

# RSA NetWitness Logs

## Event Source Log Configuration Guide



## EMC NetWorker

Last Modified: Thursday, June 22, 2017

### Event Source Product Information:

**Vendor:** [EMC](#)

**Event Source:** EMC NetWorker

**Version:** 7.6 SP2

**Additional Download:** `nicstfpageant.conf.emcnetworker`

### RSA Product Information:

**Supported On:** NetWitness Suite 10.0 and later

**Event Source Log Parser:** `emcnetworker`

**Collection Method:** File

**Event Source Class.Subclass:** `Storage.Storage`

To configure EMC NetWorker, you must complete these tasks:

- I. File Locations on EMC NetWorker
- II. Set Up the SFTP Agent
- III. Set up the File Service

## EMC NetWorker File Locations

Events generated in the NetWorker Management Console can be viewed in the Monitor window. These events are stored in **install\_dir\_path\nsr\logs**.

Log file locations of EMC NetWorker:

File	Location
daemon log file	install_dir_path\nsr\logs\daemon.raw
messages	install_dir_path\nsr\logs\messages
networker.raw	install_dir_path\nsr\logs\networker.raw

## 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 SA SFTP Agent shell script](#)

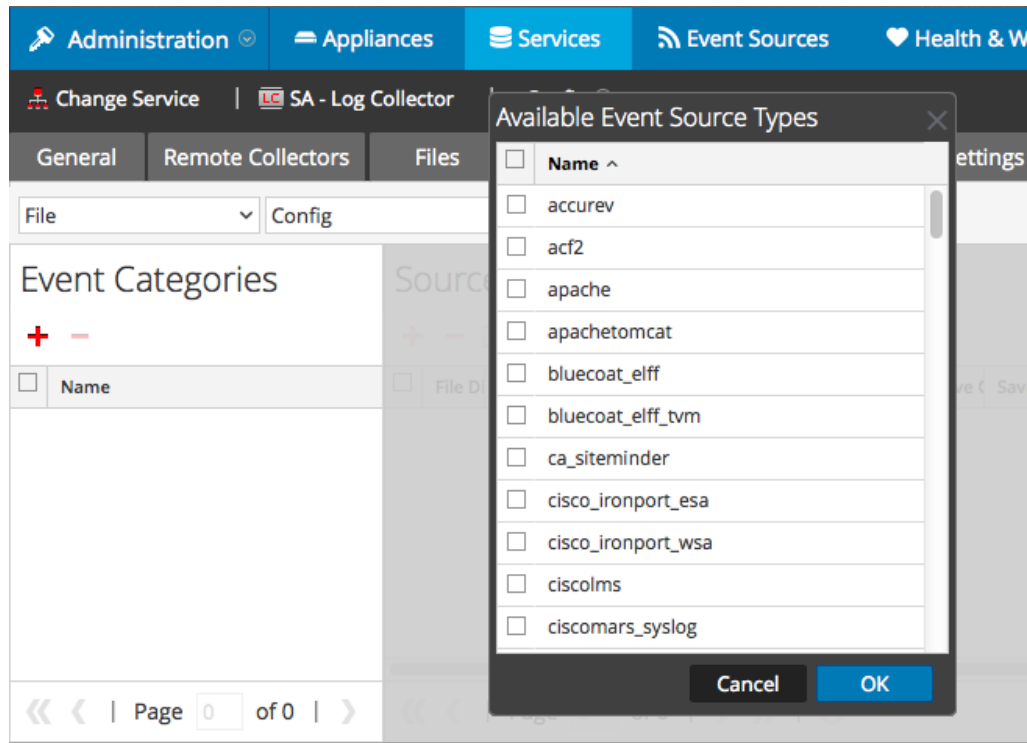
## Configure the Log Collector for File Collection

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 **+**.

