

Maintaining network compliance in the face of change

Ensuring that policies are enforced using IBM Tivoli Netcool Configuration Manager



Highlights

- Monitor policies and receive alerts of changes that threaten compliance status
 - Provide intelligent remediation when a change takes the network or a device out of compliance
 - Integrate with other Tivoli solutions to identify non-compliant changes and assess impact
-

Despite the importance of regulatory compliance, most organizations lack the ability to automatically and intelligently monitor and enforce the policies that enable their networks to meet standards. Once policies are established, their status must be constantly checked, unauthorized and incorrect changes must be prevented, and alerts must be issued when compliance is not maintained. Even policies governing routine actions such as updates to passwords require regular attention. Failure to ensure compliance with properly managed policies can incur consequences that range from fines or other regulatory agency penalties to increased network downtime, vulnerability in network security, lost productivity, higher cost in network operations and other overhead associated with compliance.

Enforcing compliance policies can be a challenge in complex, dynamic, multivendor environments. But careful and effective enforcement is necessary when even a single configuration error can jeopardize the entire network's compliance status or open it to a security breach.

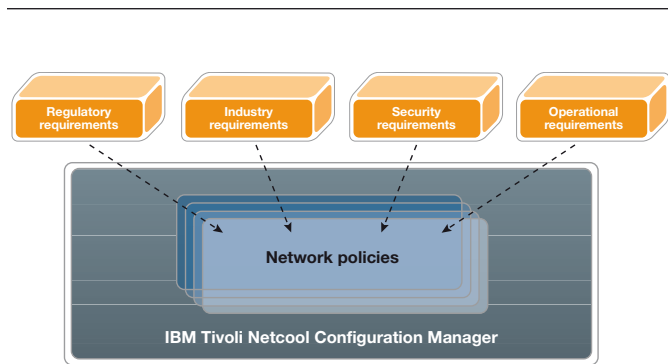
IBM Tivoli® Netcool® Configuration Manager delivers capabilities that take policy management for network compliance to a new level. Its advanced business logic provides key capabilities for enabling large enterprise and service provider environments—with their complex, heterogeneous, frequently changing networks and their strict needs for high availability and security—to meet regulatory, industry, security and operational requirements.

Tivoli Netcool Configuration Manager is a comprehensive network solution designed to define and manage policies, continually validate device configurations, alert users when policies have been or are about to be violated as a result of a change or potential change,



and intelligently remediate non-compliant conditions. Eliminating the unreliability of error-prone manual configuration solutions, Tivoli Netcool Configuration Manager automates the network compliance life cycle to define policies, validate devices against policies, resolve violations and report results in a continuous and closed-loop manner.

It provides auditing and enforcement for a wide variety of regulatory, industry, security and operational compliance requirements—including the Sarbanes-Oxley Act (SOX), European Union Safe Harbor regulations, the Payment Card Industry (PCI) Data Security Standard (DSS) and the Health Insurance Portability and Accountability Act (HIPAA)—as they pertain to networks.



Tivoli Netcool Configuration Manager can automatically ensure that network policies remain compliant with requirements from a number of sources.

Integration with Tivoli solutions enables a proactive response

For organizations required to comply with industry or government standards, establishing policies is only the first step. They also need to establish processes that make sure their policies are followed. These processes must enforce compliance for policies and the areas they govern, and they must correct non-compliance on an ongoing basis.

The most effective techniques include automated processes that are integrated with the organization's change management solution, its trouble ticketing system and its fault management system. Without integration, it's not possible to correlate a policy violation with the change that caused it. Without integration, an alert can be stranded on a dashboard or in an inbox and the non-compliant status may not be corrected.

Tivoli Netcool Configuration Manager integrates its change and policy management capabilities out of the box with IBM Tivoli Netcool/OMNIBus operations management software, which consolidates IT and network operation management tasks. This integration enables users to act as soon as change occurs that violates policy, assessing the impact and correcting the issue without waiting to receive a trouble ticket.

The solution also enables flexibility in the ways it validates policies. Users can use interrogation commands to validate against a database or data retrieved real time, using device-specific policy definition. They can validate against native configurations, building validation with blocks of text or multiple configuration snippets. Or they can use the SmartModels™ feature built into Tivoli Netcool Configuration Manager, which creates technology-independent configuration definitions and provides an XML-based, point-and-click interface to focus compliance validations.

