RSA NetWitness Logs

Event Source Log Configuration Guide

Juniper Networks NetScreen-Security Manager

Last Modified: Thursday, May 25, 2017

Event Source Product Information:

Vendor: Juniper Networks
Event Source: NetScreen-Security Manager
Versions: 2006, 2007, 2010, 2011, 2012.2R3
Additional Download: nicsftpagent.conf.nsm

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: nsm
Collection Method: Syslog, File
Event Source Class.Subclass: Network.Configuration Management

Configure Juniper Networks NetScreen-Security Manager

This document includes configuration instructions for configuring the following:

- Juniper Networks NSM version 2010, 2011, or 2012
- Juniper Networks NSM version 2006 or 2007
- Juniper Networks NSM version 2004

Configure Juniper Networks NetScreen-Security Manager 2010, 2011, or 2012

You can configure Juniper Networks NetScreen-Security Manager for Syslog or File collection.

Configure Juniper Networks NSM 2010, 2011, or 2012 for File Collection

You must complete these tasks to configure Juniper Networks NetScreen-Security Manager for File collection:

I. Set up the Juniper NSM for File

II. Set up the SFTP Agent

III. Set up the File Service

To configure Juniper NSM 2010, 2011 or 2012 for File collection:

1. Log on to the NetScreen-Security Manager utility with administrative credentials.
2. From the navigation pane, select the **Administer** tab, expand **Action Manager**, and select **Action Parameters**.
3. From the Action Parameters window, click the **Edit**, and follow these steps depending on your collection method:
   a. In the CSV section, in the **File Path** field, enter a file path, for example **/temp/nsm.csv**.
   b. Ensure that **Print Header** is selected.
   c. Click **Apply**, and click **OK**.
4. From the navigation pane, expand **Action Manager**, and select **Device Log Action Criteria**.
5. From the Device Log Action Criteria window, click the **Add** icon, and follow these steps depending on your collection method:

a. On the **Action** tab, select **Write to CSV File**.

b. Click **OK**.

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see Install and Update SFTP Agent
- To set up the SFTP agent on Linux, see Configure SA SFTP Agent shell script

Configure the Log Collector for File Collection

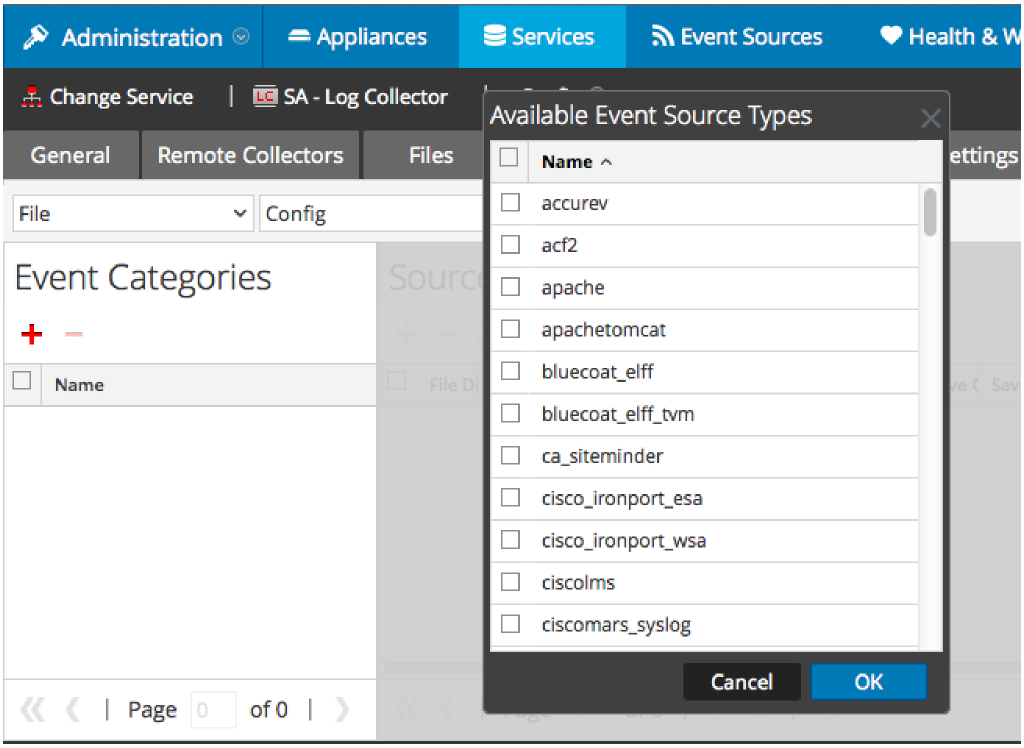
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **File/Config** from the drop-down menu.

