Overcoming Network Degradation Blues with

OpManager NCM Plug-in

Unified Network Management

ManageEngine

Powering IT ahead

V. Balasubramanian, ZOHO Corp.

Abstract

Enterprises depend on network availability for business continuity. To keep the network up and running, it is bare essential to have a robust, reliable fault and performance management software that helps in effectively monitoring the network. With world-class ManageEngine OpManager in place, you have perfect control over the Network Monitoring arena. But, to prevent network problems and performance degradation issues arising due to faulty device configuration changes, OpManager NCM plug-in is essential. OpManager and NCM Plug-in together make Network Management not only efficient, but also truly centralized. This paper discusses the network configuration management challenges, the need for the NCM plug-in and its benefits.

Contents

The Challenge

Enterprises – big and small, depend on network availability for business continuity. In heterogeneous networks with hundreds/ thousands of mission-critical edge devices such as switches, routers, firewalls and others from multiple hardware vendors, managing the network becomes a challenging task. Even a few minutes of network outage could have a rippling effect on the revenue stream as critical business services get affected.

As business needs grow, network complexity also grows up exponentially. The enterprise naturally puts the squeeze on the few network administrators mandating them with the responsibility of ensuring network availability. Not just network availability, but also ensuring security and reliability, optimizing performance, capacity and utilization of the network fall under the ambit of the administrators.

To keep the network up and running, it is bare essential to have a robust, reliable fault and performance management software that helps in effectively monitoring the network. With world-class **ManageEngine OpManager** in place, you have perfect control over the Network Monitoring arena. But, that alone may not be sufficient to prevent all network outages.

Network Management experts repeatedly point out that more than half of the network outages and performance degradation issues are caused by faulty configuration changes. So, it is highly important to prevent network outages arising due to faulty configuration changes.

To keep the network up and running, it is bare essential to have a robust, reliable fault and performance management software that helps in effectively monitoring the network. With world-class ManageEngine OpManager in place, you have perfect control over the Network Monitoring arena. But, that alone may not be sufficient to prevent all network outages.

Business needs are in a constant state of flux and administrators are required to respond to the needs often by configuring the network devices, which is a sensitive and time-consuming task. It requires specialized knowledge, familiarity with all types of devices from different vendors, awareness on the impact of changes, precision and accuracy.

Naturally, the highly skilled network administrators carry out the configuration changes. But, even the highly skilled are not immune to committing mistakes.

Ironically, most of the configuration changes are repetitive, labor-intensive tasks - for instance, changing passwords and Access Control Lists. Yet, as even minor errors in configuration changes to the devices in production carry the risk of causing network outage, the skilled network administrators spend a significant part of their time on configuring the devices. They find it hard to concentrate on strategic network engineering and administration tasks.

Besides, with increasing security threats to mission-critical network resources and serious legal consequences of information mis-management, enterprises everywhere are required not just to follow standard practices,

internal security policies, stringent Government regulations and industrial guidelines, but also demonstrate that the policies are enforced and network devices remain compliant to the policies defined. Ensuring compliance has become a priority for network administrators nowadays. This drives them take extra care while changing configurations.

Administrators also have to continuously monitor the changes carried out to the devices, as any unauthorized change can wreak havoc to the network.

It is evident that administrators face pressures from multiple angles; but, how do they normally manage configurations? Let us have a look at some of the traditional network configuration management practices:

- While carrying out changes, most of the administrators document the proposed changes. They login to each device separately and carry out the change. In case, the configuration changes are not successful, they will turn the configuration to the previous working state by undoing the changes as recorded by them in the documentation.

- In big enterprises with a large number of devices, the administrators cannot follow the 'change documentation' process. Instead, they develop custom scripts to push configurations to multiple devices. With the enormous diversity of hardware vendors, the administrators develop numerous custom scripts to suit the syntax of each device type.

