CITTIO

Best Practices When Selecting System and Network Monitoring Technology

by Jamie Lerner

May 2006

Introduction

All companies rely on computers, computer networks and software to conduct business. These computers and networks must remain healthy in order for a business to continue to operate. Due to the decreasing cost of computing equipment, businesses now use many computing devices from many vendors often spread across many locations. Should any computing equipment fail unexpectedly, the negative impact on the business can be severe.

A conservative estimate from Gartner speculates the hourly cost of downtime for computer networks at $42,000. Gartner also approximates that on average companies experience a total of 87 hours of downtime per year. A company who experiences a worse than average downtime of 175 hours per year could save about $3.6 million annually by implementing monitoring technology to achieve just the average amount of downtime.[1]

Due to the increasing complexity and quantity of both computing equipment and software, the task of monitoring the health of these systems cannot be performed manually. Therefore, specific monitoring software must be used to continuously perform tests and checks to ensure all the computers, network devices and software components are working properly.

Gartner states that when crucial servers and networks crash, businesses pay dearly in terms of productivity, damaged reputation and financial performance. According to *USA Today*, U.S. companies lost an estimated $100 billion due to network outages in 1999 alone. Even for average companies, the Standish Group warns that the cost of a single minute of downtime for a mission-critical application is $10,000. For large companies, the price can reach millions of dollars per minute.[2]

To reduce or eliminate expensive business disruptions caused by computing outages, system and network monitoring products have been available from major vendors such as Hewlett-Packard, IBM, BMC and Computer Associates. Network Management System (NMS) software now accounts for a significant portion of IT budgets. Last year alone, companies spent $7.1 billion on such products.[3]

Unfortunately, the monitoring products that traditionally have been available are not only very expensive, but also difficult to install and maintain. This stems from several key factors:

- Traditional system and network monitoring products were built on client server technology to monitor mainframes, mini-computers and large client server systems and networks that rarely change.
- Because the systems were not meant to change often, the fact that the software was complex and lengthy to implement, was tolerable because once configured, the software could conceivably run for a long time.
- Traditional systems grew in size and complexity as they gained momentum, resulting in large install bases with large recurring support revenues. Because of this, it has been very slow and difficult for traditional vendors to modernize their platforms.
- The license fees were developed during the client server era when spending over a million dollars and taking up to a year to deploy a monitoring solution was commonplace.
- As these systems grew and functionality was added, vendors ended up adding scores of add-on modules from partners, acquisitions and separate business units. These add-on modules often need to be integrated by hand or have lengthy configuration processes, resulting in the monitoring solution appearing as a patchwork of poorly integrated technology. Some vendors now offer over 100 add-on modules each with separate pricing models and configuration processes.
- Support fees often account for up to 60% of traditional vendors' revenues, and support revenues are calculated as a percentage of the license fees. This has led to strong reluctance to lower the license fees.

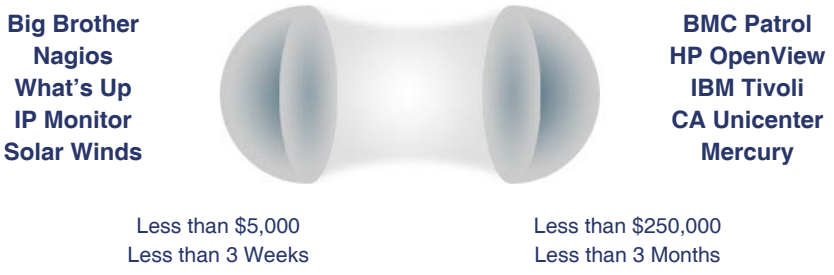
While system and network monitoring products have been available for many years, their high cost and complexity of installation and maintenance have caused the following to occur in the market:

- Many companies that have attempted to install traditional system monitoring technology have either failed or abandoned the project.
- Many companies have not deployed any formal monitoring technology.

- Many companies who need monitoring technology, yet have been unwilling to move forward with complex and expensive traditional systems, have deployed very low-end monitoring systems. By doing so, companies are sacrificing much of the functionality they require in exchange for a partial solution that is easy to use and inexpensive.
- Many companies have deployed homegrown or patched together open source solutions with mixed success due to the lack of support, functionality and documentation.

