RSA NetWitness Logs

Event Source Log Configuration Guide

IBM Mainframe DB2 for z/OS

Last Modified: Monday, October 9, 2017

Event Source Product Information:

Vendor: IBM
Event Source: DB2 Universal Database
Versions: 9.1, 10.1, 11.1
Platforms: Mainframe z/OS v1.9, v1.10, v1.11, v1.12, v1.13, v2.1 and v2.2
Additional Downloads:

- DB2GRABR.cfg
- DB2SFTP.jcl
- SFTPCMD.txt.IBMDB2
- DB2GRABR_v9.trs
- DB2GRABR_v10.trs
- DB2GRABR_v11.trs

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: ibmdb2
Collection Method: File
Event Source Class.Subclass: Storage.Database

To configure IBM Mainframe DB2 to work with RSA NetWitness Suite, you must complete these tasks:

I. Configure IBM Mainframe DB2

II. Configure NetWitness Suite for File Collection

Configure IBM Mainframe DB2

To configure IBM Mainframe DB2 UDB:

1. Use a browser to navigate to the IBM Mainframe DB2 Additional Downloads page in the RSA NetWitness® Event Source Downloads space.
2. Download the following files:
   - **DB2GRABR.cfg**
   - For SFTP, download **DB2SFTP.jcl** and **SFTPCMD.txt.IBMDB2**. Follow the setup instructions in those files.
   - Download the appropriate TRS file for your system:
     - DB2GRABR_v9.trs
     - DB2GRABR_v10.trs
     - DB2GRABR_v11.trs
3. To configure the 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:

      Note: If your DB2 V10 (or above) configuration uses the SMF Type 101 and 102 record compression feature, the file that is used for SMFIN must be decompressed before running DB2GRABR.

      - In the **SMFIN** field, specify the SMF dataset to be processed by DB2GRABR.
      - In the **OUTPUT** field, specify the sequential file generated by DB2GRABR to be used as input to the **SFTP step**.
      - (Optional) In the **CONFIG** field, specify the dataset containing the configuration file, or change the DD statement to //**CFG DD DUMMY**.
      - Rename SFTPCMD.txt.IBMDB2 to SFTPCMD before uploading to the mainframe, then follow the instructions in the **DB2SFTP** and **SFTPCMD** 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:

- '/u/db2grabr/ascii.zOS_device.data' with your Unix HFS
directory and file name.

- 'var/netwitness/logcollector/upload/ibmdb2tvm/ibmdb2tvm/'
with the upload directory that the z/OS device event source
uses to communicate to the Security Analytics appliance.

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 appropriate TRS file for your system.

Note: If Unicode encoding is included in the SMF type 101 and 102 records that are processed by DB2GRABR, then use the appropriate TRS version to convert the Unicode encoded fields to EBCDIC:

- DB2GRABR_v9.trs for DB2 V9.1
- DB2GRABR_v10.trs for DB2 V10.1
- DB2GRABR_v11.trs for DB2 V11.1

Note: The TRS files are "TERSED" files containing the **DB2GRABR** 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 DB2GRABR.TRS file into a PDS containing the DB2GRABR program:

```
//UNLOAD JOB (T,JXPO,JKSD0093),TEST,
// MSGCLASS=P,
// REGION=0M
//*************************************************************
**********
//SET1 SET INFILE='YOUR_HIGH_LEVEL.DB2GRABR.TRS',
//     OUTFILE='YOUR_HIGH_LEVEL.DB2GRABR.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
//
```

Configure NetWitness Suite for File Collection

To configure File collection for IBM Mainframe DB2, complete the following tasks:

I. Generate the Key Pair

II. Configure the Log Collector for File collection

Generate the Key Pair

You need to generate a public/private key pair, and then add the public key to the Log Collector.

1. On the IBM DB2 Mainframe event source, run the following command to generate the public/private key pair:

   ```
   ssh-keygen -b 1024 -t rsa
   ```

   This command creates id_rsa in OpenSSH format, which is used by RSA NetWitness Suite. If your Linux system creates IETF SECSH format by default, run the following command to convert it:

   ```
   ssh-keygen -f ~/.ssh/id_rsa.pub -i
   ```

2. Copy the public key and save it in a temporary file so that you can paste it in RSA NetWitness Suite in step 7 in the following procedure, **Configure the Log Collector for File Collection**.

