MICRO FOCUS®

Data Sheet

IT Operations Management

Network Automation

Micro Focus® Network Automation (NA) helps Global 2000 companies, government agencies, and service providers manage network configurations and meet compliance. Its process-driven model prevents errors and reduces costs. NA is included with Network Operations Management—our comprehensive network management solution.

Network Operations Management: **microfocus.com/nom**

Product Highlights

Management of modern networks relies on automation to contain costs, effectively manage network changes, and maintain security compliance policies. The right solution can even orchestrate whole new deployments to add new services to support urgent business requirements with high quality.

Network Automation automates the complete operational lifecycle of network devices from provisioning to policy-based change management, compliance, and security administration. The complete set of capabilities of Network Automation and Network Node Manager i is included in Micro Focus Network Operations Management, our comprehensive management solution including network fault, availability, and performance with change, configuration, compliance, and automated diagnostics.

Beyond simple scripting solutions, Network Automation provides process-powered automation when combined with the embedded workflow engine, enabling you to automate network workflows beyond traditional network change and configuration management. The value of automation is reduced greatly if your solution doesn't have deep understanding of device vendor specific devices including protocols, security, ACLs and more. This is why Network Automation supports an exhaustive set of network devices from over 180 vendors, including virtual and SDN devices, giving you comprehensive network change and configuration management coverage for an extensive range of devices. NA driver packs are updated on a bi-monthly basis, and requested support is a priority and are loadable without upgrading the NA application.

IPC

35 hours/month savings through automation and **scaled network by 300%** without increased headcount

Key Features and Benefits

- Reduce costs by automating time-consuming manual change, configuration, and compliance tasks tasks across physical, virtual, SDN and wireless networks.
- Pass audit and compliance requirements easily with proactive policy enforcement and audit and compliance reports including: ITIL, PCI, Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act.
- Increase network stability and uptime by preventing the inconsistencies and misconfigurations that are at the root of most network problems.
- Deliver full network lifecycle workflow automation with a uniquely powerful process-driven configuration automation in a granular and flexible method—without scripting.
- Quickly deploy wide-scale image updates with automated software image management.
- Manage virtual switch and virtual context environments to support new cloud computing, SDN, and virtual network deployments.
- Supports secure, 2-factor, 64-bit RSA for common device authentication.

Key Benefits

Without the right tool, bringing networks into compliance with corporate or regulatory standards is a nontrivial, labor-intensive, and ultimately difficult task. Network Automation helps you meet compliance standards through a real-time network compliance model that maps device information, including configurations and run-time diagnostics, as well as policies and user roles, into a normalized structure to prevent compliance violations before they occur. Network Automation extends policy-based compliance to include the run-time state of your network to dramatically reduce manual misconfigurations that open the door 85% of security breaches that can result in financial penalties and/or significant network downtime.

