MySpamGuard 1.1-3
Installation Manual

Research & Development Unit
Open Source Competency Centre (OSCC),
MAMPU,
Lot E302-34, Enterprise Building 3,
63000 Cyberjaya, Selangor
Tel: 03-8319 1200
Fax: 03-83193206
http://opensource.mampu.gov.my

Table of Contents

Introduction

MySpamGuard is an email spam solution. It searches the headers and text of incoming emails to determine whether it is spam based on the procmail instruction or rules set by the user. MySpamGuard will classify the suspected spam accordingly; email sent by a virus, email from a known spam source which is definitely spam, and email which is probably spam. It then tags the filtered out email with the appropriate header and respond accordingly to the action specified by the users.

New features in MySpamGuard 1.1

- Easy installation process. The files needed will be downloaded automatically by the installer.
- All modules needed in MySpamGuard are combined as one package. The modules are:

  SpamAssassin – spam checking aplication

  MailScanner – email scanning for general filtering

  ClamAV – anti virus solution
- Minimum configuration because most of the configuration is installed automatically by the installer
- Automatic update for all package from OSCC repository server
- Easy to upgrade to the next version

Hardware and Software Requirements

Hardware

Recommended hardware

-Pentium IV and above

-512MB RAM and above

-10GB HD and above

-1 NIC Card

Software

- CentOS 5 / Red Hat Enterprise Linux – Operating System
- Postfix – Mail Transport Agent (MTA)
- SpamAssassin – Spam Checking
- MailScanner – Email Scanning
- MailWatch (php+MySQL) – Reporting and Statistics
- ClamAV – Antivirus
- Webmin – Web Based Administration (optional)

Dependencies Installation

Dependencies Resolved

Package	Arch	Version	Repository	Size
Installing:				
myspamguard	*noarch*	*1.1-3.oscc*	*oscc-repo*	*41 k*
Installing for dependencies:				
MailScanner-perl-MIME-Base64	*i386*	*3.05-5*	*oscc-repo*	*44 k*
apr	*i386*	*1.2.7-11*	*base*	*122 k*
apr-util	*i386*	*1.2.7-6*	*base*	*75 k*
clamav	*i386*	*0.91.2-1.el5.rf*	*oscc-repo*	*1.1 M*
clamav-db	*i386*	*0.91.2-1.el5.rf*	*oscc-repo*	*10 M*
clamd	*i386*	*0.91.2-1.el5.rf*	*oscc-repo*	*81 k*
gmp	*i386*	*4.1.4-10.el5*	*base*	*664 k*
httpd	*i386*	*2.2.3-11.el5.centos*	*base*	*1.1 M*
mailscanner	*noarch*	*4.74.15-2*	*oscc-repo*	*687 k*
mailwatch	*noarch*	*1.0.4-4*	*oscc-repo*	*2.4 M*
mysql	*i386*	*5.0.22-2.1.0.1*	*base*	*3.0 M*
mysql-server	*i386*	*5.0.22-2.1.0.1*	*base*	*10 M*
oscc-bayesian	*noarch*	*0.0.2-2.oscc*	*oscc-repo*	*2.2 M*
oscc-tracking	*noarch*	*0.0.2-1.oscc*	*oscc-repo*	*29 k*
perl-Archive-Tar	*noarch*	*1.30-1.fc6*	*base*	*47 k*
perl-Archive-Zip	*noarch*	*1.20-1.el5.rf*	*oscc-repo*	*100 k*
perl-Compress-Zlib	*i386*	*1.42-1.fc6*	*base*	*52 k*
perl-Convert-BinHex	*noarch*	*1.119-2.2.el5.rf*	*oscc-repo*	*34 k*
perl-Convert-TNEF	*noarch*	*0.17-3.2.el5.rf*	*oscc-repo*	*18 k*
perl-DBD-MySQL	*i386*	*3.0007-1.fc6*	*base*	*147 k*
perl-DBD-SQLite	*i386*	*1.13-1.el5.rf*	*oscc-repo*	*50 k*
perl-DBI	*i386*	*1.52-1.fc6*	*base*	*605 k*
perl-Digest-HMAC	*noarch*	*1.01-15*	*base*	*12 k*
perl-Digest-SHA1	*i386*	*2.11-1.2.1*	*base*	*48 k*
perl-Error	*noarch*	*0.17008-2.el5.rf*	*oscc-repo*	*26 k*
perl-Filesys-Df	*i386*	*0.92-1.el5.rf*	*oscc-repo*	*35 k*
perl-HTML-Parser	*i386*	*3.56-1*	*oscc-repo*	*124 k*
perl-HTML-Tagset	*noarch*	*3.10-2.1.1*	*base*	*15 k*
perl-IO-Socket-INET6	*noarch*	*2.51-2.fc6*	*base*	*13 k*
perl-IO-Socket-SSL	*noarch*	*1.07-2.el5.rf*	*oscc-repo*	*43 k*
perl-IO-Zlib	*noarch*	*1.04-4.2.1*	*base*	*15 k*
perl-IO-stringy	*noarch*	*2.110-1.2.el5.rf*	*oscc-repo*	*70 k*
perl-MIME-tools	*noarch*	*5.420-2.el5.rf*	*oscc-repo*	*276 k*
perl-Mail-SPF	*noarch*	*2.005-1.el5.rf*	*oscc-repo*	*142 k*
perl-MailTools	*noarch*	*1.77-1.el5.rf*	*oscc-repo*	*85 k*

