

Seven Best Practices for Network Management

How HP Intelligent Management Center Supports Effective Planning and Operations

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

January 2013



IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Seven Best Practices for Network Management

How HP Intelligent Management Center Supports Effective Planning and Operations

Table of Contents

Executive Summary 1

Introduction 1

Best Practices in Network Management..... 1

 Best Practice #1: Integrating Management Functions 2

 Best Practice #2: True Multi-Vendor Support..... 2

 Best Practice #3: Integrated Management of Virtual Networks & Cloud Resources 3

 Best Practice #4: Automate, Automate, Automate..... 3

 Best Practice #5: Unified Policy Management 4

 Best Practice #6: Proactive Operations Monitoring..... 4

 Best Practice #7: Communicate, Communicate, Communicate 5

HP Intelligent Management Center 5

EMA Perspective..... 6

About HP 7



Seven Best Practices for Network Management

How HP Intelligent Management Center Supports Effective Planning and Operations

Executive Summary

With networking becoming an increasingly critical component of IT infrastructure for connecting physical, virtual and cloud-based resources with users/customers, networking planning, engineering, and operations pros need to raise their game. This includes recognizing how to evolve network management best practices and how network management tools can be best deployed to help improve operational efficiency, communicate within and outside operations teams, reduce operating risks and ensure optimal resilience. This ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) white paper examines seven areas currently challenging network managers and the best practices that are emerging as a result, and further assesses how the Intelligent Management Center solution from HP (Hewlett-Packard) aligns with those practices to enable success.

Introduction

Within the realm of network management, there are many tasks, needs, and challenges facing network planning and operations professionals. While the technologies within the network are relatively mature and stable, the loads on the network are anything but. As a result, there is a constant pressure applied by the rest of the IT organization, as well as the end-user community, to make the network 100% available and 100% high-performing. While network architectures and networking products will take care of most of this challenge, management tools, technologies, and practices are essential for filling the gaps, pulling the pieces together, and making it possible to make the shift from reactive to proactive.

The network is just one piece of the IT environment, albeit the most ubiquitous one. Very little can function within a modern IT infrastructure without the services of the network. But since IT is a broad and complex entity, the total scope of IT management objectives goes far beyond simply those focused on network resilience. As a result, network management practices (and the tools that support them) must align and connect with broad IT management systems, processes, and initiatives.

Network management practices must align and connect with broad IT management systems, processes, and initiatives.

For the purposes of this paper, network management product solutions are meant to include features and functionality that support the entire lifecycle of networking technologies. Common terms for these systems include configuration management, fault/availability management, performance management, and troubleshooting. The disciplines they serve are typically known as network engineering, network planning, network management, and network operations. Further, while most organizations still maintain a dedicated network management function, an increasing number of management systems deployments are being applied towards and utilized by service-centric, cross-domain operations teams.

Best Practices in Network Management

Most networking pros will always strive to do the best job that they can. This means working with the tools and technologies they are given, understanding their role in the bigger picture as best possible, and doing whatever it takes to make sure the network is working. Best practices come to play as a means for helping networking pros put their everyday work tasks into perspective versus the specific demands of the organization they support as well as the experiences of their peers in other organizations.

Seven Best Practices for Network Management

How HP Intelligent Management Center Supports Effective Planning and Operations

It's worth considering here whether or not network managers are responsible for more than just a network. In many cases, it is helpful to understand and even to have management data around that which the network connects/delivers, and not just the network itself. Some organizations will even have cross-domain operations teams in place that (by definition) are responsible for the IT infrastructure as a whole, including networks, servers, storage, and sometimes even end-user devices. For the purposes of this analysis, the focus is placed on best practices for managing networks, with note given to points where going beyond that viewpoint is most helpful.

Following are seven categories of best practices evidenced by EMA research and dialogues with networking practitioners from organizations of all types and sizes. In particular, research projects focused on network management megatrends, management of virtualized network environments, management of mixed public/private cloud environments, and management of converged services (such as VoIP, videoconferencing, and VDI) have informed this analysis, as have countless individual interviews and inquiries. This research has been primarily focused on network management; however, it is also influenced by studies that look at networking as a part of the broader IT whole.

