RSA NetWitness Platform

Event Source Log Configuration Guide

F5 Big-IP Local Traffic Manager

Last Modified: Tuesday, November 20, 2018

Event Source Product Information:

Vendor: F5
Event Source: Big-IP Local Traffic Manager
Versions: 9.4, 10.2.0, 11.x, 12.x, 13.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: bigip
Collection Method: Syslog
Event Source Class.Subclass: Network.Switch

To configure the F5 Big-IP Local Traffic Manager event source, you must:

I. Configure Syslog Output on F5 Big-IP Local Traffic Manager

II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on F5 Big-IP Local Traffic Manager

The following procedures describes how to configure Syslog output on your device.

The RSA NetWitness Platform supports several versions of Big-IP Local Traffic Manager in addition to iRule scripting. Use the appropriate set of instructions for your version:

- Configure Big-IP Local Traffic Manager version 11.x, 12.x, or 13.x
- Configure Big-IP Local Traffic Manager version 10.2.0
- Configure Big-IP Local Traffic Manager version 9.4
- Configure iRule support for Big-IP Local Traffic Manager

Configure Big-IP Local Traffic Manager version 11.x, 12.x, or 13.x

To configure Big-IP Local Traffic Manager version 11.x and 12.x:

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 **tmsh**, and press ENTER.
5. Type the following:

   ```
   modify /sys syslog remote-servers add { <config_name> { host <Platform_IP> remote-port 514 } }
   ```

   where <*config_name*> is the name for the syslog event source you are adding and <*Platform_IP*> is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
6. Type **list /sys syslog remote-servers** and press ENTER.
7. Confirm that your RSA NetWitness Platform has been configured correctly.
8. Type **stop sys service all** and press ENTER

9. Type **start sys service all** and press ENTER
10. Type **quit**, and press ENTER.

Configure Big-IP Local Traffic Manager version 10.2.0

To configure Big-IP Local Traffic Manager version 10.2.0:

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 **bpsh**, and press ENTER.
5. Type the following:

   ```
   syslog remote server add host <Platform_IP>
   ```

   where *<Platform_IP>* is the IP address of the RSA NetWitness Log Decoder or 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 Big-IP Local Traffic Manager version 9.4

To configure Big-IP Local Traffic Manager version 9.4:

1. Log on to the command line.
2. Change directories to the **/etc/syslog-ng/** directory by typing the following command:

   ```
   cd /etc/syslog-ng/
   ```
3. Back up the current **syslog-ng.conf** file by typing the following command:

   ```
   cp syslog-ng.conf syslog-ng.conf.original
   ```
4. Use a text editor to open the **syslog-ng.conf** file.
5. Add the following to the end of the **syslog-ng.conf** file:

   Note: Replace x.x.x.x with the the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

```
# Direct all log information to remote syslog server
destination remote_server {
udp("x.x.x.x" port (514));
};
filter f_alllogs {
level (debug...emerg);
};
log {
source(local);
filter(f_alllogs);
destination(remote_server);
};
```

6. Save the changes to the file.
7. Run the following command to retain your changes to the **syslog-ng.conf** file after restarting:

   ```
   bigpipe
   ```

8. Restart the **syslog-ng** utility by typing the following command:

   ```
   bigstart restart syslog-ng
   ```

Configure iRule support for Big-IP Local Traffic Manager

The RSA NetWitness Platform supports up to eight iRule commands. The iRule log function must adhere to a `name=value` format, where each `name=value` pair is delimited by a double-caret (^^). The following is the general syntax of an iRule:

`log local0. "iRule name1=[value1]^^name2=[value2]^^name3=[value3]^^name4=[value4]"`

Below is a table charting variable names to iRule commands that are currently supported by the RSA NetWitness Platform:

Static Variable	iRule Command
c-ip	IP::client_addr
method	HTTP::method
uri	HTTP::uri
host	HTTP::host
s-ip	LB::server addr
pool-name	LB::server pool

Static Variable	iRule Command
s-port	LB::server port
status	HTTP::status

The following is a sample iRule that uses all of the supported RSA NetWitness Platform variables:

```
log local0. "iRule c-ip=[IP::client_addr]^^method=[HTTP::method]^^uri=
[HTTP::uri]^^host=[HTTP::host]^^s-ip=[LB::server addr]^^pool-name=
[LB::server pool]^^s-port=[LB::server port]^^status=[HTTP::status]"
```

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 **bigip**.

Configure Syslog Collection

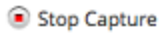
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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 

, click the icon to start capturing Syslog.
- If you see 

, 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.