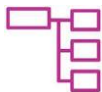




# Five Steps to Optimizing Modern Networks

Optimizing modern networks requires a new approach to planning, implementing and managing across continually evolving technologies. By consolidating both silos of functions and organizations, increased efficiencies can be achieved without the need for increased resources, while executives can stay informed of progress and security risks.

## Network Operations Management Key Capabilities:



Topology, Health and Configuration of Network Services



Performance and Capacity



Policy-Driven Configuration Management



Automation and Orchestration



Executive Dashboards and Custom Reporting

## Optimizing Modern Networks: New Tools and Processes for New Challenges

As enterprises continue to utilize multiple network technologies for the foreseeable future, optimum management must have end-to-end visibility across all deployed technologies to provide required service levels to users wherever they work: on-site, in remote offices, or a local café. Behind the scenes, modern distributed server and middleware applications increasingly require healthy and performant networks to deliver an optimized user-experience, especially on a global scale and with access to public and private clouds. Specifically, the modern trend to micro-services increases the workload on modern networks as they require increased interconnections with low latency requirements. Management of network services vs. individual devices is required to effectively monitor and respond to issues affecting users. To support the business, network infrastructures are continuing to transition to newer, faster, more dynamic and agile technologies, while at the same time increasing network security. Managing modern infrastructure can be an increasingly complex task without a unified toolset.

## Network Operations Management from Micro Focus—A New Way to Optimize Effectiveness and Efficiency with Reduced TCO and Increased Security

Network Operations Management (NOM) represents the next generation step to optimizing management of modern networks, whether in an enterprise or for your managed service customers. This solution was created to respond to the need to manage more dynamic, programmable networks in conjunction with existing physical infrastructure within a unified management workflow. By providing end-to-end knowledge across multi-vendor technologies, NOM consolidates the critical management functions of health, performance and configuration status for both staff and their management.

NOM delivers a single platform that brings robust depth and breadth, unlocking efficiencies across operations and engineering by breaking down siloes of management and reducing tool sprawl. This is supported by a recent study by EMA which found a 48% increase in early problem detection when using a reduced network management toolset.<sup>1</sup> Additionally, total cost of ownership is reduced through fewer software purchases with related lower support and training costs.

<sup>1</sup> EMA, "Network Management Megatrends 2016: Managing Networks in the Era of the Internet of Things, Hybrid Cloud, and Advanced Network Analytics," April 2016

**The Five Steps**

The first step in optimization is to enable your staff to work smarter and more efficiently by breaking down traditional network management siloes.

Figure 1, depicts how NOM works across traditional functional tool siloes, and across multiple technologies, while also future-proofing the deployment hosting options in physical, virtual and cloud environments. Efficiencies are also gained through presentation of rich decision-support data and by user-directed workflows which increase operator effectiveness by leading them through typical diagnostic scenarios. NOM's workflows reduce training time and educates operators on best practices to resolve issues fast and properly. Reduced mean time to resolution (MTTR) is a major benefit to your organization without increasing staff size.

Support for more than 180 vendors and 3,400 network devices helps NOM deploy quickly into multi-vendor environments. NOM captures vendor-specific health, performance and configurations beyond what simple SNMP and ICMP monitoring can provide. This is critical to maintain a heterogeneous network at optimal health, performance and compliance. Combined with the largest single and multi-management system scale, NOM not only provides a complete view of your current network, but is a solution you won't outgrow. As network professionals identified network security monitoring as the top missing capability when deploying SDNs, maintaining security for your total network is not a given as you move to new technologies.<sup>2</sup>

The second step is to optimize your network services by tracking performance and traffic capacity holistically. Knowing these properties of your network across critical

