Nagios Log Server - Troubleshooting SELinux and rsyslog

Article Number: 490 | Rating: 1/5 from 2 votes | Last Updated: Tue, Dec 18, 2018 at 5:37 PM

Overview

If one of your Linux hosts is running SELinux and rsyslog, you may be running into issues receiving logs from from this host on one of your Nagios Log Server nodes.

This article will show you how to resolve this problem.

In this article:

- The Linux server with SELinux and rsyslog will be referred to as **sending_server**
- The Nagios Log Server receiving the logs will be referred to as **receiving_server**

Problem Description

Execute the following command on the **sending_server**:

```
tail /var/log/audit/audit.log | grep syslog
```

The following output will indicate that you are experiencing the problem:

```
type=AVC msg=audit(1459307833.315:38): avc:  denied  { name_connect } for  pid=1752 comm=72733A616374696F6E203120717565 dest=5544
scontext=unconfined_u:system_r:syslogd_t:s0 tcontext=system_u:object_r:port_t:s0 tclass=tcp_socket

type=SYSCALL msg=audit(1459307833.315:38): arch=c000003e syscall=42 success=no exit=-13 a0=2 a1=7fddc80016b0 a2=10 a3=40 items=0
ppid=1 pid=1752 auid=0 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=1 comm=72733A616374696F6E203120717565
exe="/sbin/rsyslogd" subj=unconfined_u:system_r:syslogd_t:s0 key=(null)
```

Further diagnosis can be made using the **semanage** program which requires some python libraries to be installed:

RHEL | CentOS

```
yum install -y policycoreutils-python
```

Debian 8 | Ubuntu 14/16

```
apt-get install -y policycoreutils
```

Debian 9 | Ubuntu 18

```
apt-get install -y policycoreutils-python-utils
```

Once the python libraries are installed, execute the following command:

```
semanage port -l | grep syslog
```

The command should output something similar to:

```
syslogd_port_t                 tcp      6514, 601
syslogd_port_t                 udp      514, 6514, 601
```

What is important here is that we know know what syslog ports SELinux will allow.

The resolution is to configure the **sending_server** to send logs on TCP port `6514` and the **receiving_server** to receive logs on on TCP port `6514`. We are choosing `6514` as there

Resolving The Problem

First step is to make changes to the **receiving_server**.

- Open the Nagios Log Server web interface on the **receiving_server**.
- Click the **Configure** menu at the top
- Global (All Instances) > **Global Config**
    - Under **Inputs** click the **Add Input** button and select **Custom**
        - In the "Block Name" field type **Syslog (SELinux)**
        - In the blank space below the code you need to type (or copy and paste) is as follows:

```
tcp {
    port => 6514
    type => syslog
}
udp {
    port => 6514
    type => syslog
}
```

- Click the **Save** button

- Under **Filters** click the **Add Filter** button and select **Custom**
  - In the "Block Name" field type **Syslog (SELinux)**
  - In the blank space below the code you need to type (or copy and paste) is as follows:

```
if [type] == "syslog" {
    grok {
      match => { "message" => "<%{POSINT:syslog_pri}>%{SYSLOGTIMESTAMP:syslog_timestamp} %{SYSLOGHOST:syslog_hostname} %
    }
  }
```

  - Click the **Save** button

- Config > **Apply Configuration**
  - Click the **Apply** button
    - Click **Yes, Apply Now**
  - *Wait while the configuration is applied to all the nodes in the cluster*

Open an SSH session to the **receiving_server** and execute the following commands (depending on your OS):

```
iptables -I INPUT -p tcp --destination-port 6514 -j ACCEPT
iptables -I INPUT -p udp --destination-port 6514 -j ACCEPT
service iptables save
```

RHEL 6 | CentOS 6

There are separate firewall daemons for for IPv4 and IPv6 and hence there are separate commands which are provided below:

IPv4

```
iptables -I INPUT -p udp --dport 6514 -j ACCEPT
iptables -I INPUT -p tcp --dport 6514 -j ACCEPT
service iptables save
```

IPv6

```
ip6tables -I INPUT -p udp --dport 6514 -j ACCEPT
ip6tables -I INPUT -p tcp --dport 6514 -j ACCEPT
service ip6tables save
```

RHEL 7 | CentOS 7

Add the firewall rules by executing the following commands:

```
firewall-cmd --zone=public --add-port=6514/udp
firewall-cmd --zone=public --add-port=6514/tcp
firewall-cmd --reload
```

Debian

Add the firewall rules by executing the following commands:

```
iptables -I INPUT -p udp --destination-port 6514 -j ACCEPT
iptables -I INPUT -p tcp --destination-port 6514 -j ACCEP
```

Ubuntu

Add the firewall rules by executing the following commands:

```
ufw allow proto udp from any to any port 6514
ufw allow proto tcp from any to any port 6514
ufw reload
```

This is all the changes required on the **receiving_server**.

Open an SSH session to the **sending_server** and edit the file:

```
vi /etc/rsyslog.d/99-nagioslogserver.conf
```

Change this line:

```
*.* @@receiving_server_address:5544                                    # NAGIOSLOGSERVER
```

To:

```
*.* @@receiving_server_address:6514                                    # NAGIOSLOGSERVER
```

Save the file.

Now you need to restart the rsyslogd daemon:

```
service rsyslog restart
```

This is all the changes required on the **sending_server**.

Test

Now that the changes have been made on both servers, you can easily test this by adding a test log to the **sending_server**'s syslog.

In an SSH session on the **sending_server** execute the following command:

```
logger TroubleshootingTest
```

On the **receiving_server** log into Nagios Log Server and click the **Dashboards** menu.

In the default dashboard we can search for the test logs we generated.

In the Query field type:

```
TroubleshootingTest
```

Press **Enter** and you should see the results below in the "Events Over Time" and "All Events" panels.

Final Thoughts

For any support related questions please visit the Nagios Support Forums at:

http://support.nagios.com/forum/

Posted by: **tlea** - Wed, Mar 30, 2016 at 12:21 AM. This article has been viewed 2249 times.

Online URL: https://support.nagios.com/kb/article/nagios-log-server-troubleshooting-selinux-and-rsyslog-490.html