Rationalizing the Multi-tool Monitoring Environment

INTRODUCTION

Over time, businesses are likely to acquire multiple, redundant tools for monitoring the availability, performance and capacity of their IT infrastructure. This proliferation of tools is a natural result of personnel turnover, persuasive software vendors, and the cumulative effect of mergers, acquisitions and divestments. Unfortunately, the proliferation of monitoring tools impairs incident response and produces inconsistent data on infrastructure availability and performance. The result is low IT service levels and reduced cost effectiveness of the tools deployed.

An alternative approach, integrating multiple tools to work together, improves results while addressing the data needs for IT service management. Benefits include improved performance, easier operation and systems maintenance, and significantly lower capital investments and operating costs.

RATIONALIZING THE MULTIPLE-TOOL ENVIRONMENT

The rationalized multi-tool approach requires an architecture and integration strategy for the simultaneous use of multiple tools. Monitoring tools are assigned different functional responsibilities, or "levels" as illustrated in the diagram below.

Level 1 tools monitor the availability of applications and infrastructure components and respond to failures. Level 1 monitoring can be accomplished by open source tools like Nagios or Mon, or with inexpensive availability management software. Well-designed framework solutions adopt a similar approach using their console functions to manage Level 1 failure alarms.

Level 2 tools proactively warn of impending failures and the need for situational maintenance, and they specify the data to collect for capacity management. Level 2 tools may also perform configuration/asset management and software distribution tasks for the components they manage.

To implement the rationalized multi-tool approach, a single Level 1 tool is deployed across the entire infrastructure. Where segments of the infrastructure are operationally separated, a Level 1 system is provided for each segment. As a result, each infrastructure component, whether hardware or software is monitored by the Level 1 monitoring tool and by a Level 2 tool.

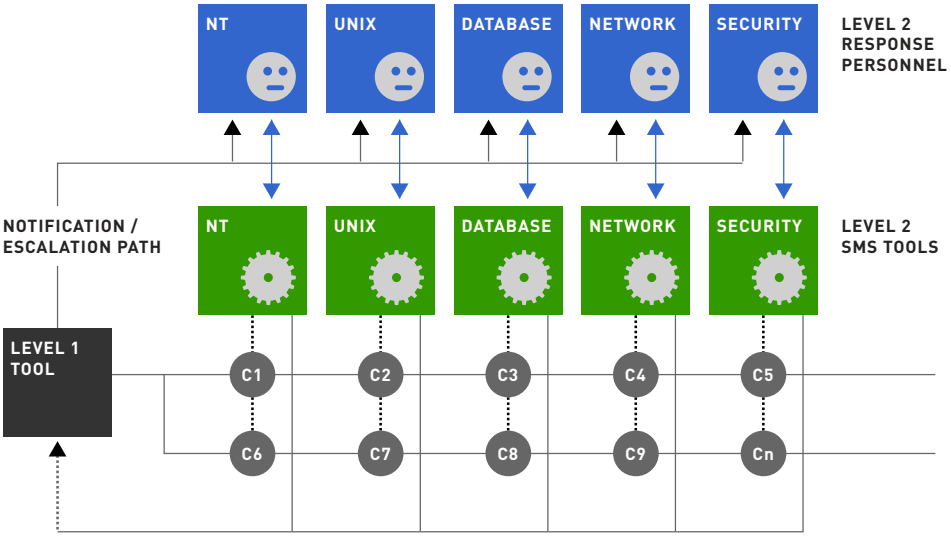

Figure 1: Message path for high priority alarms

Level 1 monitoring system functions:

1. Availability (up/down) monitors for each router, switch, load balancer, link, firewall, and server, including high priority incidents received from Level 2 monitoring systems
2. Service level monitors using synthetic transactions to directly measure the availability of mission critical applications
3. Availability dashboards containing live displays of infrastructure availability status
4. Live interfaces to customers' service level dashboards
5. Notification and escalation via pager, email or via ticketing system interface
6. Reports on availability and performance of all components and mission critical applications

