CiscoWorks Network Compliance Manager 1.5

CiscoWorks Network Compliance Manager (NCM) tracks and regulates configuration and software changes throughout a multivendor network infrastructure. It provides superior visibility into network changes and can track compliance with a broad variety of regulatory, IT, corporate governance, and technology requirements. NCM helps IT staff identify and correct trends that could lead to problems such as network instability and service interruption.

Product Overview

Enterprises seeking to facilitate high performance business applications increasingly rely on sophisticated networking infrastructure and the power of new technologies. Network operations and security managers rely on systems that can automate network deployments, handle large and complex topologies, and track and audit how actual network deployments comply with design requirements and best practices. Enterprise networks must comply with regulatory policies, corporate IT methodologies, and technology best practices—independently of scale, networking technologies deployed, and the combination of vendors providing networking equipment. NCM helps users meet regulatory compliance goals and enforce internal IT best practices.

Network Lifecycle Automation

NCM automates the complete operational lifecycle of network devices, which includes:

- Discover and track: Includes discovering and cataloging the network, visualizing the Layer 2 and Layer 3 network topology, initial device turn-up, and creating initial snapshots of device configurations
- Change and configure: Includes creating and deploying configuration changes in a structured manner, such as using configuration templates or scripts, peer reviewing and approving proposed changes, and maintaining an archive of previous configurations
- Audit and enforce: Includes defining compliance policies for your network devices, detecting violations in real time, and autoremediating problems.
- Maintain and support: Includes providing reports on device inventory, change activity, and compliance.

Enforce Policies, Standardize Operations, and Meet Compliance

Bringing networks into compliance with corporate or regulatory standards is a nontrivial, labor-intensive, error-prone, and difficult task. NCM helps you meet compliance standards through a 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.

Built-in best practices immediately measure network compliance against industry-accepted best practices. NCM incorporates policies such as the National Security Agency (NSA) router configuration guidelines.

Predefined reports for Information Technology Infrastructure Library (ITIL), the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry (PCI) standard, and other regulations offer immediate insight into network compliance. These reports provide the metrics that each of these regulations or processes requires, increasing visibility and saving auditors and network engineers time.

Prevent Network Downtime and Increase Stability

Peer reviews can reduce the number of configuration defects in a network. NCM automates peer reviews, ticketing, and approval processes to reduce the time between approving a configuration change and implementing it on your network.

New Features in CiscoWorks NCM 1.5

NCM 1.5 includes the following new features:

- **Virtual device and virtual context support:** NCM now provides support for virtual devices, including VMware's Virtual Switch (vSwitch) technology available through VMware's Infrastructure (ESX) and the Cisco® Nexus 1000v Series switches. These new virtual devices can be managed alongside legacy devices, providing centralized support. Virtual devices, as well as devices that support virtual contexts, now benefit from device relationship enhancements that provide management of non-IP addressed contexts, as well as views of the underlying relationships between the actual hardware and virtual contexts.
- **Enhanced relationship modeling:** Devices may have relationships with other devices or contained modules that run an independent operating system—complete with a full configuration and interfaces. NCM 1.5 distinguishes relationship types including both user-defined and system-defined relationships.
- **Enhanced task scheduling:** Two key task management features, task prioritization and round-robin execution of group tasks, have been implemented to improve the execution order of tasks.
- **Enhanced Device Selector and Device Group Explorer:** With the enhanced Device Selector and Device Group Explorer you can easily navigate group trees to select devices and device groups for a variety of use cases.
- **Enhanced VLAN support:** NCM now provides functionalities necessary to view fully and to provision VLANs on network switches from different vendors.
- **Link aggregation support:** Using link aggregation support, NCM can list all of the links (or connections) associated with a specific port on a device. This information is gleaned from enhanced diagnostics or from new device context information. Link aggregation lets you manage a device with virtual contexts that assign multiple connections to a physical port.
- **Provisioning and scripting API enhancements:** You can now list device templates, show device template configurations, modify device template configurations, and provision devices using the Device Relationships API.
- **Solaris 64-bit support:** When installing NCM on a Solaris platform, NCM uses the 64-bit Java Virtual Machine (JVM). As a result, NCM can utilize more memory and achieve enhanced scalability and performance.
- **Caching improvements:** Caching improvements increase performance of many functions across the NCM product. Minimizing redundant data lookups such as driver lookup and device lookup while using memory more efficiently on both 32-bit and 64-bit systems have been implemented.
- **Driver-defined diagnostics:** Driver-defined diagnostics allow drivers to specify the set of diagnostics that are "standard" for that driver and define new basic diagnostics that the system will treat as "built in." The ability to define "standard" diagnostics for a device will allow more up-to-date diagnostic implementations for any given device.

Table 1 provides a summary of the key CiscoWorks NCM features, along with a description of each feature and its benefits.

