NetWitness® Platform

Tenable Nessus Event Source Configuration Guide

NETWITNESS
Platform

Tenable Nessus

Last Modified: Wednesday, July 17, 2024

Event Source Product Information:

Vendor: Tenable

Event Source: Tenable Nessus

Versions: 4.0.1, 4.2, 4.4, 5.0, 7.x, 8.x

Note: NetWitness supports the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case in the NetWitness Community Portal for support.

Additional Downloads: sftpagent.conf.nessusvs

RSA Product Information:

Supported On: NetWitness Platform 12.0 and later

Event Source Log Parser: nessusvs

Collection Method: File

Event Source Class.Subclass: Security.Vulnerablility

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

February, 2024

Contents

To collect Nessus scan results, you must complete these tasks:

I. On Nessus, perform the following tasks:
   i. Configure Nessus report collection
   ii. Configure scan with Nessus 4.2, 5.0, 7.x, or 8.x Web Interface, or Nessus 4.0.1 Client

II. OnNetWitness Platform , configure the Log Collector for file collection.

Configure Nessus

On the Nessus event source, configure report collection and scan.

Configure Nessus Report Collection

The server administrator must download the SFTP Agent script from SCOL. The download package contains the script and installation instructions. The script sends the logs to the enVision Collector through SFTP, SCP, or FTP.

Use the instructions appropriate to your OS:

- Configure report collection on Windows
- Configure report collection on UNIX/Linux

Configure report collection on Windows

To configure Nessus report collection on Windows:

1. On the system containing the Nessus client, create a folder to store all Nessus reports.
2. Install the SFTP Agent, and configure it to check for reports in the folder that you created in step 1 using the supplied Nessus sample configuration file. For details, see Install and Update the SFTP Agent.

   Note: The sample file is available as a download for Tenable Nessus in the Tenable Nessus Additional Downloads page in theNetWitness Platform Event Source Downloads space.

Configure report collection on UNIX/Linux

To configure Nessus report collection on UNIX/Linux:

1. Create the **/usr/local/nessus_reports** folder to store Nessus reports.
2. Configure the Shell script:
   a. View the details in the Configure Shell Script File Transfer document.
   b. Copy the **sasftpagent.sh** shell script file (from https://community.netwitness.com/t5/netwitness-platform-downloads/tenable-nessus/ta-p/539488) to the system that creates the Nessus reports. For example, copy the file to `/usr/local/nic/sasftpagent.sh`.
3. In the system's **crontab**, to send the **nicsftpagent.sh** file to the Log Collector, do the following:
   a. From the account that will be sending the file, run the following command:
      `crontab -e`
   b. In the user account's default editor, edit the **crontab** to execute the **sasftpagent.sh** command at a specific interval. For example, the following line is set to execute the **sasftpagent.sh** command one minute after every hour every day. The interval between collections is up to you to define.
      `1 * * * * /usr/local/nic/sasftpagent.sh`
      where **/usr/local/nic** is the full path to the executable script that you already created.

Scan with Nessus, 8.x, 7.x, 5.0 or 4.2 Web Interface, or Nessus 4.0.1 Client

This section describes settings that are required for integration with Prod (NetWitness Platform) on the following clients:

- Configure Nessus 4.2, 5.0, 7.x, or 8.x Using Web Interface
- Configure Nessus 4.0.1 Client

Configure Nessus 4.2, 5.0, 7.x, or 8.x Using Web Interface

Note: For Version 5.0 the default setting is to cipher reports. To change it go to **Configuration** > **Advanced Setting** > **Add Setting**, then **Add** new setting with **Name="cipher_files_on_disk"** and **Value="no"**. This step will add setting "Cipher Files On Disk" and the server will not cipher reports and you can collect reports as you used to do with the previous version

Follow Tenable Nessus documentation for running a scan on your network, with the following requirements for integration with NetWitness Platform:

- Adding Targets: When using the **Single host** or **Hosts in file** to add new targets, specify the targets by IP address, not by hostname.
- Configure Scan options as follows:

1. Click the **Policies** tab.
2. Select your policy configuration and click **Edit**.
3. In the Edit Policy window:
   a. On the **General** tab, ensure **Designate hosts by their DNS name** is not selected.
   b. On the **Plugin Selection** tab, ensure the following plugins are enabled:
      - **General** > **OS Identification** (Nessus plug-in ID 11936)
      - **Service detection** > **Service detection** (Nessus plug-in ID 22964)
4. Click **Submit**.
5. Click the **Reports** tab.
6. Select the report that you want to download, and click **Download**.
7. In the Download Report window, select the download format from the drop-down list.
8. Click **Submit**.

- Downloading Reports: When finished scanning, download reports with the default .nessus extension to the folder selected in Configure Nessus Report Collection.

Configure Nessus 4.0.1 Client

Follow Tenable Nessus documentation for running a proper scan on your network, with the following requirements for integration with enVision:

- Adding Targets: When using **Single host** or **Hosts in file** to add new targets, specify the targets by IP address, not by hostname.
- Configure the scan options as follows:
  - On the **Options** tab, ensure that **Designate hosts by their DNS name** is not selected.
  - On the **Plugin Selection** tab, ensure that the following plug-ins are enabled:
    - **General** > **OS Identification** (Nessus plug-in ID 11936)
    - **Service detection** > **Service detection** (Nessus plug-in ID 22964)
- Saving Reports: When the scan finishes, download reports with the default .nessus extension to the folder that you created in Configure Nessus Report Collection.

Configure NetWitness Platform

On NetWitness Platform, configure the Log Collector for file collection.

Configure the Log Collector for File Collection

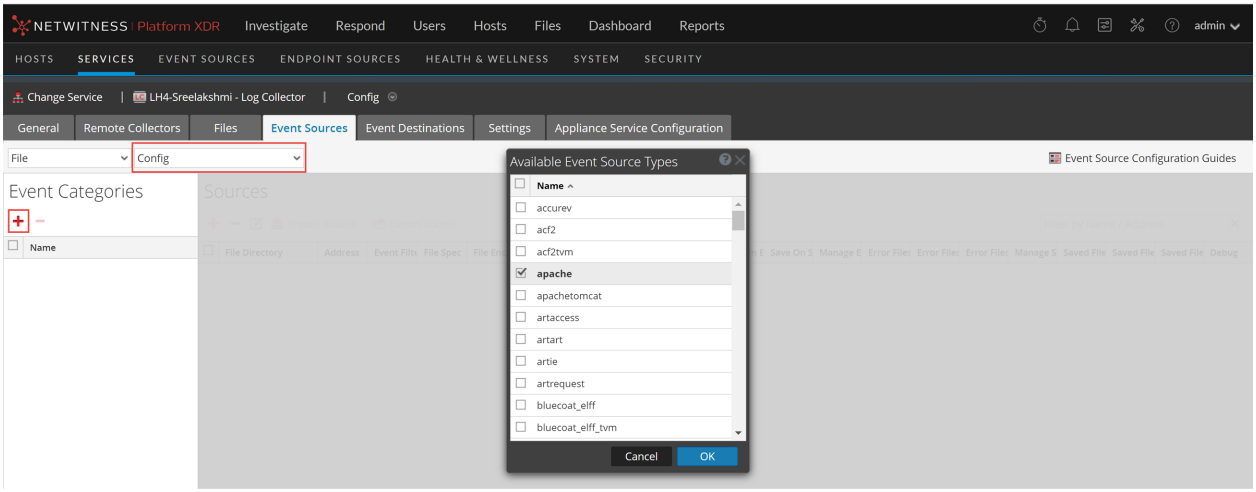
Perform the following steps to configure the Log Collector for File collection.

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.