Effective management addresses the full range of challenges

Traditional network compliance solutions are often script-based and narrowly focused on regulatory or security compliance. They can ignore the need for holistic and comprehensive network compliance—and as a result, they often do not support all business requirements as they pertain to networks.

Traditional network compliance solutions also do not have the intelligence, flexibility or scalability to address the complex requirements of enterprise and carrier-class networks. They take a top-down approach to compliance, in which policies are put into practice across the network. Delivering effective network compliance, however, requires a thorough bottom-up analysis that is based on the real-time state of the network devices and the impact of changes on network integrity. An effective approach to policy management—like the approach provided by Tivoli Netcool Configuration Manager—addresses a full range of issues.

Reduce regulatory and industry compliance overhead

Enterprises face a plethora of regulatory and industry compliance audits and costs. Some result from legislative initiatives such as SOX in the United States and Safe Harbor in the European Union. Others are responses to industry mandates such as PCI DSS, which requires conformity by networks supporting credit or debit card transactions. Regardless of the cause, they add complexity to network operations. Organizations need solutions that can efficiently manage audits and reduce their associated overhead.

Maximize network availability and business continuity

Compliance regulations typically require high levels of network availability and business continuity. But device misconfiguration and other errors that violate policies during network change can lead to disruptions that negatively impact business operations and the ability to maintain compliance. Organizations need solutions that support policies to ensure accurate network configuration and continued compliance in the face of change.

Eliminate network security risks

Security vulnerabilities and violations can expose enterprises and carrier networks to devastating consequences—both in their business operations and their ability to comply with

regulations. To avoid exposure, organizations need solutions that support continual steps to eliminate security breaches caused by policy errors so that sensitive customer information is not compromised, compliance remains intact and the company's brand image is not damaged.

Lower operational costs, increase efficiency and reduce disruptions

Manual processes and script-based solutions are unreliable and cannot scale to meet the operational requirements of today's enterprise networks. These networks can be highly complex, with hundreds or thousands of devices from multiple vendors—and they can be highly dynamic due to frequently changing business and application demands. Organizations need a solution that can tame network complexity by following policies, minimizing operational costs, maximizing efficiencies and reducing service disruptions.

Deliver services accurately and rapidly

Communication service providers need to enable rapid and accurate provisioning of next-generation services such as IP-based television (IPTV), video on demand (VOD) or voice over IP (VoIP). They also must meet stringent service level agreements (SLAs) for their customers. However, most lack policies to ensure accurate network configuration and change management. Service providers need solutions that can manage policies in ways that reduce device misconfiguration and resulting downstream or cascading network impacts such as higher provisioning errors, breach of customer SLAs, unreliable quality of service and non-compliance.

A comprehensive solution for network compliance

Tivoli Netcool Configuration Manager is designed to meet the total compliance needs—including regulatory, industry, security and operational requirements—of the dynamic, complex and heterogeneous networks operated by today's network-driven organizations. Such needs typically include authentication policies to protect against unauthorized access

to sensitive data, audit policies to track who made what changes to the network, security policies to apply inbound anti-spoof filters, and operational policies to enable SNMP traps.

Based on networking expertise and a deep understanding of network devices, the policy enforcement capabilities of Tivoli Netcool Configuration Manager support a compliance management solution for a new generation of needs. It embodies the flexibility and scalability required to maintain high network availability and reliable service delivery. It provides an effective way for network organizations to gain greater control of network resources in a dynamic and complex environment. At the same time, it enables timely access to critical network compliance information for business units across the organization.

Key functions of Tivoli Netcool Configuration Manager

- Helps fulfill the regulatory, industry, security and operational compliance requirements of network-driven organizations
 - Enables a closed-loop process to support the entire compliance life cycle, from policy creation through correlation with network configuration to the compliance validation and detection of violations, as well as monitoring and reporting of policies
 - Enforces device-specific and network-wide compliance policies regardless of vendor, type, model or operating system
 - Supports a large combination of network compliance policies and devices, from a few hundred to tens of thousands
 - Utilizes intelligent remediation to effectively resolve out-of-compliance device conditions on an ad-hoc, scheduled or automatic basis
 - Delivers comprehensive reports for executives, compliance departments, security teams, business units, network engineering and network operations, showing point-in-time and historical data regarding policies and compliance as well as trends for auditing purposes
 - Provides flexible integration points to help integrate with third-party business and operational applications
-

A closed-loop process for compliance management

Tivoli Netcool Configuration Manager delivers functions for managing the entire policy management and compliance life cycle within an ongoing, closed-loop process that defines compliance policies, runs policy validations on the active network configuration, provides automated or user-driven resolution of policy violations, and provides reports for audit and business purposes. These functions include the following capabilities:

- Compliance unbound: Defining policies
 - Supports a unique range and combination of compliance policies
 - Enables policies to capture a large variety of rules and standards
 - Fosters reuse of existing policies through parameter management
 - Incorporates a drag-and-drop, easy-to-use interface for rapid policy creation
 - Provides out-of-the-box policies, for example, NSA router guidelines
- “Always on” compliance: Validating devices against policies
 - Validates against any device type
 - Supports more than one million validations per hour
 - Enables scheduled, ad-hoc and automatic policy validation
- Intelligent remediation: Resolving policy and compliance violations
 - Applies corrective actions automatically or through user intervention
 - Allows corrective actions to be based on the type of violation, historical compliance status of the device and other user-defined parameters
 - Supports policy and compliance exemptions and avoids unnecessary alarms
- Audit readiness: Generating compliance reports for audit purposes
 - Publishes a variety of standard reports for auditing and business purposes
 - Enables dedicated reports for both business and technical audiences

Highly scalable solutions for network-driven organizations

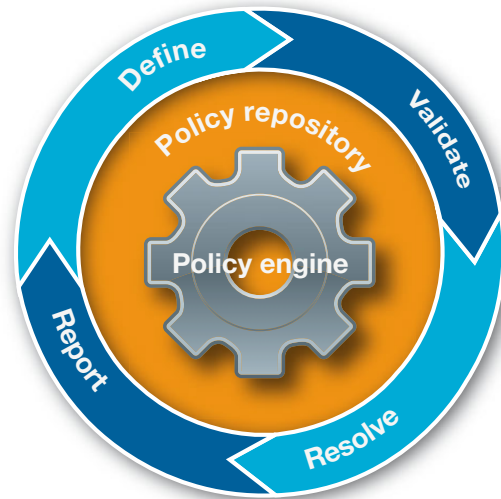
The policy management and compliance capabilities of Tivoli Netcool Configuration Manager have been specifically designed for the demanding needs of network-driven organizations and very large, complex networks. These functions manage the inherent network complexity of such environments while helping to balance the competing demands of absolute compliance and business continuity.

Recognizing that the status of compliance policies frequently changes, they support dynamic compliance at multiple levels and allow policies to be adapted as business needs evolve.

The software also provides an actionable solution for effective collaboration between those responsible for articulating policy and compliance requirements (such as executives, line-of-business managers, and compliance and security officers) and those responsible for implementing those policies (such as network and IT professionals).

Integration across platforms and management systems

Tivoli Netcool Configuration Manager is an open-architecture solution designed to facilitate integration with third-party business and operational applications. It operates on a variety of platforms including UNIX® and Linux® to serve as an abstraction layer for the underlying network by translating device configuration information into standardized device models and by storing application data,



Tivoli Netcool Configuration Manager supports the full policy life cycle.

compliance definitions and historical policy validation information in a relational database. The resulting network views provide a single control plane for making changes to network devices in a consistent manner, continuously maintaining the real-time state of the network, ensuring ongoing regulatory compliance during network change, delivering a high quality of network service, and supporting network user satisfaction.

For more information

To learn more about Tivoli Netcool Configuration Manager and how it can help support your network compliance efforts, contact your IBM sales representative or IBM Business Partner, or visit ibm.com/software/tivoli/welcome/netcool

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT life-cycle management, and is backed by world-class IBM services, support and research.

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: ibm.com/financing

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.



© Copyright IBM Corporation 2010

IBM Corporation Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
September 2010
All Rights Reserved

IBM, the IBM logo, ibm.com, Netcool and Tivoli are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

No part of this document may be reproduced or transmitted in any form without written permission from IBM Corporation.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information provided in this document is distributed "as is" without any warranty, either express or implied. IBM expressly disclaims any warranties of merchantability, fitness for a particular purpose or noninfringement. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.



Please Recycle