RSA NetWitness Platform

Event Source Log Configuration Guide

Accurev

Last Modified: Tuesday, January 14, 2020

Event Source Product Information:

Vendor: Accurev
Event Source: Accurev
Versions: 6.0.1
Additional Downloads:

- sftpagent.conf.accurev
- passwdConfig.pl
- passwdUtils.pl
- server_admin_trig.pl
- server_user_utilities.pl
- server_utilities triggers.pl
- server_auth_trig.pl

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: accurev
Collection Method: File
Event Source Class.Subclass: Storage.Content Management Systems

Configure Accurev

To configure Accurev, you must complete these tasks:

I. Configure Accurev to generate logs

II. Set Up the SFTP Agent

III. Set up the File Service

Configure Accurev to generate logs

1. Create a **triggers** directory inside the `storage/site_slice` directory.
2. Use a browser to navigate to the Accurev Additional Downloads page in the RSA® NetWitness® Platform Event Source Downloads space.
3. Download the following trigger PERL scripts and copy them into the **triggers** directory that you created in step 1.
   - server_auth_trig.pl
   - passwdConfig.pl
   - passwdUtils.pl
   - server_admin_trig.pl
   - server_user_utilities.pl
   - server_utilities triggers.pl
4. Change the extension for the files based on your OS. For example, rename **server_auth_trig.pl** as follows:
   - Linux/UNIX: leave as **server_auth_trig.pl**, or rename to **server_auth_trig**
   - Windows: rename to **server_auth_trig.bat**
5. In the same manner, change the extensions for the other files.

   For example on Windows, you might have the following path for **server_admin_trig.bat**:

   ```
   C:\Program Files\AccuRev\storage\site_slice\triggers\server_admin_
   trig.bat
   ```

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

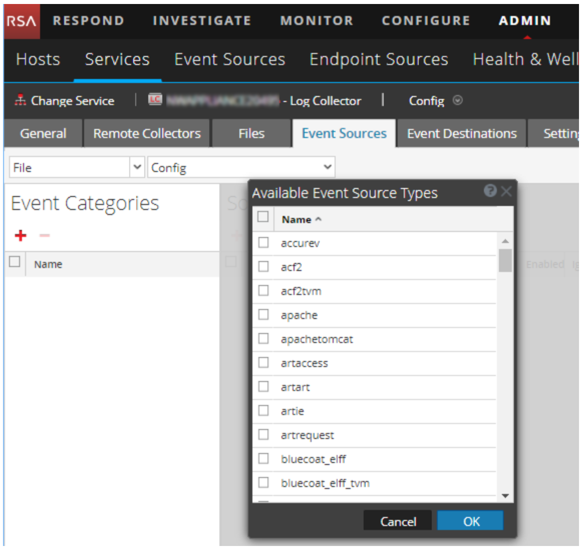
Perform the following steps to configure the Log Collector for File collection.

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.

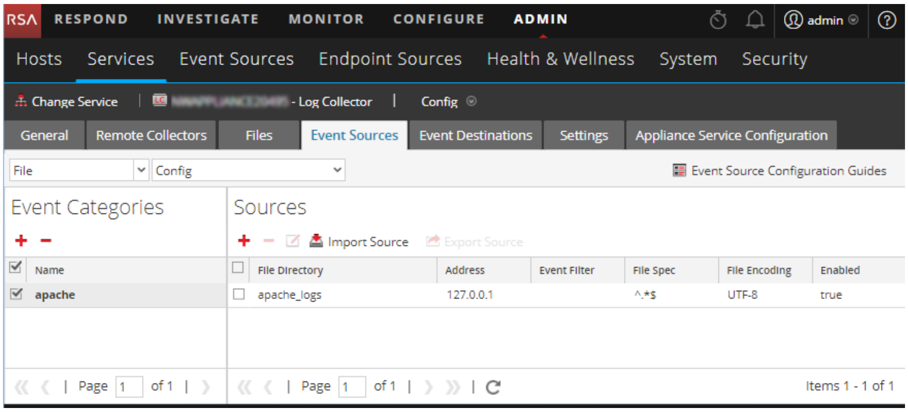


5. Select the correct type from the list, and click **OK**.

   Select **accurev** 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.



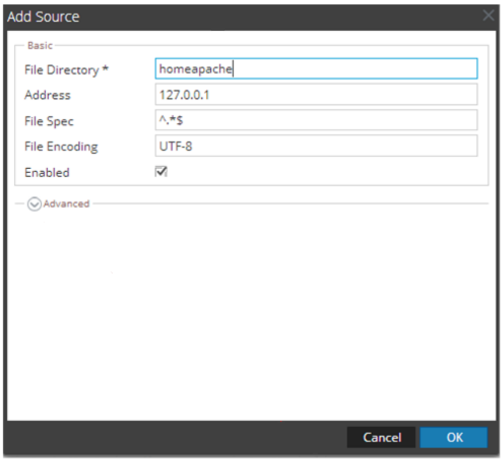
☑	Name
☑	apache

□	File Directory	Address	Event Filter	File Spec	File Encoding	Enabled
□	apache_logs	127.0.0.1		^.*$	UTF-8	true

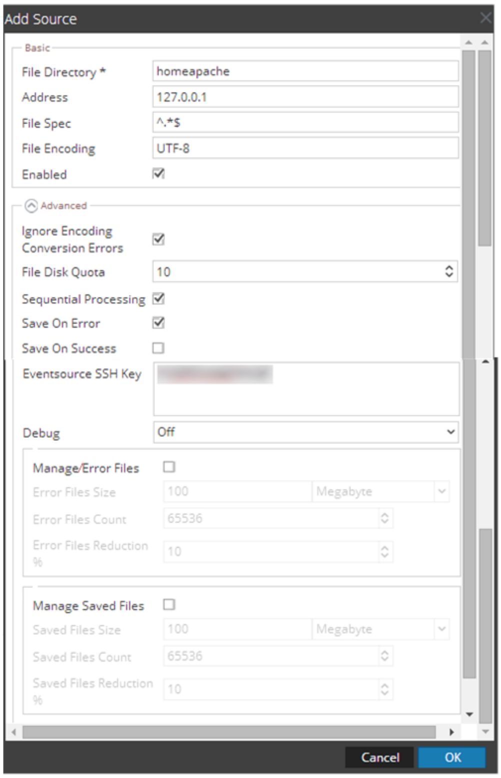
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.