RSA NetWitness Logs

Event Source Log Configuration Guide

Microsoft Internet Security and Acceleration Server

Last Modified: Thursday, June 08, 2017

Event Source Product Information:

Vendor: Microsoft
Event Source: Internet Security and Acceleration Server
Versions: 2000, 2004, 2006
Additional Download: sftpagent.conf.msisa

RSA Product Information:

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

To configure Microsoft ISA Server, you must complete these tasks:

I. Configure your version of Microsoft ISA Server

II. Set Up the SFTP Agent

III. Set up the File Service

Configure Microsoft ISA Server

The instructions are specific to the version of Microsoft ISA Server.

Microsoft ISA Server 2004 and 2006

To configure Microsoft ISA Server 2004 or 2006:

1. Click **Start > Programs > Microsoft ISA Server > ISA Server Management**.
2. Expand the target array, and select **Monitoring**.
3. Click the **Logging** tab.
4. From the **Tasks** list, select **Configure Firewall Logging**.
5. In the Firewall Logging Properties window, on the **Logs** tab, follow these steps to configure log storage:
   a. Under **Log storage format**, select **File**, and, from the **Format** list, select **W3C extended log file format**.
   b. Select **Enable logging for this service**.
6. On the **Fields** tab, click **Select All**.
7. Click **OK**.
8. From the **Tasks List**, select **Configure Web Proxy Logging**.
9. In the Web Proxy Logging Properties window, on the **Logs** tab, follow these steps to configure log storage:
   a. Under **Log storage format**, select **File**, and, from the **Format** list, select **W3C extended log file format**.
   b. Select **Enable logging for this service**.
10. On the **Fields** tab, click **Select All**.
11. Click **OK**.
12. Click **Apply**.

Microsoft ISA Server 2000

To configure Microsoft ISA Server 2000:

1. Click **Start > Programs > Microsoft ISA Server > ISA Management**.
2. Expand the target array, and then expand **Monitoring Configuration**.
3. Select the **Logs** folder.
4. Double-click **Packet filter** in the right-hand pane to open the properties sheet.
5. On the **Log** tab, follow these steps to configure log storage:
   a. Under **Log storage format**, select **File**.
   b. From the **Format** list, select **W3C extended log file format**.
   c. From the **Create a new file** list, select one of **Daily**, **Weekly**, **Monthly**, or **Yearly**.
   d. Ensure that **Enable logging for this service** is selected.
   e. Under **File**, click **Options**.
   f. Select **ISA Logs folder** to store the log files in the default folder, or select **Other folder** to browse for a location.
   g. (Optional) Select **log file compression** and **log file number limits**.
   h. Click **OK**.
6. On the **Fields** tab, click **Select All**.
7. Repeat steps 4 through 6 for **ISA Server Firewall service** and **ISA Server Web Proxy service**.
8. Click **OK**.

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

Configure the Log Collector for File Collection

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

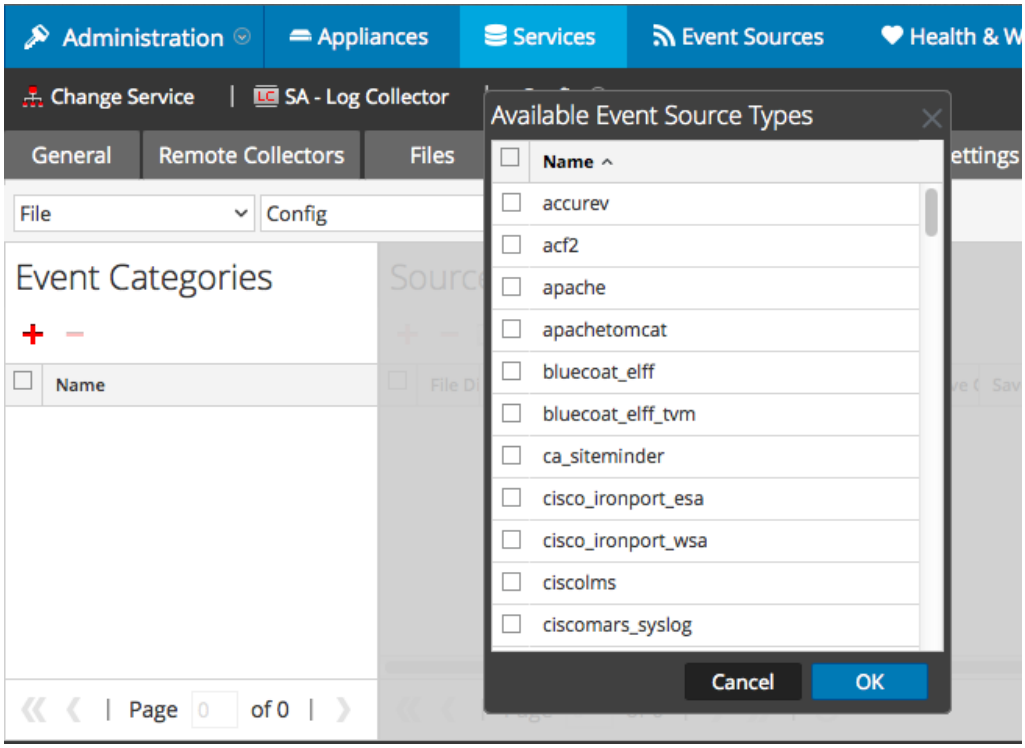
To configure the Log Collector for file collection:

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.

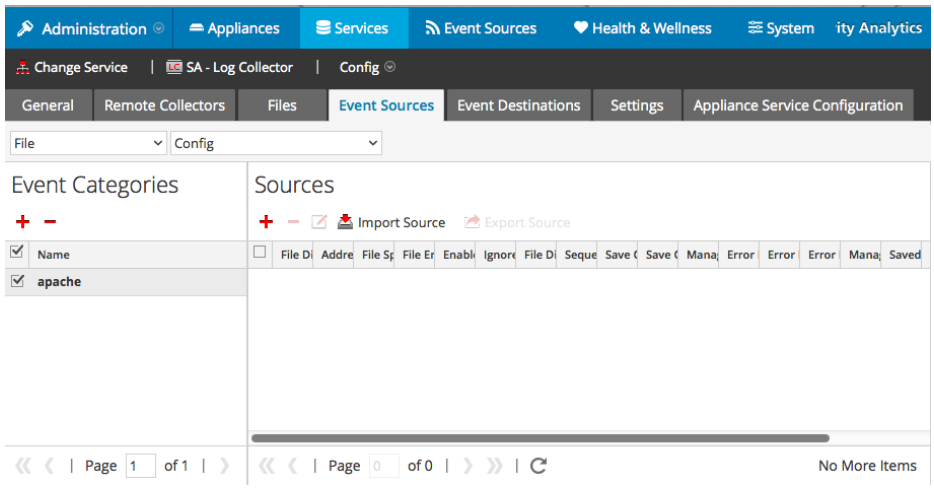


5. Select the correct type from the list, and click **OK**.

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

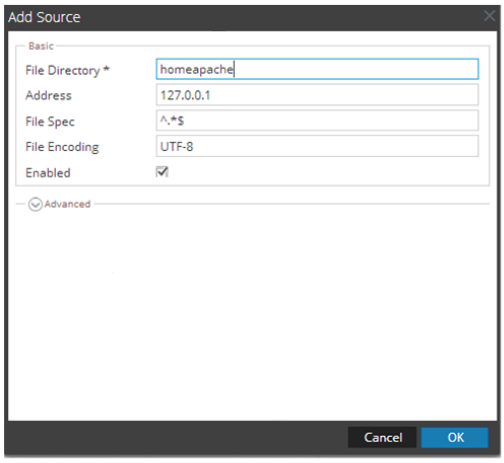
   The newly added event source type is displayed in the Event Categories

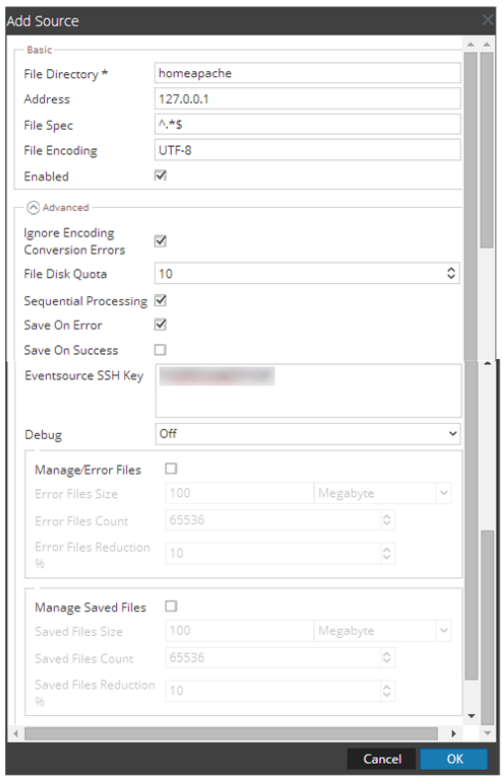
panel.



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