Seven Priorities for Integrated Network Management

How HP Intelligent Management Center Delivers an Enterprise-class Solution

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Hewlett-Packard

March 2011

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

Seven Priorities for Integrated Network Management

How HP Intelligent Management Center Delivers an Enterprise-class Solution

Table of Contents

Seven Priorities for Integrated Network Management

How HP Intelligent Management Center Delivers an Enterprise-class Solution

Executive Summary

Given the constant pace of change in infrastructures, IT Operations must be forever on their toes when it comes to ensuring that the best management tools, technologies and practices are being followed. Nowhere is this more true than in the network layer, given that networks are becoming increasingly critical as the means of delivering the applications and services upon which IT end users, and the businesses and organizations they drive, so heavily depend. The time has never been better for evaluating current management strategies and considering the efficiency and effectiveness improvements possible through integrated, multi-function, multi-vendor network management solutions. This ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) white paper examines seven core network management requirements deserving of special attention in today's operating environments, and evaluates how one multi-vendor, multi-function, integrated management solution, HP's Intelligent Management Center, measures up.

Introduction

The relentless pace of change in IT, due to growth and innovation, combined with the resulting complexity in delivery infrastructures, has pushed the network into an increasingly critical role within businesses and organizations of all sizes. In order to assure that planning and operations priorities are in tune with the needs of the business, service-oriented management practices are also gaining importance across all IT domains. And coupled with all of this, management and operations resources never seem to grow as fast as the demand upon them, largely due to the common perception of these functions as elements of cost centers which need to continually be squeezed. As a result, network managers need the best possible tools at hand for managing the network infrastructure and assuring that it will play its essential part in supporting the organization in a reliable, predictable, efficient and cost-effective manner.

Network managers need the best possible tools at hand for assuring the network can play it's essential role.

This new world order for network managers requires that network management tools and technologies adequately support their needs. In particular, there are several categories of requirements that emerge as the most dominant areas for product assessment and evaluation. Firstly, products must show an ability to scale from small initial deployments to enterprise-class, easily and seamlessly. Second, products must be flexible so they can be adapted to the specific needs of any particular organization and readily accommodate the introduction of new technologies into the managed environment. Third, tools must possess a means for organizing data and offering workflow that is oriented to the services ultimately being provided to the supported organization. Along the way, automation should be available to be applied whenever and wherever possible, clear and efficient capabilities for supporting collaboration must exist, and there should be integral capabilities for monitoring and managing the security aspects of operations alongside functional assurance. And lastly, solutions that offer such scope of capabilities in a single, multi-function, tightly integrated manner will typically represent the best options in terms of total cost of ownership.

This EMA white paper focuses on a refreshed review of these major requirements for network management solutions in the face of today's challenges. Further, it assesses Hewlett-Packard's Intelligent Management Center network management solution and the degree to which it fulfills these major categories of requirements.

Emerging Network Management Requirements

As with all things, priorities and requirements for network management solutions change and evolve, just as the managed environment continues to change and evolve. As a result, all network management and operations professionals should keep a continuous watch on how the changes they are experiencing affect the needs they in turn have for their network management tools and technologies. Following are seven major areas that EMA recommends practitioners keep in mind:

1. **Scalability**: The vast majority of managed environments are growing, and increasingly greater numbers of IP-enabled elements are being added to the mix. The move towards virtualization within all portions of the IT infrastructure also contributes to a growing number of elements to bring under management. Network management tools must be able to keep up, bringing rich functionality for small environments that can scale gracefully upwards to enterprise class with a minimum of difficulty or disruption.

2. **Flexibility**: Good, high-value network management tools are "future-proof," meaning that they support multiple vendors, multiple functions, and are kept current with the latest in technological innovations within the managed environment. They must also be easy to adapt to handle new managed elements and infrastructures, preferably through configuration rather than customization.

