How To Monitor Windows Event Logs in Nagios XI 2024

Purpose

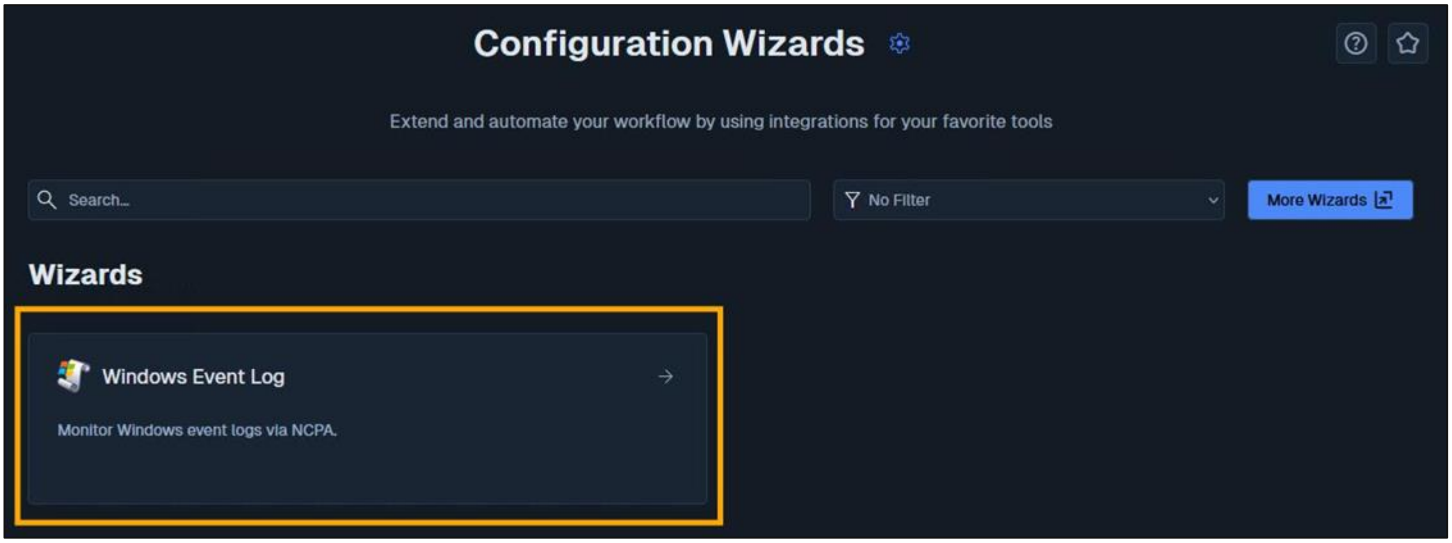
This document describes how to monitor Windows Event Logs in Nagios XI 2024.

Prerequisites

Before you can use the instructions outlined in this document, you must first install NCPA on the target Windows machine you wish to monitor. Instructions for installing NCPA can be found in the Installing NCPA documentation.

