JUNIPER NETWORKS

Network Configuration Example

Configuring a Branch SRX Virtual Chassis to Send Data Plane System Log Messages to NSM

Release
12.1

Published: 2012-05-03

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Network Configuration Example Configuring a Branch SRX Virtual Chassis to Send Data Plane System Log Messages to NSM
Release 12.1

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Introduction

This document describes how system log messages are sent to a Network and Security Manager (NSM) device. It shows how to enable data plane logging on SRX Series Services Gateways through NSM and add an SRX Virtual Chassis cluster device to NSM to send logs over UDP. It also shows how to synchronize the configuration, update the configuration file, import the configuration file, and generate system logs using the NSM GUI.

Finally, this document explains how to verify the system log messages in NSM log viewer and how to use the information.

System Log Messages Overview

A system log message records the following key information:

- List of incoming and outgoing IP flows, including services.
- Security attributes associated with a flow, for example, the policies that apply to traffic belonging to that flow.
- Sessions, the session timeout value, the active session time, the duration of the active session, the active traffic on the session, and detailed information specific to sessions.
- Software process that generated the message and a brief description of the operation or error that occurred.

You can configure the Network and Security Manager (NSM) to send specific system log messages to an external system log server.

For information about system logs, see the *Junos OS System Log Messages Reference*.

Related Documentation

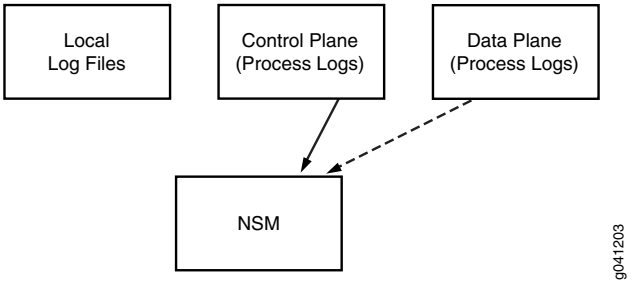
- Sending Data Plane System Log Messages to NSM Overview on page 1
- Example: Configuring a Branch SRX Virtual Chassis to Send Data Plane System Log Messages to NSM on page 2

Sending Data Plane System Log Messages to NSM Overview

A data plane log message records session details that include the source address, destination address, and port address. Data plane log messages are sent to the Routing Engine by default. Using stream mode, you can send the locally stored system log messages to the Network and Security Manager (NSM) from both the nodes in a Virtual Chassis. Data plane log messages are sent from every interface, except fxp0, that is tied to the Routing Engine.

Figure 1 on page 2 illustrates the data plane system log messages sent to NSM.

Figure 1: NSM Stream Mode Logging



Stream mode logging is the high performance method of delivering log messages to the syslog server. Stream mode logging is recommended if the log rate is high or the CPU load on the Routing Engine is high.

By default, data plane log messages are not saved to any local log file. To save log files, you must set the name, format, and category for stream logging in NSM. To forward specific system log files to a certain server, use the message filter.

System log files can be viewed, using the **start monitor default-log-messages** command.

Related Documentation

- System Log Messages Overview on page 1
- Example: Configuring a Branch SRX Virtual Chassis to Send Data Plane System Log Messages to NSM on page 2

Example: Configuring a Branch SRX Virtual Chassis to Send Data Plane System Log Messages to NSM

This example shows how to configure a branch SRX Series Virtual Chassis to send data plane system log messages to the Network and Security Manager (NSM).

This topic includes the following sections:

Requirements

This example requires the following hardware and software components:

- Juniper Networks branch SRX Series Services Gateways
- SRX Series Services Gateways Virtual Chassis running Junos OS Release 11.4R1.2 or later
- NSM Release 2011.1 or later system
- SRX Series Services Gateways cluster that is in sync with the Virtual Chassis in NSM

NOTE: This example uses the 2011.1 version of NSM software.

