RSA NetWitness Platform

Event Source Log Configuration Guide

CA ACF2

Last Modified: Tuesday, January 14, 2020

Event Source Product Information:

Vendor: CA
Event Source: ACF2 (formerly IBM Mainframe ACF2)
Versions: r14 and higher
Supported Platforms: z/OS v1.9, v1.10, v1.11, v1.12, and v1.13
Additional Downloads:

- ACF2SFTP.jcl
- ACF2EXTR.trs
- ACF2EXTR.cfg
- SFTPCMD.txt.CAACF2

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: ibmacf2
Collection Method: File
Event Source Class.Subclass: Host.Mainframe

Configure CA ACF2

To configure CA ACF2, you must complete these tasks:

I. Configure scripts on CA ACF2

II. In RSA NetWitness Platform, set Up the SFTP Agent

III. In RSA NetWitness Platform, set up the File Service

For reference, see the ACF2 Record Types Supported by RSA NetWitness Platform table below.

Configure Scripts on the CA ACF2 Event Source

ACF2 is a set of programs that enable security on mainframes. ACF2 prevents accidental or deliberate modification , corruption, mutilation, deletion, or viral infection of files.

To configure CA ACF2:

1. To download files from the RSA Link website, follow these steps.
   a. Log on to the RSA Link Event Source Additional Downloads space and navigate to the page for AC ACF2:

      https://community.rsa.com/docs/DOC-45352

   b. Click the **acf2extr.trs** file: it will be downloaded to your default download directory.

   c. Click to display the following files in your browser:

      - **acf2extr.cfg**: save the file to your computer.
      - **SFTPCMD.txt.CAACF2**: save the file to your computer, then rename the file to SFTPCMD.
      - **ACF2SFTP.jcl**: save the file to your computer, then rename the file to ACF2SFTP.

      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:

- 'acf2_10.100.255.255' with the source directory that the z/OS device
event source uses to communicate to RSA NetWitness Platform.
```

```
- '/u/acf2/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 files that you saved to your Mainframe.

