NiCE Log File MP

Using the NiCE Log File MP to Monitor Missing Log Entries

for use with System Center Operations Manager

Whitepaper
NiCE LogFile Management Pack
Version 01.3x
May 2017

NiCE
IT Management Solutions

Contents

Contents 2

Purpose of this Document 3

Overview 4

Use Case Scenario 5

Steps to Setup an Example Missing Log Entries Rule 6

Purpose of this Document

This document describes a use case scenario for the NiCE Log File MP, highlighting where it can be used to alert for missing entries in 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, which facilitates an in-depth understanding of the issues related to working in high availability environments.

Overview

The NiCE Log File Management Pack monitors log files on the Windows platform and alerts based on matching patterns. The MP has built-in wizards to create rules/monitors that are triggered if there are no matching patterns. This paper walks you through how this can be achieved using the NiCE Log File MP Missing Log Entries wizard.

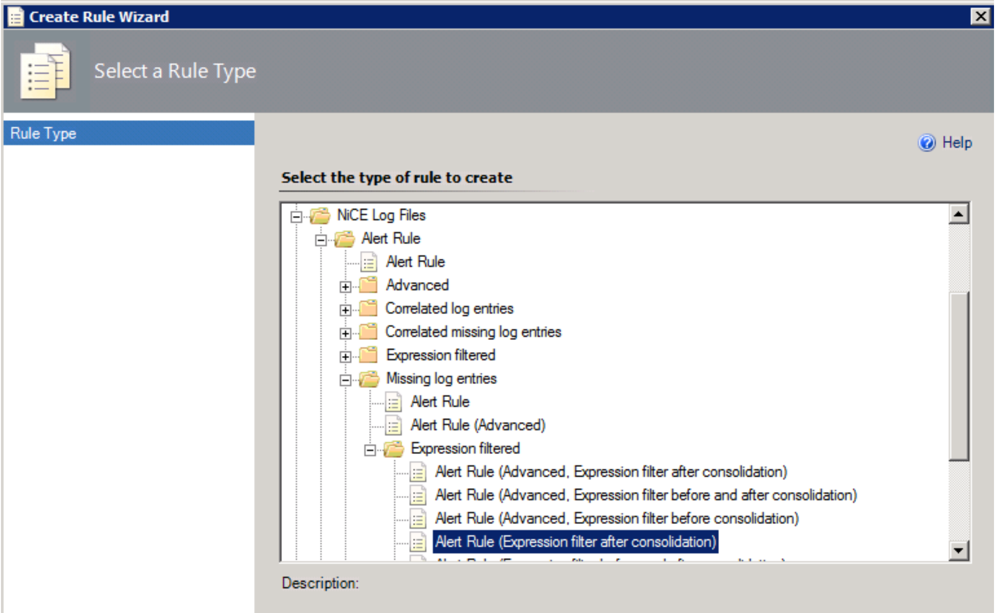
Use Case Scenario

The user wants to monitor a log file for a specific pattern to happen at least 2 times within a 5 minute window. If the log file is not updated, or if above requirements are not met, then an alert should be generated.

