RSA NetWitness Platform

Event Source Log Configuration Guide

IBM Mainframe Syslog and Hardcopy Log Facility

Last Modified: Wednesday, January 16, 2019

Event Source Product Information:

Vendor: IBM
Event Source:Mainframe Syslog and Hardcopy Log Facility
Platforms: Hardcopy logs on IBM Mainframe z/OS v1.9, v1.10, v1.11, v1.12, v1.13, v2.x
Additional Downloads: HCLEXTR.cfg, HCLEXTR.trs, HCLSFTP.jcl and SFTPCMD.txt.IBMHCL

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: ibmmfzossyslog
Collection Method: File
Event Source Class.Subclass: Host.Mainframe

To configure IBM Mainframe Syslog and Hardcopy Log to work with RSA NetWitness Platform, you must complete these tasks:

I. Configure IBM Mainframe Syslog and Hardcopy Log Facility

II. Configure the Log Collector for File Collection

III. Set Up the SFTP Agent for **HCLSFTP**.

Configure IBM Mainframe Syslog and Hardcopy Log Facility

To configure IBM Mainframe Syslog and Hardcopy Log Facility for IBM Mainframe z/OS:

1. Download the IBM Mainframe Syslog and Hardcopy Log files from RSA Link at the following URL: https://community.rsa.com/docs/DOC-46784.
2. Download the following files to the mainframe: **HCLEXTR.cfg**, **HCLEXTR.trs**, **HCLSFTP.jcl**, and **SFTPCMD.txt.IBMHCL**, and follow the setup instructions in those files.

   Note: The **HCLEXTR.trs** file contains the following two loadlib modules:

   - Use the HCLEXTRA module if your Syslog backup input file contains printer carriage control characters (RECFM=FM, FBA, VBA).
   - Use the HCLEXTR module if your Syslog backup input file does not contain printer carriage control characters (RECFM=FB, VB).

3. Rename SFTPCMD.txt.IBMHCL to SFTPCMD before uploading to the mainframe. Then follow the instructions in the file.

   For reference, here are the instructions that appear in the SFTPCMD file:

   ```
   This SFTP script is called by the SFTP step in your JCL to send the audit
   data to the RSA appliance. It is critical that ONLY the command portion of
   this document is used for the SFTP script file for the z/OS device to
   execute the SFTP script correctly. In the statements below, replace:

   - 'hcl_10.100.255.255' with the source directory that the z/OS device
   event source uses to communicate to communicate to RSA NetWitness
   Platform.

   - '/u/hcl/ascii.zOS_device.data' with your Unix HFS directory and file
   name.

   These SFTP commands will be copied from MVS to a Unix HFS shell script
   that will be used by BPXBATCH to control your SFTP.
   ```

4. To configure the JCL for your site naming conventions, follow these steps:

a. Set up the job cards.

b. To change the dataset name to match your site's conventions, set the following fields:

- In the **HCLIN** field, specify the Syslog Backup dataset to be processed by HCLEXTR.
- In the **HCLOUT** field, specify the sequential file generated by HCLEXTRA or HCLEXTR to be used as input to the **SFTP Step**.
- (Optional) In the **CFG** field, specify the dataset containing the configuration file, or change the DD statement to //**CFG DD DUMMY**.
- In **STEP010**, depending on the loadlib module that you use, specify **PGM=HCLEXTR** or **PGM=HCLEXTRA**.
- For the **HCLSFTP** JCL, follow the instructions in the JCL and in SFTPCMD.

c. Decompress the **HCLEXTR.TRS** file.

Note: HCLEXTR.trs is a "TERSED" file containing the **HCLEXTR** program. This file is similar to a .zip file. You must use the IBM TRSMAIN program to decompress this file. This program is available from www.ibm.com. When uploading the .trs file from a workstation, pre-allocate a file with the following DCB attributes: **DSORG=PS**, **RECFM=FB**, **LRECL= 1024**, **BLKSIZE=6144**. The file transfer type must be binary and not text. The following is a sample JCL for unloading the **HCLEXTR.TRS** file into a PDS containing the HCLEXTR program:

```
//UNLOAD JOB (T,JXPO,JKSD0093),TEST,
// MSGCLASS=P,
// REGION=0M
//*****************************************************************
**
//SET1 SET INFILE='YOUR_HIGH_LEVEL.HCLEXTR.TRS',
//     OUTFILE='YOUR_HIGH_LEVEL.HCLEXTR.LINKLIB'
//DEL  EXEC PGM=IEFBR14
//DD1  DD DISP=(MOD,DELETE),DSN=&OUTFILE,
//     UNIT=SYSDA,
```

```
//     SPACE=(CYL,(10,10))
//UNLOAD EXEC PGM=TRSMAIN,REGION=0K,
//     TIME=1440,
//     PARM='UNPACK'
//SYSPRINT DD SYSOUT=*,DCB=(LRECL=133,BLKSIZE=12901,RECFM=FBA)
//INFILE   DD DISP=SHR,DSN=&INFILE
//OUTFILE  DD  DISP=(MOD,CATLG,DELETE),DSN=&OUTFILE,
//    SPACE=(CYL,(10,10,5),RLSE),
//    UNIT=SYSDA
//
```

