Essential IT Monitoring: Seven Priorities for Network Management

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for SolarWinds

September 2013

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Essential IT Monitoring: Seven Priorities for Network Management

Essential IT Monitoring

Fundamental to achieving effective enterprise IT management is enabling comprehensive visibility into all essential technology configurations, performance, and status. To enable a consolidated view, these monitoring practices must cross multiple management disciplines, and each organization will have unique sets of requirements that will define which disciplines align most appropriately with their business. Therefore, ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts recommend the adoption of management solutions that are modular and fully integrated, allowing each organization to select the most appropriate combination of administrative resources to establish a complete view of their distinctive support stack from a "single pane of glass."

EMA's series of *Essential IT Monitoring* white papers identifies key elements enterprises must target in particular management disciplines in order to rapidly identify and resolve issues and to optimize performance across IT infrastructures. Readers are advised to adopt integrated automated monitoring solutions that bring visibility to all the identified elements in the topic areas most applicable to their IT implementation.

Monitoring Priorities for Network Management

If applications and services are the lifeblood of today's IT-enabled enterprise, then the network is the circulatory system that connects and delivers them. Monitoring the health and performance of your network has long since passed the "nice-to-have" stage and is now considered truly mission critical. But where should you start? What are the most important aspects of network monitoring, from a practices and tools perspective?

It may help to start by considering the perceptions of networks within today's connected organizations. Systems administrators think of networks as plumbing that connects their servers and storage. Application developers think of networks as a cloud – a nebulous means to reach their end users and little more. IT end users simply know the network is what connects them to IT resources so they can do their job. The help desk knows it is a checklist item of likely sources of issues. And everyone all around, largely, thinks of the network first when something's not working.

While some will deploy monitoring simply to exonerate the network, there's a much greater opportunity at play. Because the network is the connecting fabric of IT, it is also an ideal location from which to understand the overall health and activity of the systemic whole of the IT infrastructure, including connected resources, users, and customers.

EMA conducts regular field research and dialogue with network engineering and management practitioners across organizations small and large, public and private, domestic and international. Over the years, EMA has identified a number of specific network monitoring practices that yield directly recognizable advantages and results both for network managers as well as broader IT Operations.

NETWORK MONITORING TECHNOLOGY ESSENTIALS

Most network monitoring utilizes SNMP (Simple Network Management Protocol) as a primary method for communicating between network devices and management tools. An SNMP agent is available on most every IP-based network device in the marketplace today.

The available SNMP information and commands offered by a network device is defined via a MIB (Management Information Base). Many MIBs are based on IETF standards, but many more are specific to individual equipment vendors and/or specific product types and models.

Network monitoring tools will use SNMP to receive and interpret traps (asynchronous notifications), gather state or statistical information via regular polling, and take actions on the device by setting values of certain key MIB variables.

Following is a detailed assessment of the top seven priorities that EMA advocates for best practices in network monitoring. These do not have to be addressed in the order presented, though the first is an important foundational step, which all others must follow.

Priority 1: Get the Network Under Management

Getting started is often the hardest part, but in this case it may be the easiest. In order to establish effective network monitoring, the first step is to figure out which devices comprise the network and what critical resources are connected to it and by it. You can't manage what you don't know is out there, and EMA has heard countless stories of surprises resulting from initial (or even ongoing) network discovery. Start by selecting a network monitoring product. Some are simple, and some are sophisticated, but they all allow the collection of network device information for bringing devices under management.

The most basic approach for populating your monitoring tool involves manual definition of managed devices, through the entry of IP addresses and essential security information such as SNMP community strings. Many tools also offer the ability to import device information in bulk, often from a spreadsheet or CSV file, to accelerate the process. But manual techniques will commonly leave gaps, because unknown devices will remain unknown after the population process.

A better approach is to use autodiscovery features, which will scan the network, find the devices for you, and automatically populate your monitoring tool. Getting the best out of autodiscovery does depend on conformity and consistency in SNMP community strings, so that the algorithms can properly find and include device details that you will want to monitor. If possible, it is also useful at this stage to define the topological relationships between devices. This helps during subsequent engineering and troubleshooting processes, when it is important to recognize paths across the network. Some autodiscovery algorithms will do this automatically, by examining ARP (Address Resolution Protocol), Routing, switch forwarding, and related tables via the SNMP interface, or by using discovery protocols such as LLDP (Link Layer Discovery Protocol) or CDP (Cisco Discovery Protocol).