- Some others juggle with fragmented tools to do specific tasks in configuration management. They correlate the output from each tool manually.

- Still worse, some administrators follow the haphazard way of carrying out changes to live equipment without any management plan. When errors in configuration cause network outage, they end up wishing that they could move the configuration back to a proper working version. They manually troubleshoot the cause.

Administrators have to continuously monitor the changes carried out to the devices, as any unauthorized change can wreak havoc to the network. Even a trivial error in a configuration could have devastating effect on network security giving room for malicious hackers.

The Limitations of the Traditional Approach

The manual way of configuring the devices suffer various disadvantages and serious limitations. The following are prominent among the many:

- The highly skilled network administrators spend most part of their precious time on doing repetitive, time-consuming configuration tasks. They get little time to focus on strategic network administration plans and tasks. This amounts to wastage of resource, cost and time.

- There is no provision to apply configuration changes in bulk to many devices at one go. Administrators have to logon to devices separately or at best execute many custom scripts to get the work done, which would be time consuming.

- Even simple tasks like rotating passwords of devices, viewing access lists etc. could prove uphill.

- As the number of devices grows, administrators find it difficult to respond to the business priorities that require frequent configuration changes. Possibilities of committing errors become bright.

- A trivial error in a configuration could have devastating effect on network security giving room for malicious hackers. The traditional approach has no provision to check configurations before deployment from the standpoint of security.

- Administrators lose track of configuration changes. As a result, configuration management becomes a daunting task. In the face of a network outage, troubleshooting becomes laborious. The mean time to repair (MTTR) climbs significantly.

- There is no way to control the access to device configurations based on user roles. No way to check/prevent unauthorized configuration changes either.

- The traditional practice has no scope to ensure accountability for user actions. When something goes wrong due to faulty configuration change or when a security breach occurs, it would not be possible to trace the actions to a particular individual in the absence of audit trails.

- There is no provision to monitor and ensure compliance to government regulations, industry best practices and standards.

Issues at a Glance

- Wastage of skilled resources in repetitive configuration tasks
- Administrators require lot of time to do configuration changes
- Troubleshooting in the face of outages becomes monumental
- No provision to monitor unauthorized changes, security and compliance
- Unable to keep track of configuration changes
- No centralized control
- Lack of accountability for actions

Highly skilled network administrators spend most part of their precious time on doing repetitive, time-consuming configuration tasks. They get little time to focus on strategic network administration plans and tasks. This amounts to wastage of resource, cost and time.

