



Using the NiCE Log File MP to create Alert Rules with Regular Expressions

for use with System Center Operations Manager

Whitepaper NiCE LogFile Management Pack Version 01.3x May 2017



000010000010100101

Contents

Contents	2
Purpose of this Document	3
Overview	4
Use Case Scenario	5
Steps to setup an Example ALERT rule	6
APPENDIX1	.3
Prerequisites1	.7
nstallation and Configuration1	.8
Overview1	.8

2

Purpose of this Document

This document describes a use case scenario for the NiCE Log File MP, highlighting how to create alerting rules that use regular expression for pattern matching entries in a log file.

The NiCE Log File MP Whitepaper provides useful information in addition to the Log File MP Quick Start Guide, without replacing it or parts of it. It should be seen as a supplement to better understand and use the Log File MP features.

NiCE Whitepaper

Overview

The NiCE Log File Management Pack monitors log files on the Windows platform and alerts based on matching patterns. The MP has numerous built-in wizards that help user create rules/monitors that read the log file entries. This paper walks you through how to create a simple alert rule that uses regular expressions. The paper gives examples for some of the regular expression concepts that can be used for pattern matching.



Use Case Scenario

The user wants to read log file entries and trigger an alert based on a matching pattern in a log file.

In this example, the rule is reading a csv file which has data of the following format *Message Type,Timestamp,QVW,Path,Error Code,Error,Log File,Log File Time*

A typical line that matches the above the format will be something like this FAIL,07/04/2016 17:36,SampleData,c:\myproject\data,3,General ODBC error (Script Error=3),QlikViewError.log,07/04/2016 17:35

The user wants to create an alert if a log line matches this pattern and some of the details in the log line should be included in the alert so the SCOM user can get the relevant details.



1.) Create a new rule in the SCOM Console and select the **Alert Rule** type as seen below.

📄 Create Rule Wizard		×
Select a Rule Typ	e	
Rule Type		🕜 Help
General	Select the type of rule to create	
Preprocessing Settings		
Log File Source Settings	Event Based	_
Regular Expression Settings (Optional)	B-M Probe Based	
Configure Alerts	Domino Database Performance	
	ICE Log Files Alet Rule Alet Rule Correlated log entries Correlated missing log entries Definition filtered	

2.) Select an existing or generate a new Management Pack where the rule is going to be saved.

MCE Log Files Alert Rule Correlated log entries Correlated log entries Correlated missing log entries Correlated missing log entries Correlated missing log entries Correlated missing log entries Performance Rule Description: Management pack Select destination management pack: Custom Log File	Vew
< Previous Next > Create	Cancel



3.) Navigate through the **General** page and specify the Rule name and the Rule target values. Ideally, set the rule to be disabled and you can override it to the specific node/group.

Create Rule Wizard	escription
Rule Type	🕡 Help
General	Select rule name, description and target
Preprocessing Settings	
Log File Source Settings	Rule name: Simple Alert Bule
Regular Expression Settings (Optional)	Description (optional):
Configure Alerts	
	Management Pack: Custom Log File
	Rule Category: Alert
	Rule target:
	Windows Computer Select
	Rule is enabled
	< Previous Next > Create Cancel

7

4.) Navigate through the Log File Source Settings page and define the log file details. You can specify the log file path either with absolute values or using environment variables as shown below. Note that the environment variables are dependent on the user who is going to run this rule (Action Account). You can specify the log file name also either with the actual log file or wildcards.

By default, the rule is going to read the log file from the beginning the first time it runs and then from that point on it will read any new entries. You can see more details in the Log File MP Quick Start Guide about **Read Mode**.

📄 Create Rule Wizard		×
NiCE Log File Mo	dule (Log File Source)	
Rule Type	🖗 Helo	
General	Log file source settings	
Preprocessing Settings		
Log File Source Settings	Log file path: 🕦 🗖 Subdirectories 🌒	
Regular Expression Settings (Optional)	%TEMP%	
Configure Alerts	Log file name: 🍿	
	qlikview_logs.csv Add	
	Remove	
	Edit	
	Absolut, relative paths and wildcard like * (multiple characters) and ? (single character) are supported.	
	Find log file using regex patterns (optional): 🌒	
	Add	
	Remove	
	Edit	
	Read mode: Read from begin/end (Default)	

5.) On the **Regular Expression Settings** page, define the pattern matching that will be used to identify if a line is going to be read from the log file.

In the example defined earlier, the rule is looking for entries like this *FAIL*,07/04/2016 17:36,*SampleData*,c:\myproject\data,3,*General ODBC error (Script Error=3)*,*QlikViewError.log*,07/04/2016 17:35

The data in this line maps to following as stated in the User Requirement *Message Type, Timestamp, QVW, Path, Error Code, Error, Log File, Log File Time*

The following regular expression will match the log line and will map the specific data to a variable so it can be used later on via XPath.

(?<MsgType>\w+),(?<MsgTime>[0-9/ :]*),(?<WorkSheet>\w+),(?<Path>[A-z:\\]*),(?<ErrCode>\d+),(?<Text>[A-z ()=0-9]*),*

In this regular expression four different elements of regular expression are used as shown in the color coded value.

- (?<MsgType>\w+) -> This matches any group of word characters and maps the data to a variable called MsgType. So in this example it will map the first word "FAIL" in the line to this variable.
- (?<MsgTime>[0-9/:]*) -> This matches any group of characters that are numbers, /, : and " " (blank space) in them and map this data to a variable called MsgTime. So in this example it will map the time value "07/04/2016 17:36" in the line to this variable.
- (?<Path>[A-z:\\]*) -> This matches any group of word characters, : and \ and maps them to a variable called Path. In this example it will map the path value "C:\myproject\data" in the line.
- (?<ErrCode>\d+) -> This matches any group of numbers and maps the data to a variable called ErrCode. In this example it will map the value "3" to the line to this variable.

You can see more details of using Regular Expressions in the NiCE Log File MP Quick Start Guide under the topic **Regular Expression (Regex)**.

The wizard has a built-in Regex testing tool that you can use to build or test the regular expression using the log file line that we are trying to match.

Logfile Line: FAIL.07/04/2016 17:36.SampleData.c:\myproject\data.3.General ODBC error (Script Error=3).Quick\NewError log.07/04/2016 17:35	
Filter Regex Pattern:	
[? <klsgtype>\w+),(?<klsgtime>[0-9/ :]"),(?<worksheet>\w+),(?<path>[A-z:\\]"),(?<errcode>\d+),(?<text>[A-z ()=0-9]"),(?<filename>\w+\.\w+)</filename></text></errcode></path></worksheet></klsgtime></klsgtype>	>
Split Regex Pattern:	
	>
Replace Reney Pattern	
	Add
	Remove
	Edit
	Test Renex
Sample Output (Xmi) XPath	- rest negest
<capture>FAIL,07/04/2016 17:36,SampleData,c:\myproject\data,3,General ODBC error (Script Error=3),Quick\ViewError log</capture>	
(Group0)>	
<pre></pre> Capture>FAIL	
<th></th>	
<pre></pre> Capture>07/04/2016 17:36	
<th></th>	
<capture>SampleData</capture>	
<pre></pre> Capture>c:\myproject\data	
<pre><capture>3</capture></pre>	
(/EnCode)	
<pre></pre> <capture>General ODBC error (Script Error=3)</capture>	
(/Text>	
<pre>clasture>cluickViewError.log</pre>	
	-

Once you have built the regular expression then you can use that as shown below to do pattern matching



OOOOOIOIO

6.) On the **Configure Alerts** pages, define the alert that the rule will generate if there is a matching line in the log file.

In the previous step, we used regular expressions to map data from the log line to specific variables. We can use these variables in the alerts using XPath and so the alert has meaningful information to the user.

You can see more details on XPath in the NiCE Log File MP Quick Start Guide topic **XPath**.

📄 Create Rule Wizard			×
Configure Alerts			
Rule Type			(2) Help
General	Conside the information that will be generated by the al		
Preprocessing Settings		ert	
Log File Source Settings	Alert name:		Priority:
Regular Expression Settings (Optional)	Simple Alert Rule		Medium
Configure Alerts	Alert description:		Severity:
	The log file \$Data/RegexMatch/filename\$ has the following entry: Error Status: \$Data/RegexMatch/MsgType\$ Time of Error: \$Data/RegexMatch/MsgTime\$ Error Code: \$Data/RegexMatch/ErCode\$ Error Description: \$Data/RegexMatch/Text\$		Waming 👱

- 7.) Save the rule and the Alert Rule is now created in the custom MP.
- 8.) Override the rule as appropriate for your environment so it gets enabled on the node where you have the log file that needs to be monitored.

9.) If all goes as expected, then when a pattern matching line is there in the log file then it will trigger an alert in the SCOM Console. Here is an example alert when a matching line is in the log file.

Alert	Properties					
General	Product Knowledge	Company Knowledge	History	Alert Context	Custom Fields	
Δ	Simple Alert Rule					
Key De	tails:					
Alert so	ource:	TAUVERY11.lab20	.nicelab.o	de		
Severity	y:	Warning				
Priority		Medium				
Age:		17 Hours, 29 Minutes				
Repeat	Count:	0				
TFS Wo	ork Item ID:					
TFS Wo	ork Item Owner:					
Owner:					Change	
Ticket I	ID:					
lert D	escription:					
The lo Error S Time o Error I Error I	og file QuickViewError. Status: FAIL of Error: 20/04/2016 2 Code: 3 Description: General (log has the following en 20:38 DDBC error (Script Error	try: =3)			
Alert	Properties					
	Desident Verside des		1	Alast Cantaut	1	

< DataItem type =" NICE.L onFile Monitoring.L onFileMonitoringDataItem " time =" 2016-04-20T18:49:04.04937487
"sourceHealthServiceId ="2106a651-11f5-bd8d-4b0b-e97af2a73dc1" >
< Loc FieDirectory > c:\temp loc FieDirectory
< Intelletane > dilation log cov
< EulPath > c/temp/olikyiaw loss csy
< Installed in a SEATL 20/04/2016 20/38 SampleData c/muneroject/data 3 General ODBC error (Scrint
Error=3) Ouic/VioyError Ion 20/04/2016 20:38 (Inspire Jeans) Outrie Inspire State (Inspire Jeans)
< ReneWatch >
< regenination >
Contract Sector 2010/04/2016 20:38 SampleData c:\mynchiect\data 3 General ODBC error (Script)
Error=3) Out/ViewError log 2/ Cashine >
< ManTyne >
Canhire > FAIL
< MsoTime >
< Capture > 20/04/2016 20:38
< WorkSheet >
< Capture > SampleData
< Path >
< Capture > c:\myproject\data
< ErrCode >
< Capture > 3
< Text >
< Capture > General ODBC error (Script Error=3)
< filename >
< Capture > QuickViewError.log



APPENDIX

You can see below the custom MP that would be created based on the steps listed above. Copy and paste it to any document editor and save it as **Custom.LogFile.MP.xml**.

```
<?xml version="1.0" encoding="utf-8"?><ManagementPack ContentReadable="true"
SchemaVersion="2.0" OriginalSchemaVersion="1.1"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
 <Manifest>
  <Identity>
   <ID>Custom.Log.File</ID>
   <Version>1.0.0.0</Version>
  </ldentity>
  <Name>Custom Log File</Name>
  <References>
   <Reference Alias="NiCELogFileLibrary">
    <ID>NiCE.LogFile.Library</ID>
    <Version>1.33.80.0</Version>
    <PublicKeyToken>058cf9bbd5db72a4</PublicKeyToken>
   </Reference>
   <Reference Alias="MicrosoftWindowsLibrary7585010">
    <ID>Microsoft.Windows.Library</ID>
    <Version>7.5.8501.0</Version>
    <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
   </Reference>
   <Reference Alias="System">
    <ID>System.Library</ID>
    <Version>7.5.8501.0</Version>
    <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
   </Reference>
   <Reference Alias="SystemCenter">
    <ID>Microsoft.SystemCenter.Library</ID>
    <Version>7.0.8433.0</Version>
    <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
   </Reference>
   <Reference Alias="Health">
    <ID>System.Health.Library</ID>
    <Version>7.0.8433.0</Version>
    <PublicKeyToken>31bf3856ad364e35</PublicKeyToken>
   </Reference>
  </References>
 </Manifest>
```

