RSA NetWitness Logs

Event Source Log Configuration Guide

IBM iSeries

Last Modified: Monday, May 22, 2017

Event Source Product Information:

Vendor: IBM
Event Source: iSeries AS400
Versions: V6.1.x, V7.1, V7.2
Additional Downloads: iseries_lib_indep.zip

RSA Product Information:

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

Configure IBM iSeries

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

- Configure the IBM iSeries Event Source
- Configure the RSA NetWitness Suite Log Collector for File Collection
- Set up the SFTP Agent

Configure the IBM iSeries Event Source

To configure IBM iSeries:

1. Follow these steps to download the files that you need.

   Note: The files are available on RSA SecurCare Online (SCOL) and on the RSA NetWitness Suite appliance.

   a. Log on to SecurCare Online (SCOL).

   b. Visit the RSA NetWitness Suite Event Source Configurations page.

   c. From the list, find the **IBM iSeries (AS400)** event source.

   d. All of the necessary files are bundled into the **iseries_lib_indep.zip** archive. Download this file and extract all of the individual files.

2. For SFTP, rename sftpcmd.txt.IBMISERIES to SFTPCMD before uploading the file to the iSeries / AS400.

3. Set up and run the appropriate files. For details, see Script File Details.

Configure the Log Collector for File Collection

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

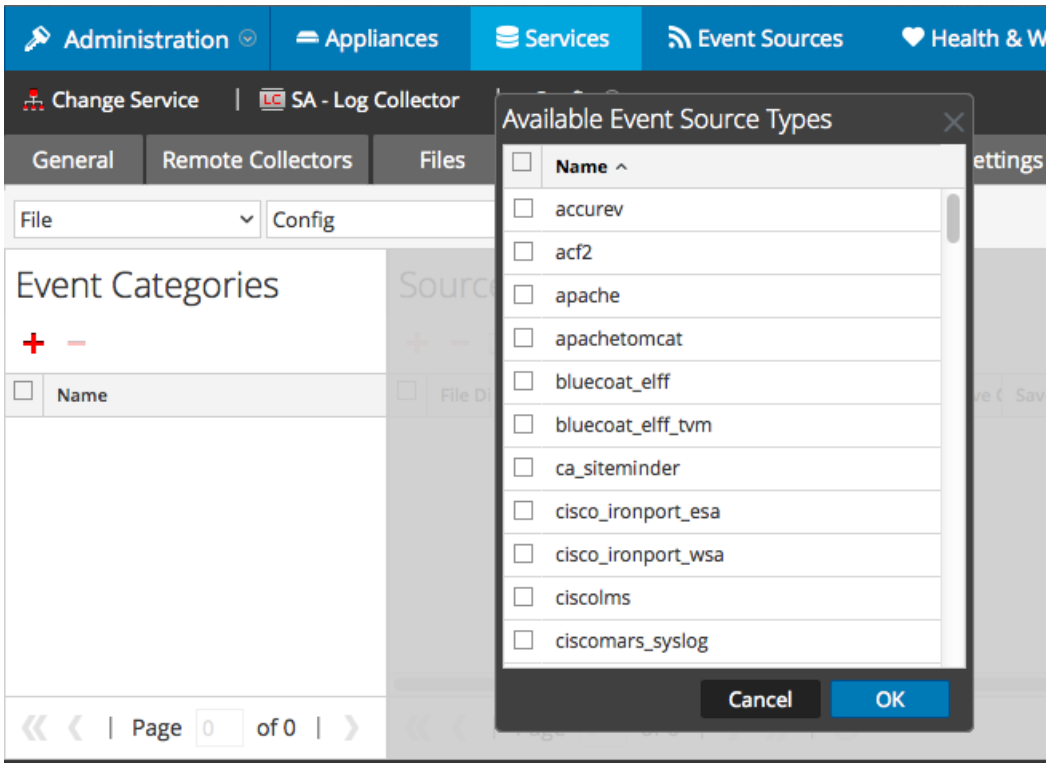
To configure the Log Collector for file collection:

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 +.

