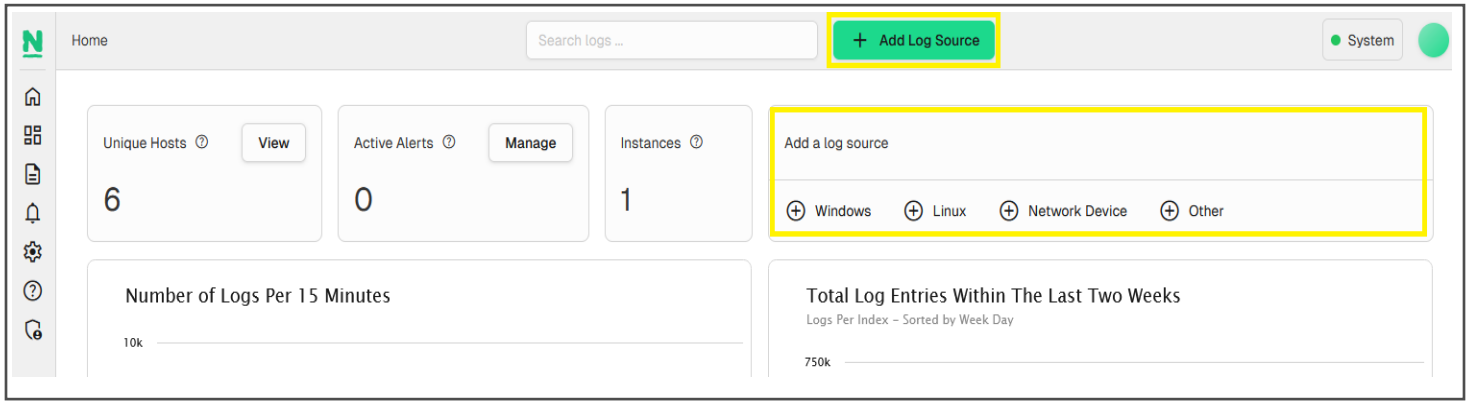
Monitoring a New Log Source with Nagios Log Server 2024R2

Purpose

This document describes how to configure a new log source to send log data to Nagios Log Server 2024R2.

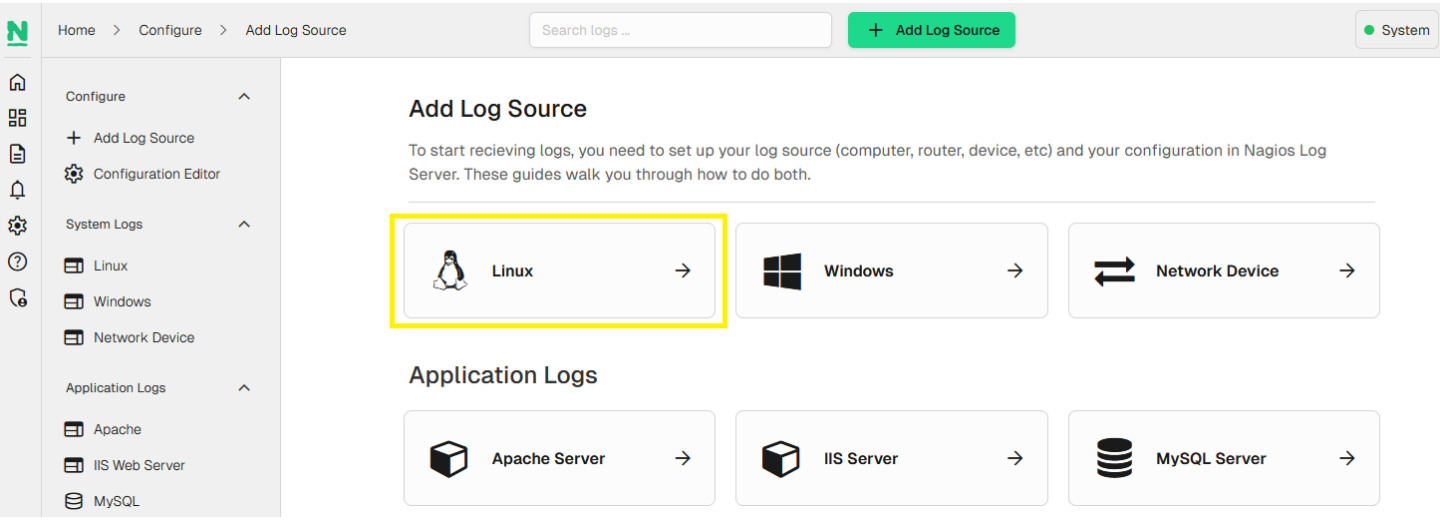
Add a Log Source

When you log in to Nagios Log Server you are presented with the Home page. At the very top you will see the green **+ Add Log Source** button. You will also notice an 'Add a log source' section on the upper right of the Home page where you can quickly access the specific setup guide for common sources:



While this documentation will detail setting up a Linux source, Log Server can collect data from many source types.

Click on the **+ Linux** button on the top right of Home, or click the button, then select Linux:



Add a 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 and will be the address used in your web browser, being taken from the URL you are using to access the Nagios Log Server web interface. It could be something like `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.

