RSA NetWitness Logs

Event Source Log Configuration Guide

IBM AIX

Last Modified: Thursday, November 2, 2017

Event Source Product Information:

Vendor: IBM
Event Source: AIX
Versions: 5L (Security and Authentication messages only), 6.1, 7.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 Suite 10.0 and later
Event Source Log Parser: aix
Collection Method: Syslog
Event Source Class.Subclass: Host.UNIX

To configure the IBM AIX event source, you must:

I. Configure Syslog Output on IBM AIX

II. Configure RSA NetWitness Suite for Syslog Collection

Configure Syslog Output on IBM AIX

To configure Syslog output on IBM AIX:

1. Open the **/etc/syslog.conf** file in a text editor.
2. To log all messages of debug level and higher to the RSA NetWitness Suite, add the following lines:
   - `auth.debug @xxx.xxx.xxx.xxx`
   - `daemon.debug @xxx.xxx.xxx.xxx`
   - `kern.debug @xxx.xxx.xxx.xxx`
   - `user.debug @xxx.xxx.xxx.xxx`

     where *xxx.xxx.xxx.xxx* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
3. Save the file and close the text editor.
4. To restart the syslog daemon, run the following command:

   ```
   refresh -s syslogd
   ```

Warning: Do not use the **-n** flag when starting the syslogd daemon. This flag suppresses logging of priority and facility information for each log message. If this flag is used, RSA NetWitness Suite cannot recognize AIX messages.

(Optional) Track Changes to the Syslog.conf File

To track the changes to the syslog.conf file, you must complete these tasks:

I. Configure System Logging

II. Configure the Audit Process

Note: This step is optional. Only perform these tasks if you want to track the changes to the syslog.conf file.

Configure System Logging

To configure system logging to track changes to the Syslog.conf file:

1. Open the **/etc/syslog.conf** file in a text editor.
2. To log all messages from the syslog.conf file, add the following lines:

   ```
   *.debug @xxx.xxx.xxx.xxx
   ```

   where *xxx.xxx.xxx.xxx* is .the IP address of the RSA NetWitness Log Decoder or Remote Log Collector
3. Save the file and close the text editor.
4. To restart the syslog daemon, run the following command:

   ```
   refresh -s syslogd
   ```

Configure the Audit Process

To configure the Audit process to track changes to the Syslog.conf file:

1. Log on to your AIX machine.
2. Open the file named **/etc/security/audit/objects** in a text editor.
   a. In the **/etc/security/audit/objects** file, add this line:

   ```
   /etc/syslog.conf
         w = "SYSLOG_WRITE"
   ```

Note: The tag "SYSLOG_WRITE" must be copied exactly. No other tags will be parsed.

b. Save the changes.

3. In the **objects** section, open the file named **/etc/security/audit/events**.

   a. In the **/etc/security/audit/events** file, add this line:

   ```
   *Tab/etc/syslog.conf
   /etc/syslog.conf
        SYSLOG_WRITE = printf "#s"
   ```

   where *Tab* means press the TAB key.

   b. Save the changes.

4. Open the file named **/etc/security/audit/config**.

   a. In the **Start** tag, confirm this line.

   ```
   binmode = off
   streammode = on
   ```

   b. In the **Stream** tag, confirm this line.

   ```
   cmds = /etc/security/audit/streamcmds
   ```

   c. In the **Classes** section, under general and objects, add

   ```
   SYSLOG_WRITE
   ```

   d. In the **Users** section, define the users to monitor for the audit events. For example,

   ```
   root = general
   name = general
   ```

   where *name* is a user name.

   e. Save the changes.

5. Open the file named **/etc/security/audit/streamcmds**.

   a. Comment out the first statement.

   ```
   #/usr/sbin/auditstream | auditpr >
   ```

```
/audit/stream.out &
```

b. Add the following statement.

```
/usr/sbin/auditstream | auditpr -v | grep
SYSLOG | /usr/bin/logger -p local0.debug &
```

c. Save the changes.

6. Start the audit system.

```
/usr/sbin/audit start
```

7. Check if the audit system is running.

```
/usr/sbin/audit query
```

a. After the query runs, at the beginning of the output, confirm this line.

```
auditing on
bin processing off
```

b. Under **audit objects**, confirm this line.

```
/etc/syslog.conf
     w = SYSLOG_WRITE
```

8. To restart the syslog daemon, run the following command.

```
refresh -s syslogd
```

9. If you do not observe logs in real time, you must shut down the audit system and start it again by running these commands.

a. Shut down the audit system.

```
/usr/sbin/audit shutdown
```

b. Start the audit system.

```
/usr/sbin/audit start
```

c. Restart the syslog daemon.

```
refresh -s syslogd
```

Configure RSA NetWitness Suite

Perform the following steps in RSA NetWitness Suite:

- 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 Suite 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 **aix**.

Configure Syslog Collection

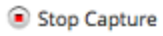
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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.

Trademarks