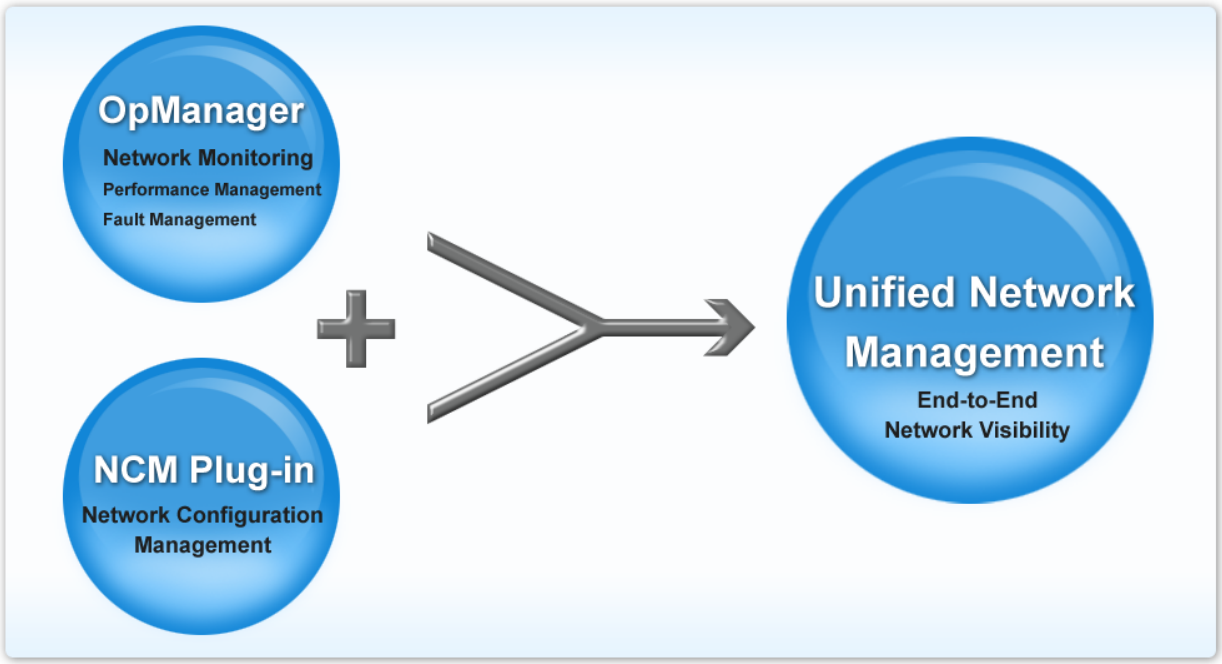
The Solution: Use OpManager NCM Plug-in

Conquering the complex, multifaceted operational and technological challenges of network configuration management requires deployment of a Network Change and Configuration Management (NCCM) solution.

ManageEngine OpManager's NCM plug-in comes into play here.

OpManager NCM-Plug-in seamlessly integrates the Network Change and Configuration Management functionalities with the all-important fault and performance management capabilities of OpManager.

OpManager and NCM Plug-in together make Network Management not only efficient, but also truly centralized. From a single console, you will be able to monitor network performance, identify performance bottlenecks and take total control of device configurations. You will be able to troubleshoot issues arising due to faulty configuration. In short, you will get end-to-end network visibility and also a handle to resolve conflicts.



