Essential IT Monitoring: Ten Priorities for Systems Management

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

October 2013

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

Essential IT Monitoring: Ten Priorities for Systems Management

Table of Contents

Essential IT Monitoring 1

Monitoring Priorities for Systems Management 1

- Priority 1: Operating System Performance and Availability 2
- Priority 2: Server Hardware Status 2
- Priority 3: Data and Storage Availability 3
- Priority 4: Directory Services 3
- Priority 5: Patches and Updates 3
- Priority 6: Virtualization Infrastructure Performance 4
- Priority 7: Problem and Incident Alarming and Reporting 4
- Priority 8: Change Detection 5
- Priority 9: Capacity Planning 5
- Priority 10: Email Server Monitoring 5

EMA Perspective 5

About SolarWinds 6

Additional Reading… 7

Essential IT Monitoring: Ten Priorities for Systems 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 identify 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 Systems Management

The greatest challenge for IT operations is dealing with the ever-expanding complexity of IT infrastructures. In fact, each IT system is reliant on an ecosystem of interdependent hardware and software components all working in concert with each other to deliver services to the business. IT administrators must govern the provisioning, configuration, and ongoing maintenance of operating systems, patches, processes, applications, firmware and a wide variety of other systems elements, each of which is subject to its own unique set of requirements and challenges. Should one element fail, it will likely affect other system components in a domino effect that has a profound impact on the overall performance and reliability of IT service delivery.

All too often, organizations lack the essential visibility into their systems performance and configuration, resulting in inefficient and ineffective IT implementations. Without granular, real-time monitoring of the support stack, systems administrators become reactionary, spending the bulk of their time "firefighting" problems rather than supporting the business. As a consequence, systemic failures are never truly resolved, the performance of critical workloads is degraded, operational costs are increased, organizational goals are not met, and businesses are unable to effectively compete in the market.

Without granular, real-time monitoring of the support stack, systems administrators become reactionary, spending the bulk of their time "firefighting" problems rather than supporting the business.

Monitoring processes and automation are essential to enabling proactive systems management. The prompt identification of environment failures or potential failures allows administrators to resolve issues before they become impactful to the business. Additionally, monitoring facilitates the rapid identification of the root cause of problems, ending the break/fix cycle of reactive "firefighting." In this way, IT operations teams are able to affect performance improvements while actually reducing management efforts. With fewer fires to put out, administrators can focus on supporting business requirements, such as expanding existing or implementing new IT services and solutions. Additionally, data from monitoring is essential for capacity planning and resource optimization process that will substantially reduce IT costs (both CapEx and OpEx). To assist organizations with the implementation of monitoring processes, EMA has identified ten key priorities that should be included in any monitoring strategy:

Priority 1: Operating System Performance and Availability

At the core of any computing platform is its Operating System (OS). Everything runs on top of it, so, naturally, ensuring an OS is configured and performing optimally must always be a top priority for IT administrators and monitoring must be implemented on all OS platforms in the support stack (e.g. Windows, UNIX, and Linux). Monitoring processes should begin with the initial deployment of an OS, ensuring the installation was a success or identifying any errors. The ongoing availability of an OS must also be recorded and tracked by monitoring resources such as *uptime* and identifying the failover status of clustered servers. OS performance must be monitored in real-time by recording the status of system resources, including the load on CPUs, memory, and individual processes. Any system performance elements that exceed established thresholds need to be immediately reported to IT operations for prompt remediation. It is also essential to correlate OS performance with the performance of applications and other workloads. In particular, database performance issues (identified in error logs and job status reporting) can be difficult to resolve without mapping the issues to the performance of system resources (such as CPU and memory status).

Priority 2: Server Hardware Status

All devices in a support stack must also be monitored to ensure their physical hardware components are functioning optimally. Wear-and-tear from continuous use and environmental conditions can degrade a system's performance or cause it to fail outright. Catching potential hardware problems early will enable administrators to repair systems that are failing or move workloads to new systems before the issues become business impacting. Hardware components to monitor include the CPU, memory SIMMs, USB ports, and SCSI chains. Administrators should also be aware of which physical cable ports are in use and the status of any additional direct-attached devices.