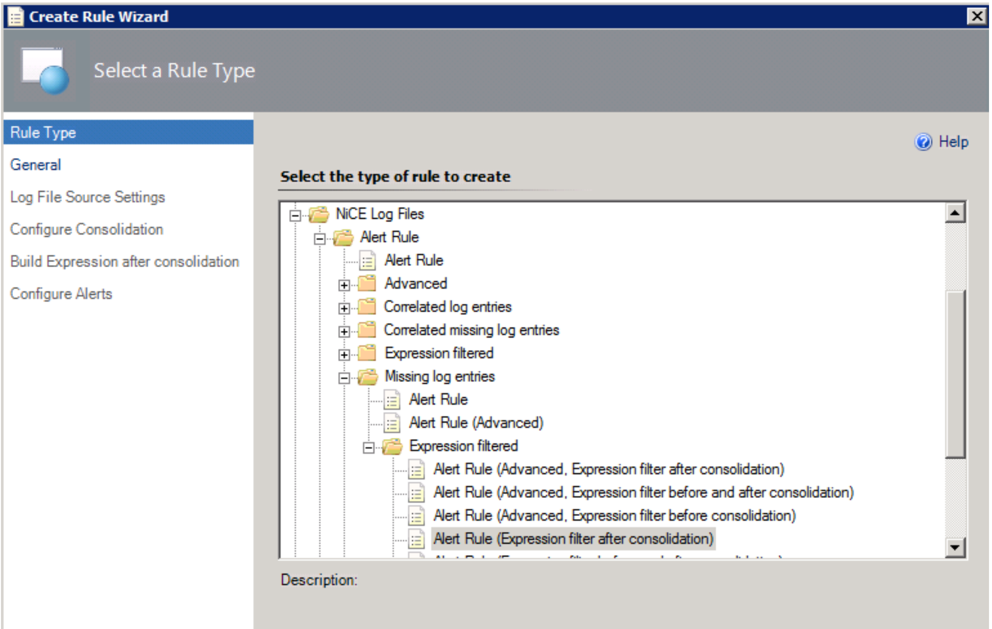
This can be accomplished by setting up a NiCE Log File MP **Missing Log Entries** rule/monitor that looks for a user defined number of pattern matches within a defined time window, and alerts accordingly.

Steps to Setup an Example Missing Log Entries Rule

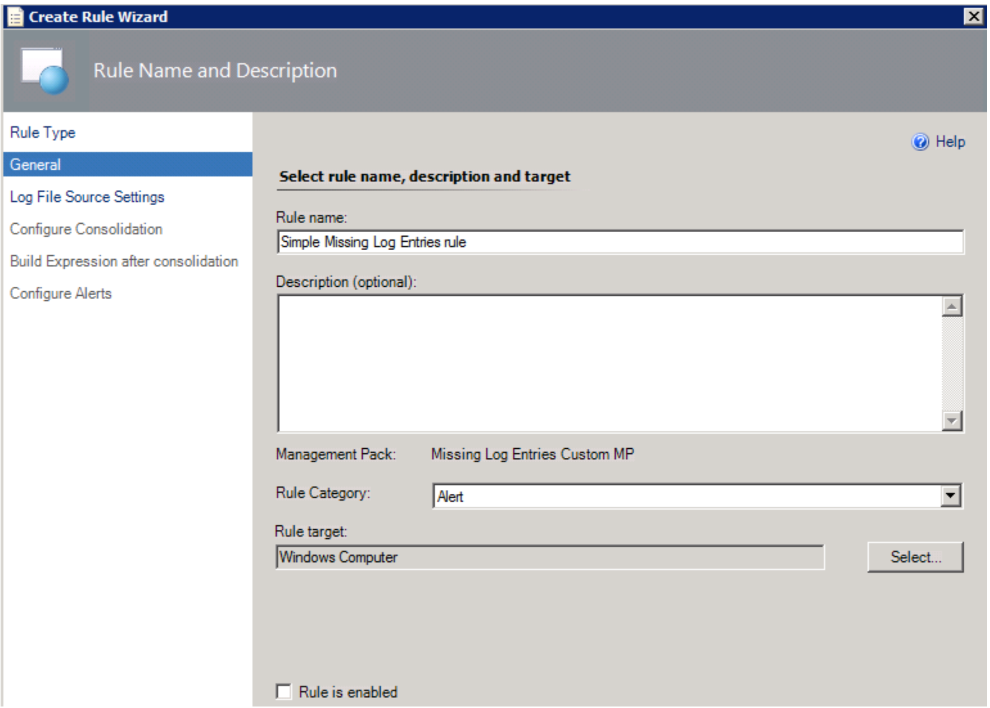
1. Launch the Missing Log Entries wizard from the SCOM Console


