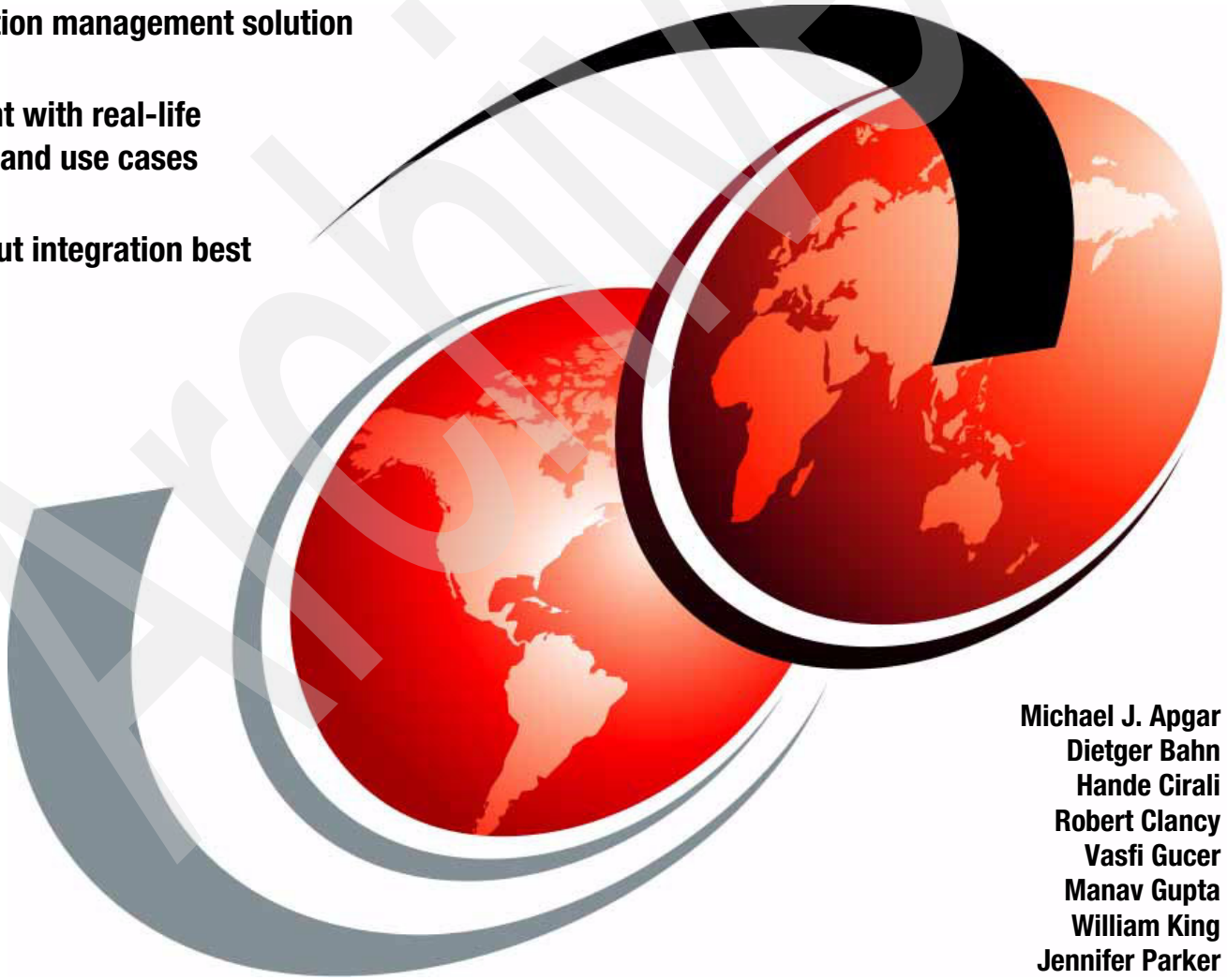
Tivoli software

IBM

# Integration Guide for IBM Tivoli Netcool/OMNIbus, IBM Tivoli Network Manager, and IBM Tivoli Netcool Configuration Manager

- Implement an integrated network and configuration management solution
- Experiment with real-life scenarios and use cases
- Learn about integration best practices




Michael J. Apgar
Dietger Bahn
Hande Cirali
Robert Clancy
Vasfi Gucer
Manav Gupta
William King
Jennifer Parker




Redbooks

ibm.com/redbooks

International Technical Support Organization

# Integration Guide for IBM Tivoli Netcool/OMNIbus, IBM Tivoli Network Manager, and IBM Tivoli Netcool Configuration Manager

October 2010



SG24-7893-00

**Note:** Before using this information and the product it supports, read the information in “Notices” on page vii.



**First Edition (October 2010)**

This edition applies to IBM Tivoli Netcool/OMNIbus Version 7.3, IBM Tivoli Netcool Configuration Manager Version 3.8, and IBM Tivoli Netcool Configuration Manager Version 6.1

# Contents

# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
*IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

# Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US 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 http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

| | | |
|---|---|---|
| IBM® | Netcool® | Redbooks (logo) ® |
| Micromuse® | Redbooks® | Tivoli® |

The following terms are trademarks of other companies:

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Windows, and the Windows logo are trademarks of Microsoft Corporation 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, or service names may be trademarks or service marks of others.

# Preface

This IBM® Redbooks® publication covers the integration scenarios for IBM Tivoli® Network Manager, IBM Tivoli Netcool/OMNIbus, and IBM Tivoli Netcool® Configuration Manager. These three products working together provide a comprehensive solution for network and event management, and network configuration management, within the context of service availability and performance management.

Tivoli Network Manager and Tivoli Netcool/OMNIbus are long established products in the IBM portfolio. Tivoli Netcool Configuration Manager (from the Intellident acquisition) is a new product in the portfolio and provides a comprehensive network configuration and change management solution and a policy-based network compliance solution for managing network devices in complex, rapidly changing environments.

This book describes practical examples and use cases where these products work together to address network configuration management and event management requirements.

IT architects and IT specialists working on integrating these Tivoli products in real life environments will benefit from this book.

## The team who wrote this book

This book was produced by a team of specialists from around the world working at the IBM South Bank Office in London, UK.

**Michael J. Apgar** works for IBM Software Group, Tivoli Division in Colorado Springs, Colorado, USA. As part of the Intellident acquisition, he brings 5 years of experience with Tivoli Netcool Configuration Manager. He has worked at providing project management and deployment support for various customers, including many customers in the telecommunications sector. He has a varied information technology career in the areas of project management, consulting, and development in multiple industries. He has a Bachelor of Science degree in Finance from Montana State University. He has the Project Management Professional (PMP) certification from the Project Management Institute.

**Dietger Bahn** is a IT Specialist working for IBM Software Services for Tivoli in Germany who specializes in Network Management solutions. His areas of expertise includes several comprehensive customer projects in the IBM Tivoli Netcool product portfolio. He has over ten years of experience in Service Availability and Performance Management, and technical administration of UNIX® operating systems, including high availability environments. He worked three years as a Support Specialist at the IBM EMEA Techline for IBM Tivoli solutions. Before joining IBM, he worked for seven years as an IT Specialist for UNIX systems. Dietger is ITIL® certified and continuative qualified in service-oriented troubleshooting.

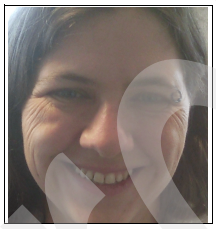
**Hande Cirali** is an Advisory IT Specialist working for IBM Software Services for Tivoli (SST) in Turkey. She has four years of experience with Tivoli products focusing on design and implementation of monitoring and network management solutions. Hande has a Bachelor of Science degree in Electrical and Electronics Engineering from Middle East Technical University. She holds two Master of Science degrees in Information Technologies Service Management from Bahcesehir University and Project Management from Northeastern University.

**Robert Clancy** works for IBM Software Group, Tivoli Netcool Business Automation as a Technical Professional, and currently provides technical pre-sales and post-sales support for customers and sales teams for the Tivoli Netcool suite of products, with specific focus on Tivoli Network Manager IP, Tivoli Netcool/OMNIbus, and Tivoli Business Service Manager. He has a broad range of experience in the Tivoli Netcool product set and technologies, and has created a number of proof of technologies for the Tivoli Netcool suite of products. He is IBM Certified for Tivoli Network Manager IP.

**Vasfi Gucer** is a Project Leader at the International Technical Support Organization, Austin Center. He has been with the ITSO since January 1999. He has more than 12 years of experience in the areas of systems management, networking hardware, and software on mainframe and distributed platforms. He has worked on various IBM Tivoli client projects as a Systems Architect in the USA. He writes extensively and teaches IBM classes worldwide on Tivoli software. Vasfi is also an IBM Certified Senior IT Specialist, PMP, and ITIL Expert.

**Manav Gupta** works for IBM Software Group, Tivoli Division, as a Service Management Solution Architect, designing Service Management solutions for General Business customers in UKI. He has a Bachelor of Science degree in Math from MDS University, India. Manav joined IBM via the acquisition of Micromuse®, and has a broad range of experience with Tivoli products, specifically with the Tivoli Netcool suite of products. Prior to his current job, Manav worked in SWG Lab Services as a Principal Consultant, deploying fault and performance management solutions for customers in Europe, the UK, the Middle East, and Canada. Manav is Certified IT Specialist and ITIL Certified IT Service Manager, and has a small but growing patent portfolio.

**William King** works for IBM Software Group, Tivoli Division, as part of the ITNM-IP SQA team. His primary role is as a network engineer developing and managing the test networks used by the ITNM-IP development and SQA teams. As a former Micromuse employee, he has been working on the Tivoli Netcool suite of products for almost 10 years. He is familiar with a range of different network equipment from Cisco, Juniper, Huawei, Nortel, Brocade and Extreme, creating test environments containing, for example, MPLS VPNs, BGP, Multicast and IPv6 protocols. He has a PhD in Immunology from Birmingham University.



**Jennifer Parker** works for IBM Software Group, Tivoli Division, for Tivoli Netcool products. She is a senior L2 engineer supporting IBM Tivoli Network Manager. She has worked for IBM for 11 years in varying roles, at varying locations, and with varying products. She is an IBM Certified Deployment Professional for IBM Tivoli Network Manager.

Thanks to the following people for their contributions to this project:

Tamikia Barrow, Leslie Parham, Alfred Schwab, Wade Wallace
**International Technical Support Organization**

Dave Mohally
**IBM Ireland**

Tina Anderson, Matthew Duggan, Amy Heimann, Andrew Hepburn, Trevor Graham, Verity Greig, Amardeep Kalsi, Bhrat Patel, Stephen Quin, Nicholas Smyth, Emma Thompson
**IBM UK**

Nick Abbott, Bill Davis, Jay Davis, Christopher Haynes, Danna Rother, Steven Shuman, Dave Thompson
**IBM US**

## Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author - all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

**ibm.com**/redbooks/residencies.html

## Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  **ibm.com**/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

## Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

# IBM Network Management solutions

In this chapter, we introduce the IBM solutions for network management within the context of service availability. IBM Tivoli Network Manager, IBM Tivoli Netcool/OMNIbus, and IBM Tivoli Netcool Configuration Manager make up these solutions.

**Note:** These products will be referred as Tivoli Network Manager, Tivoli Netcool/OMNIbus, and Tivoli Netcool Configuration Manager respectively throughout this document.

By integrating Tivoli Netcool Configuration Manager with Tivoli Network Manager and Tivoli Netcool/OMNIbus, you enrich the diagnostic information available to the Tivoli Network Manager and Tivoli Netcool/OMNIbus operators by adding network configuration and policy management capability. You also reduce the need to maintain separate data records and discovery processes, and increase the ability to cross-reference between network events.

This chapter describes following topics:

## 1.1 Products overview

In this section, we briefly go over the products that make up this integration.

**Note:** If you are not familiar with the network management terms, refer to “Glossary” on page 145.

### 1.1.1 IBM Tivoli Integrated Portal

Tivoli Network Manager, Tivoli Netcool/OMNIbus, and Tivoli Netcool Configuration Manager are web-based products. Web-based products built on the Tivoli Integrated Portal framework share a common user interface where you can launch applications and share information.

Tivoli Integrated Portal helps with the interaction and secure passing of data between Tivoli products through a common portal. You can launch from one application into another application and within the same dashboard view to research different aspects of your managed enterprise.

Tivoli Integrated Portal provides:

- Services to support a console for individual products and for integrating multiple products.
- Aggregated views that span server instances, such as the Tivoli Netcool/OMNIbus ObjectServer and Tivoli Network Manager.
- A web-based user interface with inter-view messaging between products so that the data in, say, a single tabulated report, can be gathered from multiple products.
- A common task navigator for multiple products that allows convenient selection by the task and not necessarily by the product you need to use to perform that task.
- An integration point for Netcool products. Products that in previous versions were running on the Netcool GUI Foundation (NGF) now use Tivoli Integrated Portal. This enables greater interoperability among products that are built on this converged platform or are compatible with it.

### 1.1.2 Tivoli Network Manager

Tivoli Network Manager provides the network analysis software that is needed to manage complex networks.

Formerly known as Netcool/Precision IP, this network diagnostics software from Tivoli collects and distributes Layer 2 and 3 network data and builds and maintains knowledge about physical and logical network connectivity.

Tivoli Network Manager provides the following capabilities:

- Provides physical, port-to-port connectivity between devices.
- Captures logical connectivity information, including virtual private network (VPN), virtual local area network (VLAN), asynchronous transfer mode (ATM), frame relay, and multiprotocol label switching (MPLS) services.
- Integrates easily with operational support systems (OSS) and other mission-critical workflow applications.

- Helps your operations personnel to quickly identify the source of network faults and to speed problem resolution with real-time root-cause analysis and network diagnostics.
- Delivers highly accurate network analysis software with real-time information about network connectivity, availability, performance, usage, and inventory information that is vital to achieving flow-through provisioning and maximum return on network assets.

