Log File Monitoring on Microsoft SCOM

NiCE Log File Monitor Management Pack

Windows Log File Monitoring

Log files are the primary data source for network monitoring. Log files contain data about usage patterns, activities, and operations within operating systems, applications, servers or any other devices. Such data is of great advantage in security event monitoring (SEM), security information management (SIM), security information and event management (SIEM).

The Log File Monitor Management Pack enables next-level log file monitoring on the Windows OS, integrated into Microsoft SCOM.

- ✓ Advanced Log Analytics
- ✓ 100+ Authoring Wizards
- ✓ Advanced Data Correlation
- ✓ Scalability for Enterprise Environments
- ✓ Reporting
- ✓ Microsoft SCOM integration

NiCE
IT Management Solutions

NiCE Log File Monitor Management Pack

Features

Advanced Analytics

Monitor manufacturing and application systems. Create, extract, modify and analyze logs from proprietary event and log file sources.

Absolute Path & Name

Overcome complex log file names and directory structures using wild card search. Specify and save name patterns to filter for specific files.

Log Correlation

Detect a specific counting rate and/or order of log files.

Missing Logs

Check if a log was updated in a specific timeframe or if a regular log entry such as health checks doesn't appear in time.

Repeated Logs

Create an alert if a log entry appears a specific number of times in a given time window.

Event/Manual/Timer Reset

Reset monitor state back to healthy manually via the log entry or by using a timer.

NiCE
IT Management Solutions

NiCE Log File Monitor Management Pack

Features

Expression Filtered

Monitors and rules compare the incoming data using XPATH with a static text, regex, value and more.

Maintenance Mode

Define how logs are handled during maintenance windows.

File Age Monitoring

Monitor whether a file has been updated during a specific time frame or whether a file has been created.

Multi-Line Monitoring

Monitor log entries spanning more than a single line by a regex pattern via the UI to ease reuse.

Triggered Monitoring

Trigger log file monitoring by executing a command prior to log file analysis.

Scalability Algorithms

Health Cache size limitation is overcome by introducing local state files. Aggregate commands to reduce the number of program executions.

NiCE
IT Management Solutions

NiCE Log File Monitor Management Pack

Details

Advanced Log Analytics

The NiCE Log File Monitor Management Pack is a powerful program execution interface, running scripts and programs to create, extract and modify logs from proprietary event and log file sources.
Being a part of a "Managed Module" for the Microsoft Monitoring Agent (MMA), the execution interface is absolutely agent based.
As all processes run as sub-processes of the MMA, the SCOM security concept is fully applied using SCOM actions account and run-as configuration.

Defining log file names as absolute paths, including the directory

By default log file names and locations are set by your application. The application may roll log files on a daily basis or on a service restart, resulting in complex log file names and directory structures.
The NiCE Log File Monitor Management Pack allows you to define log file names as absolute paths using a regex pattern.

NiCE
IT Management Solutions

NiCE Log File Monitor Management Pack

Details

Missing log entries
Systems write health information into log files at regular intervals. You obviously want to receive an alert if the logline, indicating the heartbeat of health information is missing. The reason for this could be the application system hangs, hence the log file could not be updated.

Correlating missing log entries
Missing correlation is used to create an alert when in a time window one log entry appears, but a second specific entry is missing.
For example, take an ERP system logging a dispatched job. Per requirement, the dispatched job must be completed in a certain timeframe. Hence, you will need to look for the log line that contains the job ID and indicates the job completion.
If the time span between the two loglines exceeds your threshold, an alert will be triggered. The Log File Monitor Management Pack Wizard helps you to easily create such “SCOM Alert” rules.

NiCE
IT Management Solutions

NiCE Log File Monitor Management Pack

Details

File Age Monitoring
File Age Monitoring is useful to check for log files that were not updated within a specific timeframe or for files that are not generated at all.

Scalability Algorithms
Limitations induced by the Operations Manager are minimized by introducing locally saved state files in the Health Cache Directory
✓ File-Size Limitation of observed logs is obsolete
✓ Limitation of Monitoring Period is obsolete
Further, a cookdown mechanism is introduced to aggregate workflows and commands to be started in coherence.

Workflow Scheduling
Schedule your workflow by using e.g. “exclude days”, if an alarm should only be sent on weekdays.

Self Monitoring
The NiCE Log File Monitor Management Pack for Microsoft SCOM constantly monitors its own health and performance to guarantee autonomous system observability.

NiCE
IT Management Solutions

NiCE Log File Monitor Management Pack

Benefits

Save Time

Identify slow queries, errors causing transactions to take too long, or bugs that impact website or application performance.

Maintain IT Security

Retrieve data matching particular criteria, identify trends, analyze patterns. Get insights to maintain the environments' IT security and performance posture and prevent data breaches.

Holistic Monitoring

Deliver outstanding performance and availability by advanced log file monitoring based on filtering, correlation, analytics, and reportings.

Leverage Investments

Reuse your existing, proven Microsoft SCOM environment.

NiCE
IT Management Solutions

NiCE Log File Monitor Management Pack

Licensing

Licensing
The NiCE Log File Monitor Management Pack for Microsoft System Center Operations Manager is a free solution and does not require licensing.

Software Support
Customers can add support services for direct help with the NiCE Log File Monitor Management Pack. The free version does not include support.

Services
To help customers get a most effective set-up, NiCE is offering remote assistance.
Remote professional services include installation and configuration, training, and custom application enhancements.

NiCE
IT Management Solutions

NiCE Log File Monitor Management Pack

FAQ

What SCOM versions are supported?
The NiCE Log File Monitor Management Pack works with Microsoft SCOM 2012R2, 2016, and 2019.

What Windows Server versions are supported?
The NiCE Log File Monitor Management Pack works with Microsoft SCOM 2012R2, 2016, and 2019.

Do you invest in Log File Monitoring?
Yes. NiCE Management Packs for Microsoft SCOM are under constant development. New features as well as support for the latest platforms are added on a regular basis.

Do you provide custom services?
Yes. Whenever you need a specialized tweak or enhancement to best fit your environment, NiCE will assist with professional Management Pack authoring services.

NiCE
IT Management Solutions

NiCE Log File Monitor Management Pack

Contact

Get in touch for more information

EMEA/APAC solutions@nice.de
www.nice.de

AMS solutions@nice.us.com
www.nice.us.com