<Monitoring> <Rules> NICE Whitepaper

```
<Rule ID="MomUIGeneratedRuleeabba150d22647cc903fe08bf76cf900" Enabled="false"
Target="MicrosoftWindowsLibrary7585010!Microsoft.Windows.Computer"
ConfirmDelivery="true" Remotable="false" Priority="Normal" DiscardLevel="100">
    <Category>Alert</Category>
    <DataSources>
     <DataSource ID="DS"
TypeID="NiCELogFileLibrary!NiCE.LogFile.Library.Advanced.LogFileProvider.DS">
      <ProviderConfig>
       <Interval>60</Interval>
       <Unit>Seconds</Unit>
       <SyncTime />
       <WorkingDirectory />
       <Command />
       <Arguments />
       <EnvironmentVariables />
       <Timeout>0</Timeout>
       <Tracing>false</Tracing>
      </ProviderConfig>
      <LogFileProviderConfig>
       <Directory>c:\temp</Directory>
       <SubDirectories>false</SubDirectories>
       <Files>
        <FileNamePattern>qlikview_logs.csv</FileNamePattern>
       </Files>
       <ReadMode>Default</ReadMode>
       <RegexFilter>(?&lt;MsgType&gt;\w+),(?&lt;MsgTime&gt;[0-9/
:]*),(?<WorkSheet&gt;\w+),(?&lt;Path&gt;[A-z:\\]*),(?&lt;ErrCode&gt;\d+),(?&lt;Text&gt;[A-z
()=0-9]*),(?<filename&gt;\w+\.\w+)</RegexFilter>
       <RegexSplit />
       <RegexReplace />
      </LogFileProviderConfig>
     </DataSource>
    </DataSources>
    <WriteActions>
     <WriteAction ID="Alert" TypeID="Health!System.Health.GenerateAlert">
      <Priority>1</Priority>
      <Severity>1</Severity>
      <AlertName />
      <AlertDescription />
      <AlertOwner />
<AlertMessageId>$MPElement[Name="MomUIGeneratedRuleeabba150d22647cc903fe08bf76cf
900.AlertMessage"]$</AlertMessageId>
      <AlertParameters>
       <AlertParameter1>$Data/RegexMatch/filename$</AlertParameter1>
```

<AlertParameter1>\$Data/RegexMatch/filename\$</AlertParameter1>
<AlertParameter2>\$Data/RegexMatch/MsgType\$</AlertParameter2>
<AlertParameter3>\$Data/RegexMatch/MsgTime\$</AlertParameter3>

<AlertParameter4>\$Data/RegexMatch/ErrCode\$</AlertParameter4> <AlertParameter5>\$Data/RegexMatch/Text\$</AlertParameter5> </AlertParameters> <Suppression> <SuppressionValue>The log file \$Data/RegexMatch/filename\$ has the following entry:</SuppressionValue> <SuppressionValue>Error Status: \$Data/RegexMatch/MsgType\$</SuppressionValue> <SuppressionValue>Time of Error: \$Data/RegexMatch/MsgTime\$</SuppressionValue> <SuppressionValue>Error Code: \$Data/RegexMatch/ErrCode\$</SuppressionValue> <SuppressionValue>Error Description: \$Data/RegexMatch/Text\$</SuppressionValue> </Suppression> <Custom1 /> <Custom2 /> <Custom3 /> <Custom4 /> <Custom5 /> <Custom6 /> <Custom7 /> <Custom8 /> <Custom9 /> <Custom10 /> </WriteAction> </WriteActions> </Rule> </Rules> </Monitoring> <Presentation> <Folders> <Folder ID="Folder_d1bf4fb26b374daeb644c9bff5e950ea" Accessibility="Public" ParentFolder="SystemCenter!Microsoft.SystemCenter.Monitoring.ViewFolder.Root" /> </Folders> <StringResources> <StringResource ID="MomUIGeneratedRuleeabba150d22647cc903fe08bf76cf900.AlertMessage" /> </StringResources> </Presentation> <LanguagePacks> <LanguagePack ID="ENU" IsDefault="false"> <DisplayStrings> <DisplayString ElementID="Custom.Log.File"> <Name>Custom Log File</Name> </DisplayString> <DisplayString ElementID="Folder_d1bf4fb26b374daeb644c9bff5e950ea"> <Name>Custom Log File</Name> </DisplayString> <DisplayString ElementID="MomUIGeneratedRuleeabba150d22647cc903fe08bf76cf900">

15

<Name>Simple Alert Rule</Name>

NiCE Whitepaper

```
</DisplayString>
    <DisplayString
ElementID="MomUIGeneratedRuleeabba150d22647cc903fe08bf76cf900.AlertMessage">
     <Name>Simple Alert Rule</Name>
     <Description>The log file {0} has the following entry:
Error Status: {1}
Time of Error: {2}
Error Code: {3}
Error Description: {4}</Description>
    </DisplayString>
    <DisplayString ElementID="MomUIGeneratedRuleeabba150d22647cc903fe08bf76cf900"
SubElementID="DS">
     <Name>Log File Provider</Name>
    </DisplayString>
    <DisplayString ElementID="MomUIGeneratedRuleeabba150d22647cc903fe08bf76cf900"
SubElementID="Alert">
     <Name>Alert</Name>
    </DisplayString>
   </DisplayStrings>
  </LanguagePack>
 </LanguagePacks>
</ManagementPack>
```



NiCE Whitepaper

Prerequisites

©2017 NICE IT Management Solutions GmbH



001000001010010

Installation and Configuration

Overview

© 2017 NiCE IT Management Solutions GmbH