The Tivoli Network Manager architecture can be divided into three layers:

- Network layer
- Data layer
- Visualization layer

The network layer interacts directly with the network. This layer contains network discovery and polling functionality. Network discovery retrieves topology data and network polling retrieves event data.

The data layer stores the topology data retrieved by network discovery and the event data retrieved by network polling. Network polling also includes storage of polled SNMP data for reporting and analysis. This layer also provides root-cause analysis functionality that correlates topology and events to determine the source of network faults, and event enrichment functionality that adds topology data to events.

The visualization layer provides the tools operators and administrators need to view topology, view events, and run network troubleshooting tools.

Figure 1-1 shows a conceptual overview of the Tivoli Network Manager functional layers.

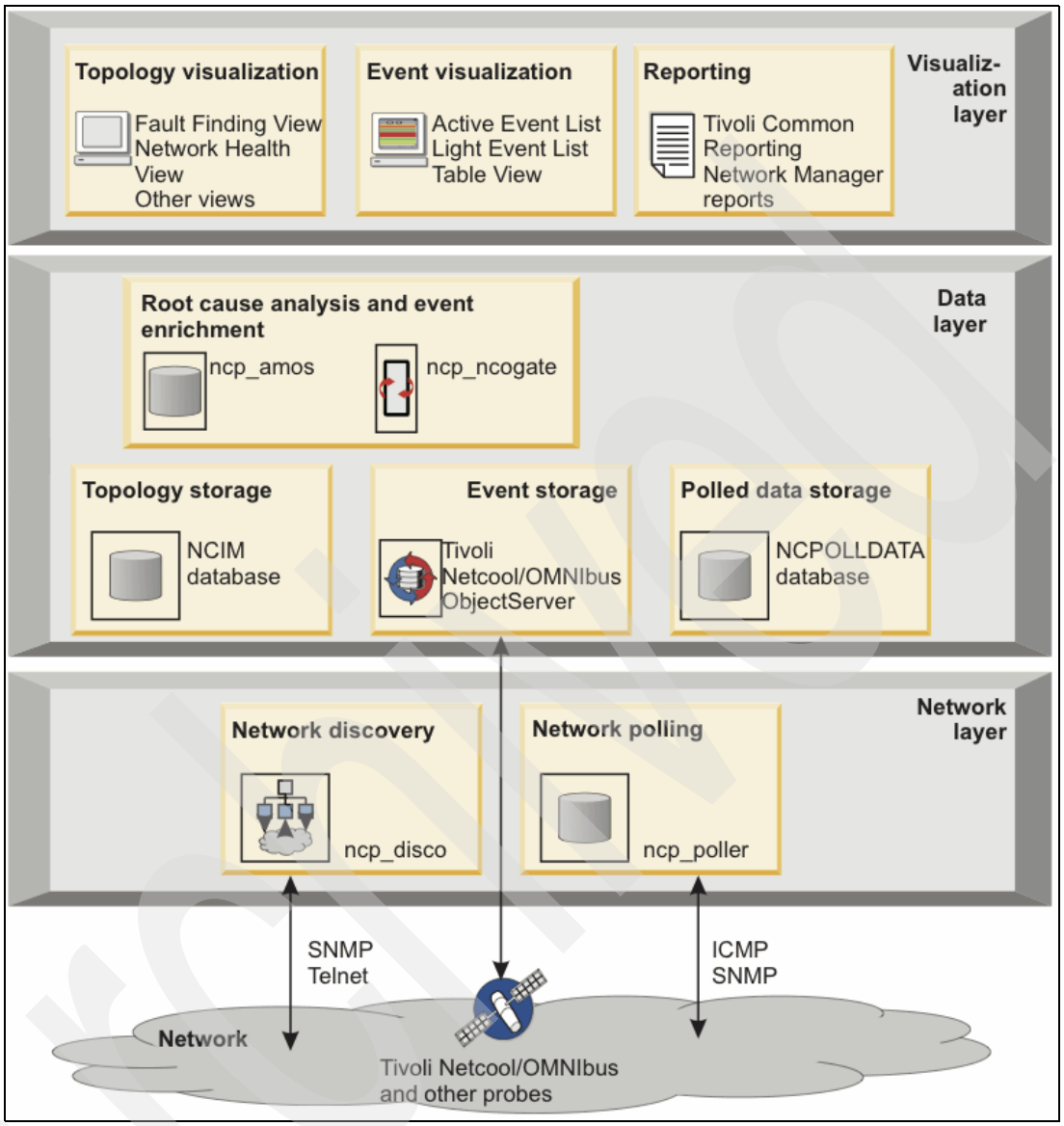



*Figure 1-1 Tivoli Network Manager functional layers*

For further details and all other related product documentation, refer to the Tivoli Network Manager documentation available at the following address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_nmip.htm

## 1.1.3 Tivoli Netcool/OMNIbus

Tivoli Netcool/OMNIbus operations management software consolidates complex IT and network operation management tasks. Tivoli Netcool/OMNIbus improves service availability and resiliency with real-time service management for data centers, network operations centers, and IT domains.

Tivoli Netcool/OMNIbus provides the following capabilities:

- Delivers a central point of real-time service management for business applications, network devices, Internet protocols, and security devices.
- Enables you to identify and resolve the most critical problems with automated event correlation, isolation, and resolution capabilities.
- Consolidates data in operational silos into real-time web dashboard views with customizable displays of events, service views, and operational indicators.
- Supports current and evolving standards and uses approved cryptographic providers to help ease security audits.
- Utilizes customizable lightweight agents to collect business and technology events from more than 1,000 sources in real time.
- Provides tight integration with the IBM Tivoli Monitoring family to measure performance and user experience with business applications and to monitor Tivoli Netcool/OMNIbus itself, generating alarms based on user-defined thresholds.
- Offers operations management software that integrates with the broader Tivoli portfolio for a single view of operations, including cross-domain correlation, and common visualization, navigation, security, and reporting and launch-in-context capabilities.

The Tivoli Netcool/OMNIbus components work together to collect and manage network event information.

The components of Tivoli Netcool/OMNIbus are:

- Probes
- Gateways
- The ObjectServer
- The Web GUI visualization component
- Desktop tools
- Administration tools

Probes send alerts to the local ObjectServer, and a gateway replicates these alerts in an additional ObjectServer in a failover configuration. Alerts that are sent to the ObjectServer can be viewed in the Active Event List in the Web GUI, or in the desktop event list. Additional gateways are also configured to forward alerts to other applications, such as a help desk or Customer Relationship Management (CRM) system, and a relational database management system (RDBMS). A Tivoli Netcool/OMNIbus administrator (and the other administration tools) can also be used to configure and manage the system.

Figure 1-2 shows an overview of the Tivoli Netcool/OMNIbus component architecture.

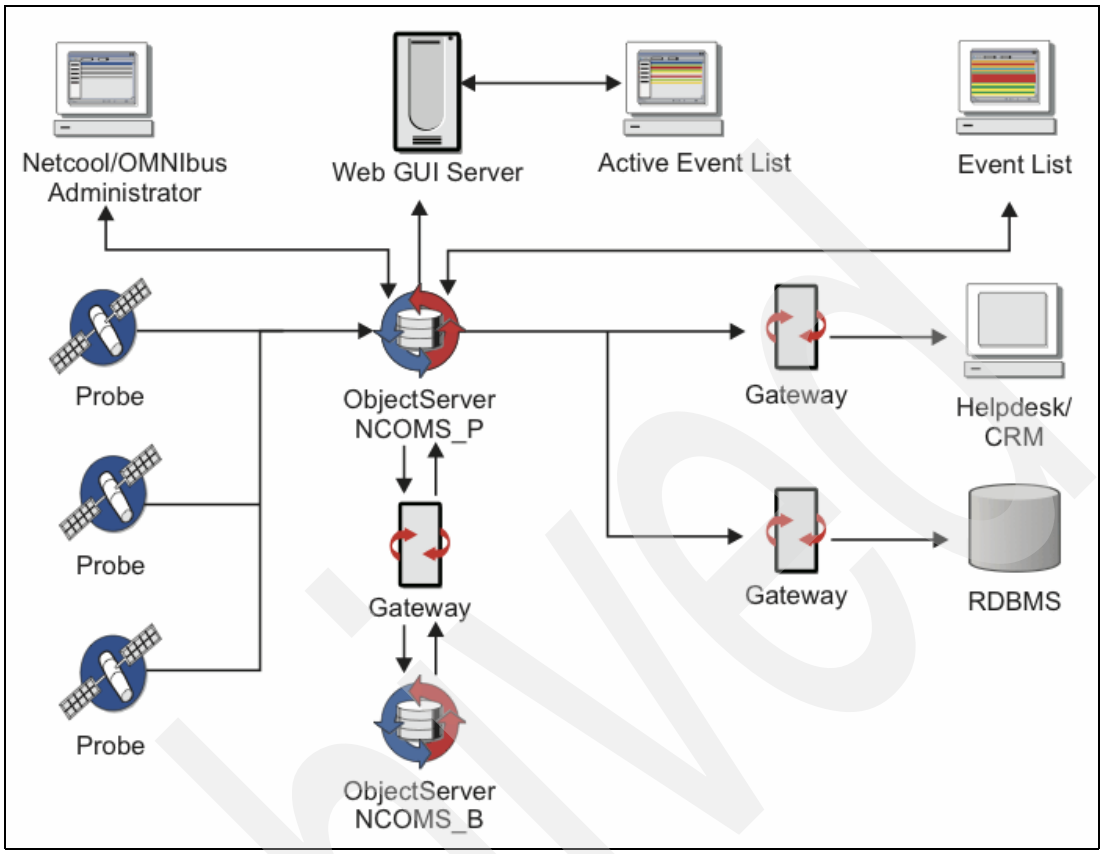



*Figure 1-2 Tivoli Netcool/OMNIbus component architecture*

For further details and all other related product documentation, refer to the Tivoli Netcool/OMNIbus documentation available at the following address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm

## 1.1.4 Tivoli Netcool Configuration Manager

Tivoli Netcool Configuration Manager provides a comprehensive network configuration and change management solution, as well as a policy-based network compliance solution for managing network devices in complex, rapidly changing environments. We briefly discuss the capabilities of the major functions of Tivoli Netcool Configuration Manager.

### Network configuration and change management

The network configuration and change management function forms the foundation for Tivoli Netcool Configuration Manager. Initially, clients load network device definitions into the application and organize these definitions into their specified categories, such as geography or function. Following the initial setup, clients can begin to manage their device configuration changes and backups through Tivoli Netcool Configuration Manager.

The following capabilities are available under the network configuration and change management function of Tivoli Netcool Configuration Manager:

- Back up device configurations dynamically or on a scheduled basis:

  The product maintains historical configuration versions as defined by the client.
- Detect out-of-band configuration changes and trigger a configuration backup.
- Apply configuration changes to device configurations:
  - You can make changes to a single device configuration.
  - You can make mass changes to multiple devices simultaneously.
  - Scheduled changes can execute during normal maintenance windows.
  - Templated changes configured and applied using command sets reduce errors that can result from manually applied changes.
- Upgrade device operating systems:

  An automated upgrade process upgrades the operating system on multiple devices.
- Access device terminals through the GUI that allows for access to devices:
  - The device terminal logs all keystrokes for a user session.
  - The device terminal allows direct access to devices by building a secure tunnel to the device.
  - The device terminal allows for automatic configuration backup following each terminal session.

## Policy-based compliance management

The policy-based compliance management function of Tivoli Netcool Configuration Manager provides a rules-based tool for checking and maintaining network device configuration compliance with various sets of policies. You can configure compliance checks to check for the presence or absence of specific commands or data in a device's configuration or a response from a query to a device. Based on the results of the compliance check, the tool either reports the results or, if desired, initiates a configuration change to bring a device back into compliance. You can organize and group related compliance checks into higher-level policies. You can schedule compliance checks to execute on a dynamic or scheduled basis. Likewise, you can set up compliance checks to trigger automatically as a result of a configuration change on a device.

The following capabilities are available in the policy-based compliance management function of Tivoli Netcool Configuration Manager:

- Policy-based compliance management uses reusable building blocks for creating compliance checks:

  **Definitions** Definitions are the lowest level component that contains the configuration data to be checked.

  **Rules** Rules are composed of definitions and the actions to take if a device configuration passes or fails.

  **Policies** Policies are composed of rules, which can be grouped together across various device types and compliance checks.

  **Processes** Processes group one or more policies to execute against a set of devices on a scheduled basis.
- The function allows you to run compliance checks in either a dynamic, scheduled, or automatically triggered manner.

- The function automatically fixes out-of-compliance device configurations to get them back in compliance.
- Policy-based compliance management allows you to configure compliance reports for automatic generation and distribution.

The Tivoli Netcool Configuration Manager architecture considers three server layers, each of which can be deployed separately across multiple machines. Each layer scales and distributes independently for maximum flexibility:

- Add presentation servers as user sessions or API transaction rate increases (optional load balancer to share client sessions across the pool of servers).
- Add worker servers as devices or work throughput rate increases.
- Add database servers to support transaction throughput for the presentation and worker layers.

The deployment architecture of Tivoli Netcool Configuration Manager, with the layers discussed above, is shown in Figure 1-3.

