RSA NetWitness Platform

Event Source Log Configuration Guide

CA Top Secret

Last Modified: Tuesday, January 14, 2020

Event Source Product Information:

Vendor: CA
Event Source: CA Top Secret
Versions: z/OX v 1.4
Supported Platforms: IBM Mainframe
Additional Downloads: earlextr.cfg, earlextr.trs, tsaudext.cfg, tsaudext.trs, EARLSFTP.jcl, SFTPCMDE.txt.CATOPSECRET, TSAUSFTP.jcl, SFTPCMDA.txt.CATOPSECRET

RSA Product Information:

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

To configure CA Top Secret, you must complete these tasks:

I. Configure either or both of the batch utility programs:
   - Configure CA Top Secret for TSSUTIL
   - Configure CA Top Secret for TSSAUDIT

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

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

Note: You can configure either or both of the batch utility programs. TSSAUDIT messages are concerned with user related changes. TSSUTIL messages are more specific to events that involve files, hardware, and so on. Keep in mind that there may be some overlap.

For reference, see the Top Secret Message Types Supported by RSA NetWitness Platform table below.

Configure CA Top Secret for TSSUTIL

To configure CA Top Secret for TSSUTIL:

1. Use a browser to navigate to the CA Top Secret Additional Downloads page in the RSA® NetWitness® Platform Event Source Downloads space.
2. Download the **EARLSFTP.jcl**, **SFTPCMDE.txt.CATOPSECRET** and **earlextr.trs** files from RSA SecurCare Online.
3. Rename SFTPCMDE.txt.CATOPSECRET to SFTPCMDE before uploading the file to the mainframe
4. Copy the files that you downloaded in Step 1 to the Mainframe.

Note: EARLEXTR.TRS is a "TERSED" file containing the terse linklib or executable (the **EARLEXTR** 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 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 **EARLEXTR.TRS** file into a **PDS** containing the **EARLEXTR**program:

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

5. Complete the following to edit the JCL to configure for your site's naming conventions:
   a. Edit the JCL file to include the RSA NetWitness Platform Log Collector's SFTP information.
   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
SMFIN1	Local SMF/RACF file input to the **TSSUTIL** program
SMFIN2	Local SMF file input to the **TSSUTIL** program
TSSOUT	Dataset created as output from the **TSSUTIL** program and input to the **EARLEXTR** program.
TSSOUT	Dataset created as output from the **TSSUTIL** program and input to the **EARLEXTR** program.
UTILOUT	Dataset created as output from the **TSSUTIL** program this file is not used in the **EARLEXTR** program as we only process the EARL data.
EARLOUT	Dataset created as output from the **EARLEXTR** program and sent via SFTP to the RSA NetWitness Platform.
CONFIG	(Optional) Dataset containing the configuration file. If you do not want to use this file, change the **DD** statement to read **//CFG DD DUMMY**
SFTPCMDE	File transfer control card file.

d. Copy the **EARLEXTR** 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 **EARLEXTR.CFG** to an existing library and modify in order to customize the data collected.

Configure CA Top Secret for TSSAUDIT

To configure CA Top Secret for TSSAUDIT:

1. Download **TSAUSFTP.jcl**, **SFTPCMDA.txt.CATOPSECRET**, and **tsaudext.trs** from RSA SecurCare Online.
2. Rename SFTPCMDA.txt.CATOPSECRET to SFTPCMD before uploading the file to the mainframe
3. Copy the files that you downloaded in Step 1 to the Mainframe.

