Configure Syslog for Network Services Orchestrator 5.X Logs

Contents

Introduction

This document describes how to configure syslog-servers for Network Services Orchestrator (NSO) 5.x.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Configuration Requirements

Once the installation is completed, these files are needed:

- Configuration file is /etc/rsyslog.conf .
- Directory defined with specific configuration file(s) is **/etc/rsyslog.d/**.

For this configuration, use the rsyslog service which is available by default in several Linux distributions. In case it is not available on the server, download it as follows (RHEL/CentOS):

```
yum install rsyslog
```

With NSO 5.1, the syslog-server elements which were a part of the ncs.conf file that was made obsolete.

> **Note**: Support for the syslog via UDP has been removed in order to comply with Cisco security requirements. The default syslog functionality via the libc syslog(3) is still available.

In order to redirect NSO logs to a remote server, refer to NSO Syslog Relay Readme file and use the syslog daemon relay configuration.

Configuration

Two sets of configuration files are needed for configuration. One is on the server where NSO is run, the sender in this case, and the other is on the receiver (remote-server) which stores all the logs.

Step 1: Check that the ncs.conf file has this section:

```
<logs>
<syslog-config>
<facility>daemon</facility>
</syslog-config>
...
</logs>
```

Step 2: Configure the /etc/rsyslog.conf as follows:

- Under #### RULES ####; section add:

```
*.* @remote_ip
```

For example:

```
*.* @10.127.200.61
```

This line directs the rsyslog service to also redirect 'all' daemon logs to the remote host at the specified IP.

Step 3: Add a new file in the /etc/rsyslog.d/ path as shown in the next example.

- The new file is a configuration file to tell the rsyslog daemon details about which files to be sent over the network to the remote server.

For example:

```
$ModLoad imfile
$InputFileName /var/log/ncs/devel.log
$InputFileTag devel:
```

```
$InputFileStateFile stat-devel
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
...
```

- Once all the files are defined and contain details, you can specify where the files are sent via the protocol:

```
# Send over UDP
local6.* @remote_ip:port
```

For example:

```
local6.* @10.127.200.61:514
```

Step 4: Restart the rsyslog service:

```
service rsyslog restart
```

> **Note**: Steps 2 to 4 must be executed on the sender, that is, the server where NSO service is up.

Step 5: Uncomment the section for UDP/TCP based on your requirement in the /etc/rsyslog.conf file:

```
$ModLoad imudp
$UDPServerRun 514
```

> **Note**: 514 is the port used for this transfer.

Step 6: Modify the **/etc/rsyslog.conf** file. Add the lines under ###MODULES### section:

```
$template FileTemplate,"/var/log/ncs-server/%programname%.log"
if $programname startswith 'devel' then -?FileTemplate
if $programname startswith 'audit' then -?FileTemplate
if $programname startswith 'ncs' then -?FileTemplate
if $programname startswith 'ncs-java-vm' then -?FileTemplate
if $programname startswith 'ncserr' then -?FileTemplate
```

> **Note**: You can use the name ncs-server for your directory.

In this step, the rules are defined to store the logs specifically to NSO in designated location.

Step 7: Restart the rsyslog service:

```
service rsyslog restart
```

> **Note**: Steps 5 to 7 must be executed on the receiver, the remote server, where the logs are intended to be stored.

Additional Configurations

The syslog daemon relay functionality must be setup with these steps. However, in a production environment the Firewall service and SELinux are usually enabled. If they are enabled, the logs are not stored remotely. To ensure this does not cause any issues, you need to add these configurations on both servers:

- semanage port -a -t syslogd_port_t -p udp 514
- firewall-cmd --add-port=514/udp --permanent
- firewall-cmd --reload

Verification

If the steps have been followed correctly, the syslog server is setup remotely. To verify this:

On the remote-server:

```
nc -l -u -p 514
```

From the sender:

```
logger "Message from client"
```

The remote server must have received this message:

```
May 11 22:12:10 nso-recreate root: Message from client
```

Troubleshoot

In situations where the relay is not successful, you need to check the config files again.

It is also useful to confirm the status of NSO and rsyslog:

1. systemctl status ncs.service
   Expected output: [root@nso-recreate ncs]# systemctl status ncs.service ncs.service - LSB: NCS Loaded: loaded (/etc/rc.d/init.d/ncs; bad; vendor preset: disabled) Active: active (runnin) since Tue 2022-05-10 21:55:59 EDT; 24h ago ... No other lines in red in the status output.

2. service rsyslog status
   Expected output: [root@nso-recreate ncs]# service rsyslog status Redirectin to /bin/systemctl status rsyslog.service rsyslog.service - System Loggin Service Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled) Active: active (runnin) since Wed 2022-05-11 01:12:08 EDT; 21h ago ... No other lines in red in the status output.

You can check for Firewall rules or SELinux configurations. These can block the log transfer to the remote destination.

1. systemctl status firewalld.service
2. sestatus