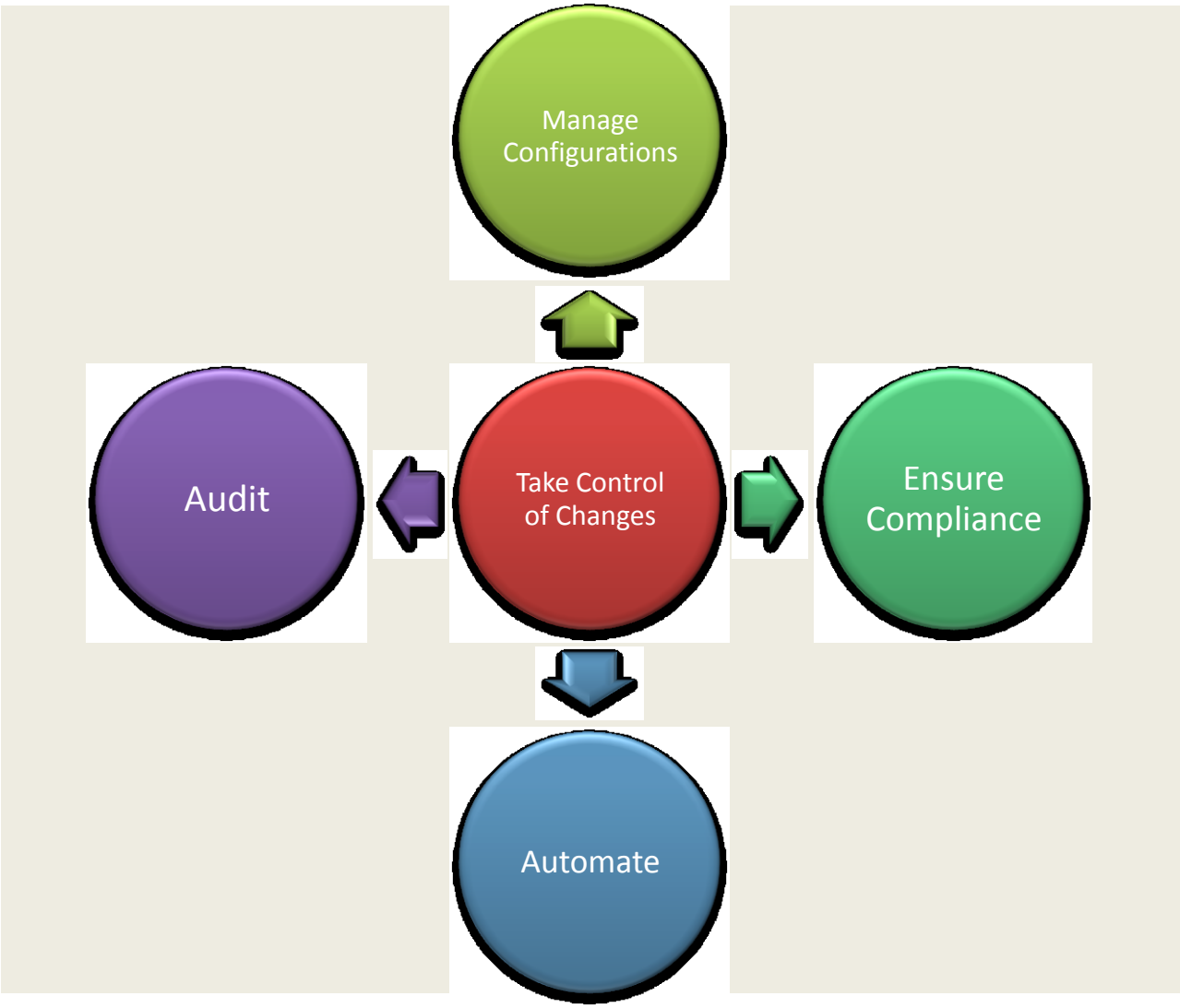
What you can do with NCM Plug-in?

Manage Configurations

- Maintain versions of configurations and view, compare, edit, label and upload them from OpManager web GUI

Take Control of Changes

- Monitor configuration changes in real-time, get notifications, prevent unauthorized changes, approve genuine changes



What you can do with NCM Plug-in?

Ensure Compliance

- Define standard practices and policies and automatically check configurations for compliance. Get reports on compliance status and satisfy your auditors.

Automate

- Automate repetitive, time-consuming configuration tasks like enabling TELNET service, changing SNMP community, forwarding syslog messages, changing the interface, changing passwords, updating NTP server entries, getting 'show version' output, uploading OS images / firmware upgrade, configuring banner message, deleting files from flash