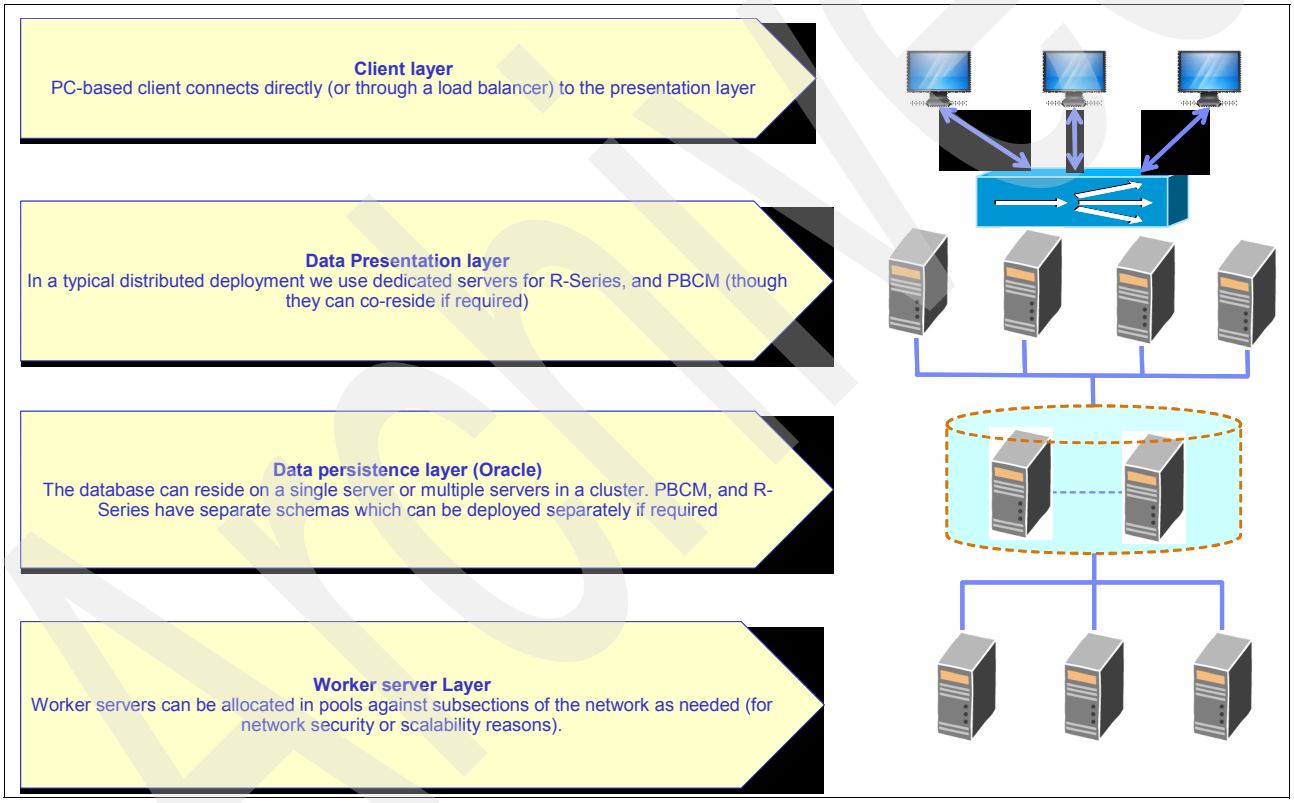



*Figure 1-3 Tivoli Netcool Configuration Manager architecture*

Figure 1-4 shows the logical architecture of Tivoli Netcool Configuration Manager.

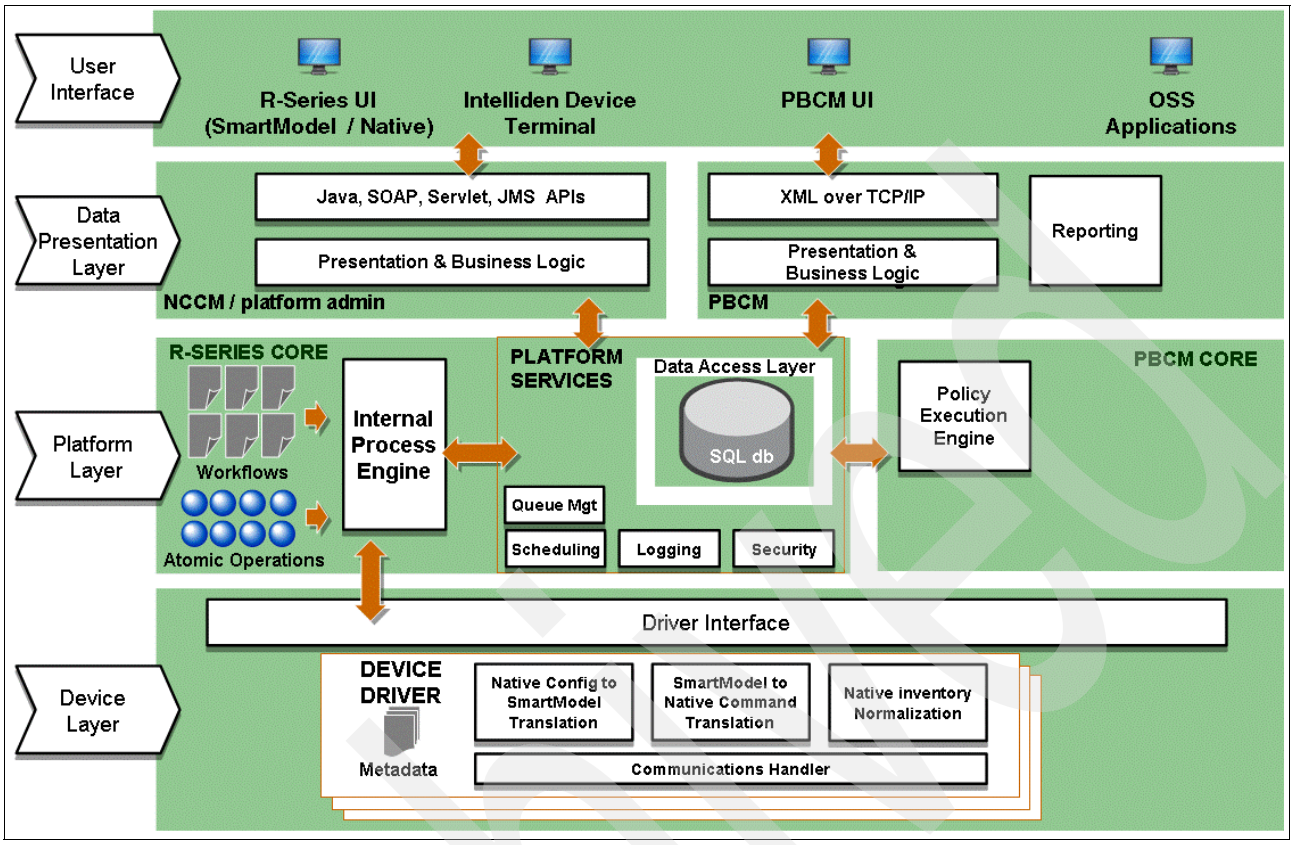



*Figure 1-4 IBM Tivoli Netcool Configuration Management logical architecture*

For further details and all other related product documentation, refer to the Tivoli Netcool/OMNIbus documentation available at the following address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_itncm.htm

**What is new in Tivoli Netcool Configuration Manager V6.1:**

If you would like to learn about what is new in Tivoli Netcool Configuration Manager V6.1, you can find a summary of new features at the following address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm/wip/common/reference/ncm_ovr_whatsnew.html

## 1.2 Benefits

The integration of Tivoli Network Manager, Tivoli Netcool/OMNIbus, and Tivoli Netcool Configuration Manager provides a closed loop network management problem resolution in one single solution.

Figure 1-5 shows the closed loop problem resolution provided by the integration of Tivoli Network Manager, Tivoli Netcool/OMNIbus, and Tivoli Netcool Configuration Manager.

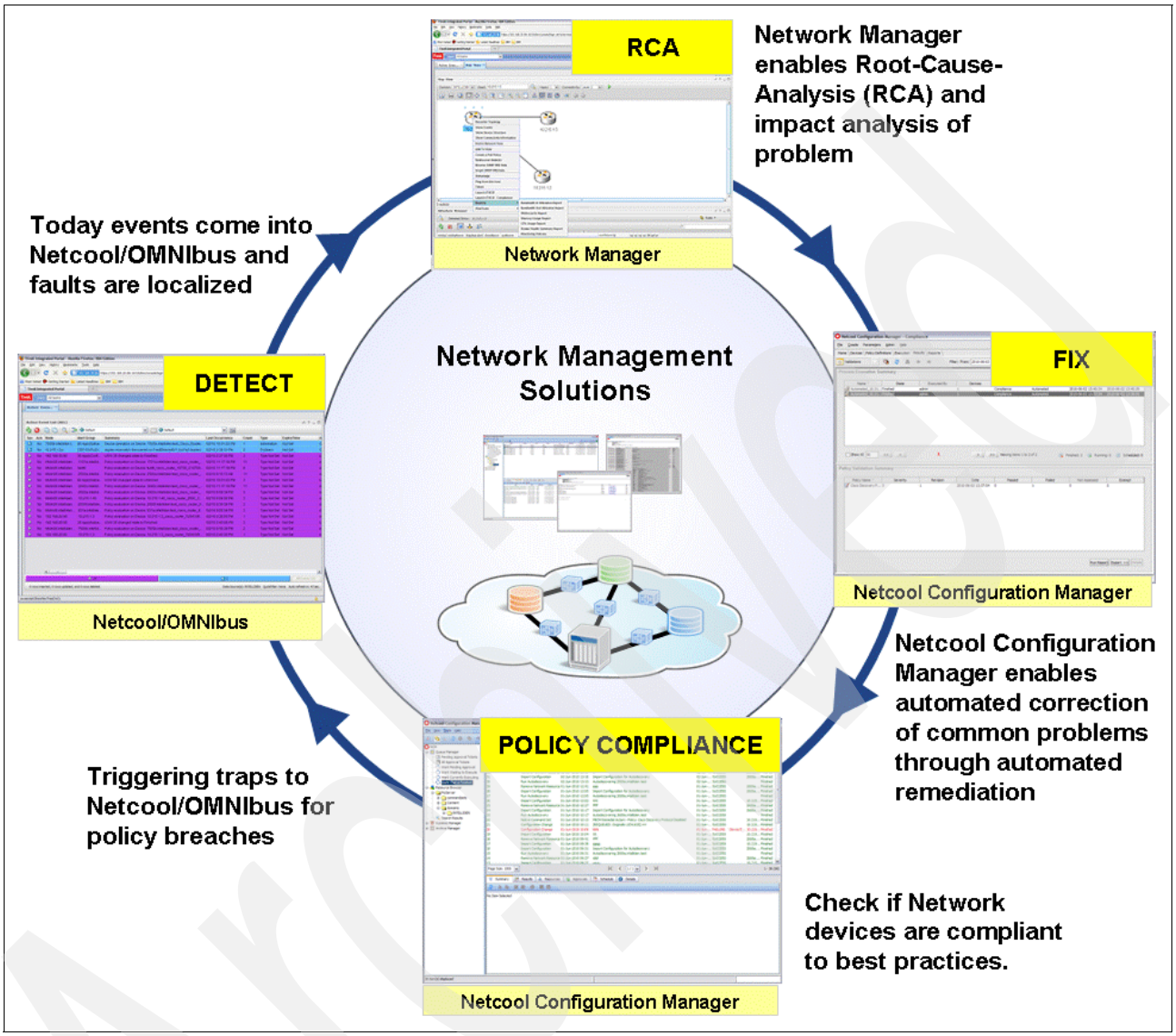



*Figure 1-5 Closed loop network management problem resolution*

The integration scenario described in this documentation provides the following benefits:

- The integration reduces inefficiencies associated with separate products to monitor different aspects of the same network. By sharing specific device information and preserving device groupings and hierarchies between Tivoli Network Manager, Tivoli Netcool/OMNIbus and Tivoli Netcool Configuration Manager, you reduce the need to run separate discoveries. The integration ensures both Tivoli Network Manager and Tivoli Netcool Configuration Manager have the same view of the network, and one that is constantly updated as the network changes. This ensures the administrators for the two products have a consistent view of network outages and enables them to isolate root cause of outages easily.
- Device configuration problems can be difficult to isolate and identify. By integrating with Tivoli Netcool Configuration Manager, a unified view of events is created that helps operators isolate the problems caused by changes to network device configuration.

- Tivoli Netcool Configuration Manager maintains a backup of network configuration, including audit trails. Accidental misconfigurations of a network device are easy to spot, isolate, and rectify, by simply rolling back the changes via Tivoli Netcool Configuration Manager.
- The integration provides the ability to implement network policies and enforce compliance by utilizing the capability of Tivoli Netcool Configuration Manager to make a change to large number of devices in one go, while ensuring the changes are accurate without manual intervention. This reduces the time to value of network management implementation

## 1.3 Integration scenarios

In this section, we provide an overview of the following integration scenarios:

- Seeding Tivoli Netcool Configuration Manager with devices from Tivoli Network Manager.
- Exploiting configuration information for problem isolation.
- Configuring a rollback after misconfiguration.
- Implementing a new network configuration standard.
- Ensuring that a configuration is appropriate to support a network service.

### 1.3.1 Integrated data flow

In an integrated Tivoli Netcool Configuration Manager, Tivoli Netcool/OMNIbus, and Tivoli Network Manager solution, data travels from the network resources that are being managed through a number of product components and networking layers, until it is presented to the network operators.

At each stage of this journey, components and processes categorize, cross-reference, and enrich the collected network data. To enable these components and processes to integrate, you perform a number of tasks.

**Note:** Our focus is on data relevant to configuration and policy management, rather than all data.

Figure 1-6 shows the data flow between product components in an integrated environment.