Today's Bifurcated Market

The path of choosing a high end enterprise solution, then abandoning the system due to expense or complexity then moving to a low-end band aid solution has lead to today's bifurcated NSM market.



Designing and Building an "Ideal" Monitoring Solution

There are a variety of best practices that should be adhered to when setting out to evaluate and select a system and network monitoring solution. These best practices have been developed from years of managing and operating data centers, as well as from performing multiple successful and unsuccessful monitoring projects. This is advice is garnered from over 10 years of data center operations and enterprise monitoring rollouts.

100% Web-based and Browser Independent

System and network monitoring tools that are 100% web-based are far more effective than client/server or partial web-based solutions. System administrators tend to work long hours on erratic schedules from different locations. By making tools available from any web browser, administrators will be much more effective at resolving issues quickly. Partial web-based solutions include tools that have web-based reports, but need a heavy client for configuration or tools that require some form of applet or active-X download. Having a partial web-based solution is better than having no web-access at all, but it is a **best practice to have a 100% web-based monitoring solution that is browser independent**.

Other reasons why a 100% web-based solution is an industry best practice for monitoring include:

- No client install or upgrades
- No client-side requirements, administrators can use whatever operating system that fits their needs
- Web-based user interfaces built in HTML tend to be simple, requiring little or no training

Customizable Portal-based Architecture with Multi-Tenancy

Portals were originally conceived by companies like Yahoo to provide a single interface to a large quantity of information that could be tailored to the needs of each individual. The portal concept is based on the idea that web sites often provide more information than most users would be interested in, so the portal technology allows users to select what things are of interest while ignoring or hiding those that are of less interest.

This same concept also holds true for system and network monitoring technology and IT departments. Often there are more monitoring statistics than an individual administrator may care or need to see. Multi-tenancy means that many users may be logged into the same monitoring solution yet see different systems or business processes. For example, an administrator in San Diego may only want to view monitoring statistics for that particular location, while an IT director in San Francisco using the same system may want to see information for all locations. Multi-tenancy is not only important to the IT department, but is critical for

the service provider who offers monitoring as a service. Multi-tenancy allows IT departments and managed service providers (MSPs) to supervise and maintain one system, while providing different information to different customers, departments, locations, or business processes.

Furthermore, IT departments have a wide array of needs that are typically met by a set of tools and products purchased from different vendors. Vendors often view the world from their perspective and only want an IT department to purchase tools from them, with little integration or support for other vendor's products. The portal allows a team to assemble all of their tools, given that they are web-based, into single dashboard. The role-based security model that is part of most portals can then be used to provide access to the appropriate tools for each administrator's needs. Therefore the portal, in conjunction with multi-tenancy, allows a single system to provide the right tools and views to the appropriate systems to meet the needs of each individual administrator, manager or executive.

The following are Best Practices that relate to multi-tenancy and a portal-based architecture:

- Multi-vendor support. Portals allow building a dashboard or collection of third-party tools that can be placed in one location.
- Portals use role based security to dynamically display user interfaces and tools for different roles in an IT organization.
- Benefits the managed service provider (MSP) by allowing re-branding of the user interface for different clients
- Benefits the IT department who provides services to different organizations or departments by allowing the creation of custom views
- Ability for security or convenience to scope what systems each person can see

Pricing Models and Add-on Modules

One of the major frustrations and pitfalls for IT managers is the complexity and hidden costs when implementing a network monitoring solution. Traditionally their monitoring projects have cost more than estimated and delivered less value than expected. The reasons for this are twofold. First, many NMS

products are sold as separate pieces, with some platforms having over 100 add-on modules and second, the difficulty of the implementation is often underestimated. It is frequently in the middle or at the end of an implementation project when one discovers the need for these add-on modules.