Overview and Topology

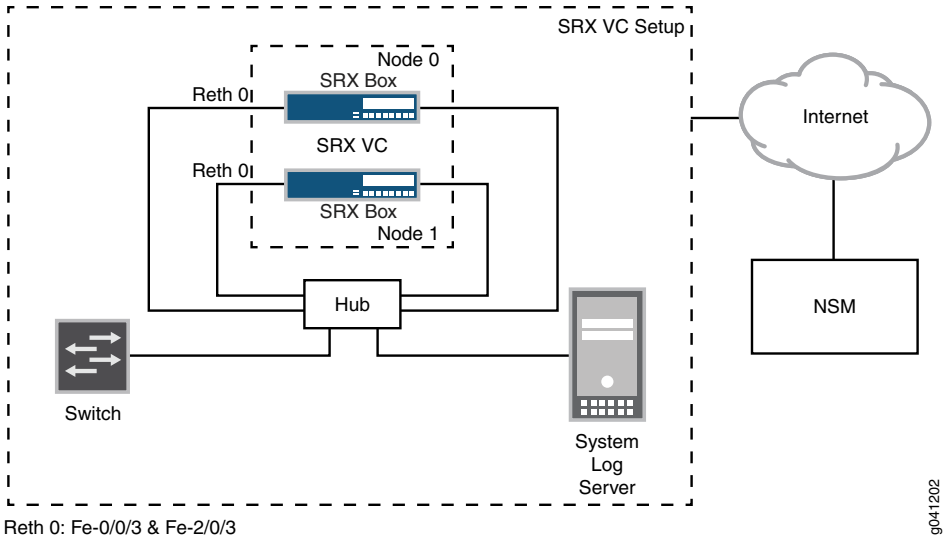
An SRX Virtual Chassis is a feature that enables in-band management of an SRX Virtual Chassis from NSM. This allows data plane system log messages to be forwarded to NSM from either node. The data plane is active regardless of which node has the active control plane: RE0 or RE1.

In the absence of an SRX Virtual Chassis, a cluster member must be configured with a dedicated interface for managing traffic bi-directionally from NSM.

Junos OS Release 11.4R1.2 or later is set up to connect to the cluster from NSM as shown in Figure 2 on page 3. In this setup, NSM connects to both the primary (RE0) and secondary (RE1) nodes. Cluster device traffic logs are sent to NSM by passing the log messages through the active nodes of the data plane regardless of the active control plane nodes: RE0 or RE1.

NOTE: Ensure that the external server receiving the log messages is reachable by both nodes.

Figure 2: SRX Series Virtual Chassis Cluster Setup



Configuration

Data plane logging on the SRX Series can be enabled on NSM or on the SRX Series CLI.

NOTE: If data logging is enabled on the SRX Series using the CLI, the configuration must be re-synchronized on NSM.

This topic includes the following sections:

Configuring System Message Logging Using the NSM CLI

Step-by-Step Procedure

To enable data plane logging on NSM over the User Datagram Protocol (UDP):

1. Connect to the NSM console or through SSH as an administrator.
2. Change directory to **/var/netscreen/DevSvr/**.

   root@nsm2011# cd /var/netscreen/DevSvr/
3. Edit the **devSvr.cfg** file.

   root@nsm2011# vi devSvr.cfg
4. Change the **devSvr.enableSyslogOverUdp** parameter to **true** and save the file.

   By default, **devSvr.enableSyslogOverUdp** is set to **false**.
5. Restart the development and GUI services.

   root@nsm2011# service devSvr restart; service guiSvr restart
6. Verify connectivity between NSM and UDP port 5140.

