NiCE Log File Management Pack

for

System Center Operations Manager 2012

Version 1.33
April 2016

Quick Start Guide

Legal Notices

NiCE IT Management Solutions GmbH makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. NiCE shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Restricted Rights Legend

Copyright Notices

Trademark Notices

Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

The version number on the title page of this document indicates software version. The print date on the title page changes each time this document is updated.

You will receive updated or new editions if you subscribe to the appropriate product support service.

Contents

Introduction

The NiCE Log File Management Pack is an extension for Microsoft® System Center Operations Manager 2012 and 2012 R2. The NiCE Log File MP enables you to create rules and monitors via the user interface (UI) so that you can monitor log files with the NiCE Log File Provider.

The information provided in this guide shows you how to install the software and make one or two recommended adjustments for your monitoring landscape.

You can use the Quick Start Guide to help you perform basic troubleshooting activities, for example, to enable or disable logging and tracing, and maintain the log and trace files.

Last but not least, the Quick Start Guide shows you how to remove the NiCE Log File management pack quickly and cleanly.

Before you start the installation process, read the important information concerning prerequisites, supported platforms, and limitations included in *Before you Start*.

Before you Start

This guide explains how to install and setup the NiCE Log File MP. Before you start the installation and configuration process, have a look at the information in this section, which covers the following areas:

- Supported Environments
- Limitations

Supported Environments

The NiCE Log File MP supports the following platforms and applications:

- System Center Operations Manager 2012, 2012 SP1, 2012 R2 have been verified and approved for production use.

Limitations

The NiCE Log File MP has the following known limitations:

- Only supported on Microsoft Windows Servers.
- Monitoring the same log file via different management groups might not work correctly (multi-homing)

Prerequisites

If you want to install and run the NiCE Log File MP, note the following prerequisites:

- .NET 2.0 SP1 must already be installed on all systems that are monitored
- System Center Operations Manager authoring experience required
- Experience in regular expressions and XPath (recommended)
- The latest update for SCOM 2012 is installed (recommended)

Installing the NiCE Log File MP

To complete the installation process for the NiCE Log File MP, you must perform the following steps:

1. Install the Log File MP Setup Package
2. Import the Management Pack

Install the Log File MP Setup Package

You perform this installation step on the Ops Mgr Management Server system or any other Windows server or computer.

It is recommended to install the setup MSI on a Management Server to have the setup package in a central location. It is also recommended to use the `%programfiles%` directory to install the NiCE Log File MP.

1. Copy the Microsoft installation package for the Log File MP (`NiCE_LogFileMP_0133.msi)` to a temporary location on the OpsMgr Server.
2. Double-click the file `NiCE_LogFileMP_0133.msi` to start the installation process.
3. Follow the instructions displayed in the setup screens and dialogs.

The Setup MSI package `NiCE_LogFileMP_0133.msi` serves as a container and only has the management pack bundle file.

Import the Management Pack Bundle

You perform this installation step on the OM Administration Console.

1. Log on to the Administration Console and import the following management-pack files:

   - **`NiCE.LogFile.Library.mpb`**

   By default, the management-pack files are located in the folder `%ProgramFiles(x86)%\NiCE\LogfileMP\MPs` on the system where the setup package was installed,

Using the NiCE Log File MP

All wizards to create a log file rule/monitor can be accessed from the System Center Console under Authoring.

Some of the wizards use Regular Expressions (Regex) or XPath. Details about them can be found in the sections “Regular Expression (Regex)” and “XPath”.

Monitor/Rules Log File Wizards

The Log File MP supports different types of wizards for monitoring the log files.

