How To Install and Use Logwatch & Log Analyzer script on CentOS .

Author : Lalit Vohra

Categories : Linux Tools

Date : Apr 24, 2015

- Facebook
- Twitter
- Google+
- Gmail

Applications create what are called “log files” to keep track of activities taking place at any given time. These files, which are far from being simple text outputs, can be very complex to go through, especially if the server being managed is a busy one

When the time comes to refer to log files (e.g. in case of failure, loss of data etc.), making use of all the available help becomes vital. Being able to quickly understand (parse) what they can tell regarding the past events and *analyzing* what exactly has happened then becomes exceptionally important for coming up with a solution.

In this article we will talk about **Logwatch**: a very powerful log parser and analyzer which can make any dedicated system administrator’s life a little bit easier when tackling application related tasks and issues.

Log Files

Administrators even today rely on logs. These application-generated files play a decisive role in tracking back and understanding what has happened in the past [at a given time] for the purposes of full / partial data recovery (i.e. from transaction logs), performance or strategy related analyses (e.g. from server) or amendments for the future (e.g. from access logs).

Simply put, log files will consist of actions and events taking place within a given time range.

A good log file should be as detailed as possible in order to help the administrator, who have the responsibility of maintaining the system, find the exact information needed for a certain purpose. Because of this very reason, log files are usually NOT concise and they contain loads of repetitions and loads of (mostly) redundant entries which need thorough analyses and filtering to make sense to a human.

This is where Logwatch, a computer application designed for this job, comes into play.

Enter Logwatch

Log management is an area consisting mostly of search, log rotation / retention and reporting. Logwatch is an application that helps with simple log management by daily analyzing and reporting a short digest from activities taking place on your machine.

Reports created by Logwatch are categorised by *services* (i.e. applications) running on your system, which can be configured to consist of the ones you like or all of them together by modifying its relatively simple configuration file. Furthermore, Logwatch allows the creation of custom analysis scripts for specific needs.

Installing Logwatch

Please note: Logwatch is a harmless application which should not interfere with your current services or workload. However, as always, it is recommended that you first try it on a new system and make sure to take backups.

On CentOS / RHEL

It is very simple to have Logwatch installed on a RHEL based system (e.g. CentOS). As it is an application consisting of various Perl scripts, certain related dependencies are required. Since we are going to be using **yum** package manager, this will be automatically taken care of. Unless you have mailx installed already, Logwatch will download it for you during the process as well.

To install Logwatch on CentOS / RHEL, run the following:

#yum install -y logwatch

1

2

On Ubuntu / Debian

Getting Logwatch for Debian based systems (e.g. Ubuntu) is very similar to the process explained above, apart from the differences in package managers (aptitude v. yum).

To install Logwatch on Ubuntu / Debian, run the following:

#apt-get install -y logwatch Configuring Logwatch

#apt-get install -y logwatch

1

2 Configuring Logwatch

3

Although its settings can be overridden during each run manually, in general, you will want to have Logwatch running daily, using common configuration.

Setting The Common Configurations of Logwatch

The default configuration file for Logwatch is located at:

/usr/share/logwatch/default.conf/logwatch.conf

1

Let’s open up this file using the nano text editor in order to modify its contents:

vim /usr/share/logwatch/default.conf/logwatch.conf

Upon running the command above, you will be met with a long list of variables the application uses each time it runs, whether automatically or manually.

In order to begin using it, we will need to make a few changes to these defaults.

> **Please remember in the future, you might want to come back to modify certain settings defined here. All services (applications) that are analyzed by Logwatch are listed on this file, as explained above. As you install or remove applications from your virtual server, you can continue to receive reports on *all* of them or *some* of them by changing the settings here (see below*).**

Please note: You will need to use your arrow keys to go up or down the lines when you will be making the following changes on the document. Once you are done going through the changes (items 1 – 6), you will need to press CTRL+X and then confirm with Y to save and close. Changes will come into effect automatically the next time logwatch runs.

1. The e-mail address to which daily digest (reports) are sent:

MailTo = root

Replace root with your email address.

Example: MailTo = lalitvohra04@gmail.com

2. The e-mail address *from* which these reports originate:

MailFrom = Logwatch

1

You might wish to replace Logwatch with your own again.

Example: MailFrom = root@mydomain.com

3. Setting the *range* for the reports:

Range

1

2 = yesterday

You have options of receiving reports for *All* (all available since the beginning), *Today* (just today) or *Yesterday* (just yesterday).

Example: Range = Today

4. Setting the reports’ detail:

Detail = Low

1

You can modify the reports' detail here. Options are: *Low*, *Medium* and *High*.

Example: Detail = Medium

5. Setting services (applications) to be analysed:

By default, Logwatch covers a really wide range of services. If you would like to see a full list, you can query the contents of the file scripts/services located at /usr/share/logwatch/.

Example: ls -l /usr/share/logwatch/scripts/service

Service = All

1

You can choose to receive reports for all services or some specific ones.

For all services, keep the line as: Service = All

If you wish to receive reports for specific ones, modify it similar to the following example, listing each service on a new line (e.g. Service = [name]).

Example:

Service = sendmail

1

Service = http

1

Service = identd

1

Service = sshd2

1

Service = sudo

1

6. Disabling daily reports:

DailyRepoty = No

1

If you do **not** wish to have daily repots generated, you should uncomment this line.

Example: DailyReport = No instead of # DailyReport = No

And that’s it! After making these changes, you will receive daily reports based on log files from your server **automatically**.To learn more about Logwatch, and creating custom services to receive reports on, you can visit its full documentation by clicking.

Running Logwatch Manually

It should be mentioned that you have the option to run Logwatch manually whenever you need through the command line.

Here are the available options [from the documentation]:

logwatch [--detail level

1

2] [--logfile log-file-group] [--service

service-name] [--print]

[--mailto

1

address] [--archives] [--range range] [--

2 debug level] [--save

3 file-name]

[--logdir

1

2 directory] [--hostname hostname] [--

splithosts] [--multiemail]

3

[--output output-]

1

2	[type] [--numeric] [--no-oldfiles-log]
3	[--version] [--help|--usage]

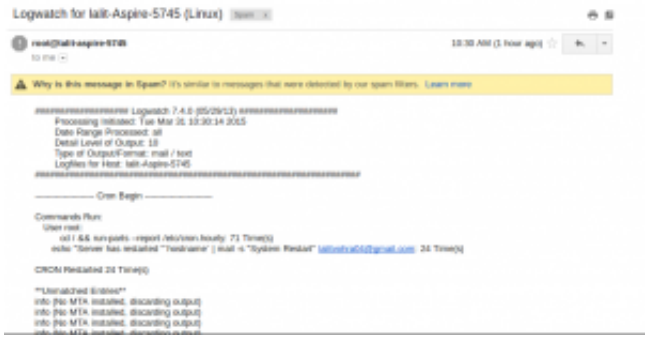
Unless you specify an option, it will be read from the configuration file.

Example:

#logwatch --detail Low --mailto lalitvohra04@gmail.com --service sshd --range today.

And here is what a Logwatch report can look like:

Now we will see the output:



This type of mail alert you will get.

1

1

Lalit Vohra

- Facebook
- Twitter
- Google+
- Gmail