Level 2 monitoring system functions:

1. Proactive monitoring, providing warning of impending failure. Examples are file system capacity monitors, log file monitors, etc. Notifications for these alarms are generally made either by email or directly through a ticketing system.
2. Transmission of high priority alarms to the Level 1 system for management via SNMP, HTTPS, HTML, etc. via the alarm bus
3. System management functions, including patch application, software distribution, and configuration/asset management for the resources being managed.
4. Distribution of configuration data to subscribing applications such as service desk, asset control, problem management, etc.
5. Measurements for use in both performance tuning and capacity planning

The multi-tool approach is both flexible and scalable. Managers of each technology silo can choose the best tool for the management of that silo based on the knowledge and experience of their team. For organizations that separate the responsibility for measuring availability from managing it, the Level 1 and Level 2 tools become the responsibility of the organizations that use their output. This is sometimes seen in large enterprises equipped with NOCs.

The architecture scales across global multi-tiered IT organizations, but may also be deployed across small networks. For smaller implementations, a single tool can address both Level 1 and 2 requirements. Because Level 1 tools are lightweight, it is easy to deploy them in multiple environments while using a top-level version to monitor cumulative lower level data and system-wide status.

WHY NOT FRAMEWORK SOLUTIONS?

A common solution to the problem of accumulated monitoring tools is to replace them with a single enterprise-class product deployed across all platforms and technologies. These products are commonly referred to as "framework" solutions, and include HP Open View, BMC Patrol, CA Unicenter and IBM Tivoli. They typically offer comprehensive monitoring and system management, including software distribution, configuration/asset management and application management across a wide variety of hardware and software platforms.

Drawbacks of the framework solutions are well understood. First, they are expensive to acquire and install. License fees can run into millions of dollars, and installation consulting costs often exceed license fees. Second, because of their multi-platform reach and functionality, they may not provide the best capability for a specific platform or technology. Often, the best tool for a particular platform or technology is the one provided by its vendor, such as Cisco Works for Cisco equipment, Enterprise Manager for Oracle applications or Insight Manager for Compaq.

Third, the tools replaced by the framework solution have often been subject to substantial customization, scripting and calibration that are wasted when the new tool is deployed. This can result in resistance from individual IT teams and significant unexpected costs. Finally, framework solutions often are complex and difficult to configure and use. IT departments typically must use senior personnel and/or specialist consultants to install and maintain them. Often the resources maintaining the infrastructure become disconnected from the people maintaining the tools. This can lead to further tools proliferation and frustration, increased training costs, and disempowerment of technical teams.

INTEGRATION WITH IT SERVICE MANAGEMENT

The rationalized multi-tool approach integrates easily with IT service management processes, as described below:

Incident management
Alarms requiring immediate action to resolve an incident and restore service are processed by the Level 1 system, which provides support for the notification and escalation process. When high priority alarms are generated within the Level 2 systems, they are passed via standard messaging formats to the Level 1 system. (SNMP, SMTP, HTTPS, and SMTP are all used as messaging formats. SOAP could also be used.) This avoids duplication of notification and escalation functions among the multiple monitoring systems and permits management and availability data to be collected from a single source.

Using simple and reliable monitors, the Level 1 tool displays the live status of all components critical to system-wide availability. Access to this consolidated "dashboard" view for help desk, NOC, and remote support personnel speeds problem diagnosis, resolution, and restoration of service during incidents. Such access also enables proactive help desk activities and reduces the number and length of help desk calls about an incident.

Service level management
End user service levels include availability and performance of applications as well as access to, and responsiveness of, help desk support. Synthetic transactions hosted by the Level 1 system directly measure the availability and performance of all applications. Measurements of service levels made in this unambiguous way are understandable to IT customers and serve to minimize the complexity of the monitoring system. Otherwise, service level measurements must be based upon calculations derived from a complex network of individual component measurements.

