RSA NetWitness Logs

Event Source Log Configuration Guide

IBM IMS

Last Modified: Monday, May 22, 2017

Event Source Product Information:

Vendor: IBM
Event Source:Mainframe IMS
Platforms: Mainframe z/OS v1.9, v1.10, v1.11, v1.12 and v1.13
Additional Downloads: imsextr.cfg, imsextr.trs, IMSSFTP.jcl and SFTPCMD.txt.IBMIMS

RSA Product Information:

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

Configure Mainframe IMS

To configure IBM Mainframe IMS to work with RSA NetWitness Suite, you must complete these tasks:

I. Configure IBM Mainframe IMS

II. Configure the Log Collector for File Collection

III. Set up the SFTP Agent for **IMSSFTP**.

Configure the IBM Mainframe IMS Event Source

To configure IBM Mainframe:

1. To download the IBM Mainframe IMS files from RSA SecurCare Online, follow these steps:

   a. Go to https://knowledge.rsasecurity.com and log onto RSA SecurCare Online (SCOL).

   b. Navigate to the **RSA NetWitness Suite Event Source Configuration Additional Downloads** page. SCOL displays available additional downloads.

   c. On the RSA Additional Downloads page, search for **IBM Mainframe IMS**, and download the following files to the mainframe: **IMSEXTR.cfg**, **IMSEXTR.trs**, **IMSSFTP.jcl** and **SFTPCMD.txt.IBMIMS**. Follow the setup instructions in those files.

   d. Rename SFTPCMD.txt.IBMIMS 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:

      - 'ims_10.100.255.255' with the source directory that the z/OS
      device event source uses to communicate to RSA NetWitness
      Suite.

