How To Select a Network Monitoring Solution

There are several factors, or challenges, that drive a business to add or replace their Network Monitoring Solution (NMS) or Network Performance Monitor (NPM). When a decision is made to inquire into the marketplace and options, having a process in place to help ask the right questions, and even collate the answers into measurable results, can be invaluable in making a rational decision based on price, performance, and reliability without being swayed by glitzy marketing.

What is Driving the Need

Generally speaking every purchasing decision comes down to two business factors, either a new opportunity or a challenge presented by the existing situation. For example, you may have started a new business or grown into a larger organization through M&A requiring you to add a Network Monitoring Solution this would be a new opportunity. Challenges often come to light when existing solutions and processes fail to deliver during a critical event, perhaps an income impacting system outage or an unexpected price increase.

Tool/Vendor Consolidation

IT teams that have grown over the years either through organic growth or M&A often find themselves with many point solutions in place. If you have many tools doing the same type(s) of functionality, or it you're using several tools to troubleshoot one device, then you may benefit from Tool and Vendor Consolidation. With Tool Consolidation you reduce the number of tools your engineers are using to monitor devices, collect performance information, and generate alerts and escalations from events. By consolidating tools you reduce the need for training, make it easier for engineers to know where to go for answers and information, and potentially reduce your licensing cost. If through Tool Consolidation you are also able to reduce your total number of vendors then you also make negotiating renewals and contracts easier, reducing the overhead on procurement.

Collaboration

We often see teams where the network engineers use one set of tools and the server team another. As a result, when user experience or application performance problems are raised neither team has a cohesive view across the entire infrastructure to understand where the performance bottlenecks may be occurring. This increases the time it takes for root cause analysis and problem resolution. Having a tool that can monitor both traditional networking equipment (routers, switches, hubs, load balancers, etc), servers (of all operating systems) and generate synthetic transactions that exercise the entire application value chain cuts through those silos and provides immediate insight into where problems are occurring.

Reduced Workload

Some network monitoring solutions, by their very design, require a great deal of feeding and care. The best NMS/NPM solutions are set and forget, requiring very little ongoing knob turning and adjustments after the initial setup and acceptance.They often do this through integration with 3rd party systems like Help Desk, CMDB, and Billing. Are your systems making use of system integration, implementing business rules that import and update devices, generate help desk tickets, and other opportunities in order to reduce your workload?

More Than Just Performance

There are numerous NMS/NPM solutions on the market that are point tools, they may be designed to work with one manufacturer's equipment, or only one one class (i.e. routers) of equipment. Others focus on collecting just one subset of performance metrics, interface bandwidth for instance, or require you to pick and choose which things you want to see now. When considering a NMS/NPM solution Try to determine not just the breadth of features, but their depth. Does the tool collect all performance metrics from a device or only a few? Can it also collect detailed device configurations and alert you to changes? Can the tool take automated, proactive response to system events or does it just shoot out an endless stream of emails?

Questions to Ask Every Tool Vendor

Deployment/Implementation vs. Ongoing Maintenance

Every NMS/NPM vendor you speak with should be able to clearly and accurately describe the effort needed to deploy their solution in your environment - both from an equipment (i.e. server) requirement to how many Full Time Employees (FTE) are required to administer the system and operate the solution. If your deployment includes integration with 3rd party systems or significant automation (i.e. adding and retiring devices, etc) the time to configure or implement should be separated from the concept of simply loading the base application and getting it working.

Support for Remote Engineers and Follow-the-Sun NOC Teams

The need for this feature is really dependent on how your company is structured and where your network team members are located. If you have multiple teams, say one on the UK, one in the US East Coast, and one in India you would want all of them to have fast, accurate access to the NMS/NPM data with not limitation in features or data availability just because of their geographic location.

Solution Flexibility and Vendor Response

If Cisco were to release a new router tomorrow, and your company bought 200 of them, how long would it take your current vendor to provide full, deep support for the device? Could your team add support for it themselves without having to engage the vendor? If you needed to add a pre or post processing step to the collection of performance data, can you do it? Does the tool include a fully detailed RESTful API for both pulling and pushing information? Understanding how flexible the tool is, how well documented those features are, and how response the vendor is to everything form support type questions to bug fixes and manufacturer support are critical to a long term (>3year) solution.

Scalability

It seems that more and more business are growing through M&A rather than organic expansion. As a result, we often see multiple solutions deployed, not interconnecting or sharing data, and issues with managing multiple vendors and contract expiration/renewal. The tool's ability to scale beyond a single server or single geographic site into both a horizontal and vertical deployment - affordably - should be a core consideration. How easily can you add another 1k devices for monitoring, what would that cost is hosting and FTE? How long would it take to deploy?

Flexible Escalation and Alerting

Can you manage alerting for different shift hours and days of the week? How about handling for holidays and vacation? What about flexibility in how alerts are created and what content/format that takes? Can you create multiple escalation paths, notifying different people if the alert remains active and unacknowledged? What's the depth of this system, can different escalation paths be created for each type of event, or for different manufacturers or types of devices? The more flexible the escalation and alerting system, the easier it is for you to scale your solution and properly manage your team's workload.

Pricing

Pricing isn't just about the license cost, although that is a consideration. It's about how are license counted, what comes with a license? How man devices can a single collection server reliably manage? Ask yourself what else needs to be bought - do you need licenses for Microsoft Server as well as Microsoft SQL-Server for every new server you deploy? Do you need to pay for user licenses as well? Is Support & Maintenance included in the license cost? What is included with Support?