Catching potential hardware problems early will enable administrators to repair systems that are failing or move workloads to new systems before the issues become business impacting.

Since the status of the operating environment can have a direct impact on hardware reliability, this too must be monitored and tracked. For instance, the status of power supplies must be identified, and any power spikes or changes in energy draw or efficiency should be recorded and alarmed. In fact, energy consumption should be tracked all along the power chain – from the grid to branch circuit boards to Power Distribution Units (PDUs) and racks – to identify any faults that could result in brown-outs or spikes that would damage delicate IT components. Similarly, temperature conditions must also be identified to ensure systems are properly cooled. This includes monitoring for data center "hot spots" and ensuring proper airflow. To further prevent systems from overheating, system fans should also be monitored to ensure they are preforming as designed.

Both hardware and environmental status monitoring can be enhanced by utilizing servers that include a service processor. A service processor is a type of embedded technology that operates independent of the primary CPU. In this way, systems can be monitored "out of band" – that is, even when they are not powered on. Although IPMI has been established as an industry standard protocol for service processors, many hardware manufacturers have introduced their own solutions (e.g. Intel vPro, Dell DRAC, HP iLO, etc.), but data from all of these can be distributed to any monitoring system via standard SNMP.

Priority 3: Data and Storage Availability

Another key pillar in systems management is ensuring the high performance and availability of storage systems. This includes monitoring disk I/O performance, disk usage, and the integrity of the file systems. Paging and swapping metrics are also important to track, especially for environments that support dynamic data management systems, such as large SQL databases. Any storage devices that include RAID technology must also be monitored and alarmed so any faulty drives can be immediately replaced to ensure uninterrupted service. Storage Area Networks (SAN) and Network-Attached Storage (NAS) also require vigilant monitoring to ensure data is being transmitted reliably between storage devices.

The increased adoption of virtual storage (i.e. the pooling of multiple physical storage devices into the appearance of a single storage unit) has created new management challenges for IT administrators. Not only does the performance of the collective data repository need to be monitored, but also that of each individual storage component, so any issues can be correlated and the root cause identified. In particular, virtual storage performance can be significantly degraded when multiple Virtual Machines (VMs) deliver their I/O streams to a hypervisor simultaneously causing them to be addressed randomly rather than sequentially (this is sometimes called the "I/O blender effect"). To identify if/when this has occurred and minimize its effects, I/O latency should be tracked and forecasted across all storage devices in an array.

Ensuring the availability of data also requires process for a backup and disaster recovery. Monitoring solutions are essential for ensuring scheduled backups have completed successfully and reporting on the location and availability of archives and replicated data.

Priority 4: Directory Services

Directory services (including Active Directory, LDAP, NIS, and DNS) provide centralized management and distribution capabilities for critical system, network, and user information that are commonly accessed by endpoints across the support stack. To ensure directory services are always accurate and up to date, all changes (adds, deletes and updates) must be tracked and reported. This includes monitoring for changes to both individual and group of users and systems. Details on change events should be tracked to add accountability to directory service management processes. These include the identification of who made the change and when it was made.

Priority 5: Patches and Updates

All server software components – including operating systems, applications, drivers, and firmware – require periodic patching and updates to new editions. These are often released to resolve performance issues, security vulnerabilities, or code bugs, and are typically provisioned by IT operations. Since it is essential to ensure that all software elements are promptly updated to ensure their security and reliability, the availability of new patches and updates must be continuously tracked and then compared against the versions currently installed on all devices in the support stack. By alarming on patches and updates that need to be installed, administrators can quickly deploy the fixes, minimizing business risks. Further, the patch deployment process itself must be monitored to assure they are successfully installed. The date and time when patches were installed should also be recorded so they can later be correlated with any system performance issues that may have resulted. This allows administrators to rollback faulty patches before they become business impacting. Centralized patch reports for all supported devices should also be generated for quick and easy proof of compliance with business and regulatory requirements.

