

# RSA NetWitness Platform

## Event Source Log Configuration Guide



## VMware View

Last Modified: Thursday, June 7, 2018

### Event Source Product Information:

**Vendor:** [VMware](#)

**Event Source:** VMware View

**Versions:** 3.1, 4.0, 4.5, 4.6, 5.0, 5.1, 5.2, 5.3, 6.0, 7.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:** `sftpageant.conf.vmware_view`

### RSA Product Information:

**Supported On:** NetWitness Platform 10.0 and later

**Event Source Type:** `vmware_view`

**Collection Method:** File, ODBC, Syslog

**Event Source Class.Subclass:** `Host.Virtualization`

## Configure VMware View

---

To configure VMware View you must do one of the following:

- [Configure NetWitness Platform for SFTP and File Collection](#)
- [Configure Syslog Collection for VMware View](#)
- [Configure NetWitness Platform for ODBC Collection](#)

## Configure NetWitness Platform for SFTP and 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](#)

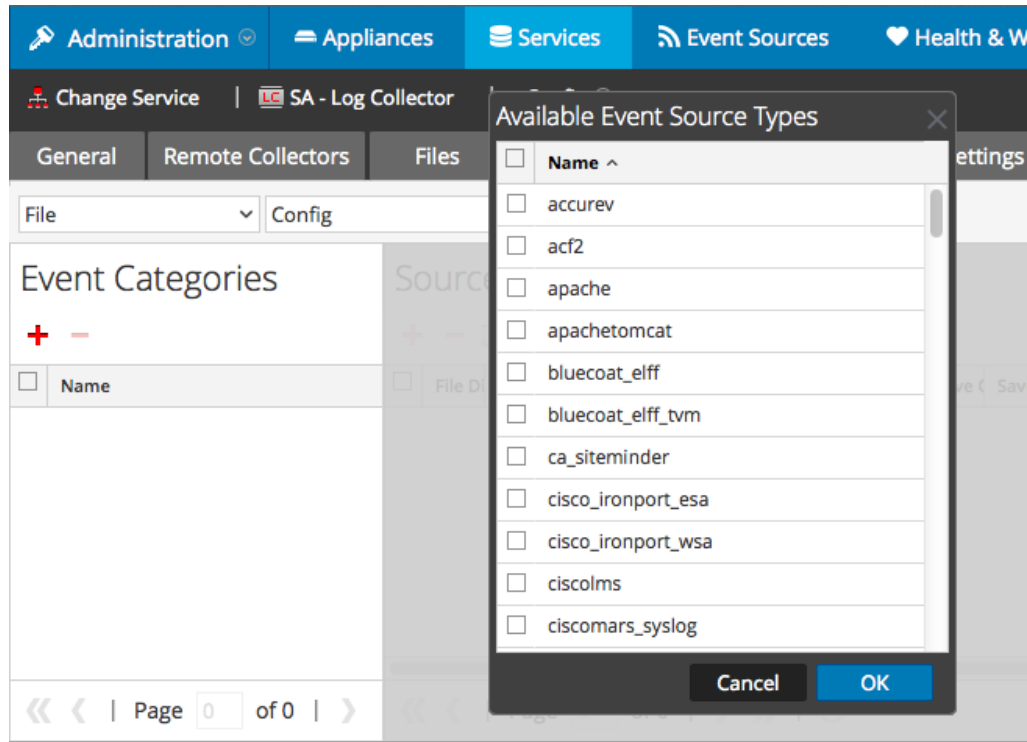
### Configure the Log Collector for File Collection

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 **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.