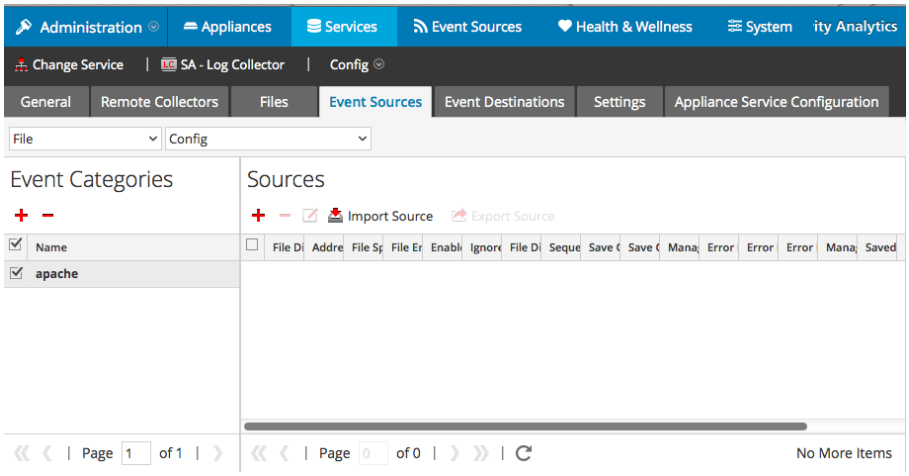
   The Available Event Source Types dialog is displayed.



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

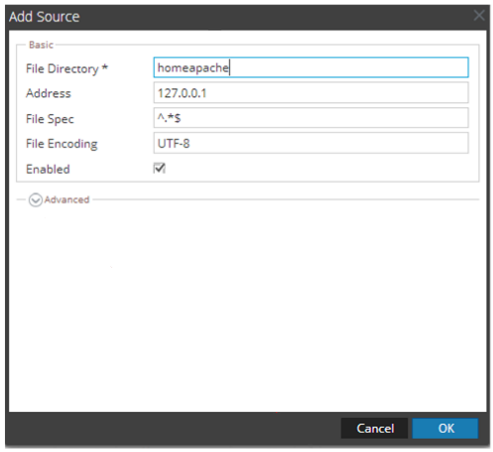
   Select **iseries** from the **Available Event Source Types** dialog.

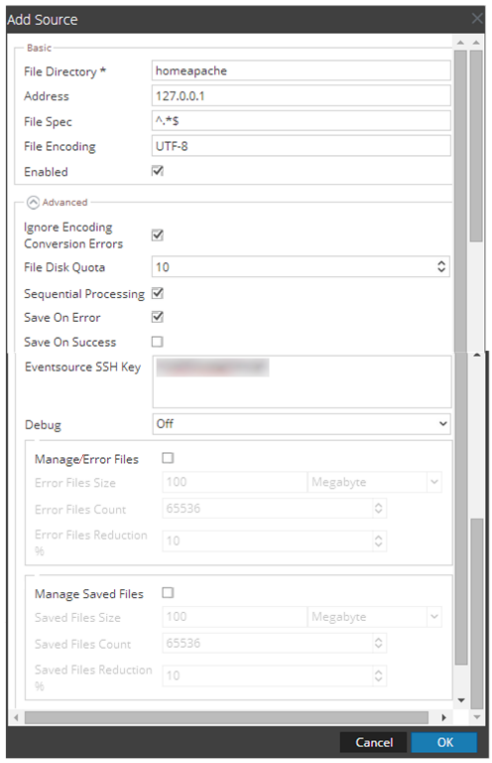
   The newly added event source type is displayed in the Event Categories panel.



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

Script File Details

There is a command file, **auditsftpc.txt**. This file writes audit data to a file and then transfers the data to the RSA NetWitness Suite. The **auditsftpc.txt** file transfers data from the iSeries to the RSA NetWitness Suite.

The **auditsftpc.txt** uses SFTP, and performs the following tasks:

- converts the audit extract file to a 'tag name = value' formatted file.
- converts the EBCDIC ‘tag name = value’ file to an ASCII formatted file.
- copies the database file to an Integrated File System file that is input to the SFTP step

There is an option for **auditsftpc.txt** to dynamically create an SFTP command file. If selected, this option generates an SFTP command file each time that **auditsftpc.txt** runs. The dynamically created SFTP command file contains a put statement that has a unique receiving (to) file name that appends the date and time as part of the receiving file names. The date and time component of the file name is in _YYMMDD_HHMMSS format. For example, the put statement generated for an audit data file created on September 20, 2012 at 03:35:15 would look like this if you are using **auditsftpc.txt**:

```
put /home/auditlib/auditdta.txt ISERIES_A.B.C.D/
auditdta_120920_033515.txt
```

To use this option, see the instructions for setting the &BLDFTPFLAG program variable in **auditsftpc.txt**.

