RSA NetWitness Logs

Event Source Log Configuration Guide

SonicWall E-Class SRA

Last Modified: Monday, November 20, 2017

Event Source Product Information:

Vendor: SonicWall
Event Source: E-Class SRA
Versions: 8.8, 9.0, 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.

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: aventail
Collection Method: File, Syslog
Event Source Class.Subclass: Security.VPN

Note: RSA supports only SonicWall E-Class SRA 10.0 for syslog collection.

You can configure SonicWall E-Class SRA to do one of the following:

- Collect FTP log files
- Collect Syslog

Collect FTP Log Files

You must perform these tasks to configure SonicWall E-Class SRA for FTP collection:

I. Configure SonicWall E-Class SRA for log file collection.

II. Configure the RSA NetWitness Suite Log Collector for File Collection

Configure SonicWall E-Class SRA for Log File Collection

To configure SonicWall E-Class SRA for FTP collection:

1. Log on to the Aventail Management Console with administrative credentials.
2. Click **Monitoring > Logging**, and select the **Configure Logging** tab.
3. In the **Aventail service log** section, follow these steps:
   a. From the **Web proxy** drop-down list, select **Info**.
   b. From the **Network tunnel** drop-down list, select **Info**.
   c. From the **Management** drop-down list, select **Info**.
   d. Click **Save**.
4. Under the top right menu, click **Pending Changes** > **Apply Changes**.
5. Log off the Aventail Management Console.
6. Log on to the command line interface with administrative credentials.
7. Copy the SFTP Shell Scripts into the **/usr/local/bin** directory.

   Note: RSA only supports the **access_server.log**, **extraweb_access.log**, **policy_audit.log**, and **extranet_access.log** files.
8. Customize the SFTP Shell Scripts for your environment.
9. Configure cron to run the scripts at the desired schedules.
10. Restart the cron process.

Configure the Log Collector for File Collection

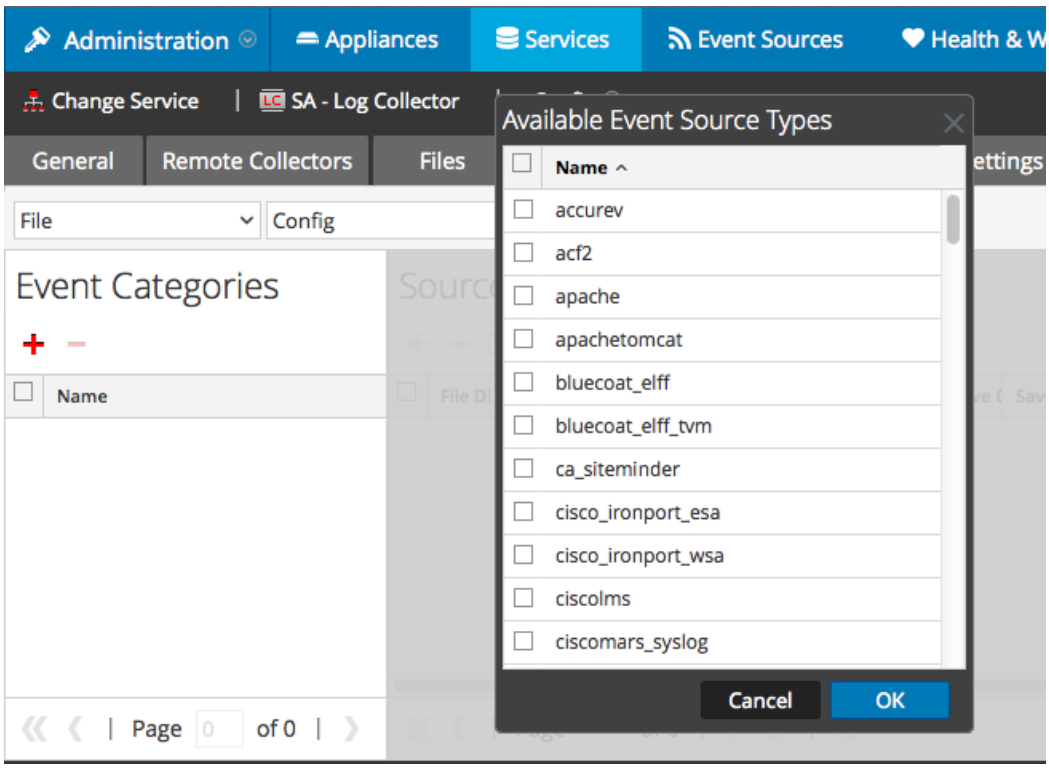
Perform the following steps to configure the Log Collector for File collection.

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.

