
- display the queue: `postqueue -p`

postsuper
This command does maintenance jobs on the postfix queue. This command required to be root. You can delete, hold, release, etc. messages in the queues.

postfix
This command controls the operation of the Postfix mail system: start or stop the master daemon, do a health check and other maintenance.

6 Interscan Messaging Security Suite

IMSS is an antivirus for the SMTP traffic, edited by Trend Micro.

6.1 Installation

Use the standard installation

```
# cd /tmp
# tar xvfz InterScanMSS-5.5/imss_linux_55_1123_en.tar.gz
# cd IMSS55_LX_GM/
# ./isint
```

```
InterScan MSS will be installed on machine redhat Red Hat Linux release
9 (Shrike)

Specify installation path
install_directory: [/opt/trend]

User choose /opt/trend as install path.
Trend Micro License Agreement
(Release Build Version 0403Nov03)
[....]

Do you agree with the Trend License Agreement? [y/n]y
Checking disk space for InterScan MSS for Unix.
Sufficient disk space is available.
Checking Postfix ...
```

```
***********************************************************************
***
Postfix version 2.1.5 has been found in your machine.
Manually change the Postfix configuration to enable the content filter
interface to the InterScan MSS for Unix scanning daemon in the
following fashion:

Insert or modify the following settings to /etc/postfix/main.cf
mydomain = your.domain.name
myhostname = your.hostname.domainname
mydestination = $myhostname, localhost.$mydomain, $mydomain
default_process_limit=200
imss_timeout=10m
imss_connect_timeout=1s
content_filter = imss:localhost:10025
imss_destination_recipient_limit=200
imss_destination_concurrency_limit=20

Insert the following settings to /etc/postfix/master.cf
#InterScan MSS: content filter smtp transport imss for InterScan MSS
imss unix - - n - - smtp
-o disable_dns_lookups=yes
-o smtp_connect_timeout=$imss_connect_timeout
-o smtp_data_done_timeout=$imss_timeout

#InterScan MSS: content filter loop back smtpd
localhost:10026 inet n - n - 20 smtpd
-o content_filter=
-o smtpd_timeout=$imss_timeout
-o local_recipient_maps=
-o myhostname=localhost.$mydomain

This message is found in the /opt/trend/installlog/ImssInstall.log.
***********************************************************************
***
Press Enter to continue .....
[…]
Type the mailserver domain name: gre44.iram.fr
The mailserver domain name is gre44.iram.fr. Is this correct?[y/n] y
Got the mailserver domain name gre44.iram.fr from the user.
Most customers install the Web administrative interface component by
default.
If your server does not have Web UI component, you may choose to skip
the installation of the Web interface.
Would you like to install Web interface now? [y/n]? (default is "yes")y

InterScan MSS allows you to manage a restricted subset of Postfix
configurations through our Web interface.
Would you like to manage these Postfix configurations through our Web
interface[y/n]?(default is "yes") n
For more information on Postfix, see Appendix I in the "Getting Started
Guide".
Install
[…]
Do you want to install the Control Manager agent? [y/n] n
Do you want to install the AMON support ? [y/n] n
buildno=Version5.5-Build_Linux_1123
Do you want to Activate Trend Micro Antivirus and eManager
now[y/n]?(default is yes)y
----------------------------------------------------
 Now registering Trend Micro Antivirus and eManager.
```

```
----------------------------------------------------
Enter Trend Micro Antivirus and eManager Activation Code: IM-M5UM-
WSZDK-3M5N3-YAA9Y-FLFKY-XR6AH

        1. Activate Code : IM-M5UM-WSZDK-3M5N3-YAA9Y-FLFKY-XR6AH
        2. Use Proxy : no
        3. Proxy IP or hostname:
        4. Proxy Port:
        5. Proxy UserName/Password:
        6. Use Sock4 Proxy : no
Is this information correct? [y/n](default is yes) y
Trend Micro Antivirus and eManager registration.
Success. [0x00000001].
Antivirus and eManager registration was successful.
Trend Micro Antivirus and eManager status.
License has not expired. [0x60010106].
Remaining 64 days before expiration.
You have successfully registered the Trend Micro Antivirus and eManager
software.
Do you want to Activate SPS now[y/n]?(default is yes)n
After installation complete, activate InterScan MSS SPS through the web
console
Start the product process.
[…]
To access the InterScan MSS for Unix Web UI, use the following URL:
https://yourhost:8445/IMSS.html
or
https://yourip:8445/IMSS.html

http://yourhost:8081/IMSS.html
or
http://yourip:8081/IMSS.html

Trend Micro periodically releases service packs
and patches to resolve known product issues.
Customers are advised to regularly check
http://www.trendmicro.com/download/product.asp?productid=12
and install any InterScan Messaging Security Suite
patches or service packs that may be available.
If you install the IMSS agent for Trend Micro Control
Manager, install the IMSS agent before installing any
service packs or patches to ensure the IMSS agent
for Control Manager is also updated.
```