Create Rule Wizard
Select a Rule Type
Rule Type
Help
Select the type of rule to create
NiCE Log Files
Alert Rule
Alert Rule
Advanced
Correlated log entries
Correlated missing log entries
Expression filtered
Missing log entries
Alert Rule
Alert Rule (Advanced)
Expression filtered
Alert Rule (Advanced, Expression filter after consolidation)
Alert Rule (Advanced, Expression filter before and after consolidation)
Alert Rule (Advanced, Expression filter before consolidation)
Alert Rule (Expression filter after consolidation)
Description:

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


Create Rule Wizard
Select a Rule Type
Rule Type
General
Log File Source Settings
Configure Consolidation
Build Expression after consolidation
Configure Alerts
Help
Select the type of rule to create
NiCE Log Files
Alert Rule
Alert Rule
Advanced
Correlated log entries
Correlated missing log entries
Expression filtered
Missing log entries
Alert Rule
Alert Rule (Advanced)
Expression filtered
Alert Rule (Advanced, Expression filter after consolidation)
Alert Rule (Advanced, Expression filter before and after consolidation)
Alert Rule (Advanced, Expression filter before consolidation)
Alert Rule (Expression filter after consolidation)
Description:

3. Navigate through the General page and specify the Rule name and the Rule Target values. Ideally, set the rule to be disabled and then during deployment, you can override it to the specific node/group.



Create Rule Wizard

Rule Name and Description

Select rule name, description and target

Rule name: Simple Missing Log Entries rule

Description (optional):

Management Pack: Missing Log Entries Custom MP

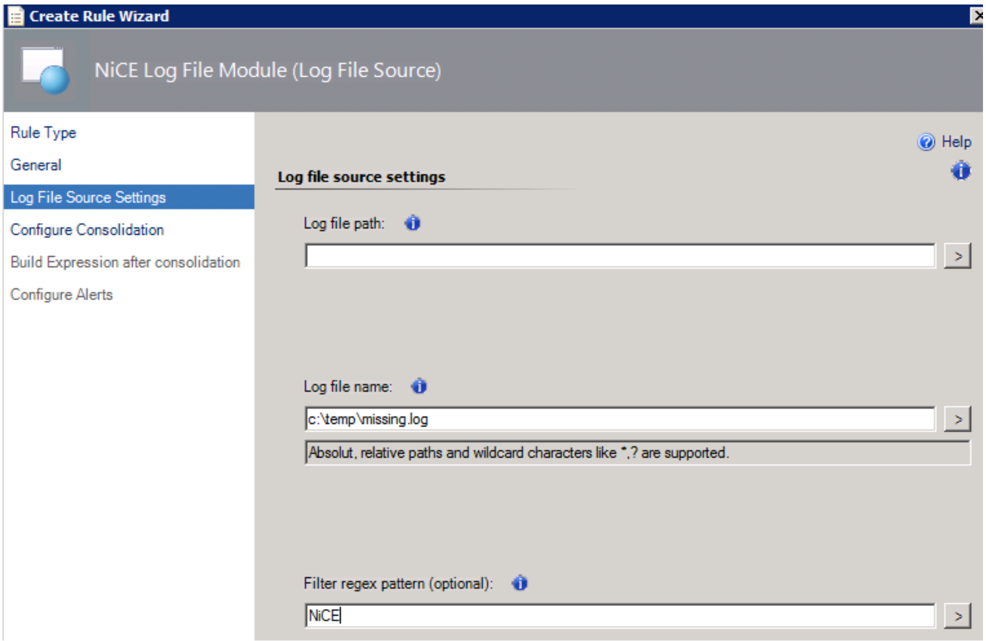
Rule Category: Alert

Rule target: Windows Computer

□ Rule is enabled

4. Navigate through the **Log File Source Settings** page and specify the log file name. You can do this either by specifying the Log file path value and then name of the actual log file. Alternatively, you can list the full path and the file name in the Log file name field as shown here.

   You can also specify any pattern matching that the rule is designed to look for in the log file, in this page. This can be regex pattern match or just text. Here the rule is looking for any log entries that has “NiCE” as the pattern match string.



Log file path:

Log file name: c:\temp\missing.log

Absolut, relative paths and wildcard characters like *,? are supported.