In order to protect against the risk of cost overruns, there are several best practices to keep in mind when reviewing the cost structure of a monitoring solution:

- Determine additional third-party products needed to make the system operate such as databases, operating systems, web servers or notification engines. **It is best to work with vendors who sell fully-bundled products with all required software.**
- **Vendors who require you to purchase additional third-party products or add-on modules tend to downplay the amount of integration that is required.** Look for systems that bundle all add-on modules in one installer. The entire system should install in less than an hour including all additional modules.
- **In addition to license fees, third-party products require additional support, upgrades and integration.**
- **Be wary of agent costs. Agents, if necessary, should be included.**
- Be cautious of add-on modules that ship from multiple vendors or were recently acquired by the vendor. These tend to be sink holes of consulting time. An external vendor typically is not as well integrated and may require you to call a different organization for support.
- **Simple pricing models are always the best pricing models**.
- Vendors who sell you 100% of their monitoring functionality in one bundle are preferable to purchasing feature bundles or add-on modules. **Add-on modules can amount to a huge hidden cost of a monitoring rollout.**
- **Be wary of per port, per probe, per monitor pricing models**. One Cisco switch could consume thousands of probes. Per node pricing models where all nodes are the same price, are the best pricing models.
- **Consider asking your vendor to provide futures**, lock in support and additional module or node pricing for several years so you know what your ongoing costs will be in advance.

Four key best practices regarding the cost structure of a monitoring solution consist of the following:

- One price per node, regardless of its size and type.
- 100% of the vendor's functionality ships in the base product, eliminating the need for add-on modules.
- The entire application stack should ship with the base product. No third party databases, notification engines, web-servers, or additional technologies need to be purchased.
- Vendor offers the option to sell multiple years of support at a locked-in price. Additional node pricing should also be established for an extended period of time.

Standards-Based Monitoring

Most organizations need to monitor the health and performance of various technologies from multiple vendors. When working across vendors and technology platforms, standards are essential for saving time from implementing one-off solutions for each vendor.

There are various competing standards in the world of system monitoring, yet only one standard has been in place for over 20 years and is implemented on every major platform with few exceptions. This standard is Simple Network Monitoring Protocol (SNMP). No industry standard or vendor specific solution has gained the ubiquity and breadth of coverage as SNMP.

- SNMP is the industry standard across all monitoring technologies
- SNMP is vendor, technology and platform neutral
- SNMP communicates using UDP rather than TCP/IP, lending to very little network impact

For these reasons, full SNMP support is a pre-requisite for any system monitoring technology.

SNMP Downside (Doesn't the "S" stand for simple?)

Despite the fact that the "S" stands for "Simple", SNMP is very complex, and can be difficult to learn. It is highly recommended that organizations choose tools that automate SNMP data collection without requiring MIB compiling or having to learn about the internal workings of SNMP. It is good practice to be able to work with SNMP, but not having to become an expert. Look for tools that use automation technology to dynamically collect performance variables for various platforms.

Not all SNMP Agents are Created Equal.

There are various forms of SNMP agents and monitoring agents. The following characteristics are recommended as best-practices for SNMP agent technology:

- Technology that leverages the pre-existing or built-in SNMP technology from a given vendor is superior to proprietary agents. For example, Citrix ships an SNMP agent with its product. This agent is complete, supported, maintained and upgraded by the experts at Citrix. Why replace this with a proprietary agent from another vendor? When you use the built-in agent from the vendor (Citrix in this case) the vendor upgrades both their software and their agent, thus saving you time. In addition, monitoring vendors do not typically provide support for new technology right away, while a vendor will upgrade their technology and their agents together.
- Lightweight agents are also more beneficial. Agents with only SNMP capabilities tend to be the best. Some vendors try to stick lots of additional functionality into their agents such as software deployment capabilities, thresholding and data collection, which consume system and network resources. These additions are hard to deploy, manage, and can destabilize the host system. Keep it simple.

Centralized Data Collection, Rather than Agent-Based

Some network monitoring solutions collect performance data at the agent or client level and set thresholds at the client level. Centrally managed systems are preferable to those that distribute monitoring rules and performance data on the agents or clients. Historical performance statistics should be kept at a centralized location. It is easier to manage a system where all the rules and data are contained in one area, rather than spreading out to every node on the network. In addition, reporting and thresholding is made easier if all of your performance data is in one central location.

