Nagios Log Server – Monitoring A New Log Source

Nagios®

The Industry Standard in IT Infrastructure Monitoring

Purpose

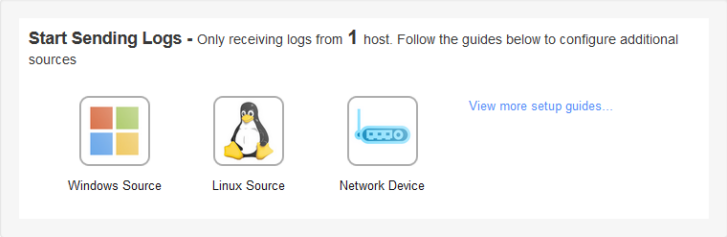
This document describes how to setup Nagios Log Server to monitor a new log source.

Target Audience

This document is intended for use by Nagios Log Server Administrators and users to setup Nagios Log Server to receive logs from a source.

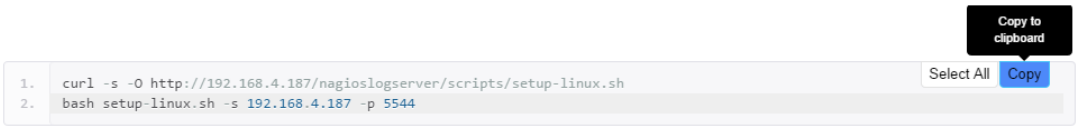
Navigate

Once you start Nagios Log Server after installation and configure the administrator account for the first time you will see a message on the **Home** page that tells you are receiving logs from 1 host (which is 127.0.0.1):



Multiple types of sources can be used, but for this documentation we will be using a Linux log source as an example by clicking on the **'Linux Source'** button above or by using the + **Log Source** button on the Nagios Log Server navigation bar.

Once you get to the Linux Source Setup page it will show you a codeblock with the `setup-linux.sh` script which will automatically configure rsyslog with your Nagios Log Server.



The path the script is located in your Nagios Log Server is here:

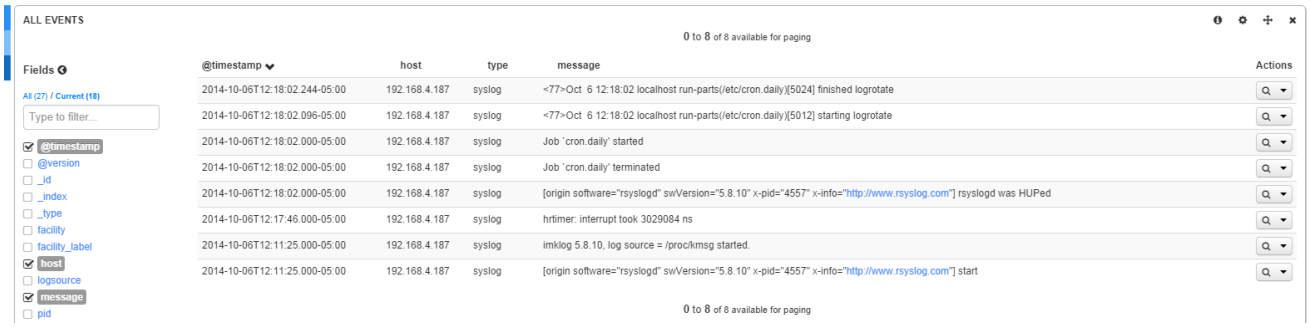
```
/var/www/html/nagioslogserver/www/scripts/setup-linux.sh
```

Use the **Copy** button to grab the code to curl the script and run it using bash. The codeblock will fill in your Nagios Log Server IP address and port automatically. Here is a successful run of the setup-linux script:

```
[root@localhost tmp]# curl -s -O http://192.168.4.187/nagioslogserver/scripts/setup-linux.sh
[root@localhost tmp]# bash setup-linux.sh -s 192.168.4.187 -p 5544
Detected rsyslog 5.8.10
Detected rsyslog work directory /var/lib/rsyslog
Destination Log Server: 192.168.4.187:5544
Creating /etc/rsyslog.d/99-nagioslogserver.conf...
rsyslog configuration check passed.
Restarting rsyslog service with 'service'...
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Okay.
rsyslog is running with the new configuration.
Visit your Nagios Log Server dashboard to verify that logs are being received.
```

This shows a successful run of the script. Once you get a similar output from the setup script navigate to your dashboard page as is indicated in the Setup Linux help section to verify you are receiving logs.