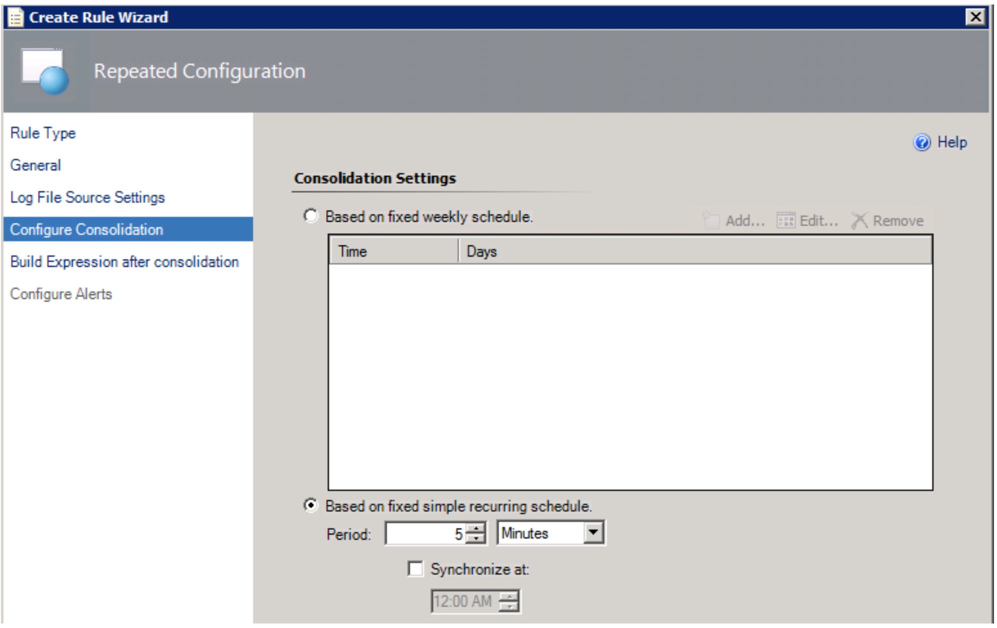
Filter regex pattern (optional): NiCE

5. On the **Configure Consolidation** page, you define time window for when the consolidation happens.

   A brief explanation on this topic. The rule reads the log file and looks for the specific pattern – in our example it is “NiCE”. Here, we are building a rule that will alert when this pattern is not found – either ‘none’ or ‘specific number’ within a specifed time window. This page defines that time window when pattern matching happens.

   Depending on the requirement, the time window can be specified as ‘fixed weekly schedule’ where you define the time, days or it can be ‘fixed recurring schedule’ where you define time increments.

   In this example, the rule is built to look for the defined pattern in the log file in 5 minute window.



Create Rule Wizard

Repeated Configuration

Consolidation Settings

○ Based on fixed weekly schedule.

Time	Days

● Based on fixed simple recurring schedule.

Period: 5 Minutes

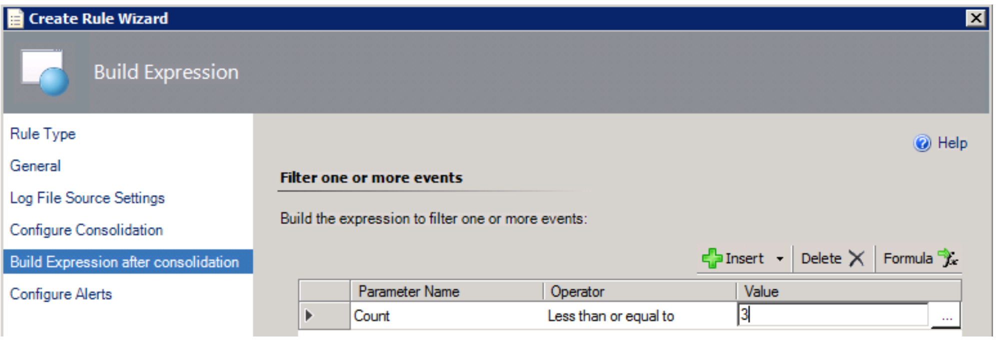
□ Synchronize at: 12:00 AM

6. On the **Build Expression after consolidation** page, you define the number of matching pattern entries before the rule triggers an alert.

