The 3 Dragons of Network Monitoring

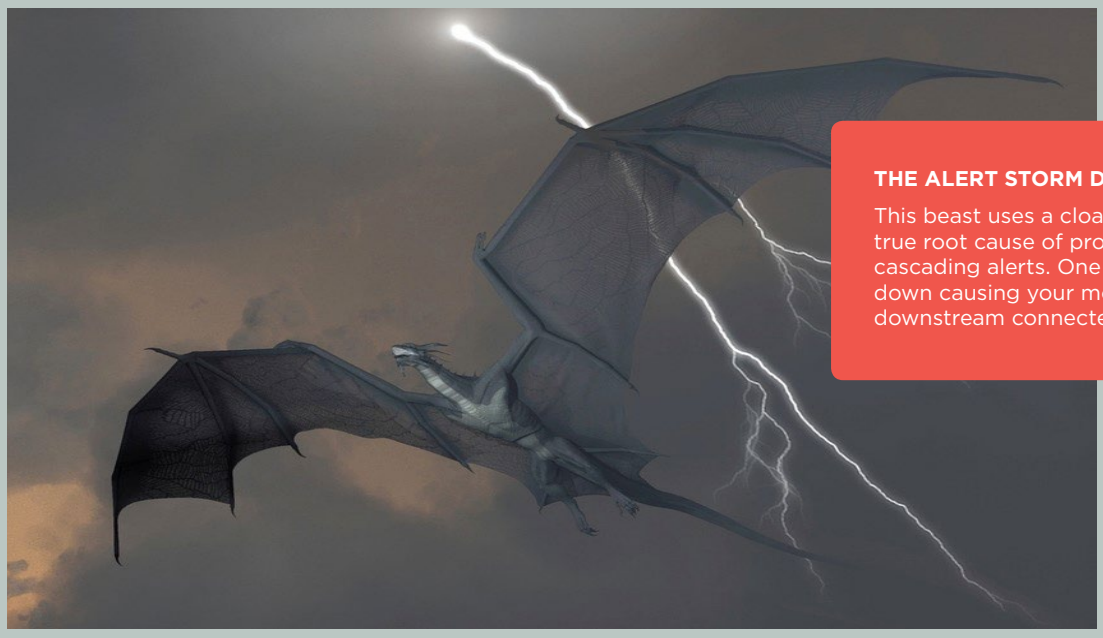
ipswitch

Network performance can be a beast

But the IT team that is properly prepared, with the right tools, can prevail in even the most difficult battles. Whether you are evolving from a disparate set of free tools, or replacing an existing monitoring tool set, you will want to focus on the core capabilities you need to tackle the scariest problems. Your team can turn into the knights in shining armor that save users and your company from the frustration and lost productivity caused by intermittent performance problems.

The Alert Storm Dragon

Without the proper tools, your monitoring environment can be plagued by alert storms. One port on a router or switch goes down making other devices invisible to your monitoring tool. This cascade of apparent failures makes it extremely difficult for you to separate real failures from false positives. With so many alarms to contend with, how can you quickly tell which ones are real and which ones aren't?



THE ALERT STORM DRAGON

This beast uses a cloak of invisibility to mask the true root cause of problems behind a storm of cascading alerts. One port on a switch or router goes down causing your monitoring tool to think that all downstream connected devices have failed.

You can end up having to review hundreds of unnecessary alerts, wiping out big chunks of your day, and preventing you from performing tasks that add more value to your organization. Alert storms delay fault isolation and resolution, which puts a huge drag on performance, availability, and user satisfaction.

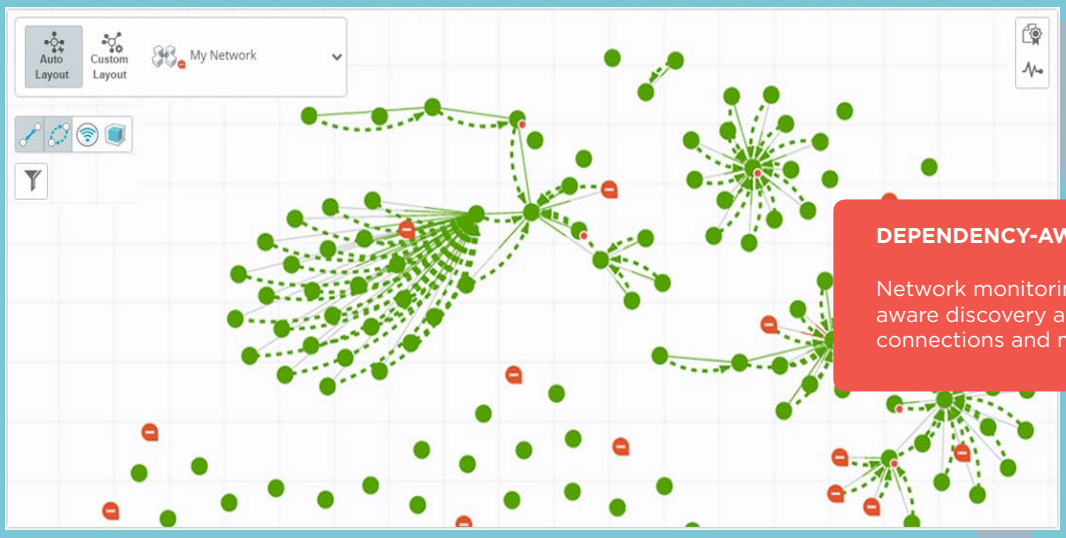
Alert storms arise when your monitoring tool is not 'dependency aware'. It fails to recognize the connections (dependencies) from one port to another. Monitoring tools that recognize dependencies will automatically suppress those alerts that are obviously generated based on these dependencies.