SNMP Reads vs. Writes

SNMP has the ability to perform reads or queries of performance information and writes, which have the ability to change the configuration of a managed node. Typically it is a best practice to NOT allow your monitoring solution to make configuration changes by not allowing SNMP writes. The reason for this is because you do not want users accidentally making changes to production systems via the monitoring system and circumventing formal change control. **A monitoring system is typically best used as a read-only system and system wide changes are made through another system specifically designed for change control.**

Automation Technology

There has been a lot of hype around the concept of automation in the area of data center operations. Data centers have traditionally required many hours of manually intense labor by highly compensated and highly skilled professionals. By being able to automate many of the routine data center tasks, these professionals are made available to perform higher order or more valuable duties.

Many traditional system monitoring tools have a high degree of routine and labor intense configuration required to install and maintain the system. When evaluating a system monitoring package, look for tools with a high degree of automation of routine tasks. Automation technology will make the installation faster and easier and will drastically reduce system maintenance hours.

The following items are often automated in more modern system monitoring packages:

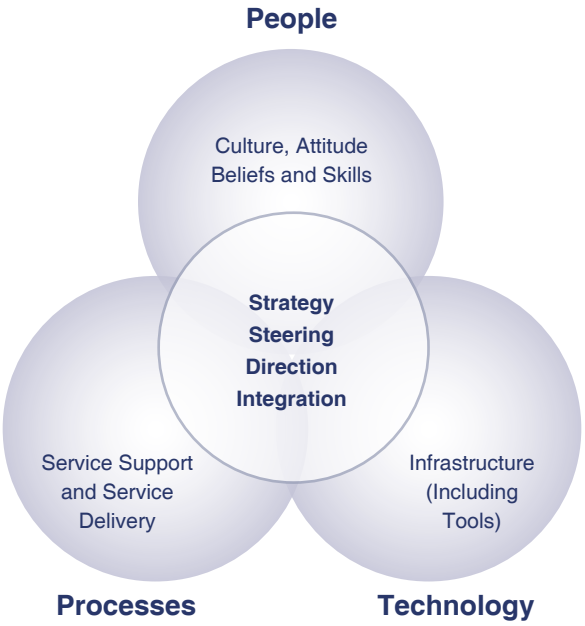
- Automatic Discovery of network nodes and their configuration.
- Automatic Discovery of services and running software.
- Simple or automated means of deploying monitoring agents.
- Automatic data collection using SNMP templates for most major platforms.
- Pre-configured industry-standard threshold templates.
- Pre-configured trap handling where major vendors trap definitions are already compiled into the product.
- Automatic discovery and removal of new nodes and services.
- 90% or more of the configuration is done within a simple user interface rather than script-based or programmatic interfaces.
- Ideal: Enter IPs and Community Strings, and the system configures the rest.

Things to be concerned about:

- Products that require SNMP MIB compiling. This is a lengthy and complex process even for experienced IT professionals; more modern products have designed ways around this process.
- Products that require creating your own graphs. An organization may monitor over 500 variables. The task of creating these graphs, including the mathematics to convert from bytes to megabytes and percentage utilization, can be extremely time consuming. Any errors made in this process can also lead to incorrect results. Graphs require QA, which will also lead to extended amounts of configuration time.
- Products that have script-based, rules-based, or programmatic interfaces for configuration: This requires training, testing, debugging, source code control and configuration management. Again, requiring valuable time and resources.

Support Operational Model – IT as a Business Process

The NSM technology is only successful to the extent that it integrates well with the people and processes of the organization that uses it. The operational model has features that allow the NSM to be customized to people and processes within an organization.



While the monitoring technology is important, equally significant is how the IT staff interacts and incorporates the monitoring technology into their day-to-day processes. The Operational Model should allow an IT organization to configure the monitoring system to fit the way they currently manage their network in the real world.

When a monitoring solution does not adequately fit the business processes of an IT organization, it tends to deliver less value and can often be ignored, resulting in a wasted investment.