Configure the Log Collector for File Collection

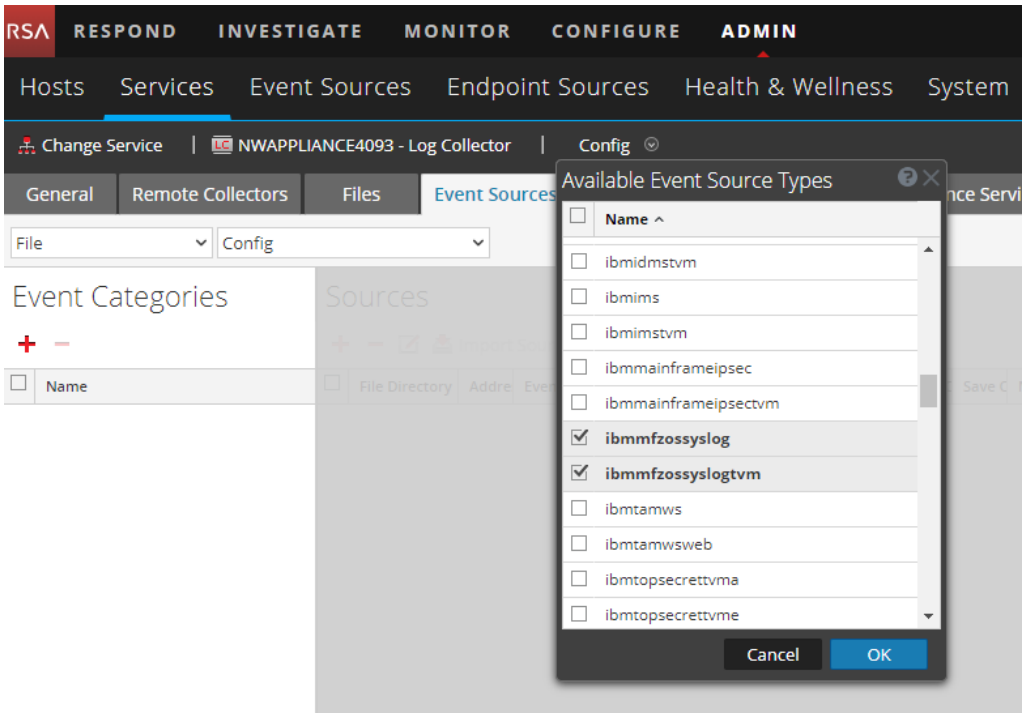
Perform the following steps to configure the Log Collector for File collection.

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.



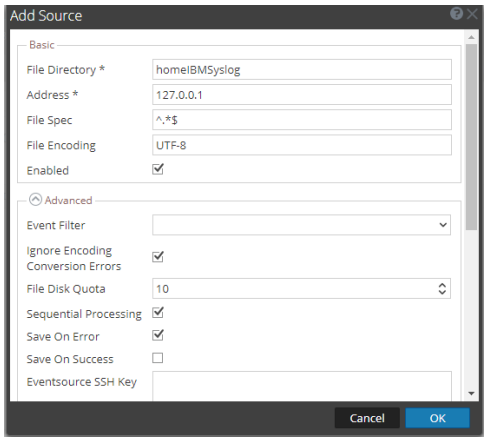
5. Based on your version, select a value, and click OK.

- For version z/OS v2.x, select **ibmmfzossyslogtvm** or
- For all earlier versions, select **ibmmfzossyslog**.

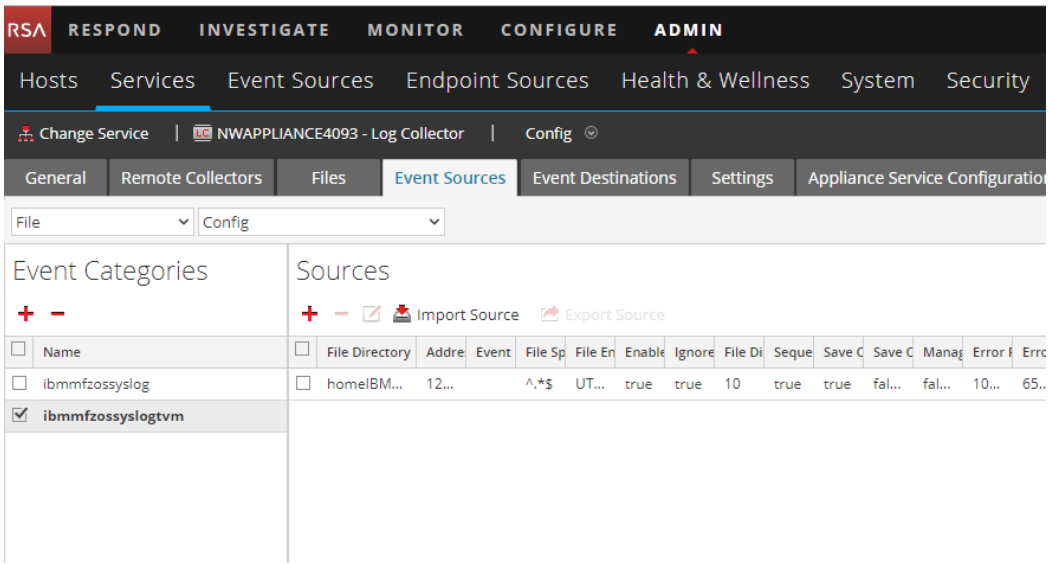
The newly added event source type is displayed in the Event Categories panel.

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.

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

Trademarks

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