RSA NetWitness Logs

Event Source Log Configuration Guide

Radiator Radius Server

Last Modified: Thursday, November 2, 2017

Event Source Product Information:

Vendor: Radiator
Event Source: Radius Server
Versions: 4.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.radiator

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: radiator
Collection Method: File
Event Source Class.Subclass: Security.Access Control

Configure Radiator Radius Server

To configure Radius, you must complete these tasks:

I. Configure Radiator to generate logs

II. Set Up the SFTP Agent

III. Set up the File Service

Configure Radiator Radius Server to generate logs

1. Load the **LogFormat** module. This module comes with the Radiator StartupHook subroutine (requires **Radius::LogFormat**).

2. Define **AuthLog** (uses the CEF formatter).

```
<AuthLog FILE>

   Identifier myauthlogger-cef
   Filename %L/authlog.cef
   LogFormatHook sub { Radius::LogFormat::format_
authlog_cef(@_); }
   LogSuccess 1
   LogFailure 1

</AuthLog>
```

   This logs both successes and failures to a file in CEF # compliant format.

3. Define a handler to use the CEF Authlogger. For example:

```
<Handler>

   <AuthBy FILE>

      :
      :

   </AuthBy>

   # Log authentication success and failure to files

   AuthLog myauthlogger-cef

</Handler>
```

With these instructions, a file named **authlog.cef** is created in the log directory. The file will contain authentication log messages in CEF format.

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

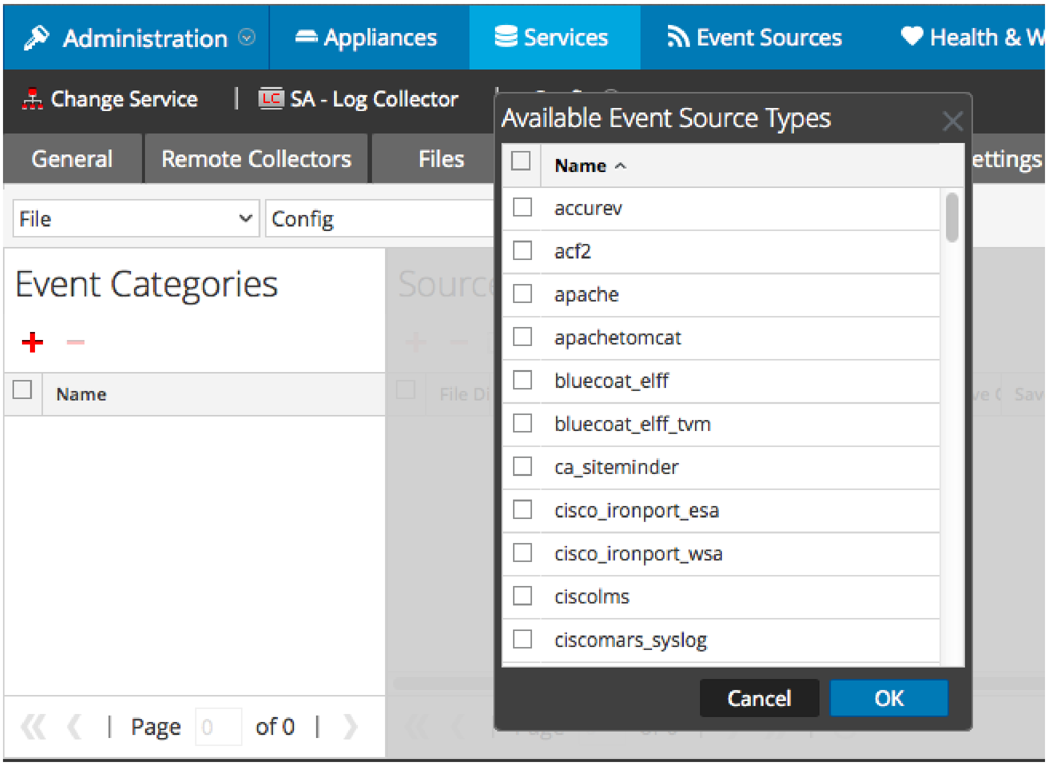
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **Administration** > **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.