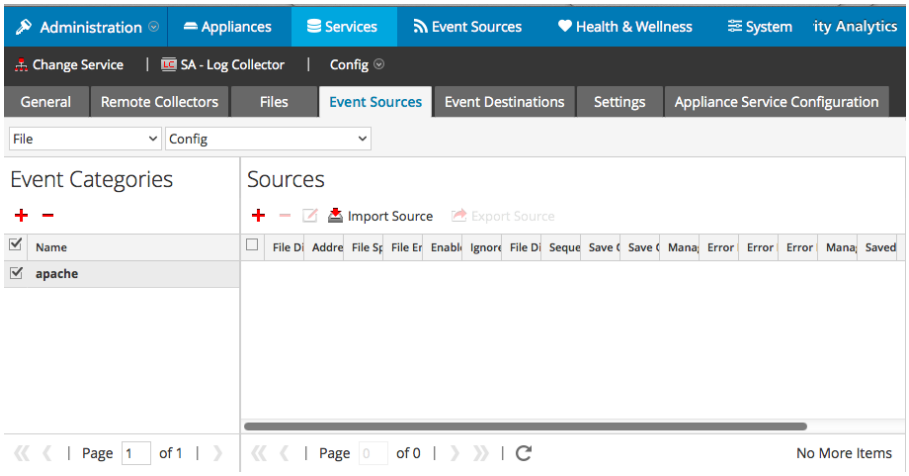


5. Select the correct type from the list, and click **OK**.

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

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

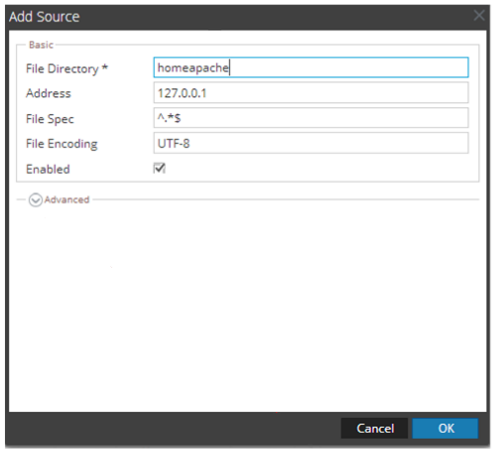
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

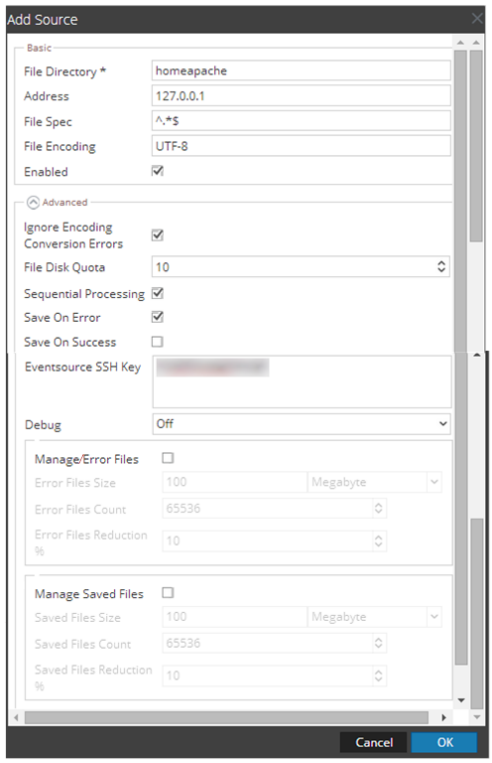


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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.

Collect Syslog

You must perform these tasks to configure SonicWall E-Class SRA for Syslog collection:

I. Configure SonicWall E-Class SRA for log file collection.

II. Configure RSA NetWitness Suite for Syslog Collection

III. Ensure the required parser is enabled on RSA NetWitness Suite

Configure SonicWall E-Class SRA for Syslog Collection

1. Log on to the Aventail Management Console with administrative credentials.
2. Click **Monitoring > Logging** and select the **Configure Logging** tab.
3. In the **Syslog configuration** section, follow these steps to send logs to your RSA NetWitness Suite server:
   a. In the **Server #1** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
   b. In the **Port** field, type **514**.
   c. From the **Protocol** drop-down list, select **UDP**.
   d. Click **Save**.

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is **aventail**.

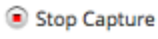
Configure RSA NetWitness Suite for Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **System**.
3. Depending on the icon you see, do one of the following:
   - If you see 

, click the icon to start capturing Syslog.
   - If you see 

, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

   The Event Categories panel displays the Syslog 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 either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced

parameters as necessary.

Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Trademarks