RSA NetWitness Logs

Event Source Log Configuration Guide

EMC Greenplum HD

Last Modified: Thursday, August 10, 2017

Event Source Product Information:

Vendor: EMC
Event Source: Greenplum HD
Version: 1.2

Supported Platforms: CentOS / Linux / UNIX

Additional Download: nicsftpagent.conf.greenplumhd

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: greenplumhd
Collection Method: File
Event Source Class.Subclass: Storage.Storage

Configure Greenplum HD

To configure Greenplum HD, you must complete these tasks:

I. Configure Greenplum HD to generate logs

II. Set Up the SFTP Agent

III. Set up the File Service

Configure Greenplum HD to generate logs

To configure Greenplum HD, you must configure the **log4j.properties** files to send syslog messages to RSA NetWitness Suite.

To configure the log4j.properties file in Greenplum HD:

1. Locate the **log4j.properties** file. The default location is **/etc/gphd/hadoop/conf/log4j.properties**.
2. Open the **log4j.properties** file, and change the line

   ```
   log4j.logger.org.apache.hadoop.hdfs.server.namenode.FSNamesystem.audit=WARN
   ```

   to

   ```
   log4j.logger.org.apache.hadoop.hdfs.server.namenode.FSNamesystem.audit=INFO
   ```

   Note: This changes the event auditing from the WARN level to the INFO level.

3. Add the following lines to the **log4j.properties** file:

   ```
   #
   # HDFS Audit Logging for NetWitness
   #
   #Log at INFO level to DRFAAUDIT appender
   hdfs.audit.logger=INFO,DRFAAUDIT
   log4j.logger.org.apache.hadoop.hdfs.server.namenode.FSNamesystem.audit=INFO,DRFAAUDIT
   #Do not forward audit events to parent appenders (i.e. Namenode)
   log4j.additivity.org.apache.hadoop.hdfs.server.namenode.FSNamesystem.audit=false
   #Configure local appender
   ```

```
log4j.appender.DRFAAUDIT=org.apache.log4j.DailyRollingFileAppender

log4j.appender.DRFAAUDIT.File=/var/log/gphd/hadoop/hdfs-audit.log

log4j.appender.DRFAAUDIT.layout=org.apache.log4j.PatternLayout

log4j.appender.DRFAAUDIT.layout.ConversionPattern=%d{ISO8601} %p %c{2}: %m%n

log4j.appender.DRFAAUDIT.DatePattern=.yyyy-MM-dd

#
```

4. Save your changes to the **log4j.properties** file.

5. Restart services on the NameNode by entering the following in a command line shell:

   ```
   service hadoop-namenode stop

   service hadoop-namenode start
   ```

   or

   ```
   service hadoop-namenode restart
   ```

6. Restart services on the DataNode by entering the following in a command line shell:

   ```
   service hadoop-datanode stop

   service hadoop-datanode start
   ```

   or

   ```
   service hadoop-datanode restart
   ```

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

While configuring the SFTP agent, use the following table for setting some of the parameters:

Setting	Description
ENVISION	Set this value to the IP address of the RSA NetWitness Log Collector

Setting	Description
ENVISION_ DIRECTORY	EMC_GREENPLUMHD_***device_ip*** Where ***device_ip*** is the IP address for the event source For example, if the IP address is 172.16.0.51, set the parameter as follows: `ENVISION_DIRECTORY=EMC_GREENPLUM_172.16.0.51`

Configure the Log Collector for File Collection

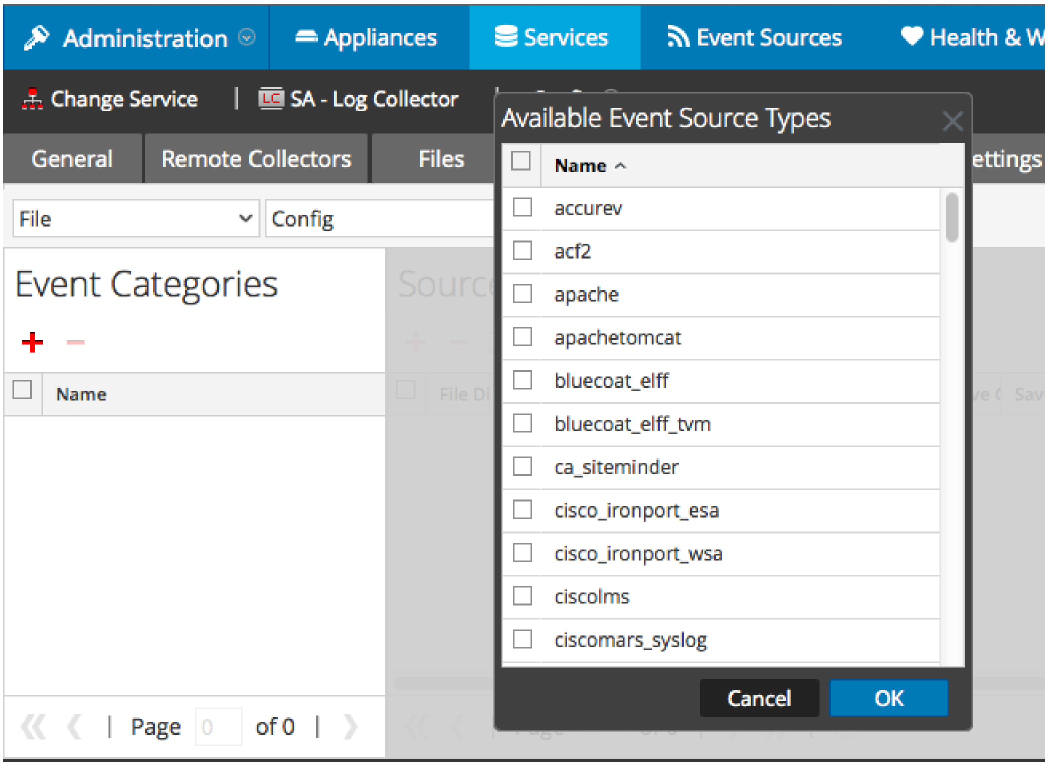
Perform the following steps to configure the Log Collector for File collection.