> **Note: acf2extr.trs** is a "TERSED" file containing the ACF2EXTR 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 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 that you use to unload the **acf2extr.trs** file into a PDS containing the ACF2EXTR program:

```
//UNLOAD JOB (T,JXPO,JKSD0093),TEST,
// MSGCLASS=P,
// REGION=0M
//*********************************************************************
//SET1 SET INFILE='YOUR_HIGH_LEVEL.ACF2EXTR.TRS',
// OUTFILE='YOUR_HIGH_LEVEL.ACF2EXTR.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. To configure the JCL file, follow these steps:

   a. Edit the JCL file to include the RSA NetWitness Platform Log Decoder or Remote Log Collector SFTP information.

   b. Set up the job cards.

   c. Edit the dataset name to match the conventions of your site, including the following fields:

      - In the **SMFIN** field, specify the local system SMF dataset to be entered into the ACF2 ACFRPTPP utility.

- In the **SMFOUT** field, specify the dataset created as output form the ACF2 utility and used as input into the ACF2EXTR program.
- In the **ACF2OUT** field, specify the dataset created as output from the ACF2EXTR program and sent by FTP to the enVision appliance.
- (Optional) In the **CONFIG** dataset containing the configuration file, change the DD statement to read //CFG DD DUMMY.
- (SFTP only) **SFTPCMD** is the SFTP control card file.

d. Copy the ACF2EXTR 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 **acf2extr.cfg** file to an existing library, and modify 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 SFTP Shell Script File Transfer

Configure the Log Collector for File Collection

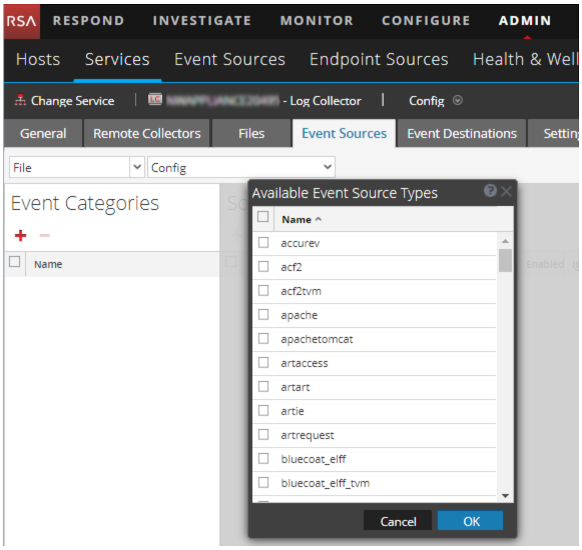
Perform the following steps to configure the Log Collector for File collection.

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.



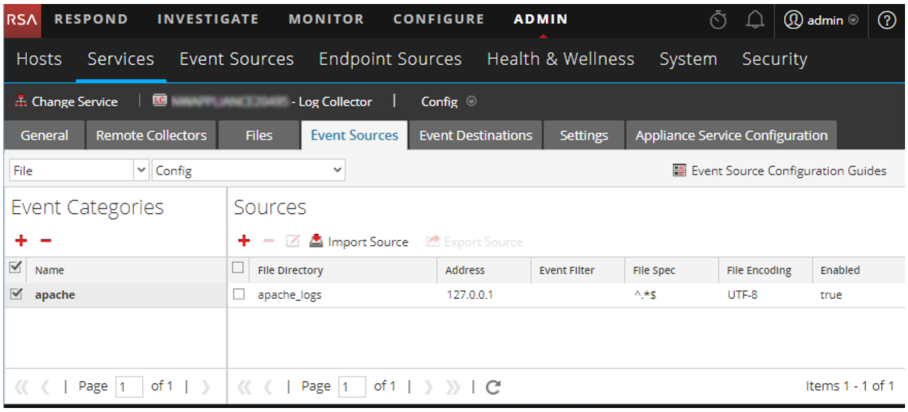
□	Name ^
□	accurev
□	acf2
□	acf2tvm
□	apache
□	apachetomcat
□	artaccess
□	artart
□	artie
□	artrequest
□	bluecoat_elff
□	bluecoat_elff_tvm

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

   Select **acf2tvm** 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.



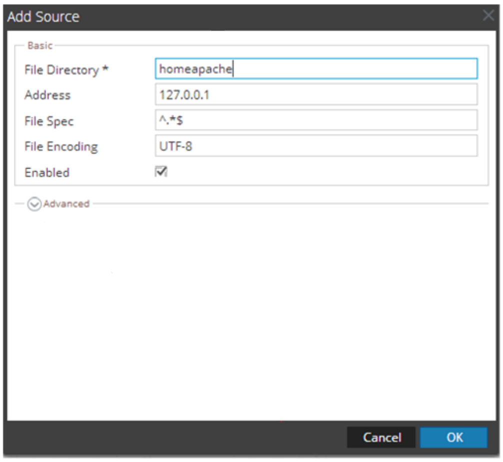
☑	Name
☑	**apache**

□	File Directory	Address	Event Filter	File Spec	File Encoding	Enabled
□	apache_logs	127.0.0.1		^.*$	UTF-8	true

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

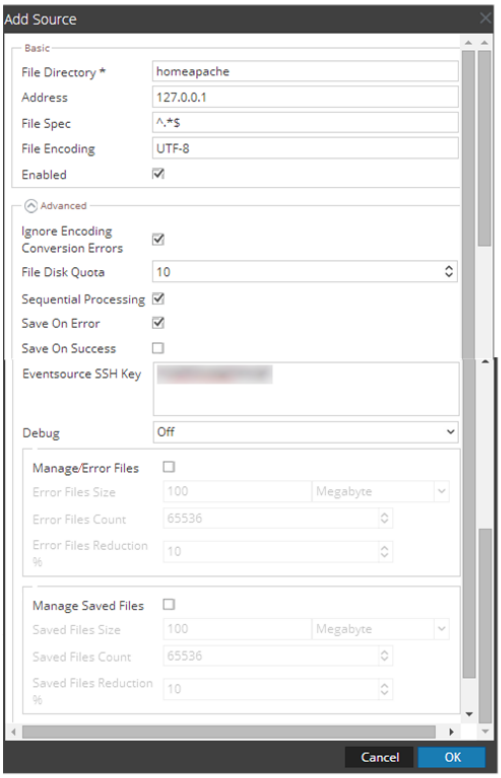
Address 127.0.0.1

File Spec ^.*$

File Encoding UTF-8

Enabled ☑

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.

ACF2 Record Types Supported by RSA NetWitness Platform

Record	SMF Record	Description	Additional Information
A	230-A	ACF2 Commands record	

Record	SMF Record	Description	Additional Information
D	230-D	Data set access event journal record	Data Set and Program Logs and Violations. Defines the fields that are available to you when generating a Type D report. The fields include all data set log entries, all data set violations, all trace records, all program log entries, and program violations.
E	230-E	Summary - Infostorage modification journal record	Infostorage Modification Log (Summary Report). Defines fields that are available to you when generating a Type E report, the fields include the record or rule set that was updated, type of update, and the record used as a model if the INSERT USING command was used.
E	230-E	Detail - Infostorage modification journal record	Infostorage Modification Log (Detailed Report). Defines fields available to you when generating a Type E report. This includes detailed information about the update request.
G	230-G	DSO record	
J	230-J	Restricted Logonid trace record	Restricted Logonid Job Record. Defines the fields available to you when generating a Type J report. This includes the name of the program, submission path, CPU that the job was submitted from, and other information about the use of jobs requiring restricted logon IDs.
L	230-L	Summary - Logonid database modification journal record	Logonid Record Modifications (Summary Report). Defines the fields available to you when generating a summary Type L report.
L	230-L	Detail - Logonid database modification journal record	Logonid Record Modifications (Detail Report). Defines the fields available to you when generating a detailed Type L report. This is available only for Type L records eTrust CA-ACF2 wrote on the z/OS and OS/390 system.
O		OpenEdition record	

Record	SMF Record	Description	Additional Information
P	230-P	System entry violation journal record	Invalid Password and Authority. Defines the fields available to you when generating a Type P report. This includes all records written during logon, sign-on, and batch job initiation.
R	230-R	Access Rule database modification journal record	Access Rule Modifications. Defines the fields available to you when generating a Type R report. This includes all records written when an access rule is added to or deleted from the Rule database.
S		SAF record	System Authorization facility.
T	230-T	TSO record	Time Sharing Option record.
V	230-V	Generalized resource event journal record	Resource Log Entries and Violations. Defines the fields available to you when generating a Type V report. This includes all resource log entries, all resource violations, and all resource trace records.
Z		DDB record	

Trademarks

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