RSA NetWitness Logs

Event Source Log Configuration Guide

Microsoft Windows DNS

Last Modified: Thursday, June 01, 2017

Event Source Product Information:

Vendor: Microsoft
Event Source: Windows DNS
Versions: Windows Server 2008, 2012, 2016
Additional Downloads: sftpagent.conf.windns

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: winevent_snare, winevent_er, winevent_nic
Collection Method: Syslog, File
Event Source Class.Subclass: Host.Windows

Configure Microsoft Windows DNS

To configure collection for Microsoft Windows DNS you can collect the following:

- DNS Server logs (using Adiscon Event Reporter)
- DNS Debug logs, either via File or Syslog collection:
  - File Collection: see Set Up DNS Debug Log Collection using File Collection, or
  - Syslog Collection (using the Epilog Snare Agent): see Set Up DNS Debug Log Collection using Syslog Collection

Set Up DNS Server Log Collection

To collect Windows DNS server logs, perform the following tasks:

I. Configure Windows for DNS Server Log Collection

II. Configure RSA NetWitness Suite for Syslog Collection

Configure Windows DNS Server Log Collection

To set up DNS server logging, configure third-party collection agent Adiscon EventReporter.

Set Up Adiscon EventReporter

To set up Adiscon EventReporter:

1. From the Windows **Start** menu, click **Programs** > **EventReporter** > **EventReporterConfiguration**.
2. In the left-hand panel, double-click **Configured Services**, and follow these steps:
   a. Click **Default EventLog Monitor** > **Advanced Options.**
   b. Select **Use Legacy Format**.
   c. Select only **Add Facilitystring**, **Add Username**, and **Add Logtype**.
   d. Click **Save**.
3. Follow these steps to configure syslog forwarding:
   a. In the left-hand panel, double-click **Rule Sets** > **Default RuleSet** > **Forward Syslog** > **Actions**.

b. Select **Forward Syslog**.

c. In the **Syslog Server** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector collecting the events.

d. Clear **Add Syslog Source when forwarding to other Syslog servers**.

e. Ensure that the **Message Format** is `%msg%`.

f. Leave all other options at the default settings.

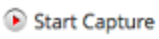
4. Restart the EventReporter service.

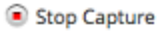
Configure RSA NetWitness Suite for Syslog Collection

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.

Set Up DNS Debug Log Collection using File Collection

To collect Windows DNS server logs, perform the following tasks:

I. Configure Windows DNS Debug Log Collection

II. Set Up the SFTP Agent

III. Configure the Log Collector for File Collection

Configure Windows DNS Debug Log Collection

You must select and enable debug logging options on the DNS server. For details, see Enable DNS Request Logging for Microsoft Windows.

Warning: When you configure the Debug logging, make sure that the **Other Options** field in the **Details** option is **not** selected. RSA NetWitness Suite does not support collection from the Windows DNS event source if that option is enabled.

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.

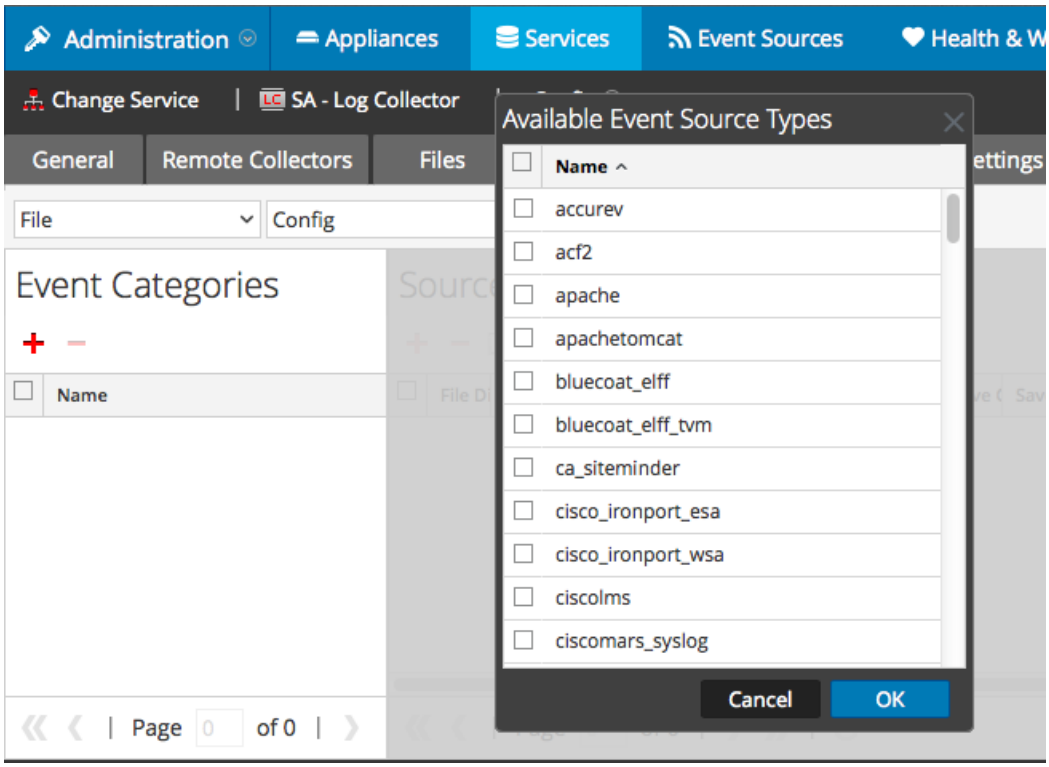
To configure the Log Collector for file collection:

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 +.

