RSA NetWitness Platform

Event Source Log Configuration Guide

Microsoft Internet Information Services

Last Modified: Wednesday, September 25, 2019

Event Source Product Information:

Vendor: Microsoft
Event Source: Internet Information Services
Versions: 5.x, 6.x, 7.x, 8.x, 10.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

Additional Downloads: sftpagent.conf.microsoftiis

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: microsoftiis
Collection Method: File
Event Source Class.Subclass: Host.Web Logs

To configure Microsoft IIS to work with RSA NetWitness Platform, complete the following tasks:

I. Configure Microsoft IIS

II. Configure NetWitness Platform for File Collection

Configure Microsoft IIS

Depending on your version of Microsoft IIS, complete one of the following tasks:

- Configure Microsoft IIS 8.x and 10.x
- Configure Microsoft IIS 7.x
- Configure Microsoft IIS 6.x
- Configure Microsoft IIS 5.x

Note: If you are using Content 1.0 to collect logs for Microsoft IIS, make sure to select all W3C Logging Fields.

Configure Microsoft IIS 8.x and 10.x

To configure IIS 8.x and 10.x:

1. Open the Microsoft IIS Server Manager Utility.
2. In the **Connections** pane, select the service for which you want to enable logging, for example, **ComputerName** > **Sites** > **Default Web Site**.
3. In the **Features View** area, double-click **Logging**.
4. In the **Log File** section, from the **Format** drop-down list, select **W3C**.
5. Click **Select Fields**.
6. In the W3C Logging Fields dialogue box, select **cs-method** and any other options that you want.

   Note: You must select **cs-method**. All other selections are optional.
7. Click **OK**.
8. In the **Log File Rollover** section, select **Schedule**, and from the drop-down list, select **Daily**.
9. In the **Actions** pane, click **Apply**.

10. Repeat steps 1 through 10 for each service for which you want to manage logs. Substitute the other services for the **Sites** folder in step 3.

Configure Microsoft IIS 7.x

To configure IIS 7.x:

1. Open the Microsoft IIS Server Manager Utility.
2. In the console tree, click **Server Manager** > **Roles** > **Web Server(IIS)** > **Internet Information Services (IIS) Manager**.
3. Select the service for which you want to enable logging, for example, **ComputerName** > **Sites** > **Default Web Site**.
4. In the **Groups** area, double-click **Logging**.
5. In the **Log File** section, from the **Format** drop-down list, select **W3C**.
6. Click **Select Fields**.
7. In the W3C Logging Fields dialogue box, select **cs-method** and any other options that you want.

   Note: You must select **cs-method**. All other selections are optional.
8. Click **OK**.
9. In the **Log File Rollover** section, select **Schedule**, and from the drop-down list, select **Daily**.
10. In the **Actions** pane, click **Apply**.
11. Repeat steps 1 through 10 for each service for which you want to manage logs. Substitute the other services for the **Sites** folder in step 3.

Configure Microsoft IIS 6.x

To configure IIS 6.x:

1. To open the Microsoft IIS Manager Utility, click **Start** > **Administrative Tools** > **Internet Information Services Manager**.
2. In the console tree, browse to the network service that you want to monitor, for example, **ComputerName** > **Web Sites**.

3. Right-click the **Web Sites** folder, and click **Properties**.
4. On the **Web Site** tab, select **Enable Logging**, and from the **Active log format** drop-down list, select **W3C Extended Log File Format**.
5. Click **Properties**.
6. In the Logging Properties window, in the **New log schedule** field, select **Hourly**.
7. Write down the directory shown in the **Log file directory** field at the bottom of the Logging Properties window. You need this information when you set up the NIC FTP Agent or NIC SFTP Agent.
8. On the **Extended Properties** tab, ensure that the following extended logging options are selected:
   - Date
   - Time
   - All of the **Extended Properties**.
9. Click **Apply**.
10. In the Inheritance Override pop-up window, select **cs-method** and any other options that you want. Repeat this for each Inheritance Override pop-up window that opens.

    Note: You must select **cs-method**. All other selections are optional.
11. Click **OK** .
12. Repeat steps 1 through 12 for each network service for which you want to manage logs. Substitute the other network services for the Web Site folder selected in step 3.

Configure Microsoft IIS 5.x

To configure IIS 5.x:

1. In the Microsoft IIS Management interface, on the **Web Sites** tab, select **Properties**.
2. Select **Enable Logging**, and, from the **Active log format** drop-down list, select **W3C Extended Log File Format**.
3. Click **Properties**, and in the **New log time period** field, select **Hourly**.

4. Write down the directory shown in the **Log file directory** field at the bottom of the Logging Properties window. You need this information when you set up the NIC FTP Agent or NIC SFTP Agent.
5. On the **Advanced** tab, follow these steps to configure extended logging properties:
   a. Select **Date**.
   b. Select **Time**
   c. Select all of the **Extended Properties**.

   Note: Do not select **Process Accounting**.
6. Click **Apply**.
7. In the Inheritance Override pop-up window, select **cs-method** and any other options that you want. Repeat this for each Inheritance Override pop-up window that opens.