Priority 6: Virtualization Infrastructure Performance

Virtualization continues to see increased adoption as a key enabler of cloud computing; however, the complexity of the resources necessary for enabling a virtualized environment has also radically increased management challenges. These difficulties can be broadly mitigated with the assistance of monitoring and analytics, which should be employed in support of all types of virtualization – including server virtualization, desktop virtualization, and application virtualization. Performance of each VM should be recorded in a similar way to how it would be recorded on a static server, and alerts should be activated if/when performance falls below established thresholds. However, VMs must also be mapped to physical infrastructures and to any software dependencies necessary for their operations. In this way, a failure or performance issue within a VM can be traced back to the physical component that is the root cause of the problem.

For end users, the availability of VMs on demand can lead to the temptation to provision new VMs for short-term or unnecessary projects. This can quickly lead to VM sprawl, where large numbers of VMs are provisioned, but left unused, resulting in the unnecessary allocation of processing, memory, and storage space. Sometimes errors in de-provisioning VMs can also contribute to VM sprawl if they leave behind orphaned or zombie VMs that use system resources, but are not connected to parent processes. To identify both types of redundant VMs, the usage of each VM should be continuously tracked and any that have not been utilized for an established period of time should be removed. Similarly, VMs that are over-provisioned can utilize more system resources than they actually need, so it is also important to monitor how much of the allocated resources a VM is actually using. To ensure end users are accountable for their VM consumption (and to help discourage VM sprawl) metering of VM use should be enabled so that individual organizations can be charged-back for their use.

Priority 7: Problem and Incident Alarming and Reporting

Despite all preventative measures, sometimes failures and performance errors will occur in any IT implementation. Incident management processes include the necessary procedures for detecting and responding to issues that have already occurred. The key to effective incident management is prompt identification of the failure – the faster it is identified, the faster it will be resolved. The entire support stack (including hardware, software, and virtual components) must be continuously monitored so administrators can be immediately alerted to failure events. Some critical areas to monitor include: system logs, application and script status reports, threshold breach alerts, process tables (e.g. to identify hung or zombie processes) and database error logs. To ensure administrators are not overwhelmed with requests, they should only be alerted to incidents that are business impacting.

The key to effective incident management is prompt identification of the failure – the faster it is identified, the faster it will be resolved.

Where incident management is primarily a reactive process, problem management introduces procedures for proactively resolving issues before they actually occur. This requires a deeper capability of predictive analytics that interprets the information on the current status of the IT environment and determines if there is a potential for a failure to occur. For example, correlating events and performance issues can help identify the root cause of systemic problems (e.g. a spike in disk I/O on multiple systems at the same time may correlate with a backup process or scheduled patch deployments), so administrators can implement a permanent cure, rather than just a "band-aid."

Priority 8: Change Detection

Both proactive problem management and reactive incident resolution are improved with addition of change detection. Nearly all IT failure events are caused by a change that was made to the environment (the only exception to that rule being hardware failures caused by normal wear-and-tear), so by identifying changes as they occur, failure events can be correlated to it and the root cause more rapidly identified. All configuration elements should be monitored for change – including OS kernel and system files, registry files, scripts, and applications – and records on each change event should include what was changed, when it was changed, and who implemented the change. The latter adds an element of accountability, allowing administrators to track back to who was responsible and determine why the change was made. Of course, IT operations teams do not have the time to evaluate every change event, so analytics should be in place to only alert them to changes that are impactful to the support stack.

Priority 9: Capacity Planning

In order to ensure the continuous availability of IT services to support business requirements, IT operations must proactively predict and promptly implement expansions to the capacity of IT resources. For instance, when servers regularly exceed about 80% of their capacity – in terms of CPU utilization, memory performance, and storage availability – they should be upgraded or replaced. Storage capacity should be identified by the amount of unallocated space, the amount of unused space in each partition, and the overall I/O performance of the storage device or array. Similarly, organizations that support virtualization implementations must monitor their capacity to support the existing number of VMs and the expected number of new VMs that will be provisioned. Database capacities must also be monitored by IT operations to ensure the system resources will be continuously available to support them. This includes monitoring database and log file sizes, buffer mangers, caches, and the number of active database user connections or open sessions.