Best Practice #1: Integrating Management Functions

While many day-to-day tasks and actions may seem simple, virtually any change or analysis process connects directly or indirectly to other tasks and functions. For instance, adding new devices or defining new interfaces on a device means that new components or elements are brought into existence that should be monitored and managed for availability and performance. Consequently, the best levels of management awareness and control exist when management tools used for various management functions are integrated, and when management tasks and processes are conducted in a way that recognizes and addresses the interrelated nature and impact of change.

The best levels of management awareness and control exist when management tools used for various management functions are integrated.

Essential objectives within this practice include coordination and continuity of workflows across functional categories, including configuration management, fault/availability monitoring, performance monitoring, and troubleshooting, resulting in improved accuracy and efficiency. From a management tools perspective, this either requires close integration and sharing of data between tools, so that handoffs from one to another are seamless and accurate, or a unified management system that supports multiple functions of a single core database and/or management data model.

Best Practice #2: True Multi-Vendor Support

Few network managers have the luxury of working with a network comprised of elements from a single manufacturer. And even those that do often find that the tools supplied by network equipment vendors may or may not be adequate for managing all of that equipment within a single system. Consequently, challenges arise around learning the detailed ins and outs of each type of element and each management system. A better, more efficient approach is to find and deploy management tools that offer true multi-vendor support. In this way, the number of tools needed for day-to-day tasks is reduced, eliminating the need for learning and maintaining multiple management tools, and improving operational responsiveness and efficiency.

Seven Best Practices for Network Management

How HP Intelligent Management Center Supports Effective Planning and Operations

Essential to success with this practice is being consistent – setting consistent network policies that will guide configurations and monitoring regimes across all devices and elements. From a management tools perspective, systems should not only offer certified, proven support for devices from multiple manufacturers, but that support should span all functional areas, from configuration to monitoring and troubleshooting.

Best Practice #3: Integrated Management of Virtual Networks & Cloud Resources

Without question, one of the greatest recent disruptive influences to networking is that of virtualization and cloud services. Virtualized server environments bring with them virtual network elements and architectures. As the latest of these trends, Software Defined Networking (SDN) further promotes the use of virtual overlay networks that can be defined independent of traditional networking. Cloud services are moving into the mainstream, and most network managers will see them either as important WAN or Internet-connected resources or, in some cases, as part of extended virtual networks. The impact of these trends is significant, bringing new elements of complexity and new types of connectivity that must be understood across the lifecycle of planning, deployment, and operations if networking pros are to provide expected levels of resilience. To meet this challenge, networking pros must make sure that their management tools provide the means for recognizing the existence and changes within virtual networks and relate them directly back to physical network architecture in a seamless, integrated fashion.

Networking pros must make sure that their management tools provide the means for recognizing the existence and changes within virtual networks.

Success within this practice starts with an understanding of virtual networks and connectivity paths within virtual computing environments as well as to/from external cloud services. First and foremost, connectivity policies need to be extended to include the virtual environment, coupled with a clear understanding of responsibilities for configuration and control of virtual networks. Visibility is also an essential here, meaning that virtual network elements must be brought into view of (if not under direct management of) integrated physical/virtual network management tools, so that monitoring may successfully embrace interrelationships and troubleshooting can be undertaken with a reasonable hope of success.

Best Practice #4: Automate, Automate, Automate

The pace of activity and change within networks continues to grow unabated. The days of simple, static networks are now in the past, and the specter of SDN points to more and faster change coming to networks in the future. As a result, networking pros need to leverage automation wherever and however possible to keep pace. Automation here should be thought of as faster ways to execute well-known tasks, not necessarily autonomic systems that make decisions on their own, taking control from the hands of practitioners.

In this light, there are many forms of automation available for regular use within network management tools and technologies. For example, autodiscovery can be used not only for initial recognition of devices to be managed, but also for incremental updates to devices and configurations. Monitoring templates can be automatically applied, either upon initial discovery or for updating large populations of elements under management. Data processing to generate calculated metrics can be automated for

Seven Best Practices for Network Management

How HP Intelligent Management Center Supports Effective Planning and Operations

presented operational intelligence alongside raw management data. Common tasks can be defined and scheduled to run on a calendar/clock basis or to be triggered based on a recognized event or scenario. Root cause analysis can automatically isolate failures and assist troubleshooting workflows. The list continues, but the message is clear – automation is a necessary and powerful point of leverage for network management tools and practices, both for keeping pace with change, accelerating work tasks, and improving accuracy of efforts.