- Additional instructions for dynamically creating an SFTP command file are provided in **auditsftpc.txt** and **sftpcmd.txt.IBMISERIES**.

The default is for the static **sftpcmd.txt.IBMISERIES** command file to be used for **auditsftpc.txt** SFTP commands.

Library Independence

For users who do not want to use the default audit library (AUDITLIB), RSA has updated the iSeries script files so that you can process audit logs in any library you specify. This feature is referred to as **library independence**.

To specify your own audit library:

Before starting this procedure, make sure you have already downloaded and extracted the ZIP archive as described earlier.

1. Open the **auditsftpc.txt** file in an editor.
2. Replace the AUDITLIB value in the **&LIBVARUC DCL** variable with the value for your library name.
3. Save the file and continue to set up the scripts as described below.
4. Repeat steps 1–3 for **AS400SAVCR.txt** and **AS400RST**.txt.

Note: All references to the AUDITLIB library in this document and in all other iSeries notes and software should be regarded as the library name that you have used in the **VALUE** parameter of the **&LIBVARUC** variable.

Set up the IBM iSeries Command File

Note: If you choose to use the default, then you must create an IFS file in the: /home/sftpinfodir/ directory name: sftpput.txt. This file will contain the SFTP commands from the sftpcmd.txt.IBMISERIES file.

The script file is **sftpcmd.txt.IBMISERIES**. This SFTP script is called by program AUDITLIB/AUDITSFTPC to send the audit data to the RSA NetWitness Suite.

To set up the iSeries command file:

1. Follow the program setup instructions in the command file for the transfer protocol (SFTP) that you are using:
   - Use **auditsftpc.txt**.

   Note: After you transfer a script file to the iSeries platform, set its CL program member type to **CLP**.
2. In the instructions for the command file, you need to replace some text with the actual IP address of the iSeries event source on the RSA NetWitness Suite appliance. The **sftpcmd.txt.IBMISERIES** command file has a line with a placeholder for a directory name on the RSA NetWitness Suite appliance: **ISERIES_10.100.255.255**. You need to replace "10.100.255.255" with the actual IP Address of the iSeries event source that you use.
3. For SFTP, rename sftpcmd.txt.IBMISERIES to SFTPCMD before uploading the file to the iSeries / AS400.
4. Follow the program run instructions in the appropriate file to transfer the log data to the RSA NetWitness Suite.

Selecting Specific Entry Types to Collect

The **auditsftpc.txt** CL program automatically selects all Entry Types for Journal Code T. To select specific Entry Types you can add an ENTTYP parameter to the DSPJRN command, for example:

```
ENTTYP(AF CA CP CY SO VN PW VP VR)
```

Starting the Collection Process from the Present Time

If you have been writing to the iSeries journal for a period of time and are concerned about running the script files for the first time, you may want to follow one of these suggestions, to start the collection process at the present time, rather than at some time in the past:

- Comment out the QSH command in **AUDITSFTPC.txt** for the first run.
- Pre-populate the AUDITLIB/TIME and AUDITLIB/DATE files with the date from which to start collecting. Otherwise, the script uses the last time that the audit data was read from the Audit Journal.

Restore a *PGM Object File from a *SAVF Object

1. Transfer the AS400SAVCR.txt file from the server to AS400SAVCR type CLP in the PF-SRC file on your AS400.
   - This file must be transferred as an ASCII file.
   - Compile the AS400SAVCR type CLP program and run AS400SAVCR. This will create / pre-allocate an empty *SAVF file in the AUDITLIB library named AS400EXT *SAVF.
2. Transfer the AS400EXT.SAVF file from the server to the empty AS400EXT *SAVF file that was pre-allocated on your AS400 in AUDITLIB by step 1.
   - This file must be transferred as a binary file.
   - This will populate the AS400EXT member in the pre-allocated AS400EXT *SAVF file.
3. Transfer the AS400RST.txt file from the server to AS400RST type CLP in the PF-SRC file on your AS400.
   - This file must be transferred as an ASCII file.
   - Compile the AS400RST type CLP program and run AS400RST. This will restore the AS400EXT *SAVF file in the AUDITLIB library to the AS400EXT *PGM executable program file.
4. The AS400EXT program is now available for use by the new AUDITPGMC and/or AUDITSFTPC CL programs.
   - The following file can be deleted from the AUDITLIB library
     - AS400EXT *SAVF.
     - AS400SAVCR *PGM.
     - AS400RST *PGM.
   - The following files can be deleted from your PF-SRC file:
     - AS400SAVCR type CLP.
     - AS400RST type CLP.

