RSA NetWitness Logs

Event Source Log Configuration Guide

IBM WebSphere Application Server

Last Modified: Monday, May 22, 2017

Event Source Product Information:

Vendor: IBM
Event Source: WebSphere
Versions/Platforms:

- 6.0.0.1/Microsoft Windows 2003
- 8.0, 8.5/Microsoft Windows 2008 R2
- 7.0.0.9/Redhat Linux/Solaris/IBM AIX/Microsoft Windows 2003
- 6.0.0.1/IBM AIX (HTTP Server Logs

Additional Downloads: sftpagent.conf.websphere

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: ibmwebsphere
Collection Method: File
Event Source Class.Subclass: Host.Application Server

To configure IBM WebSphere Application Server to work with RSA NetWitness Suite, you must perform the following tasks:

I. Configure Logging in IBM WebSphere Application Server

II. Configure Logging in IBM HTTP Server

III. Configure Log Transfers from the WebSphere Server

IV. Configure NetWitness Suite for File Collection

Configure Logging in IBM WebSphere Application Server

RSA NetWitness Suite supports the following log files:

- For IBM WebSphere 6.0, **System.out**, **System.err**, and **Trace.log** files are supported.
- For IBM WebSphere 7.0 and later, **SystemOut.log** and **SystemErr.log** files are supported.
- For IBM WebSphere 8.5, RSA has added support for Security Auditing.

Configure System Logging on the IBM WebSphere Application Server

This section describes how to configure system logging on the WebSphere event source.

To configure logging in IBM WebSphere Application Server:

1. Access the WebSphere Administrative Console with administrative credentials.
2. To configure the JVM log settings, follow these steps:
   a. From the navigation pane, expand **Troubleshooting**, and select **Logs and trace**.
   b. From the **Logging and Tracing** section, select the server from which you want to capture logs.
   c. Click **JVM Logs**.
   d. In the **File Name** field, enter the log filename.

      Note: For IBM WebSphere 6.0, the filename must end in .out or .err.

   e. From the **File Formatting** drop-down list, select **Basic (Compatible)**.
   f. In the **Log File Rotation** section, configure the log rotation. For example, to roll the logs each day at midnight, type **1** in the **Start Time** field, and **24** in the **Repeat Time** field.
   g. In the **Maximum Number of Historical Log Files** field, enter a value that meets your business needs.

h. In the **Install Application Output** section, select **Show application print statements** and **Format print statements**.

i. Click **OK**.

j. After the page reloads, click **Save** from the message at the top of the page.

3. (Optional) On IBM WebSphere 6.0, to configure the diagnostic trace log settings, follow these steps:

Warning: If you are using IBM WebSphere 7.0 or later, do not configure diagnostic trace logs. Go to step 4.

Note: Enabling this log may produce excessive data and impact the server.

a. In the navigation pane, expand **Troubleshooting**, and select **Logs and trace**.

b. In the **Logging and Tracing** section, select the server from which you are going to capture logs.

c. Click **Diagnostic Trace**.

d. In the **Trace Output** section, select **File**.

e. In the **Maximum File Size** and **Maximum Number of Historical Files** fields, enter values that meet your business needs.

f. In the **File Name** field, enter the log filename.

Note: The filename must end in .log.

g. In the **Trace Output Format** drop-down list, ensure that **Basic (Compatible)** is selected.

h. Click **OK**.

i. After the page reloads, click **Save** in the message at the top of the page.

4. To change the log detail levels, follow these steps:

a. In the navigation pane, expand **Troubleshooting**, and select **Logs and trace**.

b. In the **Logging and Tracing** section, select the server from which you are going to capture logs.

c. Click **Change Log Detail Levels**.

d. Depending on your version of IBM WebSphere, do one of the following steps:

- For IBM WebSphere 6.0, expand **All Components**, and configure the specific logging levels for each class.
- For IBM WebSphere 7.0, in the **Groups** field, only type ***=info**.

e. Click **OK**.

f. After the page reloads, click **Save** in the message at the top of the page.