   ```
   root@nsm2011# netstat -an

   Active Internet connections (servers and established)
          Proto Recv-Q Send-Q Local Address    Foreign Address         State

          udp   0      0      0.0.0.0:5140     0.0.0.0:*
   ```
7. Configure the branch SRX Virtual Chassis cluster device to send log messages over UDP by setting the following parameters under the security hierarchy:

   ```
   root@SRX_Cluster_Node_0# show security log

   mode stream;
   source-address 192.168.0.3;
   stream NSM {
     format sd-syslog;
     category all;
     host {
       192.168.0.40;
       port 5140;
     }
   }
   ```

Results

Use the **tcpdump port 5140** and **host 192.168.0.1** commands to verify that NSM is receiving syslog messages from the device.

```
[root@nsm2011 ~]# tcpdump port 5140 and host 192.168.0.1
```

```
cpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
20:19:28.110954 IP 192.168.0.1.syslog > 192.168.0.40.5140: SYSLOG uucp.info,
length: 596
20:19:28.112201 IP 192.168.0.1.syslog > 192.168.0.40.5140: SYSLOG uucp.info,
length: 609
20:19:28.124632 IP 192.168.0.1.syslog > 192.168.0.40.5140: SYSLOG uucp.info,
length: 777
20:19:28.135100 IP 192.168.0.1.syslog > 192.168.0.40.5140: SYSLOG uucp.info,
length: 609
```

Configuring the iptable Rule

Step-by-Step Procedure

An iptable rule is added if NSM is not receiving syslog messages from the device. Adding an iptable rule enables traffic movement.

To configure an iptable rule:

1. Add a rule to allow UDP port 5140.

   [root@nsm2010 ~]# iptables -I RH-Firewall-1-INPUT -p udp --dport 5140 -j ACCEPT

2. Use the **iptables -L** command to display the syslog messages.

   [root@nsm2010 ~]# iptables -L

Results

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere   anywhere
ACCEPT            all  -- anywhere    anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere   anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere            udp dpt:5140
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere            icmp any
ACCEPT     esp  --  anywhere             anywhere
ACCEPT     ah   --  anywhere             anywhere
ACCEPT     udp  --  anywhere             224.0.0.251         udp dpt:mdns
ACCEPT     udp  --  anywhere             anywhere            udp dpt:ipp
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ipp
ACCEPT     all  --  anywhere             anywhere            state
RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere            anywhere           state NEW tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp
dpt:https
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:asr
ACCEPT     tcp  --  anywhere            anywhere           state NEW tcp dpt:7801
ACCEPT     tcp  --  anywhere            anywhere           state NEW tcp dpt:7802
ACCEPT     tcp  --  anywhere            anywhere           state NEW tcp dpt:7803
ACCEPT     tcp  --  anywhere            anywhere           state NEW tcp dpt:7804
ACCEPT     tcp  --  anywhere            anywhere           state NEW tcp dpt:7808
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp
```