   Note: TSAUDEXT.TRS is a "TERSED" file containing the terse linklib or executable (the TSAUDEXT 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 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 TSAUDEXT.TRS file into a **PDS** containing the **TSAUDEXT** program:

```
//UNLOAD JOB (T,JXPO,JKSD0093),TEST,
// MSGCLASS=P,
// REGION=0M
//*****************************************************************
//SET1 SET INFILE='YOUR_HIGH_LEVEL.TSAUDEXT.TRS',
// OUTFILE='YOUR_HIGH_LEVEL.TSAUDEXT.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 JCL to configure for your site's naming conventions:
   a. Edit the JCL file to include the RSA NetWitness Platform Log Collector's SFTP information.
   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
ddname	Local APF file input to the **TSSAUDIT** program.
RECOVERY	Local Top Secret Recovery file input to the **TSSAUDIT** program.
AUDITOUT	Dataset created as output from the **TSSAUDIT** program and input to the **TSAUDEXT** program.
AUDITIN	Input parameters for the **TSSAUDIT** program.
TSAUDOUT	Dataset created as output from the **TSAUDEXT** program and sent to the RSA NetWitness Platform Log Collector.
CFG	(Optional) Dataset containing the configuration file. If you do not want to use this file, change the **DD** statement to read **//CFG DD DUMMY**.
SFTPCMD	File transfer control card file.

   d. Copy the **TSAUDEXT** 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 **TSAUDEXT.CFG** to an existing library and modify in order to customize the data collected.