Availability management
All direct measures of availability, whether of hardware or software components or entire applications, are concentrated in the Level 1 monitoring system. This allows a single reporting system to generate all of the reports and trend analyses needed for availability management. The process proactively determines where to concentrate resources to cost-effectively improve availability and related service levels.

Security management
The discussion of security management is beyond the scope of this paper. However, there are many specific relationships between the monitoring systems and the basic elements of security management, including perimeter and access control, host hardening, intrusion detection and response, and related social engineering processes.

Capacity management
Capacity management involves performance tuning of servers and network infrastructure and planning for future additions to capacity. Performance tuning is best performed using the Level 2 tools, which are well adapted for this use. Capacity planning should be based upon input from synthetic transactions, web analytics if applicable, and utilization parameters collected by the Level 2 tools. A separate off-line tool should be used to store and model this information.

Configuration management
In the rationalized multi-tool approach, configuration data resides in the Level 2 tools, which can be queried whenever the data are needed. This is often the only practical way to automatically access configuration data and keep it up to date.

Using a single platform tool for configuration management requires continuous manual updating of configuration information and almost never works. The use of multiple vendor-specific tools typically automates the collection and storage of configuration data at the source level. Configuration data required for other processes can be published and subscribed to as needed.

The multi-tool approach makes it possible to integrate existing tools and common technologies to create a configuration database, which can provide and manage configuration data for backup, asset management and provisioning. Such a database can result in significant labor savings, particularly if the environment includes 100+ plus systems and is sufficiently standardized.

COST OF THE MULTI-TOOL APPROACH

In most environments, the cost of a rationalized multi-tool approach will be 25%-50% of the cost of a framework tool, potentially less using open source tools. System, networking and database vendors' standard management products for Level 2 functions are typically free or relatively inexpensive. Nagios, an open source tool, provides the necessary functionality for the Level 1 tool. Because virtually all monitoring tools are configured to communicate via standard protocols with the consoles of other tools, establishing and maintaining tool integration is in most cases straightforward and low cost.

IMPLEMENTATION

The following implementation steps to deploy the rationalized multi-tool monitoring approach will work in most environments:

Step 1
Clearly define the IT service management business processes of the host organization and specify processes to be served by Level 1 and 2 systems.

Step 2
Deploy the Level 1 tool, including infrastructure failure alarms, simple event correlation, escalation and notification processes, availability and responsiveness reports, and IT dashboards. If needed, integrate the Level 1 tool with the online ticketing system.

Step 3
Working with one Level 2 tool at a time, use the alarm message delivery method that is appropriate and select the Level 2 alarms that will be passed to the Level 1 system, if any. Incorporate these alarms into the Level 1 alarm displays, reports, and dashboards.

Step 4
Install any needed synthetic transactions. Integrate the Level 1 and 2 tools with the Service Desk system. Deploy the IT service management dashboard. Configure all necessary reports.

CONCLUSION

The rationalized multi-tool approach is flexible, scalable and cost effective. It provides the necessary input to the IT service management business processes. It preserves prior investments in monitoring tools, empowers technologists to select the best tools with which to do their jobs, and enhances effective response to incidents. Best of all, IT managers will find that easy to maintain open source or low cost tools will achieve the integration required at a fraction of the cost of framework solutions.

ABOUT GROUNDWORK

GroundWork Open Source Solutions, Inc. provides open source-based IT infrastructure management solutions such as network and systems monitoring, service desk management and IT dashboards. GroundWork's solutions enable IT management to leverage the flexibility and low cost of open source tools to achieve enterprise-level availability, performance and operational efficiency for a fraction of the cost of commercial software.

Contact us
510.899.7700
www.itgroundwork.com
info@itgroundwork.com

GroundWork
Open Source Solutions, Inc.
2200 Powell Street, Suite 350
Emeryville, CA 94608