```
dpt:pcsync-https
REJECT     all  --  anywhere             anywhere             reject-with
icmp-host-prohibited
```

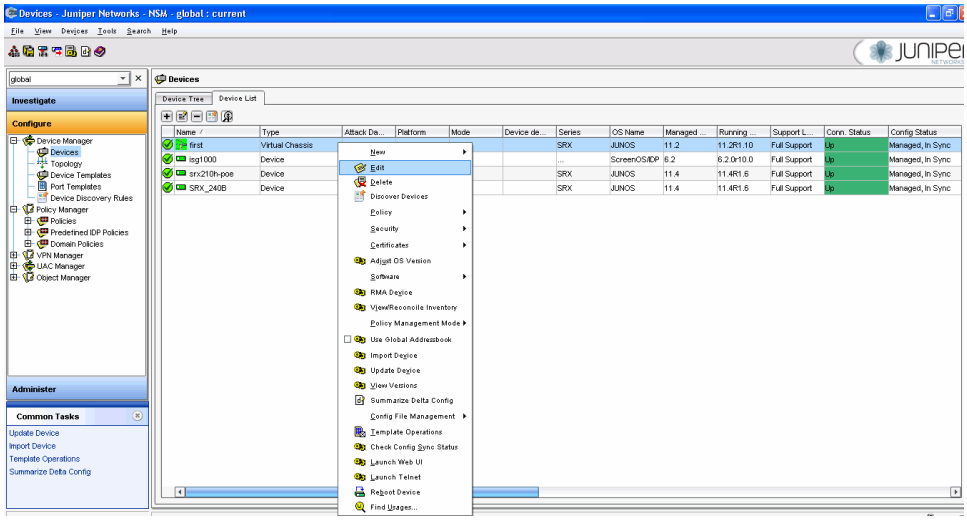
Configuring System Message Logging Using the NSM GUI

Step-by-Step Procedure

To enable data plane logging over UDP on the SRX Series device:

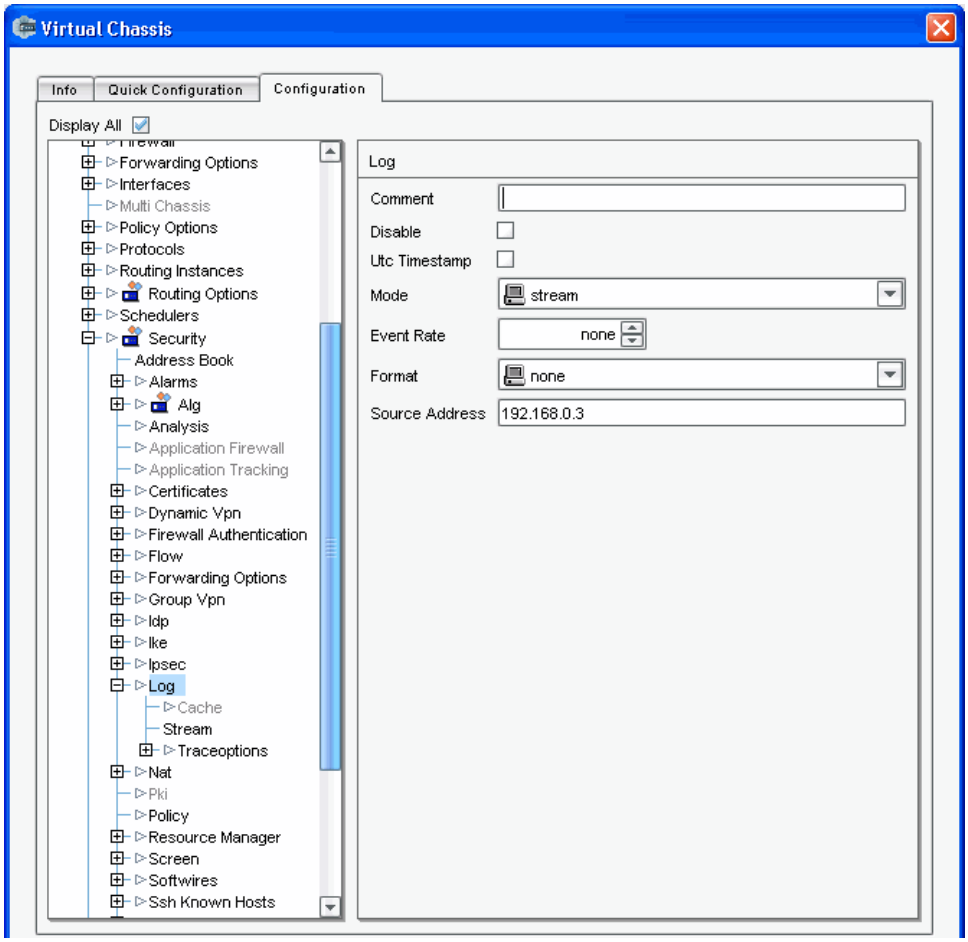
1. Right-click the device and select **Edit** as shown in Figure 3 on page 6.

Figure 3: SRX Virtual Cluster Edit Option



2. Select the **Configuration** tab.
3. Navigate to the configuration tree and select **Security**>**Log**.
