Purpose

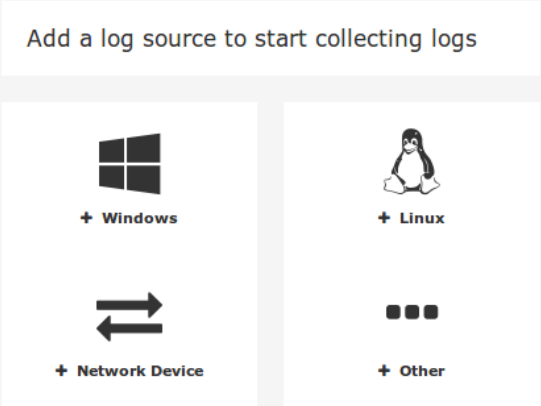
This document describes how to setup Nagios Log Server to monitor a new log source.

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.

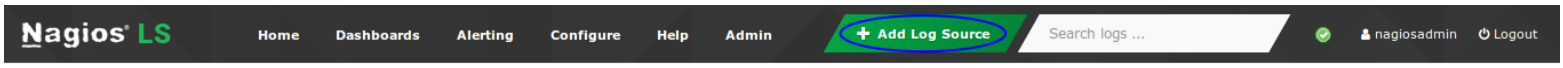
Add A Log Source

When you log in to Nagios Log Server you are presented with the Home page. In the bottom left of the page there are buttons to start sending logs to Nagios Log Server.



Multiple types of sources can be used, this documentation will be using a Linux log source as an example. Click on the **+ Linux** button.

Alternatively you can click the **+ Add Log Source** button on the navigation bar. This will take you to the Add Log Source page where you can click on the **Linux** button.



Add Linux Source

On the Linux Source Setup page you will be shown a code block with instructions on how to download and run the `setup-linux.sh` script (under **Run the Script**). This script will automatically configure rsyslog to send syslogs to your Nagios Log Server. The code block will already be populated with the address and port of your Nagios Log Server.

Note: The address in the `curl` command is automatically populated will be the address used in your web browser, it is taken from the URL you are using to access the Nagios Log Server web interface. It could be `10.25.5.86` or `nls01.domain.local`. If a DNS record is used, the Linux server that you are configuring to send logs to Nagios Log server must be able to resolve that DNS record.

Use your mouse to **highlight and copy** the code to your clipboard.

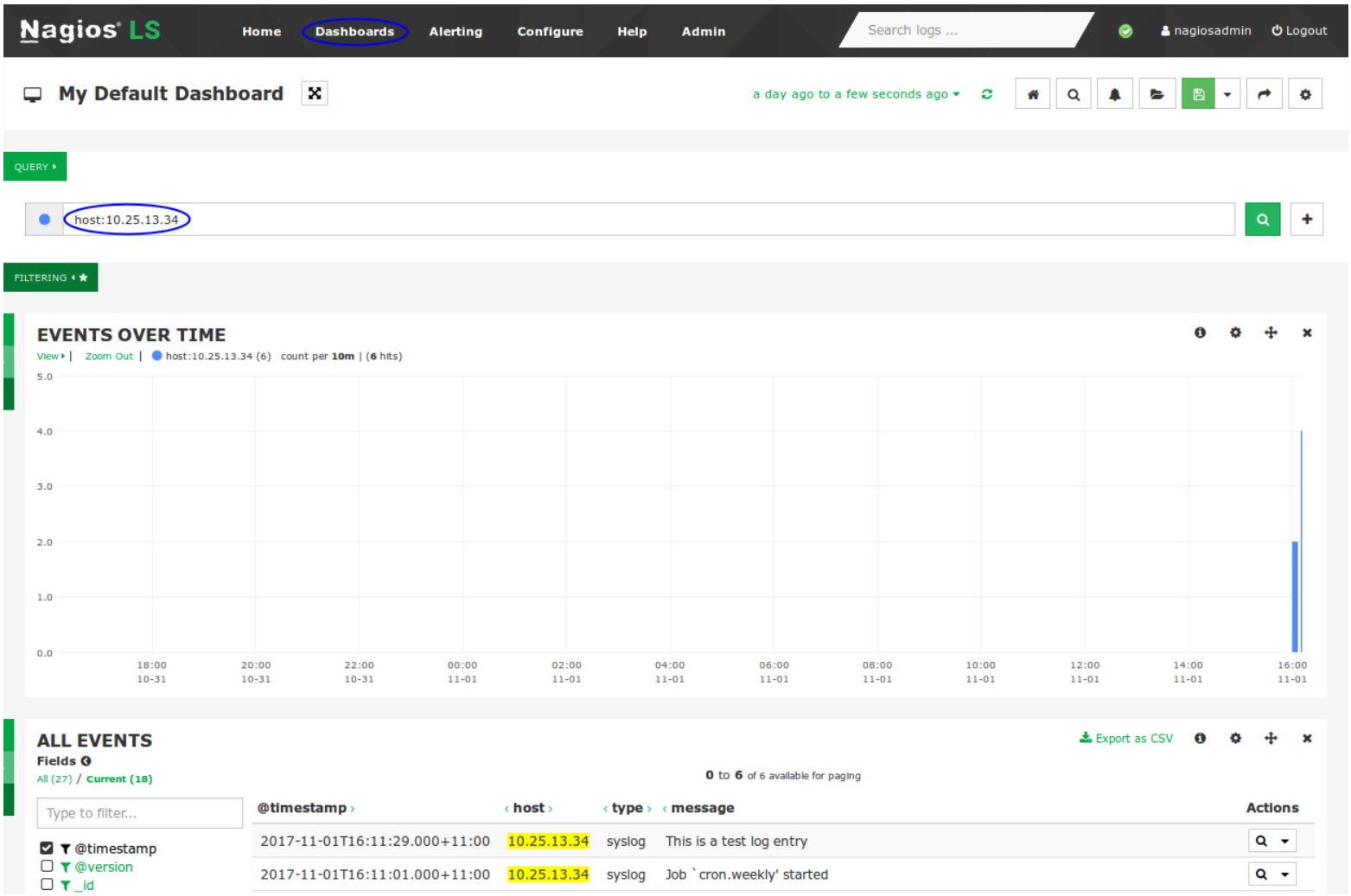
Establish a terminal session to the Linux machine that you want to configure to send logs to Nagios Log server as the root user.