Available Event Source Types

File

□	Name ^
□	accurev
□	acf2
□	apache
□	apachetomcat
□	bluecoat_elff
□	bluecoat_elff_tvm
□	ca_siteminder
□	cisco_ironport_esa
□	cisco_ironport_wsa
□	ciscolms
□	ciscomars_syslog

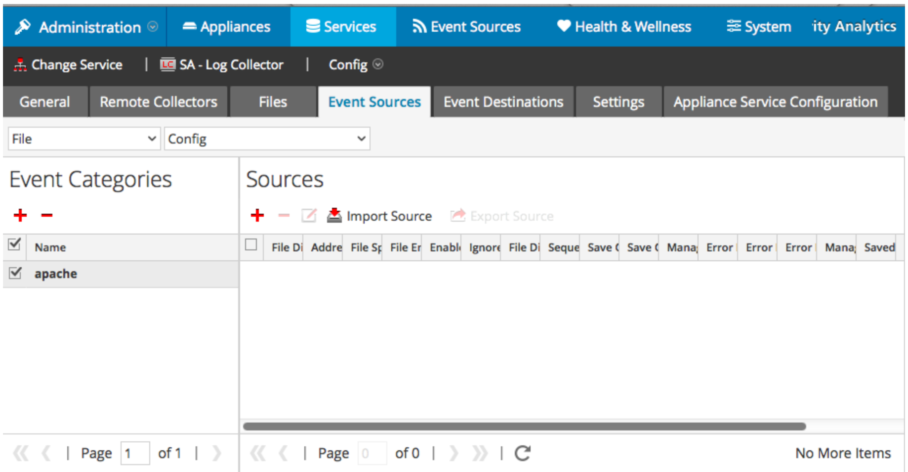
Cancel OK

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

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

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

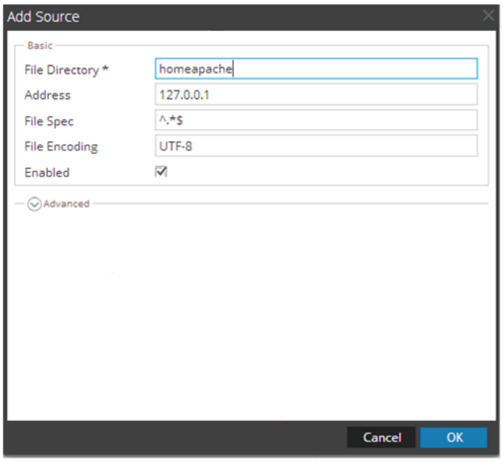
> **Note:** The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



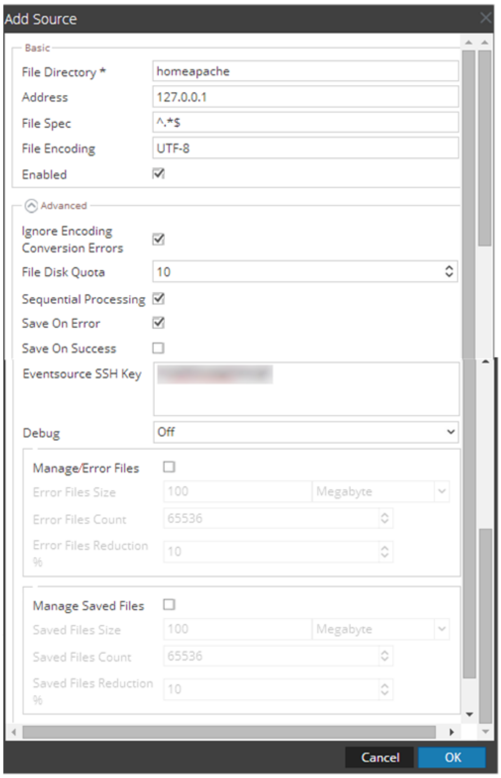
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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.



File Directory * homeapache
Address 127.0.0.1
File Spec ^.*$
File Encoding UTF-8
Enabled ☑



File Directory * homeapache
Address 127.0.0.1
File Spec ^.*$
File Encoding UTF-8
Enabled ☑
Ignore Encoding Conversion Errors ☑
File Disk Quota 10
Sequential Processing ☑
Save On Error ☑
Save On Success ☐
Eventsource SSH Key [redacted]
Debug Off
Manage/Error Files ☐
Error Files Size 100 Megabyte
Error Files Count 65536
Error Files Reduction % 10
Manage Saved Files ☐
Saved Files Size 100 Megabyte
Saved Files Count 65536
Saved Files Reduction % 10

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.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.