      - '/u/ims/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.
```

2. Copy the **imsextr.cfg**, **IMSSFTP.jcl**, **SFTPCMD**, and **imsextr.trs** files to the mainframe.

   Note: imsextr.trs is a "TERSED" file containing the **IMSEXTR** program. This file is like a PC zip file and requires you to use the IBM **TRSMAIN** program to un-zip or un-terse 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 not text. The following is a sample JCL for unloading the **IMSEXTR.TRS** file into a PDS containing the **IMSEXTR** program:

   ```
   //UNLOAD JOB (T,JXPO,JKSD0093),TEST,
   // MSGCLASS=P,
   // REGION=0M
   //*************************************************************
   ******
   //SET1 SET INFILE='YOUR_HIGH_LEVEL.IMSEXTR.TRS',
   // OUTFILE='YOUR_HIGH_LEVEL.IMSEXTR.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
   //
   ```

3. Complete the following to edit the JCL to configure for your naming conventions:

a. Edit the JCL file to include the SFTP information for your RSA NetWitness Suite Log Collector.

b. Set up the job cards.

c. Change the dataset name to match your site's conventions.

Here are some notes on the JCL DD name to assist you:

Field	Description
IMSIN	Local system IMS log backup file to be entered into the **IMSEXTR** program
IMSOUT	Dataset created as output from the **IMSEXTR** program and sent via SFTP to the RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.
CONFIG	(Optional) Dataset containing the configuration file or change the **DD** statement to read //**CFG DD DUMMY**

d. Copy the **IMSEXTR** program to an existing LOADLIB or add a **STEPLIB DD** statement with the correct dataset name of the library that will contain the program.

e. (Optional) Copy **imsextr.cfg** to an existing library and modify in order to customize the data collected.

Configure the Log Collector for File Collection

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

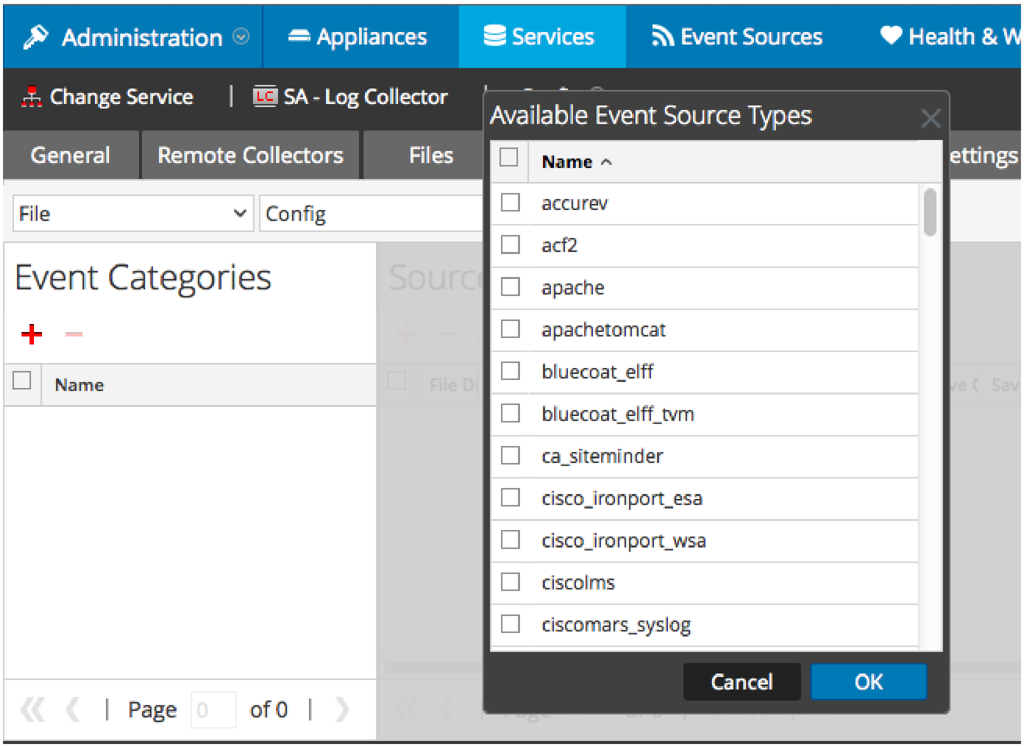
To configure the Log Collector for file collection:

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 +.

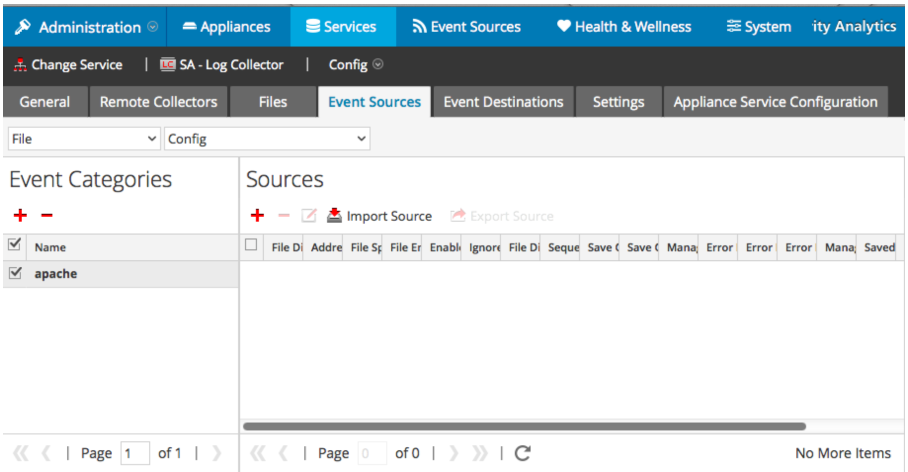
   The Available Event Source Types dialog is displayed.



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

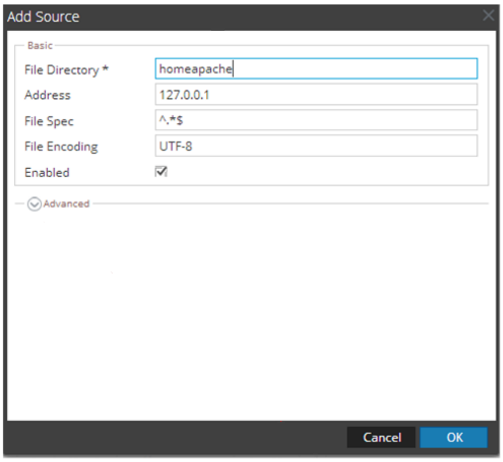
   Select **ibmims** from the **Available Event Source Types** dialog.

   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.



Add Source

Basic

File Directory * homeapache

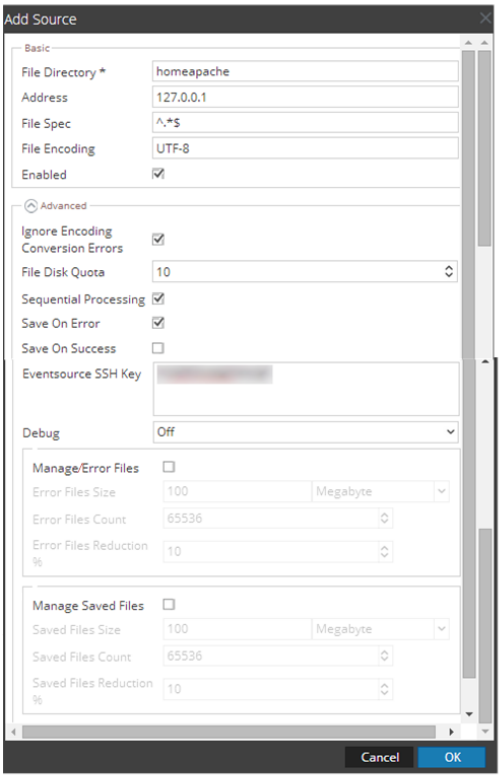
Address 127.0.0.1

File Spec ^.*$

File Encoding UTF-8

Enabled ☑

Advanced



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.

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

Trademarks