## <http://www.slsmk.com/setup-syslog-with-loganalyzer-on-ubuntu-server/>

## Setup Syslog with LogAnalyzer on Ubuntu Server

This article will cover:  
1) Setting up a syslog server to log messages from local and remote sources.  
2) Setup a GUI front end showing syslog items.

I’ve done this on both Ubuntu Server 10.04 and 12.04.

1. Get some items loaded from the repository.

# *apt-get install build-essential apache2 php5 php5-gd libapache2-mod-php5 mysql-server php5-mysql rsyslog*

1. Edit */etc/rsyslog.conf* and uncomment or add the following. This will set the server to accept inbound syslog messages on UDP port 514.

*# provides UDP syslog reception*

*$ModLoad imudp*

*$UDPServerRun 514*

1. Since the log analyzer runs on php, we need to tell apache how to handle php pages. Edit */etc/apache2/apache2.conf* and add in the following item underneath “DefaultType None”

*DefaultType text/plain*

*Addtype application/x-httpd-php .php*

Note: If this step is not done properly, you will get a message when loading the syslog web page prompting you to save the file instead of Apache displaying the file.

Note: Restart the web server after you made configuration change like: # */etc/init.d/apache2 restart*.

**On to the LogAnalyzer**.  
1. Download the latest log analyzer from the adiscon web site at http://loganalyzer.adiscon.com/downloads

cd /opt

wget http://download.adiscon.com/loganalyzer/loganalyzer-3.6.2.tar.gz

2. Unzip and extract the file.

gunzip loganalyzer-3.6.2.tar.gz

tar -xvf loganalyzer-3.6.2.tar

1. Copy the LogAnalyzer /src/ folder to the Apache www root or subfolder, copy the install script, make executable, and run the install scripts. It’s important to run the configure script from the same directory that will hold the syslog php files.

*mkdir /var/www/syslog*

*cp -r /opt/loganalyzer-3.6.2/src/\* /var/www/syslog*

*cp -r /opt/loganalyzer-3.6.2/contrib/\*.sh /var/www/syslog*

*chmod +x /var/www/syslog/\*.sh*

*cd /var/www/syslog/*

*./configure.sh*

1. Grant Apache access to syslog.

usermod -G adm www-data

Use a web browser to hit the new web service at [*http://SERVERNAME/syslog/index.php*](http://SERVERNAME/syslog/index.php) (Ex: <http://localhost/syslog/index.php>). The page will show a message stating the service is not configured. Follow the steps to setup your syslog front end.

## Go to <http://140.111.74.38/blog/post/2/632> to see the detailed information about how to initialize LogAnalyzer.