Top Secret Message Types Supported by RSA NetWitness Platform

Message Type		
Date/Time	Logon ID	RequestAccess2
MessageID	UserName	RequestAccess3
DeviceAddress	Program	ResourceClass
DepartmentName	ReturnCode	AllowAccess1
DivisionName	DetailReturnCode	AllowAccess2
ZoneName	Resource	AllowAccess3
FacilityName	SessionType	Reason
GroupName	Audit	Terminal
JobName	Bypass	Type
JobNumber	RequestAccess1	Volser

Configure File Collection on RSA NetWitness Platform

To configure file collection on RSA NetWitness Platform, perform the following tasks:

I. Set up the SFTP Agent

II. Set up the File Service

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

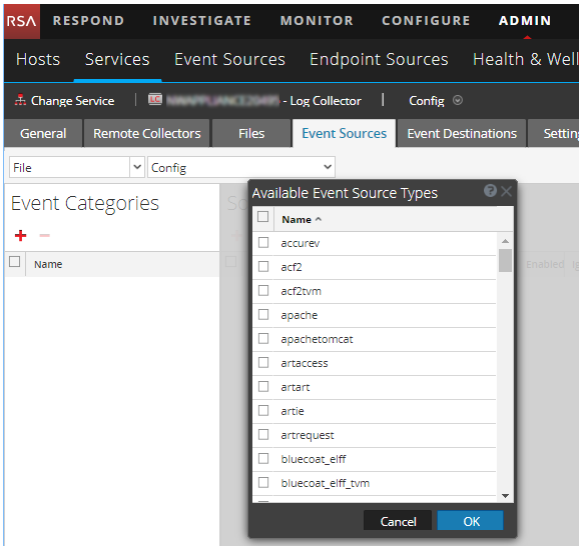
Perform the following steps to configure the Log Collector for File collection.

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.



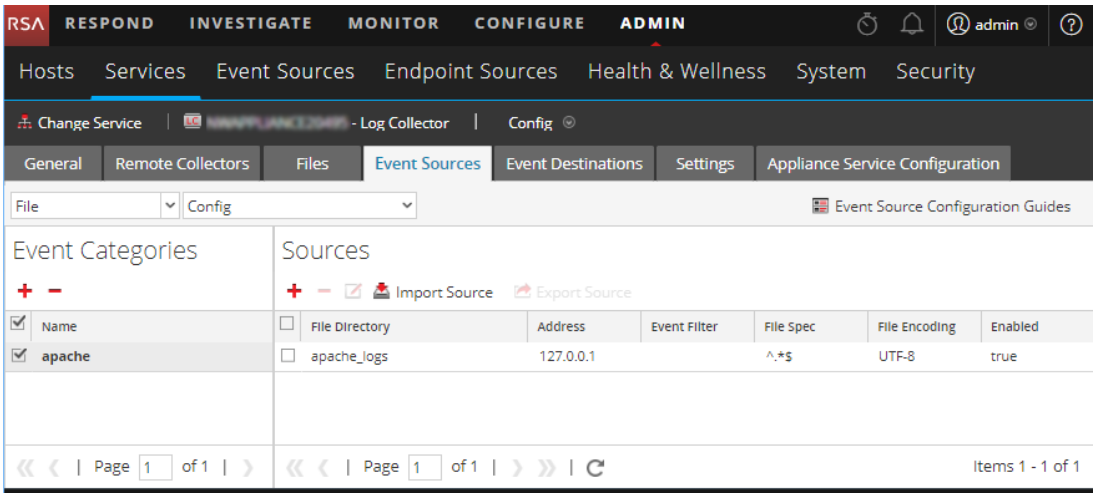
5. Select the correct type from the list, and click **OK**.

   Select one of the following types from the the **Available Event Source Types** dialog:

   - If you are configuring TSSUTIL, select **catopsecrettvme**.
   - If you are configuring TSSAUDIT, select **catopsecrettvma**.

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

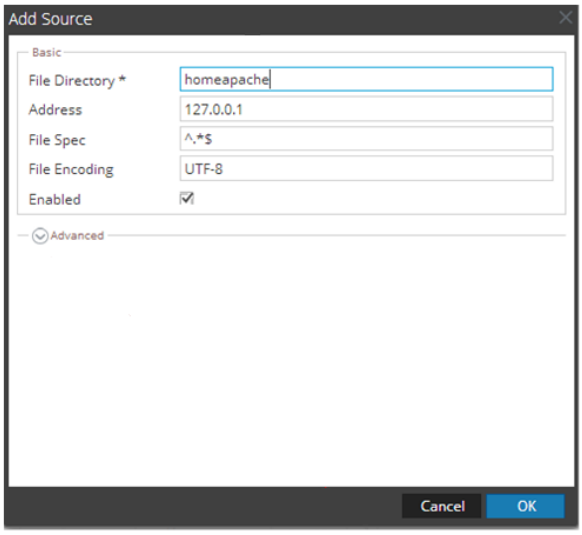
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

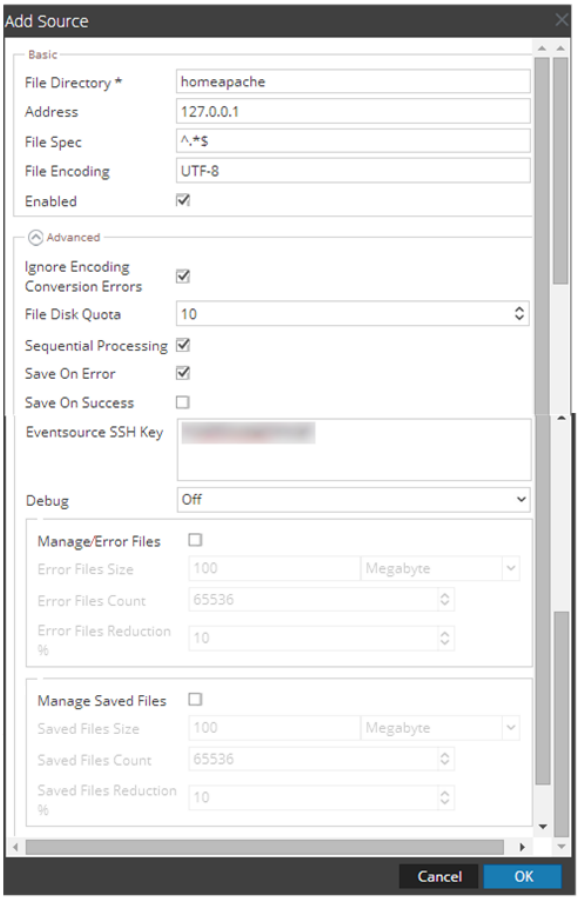


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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.





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.

Trademarks

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