perl-Net-CIDR	*noarch*	*0.11-1.2.el5.rf*	*oscc-repo*	*15 k*
perl-Net-DNS	*i386*	*0.61-1.el5.rf*	*oscc-repo*	*276 k*
perl-Net-Daemon	*noarch*	*0.43-1*	*oscc-repo*	*44 k*
perl-Net-IP	*noarch*	*1.25-2.fc6*	*base*	*31 k*
perl-Net-SSLeay	*i386*	*1.30-4.fc6*	*base*	*195 k*
perl-NetAddr-IP	*i386*	*4.007-1.el5.rf*	*oscc-repo*	*129 k*
perl-Socket6	*i386*	*0.19-3.fc6*	*base*	*22 k*
perl-Sys-Hostname-Long	*noarch*	*1.4-1.2.el5.rf*	*oscc-repo*	*12 k*
perl-TimeDate	*noarch*	*1:1.16-5.el5*	*base*	*32 k*
perl-URI	*noarch*	*1.35-3*	*base*	*116 k*
perl-libwww-perl	*noarch*	*5.805-1.1.1*	*base*	*376 k*
perl-version	*i386*	*0.72.3-1.el5.rf*	*oscc-repo*	*75 k*
php	*i386*	*5.1.6-15.el5*	*base*	*1.2 M*
php-cli	*i386*	*5.1.6-15.el5*	*base*	*2.3 M*
php-common	*i386*	*5.1.6-15.el5*	*base*	*140 k*
php-gd	*i386*	*5.1.6-15.el5*	*base*	*111 k*
php-mysql	*i386*	*5.1.6-15.el5*	*base*	*83 k*
php-pdo	*i386*	*5.1.6-15.el5*	*base*	*61 k*
postfix	*i386*	*2:2.3.3-2*	*base*	*3.6 M*
postgresql-libs	*i386*	*8.1.9-1.el5*	*base*	*196 k*
spamassassin	*i386*	*3.1.9-1.el5*	*base*	*922 k*
tnef	*i386*	*1.4.3-1.el5.rf*	*oscc-repo*	*44 k*

Transaction Summary

==========

Install	*58 Package(s)*
Update	*0 Package(s)*
Remove	*0 Package(s)*

Total download size: 44 M

This dependencies will be installed automatically by MySpamGuard Installation. Used this list to check for any missing dependencies during installation.

Prerequisites

CentOS 5 Installation

CentOS is an Enterprise-class Linux Distribution derived from sources freely provided to the public by a prominent North American Enterprise Linux vendor. CentOS is perfect for servers and cluster nodes where newer software is not a requirement.

CentOS preferred software updating tool is based on yum, although support for use of an up-to-date variant exist. Each may be used to download and install both additional packages and their dependencies, and also to obtain and apply periodic and special (security) updates from repositories on the CentOS Mirror Network. The current version of CentOS is CentOS 5.0 and it was released on April 12 2007.

How to install CentOS 5.

1) Place the DVD/CD-ROM in your DVD/CD-ROM drive and boot your system from the DVD/CD-ROM. If the DVD/CD-ROM drive is found and the driver loaded, the installer will present you with the option to perform a media check on the DVD/CD-ROM. This will take some time, and you may option to skip over this step.
2) The welcome screen will appear and click 'Next' to proceed.
3) Language selection - Select the language and it will become the default language for the operating system once it is installed. Selecting the appropriate language also helps target your timezone configuration later in the installation. The installation program tries to define the appropriate time zone based on what you specify on this screen. Once you select the appropriate language, click 'Next' to continue.
4) Keyboard Layout Selection - Select the correct layout type for the keyboard you would prefer to use for the installation and as the system default. Click 'Next' to continue installation.
5) Setup your disk partitioning, the first three option will perform automatic partitioning while

'Create customs layout' will perform manual partition.