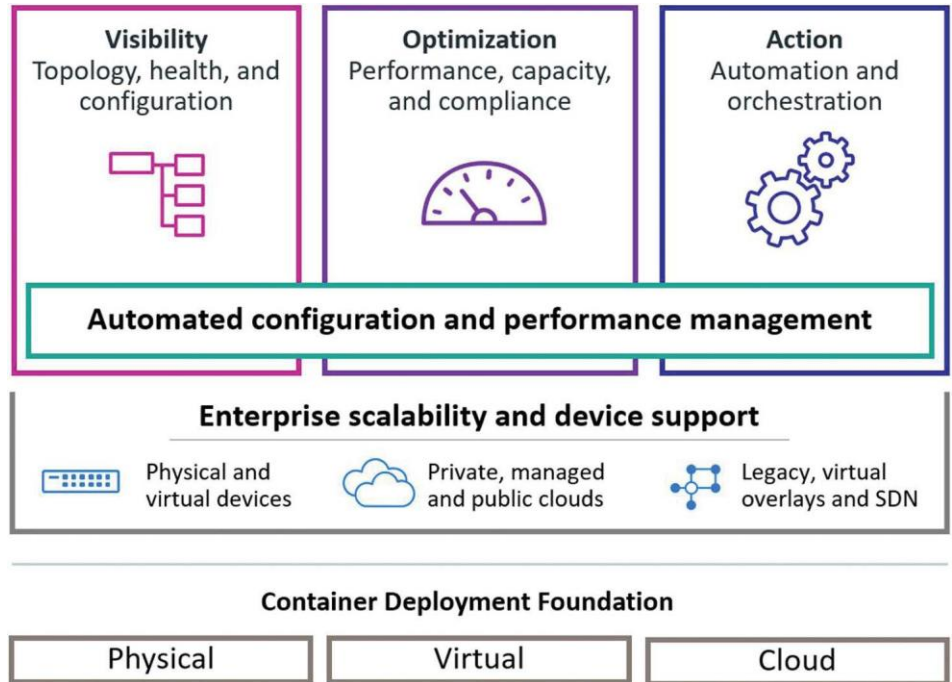


Figure 1. NOM environment and functional overview

paths (through SDN, virtual, physical, and wireless networks) is critical for diagnosing issues, planning upgrades and expansions to meet business expectations of application up-time and performance.

Third is to protect your network configurations through policy-driven configuration management. Helping you to deliver performant high-level services (such as mixed-technology WANs) to your customers, NOM uses three dimensions of compliance to maintain network configuration across all your technologies. It manages configurations, device OS versions, the running state of devices, whether physical, SDN or virtual infrastructure. NOM establishes, guards and remediates all

device configurations so they adhere to your organization's compliance policies. NOM detects any deviation from these configurations, updates dashboards, and sends intelligent alerts to your NOC operators for action. Furthermore, NOM goes even deeper, by understanding the specific changes (for example a rogue device password change), and can be configured to automatically roll back those changes to return to a compliant configuration. In Figure 2 on the following page, NOM shows a correlation between a configuration change and a device's CPU utilization spike. This level of causality saves time and effort. This leads to the automation part of your optimization journey.

<sup>2</sup> Dimensional Research SDN Survey—2018



Fourth, employ automation to achieve maximum efficiency and cost reduction. This can range from individual device configuration automation to complete orchestration of network fabric updates, replacements and even deployment of totally new network services. Transitioning to network technology requires you to be able to deal with the complexity from a mix of technologies and vendors. NOM optimizes your total network by reducing manual intervention and establishing configurations based on company standards. For example, it's common to accidentally change security configuration parameters when under pressure to resolve issues fast. NOM becomes the master-configuration resource and detects when deviations from that norm occur. NOM will automatically apply changes, check for completeness, and even rollback changes if they don't execute as designed due to unforeseen conditions.

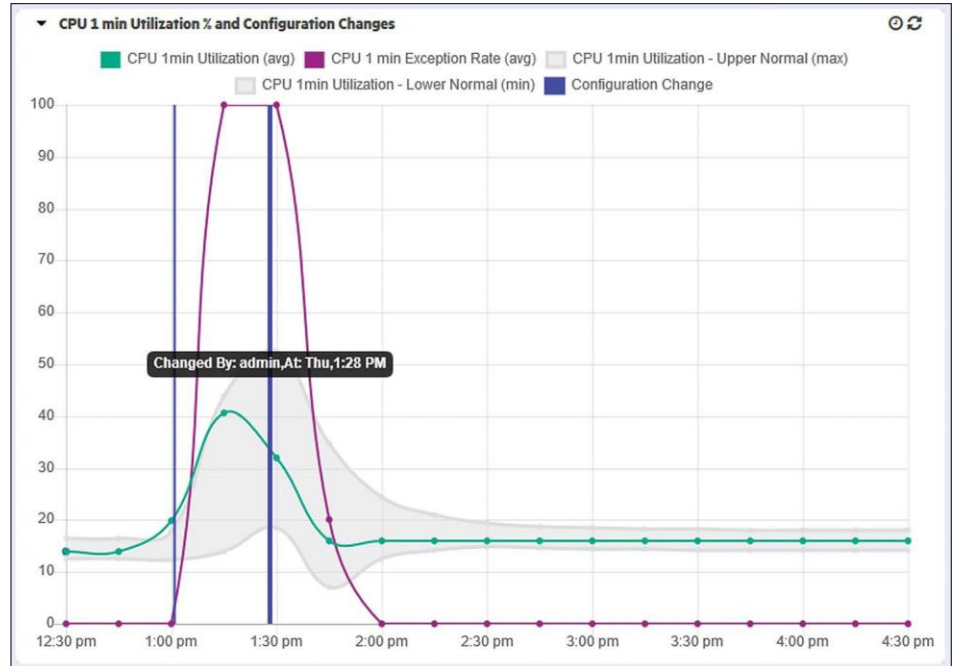


Figure 2. Automatic configuration change and performance correlation

NOM goes beyond network diagnostic and configuration automation actions to full-bore multi-system, coordinated change orchestration. Made possible via the included Micro Focus® Operations Orchestration subsystem. See Figure 3 for a network workflow example, where actions within NOM are linked to external systems including ticketing and CMDB to complete the full process for an incident.



