

Opsware Network Automation System 4.5

Network management isn't what it was 5 years ago. Today, every person in the company relies on the network, in some way, to be successful in their job. Because of the dependency on the network, what used to be an acceptable amount of network instability is no longer tolerated. With the rise of governmental regulations and increased focus on network security, successful companies are adopting best-practice disciplines, such as ITIL, to manage the network. Couple this with the facts that 80% of outages and security incidents are due to manual network misconfigurations and compliance requirements are 5 times more costly to meet when done manually and organizations are facing a choice between explosive management costs or a network unable to meet the requirements of the business.

To address this challenge, Fortune 2000 companies, governments and service providers are turning to network automation to keep network management costs contained while providing the quality and responsiveness their businesses demand. The Opsware Network Automation System (NAS) goes beyond multi-vendor network configuration management to deliver network automation. Opsware NAS immediately addresses critical IT issues by decreasing network complexity, improving network stability, enforcing regulatory compliance and increasing network security. The solution tracks, regulates and automates all configuration and software changes across multi-vendor network devices. In addition, Opsware NAS enables IT governance initiatives, automates delivery and enforcement of network change control processes, and provides automated management of security and compliance best practices.

The end result is a resilient, maintainable, and cost effective network that is compliant with company standards and government regulations.

The Opsware Network Automation System enables organizations to automate the enforcement of best practices and standards to achieve higher network stability metrics and comply with government regulations in a cost effective manner.

- Ensure compliance through automatic, real-time policy enforcement.
- Improve network security with patch management, access control list (ACL) management and device access regulation.
- Increase network stability and uptime through change detection, notification, and automatic rollback.
- Lower total cost of ownership through automation of routine tasks and management of multiple vendors via an easy to use interface.

Key Benefits

Cost Efficiency

Achieve network device to network engineer ratios as great as 2000:1 by automating the time-consuming manual compliance checks and configuration tasks.

Network Stability

Improve network stability and uptime eliminating the inconsistencies and misconfigurations that are at the root of most problems.

Audit & Compliance

Easily meet compliance requirements with audit trails, flexible, automated policy enforcement and searchable historical configuration record.

Supported device vendors

3Com
Adtran
APC
Aruba
BelAir Networks
Blue Coat
Check Point
Cisco
Cyclades
Enterasys
Extreme Networks
F5 Networks
Foundry Networks
Force 10
HP
Juniper Networks
Marconi
Netopia
NetScreen
NetApp
Network Appliance
Nokia
Nortel Networks
Packeteer
Procket Networks
Secure Computing
Terayon

Enforce policy, standardize operations and ensure compliance

Opware NAS allows IT managers to enforce policies, standards and best practices in real-time. By defining network configuration and software policy rules, NAS will report non-compliant devices and prevent deployment of non-compliant configurations. NAS supports flexible rules that can be applied to devices in a many to one relationship, eliminating the need to store and manage hundreds or thousands of rigid “blessed” configurations. Network staff set rule priority to enable automatic triage and systematically route compliance violations. In a large network, this eliminates noise and forces serious compliance violations to the top of the stack. All rules can be configured with automatic remediation that returns the device to its compliant state without network disruption.

Ensure network security

IT Managers must have clear visibility into what is changing on the network. Opware NAS delivers complete audit trails, down to the keystroke level, for all network activity so that any change can be identified, including who, what, when and why. For a quick response to emerging network threats, NAS delivers powerful ACL automation and management capabilities as well as centralized OS management. NAS empowers IT managers to monitor OS device levels, prevent the spread of vulnerable or deprecated software images and upgrade device software in a foolproof manner. To protect against internal security threats, users are limited to network information on a “need to know” basis. NAS utilizes highly granular, customizable role-based permissions that control what information the user can view, what actions the user can perform on devices and which devices user can gain direct access.

Prevent network downtime and increase stability

Peer reviews are widely recognized in the industry for being the single most important factor in detecting and preventing configuration errors in the network. Studies have shown that implementing peer reviews results in nearly 4 times fewer defects rolled out into the network. Opware NAS closes the gap between the approval of a change and the actual configuration change that is pushed to the network. Through a flexible, integrated approval model, IT managers can enforce that the approval of a change utilizes the exact configuration code that will be pushed to the network upon approval. Further, because NAS always has a real-time image of the network, approvers of a change can review the specific change in context of the entire device configuration and the business units it will affect. Opware NAS empowers IT managers to enforce that device changes are only made during defined maintenance windows. Finally, IT Managers can funnel direct device access through an approval process, eliminating unauthorized direct device access and preventing network problems before they even occur.

