3 Network Monitoring Fails and How to Avoid Them

ipswitch

Nobody's happy when systems are slow

Long wait times caused by slow responses drain productivity throughout your organization. As time passes without a fix, users start to lose patience.

It's even worse when you're dealing with recurring performance issues. Even normally patient users will join in the complaints. Upper management starts to grumble. And each member of your IT team feels like they have that target on their back. There's plenty of negativity to go around.

No team wants to feel like a failure. But identifying the cause of performance issues quickly, in increasingly complex and interdependent networked environments, can be a real challenge. Unfortunately, our human desire to find the quick fix, often leads us to processes, tools and behaviors that aren't helpful. This is what causes the fails.

Every IT team wants to be and look their best so it can be helpful to see some of the common fails. We'll also look at how to avoid those fails by employing the practices of some of the worlds highest performance teams derived from a recent study conducted by Enterprise Management Associates (EMA).

IT'S EVEN WORSE WHEN THOSE PROBLEMS KEEP COMING BACK

Normally patient users join in the complaint storm. Upper management starts to grumble. And each member of the IT team feel like they have a target on their backs.

Fail #1 - Spending too much time in reactive mode

All IT teams spend some time in reactive mode. Every organization experiences unplanned service interruptions. The measure of a good operations team, however, is how often they are reacting to versus proactively addressing performance issues.

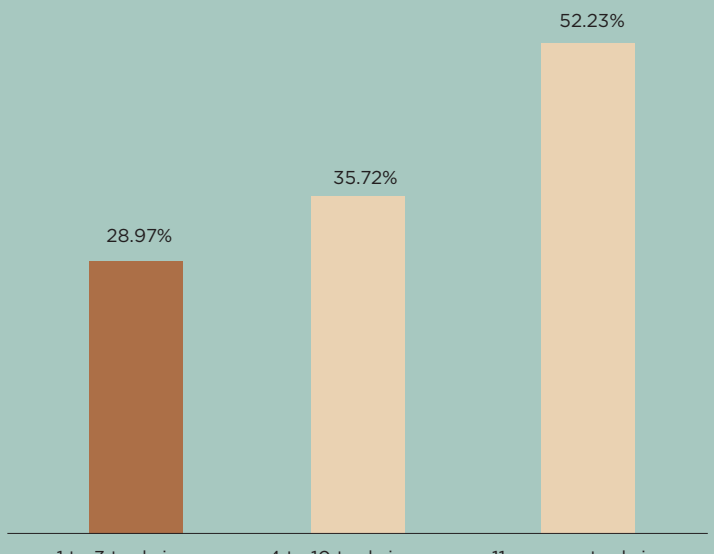
When users report a problem, and you are already working on a solution, you have a head start on troubleshooting time. If you first learn there is a problem from a user's complaint, it is more likely you will be perceived as taking too long to resolve the issue.

LOW PERFORMING IT TEAMS SPEND MORE TIME REACTING TO ISSUES THEY ARE ILL-PREPARED TO RESOLVE

Avoidance strategy

A recent study conducted by EMA measured the percentage of service affecting incidents that were first learned about from users (not through monitoring). Although it seems counterintuitive, they found a direct correlation between the percentage of user reported problems and the number of silo-specific monitoring tools in use.

Low performing teams tend to have more tools monitoring different technologies (network vs server vs application). High performing teams tend to rely on fewer tools, some of which monitor a broader range of technologies.



Percentage of problems first reported by end-users (source EMA)

The research suggests that using a smaller number of tools with a broader scope of technologies provides an advantage. End-to-end visibility and dependency-aware alerts help enable earlier detection of developing problems.

Finding the problem before the users do requires diligence. Threshold-based monitoring alerts must be set so as to provide meaningful early warnings of conditions in one technology that may lead to downstream problems.

These alert thresholds should be based on historical performance data. In this way, they can be configured to achieve the fine balance of not generating too many false positives while still catching troublesome conditions.

Fail #2 - Spending too much time resolving issues

As we said before, identifying the root cause of issues in complex networked environments can be a real challenge. Unfortunately, many IT teams set themselves up for failure by adopting processes, tools and behaviors that aren't helpful. A good example is relying on a large number of disparate, technology specific monitoring tools.

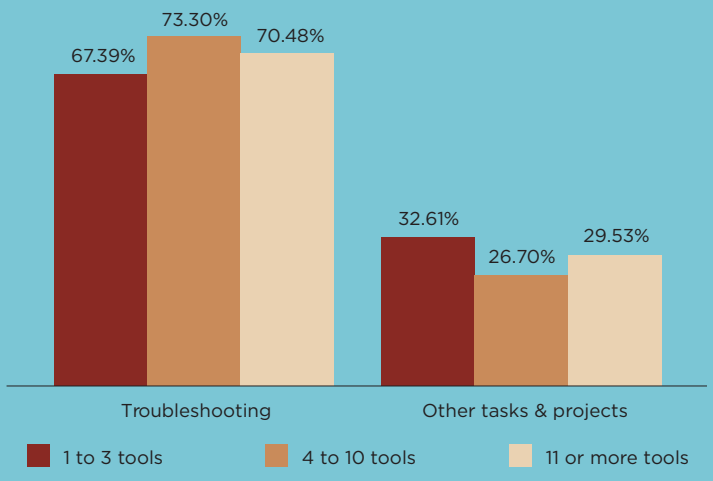
In those conditions, triage teams operate without an 'end-to-end' view of the problem they are trying to resolve. This leads to a series of best guesses as to potential causes. As each successive diagnostic path fails to address the issue, time drags on and users become more frustrated.

