**How to Install & Configure LogAnalyzer with Rsyslog On CentOS 7 / RHEL 7 /Ubuntu**

**Environment:**

Lab Setup:

**we will use  Centos 7 and Ubuntu 21.04 LTS, Centos 7 act as rsyslog server with LogAnalyzer, and Ubuntu act as rsyslog client**.

**Rsyslog Server :**

OS: CentOS 7  
IP address: 10.200.6.3

**Rsyslog Client Server:**

OS: ubuntu 21.04 LTS  
IP Address: 192.168.88.161

**1./ Install Prerequisites**

– In order for LogAnalyzer to function correctly, there are a number of prerequisite packages that need to be installed on our system.

– Install Httpd e php packages:

Login as a root user

sudo -i

yum install httpd php php-mysql wget

– Enable at boot and start Httpd

 systemctl enable httpd && systemctl start httpd

 chkconfig mysqld on && chkconfig httpd on

**OR**

After installing all packages start all services using following commands.

# service httpd start

# service mysqld start

# chkconfig httpd on

# chkconfig mysqld on

– If the **firewalld** is installed, you have to allow the http protocol :

$ firewall-cmd --permanent --add-service=http

$ firewall-cmd --reload

– Install mariadb server and rsyslog-mysql package:

yum install mariadb-server -y rsyslog-mysql rsyslog

**Only Rsyslog Package installed by default on Centos /Ubuntu**

After installing start rsyslog service and make sure syslog is stopped on server.

# service syslog stop

# chkconfig syslog off

# service rsyslog start

# chkconfig rsyslog on

– Enable at boot and start mariadb server:

systemctl enable mariadb && systemctl start mariadb

So, To setup a root password and secure mariadb server, please follow

https://mariadb.com/kb/en/mysql\_secure\_installation/

**2./ Configure RSYSLOG Database**

– Import the default database scheme offered by RSYSLOG using the below command:

# mysql -u root -p < /usr/share/doc/rsyslog-7.4.7/mysql-createDB.sql

- Create a user to access the Syslog database:

# mysql -u root -p

MariaDB [(none)]> GRANT ALL ON Syslog.\* TO 'rsyslog'@'localhost' IDENTIFIED BY 'Password';

MariaDB [(none)]> FLUSH PRIVILEGES;

MariaDB [(none)]> exit

# sudo cp /etc/rsyslog.conf /etc/rsyslog.conf.org

# sudo vi /etc/rsyslog.conf

- Find and uncomment the following lines to make your server to listen on the udp and tcp ports.

$ModLoad imudp

$UDPServerRun 514

$ModLoad imtcp

$InputTCPServerRun 514

- Add the following lines to create a new forwarding rule and a load the mysql module:

# Load the MySQL Module

module(load="ommysql")

**#\*.\* :ommysql:127.0.0.1,Syslog\_Database,syslog\_user,password**

\*.\* :ommysql:127.0.0.1,Syslog,rsyslog,Password

**"Altervative Options"**

**Create a New file Syslog.conf into rsyslog.d**

**nano /etc/rsyslog.d/Syslog.conf**

**#Add the following lines to create a new forwarding rule and a load the mysql,UDP & TCP modules**

**$ModLoad imudp**

**$UDPServerRun 514**

**$ModLoad imtcp**

**$InputTCPServerRun 514**

**# Load the MySQL Module**

**$ModLoad ommysql**

**\*.\* :ommysql:127.0.0.1,Syslog,rsyslog,Password**

**$template TmplAuth, "/var/log/%HOSTNAME%/%PROGRAMNAME%.log"**

**authpriv.\*   ?TmplAuth**

**\*.info,mail.none,authpriv.none,cron.none   ?TmplMsg**

**NOTE:Template settings are optional**

- Save and restart the rsyslog service

systemctl restart rsyslog

**3./ Install LogAnalyzer**

- Download LogAnalyzer

# VERSION=4.1.10

 cd /temp/

# sudo wget http://download.adiscon.com/loganalyzer/loganalyzer-4.1.10.tar.gz

# sudo tar -xzvf /tmp/loganalyzer-4.1.10.tar.gz

- Create the LogAnalyzer Directory under the apache web directory:

# sudo mkdir /var/www/html/loganalyzer

- Copy the installation files into loganalyzer directory using the following commands:

# sudo cp -r /tmp/loganalyzer-4.1.10/src/\* /var/www/html/loganalyzer

# sudo cp /tmp/loganalyzer-4.1.10/contrib/configure.sh /var/www/html/loganalyzer

**You may use only**

mv loganalyzer-4.1.10/src /var/www/html/loganalyzer

- Let's create a blank configuration file named config.php in loganalyzer directory and setup write permission to apache user using the following commands:

cd /var/www/html/loganalyzer

bash configure.sh

touch config.php

chmod 777 config.php

chcon -h -t httpd\_sys\_script\_rw\_t config.php

chown www-data:www-data config.php

- If the **firewalld** is installed, Allow the traffic to your server by executing the following commands:

# sudo firewall-cmd --add-port=514/{tcp,udp} --permanent

# sudo firewall-cmd --add-service=http --permanent

# sudo firewall-cmd --reload

**4./ start LogAnalyzer web installer**

After completing above steps open following url in your favorite web browser to start LogAnalyzer web installer.

http://localhost/loganalyzer

 NOTE:SELinux should be disabled

1. editing the config file, Open the /etc/selinux/config file (in some systems, the /etc/sysconfig/selinux file).
2. Change the line SELINUX=enforcing to SELINUX=permissive .
3. Save and close the file.
4. Reboot your system.

**Open Access in Firewall**

If you are using iptables to protect your system, then you need to add following rule to open port

# iptables -A INPUT -m state --state NEW -m udp -p udp --dport 514 -j ACCEPT

**Configure Rsyslog on Client Nodes**

After configuring Rsyslog centralized server, lets configure clients system to send there logs to central Rsyslog server. Login to each client nodes and add following line at end of the file

 # vim /etc/rsyslog.conf

add below line, change hostname or ip with your central Rsyslog systems ip/hostname.

\*.\*   @192.168.88.152:514

[or]

\*.\*   @logserver.example.com:514

and restart rsyslog service using following command.

# service rsyslog restart

And your centralized logging server setup has been completed successfully

If the new port was already configured in /etc/rsyslog.conf, restart rsyslog now for the change to take effect:

~]# service rsyslog restart

**Tshoot**

Problem :  
“Could not find the configured table, maybe misspelled or the table names are case sensitive”

Solution :  
edit the file config.php and change this :  
$CFG[‘Sources’][‘Source1’][‘DBTableName’] = ‘systemevents’;

TO

$CFG[‘Sources’][‘Source1’][‘DBTableName’] = ‘SystemEvents’;

and update the database :  
mysql -uuser -p  
mysql> update logcon\_sources set DBTableName =’SystemEvents’ where ID=1;  
Query OK, 1 row affected (0.00 sec)  
Rows matched: 1 Changed: 1 Warnings: 0