RSA NetWitness Platform

Event Source Log Configuration Guide

Apache HTTP Server

Last Modified: Wednesday, November 25, 2020

Event Source Product Information:

Vendor: Apache
Event Source: HTTP Server
Versions: 2.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.

Additional Downloads: sftpagent.conf.apache, nicsftpagent.conf.apache

Link: Apache HTTP Server Additional Downloads

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: apache
Collection Method: File, Syslog
Event Source Class.Subclass: Host.Web Logs

Apache HTTP Server

You can configure Apache HTTP Server depending on your operating system. Configure Apache HTTP Server as follows:

- Configure File collection
  - Configure Apache HTTP Server for Windows
  - Configure Apache HTTP Server for Unix
  - Set Up the SFTP Agent
  - Configure the Log Collector for File Collection
- Configure Syslog collection (Unix/Linux only)
  - Configure Syslog collection on Apache
  - Configure NetWitness Platform for Syslog Collection

Note: For Apache HTTP Server, you can choose to configure Syslog or File collection, but not both.

Warning: RSA prefers the use of the new logging format for configuring Apache HTTP Server for Windows and Unix.

Configure File Collection

RSA supports file collection for Windows and UNIX. Choose the appropriate steps for your Operating System.

- Configure File Collection on Windows
- Configure File Collection on UNIX

Configure File Collection on Windows

To configure File collection for Apache HTTP Server on Windows:

Depending on your logging format, do one of the following:

- For the new form of logging, verify that the following script is present (and not commented out) in the **httpd.conf** file on the Apache server:

```
LogFormat "%h %l %u %t \"%m \"%V\" \"%U\" \"%q\" %H\" %>s %b \"%
{Referer}i\" \"%{User-Agent}i\" \"%{Cookie}i\"" custom
 CustomLog '|"C:/Program Files/Apache Software
Foundation/Apache2.2/bin/rotatelogs.exe" "logs/access.log" 86400' custom
```

  where *86400* represents the number of seconds to keep the current log file open before rotating it and starting a new log.

  Note: The location of the **rotatelogs.exe** file may vary.

- For an earlier logging format, verify that the following script is present (and not commented out) in the **httpd.conf** file on the Apache server:

```
LogFormat "%h %l %u %t %r %>s %b" common
CustomLog '|"C:/Program Files/Apache Group/Apache2/bin/rotatelogs.exe"
"logs/access_log" 86400' common
```

  where *86400* represents the number of seconds to keep the current log file open before rotating it and starting a new log.

Note: These scripts create a log file called ***access_log<timestamp>*** when the log file is rotated. These are the logs that are sent to the RSA NetWitness Platform server via FTP. The RSA NetWitness Platform File service reads the files.

Configure File Collection on UNIX

To configure File Collection for Apache HTTP Server on UNIX:

Depending on your logging format, do one of the following:

- For the new form of logging, verify that the following lines are present (and not commented out) in the **apache2.conf** file on the Apache server:

  ```
  LogFormat "%h %l %u %t \"%m \"%V\" \"%U\" \"%q\" %H\" %>s %b \"%
  {Referer}i\" \"%{User-Agent}i\" \"%{Cookie}i\"" custom
  CustomLog "|/usr/sbin/rotatelogs /var/log/access.log 86400" custom
  ```

  where *86400* represents the number of seconds to keep the current log file open before rotating it and starting a new log.

- For an earlier form of logging, verify the following lines are present (and not commented out) in the **httpd.conf** file on the Apache server:

  ```
  LogFormat "%h %l %u %t %r %>s %b" common CustomLog
  "|/usr/local/apache/bin/rotatelogs /var/log/access_log 86400" common
  ```

  where *86400* represents the number of seconds needed to keep the current log file open before rotating it and starting a new log.

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see Install and Update SFTP Agent
- To set up the SFTP agent on Linux, see Configure SFTP Shell Script File Transfer

Configure the Log Collector for File Collection

Perform the following steps to configure the Log Collector for File collection.

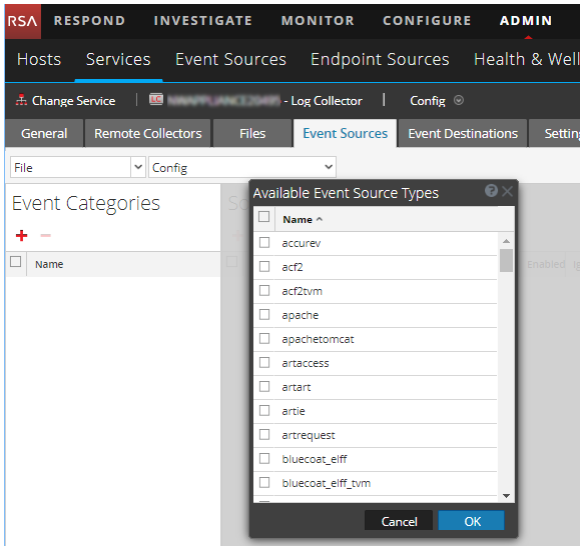
To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **File/Config** from the drop-down menu.

   The Event Categories panel displays the File event sources that are configured, if any.

4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.