6) For Network configuration, the installation program will automatically detects any network devices and its hostname. You can edit its configuration or just click 'Next' to continue.
7) Set your time zone by selecting the city closest to your computer's physical location. Select 'System Clock uses UTC' if your system is set to UTC. (for this installation, unselect it)
8) Set root password. **This is the most important steps because root account is used for system administration.**
9) You can customize software selection of your system or do it after installation.
10) A screen preparing the installation will be appear. For your reference, a complete log of your installation can be found in /root/install.log once you reboot your system.
11) This step is when the installation program installing all the packages. How quickly this happens depends on the number of packages you have selected and your computer's speed.
12) Now your installation is complete. The installation program prompts you to prepare your system for reboot.
13) Then, start your CentOS 5 in run level 5 (graphical run level), the Setup Agent is presented, which guides you through the CentOS configuration. Using this tool, you can set up your system time and date, install software, register your machine with CentOS Network and more.

Taken from: http://www.centos.org/docs/5/html/Installation_Guide-en-US/

Reference: http://www.howtoforge.com/perfect_server_centos4.5

Email Server (MTA)

Postfix

Postfix is a free software/open source mail transfer agent (MTA), a computer program for the routing and delivery of email. It is intended as a fast, easy to administer and secure alternative to the widely-used Sendmail MTA. The strengths of Postfix are its resilience against buffer overflows and also its handling of large amounts of e-mail.

Website: http://www.postfix.org/

MailScanner

MailScanner is an open source e-mail security system for use on Unix e-mail gateways, first released in 2001. It protects against viruses and spam and it is distributed under GNU General Public License. It can decode and scan attachments intended solely for Microsoft Outlook users (MS-TNEF). If possible, it will disinfect infected documents and deliver them automatically. It also has features which protect it against Denial Of Service attacks.

Website: http://www.mailscanner.info/

MailWatch

MailWatch for MailScanner is a web-based front-end to MailScanner written in PHP, MySQL and JpGraph and is available for free under the terms of the GNU Public License. It comes with a CustomConfig module for MailScanner which causes MailScanner to log all messages data (excluding body text) to a MySQL database which is then queried by MailWatch for reporting and statistics.

Features:

- displays the inbound/outbound mail queue size (currently for Sendmail/ Exim users only), Load Average and Today's Totals for Messages, Spam, Viruses and Blocked Content on each page header.
- Colour-coded display of recently processed mail.
- Drill-down onto each message to see detailed information.

- Quarantine management allows you to release, delete or run sa-learn accross any quarantined messages.
- Reports with customisable filters and graphs by JpGraph
- Tools to view Virus Scanner status (currently Sophos only), MySQL database status and to view the MailScanner configuration files.
- Utilities for Senmail to monitor and display the mail queue sizes and to record and display message relay information.
- Multiple user levels: user, domain and admin that limit the data and features available to each.
- XML-RPC support that allows multiple MailScanner/ MailWatch installations to act as one.

Website: http://mailwatch.sourceforge.net/doku.php

SpamAssassin

It is a program that is used for e-mail spam filtering which based on content-matching rules. It classify the spam by matching the combination of the comparison of words and symbols used in e-mail's header and body. It is the most effective spam filter, especially when used in combination with spam databases.

For CentOS, it is automatic installed once your distro is installed.

Website: http://spamassassin.apache.org/

ClamAV

It is free anti virus software toolkit for Unix-like operating systems. It is mainly used with a mail exchange server as a server-side e-mail virus scanner. Both ClamAV and its updates are made available free of charge. ClamAV is generally configured to automatically update its list of virus definitions via the Internet.

Website: http://www.clamav.net/

Steps of installation MySpamGuard

1. Open a Terminal

2 . Install OSCC repository and rpmforge

rpm -Uvh http://repos.oscc.org.my/centos/5/os/i386/CentOS/oscc-repos-0.0.1-1.noarch.rpm

rpm -Uvh http://dag.wieers.com/rpm/packages/rpmforge-release/rpmforge-release-0.3.6-1.el5.rf.i386.rpm

3. Disable firewall, SELinux and make sure mysql root password is set to none to ease up installation. You can change all these settings after installation.

4. Install MySpamGuard

yum install myspamguard

A warning about mirror will prompt and waiting for your answer. It will appear because CentOS is recognizing a new mirror (in this case, OSCC mirror)

warning: rpmts_HdrFromFdno: Header V3 DSA signature: NOKEY, key ID e8562897
Importing GPG key 0xE8562897 "CentOS-5 Key (CentOS 5 Official Signing Key) <centos-5-key@centos.org>" from http://mirror.centos.org/centos/RPM-GPG-KEY-CentOS-5
Is this ok [y/N]:

Type 'y' to continue.

5. Install dependencies perl-OLE-Storage_Lite

yum install perl-OLE-Storage_Lite

6. Run MySpamGuard

After the installation is complete, open web browser.

