



MYSPAMGUARD

Administration Manual

Version 2.1

OPEN SOURCE COMPETENCY CENTRE (OSCC) MAMPU

Level 3, APT E302-E304
Enterprise Building, Persiaran APEC
63000 Cyberjaya
Selangor
Tel: (6)03-8319 1200
Fax: (6)03-8319 3206
E-mail: helpdesk@oscc.org.my
<http://opensource.mampu.gov.my>

Table of Contents

- INTRODUCTION.....1
- OBJECTIVES.....1
- FEATURES.....2
- ARCHITECTURE.....2
- ADMINISTRATION.....4
 - Login Page.....4
 - MySpamGuard Console.....4
 - Status Bar.....5
 - Menu Bar.....7
- Maintenance.....15

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 application
 - 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

OBJECTIVES

MySpamGuard assists the Public Sector agencies to achieve the following objectives:

- To reduce number of incoming spam email in user's inbox..
- Easy to handle or managing the incoming spam email using MailWatch the Spam System front-end.
- Administrator have the total handling for rules use to block incoming spam email.

FEATURES

Some of the features available in MySpamGuard are:

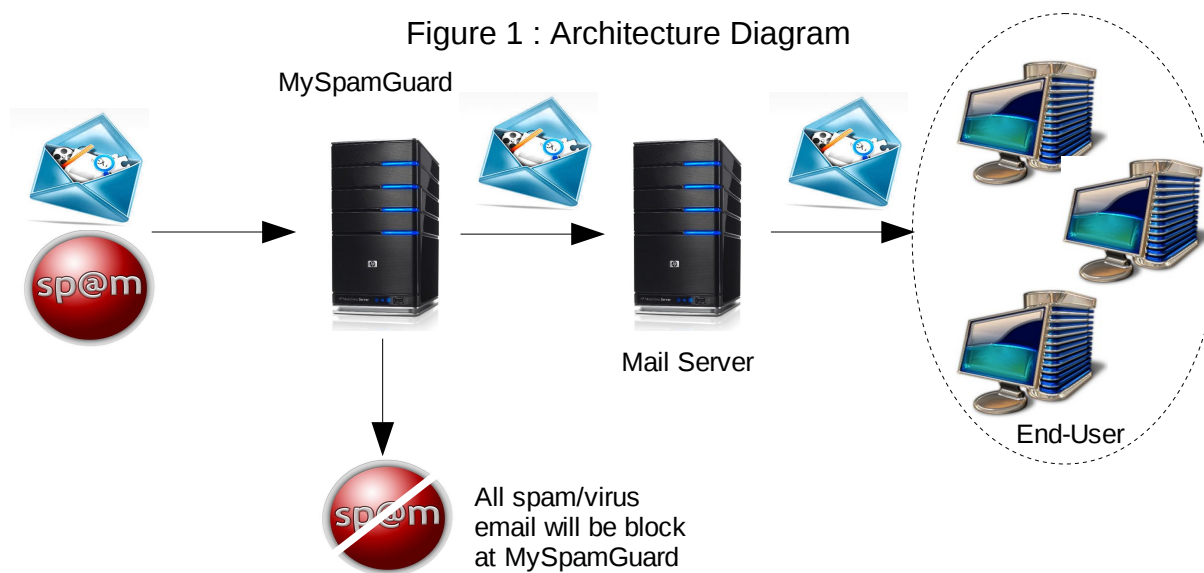
- Easy installation process. The files needed will be downloaded automatically by the installer.
- All modules needed in MySpamGuard are combined as one package. The modules are:
 - SpamAssassin – spam checking application
 - MailScanner – email scanning for general filtering
 - ClamAV – anti virus solution
- Minimum configuration because most of the configuration is installed automatically by the installer

ARCHITECTURE

There are three components in MySpamGuard which are ***Spam Component***, ***Spam Database***, and ***MySpamGuard Console***.