   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

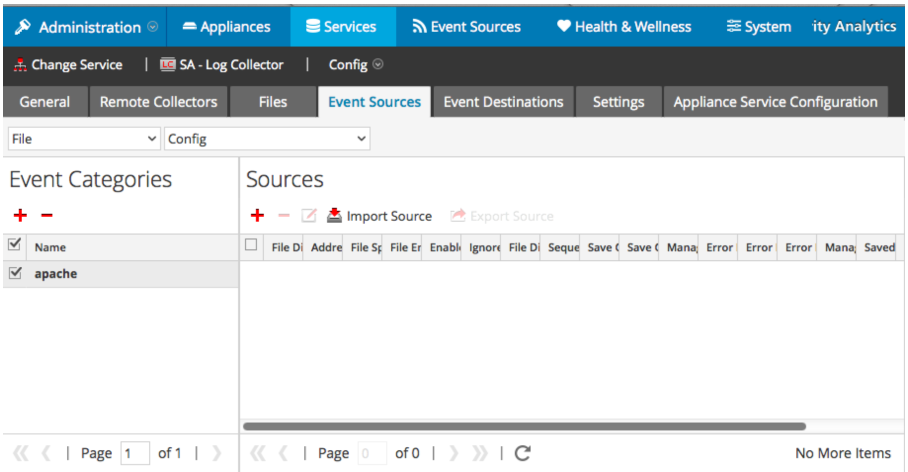
   The Available Event Source Types dialog is displayed.



5. Select the correct type from the list, and click **OK**.

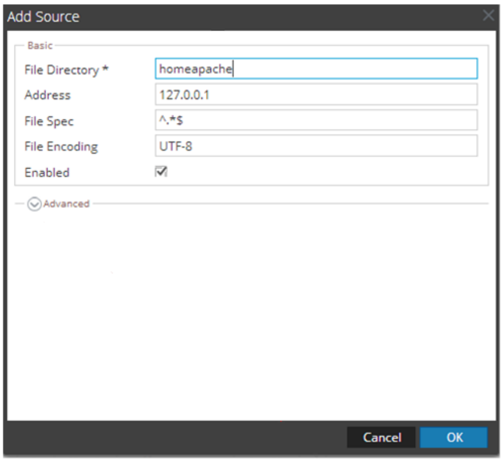
   Select **nsm_syslog** from the **Available Event Source Types** dialog.

   The newly added event source type is displayed in the Event Categories panel.



6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.



Add Source

Basic

File Directory * homeapache

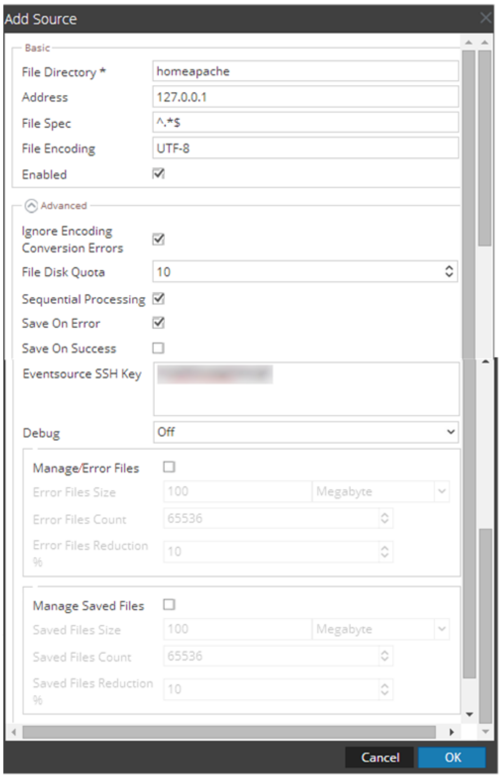
Address 127.0.0.1

File Spec ^.*$

File Encoding UTF-8

Enabled ☑

Advanced



Add Source

Basic

File Directory * homeapache

Address 127.0.0.1

File Spec ^.*$

File Encoding UTF-8

Enabled ☑

Advanced

Ignore Encoding Conversion Errors ☑

File Disk Quota 10

Sequential Processing ☑

Save On Error ☑

Save On Success □

Eventsource SSH Key [redacted]