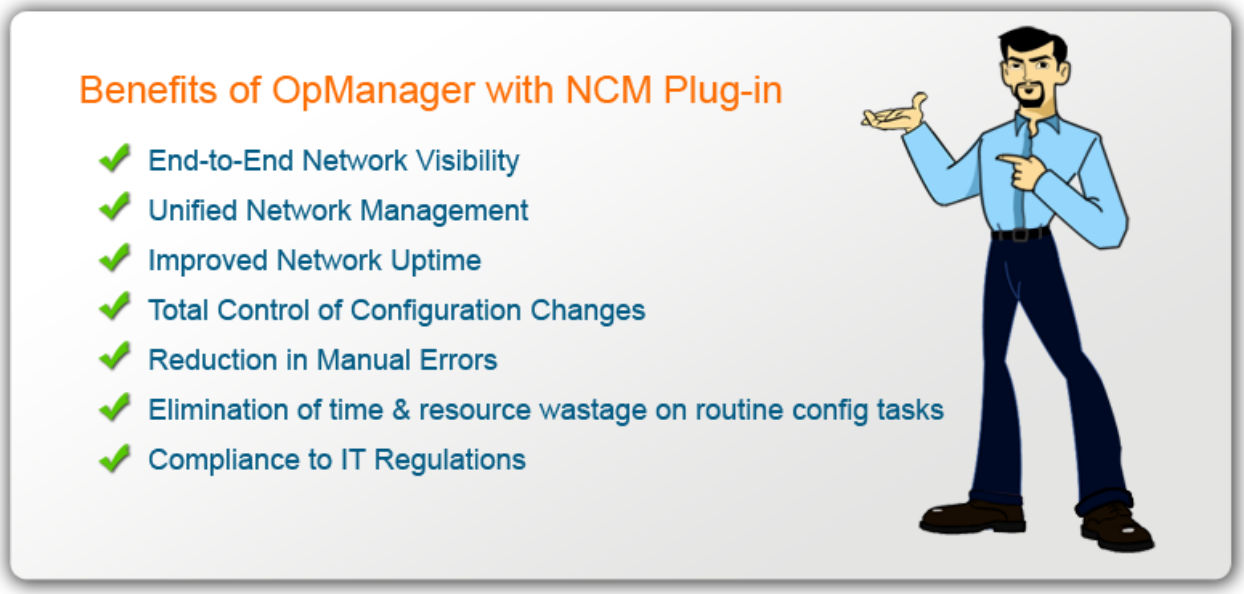
Audit

- Get completed record of who, what and when of configuration changes

Benefits of NCM Plug-in

The NCM Plug-in has been designed to automate the entire lifecycle of device configuration management. The process of changing configurations, managing changes, ensuring compliance and security are all automated. The NCM plug-in would prove to be powerful at the hands of network administrators.

Industry best practices such as Cisco's 'Gold Standard' (which explains the recommended security settings for Cisco devices) and Government and other regulations such as HIPAA, Sarbanes-Oxley, EPHI, GLBA, PCI Data Security Requirements etc. prescribe a lot of 'best practices'. By complying to the best practices and compliance policies, enterprises can avoid most of the network security issues.



By leveraging NCM-plug-in, administrators can automate the entire compliance monitoring process at all levels - on demand, automatically at regular intervals and whenever a change happens. Violations would immediately be escalated to the security personnel. Besides, comprehensive compliance reports could be generated for submission to compliance auditors. In addition, in the case of violations, remediation tips will also be offered.

NCM plug-in will also help putting in place both proactive and reactive configuration management strategies. Proactively, administrators can reduce manual errors and prevent unauthorized changes; when something goes wrong, they can react to the contingency within minutes by getting to the root cause or by rolling-back to the previous working version.

Automating Network Configuration Management will not only help Networks remain compliant to the policies, but also make the network remain in top shape. Compliance to best practices will just become a way of life.

Conclusion

Lack of efficient and effective device configuration management affects the business continuity of enterprises. Manual configuration of devices eats away the time and efforts of the skilled administrators, who are struggling to keep track of configuration changes. Increasing security threats and government regulations force enterprises to comply to standard practices and policies.

OpManager NCM Plug-in infuses configuration management capabilities to OpManager's fault and performance management and brings in a complete Network Management solution. NCM plug-in enables network administrators to take total control of the entire life cycle of device configuration management. Changing configurations, managing changes, ensuring compliance and security are all automated. These solutions improve efficiency, enhance productivity, help save time, cost and resources and minimize human errors and network downtime.

OpManager and NCM Plug-in together make Network Management not only efficient, but also truly centralized. From a single console, you will be able to monitor network performance, identify performance bottlenecks and take total control of device configurations.

With OpManager NCM plug-in in place, enterprises can make best use of their network infrastructure. They can achieve increased network uptime and reduced degradation and performance issues.

ManageEngine
Powering IT ahead

A Division of ZOHO Corp. (formerly AdventNet Inc.)
Phone: +1-925-924-9500 **Website:** http://www.opmanager.com
For Queries: deviceexpert-support@manageengine.com