RSA NetWitness Logs

Event Source Log Configuration Guide

IBM RACF

Last Modified: Monday, May 22, 2017

Event Source Product Information:

Vendor: IBM
Event Source: IBM RACF
Versions: All
Platforms: Mainframe z/OS v1.9, v1.10, v1.11, v1.12, v1.13, v2.1 and v2.2
Additional Downloads: RACFEXTR.CFG, RACFEXTR.TRS, RACFSFTP.jcl and SFTPCMD.txt.IBMRACF

RSA Product Information:

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

Configure IBM RACF

You can set up the IBM RACF event source to send log information to the RSA NetWitness Suite using SFTP.

I. Configure the IBM RACF event source

II. Set up the SFTP Agent for **RACFSFTP**

III. Configure the Log Collector for File Collection

IV. Review the list of RACF Event Codes and Record Extension supported by RSA NetWitness Suite

Note: For z/OS v2.1 and above, SMF data that is compressed with the zEnterprise® Data Compression feature is not supported.

Configure the IBM RACF Event Source

Perform the following steps to configure the event source.

To configure IBM Mainframe RACF:

1. Complete the following to download files from the RSA SecurCare Online (SCOL) web site:
   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. Locate the IBM Mainframe RACF entry in the list.
      - Right-click on the **RACFEXTR.CFG** file and select **Save Target As…**. Complete the Save As dialog box and click **Save**.
      - Right-click on the **RACFSFTP.jcl** file and select **Save Target As…**. Complete the Save As dialog box and click **Save**.
      - Right-click on the **SFTPCMD.txt.IBMRACF** file and select **Save Target As…**. Complete the Save As dialog box and click **Save**.
      - Right-click on the **RACFEXTR.TRS** file and select **Save Target As…**. Complete the Save As dialog box and click **Save**.
2. Rename files before uploading to the mainframe:

- Rename RACFSFTP.jcl to RACFSFTP
- Rename racfextr.trs to RACFEXTR
- Rename SFTPCMD.txt.IBMRACF to SFTPCMD

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

```
<Start of Instructions. DO NOT INCLUDE THESE INSTRUCTIONS IN THE
SCRIPT>

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:


- 'var/netwitness/logcollector/upload/racftvm/racftvm/' with the
upload directory that the z/OS device event source uses to
communicate to the RSA NetWitness Suite appliance.


- '/u/racf/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.

The script portion of the document is listed below. Include ONLY
what is listed below these instructions in the SFTP script file!!

<End of of Instructions. DO NOT INCLUDE THESE INSTRUCTIONS IN THE
SCRIPT>


put /u/racf/ascii.zOS_device.data
var/netwitness/logcollector/upload/racftvm/racftvm/auditdta.txt

quit
```

3. Copy **RACFSFTP**, **SFTPCMD**, and **RACFEXTR** to the mainframe.

Note: racfextr.trs is a "TERSED" file containing the **RACFEXTR** 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 you upload 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 an example of the JCL you use to unload the **RACFEXTR.TRS** file into a **PDS** containing the **RACFEXTR** program:

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

4. Complete the following to edit the RACFSFTP JCL to configure for your site's naming conventions:
   a. Follow the instructions in RACFSFTP.jcl and SFTPCMD.txt.IBMRACF. Also, refer to the SFTP instructions in the RSA NetWitness Suite SFTP Agent Guide.
   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
SMFIN	Local system SMF dataset to be entered into the RACF utility IRRADU00 (IFASMFDP).
SMFOUT	Dataset created as output from the **RACF** utility and used as input into the **RACFEXTR** program.
RACFOUT	Dataset created as output from the **RACFEXTR** program and sent via SFTP to the RSA NetWitness Suite Log Collector.
CONFIG	(Optional) Dataset containing the configuration file or change the **DD** statement to read **//CFG DD DUMMY**

   d. Copy the **RACFEXTR** program to an existing link listed library or add a **STEPLIB DD** statement with the correct dataset name of the library that will contain the program.
   e. (Optional) Copy the **racfextr.cfg** to an existing library and modify in order to customize the data collected.