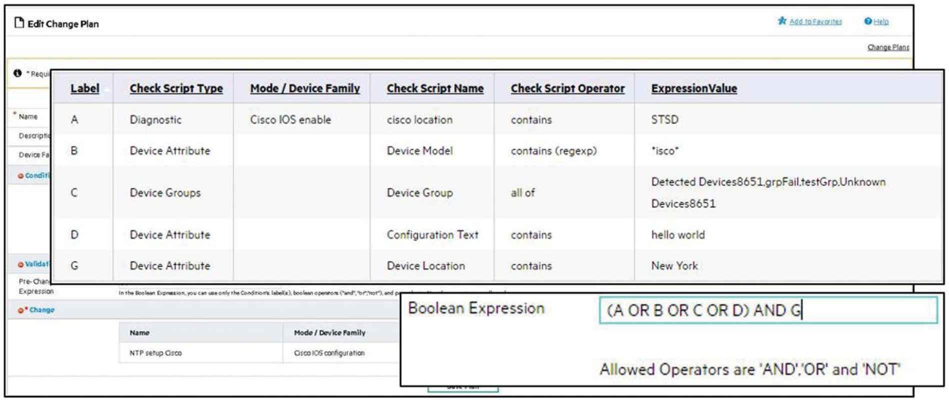
- Network Automation validates new changes against policies automatically to proactively avoid misconfigurations and noncompliant changes. If the changes do not comply, Network Automation alerts you to make appropriate corrections before applying them to a device, and can automatically remediate devices that are found to be out of compliance. Network Automation also checks the running state of the configuration and can roll-back configurations that are not compliant when operational.
- Flexibly generate out-of-the-box reports that comply with the information technology infrastructure library (ITIL) standard, the payment card industry (PCI) standard, or tailor to any other internal or external report standard.
- A single sign on for all network devices/elements and keystroke logging of CLI device access which is centrally secured for a secure, consistent and auditable configuration process for your entire network.
- Handles full and partial configurations, OSes and patches for multiple devices at a time, saving time, effort and increasing consistency.
- Enterprise-grade, multi-server architecture delivers huge network coverage with disaster recovery.
- Industry-leading heterogeneous support for more than 180 vendors and 3,400 models, including physical, virtual and SDN elements. These are added to and updated bi-monthly. Network Driver Studio provides a GUI to create custom network drivers or modify NA's delivered drivers.
- Automatic collection of Common Vulnerabilities and Exposures (CVE) and other cybersecurity vulnerability databases through the Micro Focus Marketplace. NA can be configured to implement them automatically.
- Integrates with Data Center Automation's Server Automation subsystem to combine capabilities to cover configurations beyond networks.
- Includes a flexible, integrated approval model that supports third-party ticketing systems.

Key Features

Robust Control over the Configuration Process

Configuration management is at the heart of the network engineering process and Network Automation includes three important capabilities to control the process of automatically configuring network devices:

- Granular permission within NA to control which users can control which inventory items can be modified, including separate scripting and viewing permissions. This leads to an orderly and auditable process for all levels of users.
- The use of structured logic to control change instructions increasing the accuracy of the compliance policies themselves.
- User-definable Change Plans provides a mechanism to filter target devices for configuration changes based on user-defined criteria to meet your specific change processes and ensure accurate completion. Figure 1 shows the easy and powerful logic control of Change Plans. Change Plans employs a multi-stage mechanism that first checks the device's running configuration status before executing reconfiguration. Once the change is made to the device, a post-check is done to make sure the change was accomplished as planned. If problems arise, the configuration can be rolled back to the last compliant configuration as a temporary state until the change can be accomplished correctly.



Label	Check Script Type	Mode / Device Family	Check Script Name	Check Script Operator	ExpressionValue
A	Diagnostic	Cisco IOS enable	cisco location	contains	STSD
B	Device Attribute		Device Model	contains (regexp)	*isco*
C	Device Groups		Device Group	all of	Detected Devices8651,grpFail,testGrp,Unknown Devices8651
D	Device Attribute		Configuration Text	contains	hello world
G	Device Attribute		Device Location	contains	New York

In the Boolean Expression, you can use only the Condition's label(s), boolean operators ("and","or","not"), and

Name	Mode / Device Family
NTP setup Cisco	Cisco IOS configuration

Boolean Expression: (A OR B OR C OR D) AND G

Allowed Operators are 'AND','OR' and 'NOT'

Figure 1. NA's Change Plans GUI with Boolean logic to control when and what to change