3. **Service orientation**: As IT organizations strive to become more strategic to the business, it's essential that the tools and technologies in use support service awareness. In the case of network management tools this means organizing and presenting information according to business organization and structure, and if possible adding application awareness from the network to show the direct linkage between infrastructure and the value it delivers end users, partners and customers.

4. **Automation**: The only way to keep up with the rate of change occurring in today's managed environments is to leverage automation in any and every way possible. Examples should include automated discovery, event correlation, root-cause analysis, guided workflows and configuration policy auditing, at a minimum.

5. **Collaboration**: Even the best management tools fall short of their true potential if the data they collect and the information they present cannot be easily shared with peers and served constituencies. To do this well, solutions must have flexible, graphically rich consoles and reports that can be rapidly distributed as a basis for effective communications as well as open APIs for automated data sharing and action invocation.

6. **Security**: Increasingly, operations teams are recognizing the fact that all management tasks and activities must adhere to the same security requirements as the applications being managed. Further, the network viewpoint offers the opportunity to deliver network and application security functions in parallel with operational management priorities. Important in this area are features such as partitioned access, policy audits and alerts about observed potential threats.

7. **Cost Efficiency**: With most IT operations functions classified as "cost centers," constant attention must be paid to ensuring that management tools and technology investments deliver the best bang for the buck. This means finding management tools that deliver multiple functions covering as much of the managed environment as possible within a single system solution, eliminating multiple learning curves, multiple administrative loads, and multiple vendor relationships.

Meeting all of these requirements consistently across multiple management functional areas – fault/availability, performance, configuration and security – can be daunting. Two common approaches for solving this puzzle are to embrace a single solution vendor with a suite of products that offers vendor-supported integration, or to purchase tools on a mixed, best-of-breed basis and take on the onerous task of integration internally. A third approach is to seek integrated multi-function solutions that meet these requirements across multiple functional areas within a single product.

Intelligent Management Center – Aligned to Today's Network Management Requirements

Hewlett-Packard has been a supplier of management technology and products for many years. One of the more recent additions to their portfolio of offerings for network managers is Intelligent Management Center (IMC), which comes to the HP family by virtue of the acquisition of 3Com Networks in 2010. IMC has been in use in live production for years, and thus represents a mature, fielded technology that has evolved and improved over time. Although its roots are technologies developed for managing 3Com network gear, IMC was long ago placed on a trajectory to play a broader role for network managers and operators.

HP's IMC solution is designed to support all of the major network management functional areas.

The IMC solution is designed to support all of the major network management functional areas: Fault/Availability management, Configuration management, Performance management, and Security management. IMC has evolved over time to support virtually all network technologies in use today along with sophisticated operator interfaces, reporting and service-oriented task optimization. Following is an assessment of how IMC meets and addresses the six categories of emerging network management requirements outlined above, combined with comments from EMA's conversations with two IMC customers who have put the solution into practice.

Scalability

From a raw capacity perspective, IMC is designed to handle very large environments, up to tens of thousands of managed nodes, by means of a hierarchical and/or distributed mode of deployment. But it can also scale down to an entry point of a single IMC server, which is perfect for a couple hundred up to a few thousand elements. Scalability is enhanced by virtue of an internal common information bus architecture, which all functions and modules share, separated from the rest of the platform services. The IMC solution is also designed to handle large numbers of operators, supporting up to 50 concurrently, with access and functions defined to a highly granular degree by role, group or individual. This allows multiple teams and operators sitting in geographically diverse locations to share the same operational viewpoints and intelligence.

EMA discussed an IMC deployment with a large international service provider who pushed the envelope in terms of scale. The provider was using IMC to manage one of the largest public banks in South America, covering WAN routers

across an impressive 12000 branch sites. The same system was used to monitor and manage LAN equipment down to the port level at 30% of those sites, and the operator reported that the system had scaled to this level easily and gracefully, leaving them confident of the system's ability to support any potential future growth.

