NetWitness® Platform

Microsoft SQL Server Event Source Log Configuration Guide

NETWITNESS
Platform

Microsoft SQL Server

Last Modified: Wednesday, September 11, 2024

Event Source Product Information:

Vendor: Microsoft

Event Source: SQL Server

Versions: 2000, 2005, 2008, 2012, 2014, 2016, 2019, 2022 and MS SQL Express

Additional Downloads:

- sftpagent.conf.mssql

NetWitness Product Information:

Supported On: NetWitness Platform 12.0 and later

Event Source Log Parser: mssql

Collection Method: File and Windows event logs

Event Source Class.Subclass: Storage.Database

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

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

Miscellaneous

August 2024

Contents

Microsoft SQL Collection Overview

NetWitness Platform supports several different collection methods for Microsoft SQL Server, depending on the version of SQL Server and Microsoft Windows that you are using. The following table describes the various combinations of Windows version, MS SQL version, and the collection methods used for each.

MS SQL Version	Platform	Collection Methods
2000	Windows 2000, 2003	Windows Legacy, File
2005, 2008 Standard	Windows 2003, 2008	File (ERRORLOG), Windows Eventing (MS SQL Service Logs)
2008 Enterprise and later	Windows 2008 and later	File (ERRORLOG), Windows Eventing (MS SQL Service Logs and SQL Auditing)

IMPORTANT:
- If you are running SQL Server 2000, NetWitness recommends configuring collection for both the File Service and the Windows Service.
- If you are using SQL Server 2008, then it must be SQL 2008 Enterprise Edition. SQL Server 2008 Standard Edition does not do SQL Auditing.

Windows and Windows Eventing Services

For all supported versions of Microsoft SQL Server, you can collect System and application messages stored in the Windows System and Application log files. Note the following:

- For SQL Server 2005, 2008, 2012, 2014, 2016, 2019 and 2022, you can collect audit level messages.
- For SQL Server 2000 or 2005, running on Windows Server 2003, you set up the Windows Legacy Collector.

File Service

The File Service collects system level messages stored in a local error log file.

Configure Windows Collection

To capture Microsoft SQL Server Auditing messages, you must configure both SQL Server and NetWitness Platform.

To set up SQL Server Auditing on SQL Server:

1. On the SQL Server platform, open **SQL Server Management Studio**.
2. Log onto the server using administrator credentials.
3. Navigate to **Security** > **Audits** and create a new audit.
4. Depending on your system, set the **Audit Destination** to **Application Log** or **Security Log**, and set the values of all other fields with appropriate values for your organization.

   Note: If you want to use security logs, you must set up administrative privileges on the SQL Server. To set up the appropriate privileges, follow the instructions from the Microsoft MSDN page.

5. Click **OK** to create the audit.
6. Based on the audit needs create **Server Audit Specifications** or **Database Audit Specifications** or both, and point them to the audit you created.
7. For **Server Audit specifications** or **Database Audit specifications**, configure the event types for which you want to collect audit events.

Note: The SQL Server Audit feature enables you to audit server-level and database-level groups of events and individual events. For more information, see SQL Server Audit (Database Engine).

8. To enable the audit object created, Select the Audits node in Object Explorer and right click on the audit object created earlier, and then Enable Audit. This will start the audit.

Configure WinRM Collection

If you have not yet configured WinRM collection for your system, and you want to collect login events from MSSQL via the event logs, then you should use the **winrmconfig.ps1** script. This script is available for downloading from this URL: https://community.netwitness.com/t5/community-support-forum/winrmconfig-ps1/m-p/448845. (Note that you need credentials to access this download file.)

IMPORTANT:
- If you are already collecting Application logs via WinRM, you do not need to configure Windows Collection.
- If not, and you wish to collect Application logs, you need to configure collection from the Application event logs to get the MSSQL events, because MSSQL logs to the Application event log.

To configure collection from Application event logs:

1. In the **SQL Server Management Studio**, Connect to the SQL Server in **Object Explorer**.
2. Right-click on the **SQL Server** and choose the **Properties** option from the pop-up menu.

3. Select **Security**, then choose the required option from Login auditing and click OK.

For more details about WinRM collection, see the following:

- Microsoft WinRM Configuration guide here: https://community.netwitness.com/t5/netwitness-platform-integrations/microsoft-winrm-configuration-guide/ta-p/565370
- Test and Troubleshoot Microsoft WinRM guide here: https://community.netwitness.com/t5/netwitness-platform-integrations/test-and-troubleshoot-microsoft-winrm-guide/ta-p/565850

Configure Windows Event Sources in NetWitness

To Configure Windows Event Sources in NetWitness, please refer :

https://community.netwitness.com/t5/netwitness-platform-online/log-collection-configuration-guide-for-12-4-1/ta-p/712877

Configure File Collection

To configure File collection for Microsoft SQL Server, set up the SFTP agent and configure the Log Collector for file collection.