Now install Service Pack 2

```
# cd IMSS55_LX_SP2/
# ./patchinstall install

The IMSS v5.5 installtion directory is /opt/trend/imss. Is it correct?
[y/n] Default is 'y'.
y

The installer is going to back up the original files.
The backup directory is /tmp/IMSS55_LX_SP2/b4sp2
Press Return (or Enter) Key to Continue...

Stop all IMSS services...
[…]
```

```
Installer is copying the original files to the directory
/tmp/IMSS55_LX_SP2/b4sp2 ...
[…]
Files have been backed up.

Copying the files...
[…]
Total file copied:26


Restart IMSS services...
[…]
The following is the pre-approved sender list.
[..]
*@ddj.com
*@dv.com
*@ebnonline.com
*@eet.com
*@eetnetwork.com
*@eedesign.com
*@electronicstimes.com
*@esconline.com
*@embedded.com
*@financetech.com
*@ftexpo.com

Do you want to apply the pre-approved sender list as shown above? [y/n]
Default is 'y'.
y
Apply the pre-approved sender list...
Apply the SPS value

Stop imsssysmon.
Stop regserver.
Shutting down regserver services:
Kill the PID 3140 by owner root.

[…]
The Service Pack 2 for IMSS v5.5 has been successfully installed.
```

Now we do a minimum configuration on IMSS via the web user interface
Connect https://gre44:8445/IMSS.html

- Set a password
- Download the updates
- Setup automatic hourly update
- Disable POP3

For the other settings, copy the current settings from netsrv1.iram.fr

Now edit /etc/postfix/main.cf, and append the following line to it

```
# IMSS parameters

default_process_limit=200
imss_timeout=10m
imss_connect_timeout=1s
content_filter = imss:localhost:10025
imss_destination_recipient_limit=200
imss_destination_concurrency_limit=20
```

Edit /etc/postfix/master.cf, to add the following lines:

```
#InterScan MSS: content filter loop back smtpd
   localhost:10026 inet n - n - 20 smtpd
    -o content_filter=
    -o smtpd_timeout=$imss_timeout
    -o local_recipient_maps=
    -o myhostname=localhost
```

Warning: at least one space is required at the beginning of the lines with "–o"

```
# /etc/init.d/postfix restart
# /etc/init.d/S99IMSS restart
```

Test: Send an email with an attached document and look the log in /opt/trend/imss/log and in /var/log/maillog

7 Spamassassin

Spamassassin is a very powerful open-source spam filter. It is independent from the mail transfer agent. So it works with postfix, sendmail, etc.

7.1 Installation

Download the last version of spamassassin from http://spamassassin.apache.org

```
# rpmbuild -tb Mail-SpamAssassin-3.0.2.tar.gz
# cd /usr/src/redhat/RPMS/i386/
# rpm -Uvh perl-Mail-SpamAssassin-3.0.2-1.i386.rpm spamassassin-3.0.2-
1.i386.rpm
```

If `perl-Digest-SHA1` is missing, you can found it on the RedHat 9.0 cdrom #2

7.2 Configuration

There are two alternatives to integrated spamassassin in postfix:

- via master.cf, like the IMSS case
- via procmail

The 2nd possibility is really simpler, therefore I have chosen it.

Add Procmail to /etc/postfix/main.cf

```
mailbox_command = /usr/bin/procmail -f- -a "$USER"
```

Create /etc/procmailrc:

```
# Run procmail as User
DROPPRIVS=yes
#
LOGFILE=/var/log/procmail.log
VERBOSE=ON

# Spamassassin

:0fw
* < 256000

        | /usr/bin/spamc

        :0e
        {
                EXITCODE=$?
        }
```

If you want to check the log of procmail (otherwise you will have nothing). Procmail runs as a normal user, therefore we need to modify the permissions on the log file.

```
# touch /var/log/procmail.log
# chmod 777 /var/log/procmail.log
```

Edit /etc/mail/spamassassin/local.cf to add:

```
rewrite_header Subject *****SPAM*****
```

Start automatically spamassassin

```
# chkconfig spamassassin on
# service spamassassin restart
```

send an email to test

7.3 Advanced spamassassin

To tune spamassassin, it is very convenient if you can send a raw email, without using an email client.

create /usr/local/bin/sa-filter.sh

```
#!/bin/bash
/usr/bin/spamassassin | /usr/sbin/sendmail -i "$@"
```

```
exit $?
```

Now you can test easily spamassassin settings

```
# cd /usr/share/doc/spamassassin-3.0.2/
# cat sample-spam.txt | /usr/local/bin/sa-filter.sh -f root – root
```

You can add new anti-spam rules by adding files in /usr/share/spamassassin

8 Compare with current Sendmail configuration

The current sendmail's installation uses a sandwich configuration to integrate IMSS.

This new postfix installation versus the old sendmail installation is:

- More efficient: aliases are expanded at the end, so IMSS does not scan duplicated messages.
- Easier to manage: /etc/postfix/main.cf is infinitely simpler than the old cryptic /etc/mail/sendmail.cf.
- Safer and more robust: sendmail configuration is really error-prone

Sendmail has been written for the computer, postfix for the humans.