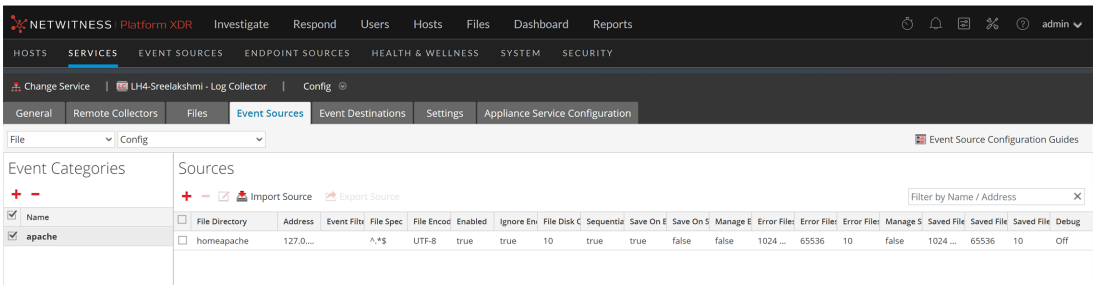
1. Select the correct type from the list and click **OK**.

   Select the following from the **Available Event Source Types** dialog:

   - **nessus_messages** to collect Nessus logs, and
   - **nessusvs** to collect Nessus reports

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

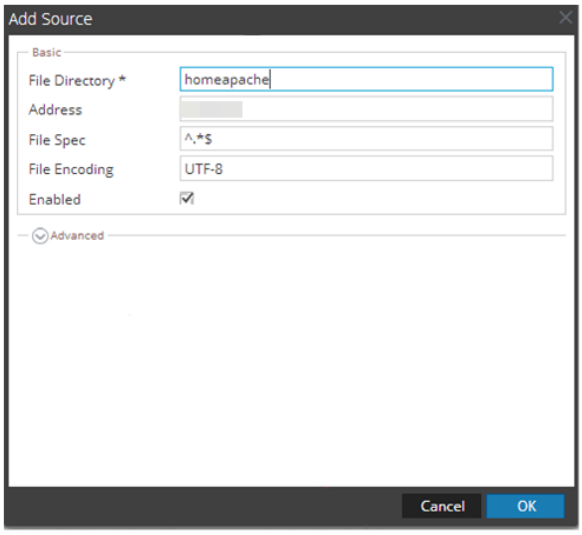
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

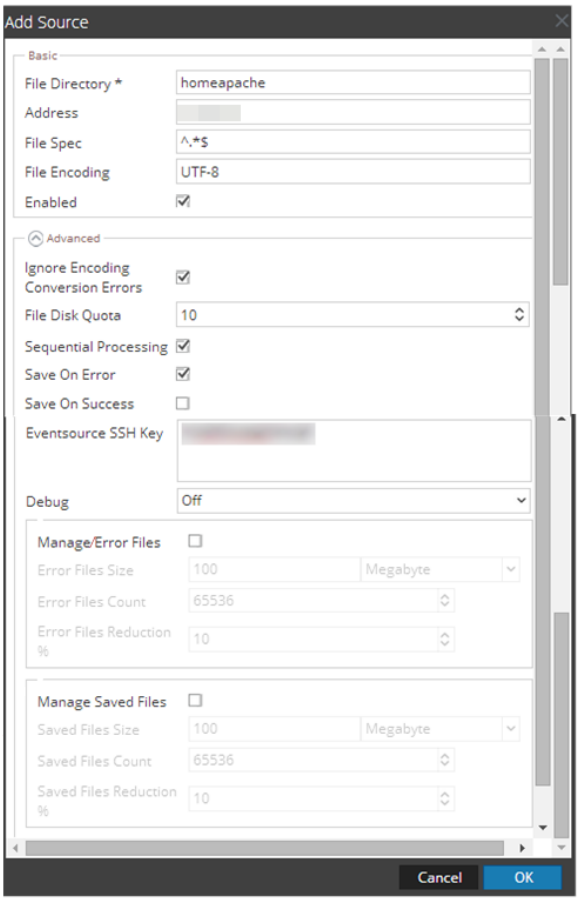


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.