Configure Security Logging on the IBM WebSphere Application Server

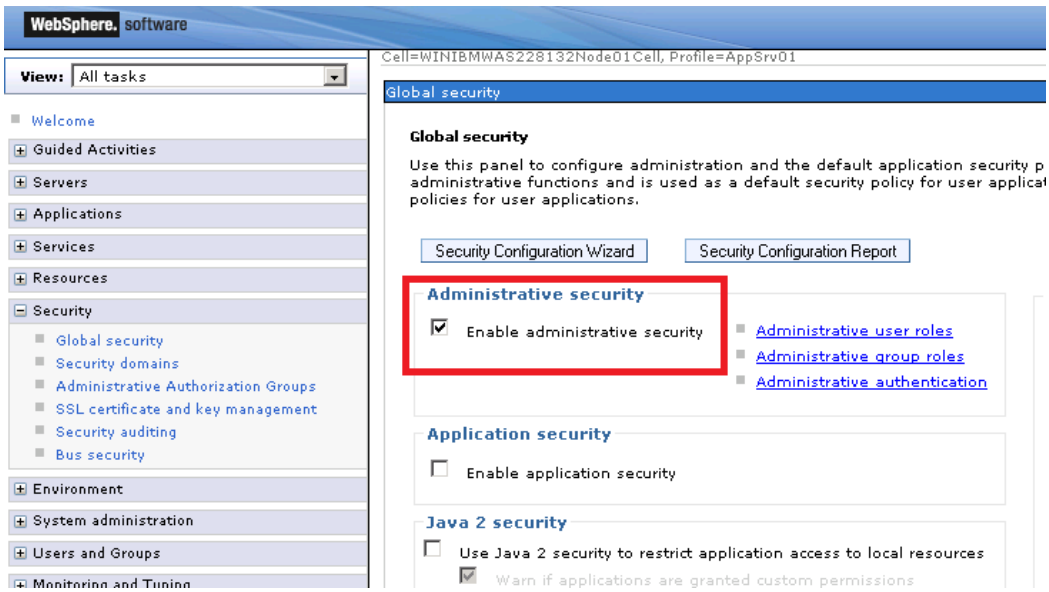
This section describes how to configure security logging on the WebSphere event source.

Note: Security logging is supported on Microsoft Windows 2008 R2 only.

First, ensure that administrative security is enabled.

To make sure administrative security is enabled:

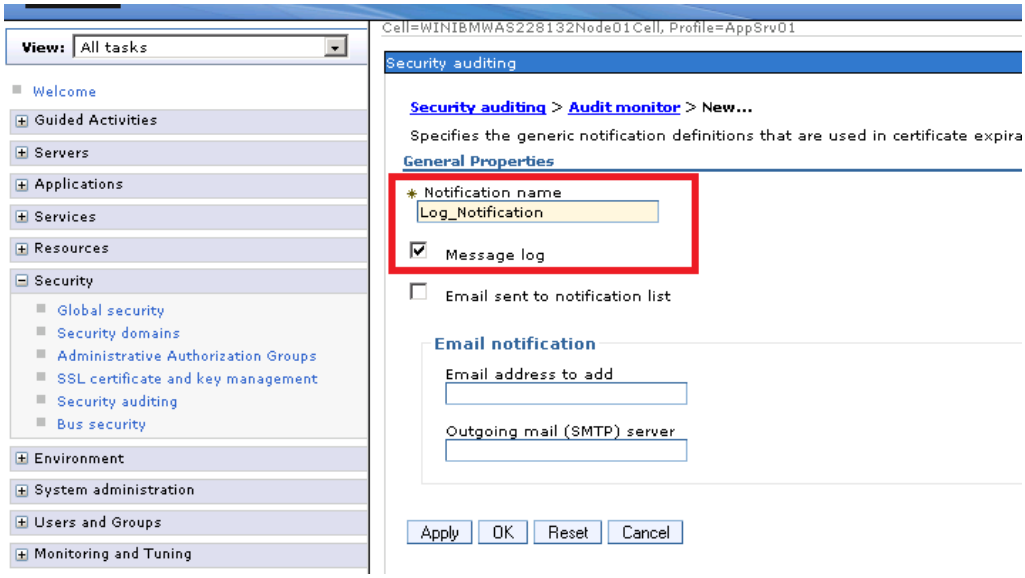
1. In the WebSphere administrative console, select **Security** > **Global security**.
2. Under **Administrative security**, ensure that **Enable administrative security** is selected.



Next, you turn on basic auditing functions and send the output to a log file.