Type this url http://localhost/mailscanner/

Use this default username and password, but we recommend you to change the password for security purpose.

username: admin

password: kambing1234

7. Edit configuration files

Stop postfix and MailScanner services before changing files

I) file: /etc/postfix/main.cf

myhostname = YOUR_HOST_NAME (eg: myspamguard.oscc.org.my)

inet_interface = all

transport_maps = hash:/etc/postfix/transport **(**add this line if it does not exist)**

relayhost = YOUR_DOMAIN_NAME (eg: http://www.oscc.org.my) **(**optional)**

II) file: /etc/postfix/transport

(add this sentence)

DOMAIN1 smtp:[MAIL_SERVER1_IP_ADDRESS]

DOMAIN2 smtp:[MAIL_SERVER2_IP_ADDRESS]

eg: oscc.org.my smtp:[10.20.20.3]

then run the command *postmap /etc/postfix/transport*

III) file: /etc/MailScanner/MailScanner.conf

%org-name% = YOUR_ORGANIZATION_SHORT_NAME (e.g: OSCC)

%org-long-name% = YOUR_ORGANIZATION_NAME (e.g: Open Source Competency Centre)

%web-site% = YOUR_ORGANIZATION_WEBSITE (e.g: http://oscc.org.my)

Dangerous Content Scanning = no

Maximum Archive Depth = 0

IV) Check the permissions of folders in /var/www/html/mailscanner/

chown apache:apache /var/www/html/mailscanner/images/cache

chmod ug+rwx /var/www/html/mailscanner/images/cache

Check sendmail services (*/etc/init.d/sendmail status*) and STOP sendmail if the services exist (*/etc/init.d/sendmail stop*)

Start postfix services. (*/etc/init.d/postfix start*)

Start MailScanner services. (*/etc/init.d/MailScanner start*)

Test application in browser with this url *http://localhost/mailscanner* (refer step no 4)

Send one testing email by typing this command:

echo "ujian123" | mail -s "test email" root@localhost

Webmin Installation (optional)

Webmin is a web-based interface for system administration for Unix. Using any browser that supports tables and forms (and Java for the File Manager module), you can setup user accounts, Apache, DNS, file sharing and so on.

Webmin consists of a simple web server, and a number of CGI programs which directly update system files like */etc/initd.conf* and */etc/passwd*. The web server and all CGI programs are written in Perl version 5, and use no non-standard Perl modules.

Websites: http://www.webmin.com

Webmin Installation and Configuration

1. Run this command to install:

   rpm -Uvh http://repos.oscc.org.my/centos/5/os/i386/CentOS/webmin-1.370-1.noarch.rpm
2. The rest of the installation wil be done automatically to the directory /usr/libexec/webmin, the administration username set to root and the password to your current root password.
3. Open your browser and go to http://localhost:10000/
4. To administer from MailScanner from Webmin, you have to install MailScanner Webmin module.
   - Download the module from http://repos.oscc.org.my/centos/5/os/i386/CentOS/webmin-module-1.1-4.wbm
   - Once inside webmin, choose 'Webmin > Webmin Configuration' from the left panel
   - Choose 'Webmin Modules'
   - Select install from local file. Select the '...' button and find the downloaded webmin module from your computer.
   - Select Install Module
   - Refresh your browser for the changes to take effect.

5. Post installation:

   The following module configuration examples should be tailored to suite your installation:

   Full path to MailScanner program = /usr/lib/MailScanner/

   Full path and filename of MailScanner config file = /etc/MailScanner/MailScanner.conf

   Full path to the MailScanner bin directory = /usr/sbin

   Full path and filename for the MailScanner pid file = /var/run/MailScanner.pid

   The following changes should be made:

   "Command to start MailScanner" add *"/etc/init.d/MailScanner start"* (without the quotes) instead of just run server.

   "Command to stop MailScanner" add *"/etc/init.d/MailScanner stop"* (without the quotes)

Maintenance

The following should be checked on a regular basis:

Network connections

The administrator should verify the server is reachable from the public network to avoid service interruption. Network monitoring is beyond the scope of these manual.

Log files

With the log files, it is possible to identify and monitor hardware and software problems on the servers. The log files should be checked at least once a week. All log files in /var/log/ directory.

Services

Used to start, stop or cancel a service on a local or remote computer. It is also a tool to set up recovery actions to take place if a service should fail. Should be checked in case of service failure.

e.g:

#/etc/init.d/[service_name] start/stop/status

Package update/patch

Check that the latest package update/patches has been installed on the servers. It should be checked and done at least once a month.

Disk Space

to verify that there is always enough space on the most mission critical servers. It should be done at least once a week. Use *df -lh* command.

Password change

Password should be changed periodically, at least every three months.

ClamAV update

Execute command *freshclam* frequently to verify automatic update is successfully done.

Check SpamAssassin rules

Execute command *sa-update -D* at least once a month to download the latest spamassassin rules.