iSeries Audit Journal Entry Types Supported by the NetWitness Suite

Code	Entry	Description
D	CG	Change file
D	CT	Create Database File
D	DF	File was deleted
D	DH	File saved
D	DZ	File restored
D	FM	File moved to different library (MOVOBJ or RNMOBJ OBJTYPE(*LIB))
F	DE	Physical file member deleted record count
F	DM	Delete member
F	FD	Physical file member forced (written) to auxiliary storage
F	JC	Change journaled object attribute
F	MR	Physical file member restored (RSTOBJ or RSTLIB)
F	MS	Physical file member saved (SAVOBJ, SAVLIB, or SAVCHGOBJ)
F	PD	Database file member's access path deleted (this entry is created when you remove the member (RMVM) or delete the file (DLTF) containing the member)
T	AD	A change was made to the auditing attribute

Code	Entry	Description
T	AF	All Authority failures
T	AP	A change was made to program adopt
T	AU	Attribute change
T	CA	Changes to object authority (authorization list or object)
T	CD	A change was made to a command string
T	CO	Create object
T	CP	Create, change, restore user profiles
T	CQ	A change was made to a change request descriptor
T	CU	Cluster Operation
T	CV	Connection verification
T	CY	Cryptographic Configuration
T	DI	Directory Services
T	DO	All delete operations on the system
T	DS	DST security password reset
T	EV	Environment variable
T	GR	General purpose audit record
T	GS	A descriptor was given
T	IP	Inter-process communication event
T	IR	IP rules actions
T	IS	Internet security management

Code	Entry	Description
T	JD	Changes to the USER parameter of a job description
T	JS	A change was made to job data
T	KF	Key ring file name
T	LD	A link, unlink, or lookup operation to a directory
T	ML	A change was made to office services mail
T	NA	Changes to network attributes
T	ND	Directory search violations
T	NE	End point violations
T	O1	Single optical object access
T	O2	Dual optical object access
T	O3	Optical volume access
T	OM	Object management change
T	OR	Object restored
T	OW	Changes to object ownership
T	PA	Changes to programs (CHGPGM) that will now adopt the owner's authority
T	PG	Changes to an object's primary group
T	PO	A change was made to printed output
T	PS	Profile swap
T	PW	Passwords used that are not valid
T	RA	Restore of objects when authority changes

Code	Entry	Description
T	RJ	Restore of job descriptions that contain user profile names
T	RO	Restore of objects when ownership information changes
T	RP	Restore of programs that adopt their owner's authority
T	RQ	A change request descriptor was restored
T	RU	Restore of authority for user profiles
T	RZ	The primary group for an object was changed during a restore operation
T	SD	A change was made to the system directory
T	SE	Changes to subsystem routing
T	SF	A change was made to a spooled output file
T	SG	Asynchronous Signals
T	SK	Secure sockets connections
T	SM	A change was made by system management
T	SO	A change was made by server security
T	ST	A change was made by system tools
T	SV	Changes to system values
T	VA	Changes to access control list
T	VC	Connection started or ended
T	VF	Server files were closed
T	VL	An account limit was exceeded
T	VN	A logon or logoff operation on the network

Code	Entry	Description
T	VO	Actions on validation lists
T	VP	A Network password error
T	VR	A Network resource was accessed
T	VS	A server session started or ended
T	VU	A network profile was changed
T	VV	Service status was changed
T	X0	Network authentication
T	X1	Reserved for future audit entry
T	X2	Reserved for future audit entry
T	X3	Reserved for future audit entry
T	X4	Reserved for future audit entry
T	X5	Reserved for future audit entry
T	X6	Reserved for future audit entry
T	X7	Reserved for future audit entry
T	X8	Reserved for future audit entry
t	X9	Reserved for future audit entry
T	YC	A change was made to DLO change access
T	YR	A change was made to DLO read access
T	ZC	A change was made to object change access
T	zm	An object was accessed using a method
T	ZR	A change was made to Object read access

Trademarks