Avoidance strategy

The EMA study also found a correlation between the number of monitoring tools in use and the time spent in problem resolution. You guessed it, more tools are not better in this case.

Silo specific tools are often configured to detect what the responsible Subject Matter Expert (SME) considers problematic. That might not be the same condition someone responsible for an end-to-end service would look for to indicate potential causes of downstream problems. What passes as a 'healthy'condition at one level of the service delivery stack may cause disastrous results at a higher level.

The 'too many siloed tools' monitoring approach often adds considerable delay to your mean time to resolution (MTTR) especially in more complex IT environments. Addtionally, IT teams with one to three monitoring tools spend almost 33% of their time on other tasks and projects. That is 10% to 20% more time on meaningful projects than teams with four or more tools.



Fail #3 - Failure to find and fix the root cause

The more complex the issue, the less likely the cause can be found quickly. Some issues, like those involving inter-dependencies between middle-ware, applications and databases, are especially difficult to isolate. When triage teams are having difficulty finding the actual cause of an issue, they become more desperate for a quick fix. Often a quick reboot of a server will resolve the performance impact. Service is restored and everyone is happy - right?

Actually, high performing IT teams realize that this approach can lead to the creation of 'zombie' problems that keep coming back to haunt them. The more service impacting incidents resolved by reboot the larger the percentage of the time spent troubleshooting recurring issues.

Avoidance strategy

It is not likely you can find the root cause of every problem you are faced with. High performance IT teams, however, find more of them thus creating fewer 'zombies'. But how exactly do fewer tools lead to higher root cause identification rates?

The trick here is that these teams are leveraging tools that monitor multiple technologies to provide more of an end-to-end view of their environments. According to Enterprise Management Associates (EMA) "While discrete network management tools often fail to reveal interdependencies among the metrics they and other tools collect, multifunction management systems reveal these interdependencies and present them to network operations in various forms, from customizable dashboards and reports to dependency-aware alerts."

Using one tool that provides a consolidated, end-to-end view of your environment provides multiple benefits. You are alerted to more problems before users report them and you are able to resolve issues faster. Combined, those two benefits give you more time, without pressure, to find the root cause of problems before users get frustrated. This allows high performance teams to identify more root causes of problem thereby creating less 'zombies'.

Avoid the 3 fails of network monitoring with WhatsUp® Gold

WhatsUp® Gold is the favorite network monitoring tool of tens of thousands of IT pros. It allows you to monitor any mix of networks, servers, virtual machines, applications, traffic flows and configurations across Windows, LAMP and Java environments. More importantly, you can do it all with one flexible, affordable license that allows you to mix and match what you are monitoring at will. There's no need to purchase individual licenses for applications, network devices or network flow sources - they're all included.

Proactively monitor networks, traffic, physical servers, VMs and applications with powerful and easy-to-use maps, dashboards and alerts. Our unique interactive map quickly shows your end-to-end network, infrastructure and virtual health, providing the context of how everything is connected and dynamically responding to interactions to give you the fastest time-to-answers.

WhatsUp Gold streamlines workflows by letting you initiate management tasks directly from the interactive map or workspace. Easily switch between physical, virtual, wireless and dependency views to accelerate root cause analysis. Workflows are optimized, intuitive and initiated from the network map or easily-customizable dashboards. The result is simpler, more intuitive troubleshooting that lets you find and fix problems faster than ever.

About Ipswitch

With over 1 million users from 42,000 companies managing more than 150,000 networks in 116 countries, Ipswitch designs and develops industry-leading software that enables the easy delivery of 24/7 performance and security across cloud, virtual and on-premise environments. IT teams worldwide rely on 25 years of innovation to optimize and secure business transactions, applications and infrastructure with Ipswitch MOVEit® secure file transfer, Ipswitch WhatsUp® Gold network monitoring and Ipswitch WS_FTP®. Available directly or through strategic alliances with leading IT vendors and the company's fast-growing global partner ecosystem, Ipswitch's wide portfolio improves application and network performance, monitors diverse IT environments and ensures secure exchange of data that meets PCI, HIPAA, GDPR and other industry and government data security and regulatory requirements.

The company has offices throughout the U.S., Europe, Asia and Latin America. For more information, visit https://www.ipswitch.com/ or connect on LinkedIn and Twitter. To learn about Ipswitch's strategic alliances or global network of partners, visit https://www.ipswitch.com/partners.

ipswitch

See how easy it is to avoid the 3 network monitoring fails.

Download your 30-Day FREE TRIAL of Ipswitch WhatsUp® Gold