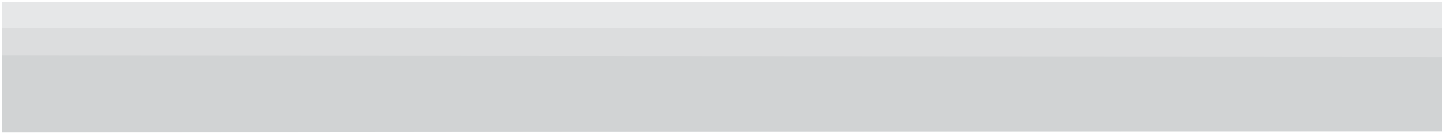


TOP 10 REQUIREMENTS FOR A NETWORK AND SYSTEMS MANAGEMENT SOLUTION

By MarketPlane Consulting Inc.



For most IT organizations, their networks and systems infrastructure have evolved into a complex, interdependent, and fast changing environment. As a result, the management tools they use to monitor infrastructure health and availability must also evolve. For example, when the rate of configuration change increases from a few times per month to several times per day, manual change processes are no longer sufficient. Moreover, device misconfigurations are the highest single cause of fault and performance events in an operations environment. With a rapidly changing and diverse infrastructure, some level of automation and intelligence and improved correlation among the different operational tasks are critical to management success.

In this document we will discuss the top 10 core and advanced functional requirements which a Network & Systems Management (NSM) solution must possess, in order to meet the management demands of today's complex network and systems infrastructure at small and mid-size businesses as well as enterprises.

I. DISCOVERY AND AUTOMATION

With the diversity and size of infrastructure typically managed by an IT organization – automated Layer 3 discovery and monitoring is a necessity and not a luxury.

Core Capabilities: Automatic discovery of device roles and identities (e.g. resolving that a discovered device is a Cisco 3500 Catalyst series switch, or a Dell PowerEdge T410 server running Windows Server 2008) using TCP and SNMP, and out-of-the-box assignment of appropriate monitors is an essential requirement. Typically a solution supporting such out-of-the-box monitoring also provides the ability to easily adjust monitor parameters to align with the management needs of a specific business environment. Without this combination of automation and flexibility, it becomes cost prohibitive for the IT organization to adapt to infrastructure changes over time.

Advanced Capabilities: This would address discovery and monitoring coverage for a broader range of devices (including offerings from smaller infrastructure vendors), support for new virtual environments (like VMware ESXi and VSphere, MS Hypervisor and Citrix Xen) and added capability for systems and application interrogation techniques using WMI, SSH and generalized SOAP/XML protocols.

II. TOPOLOGY AND DEPENDENCY MAPPING

NSM solutions need to go beyond merely identifying target devices from a seed list or in a designated network segment, to uncovering topology and interconnectivity information through combined Layer 2 and Layer 3 discovery.

Core Capabilities: NSM solutions should offer automated visibility into the network topology, mapping of device interdependencies and basic customization of map attributes. This is useful at two levels. First, it enables powerful visual representation of outages across network locations and datacenters. And secondly, it provides critical information for manually establishing rules for downstream device dependencies and related alert suppression.

Without it, operators could be flooded with downstream alerts that are a result of a root cause failure of, say, a router in a branch office. Failure of the router would make all other devices behind it inaccessible to monitoring and create their own alerts – even though those devices may be performing without issue.

Advanced Capabilities: Advanced NSM tools would combine discovered topology and mapping information with in-built technical repository of device behavior - to support the building of business rules for automated event correlation and analysis. Further, the ability to overlay higher level attributes like business groups and services on the device topology can also add new perspectives and analysis that help prioritize problem resolution.

BROAD MONITORING CAPABILITIES

The monitoring capabilities of an NSM solution need to include the ability to track both fault and performance based events through both active and passive means.

Core Capabilities: Infrastructure and technologies are diverse and a NSM solution needs to support industry standard management protocols like SNMP and WMI to collect (active) and receive (passive) management information from multi-vendor infrastructures. The solution should also have the ability to set customizable, rules based thresholds and alert occurrences on monitored parameters. For example, threshold based performance monitoring should be flexible enough to trigger alerts on a repetitive occurrence of, say, above 90% CPU utilization across 3 consecutive collection events. Beyond this level, the reasonable operation of the device may be at risk – and appropriate operations staff needs to be alerted.

