

Configuring NXLog to Send Additional Log Files in Nagios Log Server 2024

Requirements

It is assumed you have already installed NXLog on your Windows server and configured it to send logs to Nagios Log Server. This is covered in the following article:

[Monitoring A New Log Source](#)

Considerations

It's very easy to setup NXLog to monitor your own custom logs. When you configure NXLog, by default you will only be collecting new data that comes in from that point forward. If you wanted to import the contents of the existing log file there are a couple of extra steps required. This article will walk you through those steps.

This guide is going to focus on the file C:\Important Application\Logs\log.txt as an example.

Please make sure you read the entire guide, otherwise duplicate data may be imported to your Nagios Log Server.

Configure NXLog

1. Login to your Windows server and open the file C:\Program Files (x86)\nxlog\conf\nxlog.conf in Notepad.
2. Add the following to the end of the file:

```
<Input important_application>
```

```
Module      im_file
```

```
File        'C:\Important Application\Logs\log.txt'
```

```
SavePos     FALSE
```

```
ReadFromLast FALSE
```

```
Exec        $Message = $raw_event;
```

```
</Input>
```

3. In the same file, find the following section:

```
<Route 1>
```

```
Path internal, file1, eventlog => out
```

```
</Route>
```

4. Change the path line so we now reference the new input important_application

```
<Route 1>
```

```
Path internal, file1, eventlog, important_application => out
```

</Route>

5. Save the changes you just made, the next step will be to restart NXLog.
6. Open services.msc and restart the nxlog service.
7. If you have additional files that need to be imported to Nagios Log Server, repeat the steps above to add another Input and add that to the Route.

2019-02-13T14:35:12.487+11:00 10.25.14.5 eventlog This is a test 1

Q ▾

2019-02-13T14:35:12.487+11:00 10.25.14.5 eventlog This is a test 2

Q ▾

View: **Table** / JSON / Raw

⬆

Field	Action	Value	Search
<input checked="" type="checkbox"/> @timestamp	Q 🔍	2019-02-13T03:35:12.487Z	<div>Q ▾</div>
<input type="checkbox"/> @version	Q 🔍	1	<div>Q ▾</div>
<input type="checkbox"/> EventReceivedTime	Q 🔍	2019-02-13 14:35:12	<div>Q ▾</div>
<input type="checkbox"/> SourceModuleName	Q 🔍	important_application	<div>Q ▾</div>
<input type="checkbox"/> SourceModuleType	Q 🔍	im_file	<div>Q ▾</div>
<input type="checkbox"/> _id	Q 🔍	AWjk7DnG6OP9uaJfV0Tu	<div>Q ▾</div>
<input type="checkbox"/> _index	Q 🔍	logstash-2019.02.13	<div>Q ▾</div>
<input type="checkbox"/> _type	Q 🔍	eventlog	<div>Q ▾</div>
<input checked="" type="checkbox"/> host	Q 🔍	10.25.14.5	<div>Q ▾</div>
<input checked="" type="checkbox"/> message	Q 🔍	This is a test 2	<div>Q ▾</div>
<input type="checkbox"/> port	Q 🔍	49221	<div>Q ▾</div>
<input checked="" type="checkbox"/> type	Q 🔍	eventlog	<div>Q ▾</div>

To explain the changes made above, the name `important_application` is what Nagios Log Server will identify as the `SourceModuleName` field when it is received.

You can see in the screenshot from Nagios Log Server, it shows the field SourceModuleName with the value of important_application.

The following settings need to be highlighted:

SavePos FALSE

ReadFromLast FALSE

These two options will force NXLog to send the entire contents of the existing log file to Nagios Log Server. Without these options, nothing will be sent to Nagios Log Server until new content is added to the file. It can be useful to import the existing log data as it will help confirm that NXLog is successfully sending the logs to Nagios Log Server.

Check Log Server

After restarting NXLog, it won't take long for the data to be received by your Nagios Log Server:

- Login to Nagios Log Server
- Open the Default dashboard
- Perform a search for a word that exists in the C:\Important Application\Logs\log.txt file

Once you see it appear in the dashboard search results, the log is being successfully imported. The screenshot on the previous page shows just that.

Update NXLog Config

Now we need to re-configure NXLog so that it doesn't re-read the entire file the next time the service is started. If this happened, you would end up with all the same entries being sent to Nagios Log Server each time the service is stated.

Open the file C:\Program Files (x86)\nxlog\conf\nxlog.conf in Notepad and find the section you added before:

```
<Input important_application>
```

```
Module      im_file
```

```
File        'C:\Important Application\Logs\log.txt'
```

```
SavePos     FALSE
```

```
ReadFromLast FALSE
```

```
Exec        $Message = $raw_event;
```

```
</Input>
```

And change it to:

```
<Input important_application>
```

```
Module      im_file
```

```
File        'C:\Important Application\Logs\log.txt'
```

```
SavePos     TRUE
```

```
Exec      $Message = $raw_event;
```

```
</Input>
```

The change you just made was:

Changed SavePos to TRUE

Removed the line ReadFromLast FALSE

Save the changes you just made and restart the NXLog service like you did earlier. After the service restarts, only new lines that are added to the C:\Important Application\Logs\log.txt file will be sent to Nagios Log server.

For more information on configuring Nagios Log Server with Windows, see the [NXLog User Guide](#).