**The syslog-ng And Log Analyzer Guide**

**BY**

**Mukesh B. Mahale**

**Special Thanks**

**Rupesh J. Shewalkar**

**Table of Contents**

**1. Introduction to syslog-ng and Log Analyzer………………… 02**

**2. Installing syslog-ng ……………………………….....................04**

**3. Installing Log Analyzer………………………………………..10**

**4. How to Add New client to syslog-ng Server…………………15**

**Chapter 1. Introduction to syslog-ng and Log analyzer**

**1.1. What syslog-ng is?**

The syslog-ng application is a flexible and highly scalable system logging application that enables you to send the log messages of your hosts to remote servers. The logs of different

servers can be collected and stored centrally on dedicated log servers. Transferring log messages

using the TCP protocol ensures that no messages are lost.

**1.2 Which are features of Syslog-ng?**

The Syslog-ng Features are as follow:

* *Reliable log transfer*
* *Secure logging using SSL/TLS*
* *Disk-based message buffering*
* *Direct database access*:
* *Heterogeneous environments*
* *Filter and classify*
* *IPv4 and IPv6 support*





**1.3** **The structure of a log message**

This section describes the format of a syslog message, according to RFC 3164

(http://www.ietf.org/rfc/rfc3164.txt).A syslog message consists of the following parts:

■ *PRI*

■ *HEADER*

■ *MSG*

The total message must be shorter than 1024 bytes.

The following is a sample syslog message: *<133>Feb 25 14:09:07 webserver syslogd: restart*.

The message corresponds to the following format: *<priority>timestamp hostname application:*

*message*.

**1.4 What is Log Analyzer ?**

The **LogAnalyzer project provides an easy to use but powerful front end for searching,**

**reviewing and analyzing network event data, including syslog, windows event log and many**

**other event sources.** It focusses on the user-interface side of this project, so the data itself needs

to be gathered by another program, for example the stock syslogd, rsyslog (often the distro's

default syslogd), WinSyslog or MonitorWare Agent. LogAnalyzer works equally well on Linux

and Windows. It is a free, GPLed open source application written mostly in php. Data can be

obtained from databases but also from plain text files, for example those that are written by the

syslogd.

**Chapter 2. Installing syslog-ng**

This chapter explains how to install syslog-ng on the supported platforms using the RPM files.

**2.1** **What are the required packages of Syslog-ng?**

Following are the required RPM for Syslog-ng:

For Server side: syslog-ng-3.0.4-1.rhel5.i386.rpm

For Client side: syslog-ng-client-3.0.4-1.rhel5.i386.rpm

For Relay side: syslog-ng-relay-3.0.4.1.rhel5.i386.rpm

Note:-[You may use same RPM syslog-ng-3.0.4-1.rhel5.i386.rpm for server, client & relay

configuration, only configuration different]

**2.2 Downloading Site:-**

* http://www.balabit.com/

**2.3 Server Side Installation:**



*Figure 2.1. Server-mode operation*

In server mode, syslog-ng acts as a central log-collecting server. It receives messages from

syslog-ng clients and relays over the network, and stores them locally in files, or passes them to

other applications, e.g., log analyzers

**Install Server RPM**

[root@syslogserver ~] rpm -ivh syslog-ng-3.0.4-1.rhel5.i386.rpm

Now we will edit the syslog-ng configuration file. I have included my configuration file with

comments explaining what and why it is configured that way.

[root@syslogserver ~]# vi /opt/syslog-ng/etc/syslog-ng.conf

Syslog-ng configuration contain following things:

1. Global options

2. Source

3. Filter

4. Destination

5. Log Path

**1. Global options:**

* **ts\_format(iso):-**Specifies the timestamp format used when syslog-ng itself formats a

timestamp and nothing else specifies a format.

* **time\_sleep(30):-**The time to wait in milliseconds between each invocation of the poll()

iteration.

* **time\_reap(30):-**The time to wait in seconds before an idle destination file is closed.
* **mark\_freq(30):-**The number of seconds between two MARK messages.

MARK messages are generated when there was no message traffic to inform the receiver that the connection is still alive.

* **dns\_cache(yes):-**Enable or disable DNS cache usage.
* **use\_fqdn(no):-**Add Fully Qualified Domain Name instead of short hostname
* **keep\_hostname(no):-**Enable or disable checking whether the hostname contains valid

characters.

* **chain\_hostnames(no):-**Enable or disable the chained hostname format.
* **use\_dns(yes):-**Enable or disable DNS usage.
* **dns\_cache\_size(250000):-**Number of hostnames in the DNS cache.
* **dns\_cache\_expire(300):-**Number of seconds while a successful lookup is cached.
* **dns\_cache\_expire\_failed(300)**:-Number of seconds while a failed lookup is cached.
* **stats\_freq(3600):-**The period between two STATS messages in seconds.STATS are log messages sent by syslog-ng, containing statistics about dropped log messages.