Slaying the Alert Storm Dragon

There are two ways a monitoring solution can address this issue for you. The first involves enabling the manual creation of dependencies. This can be a time consuming approach which can become untenable in network environments that change frequently or involve large numbers of dependencies. Let's say you decide to manually create the network dependencies required to prevent alarm storms. This means for every ten switches with typical 48-ports, for example, you have to create as many as 480 dependencies. You're looking at days of effort—and worse, when you make changes to your network, you need go through the process all over again.

The second, and more favorable approach, is to automatically create dependencies on discovery. This requires a more sophisticated discovery tool but does not necessarily drive the up the price. A solution that's dependency aware will solve all the monitoring problems you face. When your monitoring system understands how a network is connected and the dependencies between devices on the network, it will put a halt to alarm storms.

For example, you could see the connectivity between the router, switches and servers...and get only a single alert for a failed device, with alerts for all the other connected devices suppressed. This allows you to more quickly isolate, prioritize and resolve real network problems, leading to vastly improved performance and availability.



DEPENDENCY-AWARE DISCOVERY

Network monitoring tools enabled with dependency-aware discovery allow you to understand downstream connections and minimize the impact of alert storms.

The Angry Users Dragon

Every IT team experiences unplanned service interruptions. It could be the slow down of a key application, an unexpected outage or even the result of a planned change. The measure of a good operations team, however, is how often they are reacting to versus proactively addressing performance issues. Users want IT teams that are already working on the problem when they call. The help desk that answers 'yes we know and are already working on it' instills confidence. End-users will remain satisfied longer into a prolonged issue as they understand some are more difficult to resolve than others. But, 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. The more often this is the case the lower the confidence in the IT team.

If you've already tackled the Alert Storm dragon, you are half-way to slaying the Angry Users dragon. IT teams that experience alert storms frequently also suffer from alert fatigue. There are so many alarms going off they grow numb to the fact that some of them may be big problems. By assuring your network monitoring tool features automatic discovery and mapping that is dependency-aware, you better equip your team to spot issues before the users call.