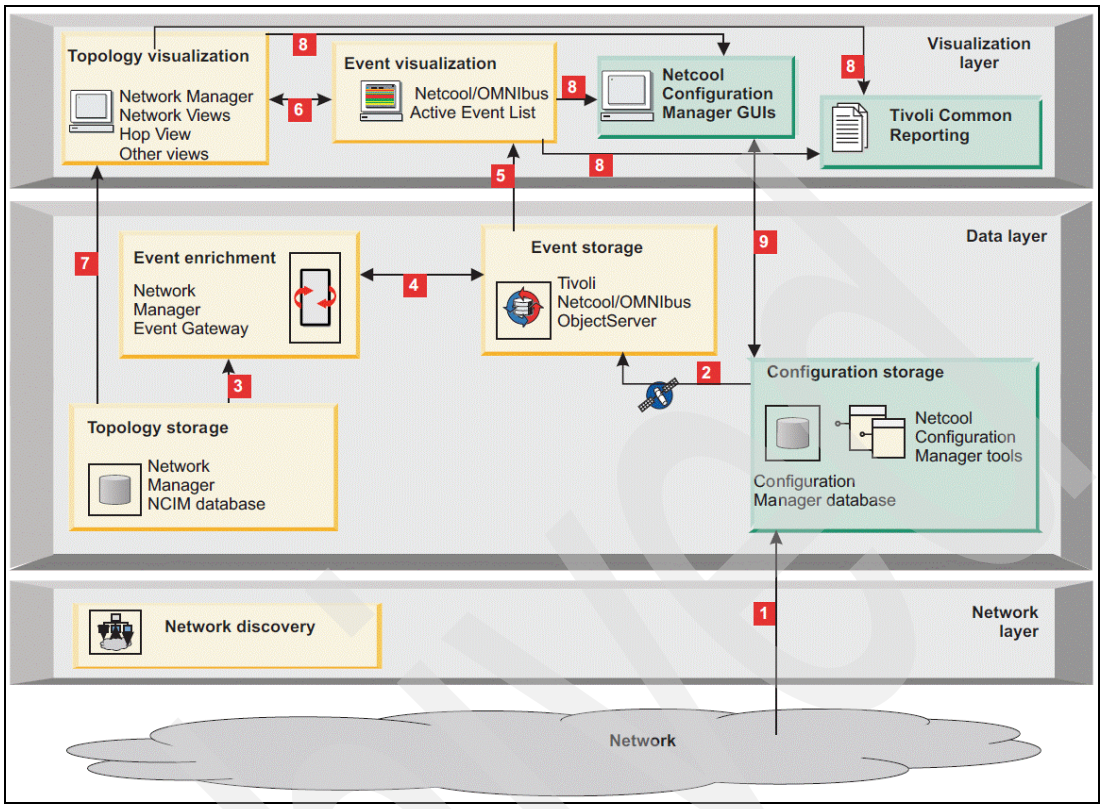



*Figure 1-6 Integrated data flow*

Where:

1. When a configuration change or policy violation occurs in a network resource, information is sent to Tivoli Netcool Configuration Manager.
2. Tivoli Netcool Configuration Manager logs the data and sends a corresponding event to the Tivoli Netcool/OMNIbus ObjectServer via the SNMP Probe.
3. Network topology data stored in the Tivoli Network Manager NCIM database is made available to the Event Gateway.
4. Tivoli Netcool Configuration Manager events are passed to the Event Gateway, where they are enriched with network topology data and then returned to the ObjectServer.
5. The Active Event List (Tivoli Netcool/OMNIbus) displays configuration change and policy violation events stored in the ObjectServer.
6. Event information is shared by the Active Event List and Tivoli Network Manager views.
7. Tivoli Network Manager GUIs display network topology data stored in the NCIM database. This data is enriched by configuration change and policy event information from the ObjectServer.
8. Configuration changes and policy violations are displayed in the Tivoli Network Manager and Tivoli Netcool/OMNIbus GUIs. Using the context menus, operators can launch across into IBM Tivoli Common Reporting, as well as into the Tivoli Netcool Configuration Manager GUIs, for further analysis.
9. The full Tivoli Netcool Configuration Manager functionality remains available through the Tivoli Netcool Configuration Manager GUIs.

### 1.3.2 Seeding Tivoli Netcool Configuration Manager with devices from Tivoli Network Manager

In this scenario, network devices discovered by Tivoli Network Manager for a specific domain are exported using the **itnmGenerateITNCMSeedFile.pl** Perl script in the `$NCHOME/precision/scripts/perl/scripts/bin` directory.

The **itnmGenerateITNCMSeedFile.pl** Perl script generates a CSV file containing the list of network devices held in one or more Tivoli Network Manager domains.

Each file produced contains comments describing how and when the seed file was generated, the format of the file, and an entry for each device that identifies the following device data:

- Tivoli Network Manager domain name
- Tivoli Network Manager entityId for the device
- Tivoli Network Manager device name
- Tivoli Network Manager host name or IP address through which the device can be contacted

Note that this scenario is implemented as part of the overall integration steps, because it is a prerequisite for the other integration scenarios. The implementation steps are described in 2.4.2, “Seeding Tivoli Netcool Configuration Manager with devices from Tivoli Network Manager” on page 26.

### 1.3.3 Exploiting configuration information for problem isolation

In this scenario, notifications of configuration changes are sent to OMNIbus, which are correlated to network faults and performance indicators to identify the root cause of a network outage.

This integration scenario consists of the following steps:

1. A change is made, such as shutting down an interface from Tivoli Netcool Configuration Manager.
2. Events show up on the Tivoli Netcool OMNIbus GUI.
3. The operator launches a report in context from the event.
4. The operator launches Tivoli Netcool Configuration Manager in context from the event.
5. The operator validates the change.
6. The operator corrects the problem by restarting the interface from Tivoli Netcool Configuration Manager.
7. Events are cleared on the Tivoli Netcool OMNIbus GUI.

This integration is described in Chapter 3, “Exploiting configuration information for problem isolation” on page 41.

### 1.3.4 Configuration rollback after misconfiguration

This integration scenario provides a launch-in-context from a network problem to restore network service.

This scenario consists of the following steps:

1. A device goes red.
2. The operator is watching the network map and notices the problem.
3. The operator launches a report in context from the device.
4. The operator launches Tivoli Netcool Configuration Manager in context from the device.
5. The operator identifies the configuration that needs to be rolled back.
6. The operator applies the rollback from Tivoli Netcool Configuration Manager.
7. The device goes green in the network map.

This integration is described in Chapter 4, “Configuring a rollback after a misconfiguration” on page 67.

### 1.3.5 Implementing a new network configuration standard

This scenario uses Tivoli Netcool Configuration Manager’s configuration command sets to implement configuration standards across all network devices.

The following steps describe the data flow:

1. The administrator has installed the mttrapd probe.
2. The administrator wants to enable the network SNMP traps.
3. The administrator launches Tivoli Netcool Configuration Manager.
4. The administrator creates multiple command sets for different devices (such as CISCO IOS, CISCO CATOS, or Juniper JUNOS).
5. The administrator applies the command sets for selected devices.
6. The administrator verifies that mttrapd events appear on Netcool OMNIbus.

This integration is described in Chapter 5, “Implementing a new network configuration standard” on page 87.

### 1.3.6 Ensuring that a configuration is appropriate to support a network service

This scenario uses Tivoli Network Manager’s view of network services to apply a compliance policy across a set of network resources to support the network service.

The data flow is described as follows:

1. A service provider receives an order to create a new VPN for a new client ZYX, with several branches.
2. Service provider wants to verify that VPN configuration is compliant across all client ZYX facing routers.
3. Tivoli Netcool Configuration Manager administrator creates a MPLS VPN policy for client ZYX.
4. The Tivoli Network Manager administrator launches Tivoli Network Manager and MPLS views.
5. In the Tivoli Network Manager and MPLS view, suitable routers are identified.

6. The Tivoli Netcool Configuration Manager administrator launches Tivoli Netcool Configuration Manager Compliance.
7. The Tivoli Netcool Configuration Manager administrator executes the policy against the selected devices.

After the policy runs, the Tivoli Network Manager administrator launches in-context compliance reports and sees if the identified devices support the new network service.

This integration is described in Chapter 6, “Ensuring that a configuration is appropriate for supporting a new network service” on page 115.

## 1.4 Publications

The publications in the Tivoli Netcool Configuration Manager PDF document set, and the prerequisite publications in the Tivoli Network Manager IP Edition and Tivoli Netcool/OMNIbus library, can be found in “Related publications” on page 147.

2

# Integration overview

In this chapter, we provide an overview about the technical integration of Tivoli Network Manager, Tivoli Netcool/OMNIbus, and Tivoli Netcool Configuration Manager.

This chapter describes following topics:

## 2.1 Prerequisites

The products and components that support the integration must be installed, and must be in an operational state before you configure the integration.

All product deployments are considered non-root installations. The installations of all components are done by the user icosuser assigned to group icosgrp.

The default installation directory `/opt/IBM/` is used for the installation of all related components within our lab environment.

Before installing the products, ensure that you review the hardware, operating system, software, and communication requirements, and consider your deployment options. Also take note of the user and system permissions that are required for the user performing the installation.

**Note:** Working within a Windows® environment, you need a Windows utility that supports `.tar` and `.tar.gz` file extractions.

Specific product versions are required to support the integration. Working knowledge of these products is assumed.

The required products are as follows:

- IBM Tivoli Netcool Configuration Manager Version 6.1
- IBM Tivoli Network Manager Version 3.8
- IBM Tivoli Netcool/OMNIbus ObjectServer Version 7.3
- IBM Tivoli Netcool/OMNIbus Web GUI Version 7.3

For a detailed list of product versions and builds used within the lab environment, refer to 2.3, “Product deployment” on page 21.

### 2.1.1 Product deployment procedure

The required installation and configuration steps are as follows:

1. Install Tivoli Network Manager, including Tivoli Netcool/OMNIbus ObjectServer.
2. Configure Tivoli Network Manager and Tivoli Netcool/OMNIbus ObjectServer.
3. Configure the MTTrapd Probe and Tivoli Netcool/OMNIbus Knowledge Library.
4. Install Tivoli Netcool Configuration Manager.
5. Configure Tivoli Netcool Configuration Manager - Base.
6. Configure Tivoli Netcool Configuration Manager - Compliance.
7. Apply Tivoli Netcool/OMNIbus ObjectServer Version 7.3 Fix Pack 2.
8. Apply Tivoli Netcool/OMNIbus Web GUI Version 7.3 Fix Pack 2.
9. Apply Tivoli Network Manager Version 3.8 Fix Pack 4.
10. Install and configure Simnet Probe Version 1.7.

## 2.2 Lab environment

The lab environment presented in this book is based on the following described environment.

Within the lab environment, the database for Netcool Configuration Manager was installed on a separate due to system performance considerations. All Tivoli Netcool Configuration Manager components were installed on a single server system.

All Tivoli Network Manager components, including Tivoli Netcool/OMNIbus, are installed on a single server system as well.

We installed the following product components in our lab environment:

- Tivoli Network Manager and Tivoli Netcool/OMNIbus
  - Tivoli Integrated Portal
  - Tivoli Network Manager Topoviz GUI
  - Tivoli Network Manager discovery processes
  - Tivoli Network Manager monitoring processes
  - Tivoli Network Manager NCIM database
  - Tivoli Netcool/OMNIbus Web GUI
  - Tivoli Netcool/OMNIbus ObjectServer
  - Netcool Knowledge Library
  - MTTrapd Probe
  - Syslog Probe
  - Simnet Probe
- Tivoli Netcool Configuration Manager
  - Tivoli Netcool Configuration Manager Base
  - Tivoli Netcool Configuration Manager Compliance
  - Tivoli Netcool Configuration Manager Device Drivers
- Oracle

  Oracle database instances for Tivoli Netcool Configuration Manager and Tivoli Netcool Configuration Manager Compliance

Tivoli Network Manager and Tivoli Netcool Configuration Manager are configured to access the network test labs in Southbank and Raleigh. The network test labs represent network devices for technologies such as MPLS, BPG, and others.

The SNMP Trap destination of the devices within the network test labs in Raleigh and Southbank are configured with the IP address of the MTTrapd Probe.

The lab environment structure is shown in Figure 2-1.

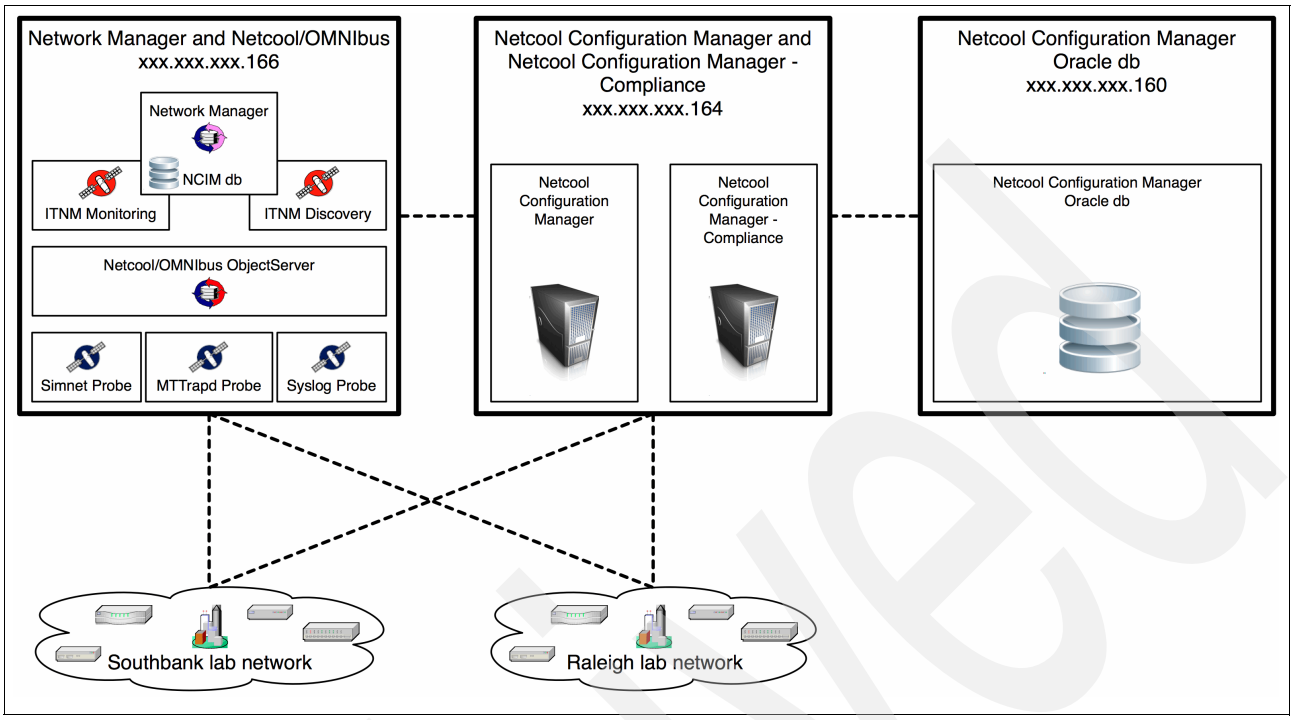



*Figure 2-1 Lab environment structure*

With the successful deployment of the lab environment, the processes shown in Example 2-1 are shown for Tivoli Network Manager, Tivoli Netcool/OMNIbus, and related Tivoli Netcool/OMNIbus Probes.