Best practices when assessing if a product has a strong operational model:

- **Support for duty schedules:** Systems and networks operate 24x7x365 and many network systems will notify the same team members of problems around the clock. These constant notifications can exhaust a team. With the ability to enter team member's on-call or duty schedules, they will only be notified when they are on duty, and can rest when they are off-duty.
- **Support for skill set based groups:** Similar to duty schedules, teams can also become exhausted when team members are constantly notified or bothered with alarms that do not pertain to their skill set. For example, a network administrator may not want to receive database related alarms. Therefore, a NSM tool should group team members by skill sets and routing relevant messages to these skill sets.
- **Support for escalations:** Certain alarms are so important that you want to ensure that someone takes immediate action. In many cases the on-call engineers may be detained or unreachable and you will want to keep "hunting" for someone to notify. Escalations are a means of creating rules by which a notification will escalate or "hunt" for different individuals or groups until someone acknowledges the alarm. This prevents an alarm from going undetected.
- **Operator instructions:** Duty schedules, skill set groups and escalations make sure that an alarm or notification gets to the right IT staff members. There is no guarantee that this person knows how to address or fix the issue, can lead to inconsistent results. By way of example, one team member may fix the problem in 10 minutes while another might take 10 hours, or different people may take entirely different approaches when addressing the problem. In response to this issue, organizations often develop run books or action/reaction tables to capture institutional knowledge, policies and procedures for addressing network events. A NSM tool should support linking network events to operator instructions so that when an IT staff member is notified of a problem, the suggested instructions and policies for repairing the event are built into the system.

  Some NSM systems even have built-in document management platforms that allow for an IT department to manage and organize all of their IT documents. This is very convenient because it eliminates the problem of operators not being able to find or locate relevant information.

- **Scheduled outages:** NSM solutions that do not account for scheduled outages can lead to two significant problems. One, without scheduled outages, planned downtime will create an outage notification and could accidentally send alarms for planned outages. Second, and more significant, these planned outages will count against your uptime SLAs in the NSM's reports, causing inaccurately low SLA numbers.

  When evaluating NSMs, make sure that outages can be scheduled on a specific date or can be repeated either weekly or monthly. These outages should mute any notification during the outage, and any resulting downtime should be automatically excluded from all uptime or SLA reports.

- **Asset management:** Organizations that have many systems in multiple locations may spend a significant portion of their downtime locating and accessing equipment, or finding support information. For example, a server may crash sending a notification that 10.100.100.51 is down. This server could be in one of multiple data centers, within that data center it could be in one of many racks, and within a rack, it could be in one of many positions. This is compounded by the fact that the data center or closet may be locked, the rack may be locked and the physical server may be locked. Assuming that one can gain access to the server, the support contract could be in a filing cabinet in an entirely different location.

  Asset Management systems that are built into an NSM provide quick linkages between event or outage information and asset information, allowing machines to be quickly located along with relevant support contract information. Gaining access to the equipment faster saves significant time in resolving outages.

  Some organizations have asset management systems that are primarily used by the accounting department to keep track of physical assets for compliance and accounting purposes. However, these systems tend to have little or no value for the IT department who really need an asset system that is tightly coupled with an NSM tool's alarms. An IT staff needs to know where their systems are and what they are doing all from within one system.

- **Resolution tracking and configuration changes:** Once events are routed to the right people, systems are located, and operator instructions are provided. An engineer may then want to log some notes on how the event was resolved. This creates an audit trail and also keeps notes on how the incident was fixed

for future reference. The system should also have the ability to enter proactive configuration changes that do not necessarily have an event associated with them. For example, an IT department may want to log software installs, patches, equipment upgrades and relocations.

- **Support for packaged best-practices frameworks such as ITIL:** The monitoring tool's operational model can often provide a framework for operating a data center or IT staff. Rather than fitting your processes to accommodate a given vendor's view of the world, it is better for the NSM vendor to adhere to an industry best-practice framework such at ITIL or COBIT, providing the ability to select the NSM tool that best suits your business.