Correlated log entries	Correlation based monitors and rules correlates 2 or more items to detect a specific counting and/or order. This type is used to create an alarm when a log must have 2 specific entries within a specific time window. More details are available under: https://technet.microsoft.com/en-us/library/hh457604.aspx
Correlated missing log entries	Missing correlation is mostly used to create an alert when in a time window one log entry appears, but the second specific entry is missing. It is the opposite of the above type of rule/monitor. More details are available under: https://technet.microsoft.com/en-us/library/hh457587.aspx
Missing log entries	Missing log entries is designed to create an alarm if a specific log entry doesn’t appear in a specific time window. This could be used for checking if a log was updated in the last x minutes or if a regular log entry like health checks doesn’t appear in time. More details are available under: https://technet.microsoft.com/en-us/library/hh457594.aspx
Repeated log entries	Repeated log entries is mostly used to create an alert if a log entry appears specific number of times in a specific time window. More details are available under: https://technet.microsoft.com/en-us/library/hh457566.aspx

Event/Manual/Timer Reset	Monitors must also support to reset its state back to healthy. This can be done by either Log Entry or Manually or by using a Timer. More details are available under: https://technet.microsoft.com/en-us/library/hh457598.aspx
Expression Filtered	Expression Filtered monitors and rules compares the incoming data using XPATH with a static text, regex, value … This is used to filter log entries which match the specified requirement. More details are available under: https://technet.microsoft.com/en-us/library/hh457585.aspx https://msdn.microsoft.com/en-us/library/jj129836.aspx

Available Whitepapers

It is recommend to download and read the Whitepapers for user friendly experience.

At the time of this document the following use cases are available:

Whitepaper	File Name	Use case
Monitor missing log entries	NiCE_LogFileMP_Whitepaper_2016Q1.pdf	This use case shows how to monitor a log for an entry which is missing in specific time window.
Create Performance Views from log files	NiCE_Whitepaper_UseCaseLog_FileMP_PerfView_2016Q2.pdf	This use case show how to create a performance rule which monitors the log for numeric values and map them to a performance counter. Further it explains how to create a performance view to show the collected data in Console.
Correlated Event Monitor	NiCE_Whitepaper_UseCaseLog_FileMP_CorrelatedLogEntry_2016Q2.pdf	This use case show how to monitor two log entries and correlate them within a specified time window.

Reference

Regular Expression (Regex)

In some of the wizard dialogs, regular expression can be used to improve the performance of the log file provider. If the regular expression is applied to a log file entry, regular expression matches, groups, and captures are created. Here is a short overview of commonly used elements of the regular expression language.

Character	Description	Regex Meaning
.	Dot	Match a single character
*****	Asterisk	Match the previous zero or more time
+	Plus sign	Match the previous one or more time
?	Question mark	Match the previous zero or one time
()	Brackets	Group
(?<*Name*>)		Named group
^	Caret	Beginning of line
$	Dollar sign	End of line
\w	Backslash w	Match word character
\W	Backslash W	Match non-word character
\s	Backslash s	Match whitespace character
\S	Backslash S	Match non-whitespace character
\d	Backslash d	Match decimal character
\D	Backslash D	Match non-decimal character
[]	Square brackets	Group of characters
[^]		Negated group of characters
\	Backslash	Escape special characters such as "." (dot) or "\\" (backslash). Example: \\. or \\\\

There is much more information available about regular expression on the following page: http://msdn.microsoft.com/en-us/library/az24scfc.aspx

Regular Expression Matches, Groups and Captures

Regular expression match

A regular expression match is created when the regular expression pattern is applied to the specified text. It contains the entire text that matches the regular expression. This could be the entire log file entry or a part of it. There could also be zero or more matches and it can contain groups and captures.

Example 1:
Text: abcabcabc
Regular expression pattern: abc

This will create 3 matches of “abc”

Example 2:
Text: abcabcabc
Regular expression pattern: [abc]+

This will create 1 matches of “abcabcabc”

Regular expression group

A regular expression group is a subset of the regex pattern. It can be used to get some parts from the log file entry. E.g. only the error message is required from the entry.
The existing unnamed groups “()” and named groups “(?<name>)”.