**2. Source:-**

Example of source defined for Linux operating system

source s\_demo {

internal();

udp(ip(0.0.0.0) port(514));

unix-stream("/dev/log"); };

The following source statement collects the following log messages:

■ *internal()*: Messages generated by syslog-ng.

■ *udp(ip(0.0.0.0) port(514))*: Messages arriving to the *514/UDP* port of any interface of the

host.

■ *unix-stream("/dev/log");*: Messages arriving to the */dev/log* socket.

**3.Filter :-**

Filters perform log routing within syslog-ng: a message passes the filter if the filter expression is true for

the particular message. If a log statement includes filters, the messages are sent to the destinations only

if they pass all filters of the log path. For example, a filter can select only the messages originating from a

particular host. Complex filters can be created using filter functions and logical boolean expressions.

Example of Filter

filter demo\_filter { host("example") and match("deny"); };

**4. Destinations:-**

A destination is where a log message is sent if the filtering rules match. Similarly to sources,

destinations consist of one or more drivers, each defining where and how messages are sent.

Example of Destinations

destination d\_demo\_tcp { tcp("10.1.2.3" port(1999)); };

**5. Log Path:-**

Log paths determine what happens with the incoming log messages. Messages coming from the

sources listed in the log statement and matching all the filters are sent to the listed destinations.

Example of Path Logs

source s\_localhost { tcp(ip(127.0.0.1) port(1999) ); };

destination d\_tcp { tcp("10.1.2.3" port(1999); localport(999)); };

log { source(s\_localhost); destination(d\_tcp); };

**Server configuration File for text based compatible to log analyzer**

@version: 3.0

#Default configuration file for syslog-ng.

############# BCCA CENTER #############################################

options {

ts\_format(iso);

time\_sleep(30);

time\_reap(30);

mark\_freq(30);

use\_fqdn(no);

keep\_hostname(no);

chain\_hostnames(no);

stats\_freq(3600);

create\_dirs(yes);

perm(0644);

dir\_perm(0666);

};

################## SOURCES ###########################################

source s\_local {

internal();

unix-stream("/dev/log");

file("/proc/kmsg" program\_override("kernel: "));

syslog(ip(31.101.1.8) port(2010) max-connections(300));

};

##################DESTINATIONS #############################################

destination d\_messages { file("/var/log/messages" ); };

destination d\_client { file("/var/log/text" template("$MSG\n")); };

destination d\_syslog { file("/var/log/systest" template("<$PRI>1 $S\_ISODATE $HOST

$PROGRAM $PID - - $MSG\n") ); };

############ FILTER #########################################

filter f\_apache\_access {message("GET|POST");};

##################### LOG PATH #########################################

log { source (s\_local); destination (d\_messages);};

log { source(s\_local); destination(d\_syslog); };

Restart the syslog-ng server (which also creates the database tables, indexes, etc.)

[root@syslogserver ~]# /etc/init.d/syslog-ng restart

**2**.**4 Client Side Installation**:-



Setup client machines to send data to the syslog server

Install Server RPM

[root@syslogclient ~]# rpm -i syslog-ng-client-3.0.4-1.rhel5.i386.rpm

The client configuration file has similar concepts/commands as the server config.

Be sure to configure your clients in a way that won't overload your syslog-ng server

(processingand/or database size).

Client configuration File for text based compatible to log analyzer

@version: 3.0

#Default configuration files for syslog-ng.

#

# For a description of syslog-ng configuration file directives, please read

# the syslog-ng Administrator's guide at:

#

# <http://www.balabit.com/dl/html/syslog-ng-admin-guide_en.html/bk01-toc.html>

######################## GLOBAL OPTIONS ########################

options {

log\_fifo\_size(4096);

keep\_hostname(yes);

chain\_hostnames(no);

bad\_hostname("gconfd");

ts\_format(iso);

time\_sleep(30);

mark\_freq(30);

};

###################### SOURCES ######################################

source s\_local {

internal();

unix-stream("/dev/log");

file("/proc/kmsg" program\_override("kernel: "));

syslog(ip(31.101.1.6) port(2010) max-connections(300));

};

source s\_all\_logs {

file("/var/log/vsftpd.log" follow\_freq(30));

#file("/var/log/mysqld.log" follow\_freq(30));

};

source s\_httpd\_error {

file("/var/log/httpd/agni.hbni.ac.in-error\_log" flags(no-parse) follow\_freq(30));

