

RSA NetWitness Platform

Event Source Log Configuration Guide



F5 Big-IP Application Security Manager

Last Modified: Wednesday, December 16, 2020

Event Source Product Information:

Vendor: [F5](#)

Event Source: F5 Big-IP Application Security Manager

Versions: 10.2.0, 11.2, 11.5.x, 11.6, 13.x, 14.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: bigipasm

Collection Method: Syslog

Event Source Class.Subclass: Security.Application Firewall

To configure the F5 Big-IP Application Security Manager event source, you must:

- I. Configure Syslog Output on F5 Big-IP Application Security Manager
- II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on F5 Big-IP Application Security Manager

To configure Big-IP Application Security Manager to work with the RSA NetWitness Platform, you must complete these tasks:

- I. Create a logging profile, depending on your version
- II. For version 11.5 and higher, Create a new security profile
- III. Activate the logging profile

Create a logging profile

Use the procedure that corresponds to your version:

- [Create Logging Profile for v 11.5 and higher](#)
- [Create Logging Profile for v 10.2 and 11.2](#)

Create Logging Profile for v 11.5 and higher

To create the logging profile for version 11.5 and higher:

1. Log on to the Big-IP web UI.
2. **Select Security > Event Logs > Logging Profiles.**
3. Click **Create**.
4. In the **Profile Name** field, enter the logging profile name.
5. For the **Application Security** field, select **Enabled**.
6. From the **Configuration List**, select **Advanced**.
 - a. For **Remote Storage**, select **Enabled**.
 - b. For **Remote Storage Type**, select **Arc Sight**.
 - c. From the **Protocol** list, select **TCP** or **UDP**.

- d. In the **Server IP** field, type the IP address of the RSA NetWitness Log Decoder or Remote Log Collector and click **Add**.
7. Select **Report Detected Anomalies**.
8. From the **Request Type** list, select **All Requests**.
9. Click **Create**.

Create Logging Profile for v 10.2 and 11.2

To create the logging profile for versions 10.2.0 and 11.2:

1. Log on to the Big-IP web UI.
2. Select **Application Security > Options > Logging Profiles**.
3. Click **Create**.
4. From the **Configuration** list, select **Advanced**.
5. In the **Profile Name** field, enter the logging profile name.
6. (Optional) In the **Profile Description** field, enter a description of the logging profile.
7. Select **Remote Storage**.
8. From the **Type** list, select **Arc Sight**.

Note: In version 11.2, the **Type** list is called **Remote Storage Type**.

9. From the **Protocol** list, select **TCP** or **UDP**.
10. In the **Server IP** field, type the IP address of the RSA NetWitness Log Decoder or Remote Log Collector and click **Add**.
11. Select **Guarantee Logging**.

Note: In version 11.2, please skip step 11. The **Guarantee Logging** button does not exist in version 11.2.

12. Select **Report Detected Anomalies**.
13. From the **Request Type** list, select **All Requests**.
14. Click **Create**.

Create a new Security Policy for version 11.5 and higher

To create a new Security Policy for version 11.5 and higher:

1. In the **Main** tab, click **Security > Application Security > Security Policies**.
2. Click **Create**.
3. Modify the policy as per your organization's needs.

Activate the logging profile

See the procedure that applies to your F5 Big-IP ASM version:

- [Active Logging Profile for Version 11.5 and higher](#)
- [Active Logging Profile for Version 11.2](#)
- [Active Logging Profile for Version 10.2](#)

Active Logging Profile for Version 11.5 and higher

To activate the logging profile in version 11.5 and higher:

1. On the **Main** tab, click **Local Traffic > Virtual Servers**.
2. Select the virtual server from which you want to collect logs.
3. In the **Security** tab, select **Policies**.
 - a. Set **Application Security Policy** to **Enabled**.
 - b. Select the policy you have previously created.
 - c. Set **Log Profile** to **Enabled** and select the Log Profile you previously created.
 - d. Click **Update**.

Active Logging Profile for Version 11.2

To activate the logging profile in version 11.2:

1. On the **Main** tab, click **Application Security > Security Policies**.
2. Click the name of the security policy.

Note: The security policy is created on the F5 Big-IP Application Security Manager interface. If there are no security policies currently defined, you can create them using Big-IP Application Security Manager.

3. For **Logging Profile**, select the profile you want to use for the security policy.
4. Click **Save**.
5. Click **Apply Policy**.

Active Logging Profile for Version 10.2

To activate the logging profile in version 10.2:

1. Select **Application Security > Web Applications > Web Applications List**.
2. From the **Web Applications** list, select the web application that you want to update.
3. From the **Logging Profile** list, select the logging profile.
4. Click **Update**.

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 **bigipasm**.



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.

© 2020 RSA Security LLC or its affiliates. All Rights Reserved.

November 2020

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.