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

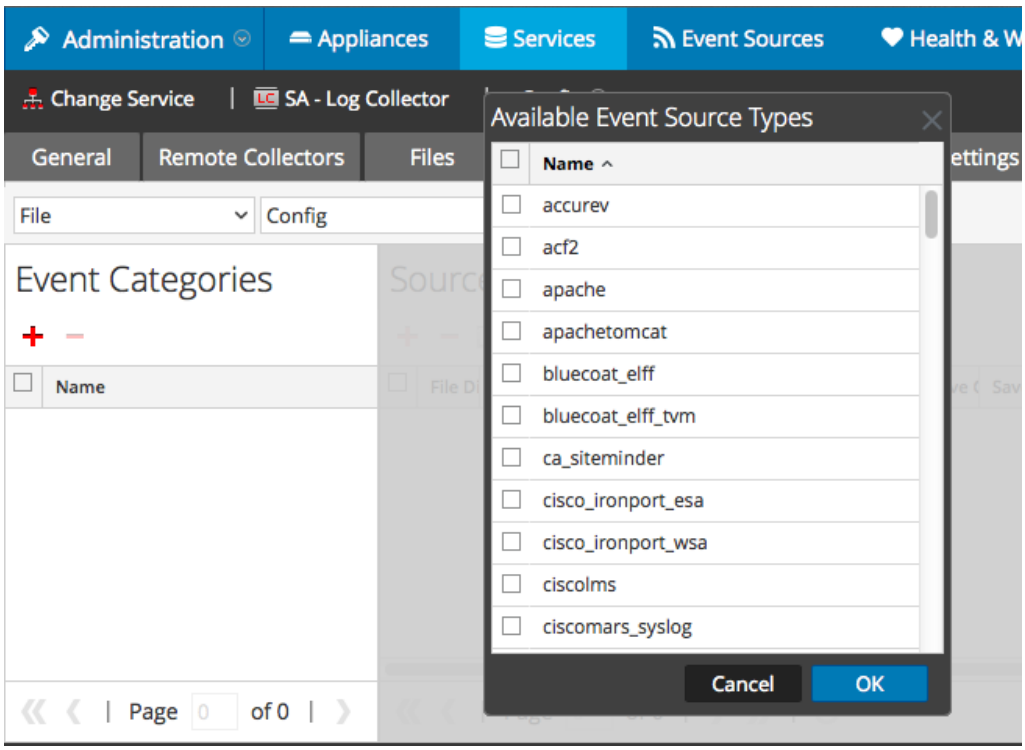
Perform the following steps to configure the Log Collector for File collection.

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 +.

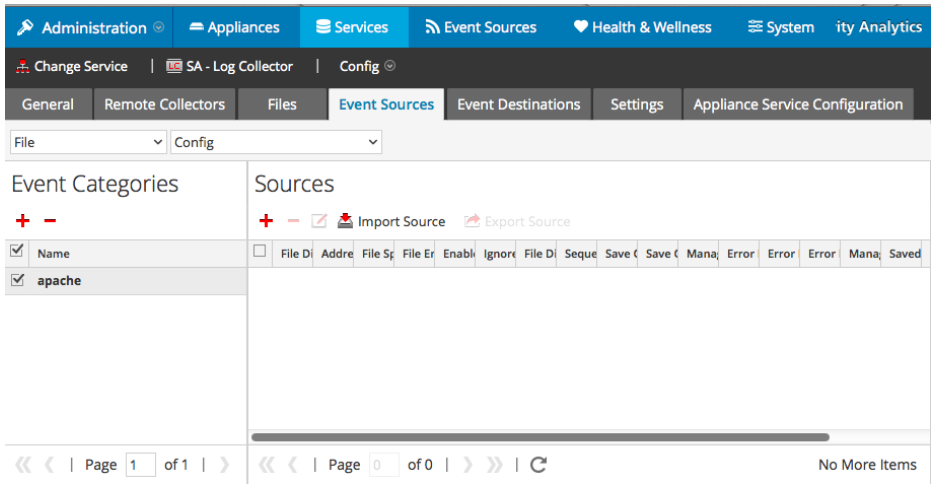
   The Available Event Source Types dialog is displayed.



