RSA NetWitness Platform

Event Source Log Configuration Guide

SQUID

Last Modified: Friday, May 22, 2020

Event Source Product Information:

Vendor: Open source
Event Source: Squid
Versions: 2.5.9, 2.7, 3.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: nicsftpagent.conf.squid

RSA Product Information:

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

To configure SQUID, you must complete these tasks:

I. Configure SQUID to generate logs

II. Configure RSA NetWitness Platform for File Collection

Configure Squid Log Format

RSA NetWitness Platform supports two log formats for Squid:

- Custom Squid Log Format

  Note: Squid 2.5.9 does not support RSA custom Squid log format.

- Squid native log format

For Version 3.1 and Later

For version 3.1, Squid has updated their log format. Use the following procedures to configure Squid log format for versions 3.1 and later.

To configure custom Squid log format for version 3.1 and later:

1. Locate the **squid.conf** file on your system. The default locations are as follows:

Operating System	Path
Ubuntu	/etc/squid
Redhat Linux	/etc/sysconfig/squid

2. In the **squid.conf** file, add the following two lines:

```
logformat custom_squid %>a %>p [%tl] "%rm %ru HTTP/%rv" %<A %ui %un "%rp"
%>Hs %mt %<st "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh

access_log /usr/local/squid/var/logs/access.log custom_squid
```

   Note: Make sure to add the first line of the above text (**bolded line**) on a single line, without any line breaks.

To configure Squid native log format for version 3.1 and later:

1. Locate the **squid.conf** file on your system. The default locations are as follows:

Operating System	Path
Ubuntu	/etc/squid
Redhat Linux	/etc/sysconfig/squid

2. In the **squid.conf** file, add the following lines:

```
logformat squid %ts.%03tu %6tr %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A
%mt

access_log /usr/local/squid/var/logs/access.log squid
```

For Versions Prior to 3.1

For Squid versions prior to 3.1, use the following procedures.

To configure custom Squid log format:

1. Locate the **squid.conf** file on your system. The default locations are as follows:

Operating System	Path
Ubuntu	/etc/squid
Redhat Linux	/etc/sysconfig/squid

2. In the **squid.conf** file, add the following two lines:

```
logformat custom_squid %>a %>p [%tl] "%rm %ru HTTP/%rv" %<A %ui %un
"%rp" %Hs %mt %<st "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh

access_log /usr/local/squid/var/logs/access.log custom_squid
```

Note: Make sure to add the first line of the above text (**bolded line**) on a single line, without any line breaks.

To configure Squid native log format:

1. Locate the **squid.conf** file on your system. The default locations are as follows:

Operating System	Path
Ubuntu	/etc/squid
Redhat Linux	/etc/sysconfig/squid

2. In the **squid.conf** file, add the following lines:

```
logformat squid %ts.%03tu %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /usr/local/squid/var/logs/access.log squid
```

Configure 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

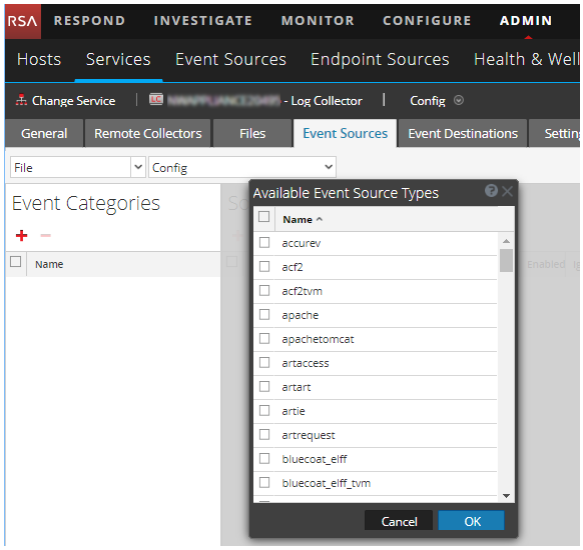
Perform the following steps to configure the Log Collector for File collection.

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.

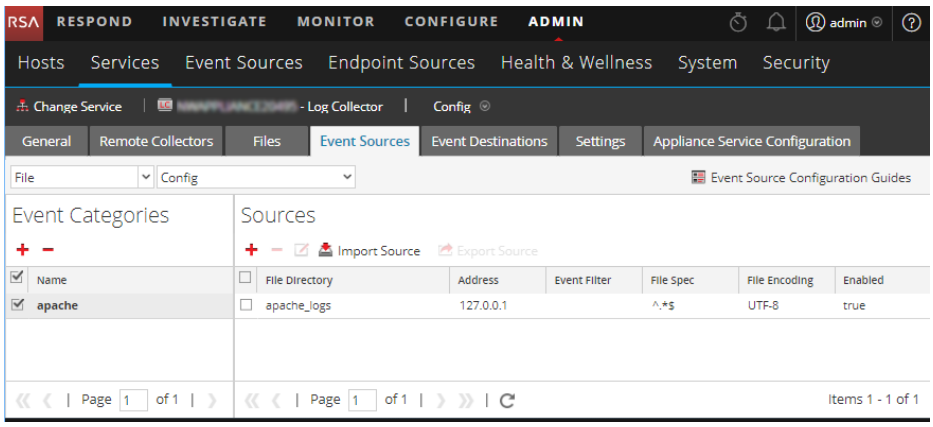


5. Select the correct type from the list, and click **OK**.

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

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

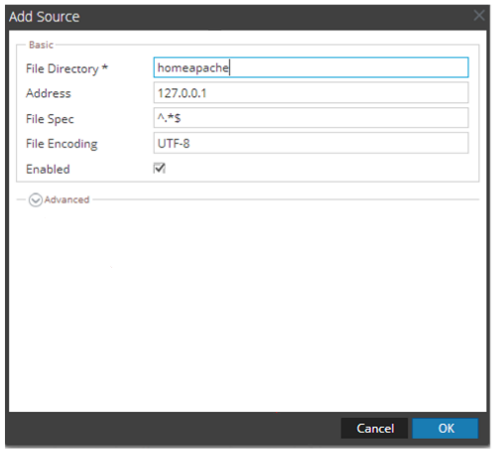
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

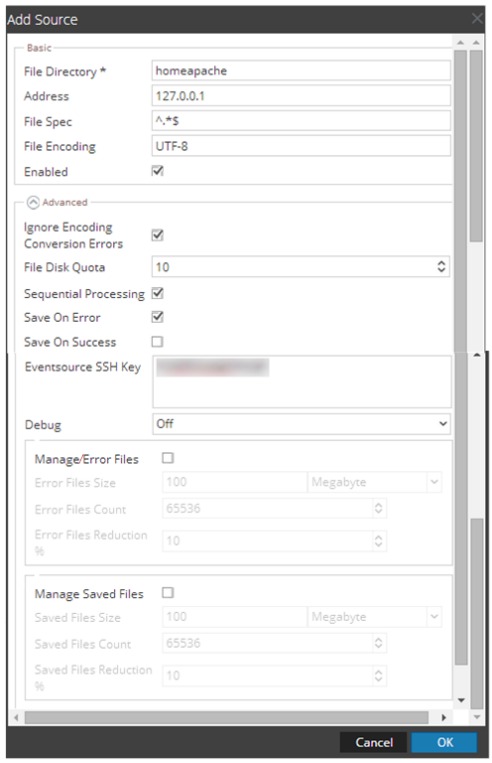


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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.