*Example 2-1 Tivoli Network Manager processes*

```
$ itnm_status
OMNIbus:
      nco_pad            RUNNING  PID=29035 NCO_PA
      nco_objserv        RUNNING  PID=29784 NCOMS
      nco_p_mttrapd      RUNNING  PID=29846 NCOMS
      nco_p_simnet       RUNNING  PID=29850 NCOMS
Tivoli Network Manager:
  Domain:  Southbank
      ncp_ctrl           RUNNING  PID=1319  Southbank
      ncp_store          RUNNING  PID=2127  Southbank
      ncp_class          RUNNING  PID=2128  Southbank
      ncp_auth           RUNNING  PID=2129  Southbank
      ncp_model          RUNNING  PID=4121  Southbank
      ncp_disco          RUNNING  PID=4567  Southbank
      ncp_f_amos         RUNNING  PID=4568  Southbank
      ncp_d_helpserv     RUNNING  PID=2130  Southbank
      ncp_config         RUNNING  PID=2131  Southbank
      ncp_poller         RUNNING  PID=7647  Southbank
      nco_p_ncpmonitor   RUNNING  PID=2135  Southbank
      ncp_ncogate        RUNNING  PID=6560  Southbank
      ncp_webtool        RUNNING  PID=2136  Southbank
  Domain:  Raleigh
      ncp_ctrl           RUNNING  PID=7348  Raleigh
```

```
      ncp_store          RUNNING  PID=8340  Raleigh
      ncp_class          RUNNING  PID=8341  Raleigh
      ncp_auth           RUNNING  PID=8342  Raleigh
      ncp_model          RUNNING  PID=8549  Raleigh
      ncp_disco          RUNNING  PID=8569  Raleigh
      ncp_f_amos         RUNNING  PID=8570  Raleigh
      ncp_d_helpserv     RUNNING  PID=8343  Raleigh
      ncp_config         RUNNING  PID=8345  Raleigh
      ncp_poller         RUNNING  PID=9675  Raleigh
      nco_p_ncpmonitor   RUNNING  PID=8346  Raleigh
      ncp_ncogate        RUNNING  PID=9025  Raleigh
      ncp_webtool        RUNNING  PID=8347  Raleigh
  Domain:  ITNM
      ncp_ctrl           RUNNING  PID=29523 ITNM
      ncp_store          RUNNING  PID=29920 ITNM
      ncp_class          RUNNING  PID=29921 ITNM
      ncp_auth           RUNNING  PID=29928 ITNM
      ncp_model          RUNNING  PID=30105 ITNM
      ncp_disco          RUNNING  PID=30142 ITNM
      ncp_f_amos         RUNNING  PID=30143 ITNM
      ncp_d_helpserv     RUNNING  PID=29936 ITNM
      ncp_config         RUNNING  PID=29937 ITNM
      ncp_poller         RUNNING  PID=32025 ITNM
      nco_p_ncpmonitor   RUNNING  PID=29950 ITNM
      ncp_ncogate        RUNNING  PID=30235 ITNM
      ncp_webtool        RUNNING  PID=29958 ITNM
Tivoli Integrated Portal:
      Server             RUNNING  PID=29822
```

## 2.3 Product deployment

For a review of all installed product, packages, components, and versions, use the following two scripts:

- The **listSw.sh** script provides a summarized output of all installed operating system packages.
- The **listIU.sh** script provides a summarized output of all deployed Tivoli products and components with detailed version information.

**Note:** You might have to source the correct environment provided by **setenv.sh** within the /home/netcool/.acsi_netcool/ directory to be able to run the **listIU.sh** and **listSw.sh** commands.

Both commands are located in the ../.acsi_*username*/bin/ directory, where username stands for the user for the deployment, which is done in a non-root installation. In the example, the deployment is done by the user netcool and the commands are located within /home/netcool/.acsi_netcool/bin/ directory.

**Note:** The correct environment is required before you apply any product Fix Packs. The installer cannot run if the **listIU.sh** and **listSw.sh** commands would fail to provide any outputs.

To make sure we have the correct environment set, we have enhanced the .bash_profile of the user icosuser within our lab environment.

The enhanced .bash_profile for the user icosuser is shown in Example 2-2.

*Example 2-2 Enhanced .bash_profile for the user icosuser*

```
# .bash_profile

# Get the aliases and functions
if [ -f ~/.bashrc ]; then
   . ~/.bashrc
fi

# User specific environment and startup programs

PATH=$PATH:$HOME/bin

export PATH

# [Begin] Added by IBM, D.Bahn 11.08.2010
echo "================================================="
echo " Set IBM Tivoli Netcool environment              "
echo " . /opt/IBM/tivoli/netcool/env.sh                "
. /opt/IBM/tivoli/netcool/env.sh
echo "-------------------------------------------------"
echo " Set IBM Tivoli Integrated Portal envrionment    "
echo " . /home/icosuser/.acsi_icosuser/setenv.sh       "
. /home/icosuser/.acsi_icosuser/setenv.sh
echo "-------------------------------------------------"
echo " May now run itnm_status, itnm_stop or itnm_start "
echo "================================================="
# [End] Added by IBM, D.Bahn 11.08.2010
```

### 2.3.1 Tivoli Network Manager

The following detailed product versions and builds are used for the Tivoli Network Manager deployment:

- IBM Tivoli Network Manager Version 3.8.0.50
- IBM Tivoli Network Manager Version 3.8.0.56 (Fix Pack 3)
- IBM Tivoli Network Manager Version 3.8.0.61 (Fix Pack 4)

Our deployment of the Tivoli Network Manager within the lab environment is based on and follows the general product installation guidelines for deploying a single, non-failover environment.

**Note:** The components of Tivoli Integrated Portal are installed automatically during the installation process of Tivoli Network Manager Topoviz GUI or Netcool/OMNIbus Web GUI components.

The general guideline for deploying a Tivoli Network Manager environment is documented in the *IBM Tivoli Network Manager - Installation and Configuration Guide*, which can be found at the following address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.networkmanagerip.doc_3.8/nmip_ins_pdf_38.pdf

To logically split up the Southbank and Raleigh lab device locations, multi-domains are configured within the Tivoli Network Manager lab environment. The lab environment is configured with following domains:

- ITNM
- Southbank
- Raleigh

The Southbank and Raleigh domains are cloned domains based on the ITNM default domain. The ITNM default domain is configured during the default installation process.

Tivoli Network Manager multiple domains are configured within the lab environment to show more detailed technical information regarding the import of the Tivoli Network Manager devices within Tivoli Netcool Configuration Manager.

### 2.3.2 Tivoli Netcool/OMNIbus

The following detailed product versions and builds are used for the ObjectServer and Probe components of Netcool/OMNIbus within the Tivoli Network Manager deployment:

- IBM Tivoli Netcool/OMNIbus ObjectServer Version 7.3.0.0
- IBM Tivoli Netcool/OMNIbus ObjectServer Version 7.3.0.2 (Fix Pack 2)
- IBM Tivoli Netcool/OMNIbus MTTrapd Probe Version 1.10.0.0
- IBM Tivoli Netcool/OMNIbus Syslog Probe Version 1.5.0.0
- IBM Tivoli Netcool/OMNIbus Simnet Probe Version 1.7.0.0

The following detailed versions and builds are used for the Web GUI component of Netcool/OMNIbus within the Tivoli Network Manager deployment:

- IBM Tivoli Netcool/OMNIbus Web GUI Version 7.3.0.0
- IBM Tivoli Netcool/OMNIbus Web GUI Version 7.3.0.2 (Fix Pack2)

Our deployment of Netcool/OMNIbus within the lab environment is based on and follows the general guidelines for deploying a single, non-failover Netcool/OMNIbus environment.

**Note:** The components of Netcool/OMNIbus ObjectServer and Tivoli Netcool/OMNIbus Web GUI are installed automatically during the installation process of Tivoli Network Manager components.

The general guideline for deploying a Tivoli Netcool/OMNIbus environment is documented within the *IBM Tivoli Netcool/OMNIbus - Installation and Deployment Guide*, which can be found at the following address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIbus.doc_7.3.0/omn_pdf_ins_master_73.pdf

The default ObjectServer name of NCOMS is used during the deployment of Tivoli Netcool/OMNIbus.

The ObjectServer NCOMS is installed and pre-configured during the installation process of the Tivoli Network Manager.

The MTTrapd- and the Syslog-Probe are also installed and pre-configured during the installation process of the Tivoli Network Manager.

### 2.3.3 Tivoli Netcool Configuration Manager

The following product version and build is used for Tivoli Netcool Configuration Manager deployment:

- IBM Tivoli Netcool Configuration Manager Version 6.1

Our deployment of Tivoli Netcool Configuration Manager within our lab environment is based on and follows the general guidelines for deploying a single, non-failover Tivoli Netcool Configuration Manager deployment.

The general guideline for deploying a Tivoli Netcool Configuration Manager environment is documented within the following guides:

- *IBM Tivoli Netcool Configuration Manager - Base Installation and Configuration Guide*, found at the following address:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm_pdf_base_ins_61.pdf

- *IBM Tivoli Netcool Configuration Manager - Driver Installation and Configuration Guide*, found at the following address:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm_pdf_driverins_61.pdf

- *IBM Tivoli Netcool Configuration Manager - OOBC Installation Guide*, found at the following address:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm_pdf_oobcins_61.pdf

- *IBM Tivoli Netcool Configuration Manager - Compliance Installation and Upgrade Guide*, found at the following address:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm_pdf_comp_ins_61.pdf

- *IBM Tivoli Netcool Configuration Manager - Integration Guide*, found at the following address:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm_pdf_int_master_61.pdf

## 2.4 Data integration

This section describes the data integration of Tivoli Network Manager, Tivoli Netcool/OMNIbus, and Tivoli Netcool Configuration Manager in technical detail.

**Note:** We recommend following the *IBM Tivoli Netcool Configuration Manager - Integration Guide* for step-by-step deployment instructions.

The data integration steps are:

1. Deploying default Tivoli Netcool Configuration Manager reports
2. Seeding Tivoli Netcool Configuration Manager with devices from Tivoli Network Manager
3. Applying customized rules for Tivoli Netcool Configuration Manager

The data integration steps for Tivoli Network Manager, Tivoli Netcool/OMNIbus, and Tivoli Netcool Configuration Manager are covered in details in the *IBM Tivoli Netcool Configuration Manager - Integration Guide*, found at following address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm_pdf_int_master_61.pdf

## 2.4.1 Deploying default Tivoli Netcool Configuration Manager reports

To support reporting, a set of default reports is supplied with your Tivoli Netcool Configuration Manager deployment. You must add these reports to your Tivoli Common Reporting installation.

The detailed steps for deploying the reports are described in Chapter 3, “Integrating the products”, in *IBM Tivoli Netcool Configuration Manager - Integration Guide.* Refer to the following address for a detailed description of all the required steps:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm/wip/int/task/ncm_int_installingdefaultncmreports.html

The deployed Tivoli Netcool Configuration Manager reports are shown in Figure 2-2.

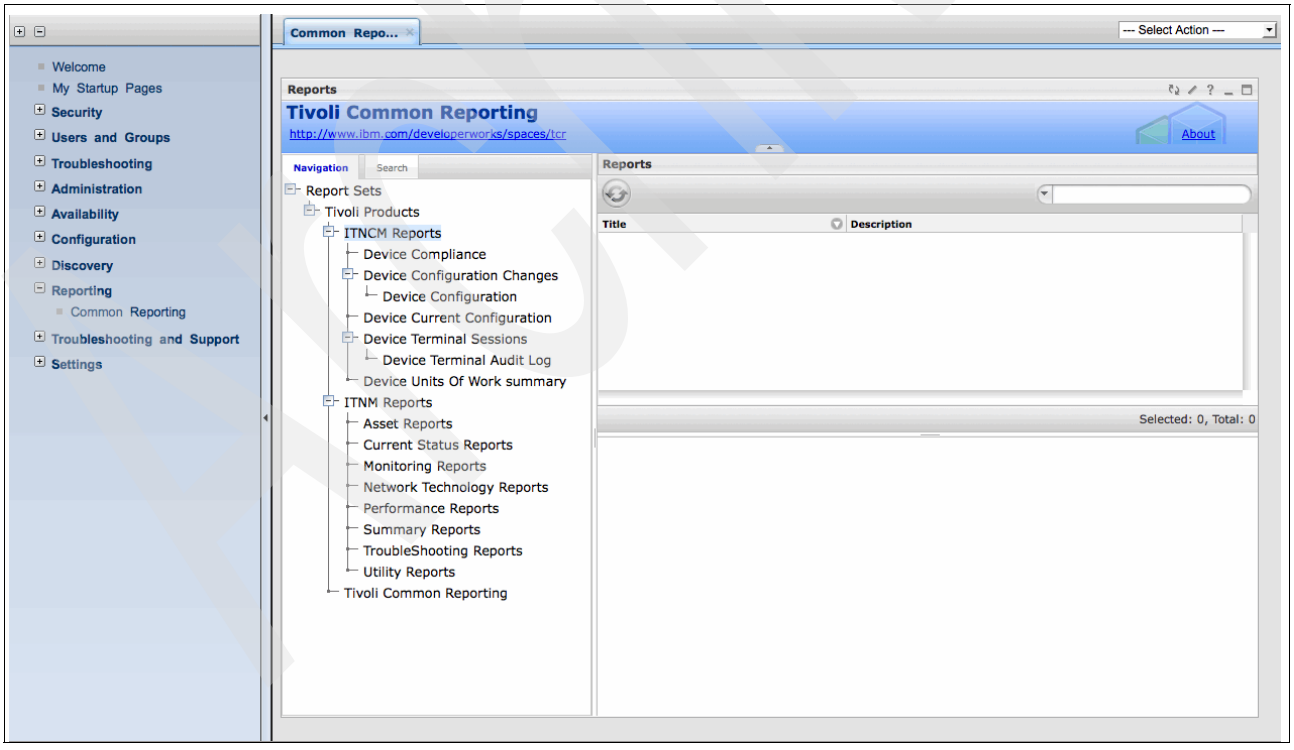



*Figure 2-2 Tivoli Netcool Configuration Manager reports*

## 2.4.2 Seeding Tivoli Netcool Configuration Manager with devices from Tivoli Network Manager

This section provides additional integration information regarding seeding Tivoli Netcool Configuration Manager devices from Tivoli Network Manager.