   Note: You must select **cs-method**. All other selections are optional.
8. Click **OK**.
9. Repeat steps 1 through 8 for each server type for which you want to manage logs. Substitute the server type name for the **Web Sites** tab selected in step 1.

Configure NetWitness Platform for File Collection

You must complete these tasks to configure RSA NetWitness Platform for File Collection.

I. Set up the SFTP Agent

II. Configure the Log Collector for File Collection

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

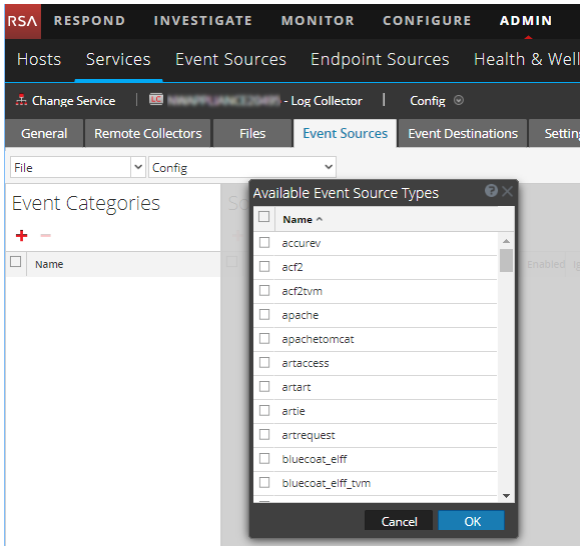
Perform the following steps to configure the Log Collector for File collection.

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.

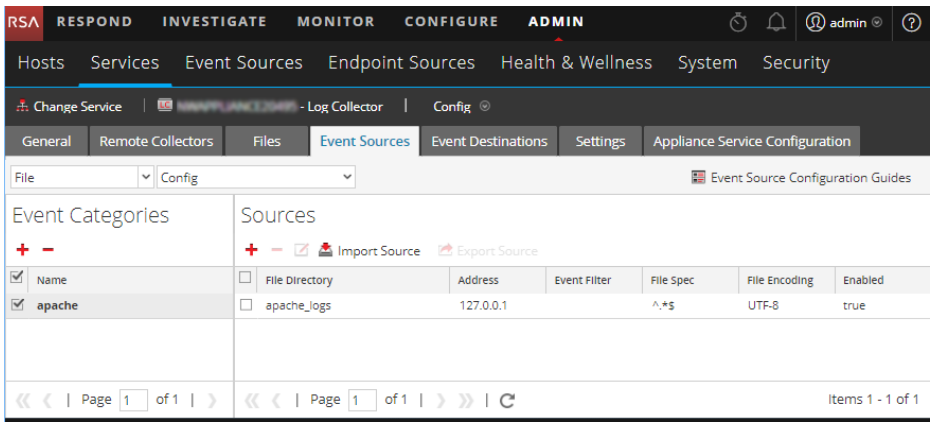


5. Select the correct type from the list, and click **OK**.

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

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

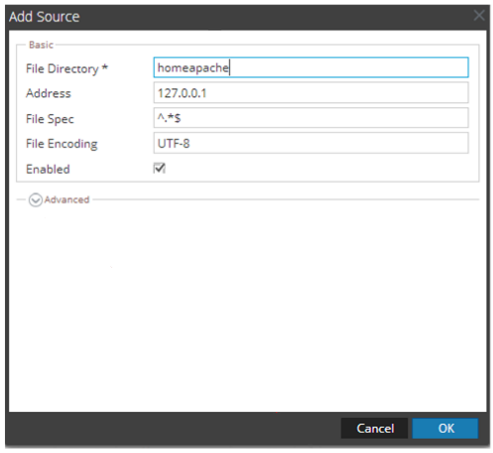
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

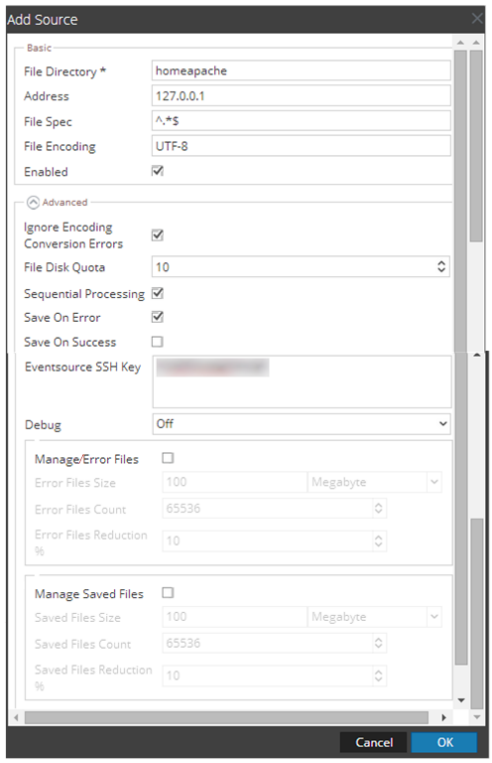


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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. 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.