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

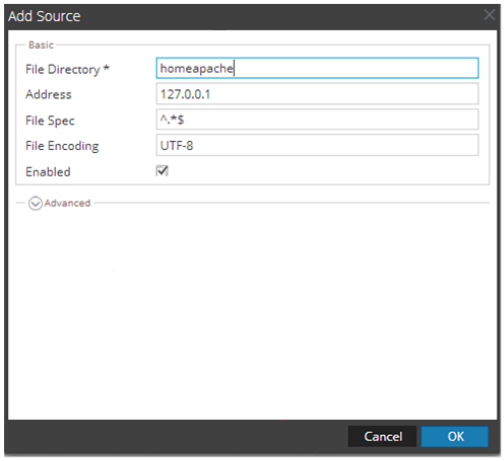
   Select **racftvm** from the **Available Event Source Types** dialog.

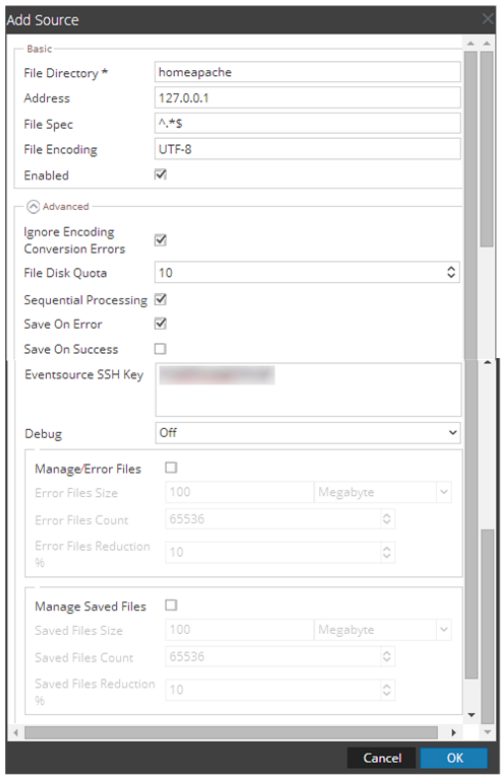
   The newly added event source type is displayed in the Event Categories panel.



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.

RACF Event Codes and Record Extension supported by RSA NetWitness Suite

The following table lists the record extensions that are supported in RSA NetWitness Suite.

access	accr	addgroup	addsd
adduser	addvol	altdsd	altgroup
altuser	appclu	autoprof	chaudit
chdir	chkfown	chkpriv	chmod
chown	ckown2	clasname	clrsetid
connect	daccess	define	deldsd
delfacl	delgroup	delres	deluser
delvol	dirsrch	dsaf	exesetid
faccess	general	getpsent	initacee
initoedp	ipcchk	ipcctl	ipcget
jobinit	kill	kticket	link
mkdir	mknod	mntfsys	openfile
openstty	password	pdaccess	permit
pgmveryf	pkiaurnw	pkidpubr	ptcreate
pteval	ptrace	racdcert	racfinit
raclink	racmap	ralter	rdataupd
rdefine	rdelete	renameds	renamef

rmdir	rpkiexpt	rpkigenc	rpkiqrec
rpkiread	rpkiresp	rpkiscep	rpkiupdc
rpkiupdr	rremove	rvary	setegid
seteuid	setfacl	setfsecl	setgid
setgroup	setropts	setuid	symlink
termoedp	umntfsys	unlink	writedwn

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.