};

source s\_httpd\_access {

file("/var/log/httpd/agni.hbni.ac.in-access\_log" flags(no-parse) follow\_freq(30));

};

################## DESTINATION ##########################

destination d\_messages { file("/var/log/messages"); };

destination d\_syslog\_tcp {

syslog("31.101.1.8"transport("tcp") port(2010) template("$MSG\n"));};

destination d\_httpd\_error {

syslog("31.101.1.8" port(2010) template("$MSG-File ERROR\_LOG\n") ); };

destination d\_httpd\_access {

syslog("31.101.1.8" port(2010)template("$MSG")); };

############## LOG PATH ########################

log { source(s\_local); destination(d\_messages); };

log { source(s\_local); source(s\_all\_logs); destination(d\_syslog\_tcp); };

log { source(s\_httpd\_access); destination(d\_httpd\_access); };

log { source(s\_httpd\_error); destination(d\_httpd\_error); };

**Chapter 3. Installing Log Analyzer**

**Steps to Do**

**To install LogAnalyzer, you need:**

Apache or IIS Webserver

PHP5

Optionally, you may need:

MySQL Database

For obvious reasons, you also need some syslog data. Any standard syslogd will do. From a

feature and stability point of view, we recommend either one of these (which we also wrote ;) ):

WinSyslog (for the Windows platform)

rsyslog /Syslog-ng(for the Linux/Unix platform)

Both of them are also capable of writing to databases. Rsyslog is a drop-in replacement for stock

syslogd and also \*is\* the stock syslogd on some platforms (e.g. Fedora 8 and above).

**Step 1 - Download Software**

For obvious reasons, you need to download LogAnalyzer. Here, I assume that you use a

distribution tarball.

Load the most recent build from http://loganalyzer.adiscon.comdownloads. Extract the software

with "tar xzf -nameOfDownloadSet-". This will create a new subdirectory LogAnalyzer-version

in the current working directory. CD into that.

**Step 2**

Upload all files from the loganalyzer/src/ folder to you webserver. The other files are not needed

on the webserver.

**Step 3**

If your webserver has write access to the LogAnalyzer folder, you can skip the following step:

Upload the scripts configure.sh and secure.sh from the contrib folder to your webserver, into the

same folder where you uploaded the other LogAnalyzer files into. Then set the execution flag to

them (chmod +x configure.sh secure.sh).

Now run ./configure.sh, this will create a blank config.php, and will also set write access to everyone to it.

You can of course do this manually if you want.

**Step 4**

Now open your LogAnalyzer installation in your favourite webbrowser, you will see an error,

and you will be pointed to the installation script. The install script will guide you through the

LogAnalyzer installation, just follow the instructions.

**Step 4.1**

Prerequisites Beginning of installation / welcome site. This is the first page of the installation. It

just tells you, that before installing, some file permission have to be checked. Simply click

"Next" to start the process.

**Step 4.2**

Verify the file permissions Here you will see, if the config.php can be written or not. If it cannot

be written, you have to repeat the complete Step 2.

**Step 4.3**

Basic Configuration

You can set several basic options here.

· Number of syslog messages per page = 50 (default)

This is the number of syslog messages displayed on each page. You can increase the

value (makes LogAnalyzer slower) or decrease the value (makes it faster).

· Message character limit for the main view = 80 (default)

Set the number of characters per message which will be shown in the last column of the

main view. Full messages can be reviewed by hovering the mouse over it. **Many folks**

**prefer to use a setting of "0", which means complete messages will be displayed**<

· Show message details popup (default yes) = yes (default). Note that many people find the

popups intrusive and prefer to disable them. Use "no" in this case.

**Step 4.4**

Not implemented yet, some real magic may happen here at a later stage ;-) - for now, just skip it.

**Step 4.5**

Create the first source for syslog messages. This is the most important step. Here, you will

configure your first data source, which holds all your syslog data.

Mainly, you have to choose a "Name of the Source" and a "Source Type". The name will be

displayed later in a drop-down menu with which you choose your active syslog source. The

"Source Type" can be a file, a MySQL database or the PHP PDO which supports different

database types like mssql, PostgreSQL, odbc, oracle or even ibm db2.

**If you choose the diskfile, you have to provide the following information:**

· Logline Type = Syslog / Rsyslog (default) or Adiscon WinSyslog

This tells LogAnalyzer, how the lines look like. This is necessary for show the log

messages properly.

· Syslog File = /var/log/syslog (default)

This is the position of the logfile in your file system.

**If you choose MySQL native as data source, following information is needed:**

· Table Type = monitorware (default)

This is the table layout. Currently, you can use "monitorware" or "syslogng". For more

details see "Note on MySQL Databases" below.

