

RSA NetWitness Platform

Event Source Log Configuration Guide



Huawei VRP

Last Modified: Tuesday, May 26, 2020

Event Source Product Information:

Vendor: [Huawei](#)

Event Source: Versatile Routing Platform (VRP)

Versions: 5.x, 6.x, 8.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.

Platforms: Quidway AR46, AR1200, AR2200, AR3200, and NE5000E Series routers

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: huaweivrp

Collection Method: Syslog

Event Source Class.Subclass: Network.Router

The Huawei VRP (Versatile Routing Platform) is a network OS that supports a number of Huawei network systems. It features an IP forwarding engine, and integration of real time OS technology, equipment and network management technology and various network application technologies. It supports a large number of protocols and features, and thus allows you to build an end-to-end, secure network.

This document contains the following sections:

- I. Configure the Huawei VRP (Versatile Routing Platform) Event Source
- II. Configure RSA NetWitness Platform for Syslog Collection

Configure the Huawei VRP

You can create or edit an ACL (Access Control List), and then add a rule to the ACL to allow the event source to communicate with RSA NetWitness Platform.

To configure Huawei VRP to send data to RSA NetWitness Platform:

1. Log onto the Huawei VRP event source, and open a command prompt.
2. Type the following:

```
info-center loghost NetWitness-ip
```

where *NetWitness-ip* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
3. Enter one of the following commands, depending on the version of Huawei VRP that you are using:
 - For version 5.20, enter the following:

```
info-center timestamp loghost date
```
 - For version 5.30 and later, enter the following:

```
info-center timestamp log date
```
4. Type

```
acl ACL_Number
```

where *ACL_Number* is the number of an Access Control List.
5. Type the following:

```
rule Rule_Number permit source NetWitness-ip 0
```

where *Rule_Number* is the rule number, and *NetWitness-ip* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
6. Type the following:

```
rule Rule_Number comment *syslog
```

where *Rule_Number* is the rule number.

Note: Create a new *ACL_Number* or add to an existing one. Use a new **Rule_**
Number.

For example, on a 5.30 system, you might enter the following set of commands:

```
info-center loghost 10.212.41.11
info-center timestamp log date
acl number 2014
rule 1 permit source 10.212.41.11 0
rule 1 comment *syslog
```

Configure RSA NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- 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 Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN > 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 **huaweivrp**.



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 **ADMIN > 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 **ADMIN > 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.

After 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.

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.