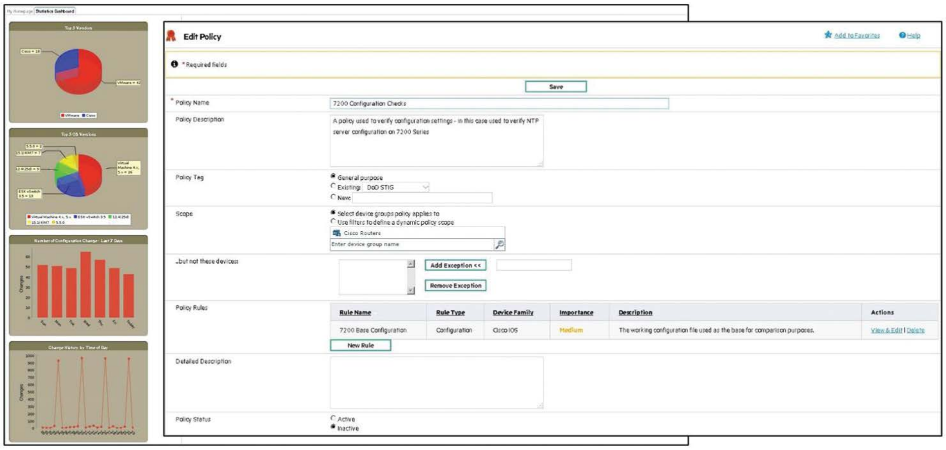
Be Ready for Compliance Audits Every Day

Unlike manual, static inventory and compliance reporting methods using spreadsheets or even databases, NA continuously keeps an up-to-date inventory of all devices, their OS images, patches and configurations. Reports are generated from the current network device status, so no additional compilation or preparation is required. This means that you are continuously ready for compliance audits as you use NA. Not only is time and effort greatly reduced, but you'll know your readiness at all times and remove the huge work effort commonly required before audits are due. When an audit is requested, NA makes it easy to inquire on devices ad-hoc as it captures the running configuration status—which may vary from the intended configuration as previous instructions may not have been completed due to errors.

NA's device status and compliance dashboards are valuable content for audit reports. In Figure 1, you can see graphs summarizing the network's configuration and compliance status. It also shows an example of how easy it is to create/edit a compliance policy through the GUI. In this case it's a base configuration for all Cisco 7300 routers to use. Other policies for 7300s can build upon this foundational policy.

Change the Script of Your Organization

While manual scripting can address many configuration requirements, Network Automation greatly simplifies this task and ensures all network engineering and operations can fully participate in and manage the configuration process. Its granular configuration components are reusable, and can be combined into more complex tasks, and work across multiple vendors' OSes and CLIs, reducing the need to be experts on each vendor/model/device combination. This is done by abstracting the tasks into a set of common, neutral set of instructions. The result is a one-click execution of tasks or automatically via configurable triggers. This increases efficiency and removes the difficulty of maintaining scripts written by someone else. NA supports access security methods including TACACS+, RADIUS, SecurID, Active Directory, and LDAP, so it can be integrated into your corporate ID management solutions.


Edit Policy

*Required fields

Save

*Policy Name: 7200 Configuration Checks

Policy Description: A policy used to verify configuration settings - in this case used to verify NTP server configuration on 7200 Series

Policy Tag: ● General purpose ○ Existing: DoD STIG ○ New:

Scope: ● Select device groups policy applies to ○ Use filters to define a dynamic policy scope
Cisco Routers
Enter device group name

..but not these devices: Add Exception << Remove Exception

Policy Rules:

Rule Name	Rule Type	Device Family	Importance	Description	Actions
7200 Base Configuration	Configuration	Cisco IOS	Medium	The working configuration file used as the base for comparison purposes.	View & Edit | Delete

New Rule

Detailed Description:

Policy Status: ○ Active ● Inactive

Figure 2. NA Policy Compliance Dashboards and Editing a Policy

Policy-Based Compliance

The reason the term "policy" resonates so strongly in the security domain is that it provides a way to define consistent security across multiple devices rather than individual elements in a network. You will likely define policies for different areas of your network – for example access layer vs. core. Network Automation allows you to define your network configuration policies, monitor for changes against them, and even automatically remediate configurations back into compliance. When policies are updated, NA makes it easy to update the network elements. For example, this can be an incremental configuration change. This saves time, effort, and improves your ability to maintain, document and prove