Debug Off

Manage/Error Files □

Error Files Size 100 Megabyte

Error Files Count 65536

Error Files Reduction % 10

Manage Saved Files □

Saved Files Size 100 Megabyte

Saved Files Count 65536

Saved Files Reduction % 10

7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.

8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Configure Juniper Networks NSM for Syslog

To configure Juniper NSM 2010, 2011, or 2012 for Syslog collection:

1. Log on to the NetScreen-Security Manager utility with administrative credentials.

2. From the navigation pane, select the **Administer** tab, expand **Action Manager**, and select **Action Parameters**.

3. From the Action Parameters window, click the **Edit**, and follow these steps:

a. In the Syslog section, click the **Add** icon.and enter the following values:

Field	Value
Syslog Server	A name for the Syslog Server
Syslog Server IP	IP address of your RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.
Syslog Server Facility	Messages generated internally by syslogd

b. Click **Apply**, and click **OK**.

4. From the navigation pane, expand **Action Manager**, and select **Device Log Action Criteria**.

5. From the Device Log Action Criteria window, click the **Add** icon, and follow these steps depending on your collection method:

   a. Select the **Category** tab, and from the **Category** drop-down list, select any entry from the list.

   b. Select each subcategory for which you want to receive alerts.

   c. Click **OK**.

   d. On the **Severity** tab, ensure that all the values are selected.

   e. Click **OK**.

   f. On the **Action** tab, select **Send Syslog Messages**.

   g. Click the **Add** icon.

   h. From the Add/Edit Syslog Services window, select the Syslog services for which you want to collect logs, and click **Add**.

   i. Click **OK**.

Configure RSA NetWitness Suite for Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **System**.
3. Depending on the icon you see, do one of the following:
   - If you see ▶ Start Capture, click the icon to start capturing Syslog.
   - If you see ■ Stop Capture, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

   The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.
5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced

parameters as necessary.

Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Configure Juniper NetScreen-Security Manager 2006 and 2007

To configure Juniper NSM 2006 and 2007:

1. Log on to the NetScreen-Security Manager utility with administrative credentials.
2. From the navigation pane, expand **Action Manager**, and select **Action Parameters**.
3. From the Action Parameters window, click **Edit**, and enter the following values:

Field	Value
Syslog Server IP	IP address of your RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.
Syslog Server Facility	Messages generated internally by syslogd

4. Click **OK**, and click **Save**.
5. From the navigation pane, expand **Action Manager**, and select **Device Log Action Criteria**.
6. From the Device Log Action Criteria window, click **Add**.
7. On the **Category** tab, set the category to **Predefined**.
8. Select each subcategory for which you want to receive alerts.
9. Click **Apply**.
10. On the **Severity** tab, ensure that the following values are selected:
    - Not Set
    - Info
    - Warning
    - Minor
    - Major
    - Critical

11. Click **Apply**.
12. On the **Action** tab, select **Syslog Enable**.
13. Click **OK**, and click **Save**.

Configure Juniper NetScreen-Security Manager 2004

To configure Juniper NSM 2004:

1. Log on to the NetScreen-Security Manager utility with administrative credentials.
2. Expand **Server Manager**, and select **Servers**.
3. Under **GUI Server**, select the server you want to modify, and click **Edit**.
4. On the **Log Actions** tab, select **GUI Server**.
5. In the **Syslog Server IP** field, enter the IP address of the syslog server.
6. On the **Log Criteria** tab, click **Add**.
7. On the **Category** tab, select **New Add/Edit Log Criteria**.
8. From the **Category** drop-down list, select a log category and follow these steps:
    a. In the **Subcategory** section, select the subcategories that you want to log.
    b. On the **Severity** tab, select the severity levels that you want to log.
    c. On the **Actions** tab, select **Syslog Enable**.
    d. Click **OK**.

Trademarks