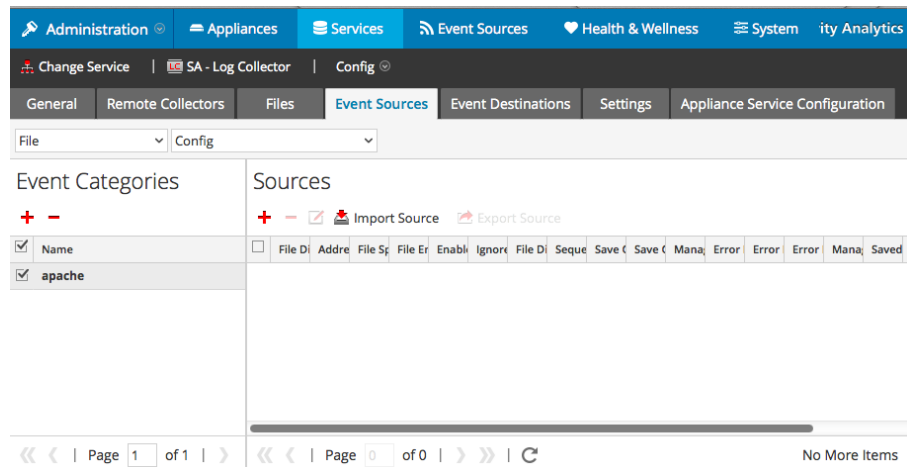


5. Select the correct type from the list, and click **OK**.

Select **vmware\_view** from the **Available Event Source Types** dialog.

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

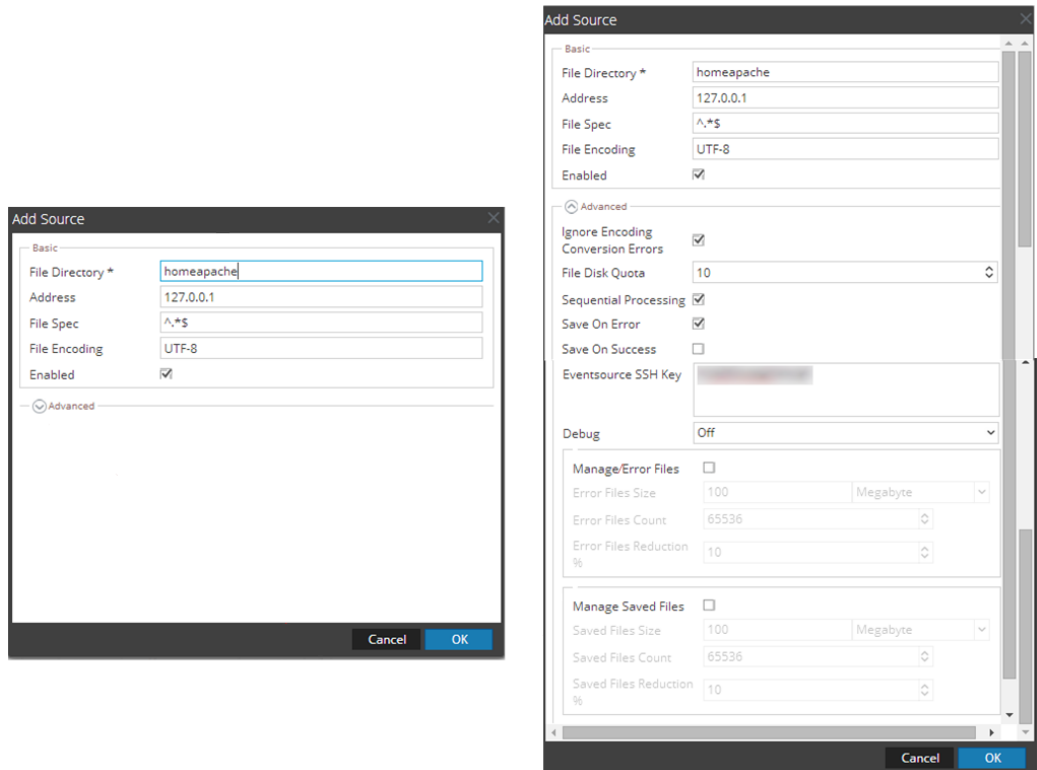
**Note:** The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



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.

## Configure Syslog Collection for VMware View

---

To configure Syslog collection for VMware View you must:



- I. Configure RSA NetWitness Platform for Syslog Collection
- II. Configure Syslog Output on VMware View

### Configure RSA NetWitness Platform 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  **Start Capture**, 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.

### Configure Syslog Output on VMware View

1. Log on to VMware View using web credentials.
2. In the Inventory, click **View Configuration > Event Configuration**.
3. Under the Syslog section next to **Send to Syslog Server**, click **add**.
  - a. Under **Server address**, enter the RSA NetWitness Platform IP address.
  - b. Leave **UDP** as the default setting at **514**.
  - c. Click **OK**.

## Configure VMware View for ODBC Collection

---

To configure VMware vCloud Automation Center for ODBC collection, perform the following tasks in RSA NetWitness Platform:

- I. Ensure the required parser is enabled
- II. Configure a DSN
- III. Add the Event Source Type

### 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 from RSA NetWitness Platform 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 `vmware_view`.