You must run a script to seed Tivoli Netcool Configuration Manager with devices from Tivoli Network Manager. This enables Tivoli Netcool Configuration Manager to make use of the topology data in Tivoli Network Manager, and ensures common network resource identification between Tivoli Netcool Configuration Manager and Tivoli Network Manager.

The detailed steps for seeding Tivoli Netcool Configuration Manager with devices from Tivoli Network Manager can be found in Chapter 3, “Integrating the products”, in the *IBM Tivoli Netcool Configuration Manager - Integration Guide.* Refer to the following address for a detailed description of all required steps:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm/wip/int/task/ncm_int_seedingncmwithdevicesfromitnm.html

### Configuring event enrichment in Tivoli Network Manager

You must also configure the Tivoli Network Manager Event Gateway, ncp_ncogate, to use the ItncmMonitoringEventNoRca event map to enrich events from the ObjectServer with topology data.

To configure enrichment of the events raised by Tivoli Netcool Configuration Manager, perform the detailed steps given in Chapter 3, “Integrating the products” in *IBM Tivoli Netcool Configuration Manager - Integration Guide.* Refer to the following address for a detailed description of all the required steps:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm/wip/int/task/ncm_int_configuringeventmappinginitnm.html

### Running the itnmGenerateITNCMSeedFile.pl Perl script

Network devices discovered by Tivoli Network Manager for a specific domain are exported using the **`itnmGenerateITNCMSeedFile.pl`** Perl script, which is in the `$NCHOME/precision/scripts/perl/scripts/bin` directory.

The **`itnmGenerateITNCMSeedFile.pl`** Perl script generates a CSV file containing the list of network devices held in one or more Tivoli Network Manager domains.

Each file produced contains comments describing how and when the seed file was generated, the format of the file, and an entry for each device that identifies the following device data:

- Tivoli Network Manager domain name
- Tivoli Network Manager entityId for the device
- Tivoli Network Manager device name
- Tivoli Network Manager host name or IP address through which the device can be contacted

We recommend using the login parameters for the Tivoli Network Manager database called NCIM. The login parameters for the NCIM database are:

- -itncmUsername NCIM_USERNAME
- -itncmPassword NCIM_PASSWORD

NCIM_USERNAME and NCIM_PASSWORD are the user ID and password for the NCIM database, which is defined during the installation of the Tivoli Network Manager database.

For both parameters, make sure to use the correct NCIM database credentials, even if they are encrypted within the `DbLogins.ITNMDOMAIN.cfg` config file. Encrypting the NCIM database credentials can be done by running the **`ncp_crypt`** command.

If the **`itnmGenerateITNCMSeedFile.pl`** script is not able to log in into the NCIM database, you receive the error message shown in Example 2-3.

*Example 2-3 NCIM password error message*

```
Level: critical Msg: The DB password must be provided on the command line for
schema  ncim  as it is encrypted in the DbLogins file

critical: The DB password must be provided on the command line for schema  ncim
as it is encrypted in the DbLogins file at ./itnmGenerateITNCMSeedFile.pl line 314
```

**Note:** Make sure you have the correct IP addresses, host names, and domain names defined within `/etc/hosts` or resolved by DNS lookup. The **`itnmGenerateITNCMSeedFile.pl`** and **`loadNCM.sh`** scripts must have the correct IP addresses or host names.

The error message about the wrong IP address or host name for Tivoli Netcool Configuration Manager within the -server parameter of the **`itnmGenerateITNCMSeedFile.pl`** or **`loadNCM.sh`** scripts is shown in Example 2-4.

*Example 2-4 ITNCM server access exception*

```
Initializing connection to ITNCM...
Exception in thread "P=377099:0=0:CT" com.intelliden.icos.EjbAccessException:
Unable to access ITNCM server.
   at com.intelliden.icos.api.impl.EjbSession.connect(EjbSession.java:207)
   at com.intelliden.icos.api.impl.EjbSession.connect(EjbSession.java:116)
   at com.intelliden.icos.api.ApiFactory.getSession(ApiFactory.java:90)
   at
com.intelliden.icos.api.tools.deviceloader.DeviceLoader.connect(DeviceLoader.java:
112)
   at
com.intelliden.icos.api.tools.deviceloader.DeviceLoader.bulkload(DeviceLoader.java
:87)
   at
com.intelliden.icos.api.tools.deviceloader.DeviceLoader.main(DeviceLoader.java:265
)
```

## Considering the Tivoli Network Manager multiple domains environment

At least one Tivoli Netcool Configuration Manager realm is created when configuring the following Tivoli Netcool Configuration Manager - Base installation. Devices in Tivoli Network Manager are grouped within domains. As devices are loaded into Tivoli Netcool Configuration Manager from Tivoli Network Manager, sub-realms are automatically created for each Tivoli Network Manager domain.

**Note:** We recommend running the **itnmGenerateITNCMSedFile.pl** script for each domain for multiple Tivoli Network Manager domains using the -watch script option. The -watch parameter is used to enable behavior to check for changes (adding devices) to the domains over time.

The processes for running multiple **itnmGenerateITNCMSeedFile.pl** scripts with two Tivoli Network Manager domains (Southbank and Raleigh) on a single server system are shown in Example 2-5.

*Example 2-5 itnmGenerateITNCMSeedFile.pl with two Tivoli Network Manager domains*

```
icosuser 27063 20759  0 14:49 pts/2    00:00:00 ncp_perl -S
./itnmGenerateITNCMSeedFile.pl -domain Southbank -ncimUsername ncim -ncimPassword
ncim -loadITNCM Y -itncmBaseIp dyn-9-196-131-164 -itncmPort 18102 -itncmUsername
admin -itncmPassword admin -debug DEBUG -watch
icosuser 29352 20759  0 15:42 pts/2    00:00:00 ncp_perl -S
./itnmGenerateITNCMSeedFile.pl -domain Raleigh -ncimUsername ncim -ncimPassword
ncim -loadITNCM Y -itncmBaseIp dyn-9-196-131-164 -itncmPort 18102 -itncmUsername
admin -itncmPassword admin -debug DEBUG -watch
```

### 2.4.3 Applying customized rules for Tivoli Netcool Configuration Manager

The MTTrapd Probe and Tivoli Netcool/OMNIbus Knowledge Library are installed on the Tivoli Netcool/OMNIbus ObjectServer host during the Tivoli Network Manger installer portion of the Tivoli Netcool/OMNIbus installation.

**Note:** If you install Tivoli Netcool/OMNIbus, the MTTrapd Probe, and Tivoli Netcool/OMNIbus Knowledge Library independently of the Tivoli Network Manager installation, you must apply manually the Tivoli Netcool/OMNIbus Knowledge Library configurations.

In addition to the MTTrapd Probe, we also install the Simnet Probe within our lab environment. This Probe installation is done manually by following the installation guidelines for the Tivoli Netcool/OMNIbus Simnet Probe.

We used the Simnet Probe in our lab environment for simulating test events.

The detailed steps for configuring the MTTrapd Probe and Tivoli Netcool/OMNIbus Knowledge Library are described in Chapter 2, “Installing and configuring the products”, in the *IBM Tivoli Netcool Configuration Manager - Integration Guide.* Refer to the following address for a detailed description of all the required steps:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm/wip/int/concept/ncm_int_installing.html

## 2.5 GUI integration

This section describes the GUI integration of Tivoli Network Manager, Tivoli Netcool/OMNIbus, Tivoli Netcool Configuration Manager, and Tivoli Integrated Portal in technical detail.

**Note:** We recommend referring to the *IBM Tivoli Netcool Configuration Manager - Integration Guide* for step-by-step deployment instructions.

The GUI integration steps are:

1. Configuring the Tivoli Netcool Configuration Manager menu and tools of the Web GUI Active Event List, and Tivoli Network Manager topology visualization GUI.
2. Configuring the Tivoli Netcool Configuration Manager menus of the Tivoli Integrated Portal GUI.

### 2.5.1 Configuring the Tivoli Netcool Configuration Manager menus of the Web GUI Active Event List and Tivoli Network Manager topology visualization GUI

You must add a menu and tools for Tivoli Netcool Configuration Manager events to the Tivoli Netcool/OMNIbus Web GUI to enable you to run device-based reports and to launch the Tivoli Netcool Configuration Manager GUIs from the Active Event List.

You can run a script to add the menu and tools to the Tivoli Netcool/OMNIbus Web GUI, and then use the Tivoli Integrated Portal console to add the menu as a submenu of the Alerts menu in the Active Event List.

The detailed steps to add menu and tools for Tivoli Netcool Configuration Manager and device-based reports are described in Chapter 3, “Integrating the products”, in *IBM Tivoli Netcool Configuration Manager - Integration Guide.* Refer to this online link for a detailed description of all the required steps:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm/wip/int/task/ncm_int_configuringwebguiaelmenu.html

You must add custom Tivoli Netcool Configuration Manager menu and tools to enable you to run device-based reports and launch the Tivoli Netcool Configuration Manager GUIs from the Tivoli Network Manager topology visualization GUIs (Topoviz).

The detailed steps to add custom menu and tools to the Tivoli Network Manager topology visualization GUIs are described in Chapter 3, “Integrating the products”, in the *IBM Tivoli Netcool Configuration Manager - Integration Guide.* Refer to this online link for a detailed description of all the required steps:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm/wip/int/task/ncm_int_confitnmtopoloviscontextmenu.html

### 2.5.2 Configuring the Tivoli Netcool Configuration Manager menus of the Tivoli Integrated Portal GUI

This section provides additional information regarding integrating Tivoli Netcool Configuration Manager and Tivoli Netcool Configuration Manager Compliance GUI within Tivoli Integrated Portal.

The graphical user interface integration provides an additional menu entry within the overall menu structure of Tivoli Integrated Portal. Within our lab environment, we configured two additional entries: One menu entry to launch Tivoli Netcool Configuration Manager and a second menu entry to launch Tivoli Netcool Configuration Manager Compliance.

You configure this additional integration by performing the following steps:

1. Adding a new folder in the Page Management tab
2. Adding a new page in the Page Management tab
3. Configuring a new folder called Configuration
4. Configuring a new page for Netcool Configuration Management
5. Configuring a new page for Netcool Configuration Compliance
6. Adding a URL for launching Netcool Configuration Management
7. Adding a URL for launching Netcool Configuration Compliance

## Adding a new folder in the Page Management tab

To add a new page to launch Tivoli Netcool Configuration Manager and Tivoli Netcool Configuration Manager Compliance, create a new folder in the Page Management tab by selecting **Settings** → **Page Management** → **New Folder.**

Figure 2-3 shows how to add a new folder called Configuration in the Page Management tab.

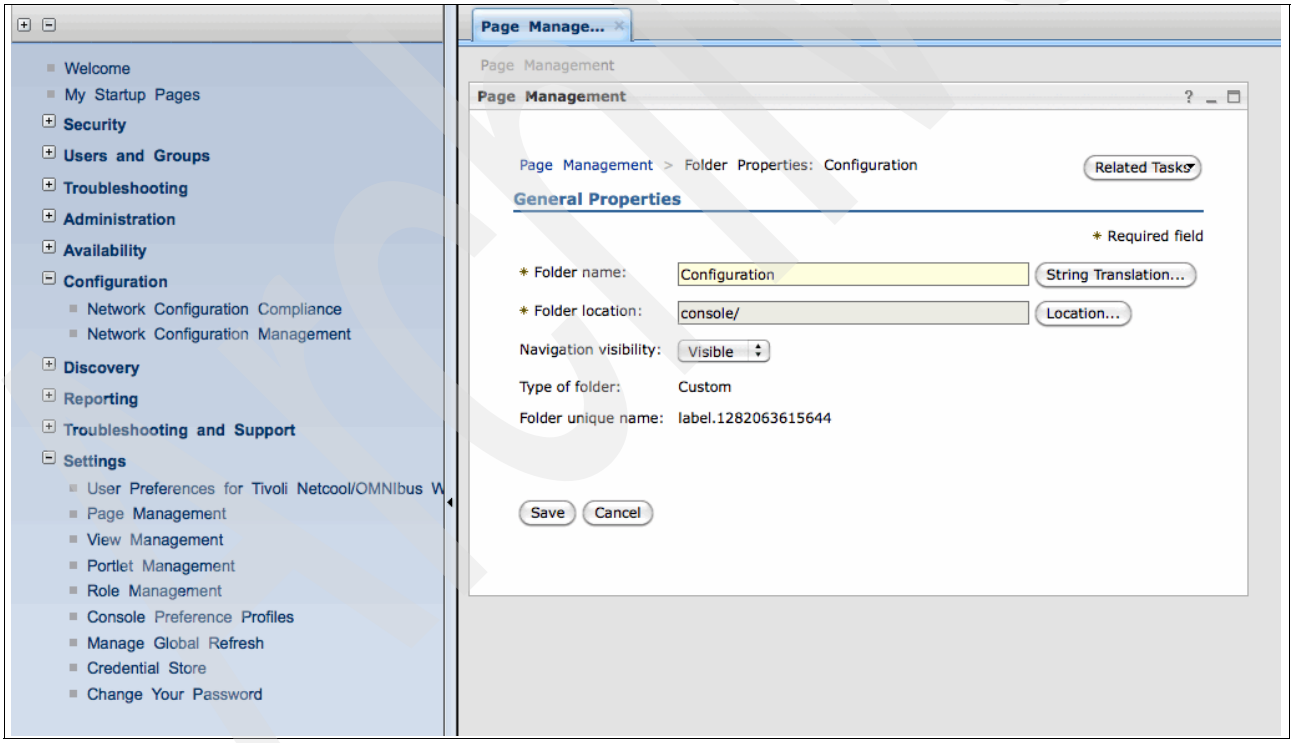



*Figure 2-3 How to add a new folder in the Page Management tab*

## Adding a new page in the Page Management tab

Perform the following steps:

1. To add a new page to launch Tivoli Netcool Configuration Manager and Tivoli Netcool Configuration Manager Compliance, select **Settings** → **Page Management** → **New Page.**

The portlet content type for both pages is Inline Frame.

