

RSA NetWitness Logs

Event Source Log Configuration Guide



IBM ICSF

Last Modified: Monday, May 22, 2017

Event Source Product Information:

Vendor: [IBM](#)

Event Source: Mainframe Integrated Cryptographic Service Facility (ICSF)

Platforms: Mainframe z/OS v1.9, v1.10, v1.11, v1.12 and v1.13

Additional Downloads: ICSFEXTR.cfg, ICSFEXTR.trs, ICSFSFTP.jcl and SFTPCMD.txt.IBMICSF

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: ibmicsf

Collection Method: File

Event Source Class.Subclass: Host.Mainframe

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

- I. Configure IBM Mainframe ICSF
- II. Configure NetWitness Suite for File Collection

Configure the IBM Mainframe ICSF Event Source

To configure IBM Mainframe ICSF for 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 ICSF**, and download the following files to the mainframe: **ICSFEXTR.cfg** and **ICSFEXTR.trs**. Also download **ICSFSFTP.jcl** and **SFTPCMD.txt.IBMICSF**, and follow the setup instructions in those files.
2. To configure the **ICSFSFTP** 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 **SMFIN** field, specify the SMF dataset to be processed by **ICSFEXTR** .
 - In the **SMFOUT** field, specify the sequential file generated by **ICSFEXTR** to be used as input to the **SFTP** steps.
 - (Optional) In the **CONFIG** field, specify the dataset containing the configuration file, or change the DD statement to **//CFG DD DUMMY**.
 - Rename **SFTPCMD.txt.IBMICSF** to **SFTPCMD** and **ICSFSFTP.jcl** to **ICSFSFTP** before uploading to the mainframe. Then follow the instructions in the files.

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:
```

- 'icsf_10.100.255.255' with the source directory that the z/OS device event source uses to communicate to RSA NetWitness Suite.

- '/u/icsf/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.

c. Decompress the **ICSFEXTR.TRS** file.

Note: **ICSFEXTR.trs** is a "TERSED" file containing the **ICSFEXTR** 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 ICSFEXTR.TRS file into a PDS containing the ICSFEXTR program:

```
//UNLOAD JOB (T,JXPO,JKSD0093),TEST,
// MSGCLASS=P,
// REGION=0M
//*****
*****
//SET1 SET INFILE='YOUR_HIGH_LEVEL.ICSFEXTR.TRS',
//      OUTFILE='YOUR_HIGH_LEVEL.ICSFEXTR.LINKLIB'
//DEL EXEC PGM=IEFBR14
//DD1 DD DISP=(MOD,DELETE),DSN=&OUTFILE,
//      UNIT=SYSDA,
//      SPACE=(CYL,(10,10))
//UNLOAD EXEC PGM=TRSMAN,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 NetWitness Suite for File Collection

To configure File collection for IBM Mainframe ICSF, complete the following tasks:

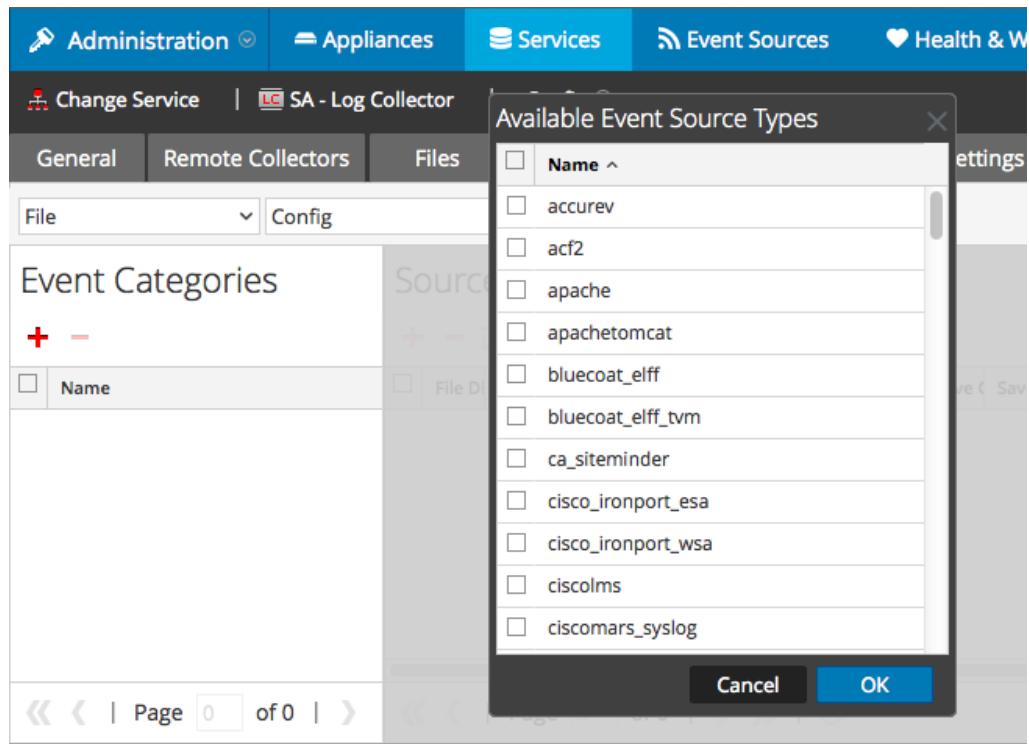
- I. Configure the Log Collector for File collection
- II. Set up the SFTP Agent

