RSA NetWitness Platform

Event Source Log Configuration Guide

Rapid7 NeXpose

Last Modified: Monday, January 13, 2020

Event Source Product Information:

Vendor: Rapid7
Event Source: NeXpose
Versions: 4.8, 5.2, 5.10, 6.x
Additional Downloads:

- sftpagent.conf.unix.nexpose (configuration file for Linux)
- nicsftpagent.conf.nexpose
- sftpagent.conf.nexpose
- sftpagent.conf.rapid7
- nexpose-audits.vbs
- nexpose-authevents.vbs
- nexpose-nscevents.vbs
- config.cfg

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: nexpose
Collection Method: File
Event Source Class.Subclass: Security.Vulnerability

To configure Rapid7 NeXpose, you must complete these tasks:

I. Configure Scripts on Rapid7 NeXpose

II. Configure SFTP Agent

III. Configure the RSA NetWitness Log Collector for File Collection

Configure Scripts on Rapid7 NeXpose

Note: This entire section is for configuring a Windows system. If you are using Linux, you can skip this section, and go straight to the Configure SFTP Agent section.

On a Windows system, to configure the Rapid7 NeXpose event source to generate logs in the proper area, configure the appropriate script.

1. Use a browser to navigate to the Rapid7 NeXpose Additional Downloads page in the RSA® NetWitness® Platform Event Source Downloads space.
2. Download the scripts you need to your local hard drive.
3. Configure scripts for your version of Rapid7 NeXpose:
   - Configure Scripts for NeXpose 5.2 or later
   - Configure Scripts for NeXpose 4.8

Configure Scripts for NeXpose 5.2 or later

To configure the scripts for NeXpose 5.2 or later:

1. Create a new folder on your NeXpose host named **C:\NeXposeScripts**
2. From the **/nexpose/scripts** folder in your Event Source Update installation directory, copy the **config.cfg**, **nexpose-audits.vbs**, **nexpose-authevents.vbs**, and nexpose-**nscevents.vbs** files, and paste them into **C:\NeXposeScripts**.
3. In the **config.cfg** file, edit the following parameter values.

Parameter	Value
FileName	***InstallPath*\nse.log**
FolderSize	**100**
FileName1	***InstallPath*\auth.log**
FolderSize1	**100**

Parameter	Value
FileName2	***InstallPath*\nsc.log**
FolderSize2	**100**

Where ***InstallPath*** is the location where the NeXpose logs are stored. For example, **C:\Program Files\rapid7\nexpose\nse**.

4. Schedule the **nexpose-audits.vbs** file:

Note: These instructions are for Microsoft Windows 2003; if you are running a different version of Windows, your instructions for scheduling a task will vary slightly.

a. From Windows, click **Start** > **Control Panel** > **Scheduled Tasks** > **Add Scheduled Task**.

b. Click **Next**.

c. Select **Command Prompt**, and click **Next**.

d. In the **Name** field, type **rapid7Batch**.

e. In the **Perform this task** field, select **Daily**, and click **Next**.

f. Add the appropriate start time and the start date for this scheduled task.

g. Click **Next**.

h. Enter your user name and password, and click **Next**.

i. Ensure that **Open advanced properties for this task when I click Finish** is selected, and click **Finish**.

j. Select the **Task** tab.

k. In the **Run** field, type **nexpose-audits.vbs**.

l. In the **Start in** field, type **C:\NeXposeScripts**.

m. Select the **Schedule** tab, click **Advanced**.

n. Select **Repeat task**.

o. Select **1 Minute**, and click **OK**.

p. Click **Apply**, and enter your user name and password.

q. Click **OK**.

Configure scripts for your version of Rapid7 NeXpose:

5. Schedule the **nexpose-authevents.vbs** file. Repeat all instructions from Step 4, except for step 4.j, where you should type **nexpose-authevents.vbs** in the Run field.
6. Schedule the **nexpose-nscevents.vbs** file. Repeat all instructions from Step 4, except for step 4.j, where you should type **nexpose-nscevents.vbs** in the Run field.

Configure Scripts for NeXpose 4.8

To configure the scripts for NeXpose 4.8:

1. Create a new folder on your NeXpose host named **C:\NeXposeScripts**
2. From the **/nexpose/scripts** folder in your Event Source Update installation directory, copy the **config.cfg** and **nexpose-audits.vbs** files, and paste them into **C:\NeXposeScripts**.
3. In the **nexpose-audits.vbs** file, edit the following parameter values.

Parameter	Value
FileName	***InstallPath*\nexpose\nse\nse.log**, where ***InstallPath*** is the location where NeXpose is installed, for example, C:\Program Files\rapid7.
FolderSize	**100**

4. Schedule the **nexpose-audits.vbs** file:
   a. Click **Start** > **Control Panel** > **Scheduled Tasks** > **Add Scheduled Task**.
   b. Click **Next**.
   c. Select **Command Prompt**, and click **Next**.
   d. In the **Name** field, type **rapid7Batch**.
   e. In the **Perform this task** field, select **Daily**, and click **Next**.
   f. Click **Next**.
   g. Enter your user name and password, and click **Next**.
   h. Ensure that **Open advanced properties for this task when I click Finish** is selected, and click **Finish**.
   i. Select the **Task** tab.
   j. In the **Run** field, type **nexpose-audits.vbs**.

k. In the **Start in** field, type **C:\NeXposeScripts**.

l. Select the **Schedule** tab, click **Advanced**.

m. Select **Repeat task**.

n. Select **1 Minute**, and click **OK**.

o. Click **Apply**, and enter your user name and password.

p. Click **OK**.

