



## Purpose

This document describes how to configure Nagios Log Server to listen on privileged ports (ports below 1024).

## Target Audience

This document is intended for use by Nagios Log Server Administrators who would like configure Nagios Log Server to listen on ports below 1024 which are privileged in Linux. This can be useful if you have legacy devices that can only send on specific ports (e.g. syslog on port 514)

## Background

Ports below 1024 are privileged on Linux and only allow the root user to listen on them. This document provides two solutions to this situation.

1. [Run Logstash as root](#)
2. [Use setcap](#)

## Editing Files

In many steps of this documentation you will be required to edit files. This documentation will use the vi text editor. When using the vi editor:

- To make changes press **i** on the keyboard first to enter insert mode
- Press **Esc** to exit insert mode
- When you have finished, save the changes in vi by typing **:wq** and press Enter

## Method 1: Run Logstash as root

This method configures logstash to run as the `root` user. Edit the `logstash` config file by executing the following command:

### RHEL | CentOS | Oracle Linux

```
vi /etc/sysconfig/logstash
```

### Debian | Ubuntu

```
vi /etc/default/logstash  
or  
sudo vi /etc/default/logstash
```

Find the line:

```
LS_USER=nagios
```

Change the line to:

```
LS_USER=root
```

Save the file and close vi.

Now proceed to the [Restart Logstash Service](#) section of this document.

## Method 2: Use setcap

This option will preserve logstash running as the `nagios` user however this method may be less secure in some environments as it will allow any Java process to listen on privileged ports

The `logstash` init configuration file requires three lines to be added to the end of it, open the file with the following command:

### RHEL | CentOS | Oracle Linux

```
vi /etc/sysconfig/logstash
```

### Debian | Ubuntu

```
vi /etc/default/logstash  
or  
sudo /etc/default/logstash
```

Add the following three lines to the end of the file:

```
echo $(dirname $(find /usr/lib -name libjli.so)) | awk '{print $1}'> /etc/ld.so.conf.d/java.conf  
eval "$(which ldconfig)"  
setcap 'cap_net_bind_service=+ep' $(readlink -f $(which java))
```

Save the file and close vi.

Now proceed to the [Restart Logstash Service](#) section of this document.

## Restart Logstash Service

The `logstash` service needs to be restarted for these changes to apply:

**RHEL | CentOS | CentOS Stream | Oracle Linux | Debian | Ubuntu**

```
systemctl restart logstash.service  
or  
sudo systemctl restart logstash.service
```

Please proceed to the [Add Inputs](#) section of this document.

## Add Inputs

After implementing the chosen method you can add inputs to the configuration for ports below 1024. The following documentation explains how to create an input in Nagios Log Server:

[Configuring Nagios Log Server Inputs](#)

**Note:** Any ports lower than 1024 will not be listed in the "Logstash is currently collecting" banner on the Admin Overview page because the process listing the ports is not privileged and thus can not see any ports lower than 1024.

## Finishing Up

This completes the documentation on how to configure Nagios Log Server to listen on privileged ports. 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>