Next, think beyond standard network devices. There are a number of critical connected resources that should also be incorporated as part of the initial monitoring push:

- Network-enabling resources, such as DNS (Domain Name Service) and AD (Active Directory) servers, as well as IP address management systems such as DHCP (Dynamic Host Control Protocol), should be defined or discovered and added. These services are critical to basic network functionality, and when any of them stop functioning properly, network and application health and performance suffers. For instance, if AD authentication is not occurring because the server is down, users will not be able to access their Exchange email.
- Network security elements such as firewalls and IDS/IPSs (Intrusion Detection/Prevention Systems) will commonly sit in-line as part of the network path.
- Critical connected application servers are important too. You want to know that those systems are up, and at the very least that their Network Interface Cards (NICs) are functioning properly, so they can access the network without problems.

Priority 2: Define Device Groupings

Once all network components have been found and brought under management, the next step is to organize the elements to be monitored. This essential step allows network monitoring teams to designate the relative importance of each component, according to specific characteristics of the organization and the managed infrastructure. Basically, the goal of this step is to link the monitored network to the organization that it connects and supports.

There are three types of grouping approaches that EMA finds to be most common and useful across settings both large and small, and using them helps to answer the what, where, and who of problem isolation and management. Following are some key types:

- ***Device Type***: Network managers most often start with views into the managed network that bring together devices by category, such as routers, switches, and access points. This approach to grouping facilitates inventory management, device administration, and general health assessments. This will often be the place to figure out precisely what is the source of a problem under investigation.
- ***Geographical***: For any organization that has more than one operating location, a geographical or site-based grouping of monitored devices is perhaps the most easily understandable way of looking at the network. This answers the question of where problems have occurred. Graphical topology map views fill this need and are often used as a primary display in the NOC (Network Operations Center) as a visual guide to operations status. It is also very helpful for quickly isolating the scope and impact of any problem.
- ***Organizational***: The most direct technique for relating network monitoring information to the connected community is to group network elements in terms of which part of the business or organization they serve. This addresses the question of who is impacted by any issue or problem. There will be a lot of overlap here, when considering core devices, but this is key to recognizing and accurately communicating with end-user and line of business communities, whether for regular status reporting or during a troubleshooting and recovery scenario.

Priority 3: Prioritized Availability Monitoring

The next step and priority is to define which devices, groups, and/or sites are to be designated as most critical to the organization. Any time one of these switches or ports is down unexpectedly, it's likely that access to important applications has been interrupted or, at best, impaired. These will be the network components that will be assigned the highest priority for sustained monitoring – when any of these elements or locations suffers an availability incident, they will receive priority attention from the operations staff.

Network availability monitoring gathers events, commonly in the form of SNMP traps or other asynchronous notifications, combined with regular "heartbeat" checks on device/component health and status, commonly via SNMP polling. Any events received or atypical test results will be translated into alerts or alarms within the network monitoring system. Those alerts and alarms are then assigned relative priority, often ranging in severity from informational to critical. Critical alerts indicate severe impairment of networking function and, usually, loss of connectivity, whereas major alerts may represent impairment but no loss of connectivity, and so on down the line. Most network management platforms include features for automatically notifying operations personnel of high priority or critical alerts, via email, text, or other means – even social media.

Prioritized availability monitoring involves setting up alert/alarm severity definitions as well as escalation processes to be used as part of every day operational monitoring. Typically, focus is put upon handling of the most critical availability issues – the ones where connectivity has been lost. But it also makes sense to set up priority notification and escalation for the most mission-critical network devices, network-enabling services, and network-connected resources. This helps operations teams recognize not only whether or not the network is operational, but also if the broader IT infrastructure and ecosystem are being served adequately.

Prioritized availability monitoring involves setting up alert/alarm severity definitions as well as escalation processes to be used as part of every day operational monitoring.

Priority 4: Add Device-level Performance Monitoring

With availability monitoring in hand, network managers can turn towards the next major set of challenges – recognizing and managing the performance of the network. The objective here is to move beyond being able to answer the question "is the network up?" and onto "is the network meeting performance and throughput expectations?" The most common mechanism for this is to expand availability-oriented SNMP polling to collect a broad range of health and activity metrics from network devices on a repeating periodic basis. That data is then archived and kept in a historical database, so that trends can be identified and normal versus abnormal activity revealed.

From a tools perspective, performance monitoring requires a scalable polling engine for gathering large volumes of metrics, together with a sufficiently high-performing database and reporting features. In large managed environments, multiple polling engines and multiple databases may be required, and will need to work in a fully integrated fashion, so that data can be pulled from all sources during reporting and analysis activities.