Configure SFTP Agent

If you are using Windows, see the Install and Update SFTP Agent guide on RSA Link.

To set up SFTP agent on Linux, follow these steps:

Note: Complete details about the script are available from this link in RSA Link: Configure SFTP Shell Script File Transfer.

1. Download the Shell script, **sasftpagent.sh**, from RSA Link (https://community.rsa.com/docs/DOC-45018), and save the file to **/usr/local/sa**.
2. Download the **sftpagent.conf.unix.nexpose** file from RSA Link here: https://community.rsa.com/docs/DOC-47295.
3. Save the file as **sftpagent.conf** in `/etc/rsa`, and change permissions as follows:

   ```
   chmod 777 /etc/rsa/sftpagent.conf
   ```

4. Edit the file, and confirm the configuration parameters are set as follows (for more details and guidelines, see Configure SFTP Shell Script File Transfer):

   ```
   SA=<The name or IP address of your RSA NetWitness Log Collector host>
   DATA_
   DIRECTORY=/opt/rapid7/nexpose/nsc/logs/auth.log:/opt/rapid7/nexpose/nsc/
   logs/nsc.log:/opt/rapid7/nexpose/nsc/logs/nse.log
   FILESPEC=*.log
   DEPTH=1
   SA_DIRECTORY=/upload/nexpose/nexpose
   PERSINFO_DIRECTORY="/var/lib/rsa/$NAME"
   TRANSFER_METHOD=SFTP
   USERNAME=sftp
   IDENTITY=~/.ssh/id_rsa
   UPLOAD_SPEC=tmp
   FLAG_REMOVE_FILE_AFTER_SEND=no
   EXPECTED_SFTP_OUTPUT_LINES=3
   USEHEAD=0
   LOG_FILE="/var/log/rsa/$NAME.log"
   LOCK_TIMEOUT=300
   ```

5. Set up a cron job to run the script periodically.
6. Check **/var/log/rsa/sasftpagent.log** to verify that File collection is working.

Configure the RSA NetWitness Log Collector for File Collection

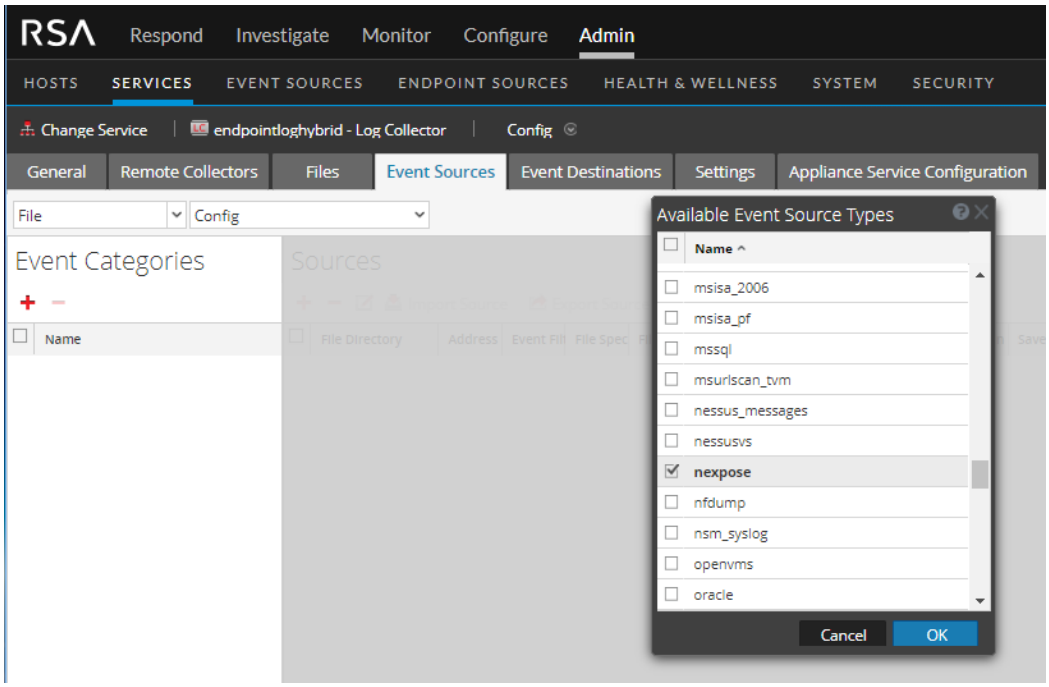
Perform the following steps to configure the Log Collector for File collection.

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 **nexpose** from the **Available Event Source Types** dialog, and click **OK**.

   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**.

   Note: For the **File Directory** parameter, enter **nexpose**. This must match the SA_DIRECTORY parameter that you set in the **sftpagent.conf** file earlier. The final portion of that path must match the directory name you enter here (`/upload/nexpose/`**`nexpose`**).

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.