· Database Host = localhost (default)

This is the host, where the database is located. By default this is localhost. You can

specify any other host if necessary.

· Database Name = loganalyzer (default)

The name of the database you want to use.

· Database Tablename = systemevents (default)

This is the name of the table in which the data is stored. The default tablename

corresponds to the tables created with the MonitorWare Line of products.

· Database User = user (default)

The username for the database.

· Database Password = not set by default

The password for the username.

· Enable Row Counting = No (default)

If configured to "Yes", the amount of rows in the table will be counted with every query,

giving you the total records for your search, though having a lot of impact on your system

when using a very large database. If configured to "No", the rows will not be counted,

providing you a lot more performance.

**If you choose Database (PDO), the following has to be defined:**

· Database Storage Engine = MySQL Server (default)

Choose the engine of the database you are using. These databases are supported: MySQL

Server, Microsoft SQL Server, ODBC Database Connection, PostgreSQL, Oracle Call

Interface, IBM DB2, Firebird/Interbase 6, IBM Informix Dynamic Server, SQLite 2.

· Table Type = monitorware (default)

This is the table layout. Currently, you can use "monitorware" or "syslogng". For more

details see "Note on MySQL Databases" below.

· Database Host = localhost (default)

This is the host, where the database is located. By default this is localhost. You can

specify any other host if necessary.

· Database Name = loganalyzer (default)

The name of the database you want to use.

· Database Tablename = systemevents (default)

This is the name of the table in which the data is stored. The default tablename

corresponds to the tables created with the MonitorWare Line of products.

· Database User = user (default)

The username for the database.

· Database Password = not set by default

The password for the username.

· Enable Row Counting = No (default)

If configured to "Yes", the amount of rows in the table will be counted with every query,

giving you the total records for your search, though having a lot of impact on your system

when using a very large database. If configured to "No", the rows will not be counted,

providing you a lot more performance.

**Step 4.6**

Finish :)

**Step 5**

If everything went right, you should see syslog messages already in your LogAnalyzer

installation. You can now remove the install.php script now.

**Note on Accesing Files**

In most environments the webserver has only access to the web directory. If you want to read

files e.g. from /var/log/ you have to grant the necessary permisson to your webserver.

Of course, you always need to make sure that the user the web server runs under also has the

correct file permissions. Be careful when doing this, you may create a security vulnerability by

granting too much to too many users.

**Note on MySQL Databases**

LogAnalyzer does support using a MySQL database as syslog source. LogAnalyzer supports

Adiscon's MonitorWare database schema. The schema used by php-syslog-ng is also partly

supported. That schema, however, is somewhat inefficient in that it stores facility and severity

codes as textual values. We do not currently convert these values back to their native format and

consequently facility and severity cannot be taken from a php-syslog-ng database.

Required Setting in Log Analyzer during adding source



Note:-[you must use message parser for apache log it will parse log in web field view, available

parser in Log Analyzer are: 1.apache2 for combined log format of apache & 2. apache2common

for common log format of apache]

**Chapter 4. How to Add New client To syslog-ng Server**

**Step:1**

Install Server RPM

[root@syslogclient ~]# rpm -i syslog-ng-client-3.0.4-1.rhel5.i386.rpm

**Step:2**

Follow above client configuration file.

**Step:3**

Add host on server site in /etc/hosts file

Example

[root@syslogserver~]#vi /etc/hosts

# Do not remove the following line, or various programs

# that require network functionality will fail.

127.0.0.1 localhost.localdomain localhost

31.101.1.8 icinga.hbni.ac.in icinga

31.101.16.123 windows.hbni.ac.in windows

31.101.1.1 medha.hbni.ac.in medha

31.101.1.6 agni.hbni.ac.in agni

31.101.1.7 pathshala.hbni.ac.in pathshala

**Step:4**

Add **log rotation** of new client to **/usr/local/script/logratation.sh** & **/etc/logrotate.d/syslog-ng** on **server** site.

**Step:5**

Firewall Policy:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **RULE** | **ACTION** | **SOURCE** | **DEST** | **PROTO** | **DEST-PORT** |
|  |  |  |  |  |  |
| CLIENT : Send to Server | ACCEPT | $FW | 31.101.1.8 | tcp | 2010 |
| SERVER : Recieve from Client | ACCEPT | Agni | $FW | tcp | 2010 |
|  |  |  |  |  |  |

**IPtables**

Rule for Client :

$IPTABLES -t filter -A OUTPUT -p tcp -d 31.101.1.8--dport 2010 -j ACCEPT

Rules for Server :

$IPTABLES -t filter -A INPUT -p tcp -s Agni --dport 2010 -j ACCEPT