RSA NetWitness Logs

Event Source Log Configuration Guide

IBM WebSphere DataPower

Last Modified: Friday, January 5, 2018

Event Source Product Information:

Vendor: IBM
Event Source: WebSphere DataPower
Versions: 3.8.1, 7.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

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

To configure the IBM WebSphere DataPower event source, you must:

I. Configure Syslog Output on IBM WebSphere DataPower

II. Configure RSA NetWitness Suite for Syslog Collection

Configure Syslog Output on IBM WebSphere DataPower

DataPower Overview

IBM WebSphere DataPower produces appliances for processing XML messages as well as any-to-any legacy message transformations (such as flat files, COBOL, or text files). DataPower created network devices to implement a broad XML-aware and application-oriented network strategy.

DataPower can be used to offload XSLT processing, XPath routing, legacy-XML conversion, and other resource-intensive tasks from servers to reduce latency, improve throughput, and to free up computer resources.

Configure IBM WebSphere DataPower

You must configure DataPower through a web interface.

To configure DataPower to send logs to RSA NetWitness:

1. Log on to the Web GUI for your DataPower installation.
2. In the log on dialog box, provide your username and password, and select the appropriate domain.
3. From the Control Panel, select **Objects** > **Logging Configuration** > **Log Target**.
4. Add a new target, and set the parameters as follows.

Field	Setting
Name	Enter a name for the log target.
Target Type	From the drop down menu, select **syslog**.
Local Identifier	Enter a descriptive string that may be used by a remote recipient to identify this specific log target.

Field	Setting
Remote Host Address	Enter .the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Remote IP Port	Enter **514** for the port.
Syslog Facility	From the drop down menu, select **user**.

5. For all other fields, accept the default values.
6. Click **Apply** to save your log target.

Configure RSA 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 **ibmwebspheredp**.

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 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