Based on EMA research and practitioner dialogue, following are a set of essential areas to focus upon for establishing device-level network performance monitoring:

- ***Monitoring device resources***: Collecting metrics on current levels of device resources such as CPU usage, memory usage, power levels, temperature (and more) reveals a detailed view of the operational capacity and health of each device.
- ***Monitoring ports/interfaces***: By harvesting counters such as packets, octets, discards and errors both coming into and going out of each logical and physical interface, it is possible to recognize congestion issues as well as operational viability of the many touch points that comprise the connectivity fabric.
- ***Setting performance thresholds***: Default performance alerts/alarms should be configured to watch for extreme high values in monitored metrics across all devices, such as interface utilization or device CPU exceeding 90%, and tuned more finely for critical/essential devices and resources. This provides indications to network managers that network links may be approaching saturation, before the network begins to fail.
- ***Identifying trends***: Your monitoring system should provide reports on performance metrics over time so that you can recognize trends over weeks, months, or even the past year. This provides network engineering the data necessary to accurately plan capacity, and network managers the ability to recognize changes in usage patterns or quality indicators that warrant proactive mitigation.

Priority 5: Get Change Under Control

Enemy number one, when it comes to stability and performance of the network, is unplanned change or unintended consequences of change. Consequently, an essential aspect of monitoring networks for both performance and health must include recognition of changes being made to the network or occurring within the network. For instance, a routing change can break a network path between sites, a network QoS tag could be misconfigured and starve a latency-sensitive application like VoIP of necessary priority delivery, or a firewall rule change could block access to a critical application. Having change indicators on hand can significantly accelerate both problem troubleshooting as well as remediation.

An essential aspect of monitoring networks must include recognition of changes being made to the network or occurring within the network.

There are two techniques for integrating change awareness into network monitoring. The first involves finding and capturing change indicators, and adding them into the primary monitoring platform and process. These indicators can often be found in the form of device traps or notifications (sometimes via API). Another good source is log files, where the exact change made, the time it was made, and often who made the change is captured and recorded.

The second important approach for establishing control over change is to leverage the ability of NCCM (Network Change and Configuration Management) tools to automatically scan devices, compare their configurations to expected norms, and automatically report variances. This latter approach can help reveal potential problem sources while also providing the added value of assuring policy and regulatory compliance. NCCM tools may be available as a module that works directly with your network monitoring platform, which will be easiest to integrate into monitoring practices, or may be stand-alone in nature, in which case a bit more effort will be needed to incorporate change indicators and scan results.

Priority 6: Add Application Awareness

With the network layer well in hand, being monitored for availability, performance, and change, network managers can turn their focus upon adding the crown jewel of monitoring – application awareness. The objective here is to understand exactly what is traveling over the network, from where to where, in what volumes, and at what times. This is the touch point between a network and the served organization, yielding direct insight into the applications and services that the network is entrusted and expected to deliver. It also represents one of the most direct opportunities for recognizing how individuals as well as groups utilize and gain value from the network.

EMA advocates using a mix of techniques in order to establish the broadest and richest possible application visibility.

To get started, it is essential to deploy agents, probes, or tools that can measure and report application flow activity, or harvest that data from where it already resides. A common technique is to harvest NetFlow/sFlow/JFlow/IPFIX records that are generated by network devices and that document application flows. This data can also be gathered via active, synthetic testing with features such as Cisco's IP SLA, from log files on systems and devices, or from direct inspection of packets as they traverse network links. Each approach has its strengths and its costs, and EMA advocates using a mix of techniques in order to establish the broadest and richest possible application visibility while staying within an acceptable total cost envelope.

With application-aware data incorporated into the monitoring process, measures can be taken to leverage it in a manner similar to device-based performance outlined above. Network managers will want to set thresholds so that they may be notified of unexpected spikes or high levels of activity of any individual application or any individual end-user. Unexpectedly low levels of activity may also be of interest, as it may be an indication of impaired application or transaction activity.

Most application-aware approaches will also provide some means of measuring and monitoring end-user response times, which serves as a proxy for user experience. Monitoring and setting thresholds against lengthy response times is an important technique for recognizing disruptions affecting the end-user community, whether or not they are rooted in the network. This measure alone brings network monitoring directly into the fold as part of broader cross-domain, service-oriented operations and is consistent with strategic shifts that EMA has been documenting within the IT function.

Finally, as with device-based performance monitoring, network managers should identify and tune thresholds so that alerts are raised against the most mission critical applications on a timely basis, allowing faster response and restoration when issues arise.

