Nagios Log Server – Listening On Privileged Ports

Nagios®

The Industry Standard in IT Infrastructure Monitoring

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 will outline 2 possible workarounds to this situation.

1. Run Logstash as root

You can change logstash to run as the root user. Open /etc/sysconfig/logstash and find the line:

```
LS_USER=nagios
```

Change this line to read

```
LS_USER=root
```

Restart the logstash service:

```
# service logstash restart
```

2. Use setcap

The second option will preserve logstash running as the nagios user, however it should be pointed out that this method may be less secure in some environments as it will allow any java process to listen on privileged ports. To use this method, run the following commands:

```
#echo -e "\nsetcap 'cap_net_bind_service=+ep' \$(readlink -f \$(which java))" >> \
/etc/sysconfig/logstash
# service logstash restart
```

The “Logstash is currently collecting” banner on the Admin Overview page may be briefly unavailable while logstash restarts.

Note: This option will work only on RHEL/CentOS 6. It won't work on RHEL/CentOS 7.

Add Inputs

Now you can add inputs that can listen on ports below 1024.

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 thus can not see any ports lower than 1024.

Finishing Up

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

Nagios Enterprises, LLC
P.O. Box 8154
Saint Paul, MN 55108
USA

US: 1-888-NAGIOS-1
Int'l: +1 651-204-9102
Fax: +1 651-204-9103

Web: www.nagios.com
Email: sales@nagios.com