Log Checks

Article Number: 787 | Rating: Unrated | Last Updated: Tue, Nov 28, 2017 at 4:44 PM

Log Checks

Log checks allow you to query log files or Windows Event logs.

Checking log files can be a system intensive process, especially if you have a large log file that is being checked every five minutes. A better solution is to send the log file data to a c
Nagios Log Server is the perfect solution for this and is strongly recommended over trying to check log files via a plugin or agent.

The sections below provide examples of how to perform log file checks using different methods.

Nagios Plugins

Nagios Plugins includes the `check_log` plugin. The plugin scans a log file and reports and matches to the query provided. Successive calls to the plugin will only report new pattern matche
the previous run is saved to old_log_file.

Commands:

```
./check_log -F /var/log/messages -O /var/log/messages_old -q 'Error'
```

Output:

```
(2) < Nov 27 16:09:45 xitest ndo2db: Error: Connection to MySQL database has been lost!
```

NCPA

NPCA includes a logs module that currently only works for Windows Event logs. It does not provide any Linux support OR log files that are not part of the Event log system.

Here is an example query that:

- Looks at the **System** log
- Severity has to be **warning**, **error** or **critical**
- Event is logged in the last **1 hour**

Command:

```
./check_ncpa.py -H 10.25.14.91 -t Str0ngT0k3n -M logs -q name=system,severity=warning,severity=error,severity=critical,logged_after=
```

Output:

```
OK: system has 0 logs, Total Count has 0 logs (Time range - last 1 hour) | 'system'=0;;; 'Total Count'=0;;;
```

The logs module has a lot of arguments available, this allows you to create more granular queries to meet your needs.

NSClient++ via check_nt

NSClient++ via check_nt does not include a log module.

NSClient++ via check_nrpe

NSClient++ includes two log checking methods.

Windows Event Logs

The check_eventlog module is specifically for the Windows Event Logs.

Here is an example query that:

- Looks at the **System** log
- Severity has to be **warning**, **error** or **critical**
- Event is logged in the last **1 hour**

Command:

```
./check_nrpe -H 10.25.11.3 -c check_eventlog -a log=system scan-range=-1h
```

Output:

```
OK: No entries found|'problem_count'=0;0;0
```

The check_eventlog module has a lot of arguments available, this allows you to create more granular queries to meet your needs.

Willem D'Haese has a great guide titled "Real-time Eventlog Monitoring with NSClient", please refer to his article for information on Windows Event Log monitoring.

https://outsideit.net/real-time-eventlog-monitoring/

Log Files

The check_logfile module allows you to check file(s) on the system's disk.

The check_logfile module requires the module to be enabled in the `nsclient.ini` file, execute the following command in an Administrative command prompt:

```
cd "\Program Files\NSClient++\"
nscp settings --activate-module CheckLogFile --add-defaults
nscp service --restart
```

This examples shows how you can search a log file for the word **`Failed`** in each **`line`**. If more than 0 matches are found then it is in a critical state.

Command:

```
./check_nrpe -H 10.25.11.3 -c check_logfile -a file="C:\\Logs\\server.log" filter="line like 'Failed'" top-syntax='${status}: ${coun
```

Output:

```
CRITICAL: 8/17 matches|'count'=8;0;0
```

WMI

Check WMI Plus includes a checkeventlog module. Here is an example check that:

- Looks at the **System** log
- Severity has to be **warning** (2) or **error** (1)
- Event is logged in the last **1 hour**

Command:

```
./check_wmi_plus.pl -H 10.25.14.3 -u wmiagent -p Str0ngP@ssw0rd -m checkeventlog -a System -o 1,2 -3 1 -c 1
```

Output:

```
OK - 0 event(s) of Severity Level: "Error,Warning", were recorded in the last 1 hours from the System Event Log.|'Event Count'=0;1;
```

SNMP

You will need to download a third party plugin that provides this functionality, please check out the Nagios Exchange.

Final Thoughts

For any support related questions please visit the Nagios Support Forums at:

http://support.nagios.com/forum/

Posted by: **tlea** - Tue, Nov 28, 2017 at 4:44 PM. This article has been viewed 8605 times.

Online URL: https://support.nagios.com/kb/article/log-checks-787.html