

RSA NetWitness Platform

Event Source Log Configuration Guide



F5 Big-IP Access Policy Manager

Last Modified: Monday, October 4, 2021

Event Source Product Information:

Vendor: [F5](#)

Event Source: Big-IP Access Policy Manager

Versions: 10.2.0, 11.4 HF4, 11.5.2 HF1, 15.x , 16.x

RSA Product Information:

Supported On: NetWitness Platform 11.0 and later

Event Source Log Parser: bigipapm

Collection Method: Syslog

Event Source Class.Subclass: Security.Access Control

To configure the F5 Big-IP Access Policy Manager event source, you must:

- I. Configure Syslog Output on F5 Big-IP Access Policy Manager
- II. Configure NetWitness Platform for Syslog Collection

Configure Syslog Output on F5 Big-IP Access Policy Manager

Configure Big-IP APM version 11.4 , 15.x and 16.x

You use the F5 Big-IP Configuration Utility from within a web browser to configure Big-IP APM version 11.4, 15.x and 16.x.

To configure Big-IP APM v 11.4, v 15.x and v 16.x to work with RSA NetWitness Platform:

1. Open a browser window, and log onto the F5 Big-IP Configuration Utility.
2. From the left navigation pane, select the **Main** tab.
3. Select **System > Logs > Configuration > Remote Logging**.
4. In the **Properties** section, in the **Remote IP** field, enter the IP address of your RSA NetWitness Platform Log Decoder or RSA NetWitness Platform Remote Log Collector.
5. Click **Add**, then **Update**.
6. Log out of the Configuration console.

Configure Big-IP APM version 10.2

You use the command line to configure Big-IP APM version 10.2.

To configure Big-IP APM v 10.2 to work with RSA NetWitness Platform:



1. Use an SSH client to access the Big-IP device.
2. Type `root` and press **Enter**.
3. Enter the Big-IP password.
4. Type `bssh` and press **Enter**.
5. Type `syslog remote server add host <Platform_IP>`, where `<Platform_IP>` is the IP address of your RSA NetWitness Platform Log Decoder or RSA NetWitness Platform Remote Log Collector., and press **Enter**.
6. Type `exit` and press **Enter**.
7. Type `service syslog-ng stop` and press **Enter**.
8. Type `service syslog-ng start` and press **Enter**.

Configure NetWitness Platform for Syslog Collection

Note: Syslog collection must be configured only for the first time when you set up an event source which uses Syslog to send its output to NetWitness.

For Syslog, configure either the Log Decoder or the Remote Log Collector. You do not need to configure both.

Log Decoder Configuration Steps for Syslog Collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the **Services** grid, choose 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.

Remote Log Collector Configuration Steps for Syslog Collection:

1. In the **NetWitness** menu, go to **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 will appear.
5. Choose either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Choose the **New Type** in the **Event Categories** panel and click **+** in the **Sources** panel toolbar.

The **Add Source** dialog will appear.
7. Enter **514** for the port, and choose **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.

© 2021 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.