Best Practice #5: Unified Policy Management

Increasingly, networking pros are expected to provide consistent levels of secure connectivity and delivery “service” to the end-user, line of business, and application development/support communities. Key to this is recognizing how to apply access and usage policies on a consistent basis. This is particularly challenging if security and network planning/administration functions are entirely independent of one another, meaning policies must be implemented through a variety of unconnected tools and systems. Whether focused on security or levels of service, *policy management* is rising in importance when it comes to the network.

Policy management is rising in importance when it comes to the network.

Achieving success in this practice requires collaboration between the security and networking planning and operations teams, to define policies and determine how best to implement and enforce them. From a management tools perspective, technologies that bring together security and usage policy definition with application and network monitoring can be of tremendous help, both in assuring that policy goals are met and maintained as well as providing a basis for forensic analysis when things break down.

Best Practice #6: Proactive Operations Monitoring

A basic objective of network operators for many years has been to establish clear, near real-time visibility into the network (and sometimes that which the network connects) so that they can quickly grasp operational health and status. With properly presented management data and contextual navigation, for drilling down into details or among groups of related elements, operations dashboards can be a powerful enabler of effective network support. Adding application and service context to the same console and dashboard views makes the result even more powerful, by providing context for prioritization and business value. Finally, baselining features that reveal normal patterns of activity help operators quickly assess abnormalities for potential preventative actions.

Integrated dashboards that present fault/availability, performance, and change event data side by side are essential

Optimizing the results of operations monitoring requires administrative efforts to assess elements under management and assign business value to them, so that monitoring regimes and priorities may be aligned appropriately. The next challenge is to keep monitoring systems current as the managed environment inevitably and continually changes. From a management tools perspective, integrated dashboards that present fault/availability, performance, and change event data side by side are essential, as are flexible means for grouping elements under management to reflect topological, organizational, or business-oriented structures. Integration of service-oriented health assessments and application awareness further improve operators’ ability to understand impact and select reactive (or proactive) responses appropriately.

Seven Best Practices for Network Management

How HP Intelligent Management Center Supports Effective Planning and Operations

Best Practice #7: Communicate, Communicate, Communicate

The very best network management practices cannot achieve their true potential without one final element – the ability and commitment to share data collaboratively with others inside and outside IT. The network viewpoint is often essential for assessing health and performance of IT services, and is regularly the first touchpoint for investigating disruptions. Making network-facing insights and information readily accessible across operations removes barriers and reduces turf battles, resulting in shorter resolution times and greater chances to convert on proactive/preventative opportunities.

Effective collaboration requires that network managers adopt an open approach to promoting and sharing data from network management systems, ideally in forms that non-networking teams can easily understand. An excellent starting point is to set up grouping definitions that reflect business or organizational alignments, to show infrastructure status in context of how it supports high priority applications and services. Dashboards and reports can then be configured using these groupings to share operational information in a common *lingua franca* with other IT and non-IT audiences. Using APIs to forward key monitoring and event data to common operating dashboards and platforms can be very valuable (if such overlay platforms are in use), as well as using management tools to automatically publish/distribute health and activity reports that have been defined to focus on each constituents' specific concerns.

Effective collaboration requires that network managers adopt an open approach to promoting and sharing data from network management systems.