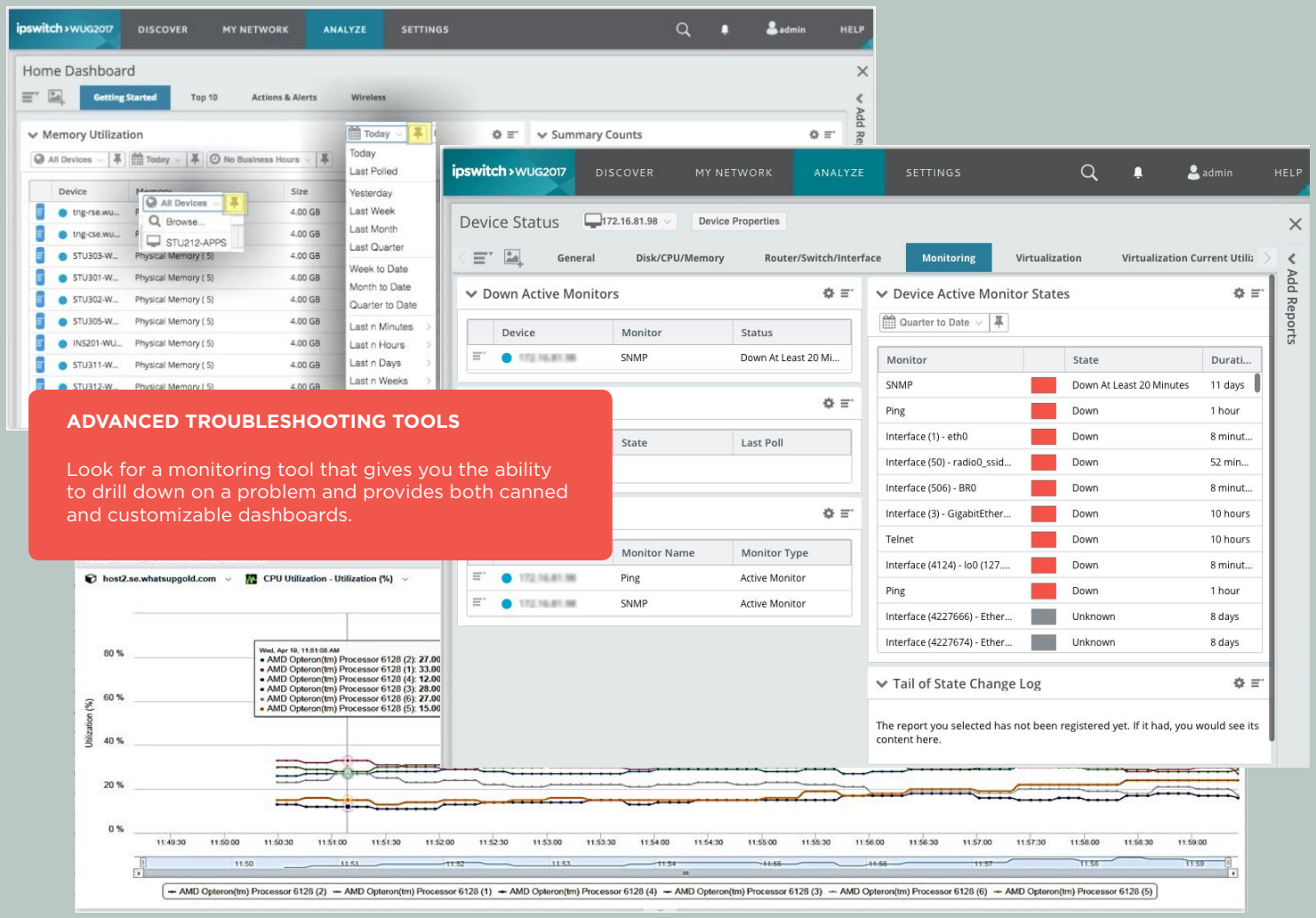
The Angry Users dragon feeds on IT teams that are always in reactive mode. If these teams also suffer from disjointed troubleshooting tools - they consider them a delicacy and often relish in causing them immense agony. Angry Users dragons tend to multiply as troubleshooting times drag on without a resolution often to the point of feeding frenzy.

Slaying the Angry Users Dragon

Sounds scary, right? Well, the good news is that it actually isn't that hard or expensive to protect yourself from the Angry Users dragon. With the right tools in your arsenal, you will rarely even see them. This dragon is opportunistic and would rather feed on the weak than to take on a worthy adversary.

The favorite tools of expert Angry Users dragon slayers are proactive alerts, customizable dashboards and user friendly drill-downs to device detail. Look for a monitoring tool that gives you the ability to drill-down to quickly pinpoint root causes. You'll want historical dashboards to identify trends and intermittent performance problems. You'll also need the ability to trigger scripts and embedded action to restart services and reboot network devices and services.

Basically, you want troubleshooting to be automated as much as possible and done the way you would do it.



The Lack of Visibility Dragon

Our final dragon is perhaps the most deadly of all. The Lack of Visibility dragon preys on IT teams that opted for 'free ware' and open source solutions to put together a hodge-podge of disparate tools. This dragon loves the confusion caused by attacking IT teams whose defenses aren't integrated. It delights in the pandemonium caused from everyone on the triage team having a different view of the problem.

These teams end up getting multiple reports on why performance is poor—each report from a different system, and more often than not, each one contradicting the other. It's no wonder finding root cause is so elusive. When they can't come up with a single, accurate answer all your IT teams can agree on— the Lack of Visibility dragon rules.

Slaying the Lack of Visibility Dragon

You should look for a monitoring tool that provides an integrated view of everything you need to manage. Whether that is switches and routers, virtual servers, wireless access devices, servers in the cloud or applications - you can't troubleshoot effectively unless you have the ability to see things in context.

Make sure you have a monitoring environment that allows you to see everything and miss nothing. Don't let a vendor force you to rely on partial solutions such as monitoring only a portion of the network.

Slay the 3 Dragons 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.

WhatsUp Gold streamlines workflows by letting you initiate management tasks directly from the interactive map or workspace. 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.

See how WhatsUp Gold can help you slay your network monitoring dragons. Learn More

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 defend your organization against the 3 dragons of network monitoring.

Download your FREE TRIAL of Ipswitch WhatsUp® Gold