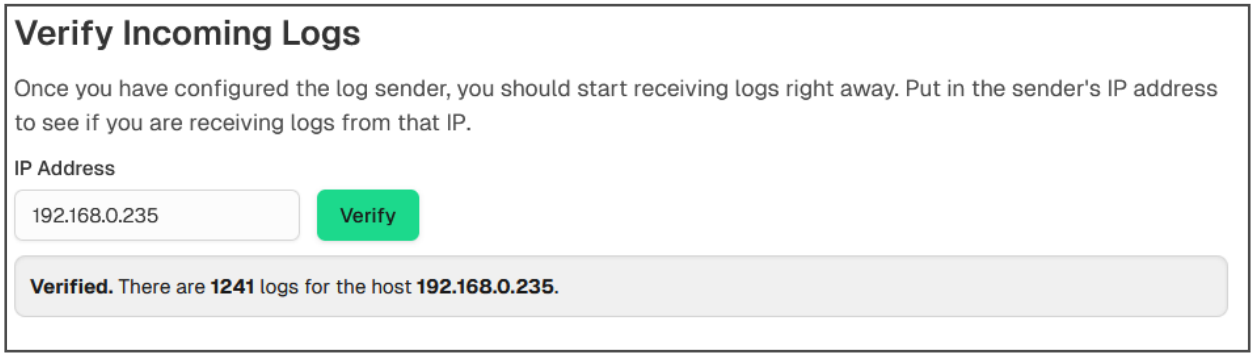
Establish a terminal session to the Linux machine that you want to configure to send logs to Nagios Log server as the root user.