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.

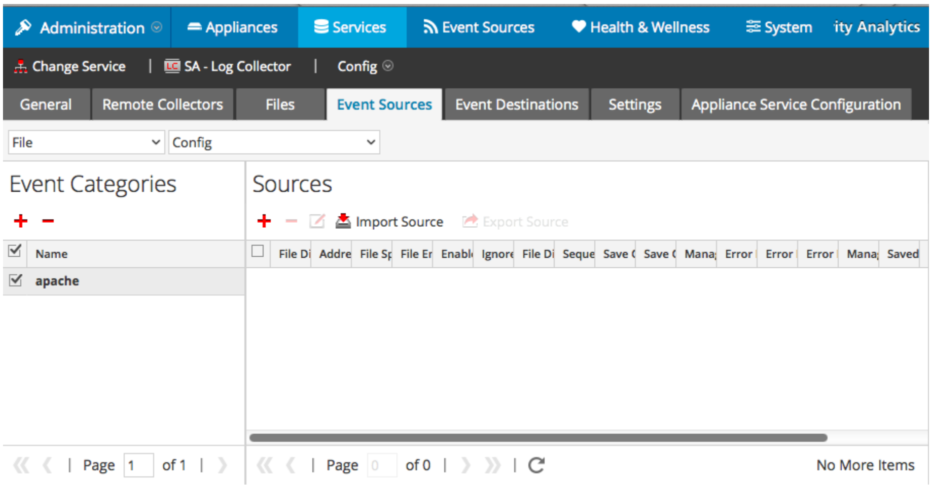


5. Select the correct type from the list, and click **OK**.

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

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

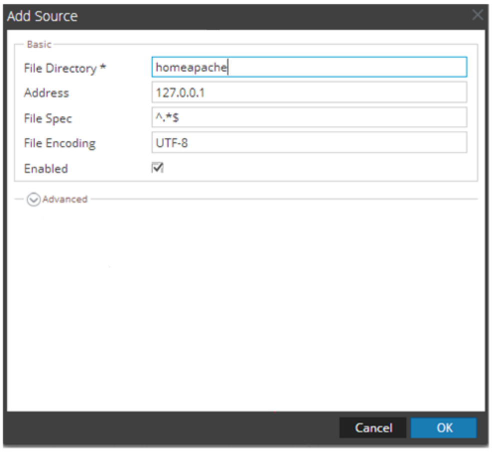
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



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.



Add Source

Basic

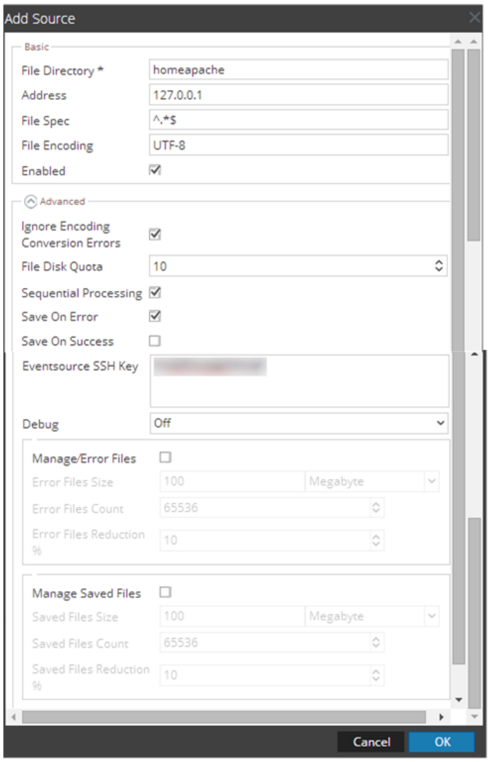
File Directory * homeapache

Address 127.0.0.1

File Spec ^.*$

File Encoding UTF-8

Enabled ☑



Add Source

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.