You should see IP address of the logs from the server that you ran the script on. Check the table under the **host** column:

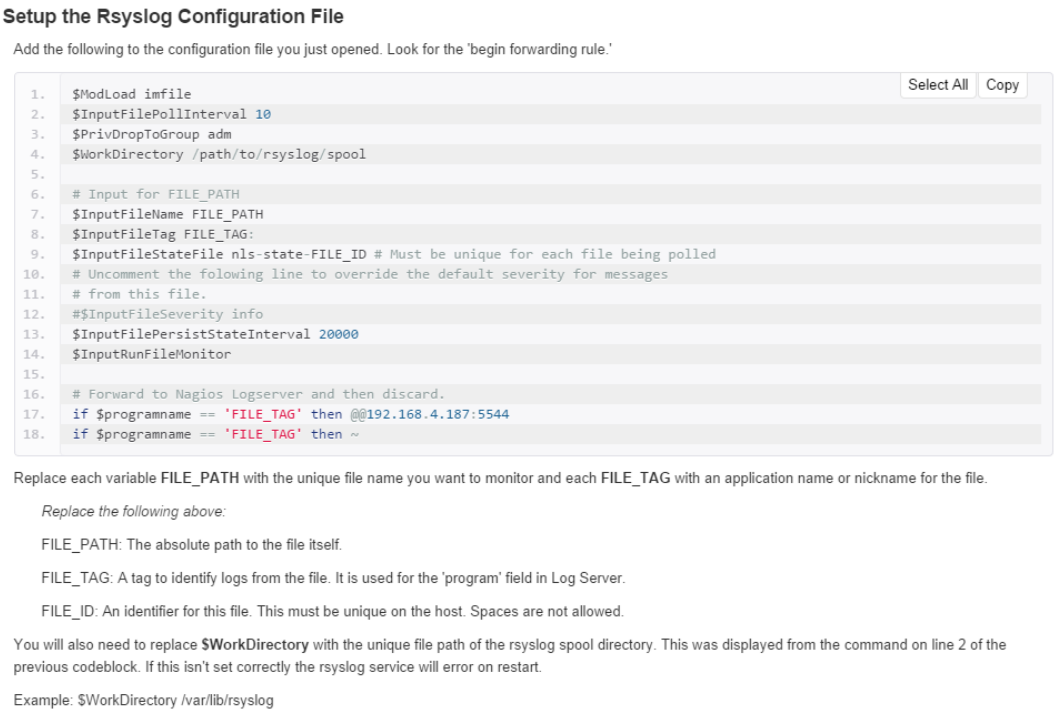


Here we see that the rsyslog service was restarted by the script and we are receiving logs from our example server.

More Sources

Once you have your first source set up you might want to setup more. Now use your **+ Log Source**  button on the navigation bar at the top of the user interface. This will bring you to the source setup selection page where you can choose what kind of source you want to add and which type of setup style you want to select.

Some Setups have a scripted method, like the one we showed above, and a manual method. The manual method shows how to manually setup your log source in a similar way the script does. These sections may allow for more customization since you are editing the configuration file yourself.



The Linux File Setup shows how to locate the configuration file using the command line on the machine that you want logs from. Then it directs you to edit the rsyslog.conf file just like the linux-setup script does.

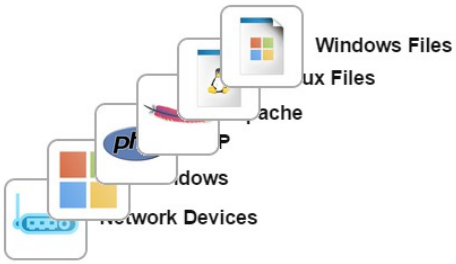
The manual part is after the above codeblock. It shows a list of sections that must be replaced. It is also important to note that the **$WorkDirectory** is where the rsyslog spool directory is located. If this path is incorrect the **rsyslog** service will not start or restart.

The path to the working directory is found by running the previous codeblock on the Linux File Source setup. Here is an example of the section being run:

```
[root@localhost tmp]# ls -d /var/lib/rsyslog || ls -d /var/spool/rsyslog || mkdir -v /var/spool/rsyslog
/var/lib/rsyslog
[root@localhost tmp]# ls -d /var/lib/rsyslog || ls -d /var/spool/rsyslog
/var/lib/rsyslog
[root@localhost tmp]# ls -d /etc/rsyslog.d || mkdir -v /etc/rsyslog.d
/etc/rsyslog.d
```

Here we see the first and second commands are telling us where the rsyslog working directory is. In this case it is `/var/lib/rsyslog`.

Now that you know how to use both the script and the manual methods check out the other types of sources you can receive logs from by looking in the source setup section by clicking the **+ Log Source** button.



Finishing Up

Now that you know how to add a log source with a script and manually following the Log Source page in the help section you can add other sources that are available including Windows event logs, Windows files, application logs, archived log files and more!

If you have questions about Nagios Log Server or of its capabilities, contact our support team via our online form at:

http://support.nagios.com/forum