Priority 10: Email Server Monitoring

Email is an essential method of communication for any modern enterprise, which is why ensuring the uninterrupted routing of email messages is also a top priority for IT operations. Email servers, such as Microsoft Exchange, must be monitored to ensure they are continuously online and functioning at peak performance. This includes monitoring to ensure all applicable protocols for outgoing mail (such as SMTP) and incoming mail (such as POP3 and IMAP) are properly functioning, and the performance of mail routing can be determined by tacking the round trip time of messages. Any mail routing failures or performance issues should be logged and correlated to determine if the cause is a common system error. Additionally, the messages themselves should be monitored to ensure they conform to enterprise policies. Any emails with inappropriate content should be blacklisted and any messages sent from a questionable source (identified by their IP address and domain names) should be blocked.

EMA Perspective

All essential systems management processes begin with monitoring. Visibility into the performance, status and configuration of IT infrastructure is the key to the prompt identification and remediation of failures and potential failures. It is also critical to making an informed decision on how best to optimize and expand IT implementations. IT operations support and management processes, in fact, are only as effective as the monitoring solutions on which they rely. With this in mind, the selection of an automated monitoring platform must be a

IT operations support and management processes, in fact, are only as effective as the monitoring solutions on which they rely.

carefully considered process. Monitoring solutions must be comprehensive enough in scope to provide the visibility necessary to achieve the breadth of business and IT requirements, including all those presented in this EMA paper. The solutions must also be centralized with a consolidated monitoring console, a single repository for logs and data, and unified reporting to enable event correlation.

As an example of a solution that delivers a comprehensive range of monitoring capabilities that are unified in a centralized view, SolarWinds offers monitoring solutions that specifically target systems management challenges. Three of its offerings, in particular, deliver key capabilities for supporting IT systems management:

- **Server & Application Monitor** – provides detailed reporting and alarming on server performance status and issue in real-time and on a wide range of heterogeneous devices. Monitored elements include operating system resources, hardware status, process tables, applications, and database performance. The consolidated reporting and view allow for events to be easily correlated and capacity issues to be promptly identified and addressed. Application monitoring extends support to custom applications, scripts, Microsoft Active Directory and Microsoft Exchange. Also included with the solution set is *AppInsight for SQL*, which enables IT administrators to visualize the status and capacity of databases, as well as to identify active user connections, storage metrics, error logs, and the status of jobs. The solution allows you to aggregate views of server and application groups by service (such as email), location, or department, making it easier to isolate where an issue is occurring. Integration with other SolarWinds products allows for the addition of more components into these business service views, including IP SLA operations, network devices, synthetic Web transactions, and virtualized infrastructure.
- **Patch Manager** – monitors for patch availability, audits desktop and servers, and deploys patches on physical and virtual endpoints. Patch compliance reporting ensures all supported devices are on the latest edition and meeting business and regulatory commitments.
- **Virtualization Manager** – currently supporting both VMware and Hyper-V server and desktop virtualization implementations, the solution monitors VM performance, tracks VM and host configurations over time, and maps virtual conditions to the physical infrastructure that supports it. The use and access to individual VMs are recorded and tracked to easily identify and eliminate those that are unnecessary or over-provisioned, reducing or eliminating VM sprawl.

All three packages (as well as many others offered by SolarWinds) are designed to be easy to use and modular, so they can be managed from a single, centralized web interface that is accessible from any networked device and includes mobile views to enable remote management on devices with smaller displays. For IT operations, the monitoring and reporting on the status and performance of systems elements (hardware, software, and virtual) is invaluable in providing the intelligence to meet service commitments. Automated monitoring platform – such as the integrated solutions offered by SolarWinds – empower administrators with the ability to deliver reliable and effective IT implementations with minimal effort and costs.

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: Seven Priorities for Network 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

2772.093013