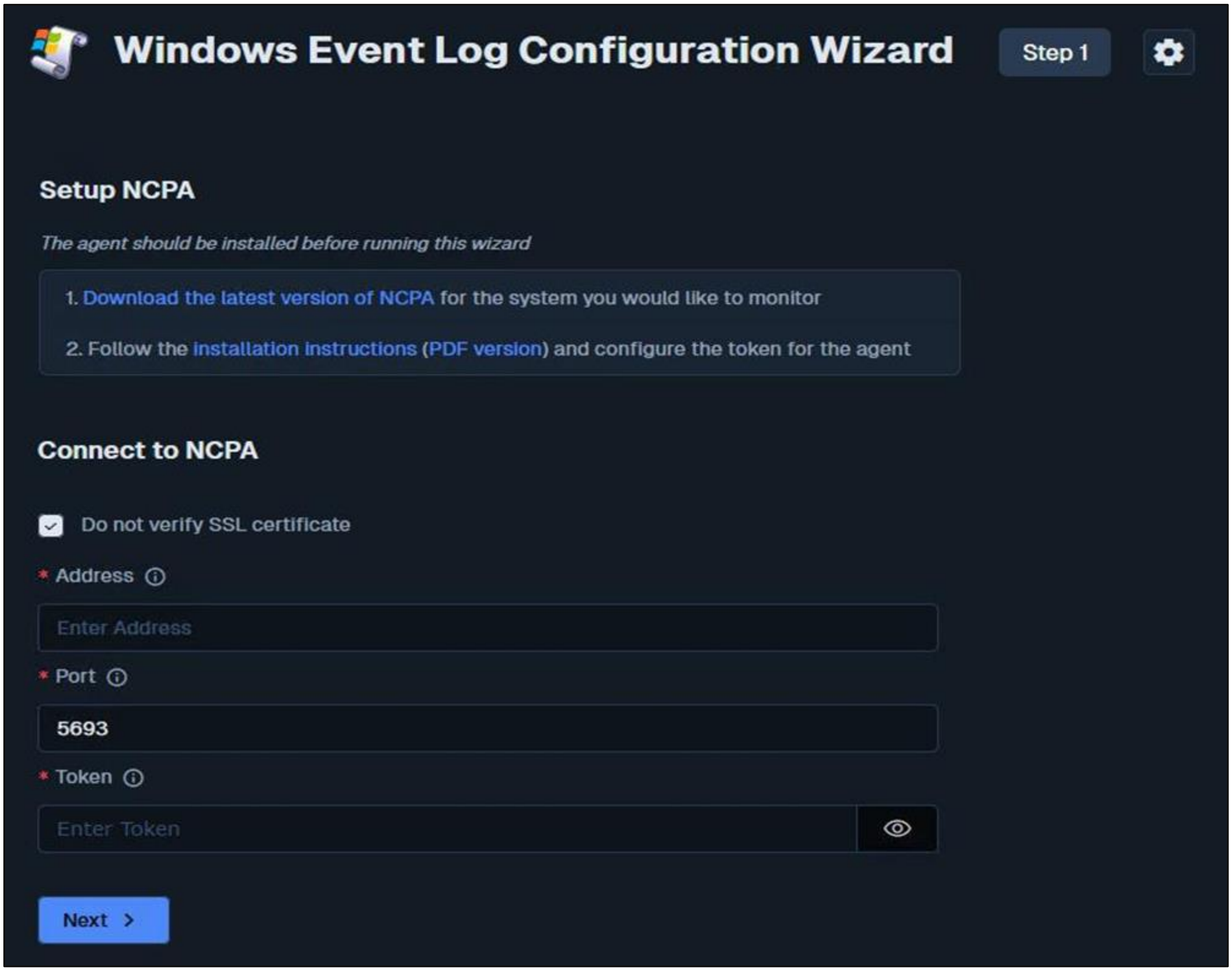
Using The Windows Event Log Monitoring Wizard

To begin using the Windows Event Log wizard navigate via the top menu bar to **Configure > Configuration Wizards** and select the **Windows Event Log** wizard. In the following screenshot you can see how the search field allows you to quickly find a wizard.


Configuration Wizards
Extend and automate your workflow by using integrations for your favorite tools
Search...
No Filter
More Wizards
Wizards
Windows Event Log
Monitor Windows event logs via NCPA.

Step 1

- Type the **IP address** or **FQDNS** name of the host you want to monitor.
- You can specify the port number if you have changed it from the default of **5693**.
- Type the **Token** you are using on the NCPA agent.
- Click **Next**.



Windows Event Log Configuration Wizard

Setup NCPA

The agent should be installed before running this wizard

1. Download the latest version of NCPA for the system you would like to monitor
2. Follow the installation instructions (PDF version) and configure the token for the agent

Connect to NCPA

☑ Do not verify SSL certificate

* Address

Enter Address

* Port

5693

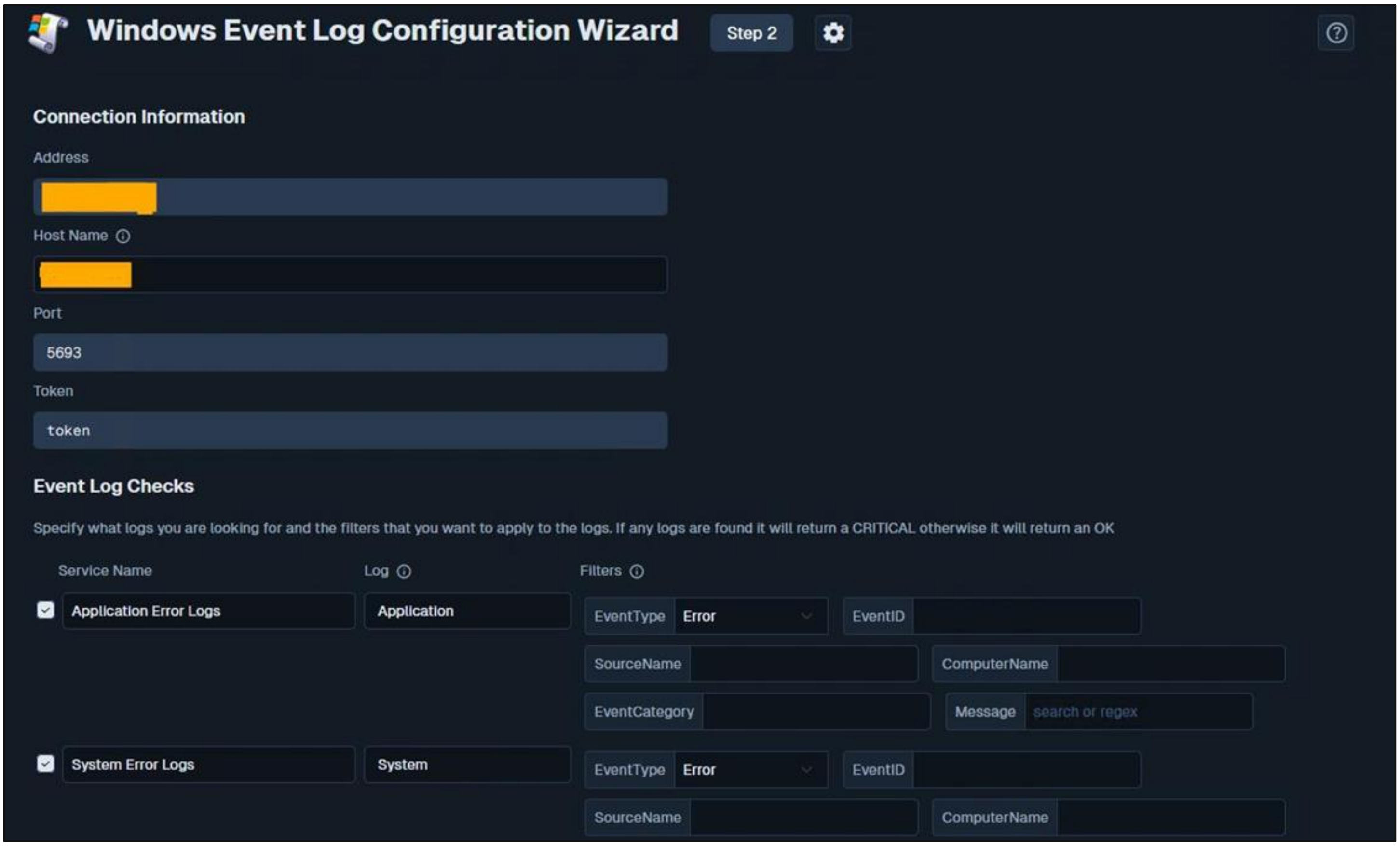
* Token

Enter Token

Step 2

On this step you will configure all the options for monitoring. In the screenshot you can see some of the options available.

- Enter a valid **Host Name**.
- Select the event logs that you would like to monitor and add any necessary filtering.
- You can add event logs that are not listed by clicking the **Add Another Check** link.
- Click **Next** once you have selected all the required options.



Connection Information

Address: [redacted]

Host Name ⓘ: [redacted]

Port: 5693

Token: token

Event Log Checks

Specify what logs you are looking for and the filters that you want to apply to the logs. If any logs are found it will return a CRITICAL otherwise it will return an OK

	Service Name	Log ⓘ	Filters ⓘ
☑	Application Error Logs	Application	EventType: Error EventID: SourceName: ComputerName: EventCategory: Message: search or regex
☑	System Error Logs	System	EventType: Error EventID: SourceName: ComputerName:

Complete the wizard by choosing the required options in **Step 3 – Step 5.**

To finish, click on **Finish** in the last step of the wizard. This will create new host and services and begin monitoring.

Once the wizard applies the configuration, click the **View status details for** link to see the new service that was created.

For more information, visit the Configuration Wizards documentation page.

Finishing Up

This completes the documentation on how to monitor Windows Event Logs in Nagios XI 2024. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum

Visit Nagios Knowledge Base

Visit Nagios Library