Advanced Capabilities: Further broadening of monitoring capabilities with generic web services based capabilities (e.g. XML/SOAP and JMX/J2EE) for out-of-the-box or custom integration into new kinds of environments (e.g. virtualized systems and applications). Adaptive thresholding - where the NSM solution ‘learns’ from the behavior of the device or system over time, is another innovative capability that is required in especially large infrastructure environments.

IV. ROBUST EVENT MANAGEMENT AND ALERTING

Success in event management and alerting depends on how individual alerts are filtered and correlated.

Core Capabilities: Consolidated alerting across different types of devices, systems and applications and multiple types of alert phenomena (e.g. hard failure, performance alert or configuration change) in a single visual pane, simplifies the task of interrelating one occurrence to the other. The NSM solution must also be able to initiate corrective action once an operations event has ensued, via automated means or by alerting operations staff based on multiple levels of notification and escalation policies.

Advanced Capabilities: This would include the ability to set rules for alert de-duplication, correlation and analysis across a complex set of infrastructure in order to diagnose root cause events. Further, the NSM system should

be able to deliver deeper visibility into the impact of an outage on affected business units and services, so that operations staff can prioritize their problem resolution activities.

V. INTEGRATED MANAGEMENT ACROSS MULTIPLE DOMAINS

While it is impossible for a single management tool to cover every aspect of the infrastructure – coverage across multiple domains is necessary for the sake of management simplicity and correlated operational troubleshooting.

Core Capabilities: The NSM solution must be able to bring together information from multiple domains including fault, performance and configuration and change management to provide effective infrastructure visibility and control.

Availability and performance of network and systems infrastructure can be impacted by a multitude of factors. More than half of infrastructure failures and performance errors result from incorrect configuration of devices. Improper capacity planning may result in excessive load on infrastructure - over-utilizing resources (like memory, compute, storage, I/O) to a level where optimal performance is not possible. Hard failures can also occur across devices or network pathways – but with redundant network and system architectures their impact on service delivery can be minimized.

Advanced Capabilities: While managing infrastructure is critical, application-centric management is important for meeting business expectations. The NSM solution should provide visibility into application-centric flow monitoring, response and traffic data to help uncover which users, applications and conversations pairs are responsible for network congestion or degradation. Added insight into security events and log monitoring would benefit operations managers in building a comprehensive dashboard view of all performance and availability impacting events.

VI. DISTRIBUTED MANAGEMENT ARCHITECTURE

Network infrastructure and applications are distributed across corporate and branch networks, datacenter locations, remote user sites and now increasingly in external ‘cloud-based’ systems.

Core Capabilities: The NSM solution must support central and remote site monitoring with consolidated alerting and reporting to enable seamless operational response across the network, regardless of location. Operations teams should be able to drill down into real-time and historical management information for any infrastructure device or application – including initiating rapid-fire triage and troubleshooting processes such as tracking a performance anomaly through high resolution, sub-second monitoring or restoring a backup configuration on demand.

Advanced Capabilities: Advanced NSM solutions need to support intelligent monitoring at remote sites coupled with centralized administration tools. For example, monitoring units at the network edge or at a branch office could continue independent operation even during a temporary loss of network connectivity to the central management console. When connectivity is restored, the central and remote management systems would automatically sync up and fill in any data gaps. Centralized administration would allow network and systems managers to deploy, maintain

and automatically distribute monitoring services across multiple remote clients with optimal load distribution and redundancy.

VII. SCALABLE ARCHITECTURE

Scalability requirements vary from one IT organization to the next, depending on the scope of the management project. However for any mid size to large business network, a scalable NSM architecture is critical to handling the hundreds to thousands of devices, alerts and monitored metrics generated.

Core Capabilities: The NSM solution must provide the resilience and workload dispersion of distributed data collection and analysis (all the way to the network edge), thereby preventing the overload of central management hubs with data or processing jobs. The intelligent collectors and processing engines at the network edge, should be able to roll-up aggregated data to the central database for longer term historical archival and reporting.

Advanced Capabilities: Highly scalable NSM solutions that need to monitor tens of thousands of devices and applications simultaneously, would offer multi-tier architectures for enhanced scalability. These systems would support real-time data and event collection at the edge; alert and key performance metrics processing with event reporting and resolution workflows at the middle layer; and centralized rules administration and propagation, long-term data archival of metrics and organization-wide reporting at the core. By separating collection, compute, storage and reporting requirements – there are fewer opportunities for one part of the system to become a bottleneck. However, increased scalability comes at the cost of higher complexity, management overhead and consequently higher cost of ownership.

