

NetMRI Event Analysis

A Real-Time Event Analysis Solution

A Dynamic NetMRI Add-on Captures Events, Identifies Symptoms, Interprets Events and Executes Corrective Policies—All in Real-Time

Overview

IT groups depend on the power of NetMRI to collect network information and provide a meaningful and actionable analysis of that data. Until now, however, IT specialists have been frustrated by the lack of detailed real-time analysis and the inability to engage in a proactive response to events and problems as they occur

NetMRI Event Analysis detects, diagnoses, and notifies you of network problems as they happen, giving you far greater insight into the minute-by-minute operations of your network than ever before. It achieves these insights by watching your syslog and SNMP trap event streams for you and analyzing them through clever and creative use of the strengths built into NetMRI. The solution augments the capabilities of NetMRI by automatically collecting, storing, and indexing event data, and then correlating network events with built-in NetMRI expert best practices rules and analysis.

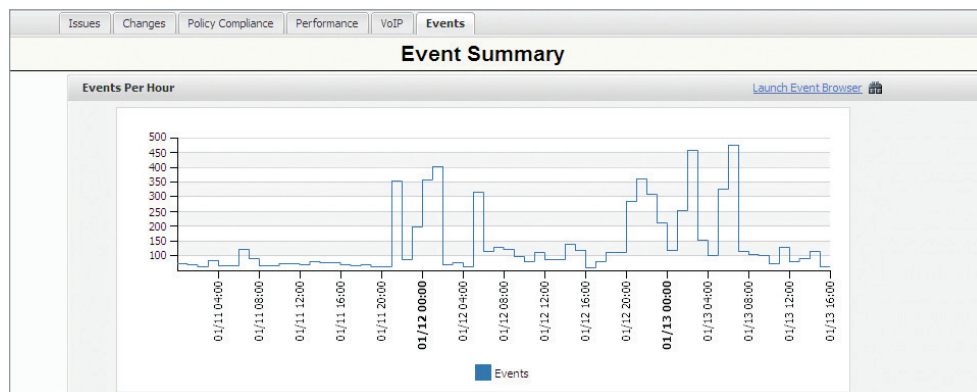
Round the Clock, Real-Time Surveillance

Many organizations use event logs only to learn what happened once they've exhausted other means of troubleshooting. However, we all know that buried within the millions of log file messages generated every day are some real gems that could provide actionable insights. The problem is finding them in time to respond before serious impacts occur. Ignoring event log data is a serious weakness for any IT organization.

NetMRI Event Analysis constantly sifts through syslog and SNMP event streams looking for the first signs of trouble. It discovers important events, including the one in a million that could cause critical business or network issues and would go unnoticed by ordinary event collection solutions. It immediately takes action by automatically creating diagnostic "Issues" in NetMRI, sending a notification, or even triggering a

Features and Benefits

- Detect, diagnose, and receive notification of network events as they happen
- Automate the collection, storage, and indexing of event data from SNMP traps and syslog
- Correlate network events with built-in NetMRI expert rules and analysis
- Automate real-time issue generation and automate issue close upon successful resolution
- Easily browse, filter, and search large numbers of current and archived events
- Generate reports on events and on event trends to help analyze and identify network vulnerabilities
- Dramatically enhance your NetMRI analytics with real-time information
- Correlate and verify problems with real-time and historical perspectives
- Improve your understanding of network events and reduce their complexity



Summary reports show top hosts and top messages, with drill down to the details of each event.



corrective action. By quickly and easily uncovering the few issues that foreshadow a network disruption, Event Analysis eliminates the ever-frustrating needle in the haystack scenario.

Built-in and User-defined Rules

NetMRI Event Analysis comes preconfigured with built-in event-driven issues that catch many of the most critical problems on today's networks. However, since no two networks are the same, it also lets you define your own event-driven issues with a simple, form-based interface. Furthermore, you can set the events so that they automatically clear themselves when the problem goes away.

Automating Issue Resolution

The NetMRI Event Analysis dramatically enhances the NetMRI analytics so that events over time offer actionable meaning that you can resolve on your own terms. You can also choose to have event trends addressed by predetermined scripts and policies you create before problems arise.

Coupling your rules with NetMRI's "pre-built" expert best practices, you can set the Event Analysis to anticipate and resolve most issues on your network. The Event Analysis will address issues automatically according to scripts you generate for resolution on your terms, including the generation of a report that the issue has been cleared.

Quick and Easy Browse and Search

The fact is, network engineers don't always know what problems they're looking for before they find them. The NetMRI Event Analysis includes powerful event indexing, search and browsing capabilities powered by Splunk, the IT Search Engine. Searching through huge amounts of event data couldn't be easier.

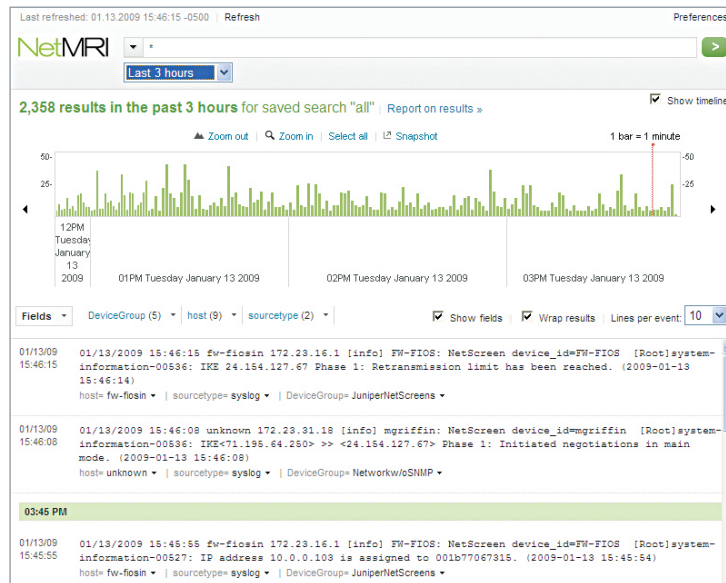
Not only are messages enhanced with NetMRI device name and

group information, but they are also hyperlinked back to the NetMRI device viewer for rapid investigation. You can even build sophisticated search criteria with little more effort than simply pointing and clicking on actual event message text.

Intuitive Summaries and Reports

The sheer number of events generated in most organizations makes monitoring logs challenging at best. In addition to automatically analyzing log data for issues, the NetMRI Event Analysis includes a rich set of summary graphs and tables to make it easy to identify troublesome trends.

The Event Activity Timeline, Top Event Device Groups, and Top Event Messages panels work together to provide an at-a-glance view into what's going on without the need to pull a log file. Additionally, drill-down summaries are always available to provide even greater detail.



Advanced searching capabilities combined with rules to filter the thousands of events received each minute, make a powerful combination.

For more information on Netcordia and our full range of automated network management solutions, please call **+1-410-573-2271** or visit **netcordia.com**