Flexibility

There are a number of discrete qualities to consider regarding the flexibility of the IMC solution. From a span of managed technologies, IMC currently boasts support for over 2600 specific devices from over 35 different manufacturers, including over 1000 products and models from Cisco Systems. New devices are added regularly to the library, and operators can add their own at any time via a MIB manager and Device Modeler. Management data can be gathered in a variety of ways – most is harvested via SNMP polling, but syslog is also supported, as are flow records (NetFlow, sFlow, NetStream, etc.) via an add-on module.

The IMC system is designed to support all networking technologies and architectures currently in common use, from traditional Layer 3 topologies to VLANs, wireless access layers, and mixed physical/virtualized infrastructures. This information can be presented graphically via table, logical topology maps, overlay maps, or in a physical view (site/location/room/rack, down to the interface level). Also included is support for discovery and mapping of virtual switch connectivity to represent intra-host connectivity between virtual server machines (VMs) on a common host/hypervisor.

Another aspect of flexibility is the means by which management information is presented and navigated – and here the key is consistent ease of navigation for intuitive workflows and peak operator efficiency. Throughout the system, IMC presents instance and status information using a common color-coded scheme and standard navigational techniques for drilldowns into any device or element representation – right click for management options and left click for hyperlinked performance information. This approach can be used to access, for instance, element configuration details, recent alarms, performance status, or configurable common Essential Actions.

The IMC system is designed to support all networking technologies and architectures currently in common use.

Finally, under the heading of flexibility, IMC offers a mature set of administrative tools that ease management of large numbers of devices and technology features, effectively reducing overhead operational workload. Examples include the Configuration Center, ACL Management, VLAN Management, QoS Manager and Security Control Center. All of these represent unified resource and configuration management functions that have been standardized across all supported element and device types, so that tasks which must span multiple touch points across the managed infrastructure can be effected quickly and efficiently through consistent representations within common integrated consoles and displays.

Service Orientation

IMC implements and delivers service orientation for network managers in three key ways. First off, the system is designed throughout to allow logical grouping of managed elements according to organizational and/or geographical structures. This is the most natural form of service orientation, allowing network managers and operators to recognize how a particular portion of the network is behaving relative to those parts of the supported organization using it.

The second element of service orientation is the inclusion of application awareness from the network perspective. IMC implements this capability by means of supporting flow data records such as NetFlow, sFlow and NetStream, displaying traffic flows across the network at Layer3/4. The Network Traffic Analysis (NTA) add-on module reveals precisely how the organization is using the network on an application-by-application, service-by-service basis with ability to correlate source IP to users. An example of the types of data available through this module is shown in Figure 1. Besides revealing actual usage activity, the NTA module allows rule-based and policy-based analysis to complement other fault, availability and performance viewpoints.

