RSA NetWitness Logs

Event Source Log Configuration Guide

IBM MQ

Last Modified: Thursday, May 25, 2017

Event Source Product Information:

Vendor: IBM
Event Source: MQ
Versions/Platforms: 7.0.1 / Windows
Additional Downloads: sftpagent.conf.ibmwebspheremq

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: ibmwebspheremq
Collection Method: File
Event Source Class.Subclass: Network.Messaging

About IBM MQ

IBM MQ is IBM's Message Oriented Middleware offering. It was originally called MQSeries, and was renamed WebSphere MQ in 2002 to join the suite of WebSphere products. In April 2014, it was renamed IBM MQ

IBM MQ allows independent and potentially non-concurrent applications on a distributed system to communicate with each other. IBM MQ provides assured one-time delivery of messages across a wide variety of platforms. The product emphasizes reliability and robustness of message traffic, and ensures that a message should never be lost if MQ is appropriately configured.

A message in the context of MQ has no implication other than a gathering of data. MQ is very generalized and can be used as a robust substitute for many forms of intercommunication. For example, it can be used to implement reliable delivery of large files as a substitute for FTP.

Configure NetWitness Suite for File Collection

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

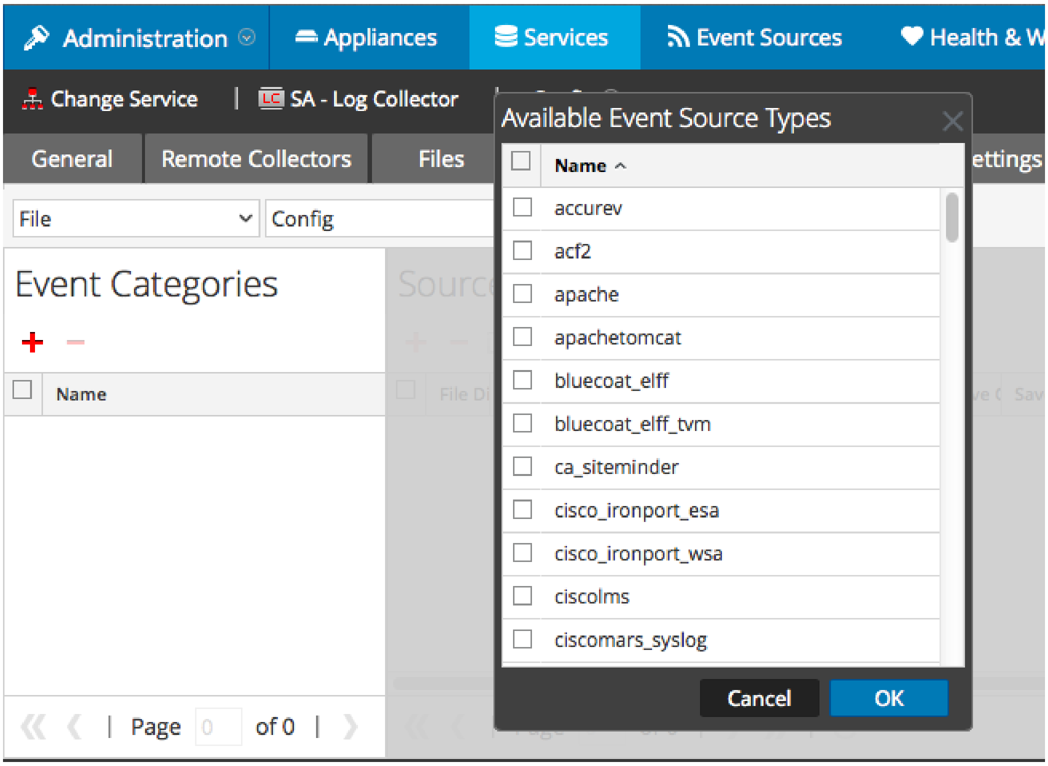
Perform the following steps to configure the Log Collector for File collection.

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 +.

