

Perytons Monitor Add-On - Overview

The Peryton-Monitor allows to locally or remotely monitor operational networks for performance and interesting scenarios.

By using the built-in Open Source Rules wizard, the user can define rules (which are practically small pieces of intuitive code) on the received packets based on the specific criteria or scenario being investigated. Rules results can be set to generate events and/or alarms and update the customized statistics charts.



Events and alarms are logged into the Event Log window, and can generate automatic e-mail or other alerts.

The Peryton Monitor Add-on SW is very useful for system integrators, operators and field engineers, looking to monitor live system performance, identify misbehavior, etc.

Defining, writing and debugging rules are enabled with the Peryton-Monitor Add-on license. Definition of rules is easy, yet allows maximal flexibility. A rule can run on any field, looking for its value, meaning, hint, text or bare existence. Functions and variables can also be defined and used within rules. Rules can be used to mark selected messages with specific color (in Time View), set bookmark to identify interesting instance in time, or add selected messages to the Message View window (such a rule makes it easier to identify processes and transactions of interest in the presence of many messages which are not relevant for the current analysis).

There is no need for external development tools for defining and running rules since the Open Source Rules wizard is included as part of the Peryton Monitor Add-on. After it has been written, the rule can be exported and shared with other Peryton Analyzer users and incorporated into their analyzer environment. Rules are also kept in the workspace for easy sharing of the tested scenario with other analyzer users.

In addition to the on-line rules, off-line rules are used for previously captured files allowing displaying only relevant messages and making it easy to analyze long captures. The process of defining off-line rules is similar to the one used for the on-line rules, and utilizes the same development environment built-in the Peryton-Monitor Add-on license.

The Peryton-Monitor Add-on can run on top of any of the Peryton models.

For more information on Open Source Rules please refer to

<http://www.perytons.com/files/Peryton-OpenSourceRules.pdf>.

The screenshot displays the Peryton Monitor software interface. On the left, a rule editor window titled "Offline Active Monitoring Rules" shows a code snippet for an "AckLatency" rule. The code includes logic for tracking message times, calculating latency differences, and logging events. In the center, a flowchart illustrates the rule's execution logic: "Get new message" leads to a decision "Does it expect ack?". If "Yes", it goes to "Add To DB" and "Process chart", which then leads to "Build histogram Into chart". If "No", it goes to "Is it ack?". If "Yes", it goes to "Search In DB", which leads to a decision "Found?". If "Yes", it goes to "Add latency To histogram" and "Generate event Add to Message View". If "No", it goes to "Time < 10msec", which also leads to "Add latency To histogram".

At the bottom left, an "Ack latency histogram" chart shows the percentage of messages versus time in milliseconds. The y-axis ranges from 0 to 16, and the x-axis ranges from 0 to 8. The chart shows a significant peak around 6 milliseconds.

At the bottom right, an "Events Log" window displays a table of logged events:

Time	Level	Logger	Message
11:16:40.765	INFO	EventLogger	Long ack latency, Message#7 10.600msec
11:16:40.812	INFO	EventLogger	Long ack latency, Message#43 10.424msec
11:16:40.828	INFO	EventLogger	Long ack latency, Message#81 10.686msec
11:16:40.828	INFO	EventLogger	Long ack latency, Message#110 10.788msec
11:16:40.843	INFO	EventLogger	Long ack latency, Message#143 10.504msec
11:16:40.859	INFO	EventLogger	Long ack latency, Message#171 11.026msec
11:16:40.875	INFO	EventLogger	Long ack latency, Message#205 10.44msec
11:16:40.890	INFO	EventLogger	Long ack latency, Message#240 10.632msec
11:16:40.906	INFO	EventLogger	Long ack latency, Message#278 10.504msec