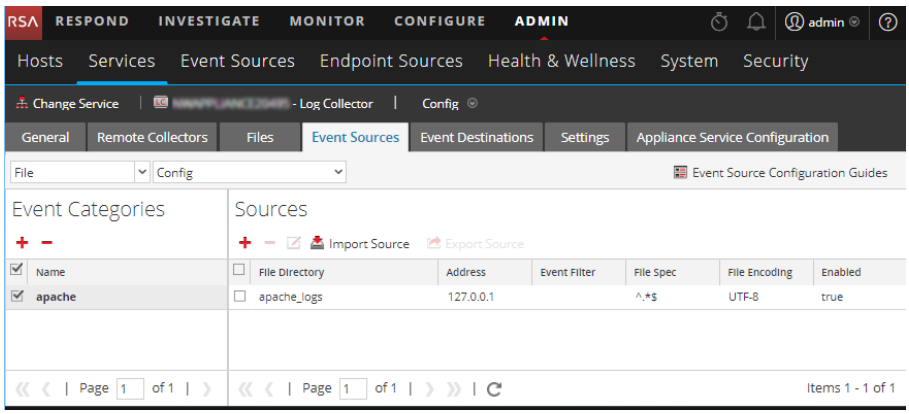


5. Select the correct type from the list, and click **OK**.

   Select **apache** from the **Available Event Source Types** dialog.

   The newly added event source type is displayed in the Event Categories panel.

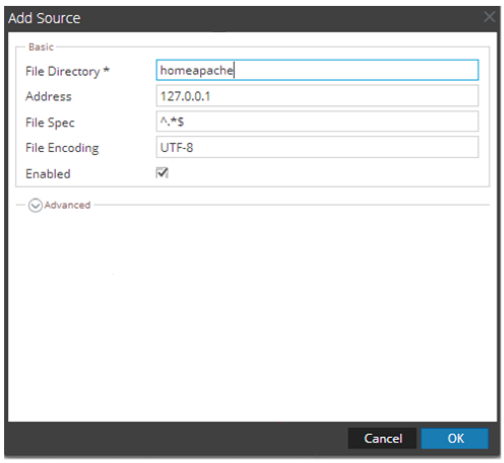
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

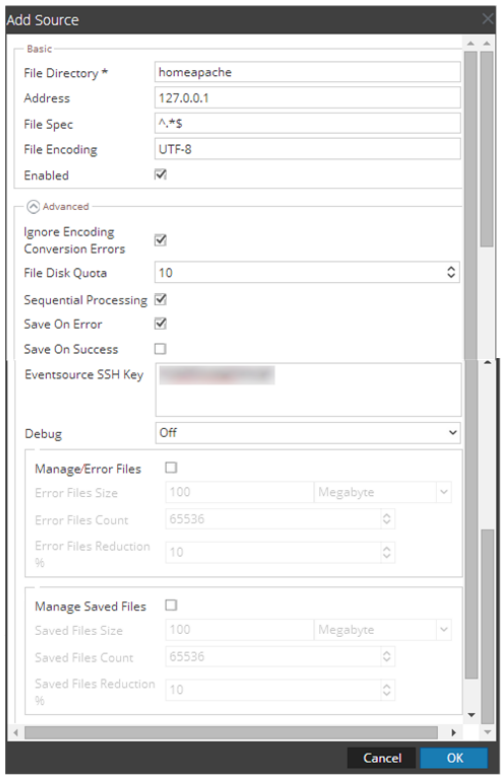


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.

   Note: Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.





7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.

8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Configure Syslog Collection for Apache HTTP Server on UNIX

For Apache HTTP Server, RSA supports syslog collection only for UNIX.

To configure Syslog Collection for Apache HTTP Server:

1. Open the **/etc/httpd/conf/httpd.conf** file, and find several lines that begin with **LogFormat**. Add the following line after the final **LogFormat** line:

   ```
   LogFormat "\"%m: %h %l %u %t \"%m \"%V\" \"%U\" \"%q\" %H\" %>s %b \"%
   {Referer}i\" \"%{User-Agent}i\" \"%{Cookie}i\"" rsa
   ```

   Note: The above line appears on two lines in this document, but you should add it as a single line into the **httpd.conf** file.

2. Find the following line:

   ```
   CustomLog logs/access_log combined
   ```

   and replace `combined` with `rsa`, so that the line reads as follows:

   ```
   CustomLog logs/access_log rsa
   ```

3. Add the following lines to the end of the **/etc/rsyslog.conf** file:

   ```
   #### MODULES ####

   $ModLoad imfile # load the imfile input module
   # Watch /var/log/httpd/access_log
   $InputFileName /var/log/httpd/access_log
   $InputFileTag %APACHE-
   $InputFileStateFile state-apache-access
   $InputRunFileMonitor
   *.* @ipaddress
   ```

   where ***ipaddress*** is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector

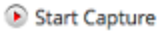
4. Restart the **httpd** and **rsyslog** services.

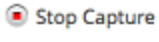
Configure NetWitness Platform for Syslog Collection

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 

, 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 **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.

Warning: This configuration will eventually make the log file grow, fill the file system, and eliminate the web server. To prevent this, provision needs to be made to rotate the log file.

November 2020

Trademarks