Example 1:
Text: abcabcabc
Regular expression pattern: (abc+)

This will create 3 match with 1 group of “abc” each match

Example 2:
Text: 2013-04-01 12:00
Regular expression pattern: (?<date>\d\d\d\d-\d\d-\d\d)\s(?<time>\d\d:\d\d)

This will create 1 match with a name group “date” with the value “2013-04-01” and a named group “time” with the value “12:00”

Regular expression capture

A regular expression group can also have one or more captures.

There is always one capture which contains the value of the entire match.

Example 1:
Text: abcabcabc
Regular expression pattern: (abc)+

This will create 1 match with 1 group and 3 captures of “abc”

Example 2:
Text: a123b456
Regular expression pattern: a(?<digit>\d)+|b(?<digit>\d)+

This will create 2 match with 1 group and 3 different captures of “1” “2” “3” for the first match and “4” “5” “6” for the second one.

Links

The following links contain more information about regular expression and the used regular expression operations:

Regular Expression Language:
http://msdn.microsoft.com/en-us/library/az24scfc.aspx

Substitutions Language (regex replace):
http://msdn.microsoft.com/en-us/library/ewy2t5e0.aspx

Regular Expression examples:
http://msdn.microsoft.com/en-us/library/kweb790z.aspx

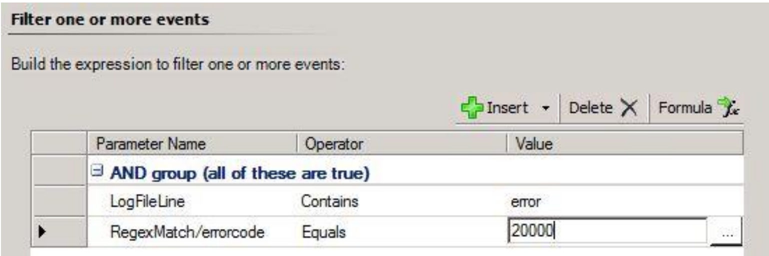
Regular Expression (programmatically):
http://msdn.microsoft.com/en-us/library/system.text.regularexpressions.regex.aspx
http://msdn.microsoft.com/en-us/library/30wbz966.aspx
http://msdn.microsoft.com/en-us/library/system.text.regularexpressions.matchcollection.aspx
http://msdn.microsoft.com/en-us/library/system.text.regularexpressions.match.aspx
http://msdn.microsoft.com/en-us/library/system.text.regularexpressions.groupcollection.aspx
http://msdn.microsoft.com/en-us/library/system.text.regularexpressions.group.aspx
http://msdn.microsoft.com/en-us/library/system.text.regularexpressions.capturecollection.aspx
http://msdn.microsoft.com/en-us/library/system.text.regularexpressions.capture.aspx
http://msdn.microsoft.com/en-us/library/system.text.regularexpressions.match.result.aspx

XPath

On `Expression Filter` or `Alert` dialogs, it is mandatory to use XPath to access the data provided by the log file provider.

On expression filter dialogs, the XPath can be used directly.

Example:



Filter one or more events

Build the expression to filter one or more events:

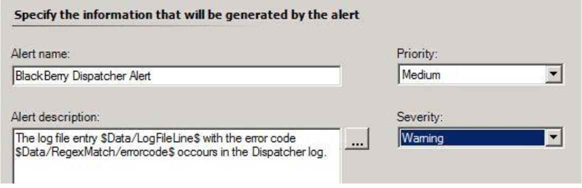
Parameter Name	Operator	Value
AND group (all of these are true)		
LogFileLine	Contains	error
RegexMatch/errorcode	Equals	20000

On alert dialogs or other dialog pages, it is mandatory to add the string `$Data/` in front of the XPath and the dollar character `$` at the end. For more information about syntax rules, see http://msdn.microsoft.com/en-us/library/ee533562.aspx

Example: `LogFileLine` in expression filter, `$Data/LogFileLine$` in the `Rule Alert` dialog, `$Data/Context/LogFileLine$` in the `Monitor Alert` dialog.

This XPath is dependent on the type of data item (`DataItem`).