4. Set the **Mode** to **Stream**, and enter the **Source Address** as shown in Figure 4 on page 7.

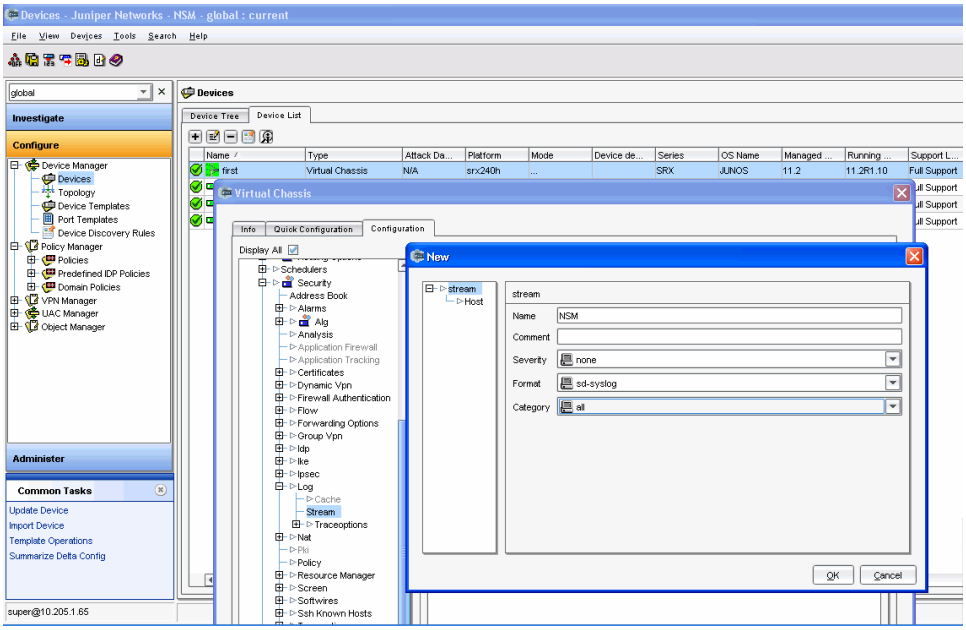
Figure 4: Virtual Chassis Configuration Option



5. Select **Stream** in the configuration tree log and click **+** to add a new destination syslog server.

6. Enter **NSM** in the Name field, **sd-syslog** in the Format field, and **all** in the Category field as shown in Figure 5 on page 8.

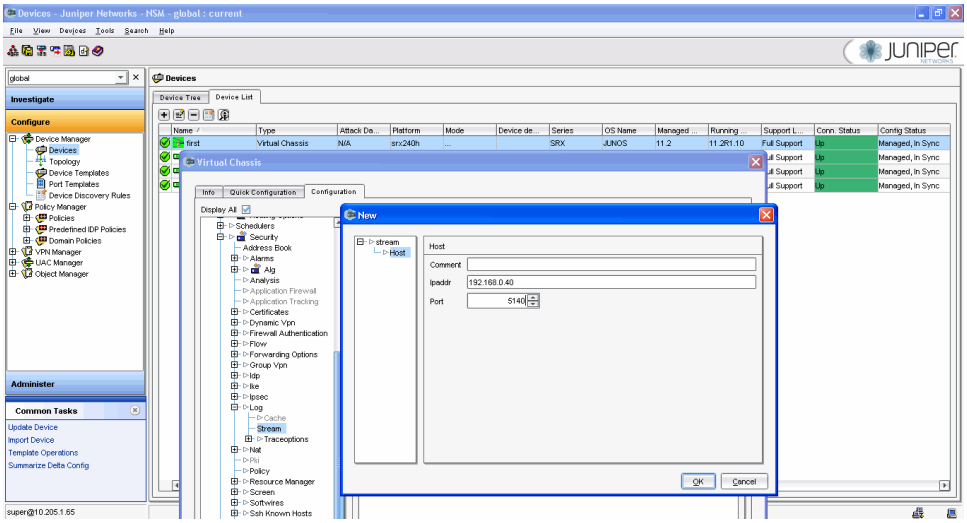
Figure 5: Virtual Chassis Stream Configuration Option