Table 1. CiscoWorks NCM Features and Descriptions

Feature	Description/Benefit
Network lifecycle management	NCM delivers a complete management and automation solution to support the full lifecycle of your network.
Process-powered automation	Using integrated, single-source software, automate IT workflows for otherwise manual processes, accomplished primarily through complex scripting.
Real-time configuration and asset tracking	In real time, detect configuration and asset information changes made across a multivendor device network, regardless of how each change is made.
Compliance control	Perform rapid troubleshooting and manage network compliance by comparing devices to well-defined, best-practice standards. Control noncompliance with automatic remediation of devices that violate standards. Speed internal and external audit processes with predefined network compliance reports for ITIL, SOX, HIPAA, PCI DSS, and more. Validate device operating states in real time to stay in compliance.
Diagramming and visualization, including Layer 2 and Layer 3 modeling	Generate a graphical representation of your network. Identify which devices are inactive or out of compliance. Use filters to immediately view isolated specific network segments. Capture a snapshot of the current state of the network, including topology and virtual LAN (VLAN) information. Identify the hosts connected to specific switches or interfaces by MAC address.
Automated software image management	Update device images and feature sets quickly, reliably, and easily.
Real-time audit trail	In real time, store a complete audit trail of configuration changes (hardware and software) made to network devices, including critical change information.
Role-based access control	Configure granular, customizable user roles to control permissions on device views, device actions, and system actions. Support common authentication systems, such as TACACS+, RADIUS, SecurID, Active Directory, and Lightweight Directory Access Protocol (LDAP).
Template-based device provisioning	Automate routine configuration tasks for updates, such as password or community string changes. Reduce the time needed to build automation scripts and increase accuracy with auto-generated scripts derived from device sessions.
Automated software synchronization and image management	Create a repository, and synchronize all device software images across your enterprise network. Use image management to automatically identify, download, and install the recommended software image for your network devices.
Automation engine	Create complex automation flows, integrating internal and third-party systems. Make use of more than 200 system triggers to drive automation.
Workflow and approvals	Enforce change processes in real time. Model complex approval processes with flexible rules. Force approvals for changes, including changes made by a direct command-line interface (CLI) session. Combine multiple tasks into a project workflow to determine whether the system should proceed to the next step.
High availability and satellite deployments	Implement high availability and disaster-recovery solutions with the high availability and satellite deployments. Administrators can effectively manage geographically dispersed networks without a single point of failure. Satellites help deal with devices located behind a firewall or handle overlapping IP address situations.
Horizontal scalability	The horizontal scalability feature offers you added flexibility in how you can grow capacity while controlling software and hardware costs.
Browser-based GUI	NCM uses a browser-based GUI and as such does not require any dedicated client software. The GUI is highly intuitive and responsive, so you can accomplish tasks quickly and efficiently.

Table 2 lists the minimum server and technical requirements for NCM.

Table 2. NCM Server Requirements and Technical Specifications

Component	Requirement
Server operating system	One of the following: • Microsoft Windows 2003 (with Service Pack 2) • Sun Microsystems Solaris 10 (SPARC) • Red Hat Enterprise Linux AS 4 (32-bit or 64-bit) • Red Hat Enterprise Linux AP 5 (64-bit) • SuSE Enterprise Linux Server 10.x
Database	One of the following: • Oracle 10g (10.2.0.2 and 10.2.0.4) Standard Edition (Enterprise Edition required for distributed system environment) • Microsoft SQL Server 2005 Standard and Enterprise Edition • MySQL 5.0.58 (included with NCM)

Application server hardware requirements	• CPU: Intel Xeon or equivalent, 3.0+ GHz (Windows, Linux), Dual UltraSparc IIIi+, 1.3 GHz (Solaris) • Memory: 4 GB RAM • Swap Space: 4 GB • Disk: 40 GB, Fast SCSI • Network: 100 Mbps Fast Ethernet, full duplex
Database server	• CPU: Intel Xeon or equivalent, 3.0+ GHz • Memory: 4 GB RAM • Swap Space: 4 GB • Disk: 60 to 100 GB, Single Channel RAID, Fast SCSI • Network: 100 Mbps Fast Ethernet, full duplex
Virtual environments (optional)	• VMware ESX 3.5 or 4.0 or • Solaris Zones

For more information on NCM 1.5 hardware and software requirements, refer to the CiscoWorks NCM 1.5 Installation and Configuration Guide at http://www.cisco.com/go/cwncm.

NCM Alert Center

CiscoWorks NCM Alert Center is an optional subscription service that provides your NCM application with the latest set of the compliance policies based on device-vendor announced security vulnerabilities. As new security vulnerabilities are found, Alert Center will deliver these vulnerabilities to the NCM server in the form of actionable compliance policies to allow you to quickly identify all vulnerable devices on your network and rapidly remediate them before hackers can compromise their security.

PACE 2.0

CiscoWorks NCM 1.5 includes Cisco Proactive Automation of Change Execution (PACE) version 2.0. PACE 2.0 is a unique bundle of tools, capabilities, and integration points that enhance the value offered by PACE solution products such as NCM.

The PACE Portal is a web-based application that integrates data from multiple components within PACE (NCM, CiscoWorks LAN Management Solution [LMS], and CiscoWorks QoS Policy Manager [QPM]) and provides rapid access to the most relevant information and features from the underlying PACE products.

PACE components include a suite of value-added capabilities for NCM users. These capabilities include integration points between NCM and other PACE products, as well as new software tools:

- Cisco PACE Syslog Analyzer offers highly scalable syslog collection and real-time monitoring of network alerts.
- A software adapter for NCM automatically notifies QPM when configuration changes are detected, thereby allowing QPM to validate quality of service (QoS) policies changes.
- End of sale/end of life reports help protect the network by ensuring that only actively supported device hardware and software versions are deployed.

NCM Collaboration Portal

A new collaboration portal is available for the NCM user community at https://networkautomation.itorigin.net. This portal provides a wealth of information about NCM such as detailed training material, archived Video on Demands (VODs), discussion forums, NCM virtual machines, and other useful information.

Evaluation and Ordering Information

NCM 1.5 can be ordered through regular sales channels. NCM 1.5 is also available for evaluation at http://www.cisco.com/go/nmsevals

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, see Cisco Technical Support Services or Cisco Advanced Services.

For More Information

For more information about NCM, please visit http://www.cisco.com/go/cwncm, contact your local account representative, or send an email to ask-ncm-pm@cisco.com. For more information about PACE, please visit http://www.cisco.com/go/pace.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-573740-00 12/09