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:

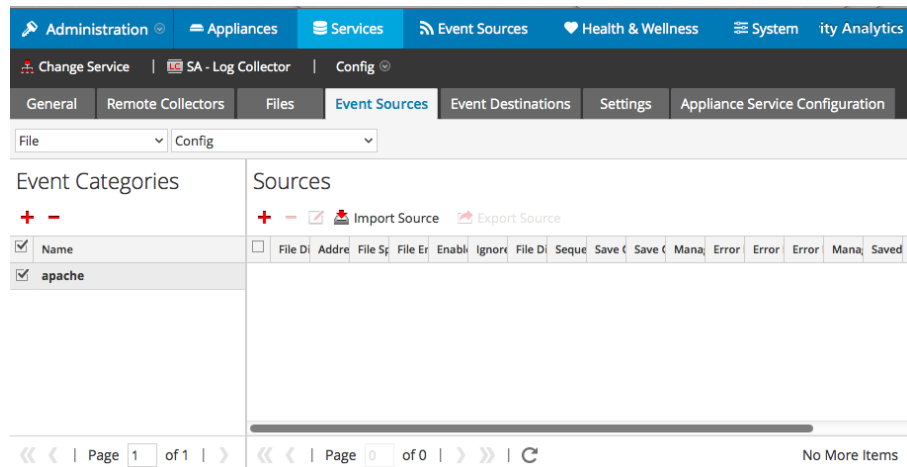
1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
3. Select **File/Config** from the drop-down menu.
The Event Categories panel displays the File event sources that 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**.

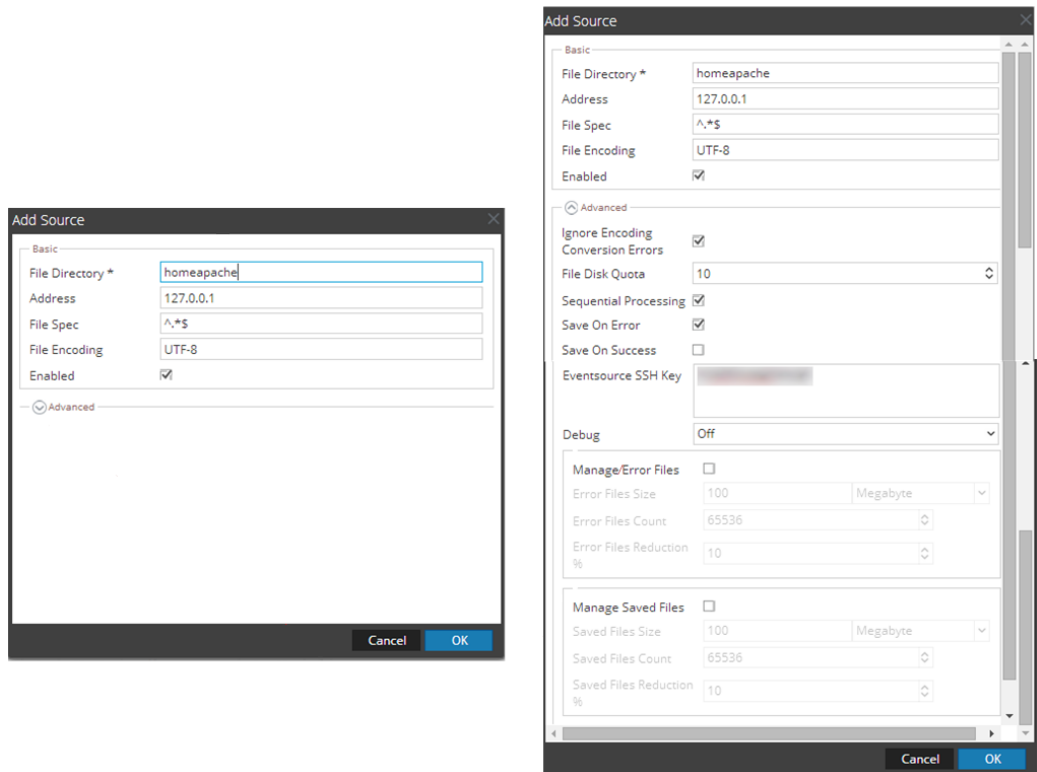
Select **ibmicsftvm** from the **Available Event Source Types** dialog.

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.

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](#)

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.