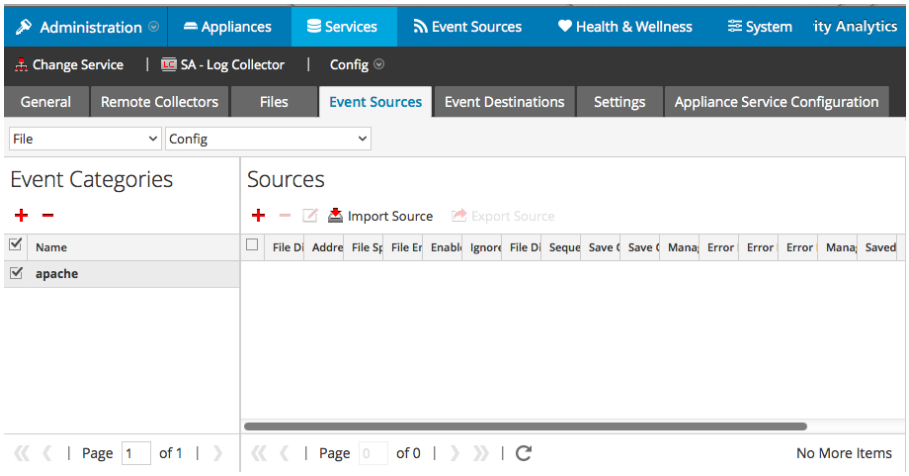
   The Available Event Source Types dialog is displayed.



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

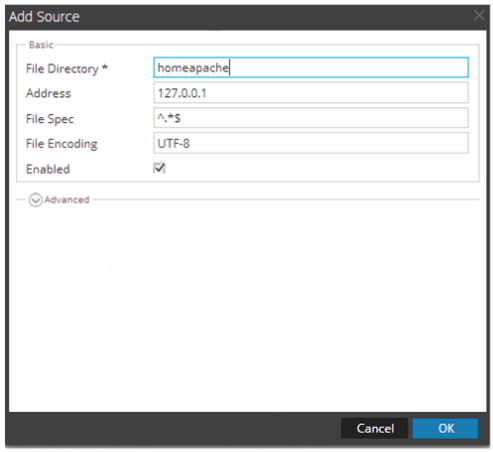
Select **windns** from the **Available Event Source Types** dialog.

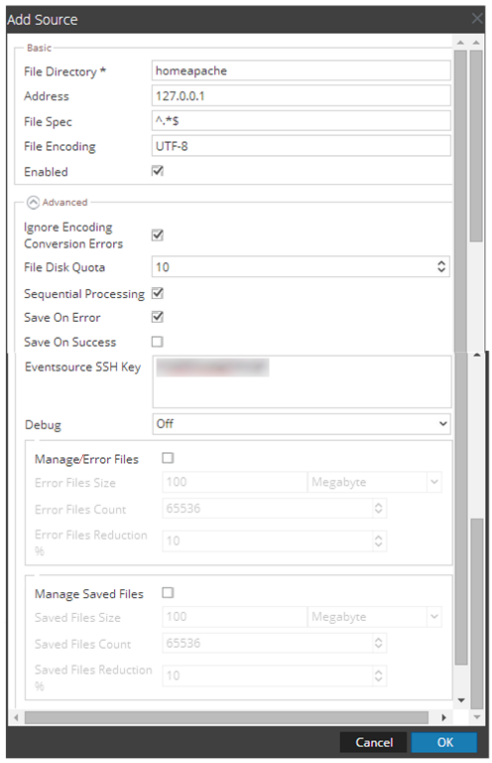
The newly added event source type is displayed in the Event Categories panel.



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.

Set Up DNS Debug Log Collection using Syslog Collection

To collect Windows DNS server logs, perform the following tasks:

I. Configure Windows DNS Debug Log Collection

II. Configure Epilog Agent to Send Syslog

III. Configure RSA NetWitness Suite for Syslog Collection

Configure Epilog Agent to Send Syslog

Use the Snare Epilog web interface to configure the agent to send syslog.

1. Log onto the Snare Epilog web interface.
2. From the left navigation pane, select **Network Configuration**.

   The SNARE Network Configuration screen is displayed.

   a. Set the **Destination Snare Server Address** to the IP address of the RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector collecting the events.

   b. Set the **Destination Port** to 514.

   c. Ensure **Enable SYSLOG Header** is selected.

   d. In the **SYSLOG Facility** drop-down field, select Syslog.

   e. In the **SYSLOG Priority** drop-down field, select Debug.

   f. Click **Change Configuration**.
3. From the left navigation pane, select **Log Configuration**.

   The SNARE Log Configuration screen is displayed.

   a. Click **Add** to add a new log monitor.

   b. In the **Select the Log Type** drop-down field, select **Custom Event Log**, and enter the following:

   ```
   DNSServer,0,
   ```

c. In the **Log File or Directory** field, specify the location that you set the DNS logs to write to. For example, `c:\dns.log`.

d. To save your changes, click **Change Configuration**.

4. **Optional.** You can exclude log files from which you do not want to collect.

   a. From the left navigation pane, select **Objectives Configuration**.

      The SNARE Filtering Objectives Configuration screen is displayed.

   b. If you want to collect from all log files in the specified folder, use the default value (*). Alternatively, you can specify files to exclude, using wildcards.

   c. Click Change Configuration to save your changes, and exclude files that you've specified

5. From the left navigation pane, select **Apply the Latest Configuration**.

6. When the **Apply the Latest Configuration** screen is displayed, click **Reload Settings**.

Trademarks