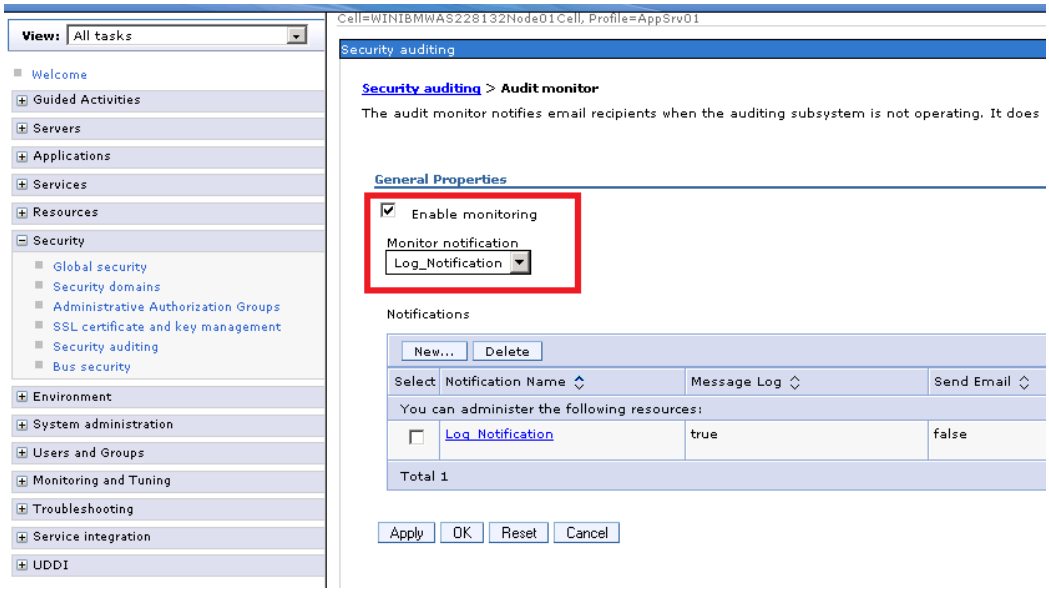
To turn on basic auditing functions:

1. In the WebSphere administrative console, select **Security** > **Security Auditing**.
2. Under **Related Items**, select **Audit monitor**.
3. Under **Notifications**, select **New**.
4. Enter a name in the **Notification name** field (for example, **Log_Notification**) and check the **Message log** box. Optionally, configure email notifications if needed.



> **Note:** Remember the name that you enter the **Notification name** field: you need to select it in step 6.

5. Click **Apply** and **Save**.
6. Now that a notification definition exists, you can configure auditing to use that notification. On the same screen, check the **Enable monitoring** box and verify that the name you entered in the **Notification name** field has been selected in the **Monitor notification** drop-down menu.



7. Click **Apply** and **Save**. This returns you to the main **Security auditing** screen.

Now that you have completed setting the configuration, you can enable auditing.

To enable auditing:

1. From the main Security auditing screen, check the **Enable security auditing** box.
2. From the **Audit subsystem failure action** drop-down menu, select **Log warning**.
3. From the **Primary auditor user name** drop-down menu, select a user that has been assigned the **Auditor** role. For details on adding and editing users, refer to your WebSphere Administrator documentation.
4. Click **Apply** and **Save**.
5. Restart the server to have these changes take effect.

Configure Logging in IBM HTTP Server

To configure logging in IBM HTTP Server, do one of the following:

Note: RSA supports custom and common logging formats. More information is captured if the custom logging format is used.

- For custom logging, verify that the following lines are present and not commented out in the **httpd.conf** file on the IBM HTTTP server:

  ```
  LogFormat "%h %l %u %t \"%m \"%V\" \"%U\" \"%q\" %H\"
  %>s %b \"%{Referer}i\" \"%{User-Agent}i\" \"%
  {Cookie}i\"" custom
  ```

  ```
  CustomLog "|/home/IBM/HTTPServer/bin/rotatelogs
  /home/IBM/HTTPServer/logs/access.log 86400" custom
  ```

  where */home/IBM/HTTPServer/bin/rotatelogs* is the location of rotatelogs

  where */home/IBM/HTTPServer/logs/access.log* is the location where you want access logs to be stored.

  where *86400* represents the number of seconds to keep the current log file open before rotating it and starting a new log.

- For common logging, verify the following lines are present and not commented out in the **httpd.conf** file on the IBM HTTP server:

  ```
  LogFormat "%h %l %u %t %r %>s %b" common
  ```

  ```
  CustomLog "|/home/IBM/HTTPServer/bin/rotatelogs
  /home/IBM/HTTPServer/logs/access.log 86400" common
  ```

  where *86400* represents the number of seconds to keep the current log file open before rotating it and starting a new log.