7. Select **Host** >**Stream** and set the syslog server parameters.

   Use **Port 5140** for NSM as shown in Figure 6 on page 8.

Figure 6: Virtual Chassis Stream Host Configuration Option



8. Click **OK** in each window to get back to the NSM Device Manager window.
9. Right-click and select **Update Device** as shown in Figure 7 on page 9.

   The device update notification is displayed as shown in Figure 8 on page 9 and Figure 9 on page 10.

Figure 7: SRX Device Update Option

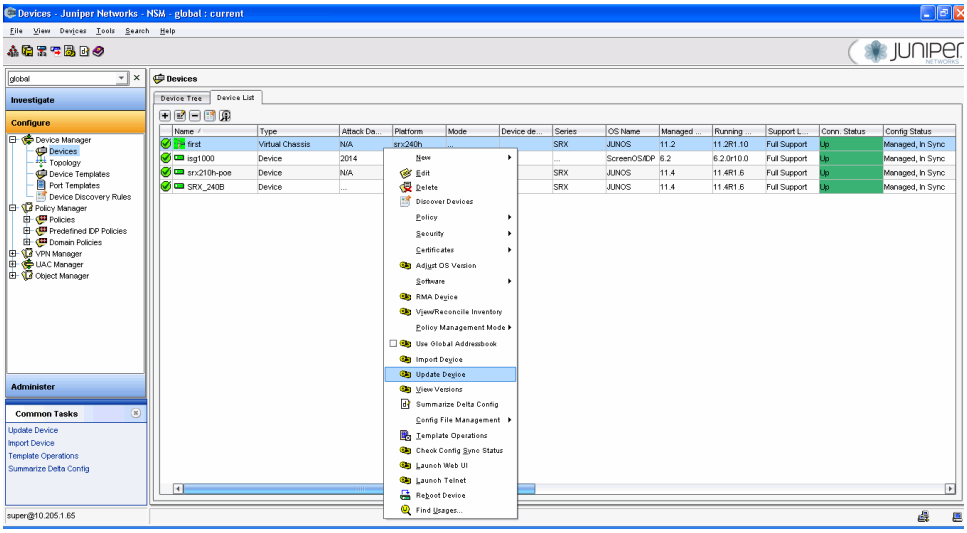


Figure 8: Device Update Option