Greater automation and lower total cost of ownership

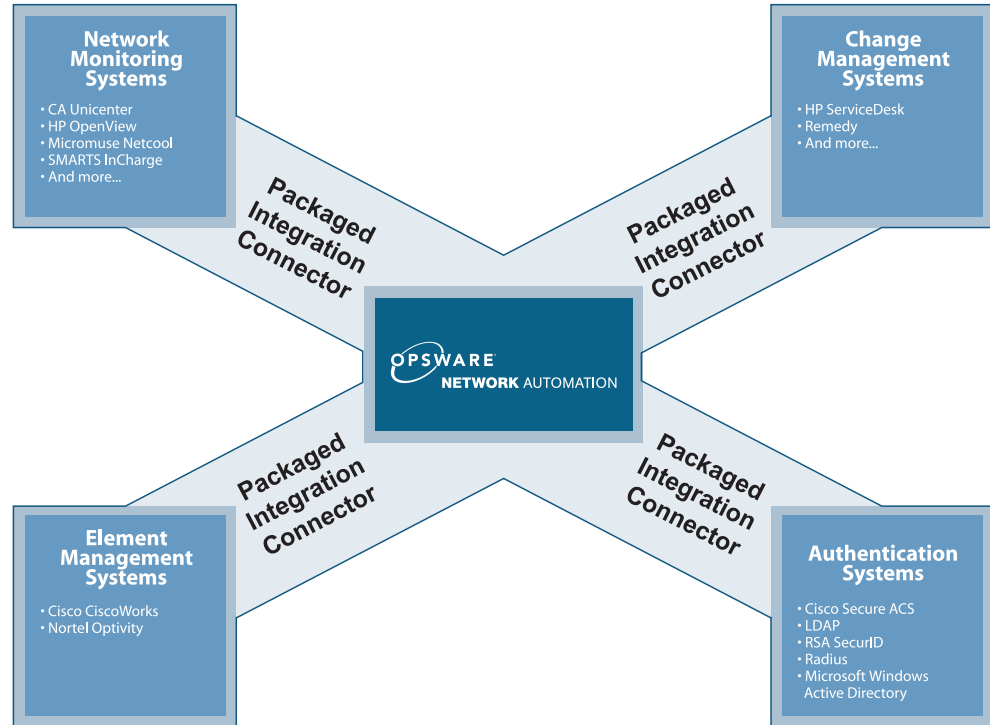
By automating key tasks, such as policy compliance, OS upgrades and configuration management in a multi-vendor network, IT departments can achieve over 400% improvement in their productivity. Using Opware Network Automation System, IT staff can update 6000 device configurations in less than two hours and reduce device provisioning time from six hours to twenty minutes.

OPSWARE NETWORK AUTOMATION SYSTEM CAPABILITIES

Network Auto-discovery & Intelligent Device Management	Perform a network scan or accept an import feed and automatically identify devices not under Opsware Management. Utilize user-defined, heuristic rules for assigning the primary management IP address for devices. Automatically de-duplicate devices from inventory which have been discovered via multiple IP addresses.
Real-time Configuration & Asset Tracking	Detect, in real-time, all configuration and asset information changes across multi-vendor devices, regardless of how the change was made.
Audit Trail	Store complete audit trail of configuration, hardware and software changes on network devices, including the critical who, what, when and why.
Role-based Access Control	Configure granular, customizable user roles to control permissions on device views, device actions and system actions. Utilize common authentication systems, such as TACACS+/Radius, SecurID or Active Directory/LDAP, out of the box.
Network Lockdown	Manage all device access and authorization via a centralized control model deeply integrated with your workflow and approvals processes.
Compliance Control	Enable rapid troubleshooting and control network compliance by comparing devices to defined, best practice standards. Control network drift towards non-compliance with controlled, automatic remediation of devices in violation of standards. Speed internal and external audit processes with out of the box network compliance reports covering ITIL, SOX, HIPAA, CISP & more.
Device Provisioning	Automate routine configuration tasks to perform vendor-agnostic updates, such as password or community string changes. Simplify and automate complex network tasks with project staging and workflow. Reduce the time needed to build automation scripts and increase accuracy with auto-generated scripts derived from device sessions.
Configuration Deployment & Rollback	Deploy compliant configurations across groups of devices, regardless of vendor. Instantly roll back to a previous known good configuration, dramatically decreasing time to repair.
ACL Management & Automation	Respond quickly to emerging network threats with powerful, centralized, batch ACL editing and deployment. Utilize ACL templates to ensure ACL homogeneity and stability.
Device OS management	Deploy and monitor OS images easily from a centralized network patch management system. Control deployment of images via specific requirements to prevent mistakes before they happen.
Automation Engine	Easily create complex automation flows, integrating internal and 3rd party systems. Leverage over 200 system triggers to drive automation.
Workflow & Approvals	Close the change loop with real-time process enforcement. Model complex approval processes with highly flexible rules. Force approvals for specific changes, including changes made by a direct CLI session. Chain multiple tasks together into a project workflow with intelligent logic on whether system should proceed to the next step in the flow.
Data Mining & Reporting	Provide dynamic, real-time reports into the hardware, software, configuration and operational activities across complex, heterogeneous data centers. Deliver management reports, including network best practice SLA reports, activity correlation reports and network automation summary reports, out of the box.

The Opsware Network Automation System is a multi-tiered solution that can be deployed on Windows, Linux or Solaris. Databases capabilities can be provided by Oracle, Microsoft SQL Server or MySQL.

NAS offers a variety of value added Integration Connectors



About Opsware, Inc.

Opsware Inc. provides the most comprehensive solution to automate the entire operations lifecycle for server, hardware, software, and network infrastructure. Opsware solutions have been proven in large organizations worldwide, including corporate enterprises, government and intelligence agencies, service providers and network device manufacturers. Please visit www.opsware.com to learn more Opsware and its products.

Opsware Server Automation System immediately addresses critical IT issues such as cost reduction, regulatory compliance, and system security while generating massive efficiency and quality gains to achieve operational agility, improved productivity, standardization, and higher levels of server uptime. Through a simple, intuitive user interface, all aspects of server and application management are addressed, including: automated discovery, change and configuration management, audit and compliance, and reporting.

Opsware Asset Management System is the leading discovery and repository solution for complex, distributed IT environments, utilizing the most accurate and comprehensive auto-discovery technology available. Automatically capturing detailed configuration and component inventory information on every IT asset in the enterprise, including hardware (servers, desktops, laptops, network and SNMP devices, PDAs, etc) and software (installations, usage patterns, configuration changes), Opsware Asset Management System provides a comprehensive physical blueprint of the whole organization.



Corporate Headquarters

599 North Mathilda Avenue Sunnyvale California 94085 USA
T 408.744.7300 | F 408.744.7383 | www.opsware.com