Configure Log Transfers from the WebSphere Server

To configure file transfers:

1. On the WebSphere server where the logs are being saved, install and set up the SFTP Agent. To set up the SFTP Agent Collector, visit 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
2. Depending on your operating system, follow one of these steps:
   - For Linux, AIX, and Solaris, you must follow the steps in Configure SA SFTP Agent shell script.

     Warning: The Shell Script File Transfer document directs you to download the **nicsftpagent.sh** file. In that file, you must set the `FILESPEC= parameter` to **System*.log**.
   - For AIX, RSA supports HTTP Server logs. To transfer these logs to RSA NetWitness Suite, you need an additional **nicsftpagent1.sh** file.

     Warning: The Shell Script File Transfer document directs you to download the **nicsftpagent.sh** file. Change the file name to **nicsftpagent1.sh** if **nicsftpagent.sh** has already been used by IBM Websphere logs. In that file, you must set the FILESPEC=parameter to **access.log.***. The file path to where the logs are to be collected is mentioned when you configure httpd.conf file.
   - For Windows, edit the log file paths in the **sftpagent.conf.websphere** file in the install directory of the SFTP Agent to match the location of the logs that you set up in Task I. Follow these steps:
     a. Specify the following paths as shown in this table:

        `file0=`***`SystemOut`***, where ***SystemOut*** is the file path of the Out log files.

        `file1=`***`SystemErr`***, where ***SystemErr*** is the file path of the Error log files.

        For WebSphere v6 only: `file2=`***`TraceLogs`***, where ***TraceLogs*** is the file path of the Trace log files.

For WebShere 8.5 only: `file3=`***`BinaryAuditLogs`***, where ***BinaryAuditLogs*** is the path of the binary audit logs. The binary audit logs path has the following format:

`BinaryAudit_`***`<cell>_<node><server>`***`.log`

The following is an example:

```
BinaryAudit_WINIBMWAS228132Node01Cell_
WINIBMWAS228132Node01_server1.log
```

b. Rename the **sftpagent.conf.websphere** file to **sftpagent.conf**.

Note: The file paths vary depending on your platform. For example, the SystemOut log file path could be set as one of the following:

On Windows:

```
C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\
SystemOut.log
```

On Linux:

```
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1/SystemOut.log
```

On AIX

```
/usr/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1/SystemOut.log
```

On Solaris:

```
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1/SystemOut.log
```

3. If you have servers with multiple profiles, repeat step 2 for each profile folder of the application server instance, specifying file paths for each profile.

Configure NetWitness Suite for File Collection

Configure the Log Collector for File Collection

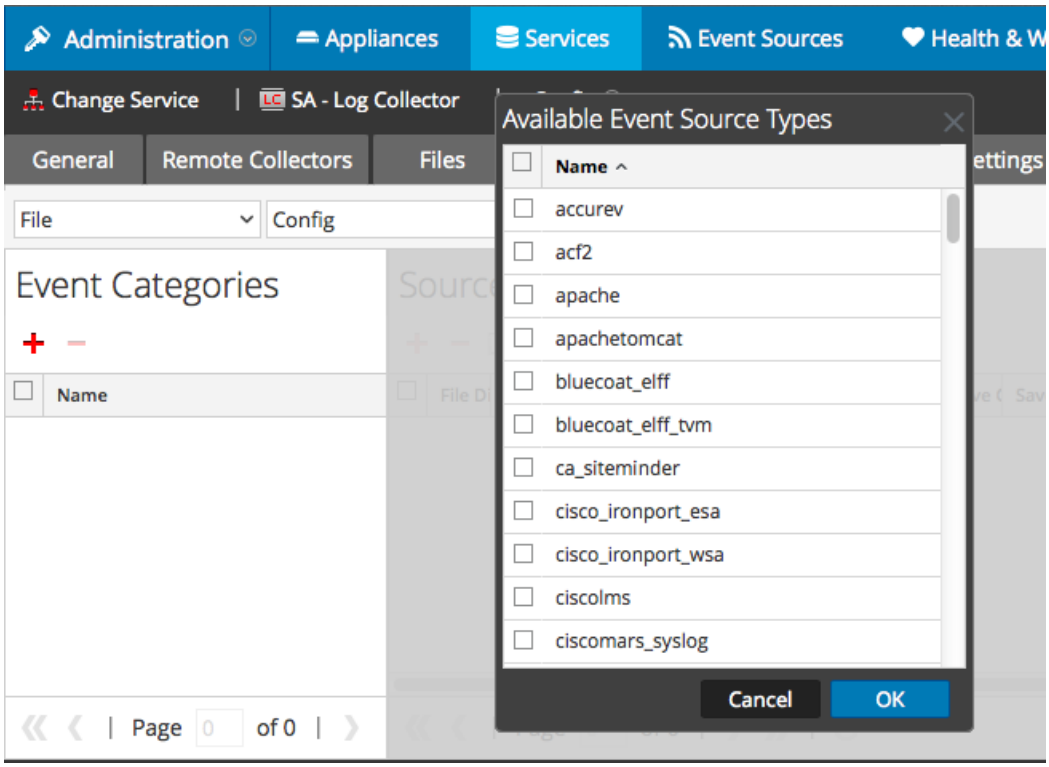
Perform the following steps to configure the Log Collector for File collection.