VIII. INTUITIVE, SINGLE PANE OF GLASS REPORTING

The success of an NSM solution depends to a large extent on its intuitive usability and reporting.

Core Capabilities: The NSM solution must provide single pane of glass alerting and reporting to effectively make sense of the multiple kinds of alerts and performance information generated by the infrastructure. If the operations staff has to navigate through multiple reporting interfaces to understand the impact of a single failure, it would inhibit their ability to rapidly respond to problems and assure service delivery. Multiple modes of reporting across web and mobile device access is also desirable to enable anytime, anywhere operation.

Advanced Capabilities: The NSM solution would support personalizing the reporting system for audiences such as technical users, business unit staff and senior IT management audiences. With the reporting needs of each audience being different, the NSM solution would need to present the right level of meaningful information and analytics to each group.

IX. DEPLOYMENT, MANAGEMENT AND ADMINISTRATION

The total cost of ownership of a NSM solution is largely dictated by its cost of ongoing operation - which includes cost of deployment, annual maintenance fees, and labor costs related to system administration. For complex NSM solutions, the upfront cost of acquisition may only be a small fraction of this overall cost.

Core Capabilities: Ease of deployment and management are very desirable factors in a NSM solution. Depending on infrastructure scale and complexity, the deployment project for an easy to configure and manage solution could range from less than a day for a small network to several weeks for large, multi-tier infrastructures. Complex NSM solutions that take multiple months or years to deploy – inevitably exceed budget expectations and generate poor return on investment.

Advanced Capabilities: The NSM solution would include self-monitoring and fail-over features to ensure the management system itself is not responsible for a loss in monitoring coverage. For example, proactive monitoring of internal system components would alert operations staff when archived data sizes exceed targeted levels or host server resource consumption is over-utilized.

X. INTEGRATION WITH OTHER MANAGEMENT SYSTEMS

No discussion about an NSM solution is complete without laying down the basic requirements for integration with other management systems. After all, no management tool operates in isolation and they necessarily need to fit into the overall operations environment.

Core Capabilities: The NSM solution must support the simplest type of integration, the ability to generate alerts that can be assimilated into central Help Desk architectures – and support a consolidated response. They also need to be able to export collected data and management information in compatible formats for integration into a federated CMDB (Configuration Management Database) or other external systems. The exported information could cover device inventory, configuration, health and state characteristics and associated changes over time.

Advanced Capabilities: Advanced NSM solutions would offer both north and south bound, standardized web service based interfaces for integration and coordinated action in concert with other management systems. This capability is crucial to ensure that change management events, like say the deployment of a new network device, will automatically trigger appropriate action in all linked systems from discovery, monitoring, correlation, alerting, resolution and reporting.

IN CONCLUSION

The functional requirements of NSM solutions vary from SMB to mid-size to large enterprises. Small to medium businesses may elect to focus more on ease of deployment and ease of operation, along with comprehensive, out-of-the-box infrastructure support.

Due to the complexity and size of their infrastructures, larger enterprises may focus on scalability and integration features and demand a high degree of customization flexibility to meet the needs of multiple internal stakeholder groups.

Generally speaking, the higher sophistication and advanced capabilities in each functional area are counterbalanced by their increased cost and complexity of management. While this Top 10 list is by no means meant to be exhaustive – we believe it will provide your IT organization with an effective starting point for NSM solution evaluation.

ABOUT IPSWITCH, INC.

Ipswitch develops and markets innovative IT software that is easy to learn and use. More than 100 million people worldwide use Ipswitch software to manage their networks with Ipswitch WhatsUp®, transfer files over the Internet using the market leading Ipswitch WS_FTP® Professional client and Ipswitch WS_FTP Server and communicate via Ipswitch IMail Server.

To view the Daily Network Monitor blog, visit www.dailynetworkmonitor.com.

For product and sales information, visit www.ipswitch.com.

Ipswitch values community involvement; to find out how to become involved visit icare.ipswitch.com.

For more information about network management and how Ipswitch WhatsUp Gold delivers both ease of use and comprehensive capabilities in distributed environments, please contact us at:

IPSWITCH, INC.

10 Maguire Road Suite 220

Lexington, MA 02421

Phone: (781) 676-5700

Fax: (781) 676-5710

www.ipswitch.com