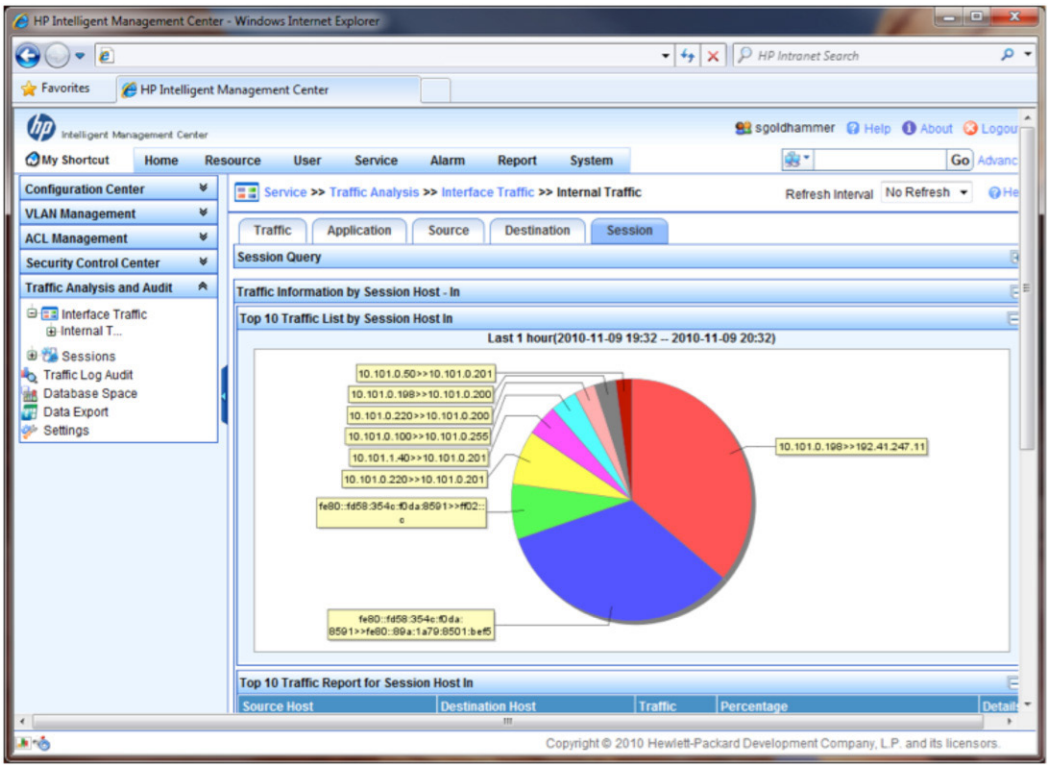

Figure 1: Service-oriented information is available via the Network Traffic Analysis module.

IMC includes a number of specific service-oriented functionality areas. For instance, the Wireless Services Manager brings together all of the technology elements and viewpoints required to understand the health and status of wireless services within the network for unified wireless and wired management. Similarly, the IPSec VPN manager provides the same capability for secure virtual networks. And lastly, the SLA manager leverages HP NQA synthetic test measurements as well as those available via Cisco Systems' equivalent technology.

The service-oriented capabilities were of particular interest to the South American service provider, allowing them to monitor the bank's network using thresholds and policies that support their Service Level Agreements (SLAs) for performance and uptime.

Automation

The IMC system leverages automation techniques in many ways. Firstly, the initial step of implementing any management tool is to populate it with the elements and devices that will be managed. IMC offers autodiscovery capabilities that take advantage of segment-by-segment discoveries and templates for specifying default management and monitoring policies. Topology views are automatically created based on the results of discovery, or connectivity can be manually instantiated and the system will automatically discover and populate data related to that connection. Incremental auto discoveries can also be run to keep up with the inevitable moves, adds and changes, which are particularly frequent when dealing with virtualized server environments. Following discovery and instantiation within IMC, each managed device and element automatically has a set of default monitors and thresholds applied so that basic health is immediately under watch.

Another common form of automation that is fully supported within IMC is Root Cause Analysis (RCA). IMC provides topology-based failure isolation as well as event correlation and de-duplication so operators can focus on the likely sources of issues and not be distracted by the symptoms. Further, IMC offers configurable auto-escalation rules so that issues and alarms of the greatest impact and importance are accorded appropriate priority attention.

Another aspect of automation supported by IMC relates to management of device configurations. Policy audits can be run to compare configurations before and after changes and make sure that compliance has been maintained. Differential findings are presented to operators in an intuitive side-by-side manner. Batch operations and tasks are also supported, such as mass device policy or password updates, or implementation and enforcement of energy savings policies.

IMC offers automation capabilities including in discovery, root cause analysis, and configuration policy audits.

Collaboration

By virtue of its maturity and long-fielded status, the IMC solution has benefited from many cycles of feedback and tuning for operator interface and reporting functions. From a dashboard perspective, IMC developers have adopted a widget-based "home page" approach so that operators can easily assemble informational views that they find most effective, either as a daily starting point or on the fly while investigating a particular problem. Primary navigation is organized by Resources, Users, and Services, three common starting points for best practices monitoring and troubleshooting, as well as Alarms, Reports, and System, three of the most common task areas. Each device under management offers a rich detailed information page including configuration details, current status, current performance and current alarms. All console views make heavy use of hyperlinks for additional detailed drilldowns, and access can be defined on a highly granular level so that individual operators can be restricted to view only that for which they are responsible. An example IMC dashboard is shown in Figure 2.