Real-Time vs. Historic Monitoring

A monitoring solution tool should allow both historic and real time visualization of performance statistics. Having the ability to monitor in real time in addition to standard performance monitoring provides a complete picture of what is happening on your network. Standard performance graphs typically gather data every 5 minutes (however this interval is often configurable) and present data over a longer period of time (days, weeks, months). Historical data is a true measure of how a particular node has been performing over a period of time, but offers little understanding as to what is happening at the current moment. With real-time monitoring the monitoring platform should be gathering statistics every 10 seconds by default and should keep a running time-series graph as long as the window is left open.

Support for Idiosyncrasies and Oddities

No two businesses are alike, and so, no two networks are alike either. Each organization is unique and builds systems to fit those unique requirements. A system monitoring product must be able to adapt to these network idiosyncrasies without weighing down the implementation with complexity and cost. The monitoring system should be able to leverage automation technology to monitor much of the network out-of-the-box, and then have the ability to support extensive customization as required.

Most frequently, organizations need the following custom monitoring capabilities:

- Support for centralized and remote custom pollers
- Support for custom data collectors

A custom poller is a simple program or script that tests a condition. A custom poller could perform a business transaction such as processing an order, or creating a new customer account. Because business systems are so diverse, the NSM **should support creating custom pollers in almost any programming language.**

The poller's location is as important as its functionality. For example, testing the processing of a check from a bank's headquarters is a very different test than processing that same transaction from a remote bank branch. The monitoring system should **support the concept of both central and remote pollers,** allowing pollers to be placed at various locations on the network.

The monitoring system should also **support different levels of sensitivity** for different segments of the network, different applications, and different equipment. For example, a bank may get great response time from equipment located at the headquarters, yet a much slower response time from remote branches. The system should be able to adapt to this by using different levels of sensitivity for different locations or applications.

In addition to pollers, organizations often have statistics and key performance metrics that are unique to their business. Therefore, the **NSM should be able to support custom data collection.** For example, a bank may want to measure the number of checks that were processed, or the number of new accounts that were created. The monitoring system should support the adding of custom data collectors in a standards compliant manner such as SNMP or WBEM.

System Monitoring can be viewed from a broad perspective that covers many different facets. In addition, many different players currently offer a wide range of different solutions. These two factors can make selecting the correct solution for your organization both difficult and confusing. Following the best practices stated above and utilizing the requirements work sheet provided below, selecting the best System and Network Monitoring will be more clear and precise.

[1]"How to Quantify Downtime"; *Network World*, 01/05/04
[2]www.simplewire.com
[3]"How to Quantify Downtime"; *Network World*, 01/05/04

Evaluating System and Network Monitoring Technology

The table below can be utilized to evaluate the network monitoring technology capabilities by vendor. The form can be printed and filled out, or it can be filled out while the file is open in Adobe Reader 6 and above. Remember to save the file after filling out the interactive form.

Requirements	*Vendor #1* (Type or write in name)	*Vendor #2* (Type or write in name)	*Vendor #3* (Type or write in name)
User Experience and Portal Functionality			
100% web-based user interface with no downloads or plug-ins required	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
100% web-based administrative interface	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Supports multiple browsers including Internet Explorer and Firefox	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ease of installation, configuration and administration that requires little/no training	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Support for personalization	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Skins for variable display attributes	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Role-based security access	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Local caching of remote content	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported

Requirements	Vendor #1 (Type or write in name)	Vendor #2 (Type or write in name)	Vendor #3 (Type or write in name)
System Cost Structure			
One price per node, regardless of the size or type of node	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
100% of the vendor's functionality ships in the base product, eliminating the need for add-on modules	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
The entire application stack should ship with the base product. No 3rd-party databases, notification engines, web servers, or additional technologies need to be purchased	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Multi-year support is available at fixed rate	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Future per-node pricing available at fixed rate	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Standards-Based Monitoring			
SNMP monitoring of any network device, server or software application	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
SNMP OID templates for major vendors - No need for MIB compiling	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
No client-side agents required other than standard SNMP agents and services	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Centralized data collection / Data not collected on each monitored node	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Automatic SNMP event trapping, no MIB compiling required	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Solution uses read-only SNMP capabilities	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Supports SNMP v1, V2c, and v3	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Support for newer standards such as WBEM and JMX	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported

Requirements	*Vendor #1* (Type or write in name)	*Vendor #2* (Type or write in name)	*Vendor #3* (Type or write in name)
Automation Technology			
Auto discovery of manageable devices	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Auto discovery of applications	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Automated means of deploying Monitoring Agents	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Automated data collection through SNMP templates for major platforms	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Pre-configured industry-standard thresholds for major platforms	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Automatic SNMP event trapping	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Automatic removal of nodes and services	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
General configuration provided through simple user interface / rather than script-based or programmatic interfaces	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to automatically email SLA reports in PDF or HTML format	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
100% automated SNMP devide identification, data collection, and graphing. Only need to enter IP address and community string	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported

Requirements	Vendor #1 (Type or write in name)	Vendor #2 (Type or write in name)	Vendor #3 (Type or write in name)
Operational Model			
Ability to perform advanced event searching based on any system or event variable	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to search for system outages and notices	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to setup admin duty schedules for 24x7 network administration	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to route alerts using rules to email, phones, or pagers	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to route alarms based on skill sets and domain expertise	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to configure escalation process for alerts	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to take ownership of an event through acknowledgement	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to configure an event to display operator instructions, documents, or links about how to fix the problem	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to easily locate equipment and service information through built-in asset management system	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Support for resolution tracking and configuration changes	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Support for Auto-Responders to run a program triggered by an alert	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Allow users to create threshold packages and threshold settings	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to quickly access out to content from thousands of reference manuals to help resolve technical issues quickly. Ability to leverage industry knowledge	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to effectively reduce false alarms and identify the true root causes of incidents	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported

Requirements	Vendor #1 (Type or write in name)	Vendor #2 (Type or write in name)	Vendor #3 (Type or write in name)
Real-time and Historic Reporting			
Support for viewing both historical trending of performance data and viewing performance data in real-time	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Real-time CPU performance monitoring	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Real-time memory (physical and page file) performance monitoring	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Real-time storage monitoring (local and remote mounts)	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Real-time interface performance monitoring	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Real-time installed software monitoring	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Real-time processes monitoring	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Real-time user and session monitoring	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
SNMP walk utility with built-in MIB compiler	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Application protocol distribution: Ability to see how much network traffic is consumed by various apps including Oracle, Exchange, HTTP, RealNetworks, etc. (Requires IP-NBAR, NetFlow running on our network equipment	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to view SLA data as graphs or numeric data	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to create custom SLA reports using SQL-based reporting tools (e.g. Crystal Reports)	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported
Ability to create synthetic transactions to accomplish end-to-end application response time monitoring and measurements for establishing and reporting on SLA	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported	☐ Fully supported ☐ Partially supported ☐ Not supported

Requirements	*Vendor #1* (Type or write in name)	*Vendor #2* (Type or write in name)	*Vendor #3* (Type or write in name)
Idiosyncrasies and Oddities			
Ability to create custom pollers	❑ Fully supported ❑ Partially supported ❑ Not supported	❑ Fully supported ❑ Partially supported ❑ Not supported	❑ Fully supported ❑ Partially supported ❑ Not supported
Ability to create remote custom monitoring scripts	❑ Fully supported ❑ Partially supported ❑ Not supported	❑ Fully supported ❑ Partially supported ❑ Not supported	❑ Fully supported ❑ Partially supported ❑ Not supported
Ability to build pollers in a variety of programming languages	❑ Fully supported ❑ Partially supported ❑ Not supported	❑ Fully supported ❑ Partially supported ❑ Not supported	❑ Fully supported ❑ Partially supported ❑ Not supported
Ability to create custom events that trigger custom notifications	❑ Fully supported ❑ Partially supported ❑ Not supported	❑ Fully supported ❑ Partially supported ❑ Not supported	❑ Fully supported ❑ Partially supported ❑ Not supported
Ability to build custom data collectors that are standards compliant	❑ Fully supported ❑ Partially supported ❑ Not supported	❑ Fully supported ❑ Partially supported ❑ Not supported	❑ Fully supported ❑ Partially supported ❑ Not supported