- ***Spam Component*** using MailScanner as the spam and virus email blocker
- All mail and data for suite component in MyWorkSpace will be stored in the ***Mail Database***.
- There are two mail transporters used in MyWorkSpace:
 - Postfix acts as a ***Mail Transfer Agent (MTA)*** which transfers electronic mail messages from one computer to another.
 - DBMail acts as a ***Mail Delivery Agent (MDA)*** which stores and retrieves email received between the MTA and database.

Figure 1 : Architecture Diagram

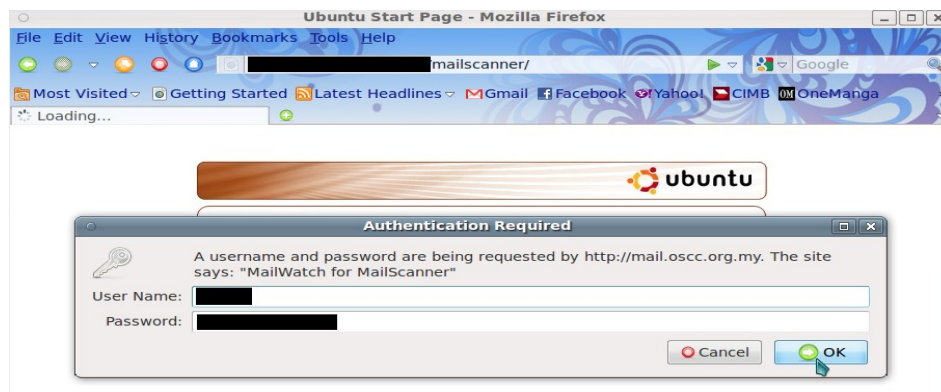


ADMINISTRATION

Login Page

Open your web browser to login into **MySpamGuard Console**, as shown below:

URL: http://DOMAIN_NAME/mailscanner



MySpamGuard Console



mailwatch.sourceforge.net

Jump to message:

Color Codes

- Bad Content/Infected
- Spam
- High Spam
- MCP
- High MCP
- Whitelisted
- Blacklisted
- Clean

Status

MailScanner: YES 5 children

Postfix: YES 1 proc(s)

Load Average: 0.04 0.05 0.08

Mail Queues

Inbound: 0

Outbound: 0

Today's Totals

Processed:	206	2.1Mb
Clean:	173	84.0%
Viruses:	0	0.0%
Top Virus:	None	
Blocked files:	0	0.0%
Others:	0	0.0%
Spam:	14	6.8%
High Scoring Spam:	19	9.2%
MCP:	0	0.0%
High Scoring MCP:	0	0.0%

Recent Messages Lists Quarantine Reports Tools/Links Logout

Last 50 Messages (Refreshing every 30 seconds)						
#	Date/Time	From	To	Subject	Size	SA Score Status
[]	18/12/09 10:37:48				3.2Kb	0.00 Clean
[]	18/12/09 10:37:41				2.9Kb	2.76 Clean
[]	18/12/09 10:35:43				22.4Kb	-2.00 Clean
[]	18/12/09 10:23:29				3.6Kb	-4.81 Clean
[]	18/12/09 10:19:51				45.6Kb	-0.44 Clean
[]	18/12/09				4Kb	-4.81 Clean

After the first login, the main console will show the **Recent Messages** of incoming email in the system.

Status Bar










The **Status Bar** contains five services which is Jump to Message, Color Codes, Status, Mail Queues and Today's Total.

Jump to message

We can use the **Jump to message** service to locate messages using message ID. For example, the message ID is 1998E1350001.40D8E, if admin key-in the ID at the field provided at **Jump to message**, admin can retrieve the e-mail summary.

Color Codes

We are using **Color Codes** to distinguish clean, spam and virus e-mail from one to another.

Color Codes	
Bad	
Content/Infected	
Spam	
High Spam	
MCP	
High MCP	
Whitelisted	
Blacklisted	
Clean	

Explanation for each color:

Illustration 1: Color Codes box

1. Bad Content/Infected 

The e-mail contains spam and virus. E-mails that are catogerised as spam e-mail (e-mail with high SpamAssassin score, by default > 6.0) are blocked at MySpamGuard server and stored in the Quarantine folder.