After you create a page, you see an error message. This error messages belongs to a not yet specified URL for the Inline Frame type of the page. This error is shown in Figure 2-4.

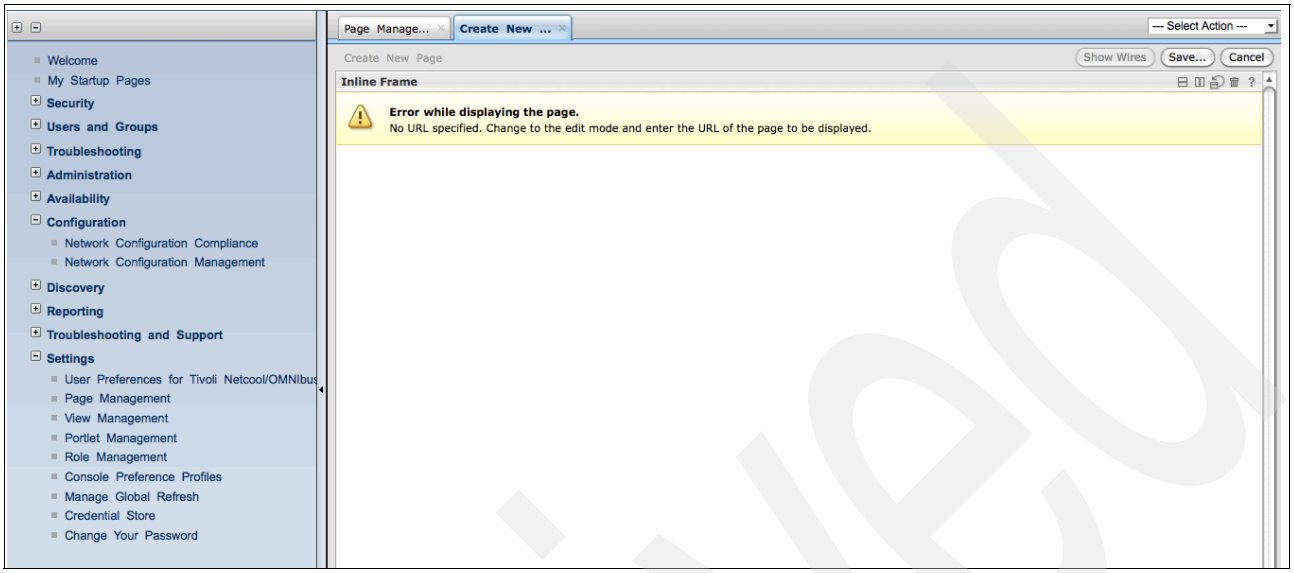



*Figure 2-4 Error regarding a not yet specified URL within the Inline Frame*

The URL is configured as shown in Figure 2-6 on page 33.

The required parameters for saving the page are shown in Figure 2-5.

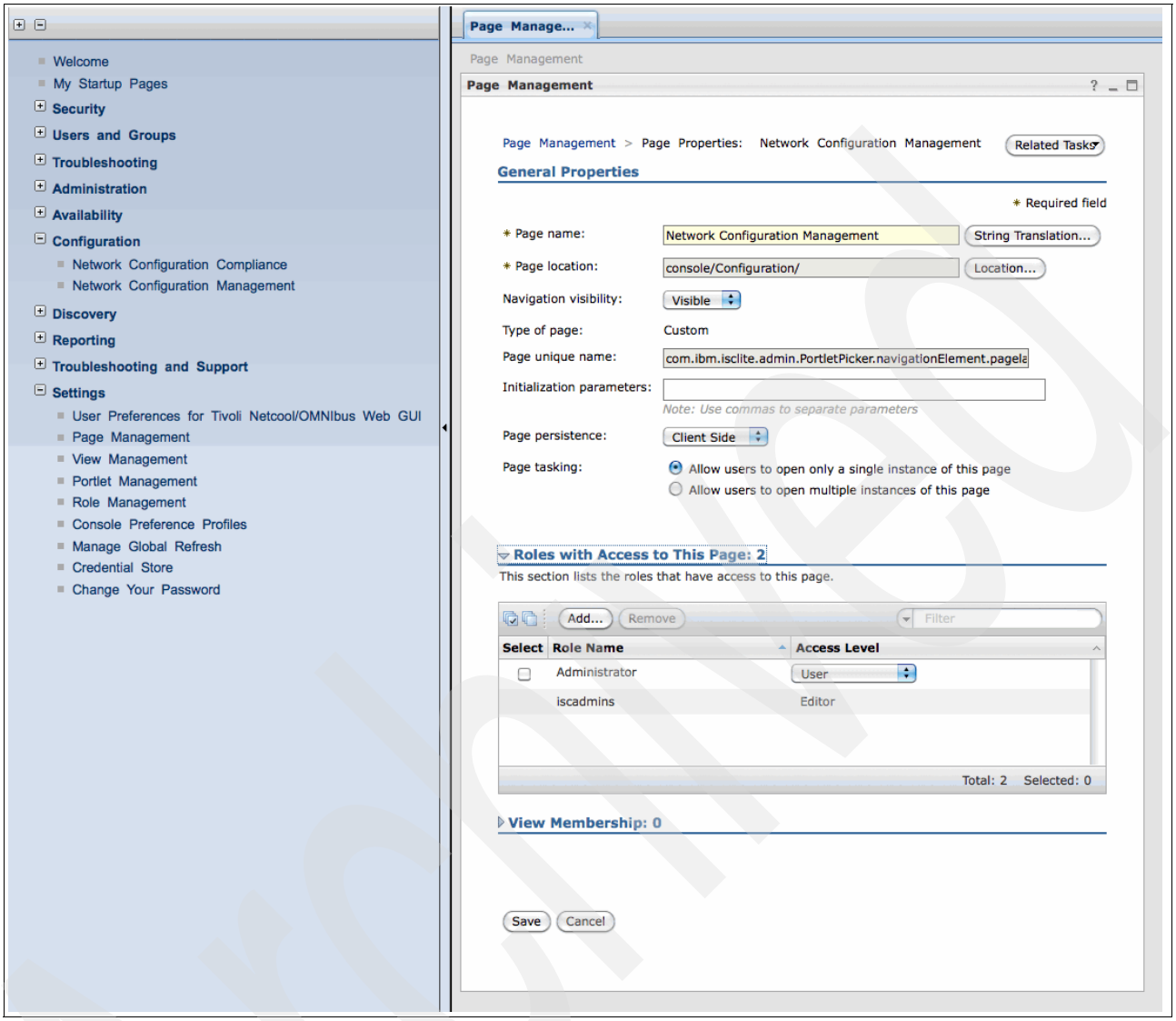



*Figure 2-5 Required parameters for saving the page*

2. In Figure 2-5, specify the following parameters:
   - Page name
   - Page location
   - Roles with access to this page

> **Note:** Make sure you configure the correct roles regarding access to the pages and view membership.

The page preferences we specified within our lab environment are shown in Table 2-1.

*Table 2-1 Page preferences*

| Page name | Page location | Roles with access to this page |
|---|---|---|
| Netcool Configuration Management | console/Configuration/ | Administrator |
| Netcool Configuration Management Compliance | console/Configuration/ | Administrator |

3. Click **Edit Defaults** at the upper right of the Inline Frame to specify the URL within the Inline Frame that launches Tivoli Netcool Configuration Manager or Tivoli Netcool Configuration Manager Compliance.

   The URL configuration used within the Inline Frame is shown in Table 2-2.

*Table 2-2 Inline Frame URL configuration*

| Component | Page name | URL |
|---|---|---|
| Tivoli Netcool Configuration Manager | Netcool Configuration Management | `http://9.196.131.164:7001` |
| Tivoli Netcool Configuration Compliance | Netcool Configuration Compliance | `http://9.196.131.164:7003` |

Figure 2-6 shows how to configure the URL within the Inline Frame.

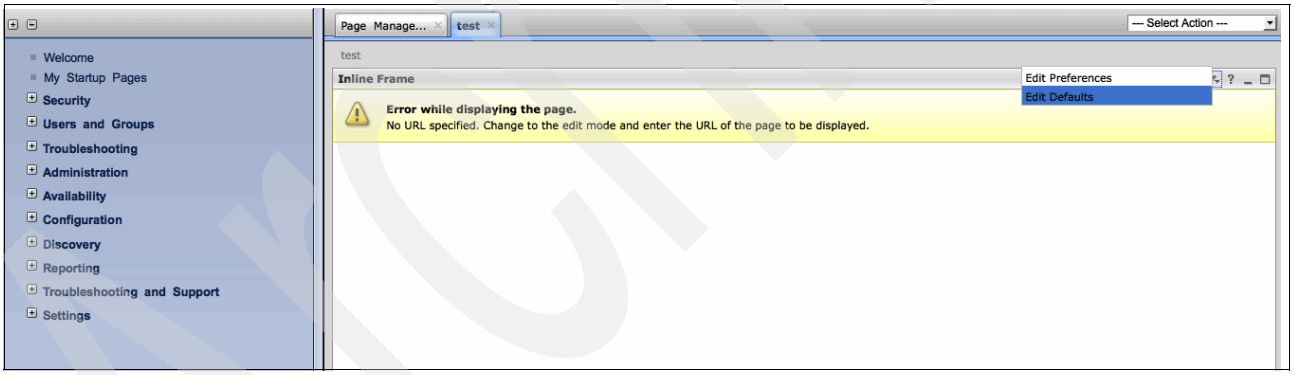



*Figure 2-6 Configuring the URL within the Inline Frame*

Figure 2-7 shows how to configure the URL for Tivoli Netcool Configuration Manager.

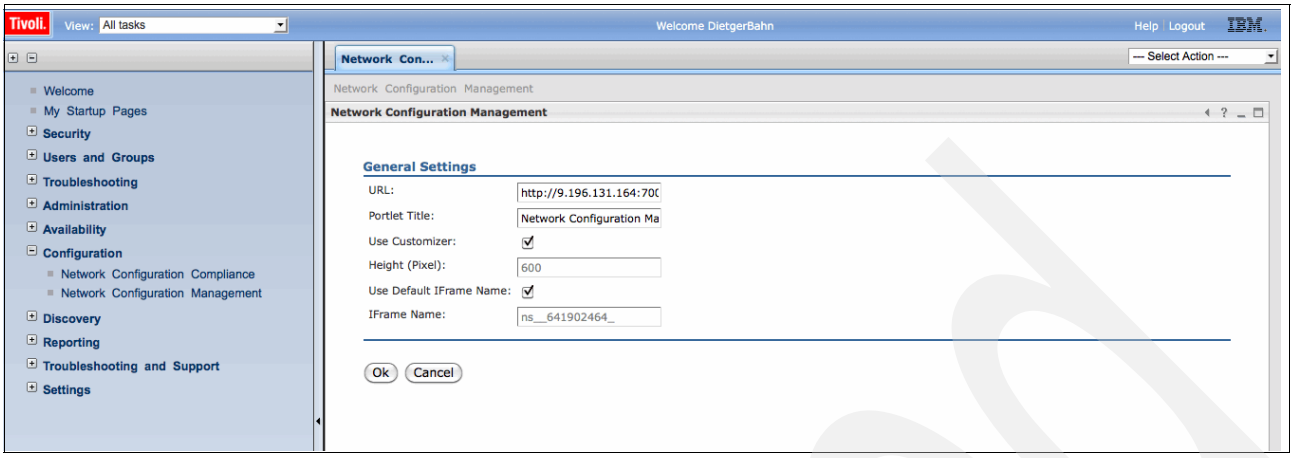



*Figure 2-7 Configuring the URL for Tivoli Netcool Configuration Manager*

The final result shows a new menu entry called Configuration in the main Tivoli Integrated Portal menu structure. In this menu entry, there are two sub-menu entries for Netcool Configuration Management and Netcool Configuration Compliance.

The integrated Tivoli Netcool Configuration Manager GUI in the Tivoli Integrated Portal is shown in Figure 2-8.