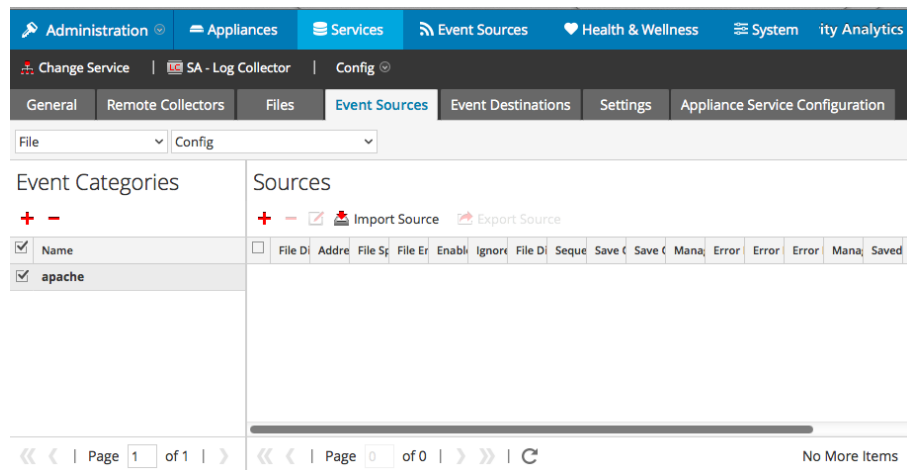
The Available Event Source Types dialog is displayed.



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

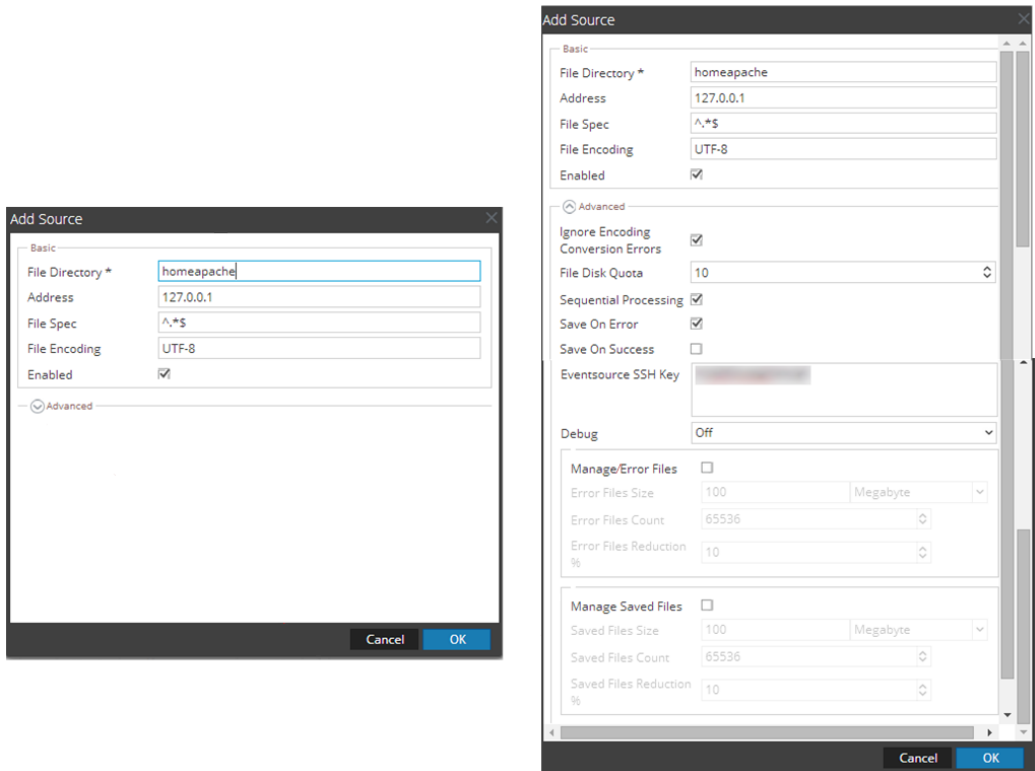
Select **emcnetworker** from the **Available Event Source Types** dialog.

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



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

The Add Source dialog is displayed.



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.

Copyright © 2017 EMC Corporation. All Rights Reserved.

## 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.