2. Spam 

E-mails with low SpamAssassin scores are identified as spam and stored in Quarantine folder.

3. High Spam 

E-mails with higher SpamAssassin (by default score is > 10.0) scores are identified as High Spam and will be stored in the Quarantine folder.

4. MCP

Message Content Protection (MCP) allows you to write rules for scanning the text content of e-mail messages in order to trap messages that contain certain numbers of keywords and/or phrases that should not leave beyond your company into the internet. It could also be used to ban mails containing pornographic phrases and so on, without having to mess with Spam Actions or have custom spam rules.

5. High MCP

E-mails with a high number of MCP are blocked at MySpamGuard.

6. Whitelisted

All e-mails which are whitelisted are allowed passage from MySpamGuard server.

7. Blacklisted

All e-mails which are blacklisted are blocked at the MySpamGuard server and not released.

8. Clean

All the clean e-mails are color-coded in grey color. These e-mails have SpamAssassin's scores below the spam score.

Status

The Status box shows the current status of two main services running in MySpamGuard which is MailScanner and Postfix. It also shows the Load Average for the whole system.

Status		
MailScanner:	YES	5 children
Postfix:	YES	1 proc(s)
Load Average:	1.01	0.50 0.40

Illustration 2: Status box

Mail Queues

The Mail Queues box notifies of Inbound or Outbound e-mails. Inbound shows incoming e-mail and Outbound shows the outgoing e-mail.

Mail Queues	
Inbound:	0
Outbound:	0

Illustration 3: Mail Queues box

Today's Total

Total box shows a summary of the total incoming e-mails, e-mails that contains spam and virus and etc.

Today's Totals		
Processed:	206	2.1Mb
Clean:	173	84.0%
Viruses:	0	0.0%
Top Virus:	None	
Blocked files:	0	0.0%
Others:	0	0.0%
Spam:	14	6.8%
High Scoring Spam:	19	9.2%
MCP:	0	0.0%
High Scoring MCP:	0	0.0%

Illustration 4: Today's Total box

Menu Bar

The Main Menu Bar provides a list of options to display recent messages, white/black list, quarantined e-mails, reports, user management tools and logout menu.

Recent Messages	Lists	Quarantine	Reports	Tools/Links	Logout
-----------------	-------	------------	---------	-------------	--------

Illustration 5: Menu Bar

Recent Messages

After the first login, the first content displayed on the MySpamGuard Console are **Recent Messages**. It shows the last 50 messages on the system and periodically updates every 30 seconds.

Lists

Using the **Lists** service, e-mails or IP addresses can be placed as whitelisted or blacklisted by selecting the appropriate boxes.

Recent Messages	Lists	Quarantine	Reports	Tools/Links	Logout
-----------------	--------------	------------	---------	-------------	--------

Add to Whitelist/Blacklist

From:

To:

List: ☐ Whitelist ☐ Blacklist

Action:

Whitelist for admin			Blacklist for admin		
From	To	Action	From	To	Action
		Delete			Delete
		Delete			Delete
		Delete			Delete
					Delete
					Delete
					Delete
					Delete
					Delete
					Delete
					Delete

Illustration 6: Lists

Quarantine

Quarantine shows all the quarantine e-mails with low SpamAssassin score. All quarantined e-mail will be kept and grouped by its date.

Recent Messages	Lists	Quarantine	Reports	Tools/Links	Logout
Folder					
18/12/2009					
17/12/2009					
16/12/2009					
15/12/2009					
14/12/2009					
13/12/2009					

Illustration 7: Quarantine

Below is the Illustration of quarantine folder:

Recent Messages

Lists

Quarantine

Reports

Tools/Links

Logout

Displaying page 1 of 2 - Records 1 to 50 of 88

<<< < 1 2 > >>>

Folder: 18/12/2009

#	Date/Time (A/D)	From (A/D)	To (A/D)	Subject (A/D)	Size (A/D)	SA Score (A/D)	Statu
[]	18/12/09 23:55:19				23.6Kb	12.13	Spam
[]	18/12/09 22:18:28				27.5Kb	11.79	Spam
[]	18/12/09 16:24:28				3.1Kb	6.00	Spam
[]	18/12/09 16:03:04				2.1Kb	103.55	Spam B/L
[]	18/12/09 15:14:19				8.4Kb	6.75	Spam
[]	18/12/09 15:13:29				2.1Kb	103.55	Spam B/L
[]	18/12/09 15:06:59				3.4Kb	20.71	Spam
[]	18/12/09 14:59:39				2Kb	103.55	Spam B/L
[]	18/12/09 14:43:51				3.1Kb	9.96	Spam
[]	18/12/09 14:05:16				2.2Kb	6.00	Spam
[]	18/12/09 13:59:39				2.4Kb	7.56	Spam
[]	18/12/09 13:37:48				3.3Kb	13.22	Spam
[]	18/12/09 13:32:43				18.5Kb	15.49	Spam
[]	18/12/09 13:11:13				3.3Kb	13.90	Spam
[]	18/12/09 13:03:48				3.2Kb	9.09	Spam
[]	18/12/09 12:31:47				18Kb	14.09	Spam
[]	18/12/09 12:19:42				17.5Kb	13.99	Spam
[]	18/12/09 12:08:17				2.5Kb	10.60	Spam
[]	18/12/09 12:06:04				8.7Kb	7.52	Spam
[]	18/12/09 11:59:16				10.2Kb	8.68	Spam
[]	18/12/09 11:51:43				2.4Kb	10.60	Spam

Illustration 8: Quarantine folder

Reports

Administrators can generate reports or statistics for a certain period. A report can also use the preferred filter such as user e-mail address (sender or recipient), e-mail header or other filter provided in **Add Filter** section. The filter option we add in the Add Filter will be the parameter use to generate the report.

Aside from that, administrator can perform SA Learn update using service **Message Operations** in **Reports** section.

Recent Messages	Lists	Quarantine	Reports	Tools/Links	Logout
-----------------	-------	------------	----------------	-------------	--------

Active Filters

None

Add Filter

Date

is equal to

Load/Save Filter

None

Statistics (Filtered)

Oldest record: 04/10/07

Newest record: 21/12/09

Message count: 1,468,871

Reports

- [Message Listing](#)
- [Message Operations](#)
- [Total Messages by Date](#)
- [Top Mail Relays](#)
- [Top Viruses](#)
- [Virus Report](#)
- [Top Senders by Quantity](#)
- [Top Senders by Volume](#)
- [Top Recipients by Quantity](#)
- [Top Recipients by Volume](#)
- [Top Sender Domains by Quantity](#)
- [Top Sender Domains by Volume](#)
- [Top Recipient Domains by Quantity](#)
- [Top Recipient Domains by Volume](#)
- [SpamAssassin Score Distribution](#)
- [SpamAssassin Rule Hits](#)
- [MCP Score Distribution](#)
- [MCP Rule Hits](#)
- [Audit Log](#)

Illustration 9: Reports

In this example, a report on **Total Messages by Date** and **Top Senders by Quantity** for period from 15 December until 20 December 2009 is produced:

First, add period time in the **Add Filter**

Active Filters

Date is greater than '09/12/15' [Remove](#)

Add Filter

Date

is less than or equal to

09/12/20

Load/Save Filter

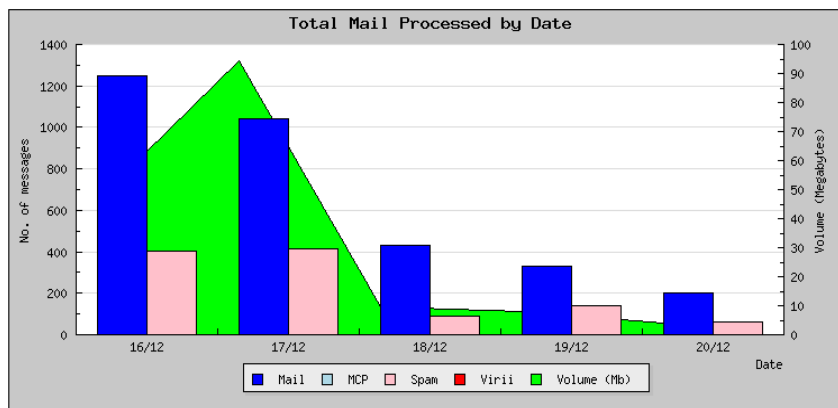
None

Illustration 10: Adding filter

You can see the total e-mail within period (period based on **Active Filter**) in the **Statistics (Filtered)**.

