RSA NetWitness Logs

Event Source Log Configuration Guide

Juniper Networks Intrusion Detection and Prevention (IDP)

Last Modified: Thursday, May 25, 2017

Event Source Product Information:

Vendor: Juniper Networks
Event Source: Intrusion Detection and Prevention (IDP)
Versions: 3.0, 3.1, 3.2, 4.0, 4.1, 5.0
Additional Downloads: nicsftpagent.conf.nsm

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: netscreenidp
Collection Method: Syslog, File
Event Source Class.Subclass: Security.IPS

Juniper Networks Intrusion Detection and Prevention (IDP)

This document contains instructions for the following:

I. Configuring IDP 4.0, 4.1, and 5.0

   i. Configure IDP 4.0, 4.1 and 5.0 for Syslog

   ii. Configure IDP for File Collection

II. Configure IDP 3.2, 3.1, and 3.0 for Syslog

III. Configure NetWitness Suite for Syslog Collection

Configure IDP 4.0, 4.1 and 5.0 for Syslog

Note: Juniper Networks IDP 4.0, 4.1, and 5.0 is configured through NetScreen-Security Manager.

To configure IDP 4.0, 4.1, and 5.0:

1. Log on to NetScreen-Security Manager with administrator credentials.
2. To set the Action Parameters, in the global navigation pane, click **Action Manager** > **Action Parameters**, and complete the following steps:
   a. Click **Edit**.
   b. In the Action Parameters window, complete the fields as follows:

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

   c. Click **OK**.
   d. On the toolbar, click **Save**.
3. To set the Device Log Action Criteria, in the global navigation pane, click **Action Manager** > **Device Log Action Criteria**, and complete the following steps:
   a. Click **Add**.
   b. In the New Device Log Action Criteria window, click the **Category** tab.
   c. In the Category drop-down list, select **Predefined (predefined)**.
   d. Select the sub-categories of alerts you wish to receive.
   e. Click **Apply**.
   f. In the New Device Log Action Criteria window, click on the **Severity** tab, and select the following:
      - Not Set
      - Info

- Warning
- Minor
- Major
- Critical

g. Click **Apply**.

h. In the New Device Log Action Criteria window, click on the **Action** tab, and select **Syslog Enable**.

i. Click **OK**.

j. On the toolbar, click **Save**.

Configure IDP for File Collection

You must complete these tasks to configure Juniper Networks Intrusion Detection and Prevention (IDP) to work with RSA NetWitness Suite:

I. Set up the SFTP Agent

II. Set up the File Service

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

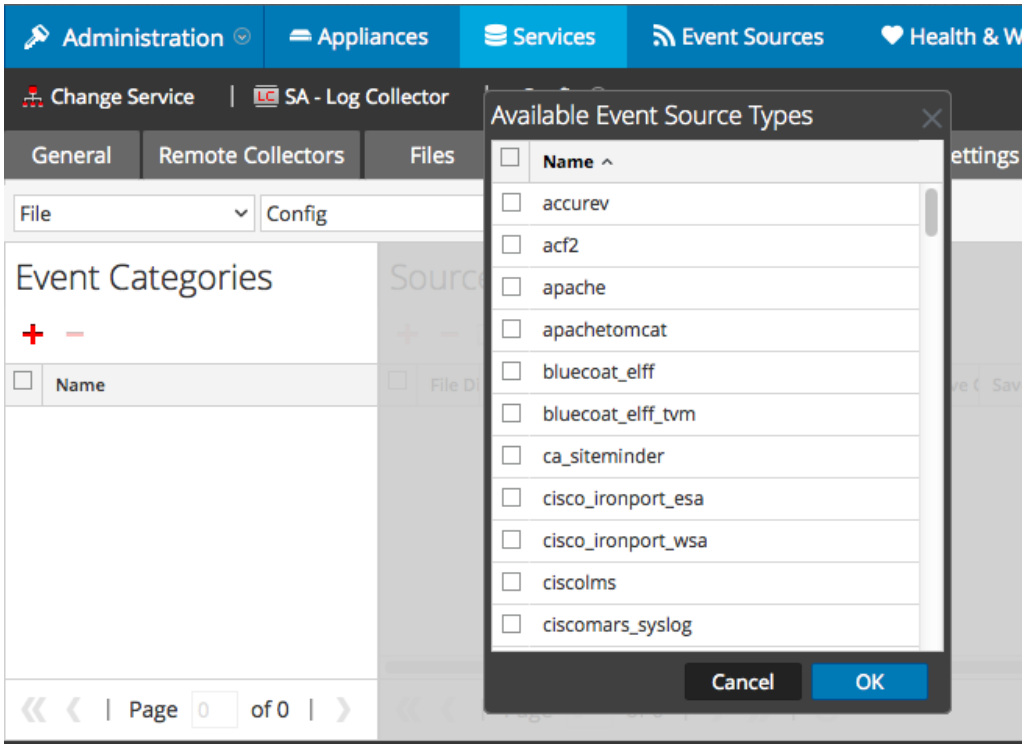
Perform the following steps to configure the Log Collector for File collection.

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 +.

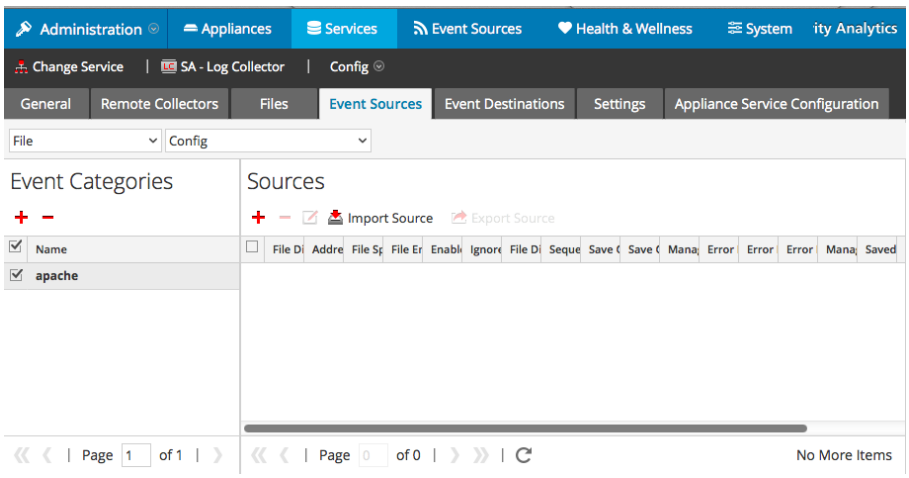
   The Available Event Source Types dialog is displayed.



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

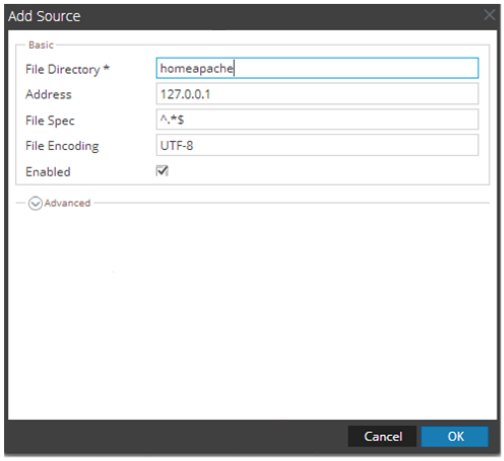
   Select **juniperidp** from the **Available Event Source Types** dialog.

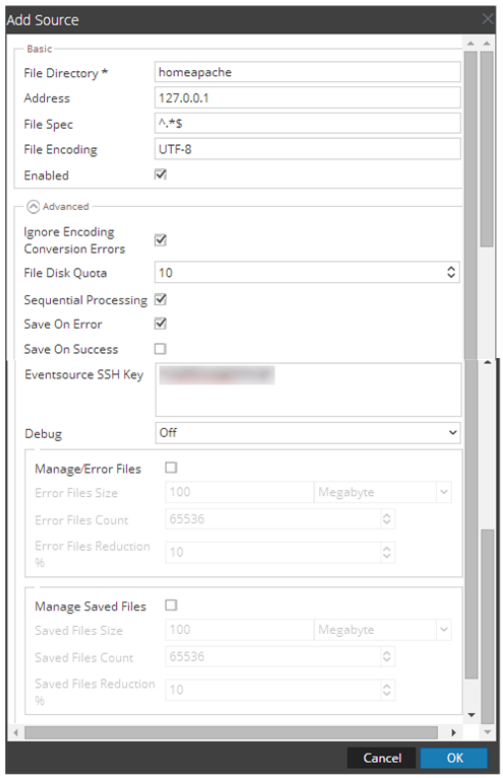
   The newly added event source type is displayed in the Event Categories panel.



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

   The Add Source dialog is displayed.





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 IDP 3.x for Syslog

For Juniper IDP version 3.2, 3.1, and 3.0, you can collect messages using Syslog.

To configure IDP version 3.2

1. Log on to the Juniper Networks IDP appliance with administrator credentials.
2. To set the Preference Settings, complete the following steps:
   a. From the top menu, click **Tool** > **Preferences**.
   b. In the Preference Settings window, select **Management Server**.
   c. In the Syslog Host field, enter the IP address of your RSA NetWitness Suite Log Decoder or Remote Log Collector.
   d. Click **OK**.
   e. When prompted to save changes, click **Yes**.
3. To set the Column Settings, complete the following steps:
   a. In the IDP Components pane, select **Log Viewer**.
   b. From the top menu, click **View** > **Choose Columns**.
   c. In the Column Settings window, select **Syslog**, and click **OK**.
   d. From the top menu, click **File** > **Save All**.
4. To set the Security Policy, complete the following steps:
   a. In the IDP Components pane, select a Security Policy.
   b. Click the Rulebase you wish to use for notification.

      Note: Syslog from the Traffic Anomalies and SYN-Protector rulebase are not supported.

      Warning: Each rule in a Security Policy must be enabled individually.

   c. In the **Notification** column, right-click on the rule and select **Configure**.
   d. Click **OK**.
   e. From the top menu, click **File** > **Save All**.
   f. From the top menu, click **Policy** > **Install**.

To configure IDP version 3.0 and 3.1:

1. Log on to Juniper Networks IDP appliance with administrator credentials.
2. Click **Tool** > **Preferences** > **Management Server**.
3. In the Syslog Host field, enter the IP address of your RSA NetWitness Suite Log Decoder or Remote Log Collector.
4. Click **OK**.

   Warning: Forwarding must be enabled individually for each attack on which you want notification.

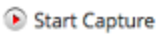
5. After defining your security policies, right-click on the desired policy in the notification column.
6. Select **Configure**.
7. Ensure **enable logging** is selected, and select **syslog**.
8. Click **OK**.

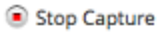
Configure NetWitness Suite for Syslog

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 

, click the icon to start capturing Syslog.
   - If you see 

, 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.

Trademarks