RSA NetWitness Logs

Event Source Log Configuration Guide

Juniper Unified Access Control

Last Modified: Monday, May 22, 2017

Event Source Product Information:

Vendor: Juniper Networks
Event Source: Unified Access Control
Versions: 2.2, 3.1, 4.5

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: juniperic
Collection Method: Syslog
Event Source Class.Subclass: Security.Access Control

To configure Juniper Unified Access Control to work with RSA NetWitness Suite, perform the following procedures:

- Configure Juniper Unified Access Control
- Configure NetWitness Suite for Syslog Collection

Configure Juniper Unified Access Control

To configure Juniper Unified Access Control:

1. Log on to the Juniper Unified Access Control web console with administrative credentials.
2. To create a new filter, follow these steps:
   a. Click **System** > **Log/Monitoring**.
   b. Select the **Events**, **User Access**, or **Admin Access** tab.

      Note: : The **Events** tab contains system events, the **User Access** tab contains end-user requests and modifications, and the **Admin Access** tab contains administrator modifications.

   c. Click **Filters**.
   d. Click **New Filter**.
   e. In the **Filter Name** field, type **NetWitness**.
   f. Navigate to the **Export Format** section, and select **Custom**.
   g. Depending on your version of Juniper Unified Access Control, in the **Format** field, type one of the following:
      - For Juniper Unified Access Control 4.5 and later:

        ```
        JUNIPERIC-%id%: %date% %time% - %node% - [%sourceip%]
        %user%(%realm%)[%role%] - %msg%
        ```

      - For Juniper Unified Access Control 3.1 and earlier:

        ```
        JUNIPERIC %date% %time% - %node% - [%sourceip%] %user%
        (%realm%)[%role%] - %msg%.
        ```

   h. Click **Save**.
3. Click **System** > **Log/Monitoring** > **Events** > **Settings**.
4. In the **Select Events to Log** section, select each type of event that you want to log.
5. In the **Syslog Servers** section, follow these steps to add a syslog server:

a. In the **Server name/IP** field, enter the name or the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

b. From the **Facility** drop-down list, select the log facility.

c. From the **Filter** drop-down list, select **NetWitness: Custom**.

d. Click **Add**.

e. To add additional syslog servers, repeat steps **a** through **d** for each server.

6. Click **Save Changes**.

Configure NetWitness Suite for Syslog Collection

Perform the following steps in RSA NetWitness Suite:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is **juniperic**.

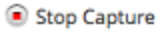
Configure Syslog Collection

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 

, 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