Active Filters	
Date is greater than '09/12/15'	Remove
Date is less than or equal to '09/12/20'	Remove
Add Filter	
Date	<input type="text"/>
is equal to	<input type="text"/>
<input type="button" value="Add"/>	
Load/Save Filter	
<input type="text"/>	<input type="button" value="Save"/>
None	<input type="button" value="Load"/> <input type="button" value="Save"/> <input type="button" value="Delete"/>
Statistics (Filtered)	
Oldest record:	16/12/09
Newest record:	20/12/09
Message count:	3,250

To generate report for Total Messages by Date, select Total Messages by Date in the Reports section. Reports will be shown in graph based from the period time used.



Date	Mail	Virus	%	Spam	%	MCP	%	Volume	Unknown Users	Can't Resolve	RBL
16/12	1,249	0	0.0	404	32.3	0	0.0	46.4Mb	0	0	0
17/12	1,040	0	0.0	414	39.8	0	0.0	94.2Mb	0	0	0
18/12	429	0	0.0	88	20.5	0	0.0	9.6Mb	0	0	0
19/12	331	0	0.0	141	42.6	0	0.0	7.8Mb	0	0	0
20/12	201	0	0.0	62	30.8	0	0.0	4Mb	0	0	0
Totals	3,250	0	0.0	1,109	34.1	0	0.0	162.1Mb	0	0	0

Illustration 11: Graph for Total Messages by Date

To generate report for Top Sender by Quantity, select **Top Sender by Quantity** in the Reports section. Reports will be shown in pie-chart form based from the period time used.

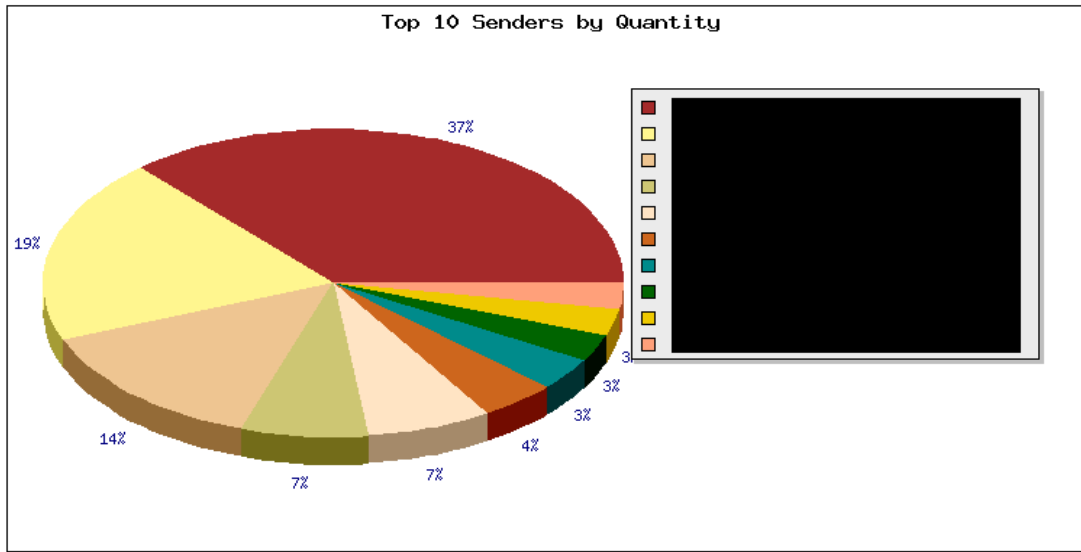


Illustration 12: Chart for Top Sender by Quantity

Tools/Links

In Tools/Links, administrator can perform few task in here:

1. Manage users such as adding new users and editing or deleting existing users under **User Management**
2. Updating package/rule such as SpamAssassin (spam scanner) and ClamAV (virus scanner)
3. Preview data (configuration) such as MailScanner and SpamAssassin

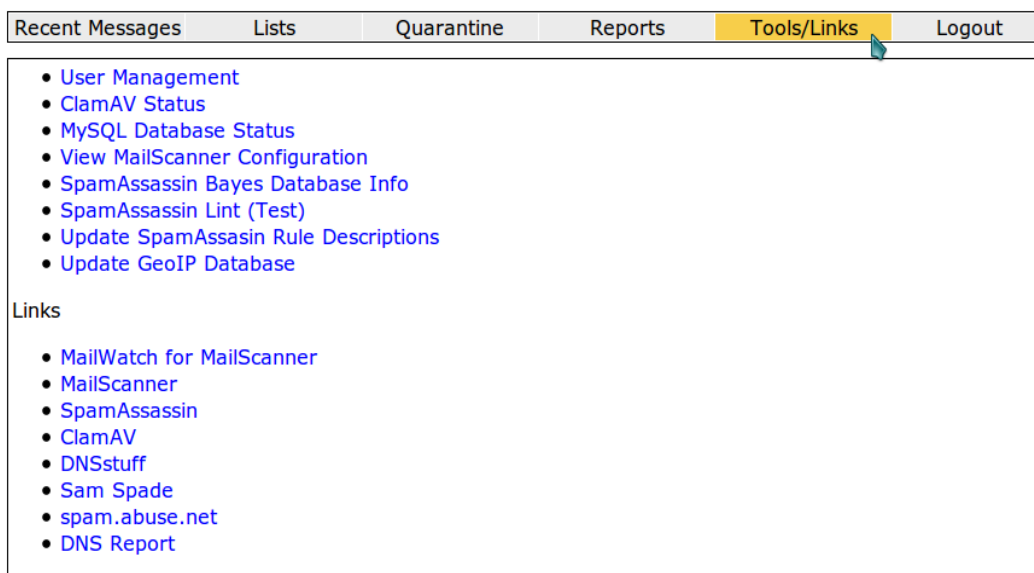


Illustration 13: Tools/Links

User Management

All user management can be done in MySpamGuard Console at Tools/Links under **User Management** section. Click at the User Management will show latest user and their role in the system.

User Management						
Username	Full Name	Type	Spam Check	Spam Score	High Spam Score	Actions
		Administrator	Y	0	0	Edit Delete Filters
		User	Y	0	0	Edit Delete Filters
		Administrator	Y	0	0	Edit Delete Filters
		Administrator	Y	0	0	Edit Delete Filters

[New User](#)

Illustration 14: User Management

Administrators have the privilege to perform actions as listed in the Actions such as editing, deleting or filtering for existing user, and aside from that, they also have the privilege to create new users for the system.

To create new user for the system, click at button **New User** under the User Management box.

New User	
Username:	<input type="text" value="ujian"/>
Name:	<input type="text" value="ujian"/>
Password:	<input type="password" value="●●●●●●●●"/>
User Type:	<input type="text" value="User"/> ▼
Quarantine Report:	<input type="checkbox"/> Send Daily Report?
Quarantine Report Recipient:	<input type="text"/> Override quarantine report recipient? (uses your username if blank)
Scan for Spam:	<input checked="" type="checkbox"/> Scan e-mail for Spam?
Spam Score:	<input type="text" value="0"/> 0=Use Default
High Spam Score:	<input type="text" value="0"/> 0=Use Default
Action:	<input type="button" value="Reset"/> <input type="button" value="Create"/>

Illustration 15: New User box

Fill in the field required such as **Username**, **Name** and **Password** for the new user. Administrators has to decide the user role/permission within the system. New roles can be added in the **User Type**.

Next, click on **Create** to create new user for the system.

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 -h* 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* at least once a month to download the latest spamassassin rules.