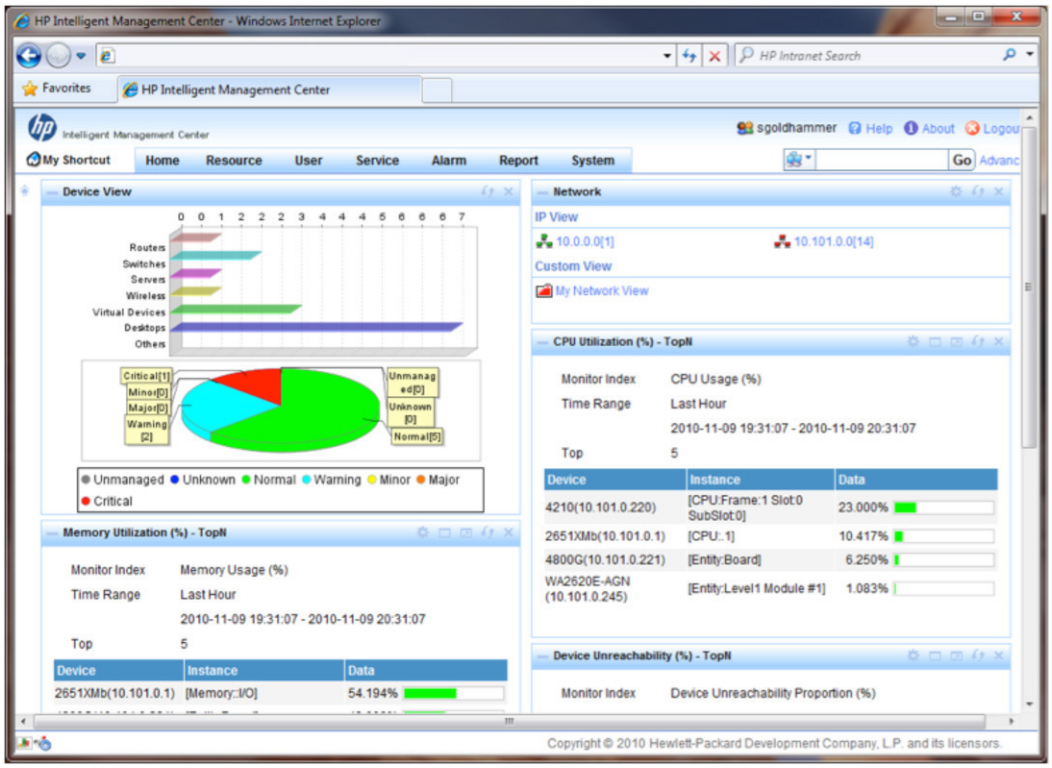

Figure 2: IMC widget-based home page dashboard.

A senior network engineer using IMC to manage thousands of HP, Cisco and BlueCoat network devices has found this consistent representation to be particularly valuable. "First thing in the morning, I can glance at the dashboard and see where the issues are right away," he said, adding "and the ability to filter events allows me to concentrate on what is most important to me rather than having to sift through all of the informational alarms."

The other primary aspect of collaboration revolves around flexibility and distribution of reports. IMC offers an extensive library of over 50 pre-existing report templates, which can be run on a regularly scheduled or *ad hoc* basis. Additional options allow operators to define and configure their own reports. Results can be formatted in PDF for distribution or delivered in CSV format for use with other tools such as Excel or Crystal Reports.

Security

The IMC solution supports integrated network security management in two primary ways – via integral controls within the core product, and by means of the Endpoint Admission Defense (EAD) add-on module. Intrinsic security-oriented features include the Security Control Center, which looks at log messages and identifies potential real-time attacks, combined with the capability to take predefined policy-based actions. Another highly useful capability is the User Behavior Audit, which can pull information on who is active on the network and correlate that with access information, traffic and data obtained through the EAD module to provide an aggregated understanding of an individual's activities.