Priority 7: Integrate and Communicate

The full value of network monitoring cannot be fully realized without sharing and collaborating, both across the IT infrastructure team as well as beyond. Since the network is the fabric connecting IT-empowered organizations, it represents a strategic viewpoint for understanding the ebb and flow of activity and health of the IT function in the eyes of those who rely upon IT for their daily tasks and work. That viewpoint is a powerful one that when effectively shared, and can facilitate improved planning, smoother rollouts, and a better collective understanding of operations between IT and their customers.

Based upon the broad range of management systems that EMA studies and covers as well as research findings in best practices in cross-domain operations management, following are recommended focus areas for integration and sharing of information into and from the network monitoring function:

- ***Help desk and trouble ticketing***: Connecting the network monitoring system to a trouble ticketing platform, and/or directly into a help desk management system, provides a link for tracking issues as they arise, the steps that have been taken to remedy them, in the final dispensation. Time-based escalation procedures can also be automated for network issues using the features in these systems, providing a better experience for IT's customers.
- ***Systems and application monitoring***: The network connects systems to end users or to other systems, to deliver application and service traffic. By aligning network monitoring with monitoring of systems and applications, IT operations teams can correlate indicators and events to recognize dependencies and accelerate identification of root causes. This may involve another layer of management technology, to serve as a central consolidation point, or may be possible within the core network management platform, if that system has been designed to incorporate data from other domains.
- ***Security monitoring and management***: Many of the technologies and data sources used for network security monitoring are the same as those used for network operations monitoring. Issues recognized within the network may, at times, actually reflect security threats. Open sharing of activity and issues found by the network monitoring team with the security team can greatly accelerate incident assessment and remediation. As with systems and applications, this may involve forwarding of events or data to a central SEIM (Security Event and Information Management) platform, or may be an integral capability of the network monitoring system.
- ***Line of business and end users***: Finally, we cannot forget those who the network serves. Providing a means for reporting or exposing current network health, availability, and even performance status to senior executive leadership and even down to end users can be very helpful in managing expectations and proving value delivered. Essential here is the ability to focus reporting upon that portion of the infrastructure that is relevant to a user, group of users, or line of business, so that they are not overloaded with information that is not pertinent to their needs.

EMA Perspective

Many will say that network management is a mature, even mundane set of technologies and practices today. EMA research and ongoing dialogues yield evidence to the contrary – while network management techniques are widely well understood, they are often not applied in a consistent or effective manner. Sometimes this is due to growing pains – small shops that cobble together some open source with some scripts, but find that the resulting approach doesn't keep pace with the demands of monitoring a growing network. Other times, the issue is fragmentation due to organizational size, where various teams have purchased the tools they need without considering the big picture or leveraging capabilities already in house. The result of either is inefficient process, gaps in visibility, slow response to problems, and never getting ahead.

By building out network monitoring based on the practices and priorities listed here, network managers and operators can move away from frenetic, reactive operations mode and towards a more proactive, strategic position. Start by getting your network under management, by aligning and grouping network resources according to organizational priorities, and by establishing and prioritizing availability monitoring. Follow that with performance monitoring, integrated change awareness, and application awareness to achieve the highest degree of visibility and control. And finally, share the results for the greatest and most lasting synergy.

By building out network monitoring based on the practices and priorities listed here, network managers and operators can move away from frenetic, reactive operations mode and towards a more proactive, strategic position.

SolarWinds is a provider of IT management technologies that covers a broad range of the network monitoring needs discussed here. At the core is Network Performance Monitor (NPM), which provides discovery, grouping, availability monitoring, performance monitoring, and alerting. SolarWinds NPM can also solve and cover some aspects of change awareness, however Network Configuration Manager (NCM) can complete those functional needs. NetFlow Traffic Analyzer (NTA) adds application awareness capabilities and identifies which users, applications, and protocols are consuming the most bandwidth. Other SolarWinds products are able to track and accommodate monitoring of essential network-connected resources such as servers and applications, DHCP/DNS servers, virtualized infrastructure, and storage arrays. And finally, the SolarWinds solution comes with a powerful complement of dashboard and reporting features that can be readily adopted for collaborative and information sharing needs.

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to small businesses. SolarWinds' approach is consistent across all market segments – focusing exclusively on IT Pros and striving to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with simplicity through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem on any scale. Additional information on SolarWinds can be found at http://www.solarwinds.com/.

Additional Reading…

For information on optimal monitoring practices in other management disciplines, please see EMA's other white papers in the *Essential IT Monitoring* series:

Essential IT Monitoring: Five Priorities for Cross-Domain IT Management

Essential IT Monitoring: Ten Priorities for Systems Management

Essential IT Monitoring: Five Priorities for Security Management

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter or Facebook.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

2770.092513