HP Intelligent Management Center

In building the Intelligent Management Center (IMC) solution, Hewlett Packard has taken on an aggressive objective of delivering a unified, multi-vendor network management solution. The system is designed to optimize networking pros' reach and efficiency, by bring together capabilities across network management functional areas for complex networking environments. IMC is delivered as a base platform with optional license-enabled modules for expanded/enriched capabilities in key feature areas. Following is an assessment of how the HP IMC solution addresses and supports each of the network management best practices detailed above:

1. **Integrating management functions:** The HP IMC solution has been built to serve a combination of management tasks and workflows spanning all phases of the lifecycle, from planning and deployment through operations and maintenance. This includes features spanning configuration management, fault/availability monitoring, and performance monitoring for wired and wireless networks, as well as complementary views into network traffic and application performance.
2. **Multi-vendor support:** The IMC solution's field-proven ability to support equipment from multiple technology manufacturers is more than just a checkbox. Current support includes dozens of non-HP vendors and thousands of hardware and software components, spanning multiple management tasks and functionalities.
3. **Integrated management of virtual networks and cloud:** HP has kept the IMC solution at the forefront of managing mixed physical/virtual environments. Besides core capabilities for recognizing VLAN and other overlay networks within the base IMC platform, the virtual network management component of the base platform adds discovery and topology views for

Seven Best Practices for Network Management

How HP Intelligent Management Center Supports Effective Planning and Operations

virtual switched networks involving hypervisors, understands and tracks VM profiles, reports VM migration, and makes migration recommendations. It is even possible to invoke vMotion directly from within the IMC console, as well as configure networks directly from vSphere via an IMC plug-in.

4. **Automation:** The IMC solution has been outfitted with a long list of automated features, ranging from discovery to monitoring templates, root cause analysis, data analytics, baselining, and configuration/image management. Direct integrations with change information sources, such as vCenter/vSphere APIs for vMotion notifications, allows the system to automatically keep pace with dynamic virtualized environments.
5. **Unified policy management:** Perhaps one of IMC's clearest differential strengths is the degree to which it supports monitoring, management, and application of consistent policies across distributed, multi-vendor networks. Modular support for Access Control List (ACL) management, network QoS policies, identity-based network services, and integrated authentication systems goes far towards eliminating overlaps and conflicts in achieving parallel security and network operations objectives.
6. **Proactive operations monitoring:** By bringing together multiple sources of management and monitoring data, the IMC solution bridges a key gap confounding those who seek to become more proactive in their operations practices. IMC's unified approach of aligning fault, performance, and change management data across elements and traffic flows (i.e. sFlow, NetFlow, NetStream, IPFIX) eliminates a major integration hurdle, thus allowing the system to present data in effective, workflow-oriented dashboards and consoles. Additional features delivered via the IMC Service Health Manager surfaces network and application Key Performance Indicators (KPIs) for sustained awareness of service quality.
7. **Communication:** HP IMC comes complete with a rich set of configuration dashboards and reports, complemented by extensive APIs for integrating with other reporting systems and dashboards as needed. Further extensions are available via the IMC Intelligent Analysis Reporter module, which enables flexible/graphical report design, output formatting, and scheduling.

The IMC solution features described here represent much of the system's scope of capabilities, but are by no means exhaustive. Additional modules address related, integrated network management functions such as endpoint analysis/defense, user access management, IPSec/MPLS VPN management, integrated VoIP management, full ITIL v3.0 Service Operations management and more.

EMA Perspective

Management of the network and its related resources has never been more important, as IT becomes increasingly essential to the day-to-day mission of businesses, governments, and organizations of all types and sizes. But network management will never be the same as it once was when all that mattered was reliable connectivity and uptime – it now requires understanding performance and degradation as well as the relative importance of various attached resources and traffic categories. Now, more than ever, network managers must tune their skills and pay attention to emerging challenges, such as cloud/virtualization and convergence, while keeping an eye towards applications and services.

Seven Best Practices for Network Management

How HP Intelligent Management Center Supports Effective Planning and Operations

Network management best practices need to evolve as well, with ongoing attention paid to integration, automation, policy management, proactive approaches, and collaboration. Network management tools such as HP's Intelligent Management Center are no longer optional. They are essential, allowing networking pros to make these transitions, keep pace with rising rates of change and complexity, and maintain a trajectory towards improved effectiveness, efficiency, and enterprise value.

About HP

HP creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society. The world's largest technology company, HP brings together a portfolio that spans printing, personal computing, software, services and IT infrastructure to solve customer problems. More information about HP (NYSE: HPQ) is available at <http://www.hp.com>.

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](#).

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2013 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:

1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
2602.011413