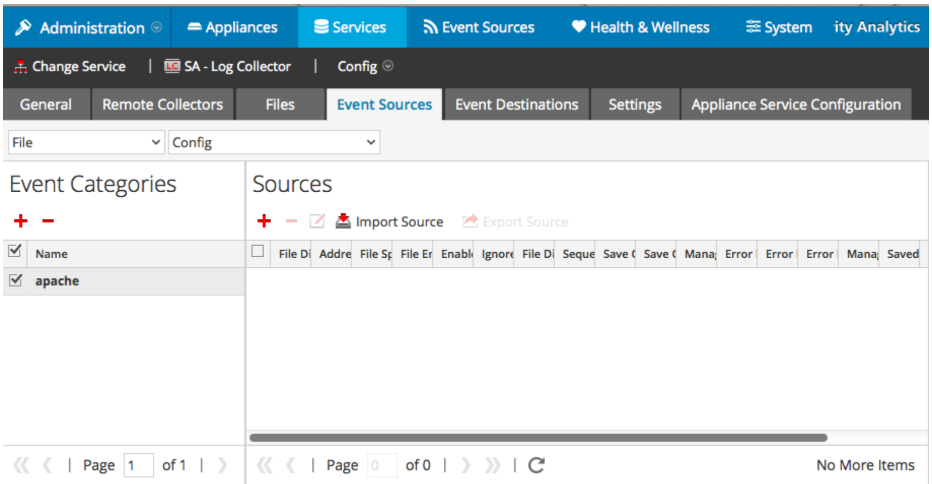
   The Available Event Source Types dialog is displayed.



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

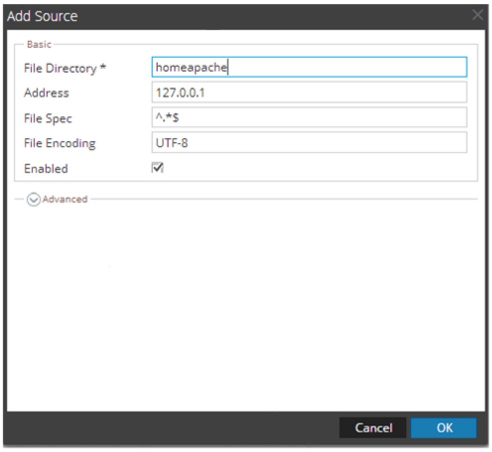
   Select **ibmwebspheremq** from the **Available Event Source Types** dialog.

   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.



Basic

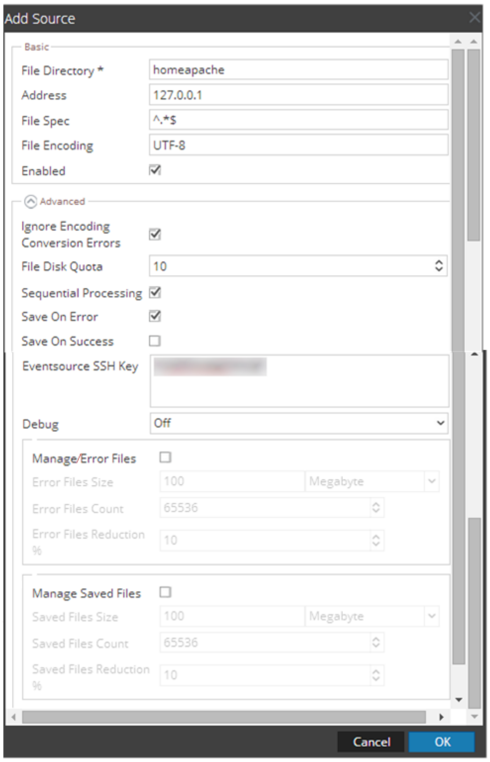
File Directory * homeapache

Address 127.0.0.1

File Spec ^.*$

File Encoding UTF-8

Enabled ☑



Basic

File Directory * homeapache

Address 127.0.0.1

File Spec ^.*$

File Encoding UTF-8

Enabled ☑

Advanced

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.