The EAD module brings with it advanced management tools for understanding and controlling access to your network and network-attached resources. The module offers full Network Access Control (NAC) features, including registry control, password control, patch level enforcement, traffic policies and control, terminal security, sharing controls, time checks, firewall controls, and more. EAD can gather deep asset information (including complete Desktop asset discovery) and provide several data theft prevention capabilities, such as the ability to monitor or block USB/CD-ROM access, data sent to printers, and changes to desktop assets such as hard disk partitions, CPU and memory. It can also integrate with LDAP and Active Directory services, providing a comprehensive yet efficient means of user access management within the network management platform.

Finally, IMC offers integration with HP's (nee 3Com's) TippingPoint Intrusion Prevention System (IPS). TippingPoint IPSs are shown in IMC topology maps when present, and the traps and log messages they generate are brought into IMC together with other management feeds. This becomes particularly useful for monitoring, tuning and balancing potentially conflicting functions, such as NAC and IPS, and allows operators overseeing both to make quarantine decisions from the IMC level.

Cost Effectiveness

The substantial scope of capabilities offered within the IMC system is further accentuated by the fact that the vast majority of them are delivered with a single integrated software product. The multi-vendor, multi-function architecture offers the best possible approach to minimal total cost of ownership for network management tools, by reducing the number of management tools required to get the job done. This translates into fewer systems to administer, fewer vendors to manage, and less training required on multiple, disparate user interfaces. Besides these savings in overhead costs, management tools consolidation eliminates multiple representations of the same managed elements, simplifying all manners of day-to-day tasks for monitoring, troubleshooting, configuring and securing the network infrastructure.

The integrated approach offered via IMC system represents the best means to minimize total cost of ownership.

This aspect of the IMC solution was especially important to the senior network engineer. "The integration of multi-vendor configuration management into the same solution we use for monitoring is very important," he said. "We won't be scaling up staff as fast as we are scaling up the network, so we plan to leverage IMC and its automated features as much as possible."

Based on industry case examples where multiple tools are replaced with singular, multi-function, multi-vendor integrated management platforms, operational cost savings can be dramatic. Some IT shops have reported dramatic reductions in administrative resource requirements, often halving staffing needs. Additionally, savings based on eliminating redundant support and maintenance contracts alone often pays back the investment in the new system in short order – in some cases in as little as 12-18 months.

EMA Perspective

With the rate of change in today's managed environments, network managers clearly need all the help they can get from their network management products. EMA strongly advocates that long-term goals of service-oriented management also be accorded a high priority when reviewing any management tools or technologies, including both intrinsic capabilities for aligning network management practices with the business, as well as means for connecting network management viewpoints and processes with other related IT constituencies.

Given the successful history and maturity of HP's IMC solution, it is not surprising to see that it covers the vast majority of current network management requirements, as detailed in this analysis. IMC has been designed to address comprehensive network management needs for environments with mixed technologies and device vendors. As a result, it represents a viable alternative to element-centric network management packages offered by network equipment manufacturers, while also comparing favorably to third party independent platform and suite solutions. IMC can also be considered complementary to the broader HP Software suite of solutions, which are designed to address global enterprise and service provider management needs through advanced, high-end modular offerings such as HP Network Node Manager and HP Network Automation.

In summary, HP's IMC solution represents a mature, integrated approach for managing complex, multi-vendor, heavily virtualized infrastructures across multiple functional areas. IMC's integral support for security management sets it apart from the many others in the marketplace, as does its approach to covering the vast majority of management tasks within a single product. The resulting solution means shorter learning curves, less administrative headaches, and better data leverage, culminating in total cost of ownership advantages.

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 IT professionals, lines of business users, and IT vendors at www.enterprisemanagement.com or follow EMA on Twitter.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

2239.032811