   Again - a brief explanation on this topic. In the earlier step we defined the time window within which the pattern matching is done. In a specified time window, each log entry with the matching pattern updates an internal counter by one. At the end of the time window, this internal counter value is what we need to compare with user defined value.

   This page defines the user defined value of how many of these matching conditions would trigger the rule. Here “Count” is a key word (case sensitive) for the Parameter Name.

   In the example below, the rule is setup such that it will send out an alert if there are less than 4 log entries within a 5 minute window with a matching pattern of “NiCE”.



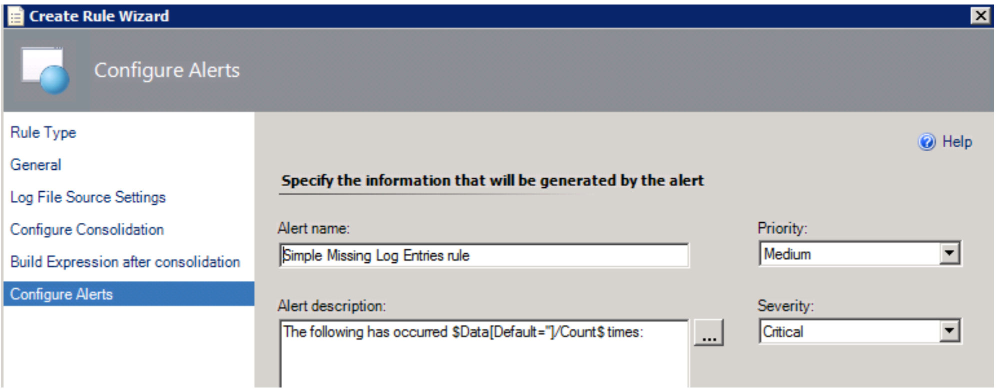
Filter one or more events

Build the expression to filter one or more events:

Parameter Name	Operator	Value
Count	Less than or equal to	3

7. In the Configure Alerts page, specify the alert description, priority and severity as per the requirements.

   If alert consolidation is needed then define the “Alert suppression….” tab and set the same value as the alert description. This way, duplicate alerts come in as ‘count’ and not clutter the SCOM Console.



Specify the information that will be generated by the alert

Alert name: Simple Missing Log Entries rule

Alert description: The following has occurred $Data[Default='']/Count$ times:

Priority: Medium

Severity: Critical

8. Save the rule and the Missing Log Entries rule is now created in the custom MP.

9. Export the custom MP as there is one manual change that need to be done.

   When creating the rule, the Parameter “Count” was used. By default, the wizard will create this parameter as a ‘string’ and here we are trying to use it as an ‘integer’ to compare it to user defined value (for example in this rule it was set to 3). To accomplish this numeric comparision, we need to edit the exported custom MP xml file.

   <u>Edit the XML file in any editor and look for this section</u>

```
<ExpressionAfter>
        <SimpleExpression>
                <ValueExpression>
                        <XPathQuery Type="String">Count</XPathQuery>
                </ValueExpression>
                <Operator>LessEqual</Operator>
                <ValueExpression>
                        <Value Type="String">3</Value>
                </ValueExpression>
        </SimpleExpression>
</ExpressionAfter>
```

