

RSA NetWitness Platform

Event Source Log Configuration Guide



Barracuda Web Application Firewall

Last Modified: Wednesday, May 30, 2018

Event Source Product Information:

Vendor: [Barracuda Networks](#)

Event Source: Web Application Firewall

Versions: Firmware version 7.4.0, 7.8.0, 7.9.2, 8.x, 9.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 Platform 10.0 and later

Event Source Log Parser: barracudawaf

Collection Method: Syslog

Event Source Class.Subclass: Security.Application Firewall

To configure Syslog collection for the Barracuda Web Application Firewall event source, you must:

- I. Configure Syslog Output on Barracuda WAF
- II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Barracuda WAF

See the procedure below that corresponds to your Barracuda Web Application Firewall version:

- [Configure Barracuda WAF version 7.8.0 and Above](#), or
- [Configure Barracuda WAF version 7.4.0](#)

Configure Barracuda WAF version 7.8.0 and Above

Note: For version 7.8.0 and above, RSA supports Audit, Web Firewall, and Access logs.

1. Log on to the Barracuda Web Application Firewall web interface with administrative credentials.
2. Select **Basic > IP Configuration** from the menu bar.
3. In the **Domain Configuration** section, in the **Default Hostname** field, type **BARRACUDAWAF**.
4. Select **Advanced > Export Logs** from the menu bar.
5. In the **Syslog** section, click **Add Syslog Server** and complete the fields as follows:
 - a. In the **Name** field, enter a descriptive name, for example: **RSA NetWitness Platform**.
 - b. In the **IP Address** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
 - c. In the **Port** field, leave the default value **514**.
 - d. For **Connection Type**, select **UDP**.
 - e. For **Validate Server Certificate**, select **No**.
 - f. For **Client Certificate**, select **No**.

- g. For **Log TimeStamp & Hostname**, select **No**.
 - h. Click **Add**.
6. In the **Logs Format** section, complete the fields as follows:
 - a. In the **Syslog Header** field, select **Custom Header** and leave the text entry field blank.
 - b. In the **Web Firewall Logs Format** field, select **Custom Format** and enter the following string:

```
%un %t %lt %seq %sl %ad %ci %cp %ri %rt %at %fa %adl %m %u %p %ua %px %pp %r
```
 - c. In the **Access Logs Format** field, select **Custom Format** and enter the following string:

```
%un %t %lt %seq %p %m %ci %cp %si %sp %u %cu %id %h %r %s %bs %br %q %c %ua %px %pp %ct
```
 - d. In the **Audit Logs Format** field, select **Custom Format** and enter the following string:

```
%un %t %lt %seq %an %trt %ct %li %tri %cn %ot %on %var %ov %nv
```
 - e. Click **Save Changes**.
7. Close the Barracuda Web Application Firewall Console.

Configure Barracuda Web Application Firewall version 7.4.0

1. Log on to the Barracuda Web Application Firewall web interface with administrative credentials.
2. Select **Basic > IP Configuration** from the menu bar.
3. In the **Domain Configuration** section, in the **Default Hostname** field, type **BARRACUDAWAF**.
4. Select **Advanced > Export Logs** from the menu bar.
5. In the **Syslog** section, complete the fields as follows:
 - a. In the **Name** field, enter a name, for example: RSA NetWitness Platform.
 - b. In the **Syslog Server** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
 - c. In the **Log Time Stamp** field, select **Yes**.

- d. In the **Log Unit Name** field, select **Yes**.
 - e. Click **Add**.
 6. In the **Logs Format** section, complete the fields as follows:
 - a. In the **System Logs Format** field, select **Custom Format** and enter the following string:

```
%t %lt %seq %md %ll %ei %ms
```
 - b. In the **Web Firewall Logs Format** field, select **Custom Format** and enter the following string:

```
%un %t %lt %seq %sl %ad %ci %cp %ri %rt %at %fa %adl %m %u %p %ua %px  
%pp %r
```
 - c. In the **Access Logs Format** field, select **Custom Format** and enter the following string:

```
%un %t %lt %seq %p %m %ci %cp %si %sp %u %cu %id %h %r %s %bs %br %q %c  
%ua %px %pp %ct
```
 - d. In the **Audit Logs Format** field, select **Custom Format** and enter the following string:

```
%un %t %lt %seq %an %trt %ct %li %tri %cn %ot %on %var %ov %nv
```
 - e. Click **Save Changes**.
 7. Close the Barracuda Web Application Firewall Console.

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 **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 **barracudawaf**.



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.

Copyright © 2018 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.