Configure the Log Collector for File Collection

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

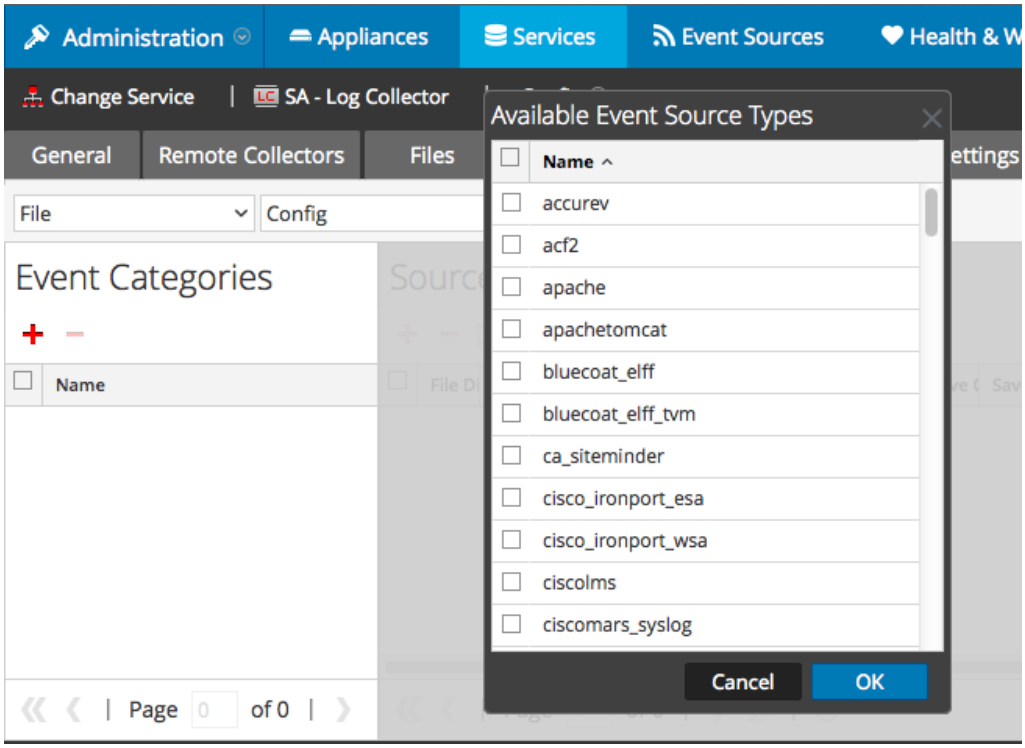
To configure the Log Collector for file collection:

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.

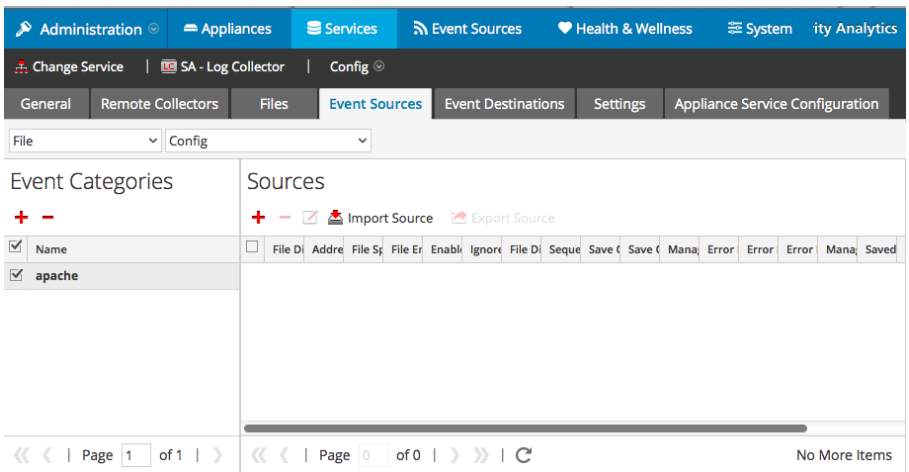


5. Select the correct type from the list, and click **OK**.

   Select **ibmdb2tvm** from the **Available Event Source Types** dialog.

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

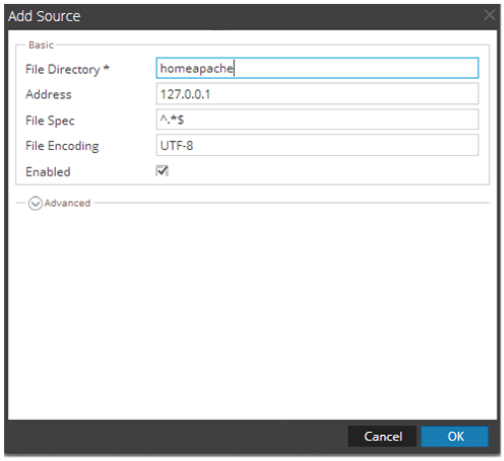
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

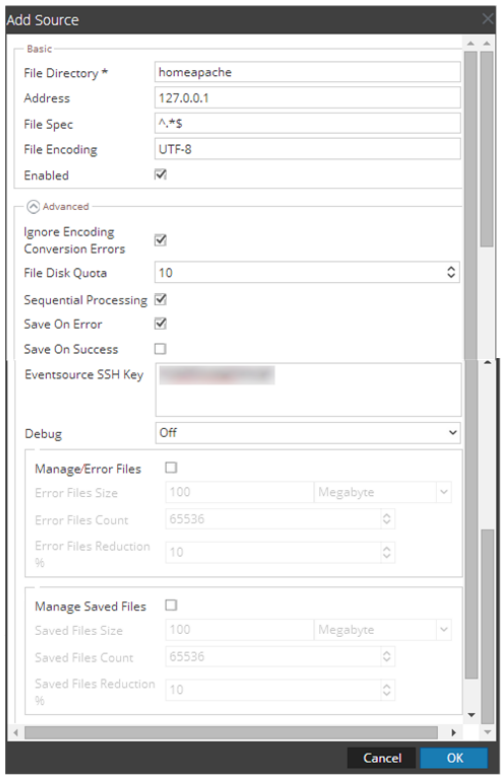


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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. Paste the public key that you generated earlier into the **Eventsource SSH Key** field.
8. Add a File Directory name, modify any other parameters that require changes, and click **OK**.
9. 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