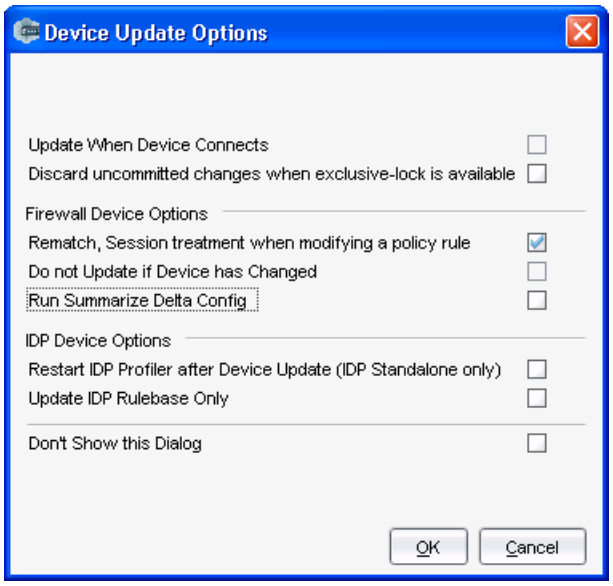
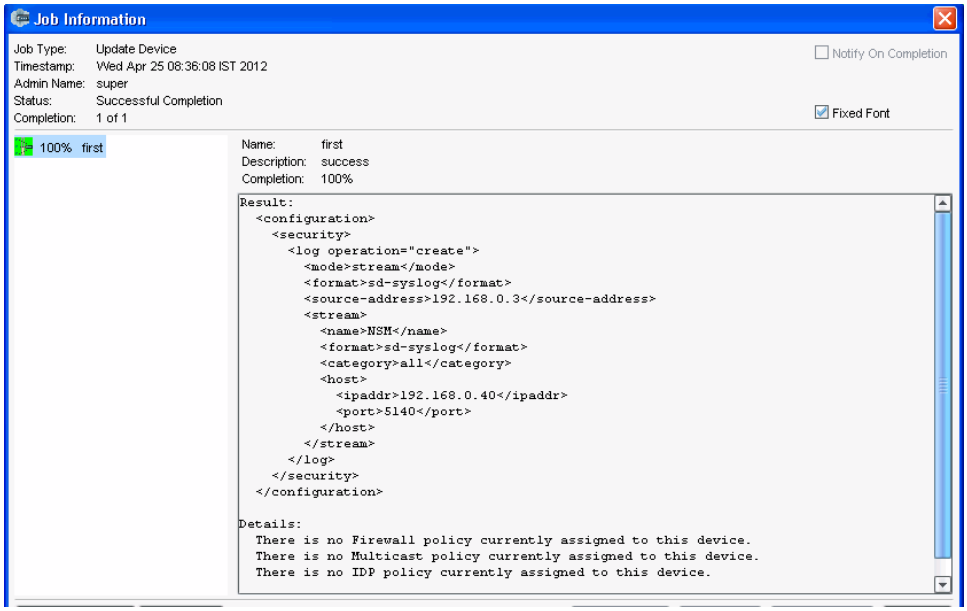


Figure 9: Job Information



10. Verify that NSM can display the logs in log viewer by selecting **Predefined**>**Traffic Logs**.

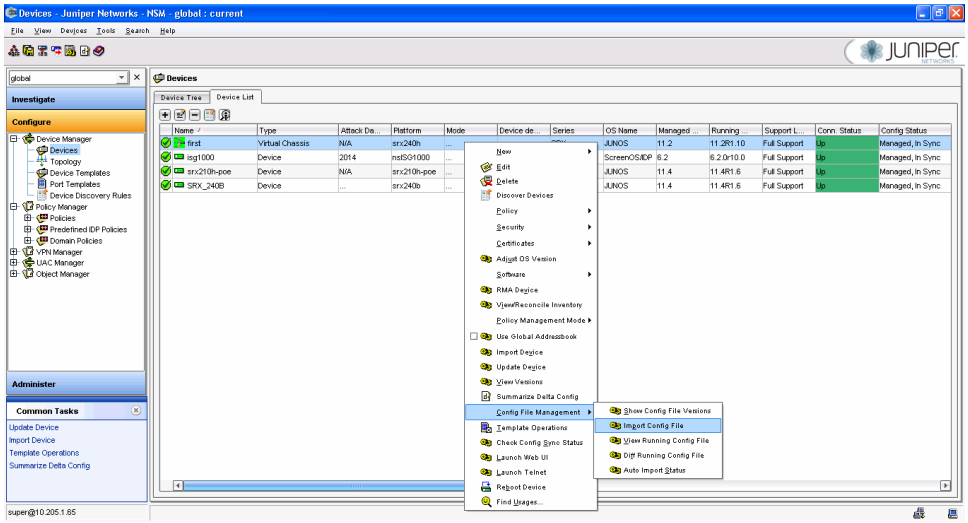
Importing the Existing Configuration File

Step-by-Step Procedure

To import the existing configuration file:

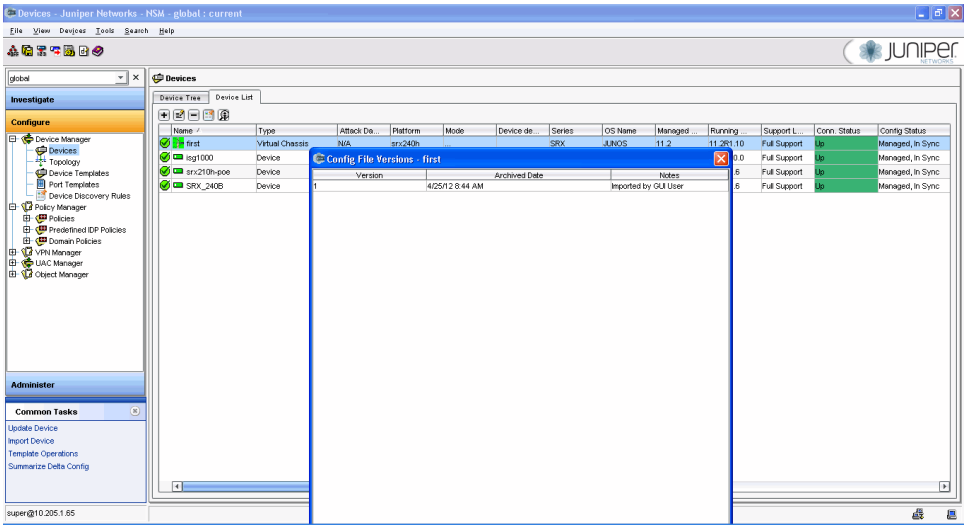
1. Right-click the NSM device and select **Config File Management** >**Import Config File** as shown in Figure 10 on page 10.