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@Cent9Datasource ~]# curl -sS -O http://192.168.0.31/nagioslogserver/scripts/setup-linux.sh
[root@Cent9Datasource ~]# sudo bash setup-linux.sh -s 192.168.0.31 -p 5544
Detected rsyslog 8.2102.0
Detected rsyslog work directory /var/lib/rsyslog
Destination Log Server: 192.168.0.31:5544
Creating /etc/rsyslog.d/99-nagioslogserver.conf...
SELinux is disabled.
rsyslog configuration check passed.
Restarting rsyslog service with 'service'...
Redirecting to /bin/systemctl restart rsyslog.service
Okay.
rsyslog is running with the new configuration.
Visit your Nagios Log Server dashboard to verify that logs are being received.
```

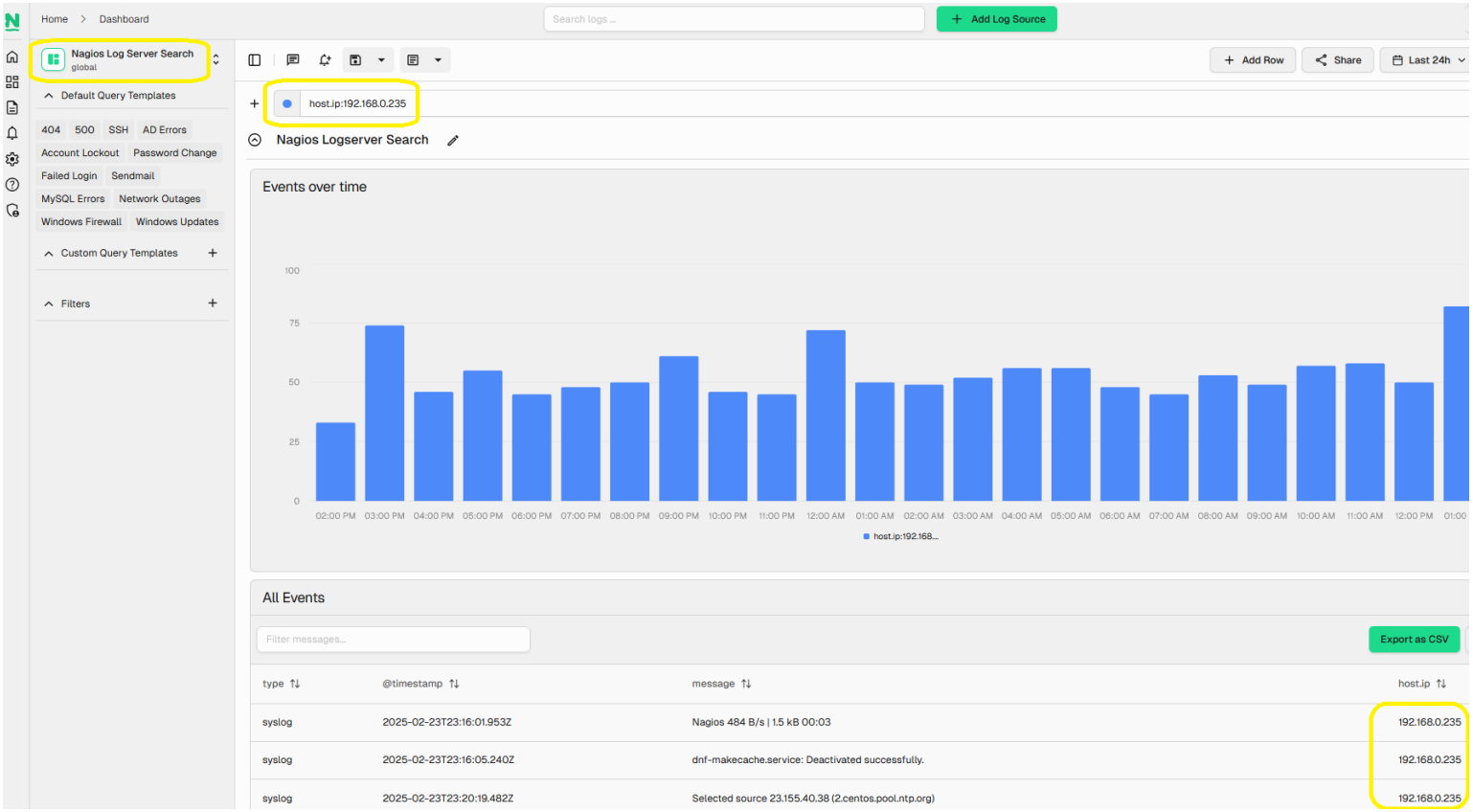
This shows a successful run of the script.

Once you get a similar output from the setup script, you can check that Log Server is now receiving logs from the new source by entering it's IP address in the 'Verify Incoming Logs' section at the bottom of the setup guide:



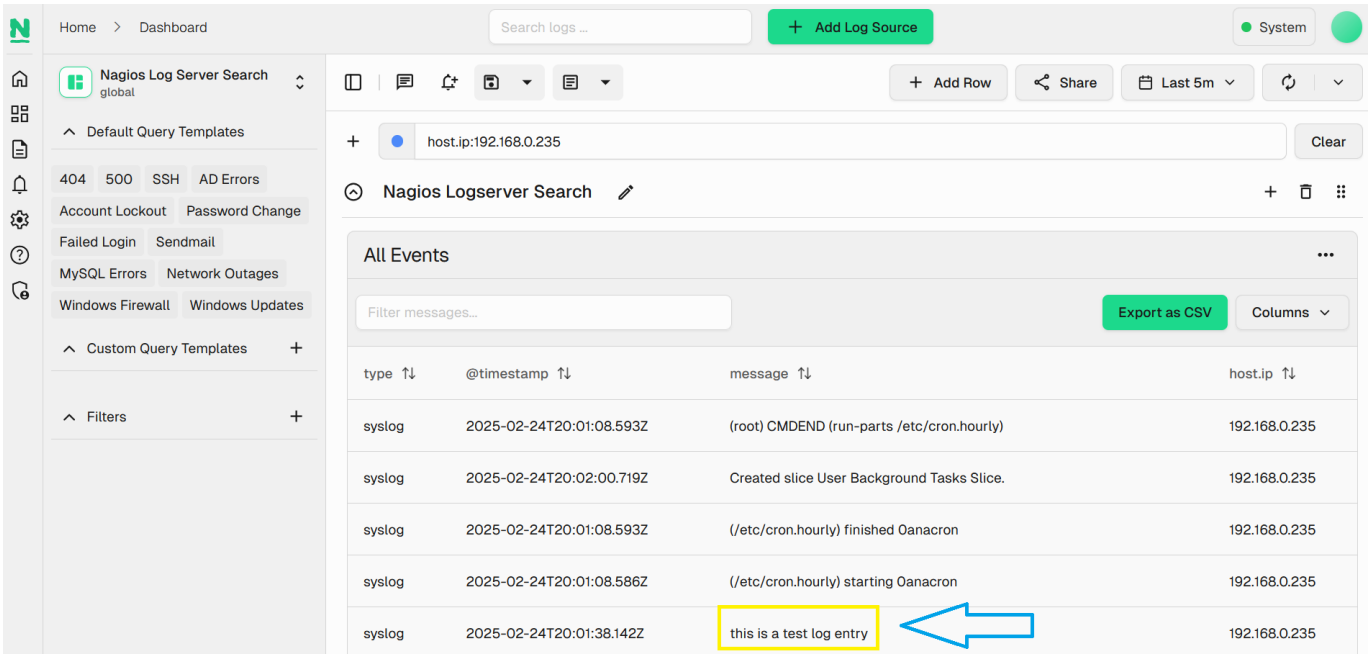
Another option is navigate to the **Dashboards** page, then the **Nagios Log Server Search** dashboard, and run a host query for the new source IP, replacing `<IP.address>` with the IP address of your source:

```
host.ip:<IP.address>
```



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
```

Manual Setup

Some Setups have a scripted method, like the one we explored above, as well as a manual method available on a separate tab. The manual method shows how to manually setup your log source in a similar way to how the scripted method does. The manual options may allow for more customization since you are editing the configuration file yourself.

The manual section for Linux shows a list of 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.

More Sources

Once you have your first source set up you might want to set up more. Clicking the **+ Add Log Source** button will bring you to the source setup selection page where you can choose what kind of source you'd like to add and which type of setup style you wish to use.

Finishing Up

This completes the documentation on Monitoring a New Log Source with Nagios Log Server 2024R2. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library