NETUITIVE®

User Experiences with System Monitoring Software

IT Pros Weigh in on Alert Management and Threshold Administration

In a recent telephone survey, 195 IT professionals shared their experiences with managing leading monitoring systems in their organizations. The discussions revealed that while most users rely heavily on their performance monitoring solutions, many find it necessary to sacrifice system functionality and/or invest significant amounts of administration time in order to avoid information overload. Many users hobble their monitoring solutions alerting functionality by intentionally setting thresholds higher than optimum (or turning off alerting altogether) to control alert volumes. Others spend significant time managing thresholds and setting baselines in order to reduce their proportion of false or non-critical alerts.

Research Highlights

Alert volumes can be overwhelming.
Overall 30% of respondents receive 100 alerts or more per day. In organizations with fewer than 100 servers, 15% of respondents receive 100 alerts or more per day. In larger organizations with 100 or more servers, 41% of respondents receive 100 alerts or more per day.

Many plagued by false alerts.
False alerts, non-critical alerts that do not indicate an immediate or impending service problem, are a common problem. Overall 30% of respondents say more than half of the alerts they receive are false alerts and 16% say that 70% or more of their alerts are non-critical.

Many set thresholds too high just to avoid alerts.
One technique many network managers use for reducing false alert volumes is to intentionally set thresholds at higher than optimum levels or simply turn off alarms. Overall 39% of the survey respondents told us that they intentionally set thresholds too high to limit alert volume. This is especially true among respondents who are getting 100 or more alerts per day. 47% of these respondents say they have already set thresholds high to reduce their alert volumes, thus limiting the system's alarm functionality.

Unfortunately this means that the users are getting less benefit than the performance monitoring software is designed to provide and they risk missing critical early notifications of impending problems.

Even diligent thresholding fails to curb false alerts.
Diligent threshold administration is supposed to control alert activity and reduce the volume of false alerts. More than half of the respondents report spending 10 hours or more per quarter (1.2 man-days) to manage the threshold settings for their performance monitoring system. 30% spend 25 hours or more (3 man-days) per quarter - that's almost two weeks per year.

However, even aggressive threshold administration fails to completely eliminate the problem of false alerts. Among respondents who devote 50 or more hours per quarter to thresholding, 43% say half or more of their alerts are false and 20% say more than 70% are false.

Alerts often arrive faster than problems can be diagnosed.
Overall, only half of respondents report that it usually takes less than 15 minutes to diagnose a problem and only 19% say it usually takes less than 5 minutes.

The scope of the problem intensifies in organizations with high alert volumes - 100 or more alerts per day. Among these, only 25% of respondents report that it typically takes less than 10 minutes to diagnose a problem. 13% report that diagnosis typically takes 30 minutes or more.

Which performance monitoring solutions does your company currently use?

BMC Software PATROL	39%
HP OpenView	8%
Mercury SiteScope	2%
Microsoft Operations Manager	11%
NetIQ AppManager	19%
Quest	2%
IBM Tivoli	3%
Other	16%

Multiple responses allowed

How many servers are you monitoring with this solution?

	On-site	Organization
None	0%	1%
1-9	7%	5%
10-49	18%	10%
50-99	12%	6%
100-999	42%	44%
1,000-9,999	15%	19%
10,000-49,999	1%	2%
50,000+	0%	1%
Don't know/no answer	5%	13%
	100%	100%

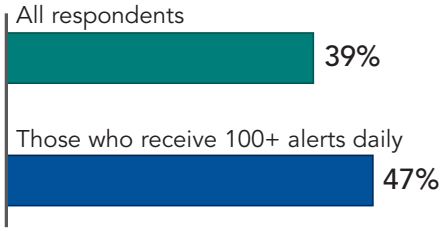
In a typical business day, how many alarms do you receive through your performance monitoring solution?

None	3%
1-49	43%
50-99	9%
100-499	18%
500-999	5%
1000-2999	4%
3000-4999	1%
5000 +	3%
Don't know/no answer	14%
	100%

How long does it usually take to diagnose a network problem from a performance monitoring alarm at your organization?

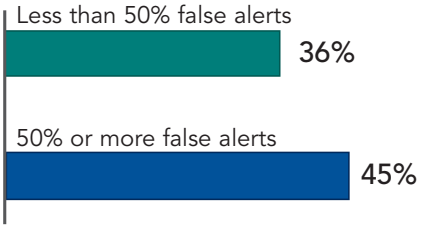
Less than 5 minutes	19%
5-9 minutes	19%
10-14 minutes	12%
15-29 minutes	15%
30-59 minutes	8%
60-120 minutes	3%
More than 120 minutes	1%
Don't know/no answer	23%
	100%

Many users sacrifice monitoring system functionality to reduce alerts



Overall 39% of respondents intentionally set thresholds higher than optimal levels simply to reduce alert volume. Among respondents who receive 100 or more alerts per day, 47% say they set thresholds too high.

Even diligent threshold administration fails to curb false alerts



Among respondents who spend 50 hours per quarter or more, false alert volumes remain high despite their effots. 45% say at least half of the alerts they receive are false alarms.

What percentage of the alarms you receive DAILY would you consider to be non-critical or false (that is, they do not indicate an immediate or impending service problem)?

None	4%
1-4%	15%
5-9%	13%
10-19%	13%
20-29%	8%
30-39%	4%
40-49%	2%
50-59%	11%
60-69%	3%
70-79%	2%
80-89%	8%
90% or more	7%
Don't know/no answer	10%
	100%

How many man-hours does your team typically spend on setting thresholds and estimating baselines for your performance monitoring software?

	Month	Quarter
None	5%	5%
1-4 Man Hours	29%	6%
5-9 Man Hours	12%	15%
10-14 Man Hours	11%	11%
15-24 Man Hours	5%	11%
25-49 Man Hours	6%	9%
50-99 Man Hours	3%	6%
100+ Man Hours	8%	14%
Don't know/no answer	21%	22%
	100%	100%

Do you set monitoring thresholds higher than the level you feel is optimum or turn alarms off simply to reduce the number of alarms you receive in your management console?

Yes	39%
No	52%
Not sure/no answer	9%
	100%

Are you currently implementing or planning to implement a Business Services Management (BSM) initiative?

Currently implementing	29%
Plan to within 6 months	9%
Plan to within 12 months	6%
Plan to within 18 months	4%
No Business Services initiative plans	30%
Don't know/no answer	22%
	100%

About the Survey

Are organizations making the most of their systems monitoring software? What is their experience using and managing them in real-world environments?

To answer these questions, Netuitive commissioned Channel Source Direct to survey IT managers and systems administrators who use these systems to manage their infrastructure.

In Summer 2005, CSD completed telephone surveys with 195 systems monitoring software users. Respondents were offered a chance to win a modest prize to encourage participation. This report summarizes their responses.

NETUITIVE®

12700 Sunrise Valley Drive
Reston, VA 20195
703 464 1390

www.netuitive.com