Figure 10: Configuration File Import Option



2. Select **Config File Management**>**Show Config File Version** as shown in Figure 11 on page 11.

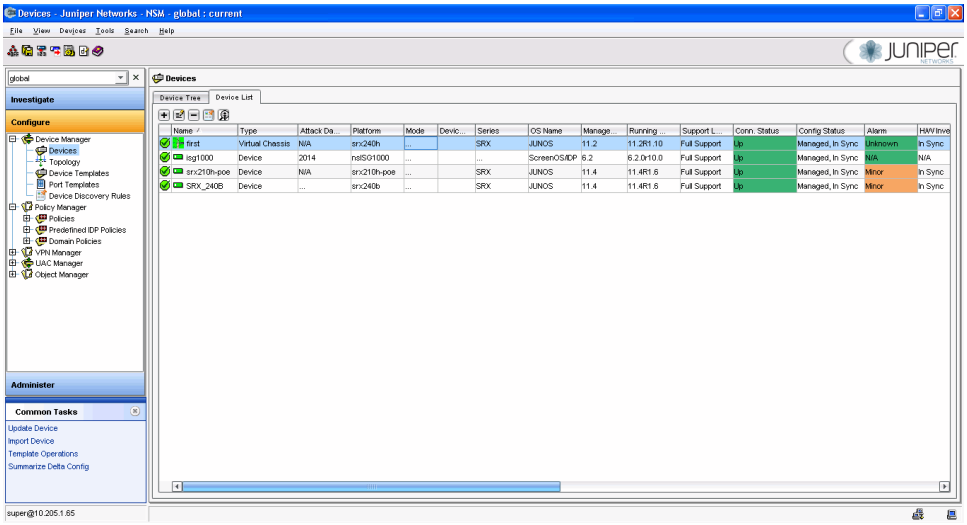
Figure 11: Configuration File Version



3. Select the latest configuration file that you imported and click **Update**.

   NSM is synchronized with the device as shown in Figure 12 on page 11.

Figure 12: File Synchronization Status



Related Documentation

- System Log Messages Overview on page 1
- Sending Data Plane System Log Messages to NSM Overview on page 1

