IT Management Solutions

Log File Monitoring

Innovative MP architecture

The NiCE Log File MP is a SCOM 2012 add-on to supercharge the log file analytic capabilities for your Windows Servers.

Business critical applications write health and performance information to log files and this is often left unattended and simply archived. It is time to tap into the pool of information that is contained in the log files.

The NiCE Log File MP is THE product to tap into the information contained in your log files. It provides more than 100 custom wizards to the SCOM Authoring console to create rules and monitors with ease. All parts of the NiCE Log File MP leverage native SCOM capabilities and provide a powerful tool that analyzes log content in full detail.

Technologies used

- Microsoft System Center Operations Manager 2012 SP1 and later
- .NET 3.5.1 Windows Server or later

Microsoft Partner
Gold Application Development
Gold Datacenter

NiCE Log File Management Pack for Microsoft System Center Operations Manager

Support for dynamic log file names and locations

Problem: It is often the case that you, as a system administrator, don't have the possibility to choose log file names and locations. It is simply set by your application. This application may roll log files on a daily basis or even on a service restart, resulting in complex log file names and directory structures. Furthermore, the out of the box log file module provided by SCOM only supports relative paths and no wild cards in paths. **Solution:** The NiCE Log File MP gives you the option to define log file names as absolute paths including the directory using a regex pattern with no restrictions.

Advanced Log Analytics

What does the NiCE Log File MP do?

Analyzing the log lines contained in a log file is the core functionality of the NiCE Log File MP. The main use case is still to analyze the individual log line. For this, the NiCE Log File MP offers a number of features. Before any filter on the log line is applied, the line can be split or matched strings replaced in memory. The logic of replacing, matching and splitting log line content follows the "Regular Expression Language".

The experience that we have amassed over the years has taught us that the use cases and requirements for the NiCE Log File MP are manifold. As such, analyzing log files also includes **looking for lines that do not exist**.

Some systems write health information in log files at regular intervals. You obviously want to receive an alert if the logline indicating the heartbeat of health information is missing. That could also mean that the application system hangs and the log file is not updated. The NiCE Log File MP gives you the option to set an alert on missing log files.

Correlating loglines is more of an advanced scenario. However, a use case exists here too.

Example: An ERP system writes information in the log about a job being dispatched. Per requirement, the dispatched job must be completed after a certain time. Hence, you will need to look for the log line that contains the job ID and indicate the job completion.

As each logline typically contains a timestamp, the time interval between the two log entries can be measured. If the time span between the two loglines exceeds a certain threshold, an alert should be triggered. This is another example use case covered by the NiCE Log File MP. The "Correlated" Log File MP Wizard can be used to easily create such "SCOM Alert" rules.

Monitor your log files according to your actual business needs

Beyond log file reading: Agent-based program execution interface

The NiCE Log File MP includes a powerful program execution interface that can run scripts and programs to create, extract and modify logs from proprietary event and log file sources.

This feature expands the usage of the NiCE Log File MP beyond just reading log files. This execution interface is part of a "Managed Module" for the Microsoft Monitoring Agent (MMA). Thus, it is truly agent based. It provides the best possible performance and no additional installation is required. As all processes run as sub-processes of the MMA, the SCOM security concept is fully applied using your SCOM actions account and run-as configuration.

Is the NiCE Log File MP something for me?

As already demonstrated, the use cases for the NiCE Log File MP are infinite. Here are just a few more examples of other use cases:

Monitor manufacturing systems

Most older manufacturing systems write all core event information to logs. All of these logs are typically proprietary to the vendor. The NiCE Log File MP monitors these critical manufacturing systems. However, in some cases it may be required to create a custom pre-processing script.

Monitor application system

Java log file? Application log files? Any type of log files in ASCII format is supported. This can be an extracted CSV file, text file or dump file. The wizards included with the Log File MP allow you to easily create an alert rule or a unit monitor for monitoring.

Microsoft Out-of-the-box capabilities vs. The NiCE Log File MP

Microsoft included a number of useful features in the out of the box product to analyze text log files. But it comes up short when files require pre-processing or log line corelation or many other use cases that are required to monitor business critical logs.

Features

- Comes with a set of custom authoring wizards to create:
  - Alert Rules
  - Performance Counters
  - Unit Monitors
- Allows you to set an alert on missing log files
- Allows you to define log file names as absolute paths
- The NiCE Log File MP interface is part of the Microsoft Monitoring Agent
- Includes a powerful program execution interface to run scripts and programs

Benefits

- Set the log file directory using a regex pattern with no restrictions
- Correlate your log lines
- Customize behavior if log file does not exist

Use Case Example

The log file of an in-house application is read by a custom script to take appropriate actions when there are issues. Per requirement, all entries in this file should be ignored during any maintenance window. Once out of maintenance window, only new entries in that log file should be read.

Log File MP has both rules and monitors that you can use to define how the file is read (Read from beginning, Read from End). Log File MP also automatically handles how the log file is read during a maintenance window as long as the file is read in an interval which is less than the length of the maintenance window.

Functionality/Use Case	Microsoft SCOM	NiCE Log File MP
Wild cards in Filenames	Yes	Yes
Customizable behavior if log file does not exist	No, gives error	Yes
Recursively process log files in subfolders	No	Yes
Filter log lines using regular expression language	No	Yes
Replace and split log line content before filtering using regular expression	No	Yes
Number of Authoring Wizards delivered	About 20	112
Process multiple log files within one module/provider	No	Yes
Alert on expected, but missing log lines	No	Yes
Option to run log file pre-processing commands	No	Yes

About NiCE

NiCE IT Management Solutions is a company that has over 25 years of experience with Cross Platform Application Monitoring Solutions on UNIX, Linux, and Windows. NiCE has amassed this wealth of experience from collaboration and integration with our valued Business Partners including HP, Microsoft, Oracle, IBM and BlackBerry.

NiCE roots come from years of developing and perfecting Smart Plug-ins (SPIs) with our Business Partner, Hewlett Packard. With the introduction of Microsoft System Center Operations Manager, NiCE started developing Application Monitoring solutions for this platform as well.

As a Microsoft Gold Datacenter & Gold Application Development Partner, NiCE provides management packs for database and communication applications.

The NiCE mission has always been to provide the best monitoring solution for IT professionals worldwide. The highly skilled NiCE team services clients from around the globe spanning from SMBs to large corporations. NiCE IT Management Solutions is focused on ensuring that our clients are completely satisfied with our products because of the value they add to their business.

Global operations

NiCE IT Management Solutions GmbH
Liebigstrasse 9, 71229 Leonberg, Germany
Phone +49 7152 939 82 0
E-Mail: solutions@nice.de

Americas operations

NiCE IT Management Solutions Corporation
3478 Buskirk Avenue, Suite 1000
Pleasant Hill, California 94523, USA
Toll-free Phone: +1 877 778 3730
E-Mail: sales@nice.us.com

All NiCE Management Packs

Active O365 MP | BlackBerry MP | Custom MPs | DB2 MP | Domino MP | Linux Power MP | Log File MP | Oracle MP | PowerHA MP | SAP MP | Veritas MP | VMware MP | zLinux MP

Microsoft Partner
Gold Application Development
Gold Datacenter

NiCE Log File Management Pack

for Microsoft SCOM

Free of charge!

Smart Application Monitoring You Can Rely On

NiCE
IT Management Solutions