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 +.

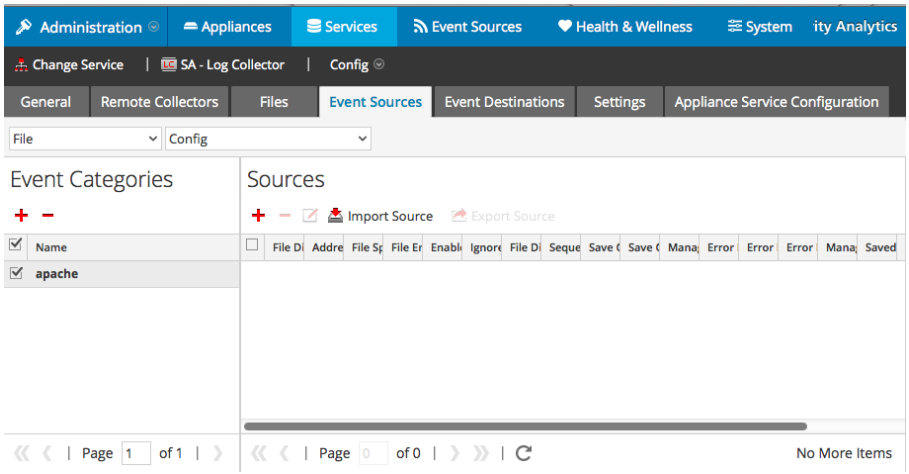
   The Available Event Source Types dialog is displayed.



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

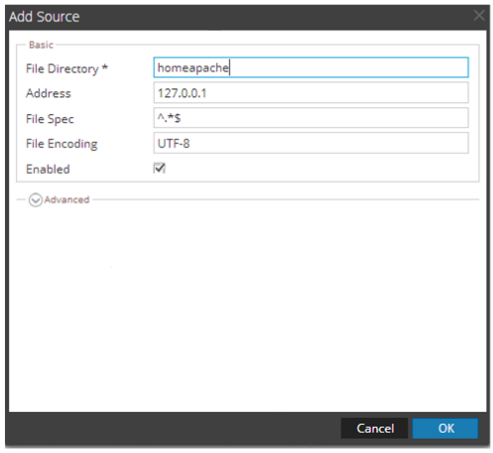
Select **ibmwebsphere** from the **Available Event Source Types** dialog.

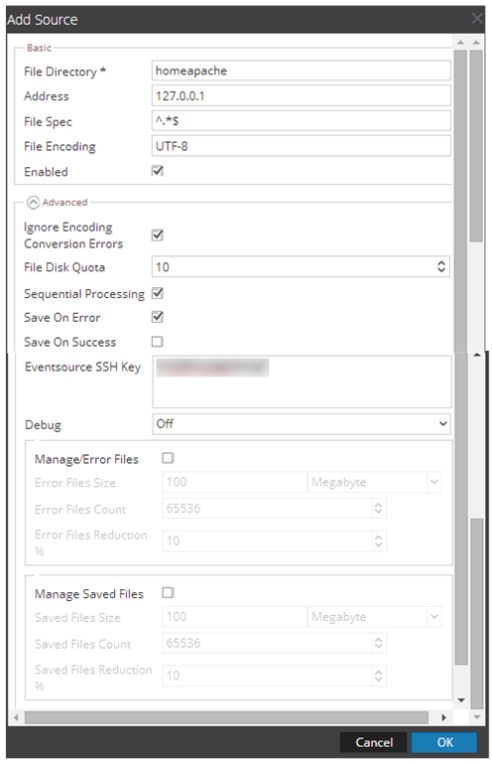
The newly added event source type is displayed in the Event Categories panel.



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.

Trademarks