LogFileMonitoringDataItem



Specify the information that will be generated by the alert

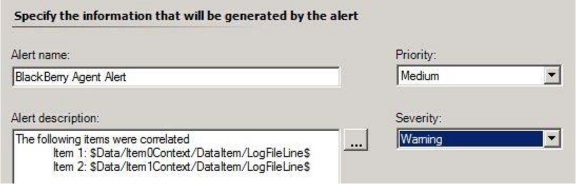
Alert name: BlackBerry Dispatcher Alert

Priority: Medium

Alert description: The log file entry $Data/LogFileLine$ with the error code $Data/RegexMatch/errorcode$ occours in the Dispatcher log.

Severity: Warning

System.CorrelatorData with 2 LogFileMonitoringDataItem



Specify the information that will be generated by the alert

Alert name: BlackBerry Agent Alert

Priority: Medium

Alert description:
```
The following items were correlated
      Item 1: $Data/Item0Context/DataItem/LogFileLine$
      Item 2: $Data/Item1Context/DataItem/LogFileLine$
```

Severity: Warning

Available XPath in Log File Provider

In the log file provider, the following XPath is available for usage.

> **Note**
>
> **XPath is case sensitive.**

This XPath is always available:

The folder where the log file is located:	`LogFileDirectory`
The name of the log file:	`LogFileName`
The folder and name of the log file:	`FullPath`
The log file entry which was read:	`LogFileLine`

> **Note**
>
> **The folder will be an absolute path. If environment variables like %temp% are used, the folder will be as example C:\Windows\Temp.**

If a regular expression is used there is more XPath available.
If a single match, group, or capture is present, a shorter version of XPath can be used.
Unnamed groups are available as Group1 … n.

> **Note**
>
> **Group0 contains the entire match and is always present.**

For a single match:
`RegexMatch`
Or
`RegexMatch/Group0/Capture`

For multiple matches:

`RegexMatch[1]`	(for the first match)
`RegexMatch[2]`	(for the second match)

Or
`RegexMatch[1]/Group0/Capture`

For a match with named group:
`//NameOfGroup`
Or
`RegexMatch/NameOfGroup`
Or
`RegexMatch/NameOfGroup/Capture`

For multiple captures:

`RegexMatch/Group1/Capture[1]`	(for the first capture)
`RegexMatch/Group1/Capture[2]`	(for the second capture)

This can all be combined:
`RegexMatch[3]/NameOfGroup/Capture[5]`
The third match of the group named “NameOfGroup” and the fifth capture of this group.

Regex replace:
If Regex replace is used, the result can be found under RegexMatch/RegexReplaced:

`RegexMatch/RegexReplaced[1]`	(for the first used regex replace)
`RegexMatch/RegexReplaced[2]`	(for the second used regex replace)

Note

Regex replaces operations only using the last capture of a group and every match separately.

Example:

Text: `a123b456`

Regular Expression: `a(?<digit>\d)+|b(?<digit>\d)+`

Regex Replace: `${digit}`

Result: One `RegexMatch[1]/RegexReplaced` with the value of “3” and one `RegexMatch[2]/RegexReplaced` with the value of “6”.

NiCE LogFileMonitoring DataItem example

```
<DataItem type="NiCE.LogFileMonitoringDataItem" …>
  <LogFileDirectory>…</LogFileDirectory>
  <LogFileName>…</LogFileName>
  <FullPath>…</FullPath>
  <LogFileLine>…</LogFileLine>
  <RegexMatch>
    <Group0>
      <Capture>…</ Capture >
    </Group0>
    <NamedGroup>
      <Capture>…</ Capture >
      <Capture>…</ Capture >
      ...
    </NamedGroup>
    ...
    <RegexReplaced>…</RegexReplaced>
    <RegexReplaced>…</RegexReplaced>
    ...
  </RegexMatch>
  <RegexMatch>
  ...
  </RegexMatch>
</DataItem>
```

Read Mode

On all read modes, the log files are read from the start or the last known position. The start position is dependent on the selected read mode. If the log file is deleted, the file size reduced, or some other changes occur, the read position can change.

