RSA NetWitness Logs

Event Source Log Configuration Guide

Cisco Aggregation Services Router

Last Modified: Wednesday, January 18, 2017

Event Source Product Information:

Vendor: Cisco
Event Source: Aggregation Services Router
Versions: 3.3

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: ciscorouter
Collection Method: Syslog
Event Source Class.Subclass: Network.Router

Configure Cisco Aggregation Services Router

After you configure the Cisco Aggregation Services Router event source, make sure that RSA NetWitness Suite is configured for Syslog Collection.

To configure Cisco ASR to send syslog messages:

1. Log on to Cisco ASR and enter CONFIG mode.

2. Type `logging` *`IP-address`* and press **Enter** to set the logging host.

   where *IP-address* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

3. Type `logging trap` *`syslog-level`* and press **Enter** to set the logging level.

   The *syslog-level* is the level of messages to be logged. Valid entries are:

   - emergencies

   - alerts

   - critical

   - errors

   - warnings

   - notifications

   - informational

   - debugging.

   > **Note:** To ensure full logging, use debugging.

4. Type `logging on` and press **Enter** to turn logging on.

5. Type `service timestamps log datetime localtime show-timezone` and press **Enter** to enable timestamps.

6. Press **CTRL+Z**.

Configure NetWitness Suite

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 **ciscorouter**.

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:

Configure NetWitness Suite

- 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.

Trademarks

Configure Syslog Collection