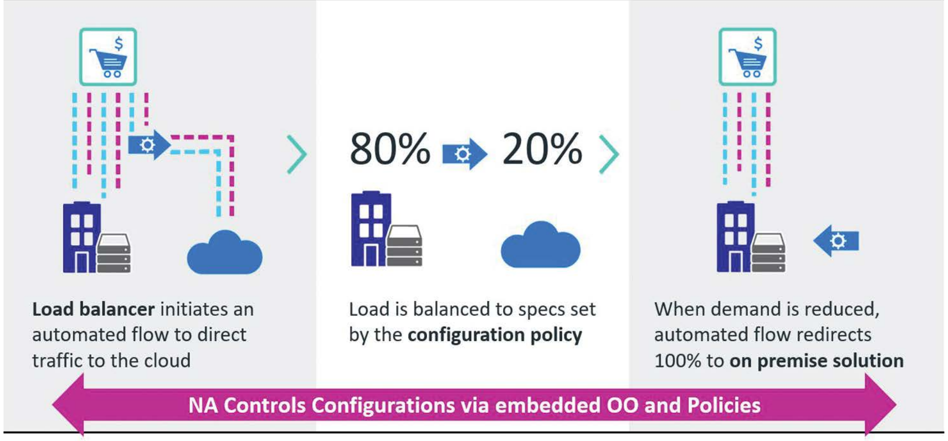

80%
20%
Load balancer initiates an automated flow to direct traffic to the cloud
Load is balanced to specs set by the configuration policy
When demand is reduced, automated flow redirects 100% to on premise solution
NA Controls Configurations via embedded OO and Policies

Figure 3. Beyond scripting—NA's ability to control network traffic to meet dynamic needs

> NA can be your best single network management investment as “39% of enterprises indicate that configuration data is the #1 data source for troubleshooting workflows.”
>
> SOURCE: ENTERPRISE MANAGEMENT ASSOCIATES, MAY 2017

Contact us at:
www.microfocus.com

Like what you read? Share it.

compliance. Policies can be applied across multiple technologies included a critical path that crosses physical, virtual, SDN and wireless fabric. This would normally require using multiple element managers (one for each device vendor), but NA works across vendors to maintain consistent policies throughout your network and reduces the requirement to use multiple element management solutions.

Continuously Updated Content

New network vendors, devices and updates are always being introduced, and Network Automation keeps up with these changes in several ways:

- Micro Focus Marketplace provides ongoing updates of device vendor security vulnerabilities without the need to update the NA application. This information comes from multiple authoritative sources and can be automatically applied to a running NA system.
- NA driver packs are updated on a bi-monthly basis, and requested support is a priority. The ever expanding support list currently includes more than 180 vendors and 3,400 device models.
- If you would like to create custom device drivers, Network Driver Studio provides customers with the ability to create their own device drivers via an intuitive interface.

Major Network Orchestration

NA goes beyond single element or even group configurations to the ability to orchestrate replacement or implementation of new network fabric. Good examples include adding new remote site networks and other similarly contained networks automatically to complete the provisioning process. One Micro Focus partner helped a retailer do just that with NA. Not only are new locations on-line faster, but their configurations meet the company’s latest security compliance policies from the start.

GreenLight group

“[Using Network Automation] we built a solution called ‘zero-touch migration’ which facilitated them to be able to, with minimal engineering involvement, deploy and replace new devices across their 4,000 outlets.” Joe Madden, Greenlight Group YouTube video here.

Enterprise-Grade Architecture to Grow with You

Network Automation architecture includes the ability to deploy satellites delivering real-time visibility and configuration control for your globally distributed network, including support for remote locations around the world and with overlapping address ranges and WAN links. Satellites also provide failover support for NA, automatically replicating information to multiple locations, allowing the new locations to use information continuously regardless of network link connections. The advanced global control from Network Automation lets network teams use best practices and knowledge across multiple locations and provides operational consistency across your enterprise.

Licensing Models to Fit Your Requirements

NA Premium Edition

Network configuration backup and restore, server, satellites, and scale-out architecture.

NA Ultimate Edition

NA Premium PLUS: Network compliance.

Learn more at
www.microfocus.com/networkauto

© 2019 Micro Focus or one of its affiliates. Micro Focus and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.

MICRO FOCUS®