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from NetWitness Link:

- To set up the SFTP agent on Windows, seeInstall 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

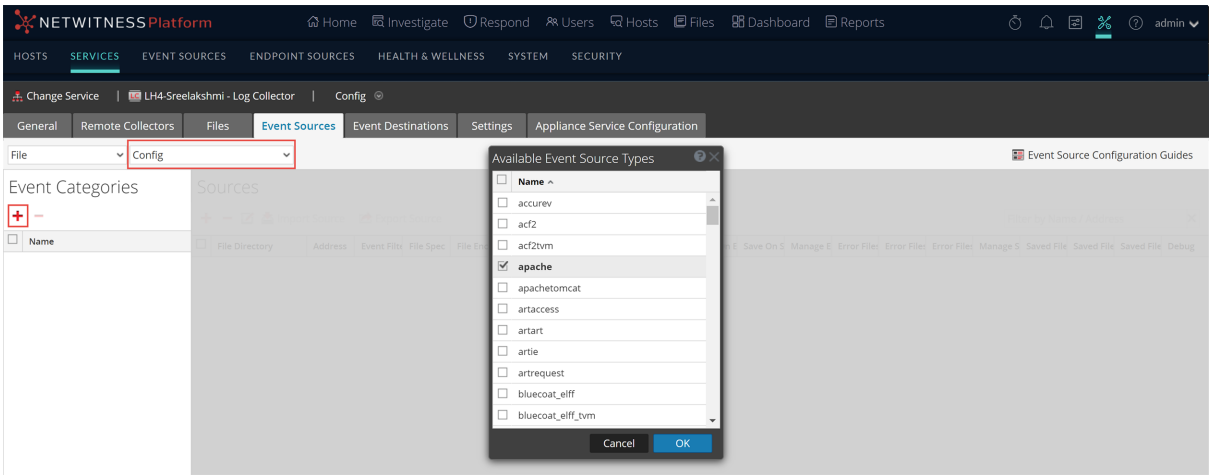
Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select (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.

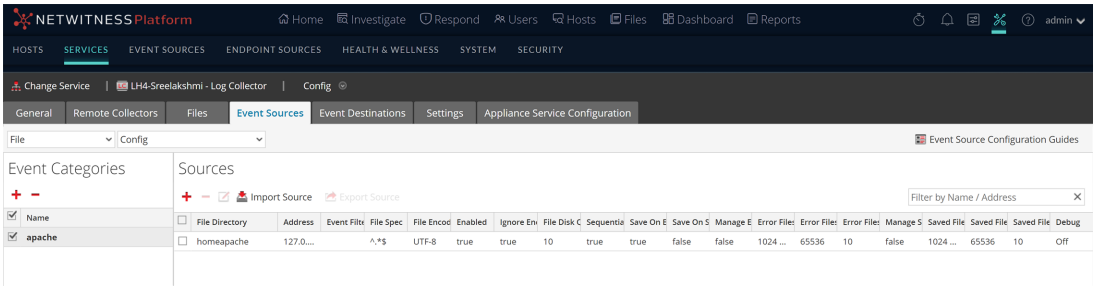


5. Select the correct type from the list and click **OK**.

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

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

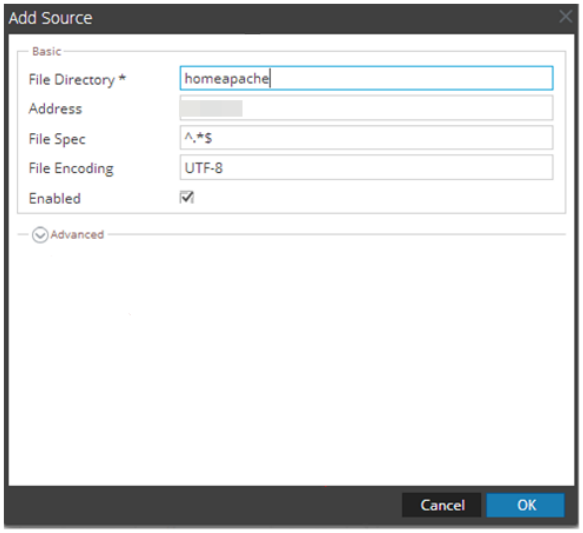
Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

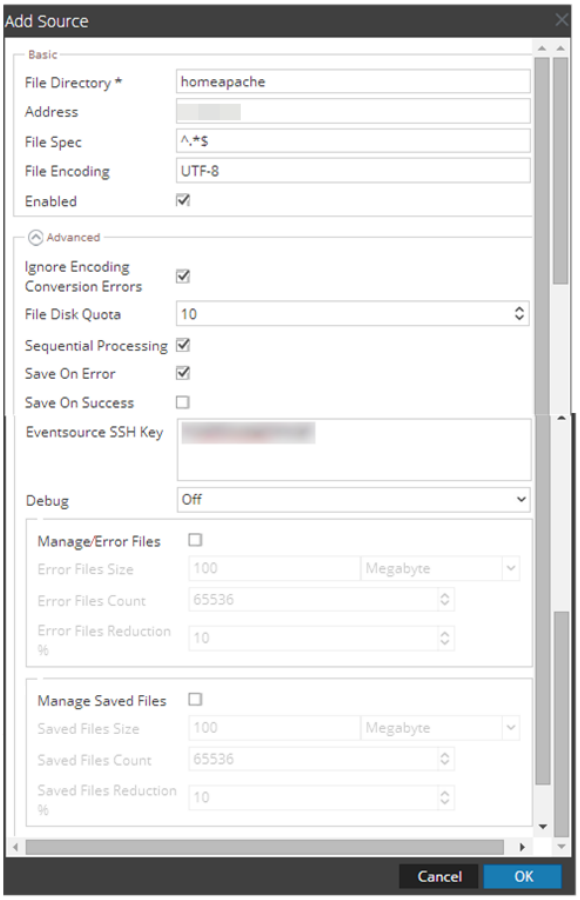


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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.

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.