Fifth, keep your staff and executives up-to-date by providing them with valuable, non-technical summaries of the state of their networks. NOM's Business Value Dashboards provide executive level information in a clear, easy to understand visualization. But, these go beyond just summary screens, as users can drill down further to see specific networks—for example the NYC network in Figure 4 on the following page is flagged for investigation. Further drill

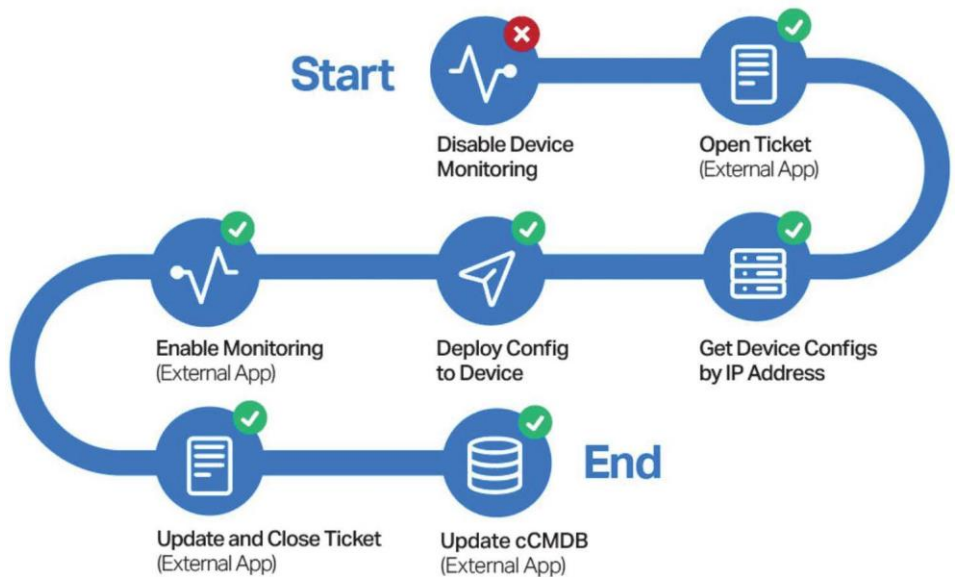


Figure 3. Multi-system automation, orchestrated through NOM's workflow subsystem

“Micro Focus Network Management is one of the best tools in our tool bag!”

SENIOR MANAGER OF IT OPERATIONS  
Leading U.S. Financial Institution

Contact us at:  
[www.microfocus.com](http://www.microfocus.com)

Like what you read? Share it.



Figure 4. Global Network Operations Center Dashboard

down presents real time operational information if required, so management can get to the same data as power-users without having to be familiar with the product’s navigation.

In addition, NOM’s extensive data collection feeds information to both executive dashboards, as well as provides detailed, specific reports for operations and engineering staff to monitor in real time and act upon. The extensive collection of included and user-tailorable NOM reports covers these areas:

- Monitoring: Health and Performance/Traffic Reports—for deep investigation of issues, and planning for adjusting capacities, for example to meet peak load times.
- Configuration and Compliance Reports—for NOCs and engineering to use in collaboration as they’re alerted to and resolve issues including network

configuration and compliance status, when changes happen and whether they’re authorized or rogue.

- Pre-formatted compliance reports meeting COBIT, GLBA, HIPPA, and PCI standards

Report tuning includes adjusting report options for displayed metrics, time ranges, grouping of metrics, adjusting for planned device outages, and more through easy to access menu selections. Reports can be viewed, emailed and exported in multiple formats including HTML, PDF, Excel, and CSV for further use. Reports can also be run in background for scheduled delivery, and includes the Cognos BI Query Studio for advanced database reporting.

To learn more about Network Operations management or start a trial see: [microfocus.com/nom](http://microfocus.com/nom)

Two-thirds of network professionals preferred a unified network management solution that includes SDN, virtual, physical, and wireless networks; as well as monitoring, configuration and compliance functions.<sup>3</sup>

3 Ibid