Paste the code that has been copied into your clipboard into the terminal session, this will download the script and run it. Here is a successful run of the `setup-linux.sh` script:

```
[root@centos16 ~]# curl -sS -O http://10.25.5.86/nagioslogserver/scripts/setup-linux.sh
[root@centos16 ~]# sudo bash setup-linux.sh -s 10.25.5.86 -p 5544
Detected rsyslog 5.8.10
Detected rsyslog work directory /var/lib/rsyslog
Destination Log Server: 10.25.5.86:5544
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 (click **Dashboards** on the top navigation bar).

Perform a query using the IP address of the logs from the server that you ran the script on.



Note: If you want to force a log entry to be sent, execute the following command on your Linux machine:

```
logger This is a test log entry
```

In the screenshot above you can see the test log entry, this confirms that Nagios Log Server is receiving logs from the Linux machine.

Script Location On Server

In the previous section the `setup-linux.sh` script was downloaded from your Nagios Log Server. The actual location of this script on your Nagios Log Server instance is:

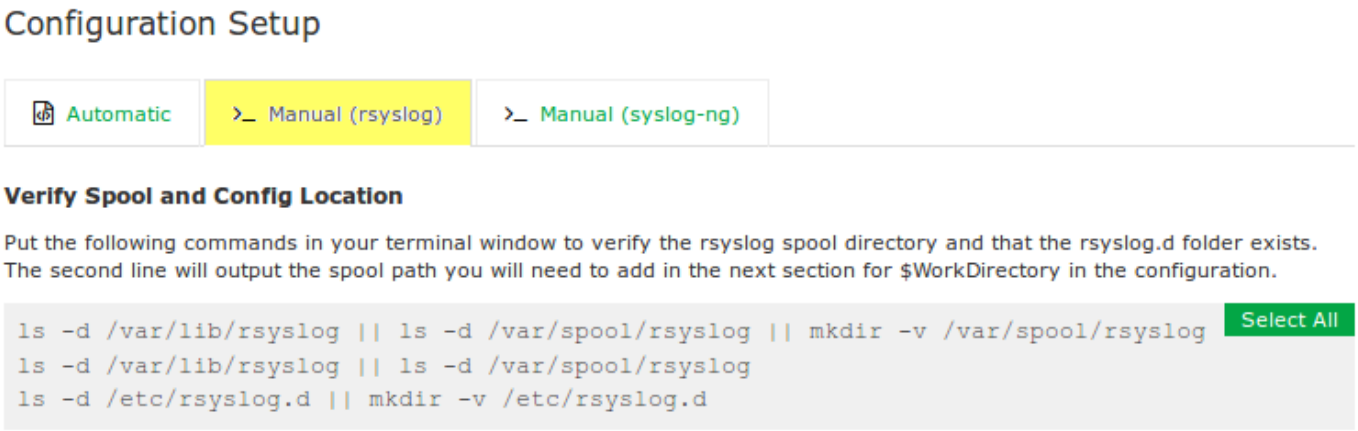
```
/var/www/html/nagioslogserver/www/scripts/setup-linux.sh
```

More Sources

Once you have your first source set up you might want to setup more. Use the **+ Add Log Source** button on the navigation bar. 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. These are available on separate tabs. 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 manual section will shows a list fields 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 commands in the code block.

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
```

You 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 **+ Add Log Source** button.

Finishing Up

This completes the documentation on monitoring a new log source in Nagios Log Server. Now that you know how to add a log source with a script and manually, you can add other sources that are available including Windows event logs, Windows files, application logs, archived log files and more!

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

https://support.nagios.com/kb