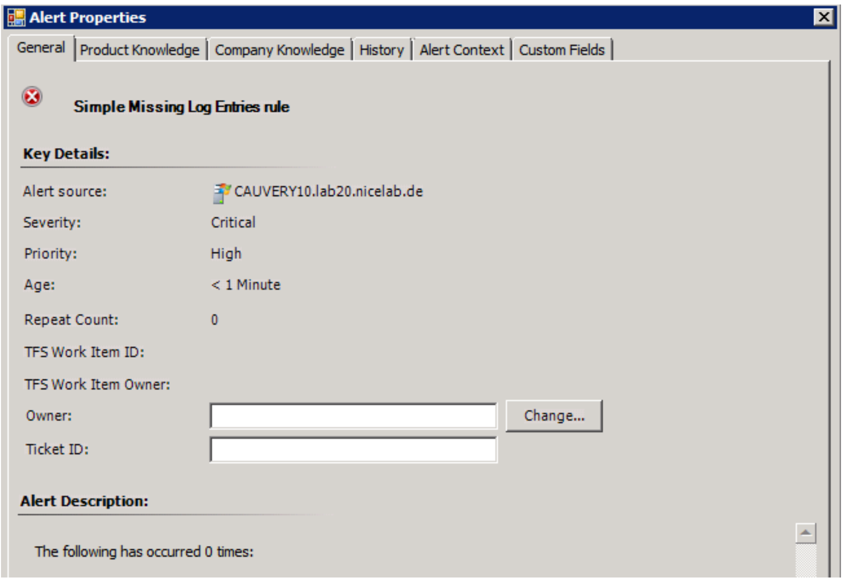
   <u>Change the Type value from “String” to “Integer” and so now this section looks like this</u>

```
<ExpressionAfter>
        <SimpleExpression>
                <ValueExpression>
                        <XPathQuery Type="Integer">Count</XPathQuery>
                </ValueExpression>
                <Operator>LessEqual</Operator>
                <ValueExpression>
                        <Value Type="Integer">3</Value>
                </ValueExpression>
        </SimpleExpression>
</ExpressionAfter>
```

10. Import the modified custom MP back into the SCOM server and verify that rule is there and everything is as you had updated.

11. 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.

12. If all goes as expected, then the rule would look for the matching pattern and generate alert based on defined count values. Here are two example alerts when there are less than 4 log entries with the pattern "NiCE" within 5 minute time window.



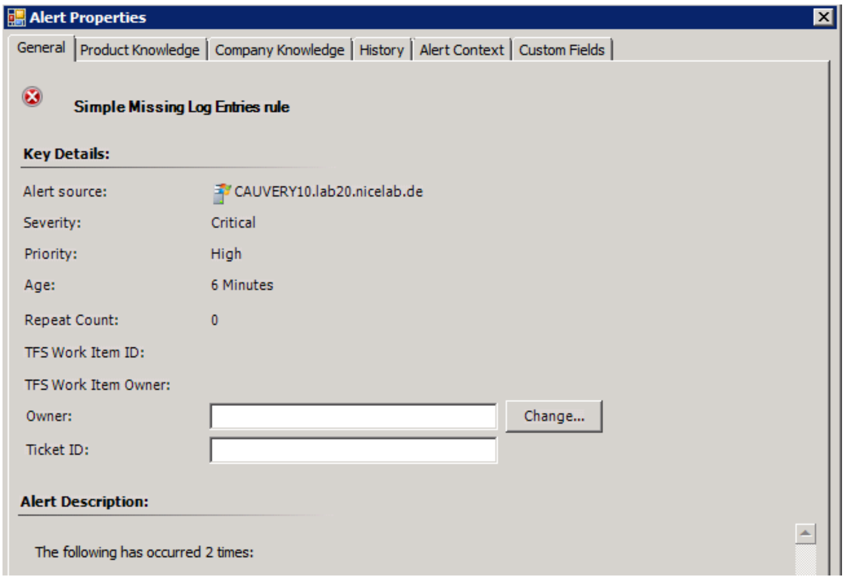
Simple Missing Log Entries rule

Key Details:

Alert source: CAUVERY10.lab20.nicelab.de
Severity: Critical
Priority: High
Age: < 1 Minute
Repeat Count: 0
TFS Work Item ID:
TFS Work Item Owner:
Owner:
Ticket ID:

Alert Description:

The following has occurred 0 times:



Simple Missing Log Entries rule

Key Details:

Alert source: CAUVERY10.lab20.nicelab.de
Severity: Critical
Priority: High
Age: 6 Minutes
Repeat Count: 0
TFS Work Item ID:
TFS Work Item Owner:
Owner:
Ticket ID:

Alert Description:

The following has occurred 2 times: