Configuring NXLog To Send Additional Log Files

Purpose

This document shows how you can extend the log collecting capabilities of NXLog on a Windows server by monitoring your own custom logs.

Target Audience

This document is intended for use by Nagios Administrators that need to configure their Windows machines to sent specific log files to Nagios Log Server.

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

Login to your Windows server and open the file `C:\Program Files (x86)\nxlog\conf\`**`nxlog.conf`** in Notepad.

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>
```

In the same file, find the following section:

```
<Route 1>
Path internal, file1, eventlog => out
</Route>
```

Change the path line so we now reference the new input **`important_application`**

```
<Route 1>
Path internal, file1, eventlog, important_application => out
</Route>
```

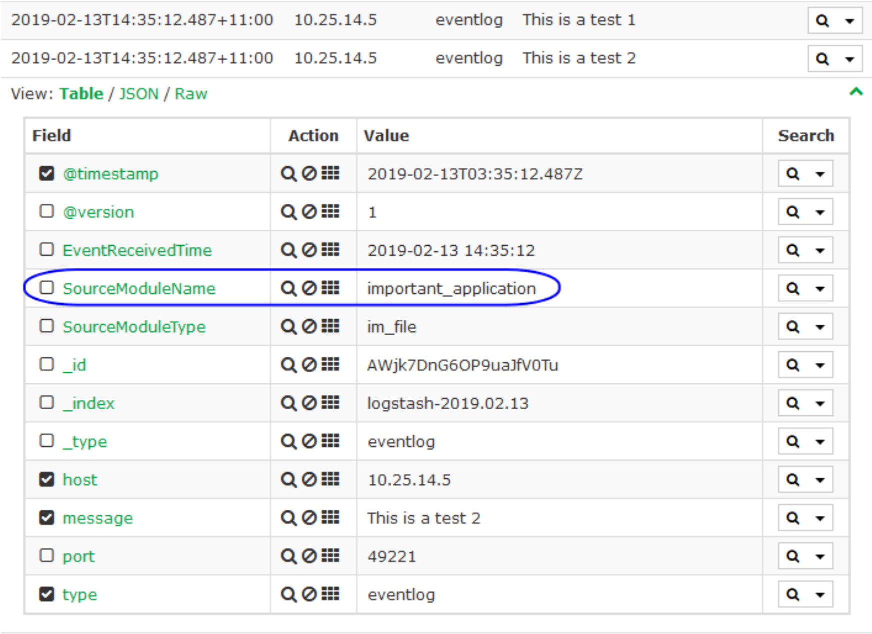
Save the changes you just made, the next step will be to restart NXLog.

Open **`services.msc`** and **restart** the **nxlog** service.

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**.

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 to the right from Nagios Log Server, it shows the field **SourceModuleName** with the value of `important_application`.



2019-02-13T14:35:12.487+11:00	10.25.14.5	eventlog	This is a test 1
2019-02-13T14:35:12.487+11:00	10.25.14.5	eventlog	This is a test 2

View: Table / JSON / Raw

Field	Action	Value	Search
☑ @timestamp		2019-02-13T03:35:12.487Z	
□ @version		1	
□ EventReceivedTime		2019-02-13 14:35:12	
□ SourceModuleName		important_application	
□ SourceModuleType		im_file	
□ _id		AWjk7DnG6OP9uaJfV0Tu	
□ _index		logstash-2019.02.13	
□ _type		eventlog	
☑ host		10.25.14.5	
☑ message		This is a test 2	
□ port		49221	
☑ type		eventlog	

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.

From now on, only new lines that are added to the C:\Important Application\Logs\log.txt file will be sent to Nagios Log server.

Finishing Up

This completes the documentation on configuring NXLog to send additional log files to Nagios Log Server. If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

https://support.nagios.com/kb