The last position will also remain known during System Center Operations Manager Agent restart or crashes.

If a log file is already being read, then when the System Center Operations Manager Agent comes out of a maintenance mode the log file will be read from the first entry after the maintenance mode. Any log entries during the maintenance window is ignored.

Read Mode	Description
Read from begin/end (Default)	This mode is dependent on the file size. For log files that are smaller than 200 KB, the log file provider will start reading from the beginning, otherwise it will read from the end. If the file size is decreasing or the last read line didn't match, the provider will read from begin or end depending on the file size. If the file was deleted or creation date changed, the provider will read the entire file from beginning.
Read from beginning (Always)	The log file provider will read the entire file always from beginning.
Read log file from end	If the file size is decreasing or the last read line didn't match, the provider will read the file from end. If the file was deleted or creation date changed, the provider will read the entire file from beginning.

Troubleshooting

The troubleshooting chapter contains information covering the following areas:

- Logging
- Tracing

Logging

All important internal states and messages from the log file provider are written to the Operations Manager Event Log.

For error and warning events, self-monitoring is available in the Management Pack and shown as alerts in the `Active Alerts` view.

Tracing

The NiCE Log File can be enabled by two types:

- Enabling using override
- Enabling using file

The information written to the trace files is designed to help the support teams to pinpoint and solve problems as quickly and efficiently as possible.

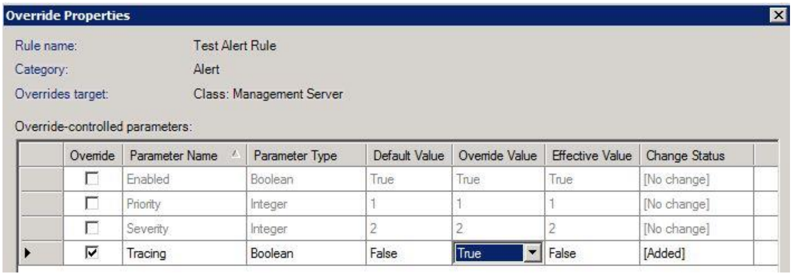
The Trace file will be written to the temp folder from the user which is used for SCOM agent.

If the SCOM Agent runs under Local System, the Temp Directory will be `C:\Windows\Temp`.

> **Note**
>
> **Tracing can produce large amounts of data in the trace file, and there is no file-size limitation for this feature.**
>
> **You should use tracing only if support asks you to do so. If you do enable tracing, make sure that tracing is switched off again after the targeted events have been triggered and the tracing actions finished.**

Enabling using override

Rules or monitors created for the log file provider contain a parameter named `Tracing`, which must be set to `true`, for example, by using an override. The `Tracing` parameter only enables tracing for the rule or monitor in which it is set.



Override Properties

Rule name: Test Alert Rule

Category: Alert

Overrides target: Class: Management Server

Override-controlled parameters:

	Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
	□	Enabled	Boolean	True	True	True	[No change]
	□	Priority	Integer	1	1	1	[No change]
	□	Severity	Integer	2	2	2	[No change]
▶	☑	Tracing	Boolean	False	True	False	[Added]

Enabling using file

To enable tracing, create the file `_spi.cfg` in the `%windir%/Temp` directory and insert the following content:

```
SPI_TRACE_STATUS ON
SPI_TRACE_PROCESS LogFileProvider
```

Removing the NiCE Log File MP

The following steps need to be performed:

1. Remove the Log File MP
2. Remove the Log File MP Installation Package

Remove the Log File MP

Perform this operation with the OpsMgr Administration Console. Delete the NiCE Log File MP Management pack and all dependent MPs from the OpsMgr Server in the Administration Console.

Remove the Log File MP Installation Package

Perform this step on each of the OpsMgr server where you installed the Log File MP package.

1. Use the `Add/Remove Programs` tool provided by the operating system and remove **`NiCE Log File MP`** entry.