### Configure a DSN

#### Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.
5. The DSNs panel is displayed with the existing DSNs, if any.
6. Click **+** to open the **Add DSN** dialog.

**Note:** If you need to add a DSN template, see the "Configure DSNs" topic in the *Log Collection Configuration Guide*, available in [RSA Link](#).

7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
<b>Parameters section</b>	
Database	Specify the database used by VMware View
PortNumber	Specify the Port Number. The default port number is <b>1433</b>
HostName	Specify the hostname or IP Address of VMware View
Driver	Depending on your NetWitness Log Collector version: <ul style="list-style-type: none"> <li>• For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3sqls27.so</li> <li>• For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3sqls26.so</li> </ul>

## Add the ODBC Event Source Type


In step 6 below, choose the appropriate value from the **Available Event Source Types** dialog:

- If you are using a version of VMware View that is earlier than 5.0, select **vmware\_view**
- If you are using VMware View version 5.0, select **vmware\_view\_v5**
- If you are using VMware View version 5.0 or later, select **vmware\_view\_v51**

### Add the ODBC Event Source Type:

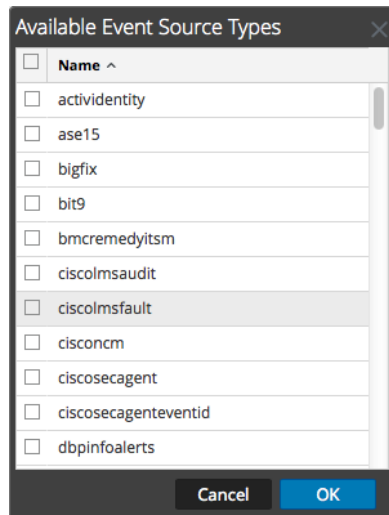
1. In the **NetWitness** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.



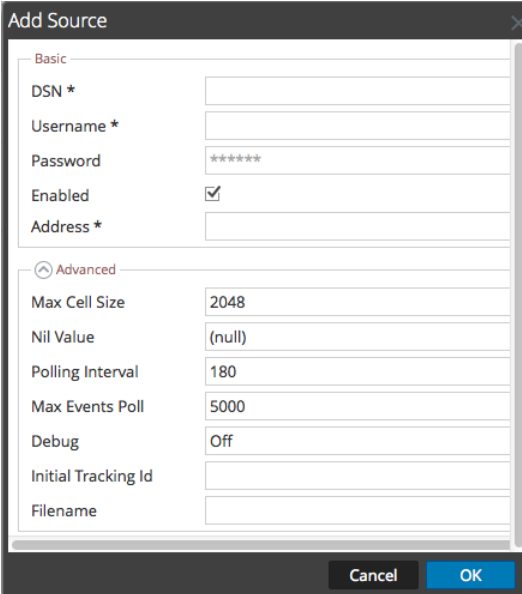
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/Config** from the drop-down menu.

The Event Categories panel is displayed with the existing sources, if any.

5. Click **+** to open the **Available Event Source Types** dialog.



6. Choose the log collector configuration type for your event source type and click **OK**.
7. Fill in the parameters and click **Save**.
8. In the **Event Categories** panel, select the event source type that you just added.
9. In the **Sources** panel, click **+** to open the **Add Source** dialog.



The screenshot shows a dialog box titled "Add Source" with a close button (X) in the top right corner. The dialog is divided into two sections: "Basic" and "Advanced".

**Basic Section:**

- DSN \*: [Empty text box]
- Username \*: [Empty text box]
- Password: [Text box containing "\*\*\*\*\*"]
- Enabled:
- Address \*: [Empty text box]

**Advanced Section:**

- Max Cell Size: [Text box containing "2048"]
- Nil Value: [Text box containing "(null)"]
- Polling Interval: [Text box containing "180"]
- Max Events Poll: [Text box containing "5000"]
- Debug: [Text box containing "Off"]
- Initial Tracking Id: [Empty text box]
- Filename: [Empty text box]

At the bottom of the dialog, there are two buttons: "Cancel" and "OK".

10. Enter the DSN you configured during the **Configure a DSN** procedure.
11. For the other parameters, see [ODBC Event Source Configuration Parameters](#) in the SA User Guide.

Copyright © 2018 Dell Inc. or its subsidiaries. All Rights Reserved.

## Trademarks

For a list of RSA trademarks, go to [www.emc.com/legal/emc-corporation-trademarks.htm#rsa](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).