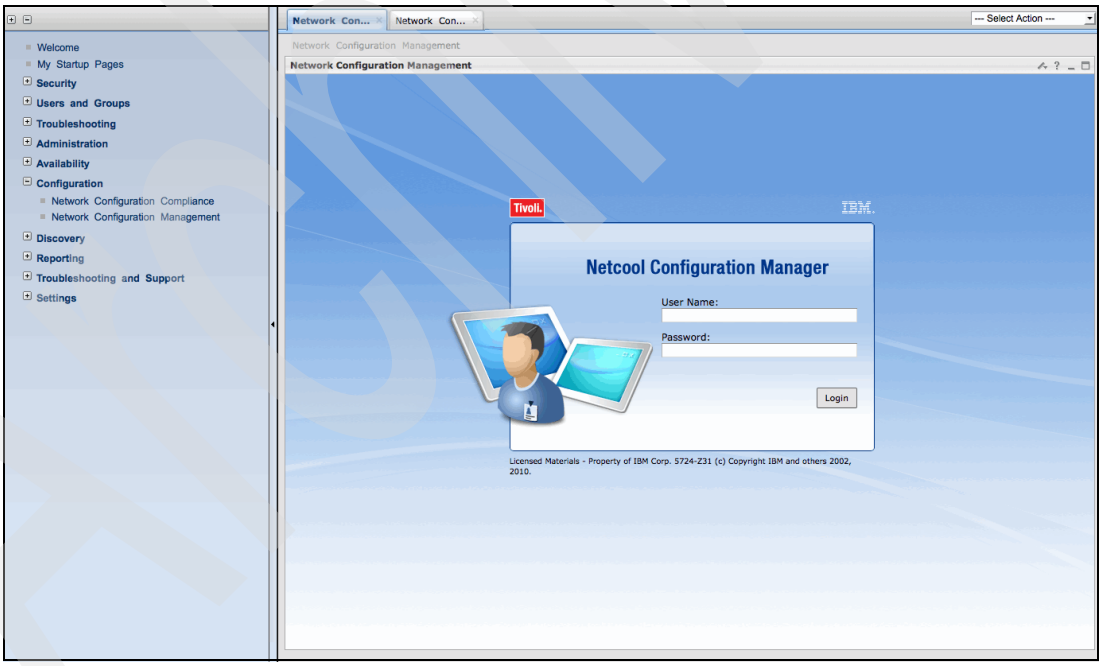



*Figure 2-8 Integrated Tivoli Netcool Configuration Manager GUI*

The integrated Netcool Configuration Compliance GUI in the Tivoli Integrated Portal is shown in Figure 2-9.

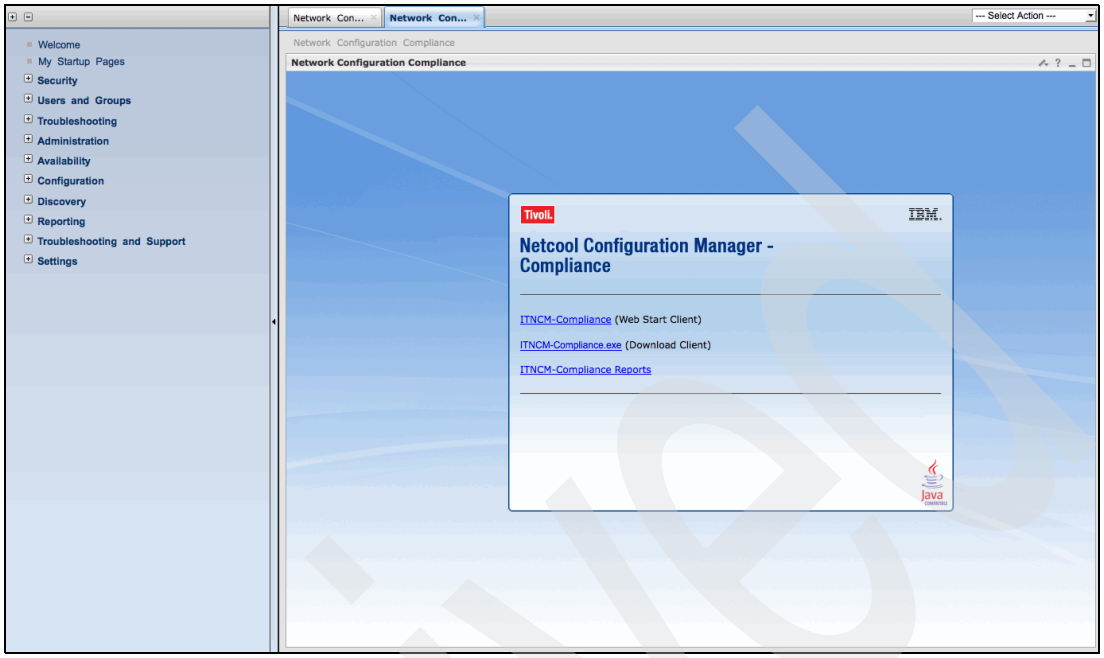



*Figure 2-9 Integrated Tivoli Netcool Configuration Compliance GUI*

## 2.5.3 Tivoli Netcool Configuration Manager Webstart GUI

We recommend the following Java™ Runtime Environment settings for the client systems when using the Tivoli Netcool Configuration Manager Webstart GUI.

**Note:** In addition to these settings, we also recommend that you clear all browser caches and clear your browsers' recent history.

These settings can help you with any possible problems when launching any Web GUIs or web pages.

**Note:** These recommendations are helpful if you experience error messages such as `Unable to launch the application.` or `Error: Must authenticate before using this service.` when launching the Tivoli Netcool Configuration Manager Webstart GUI.

Perform the following steps:

1. To view the IBM Java Runtime Environment settings, select **Start** → **Control Panel** → **IBM Control Panel for Java**. To view the Oracle Java Runtime Environment settings, select **Start** → **Control Panel** → **Java**.

Figure 2-10 shows the Control Panel window of the Windows client system with the IBM Control Panel for Java(TM) icon selected.

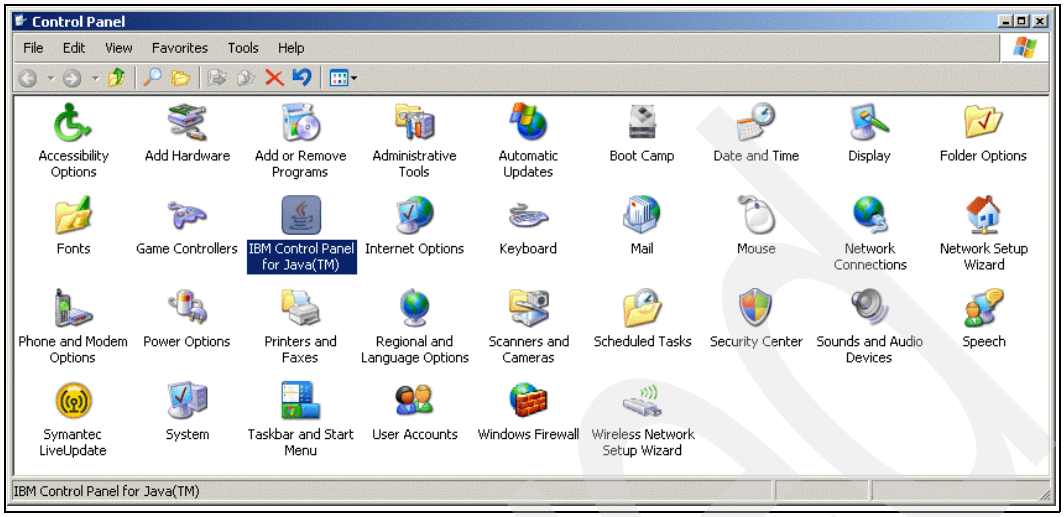



*Figure 2-10 Launching the IBM Java Runtime Environment settings*

2. Double-click the icon to open the Java Control Panel window.

   Figure 2-11 shows the Temporary Internet Files settings pane under the Java Control Panel's General tab.

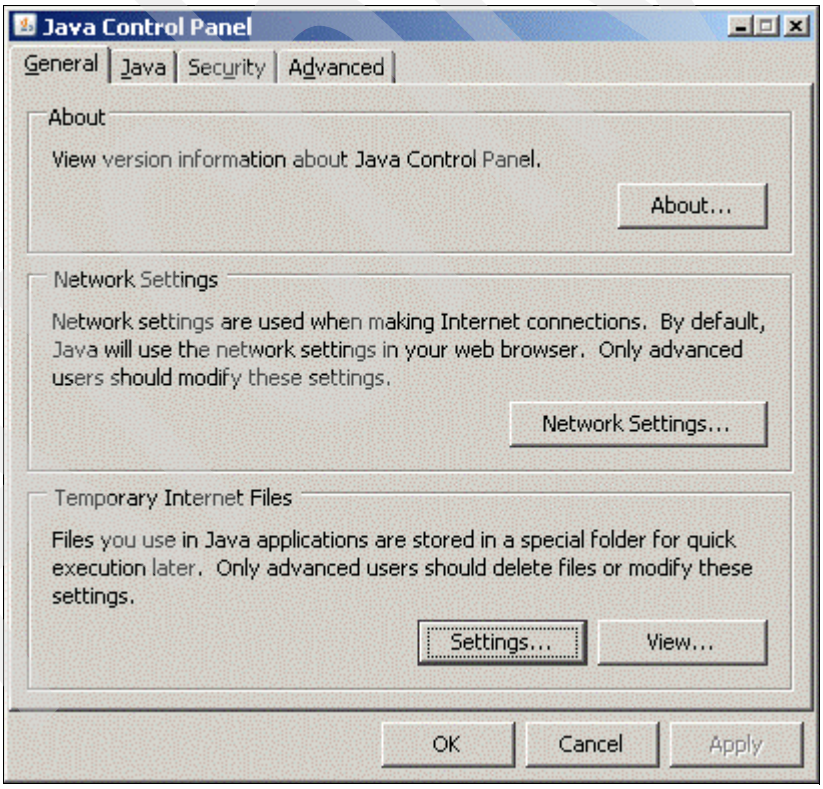



*Figure 2-11 Java Runtime Environment for temporary Internet files settings*

3. Click the **Settings...** button in the Temporary Internet Files pane.

**Note:** It is a best practice to remove the directory where the temporary files are kept. In our example, this directory is the `C:\Documents and Settings\Dietger Bahn\Application Data\Sun\Java\Deployment\cache` directory.

Figure 2-12 shows how to change the temporary files settings to the recommended values.

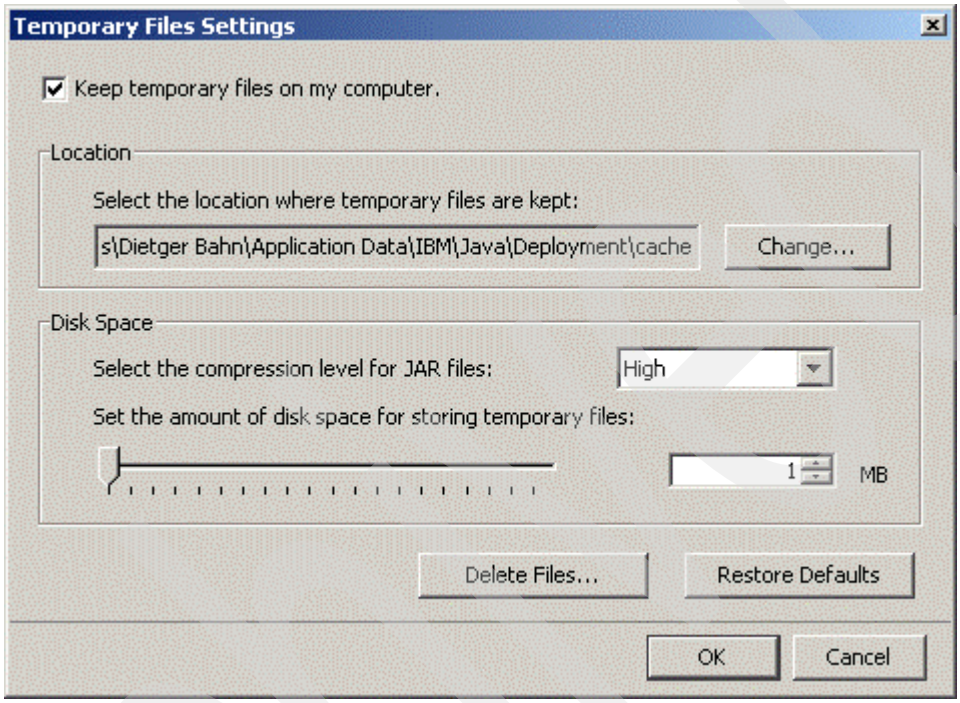



*Figure 2-12 Java Runtime Environment temporary files settings*

4. Select **Security** → **Certificates** → **Certificates**. Remove the certificate, as shown in Figure 2-13.

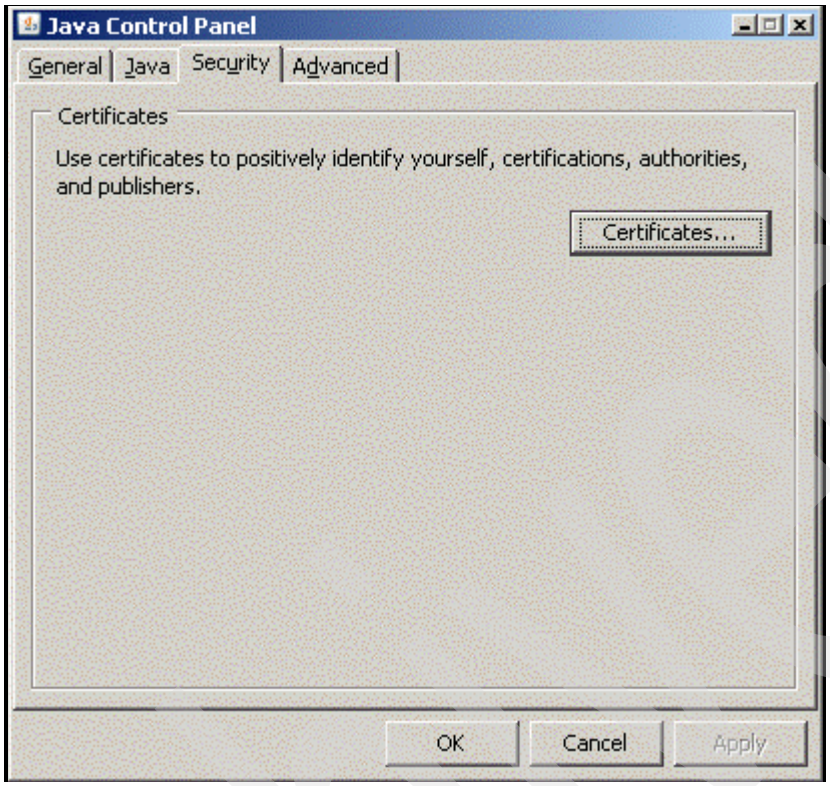



*Figure 2-13 Java Runtime Environment certificate settings*

5. You should remove the certificate, as shown in Figure 2-14.

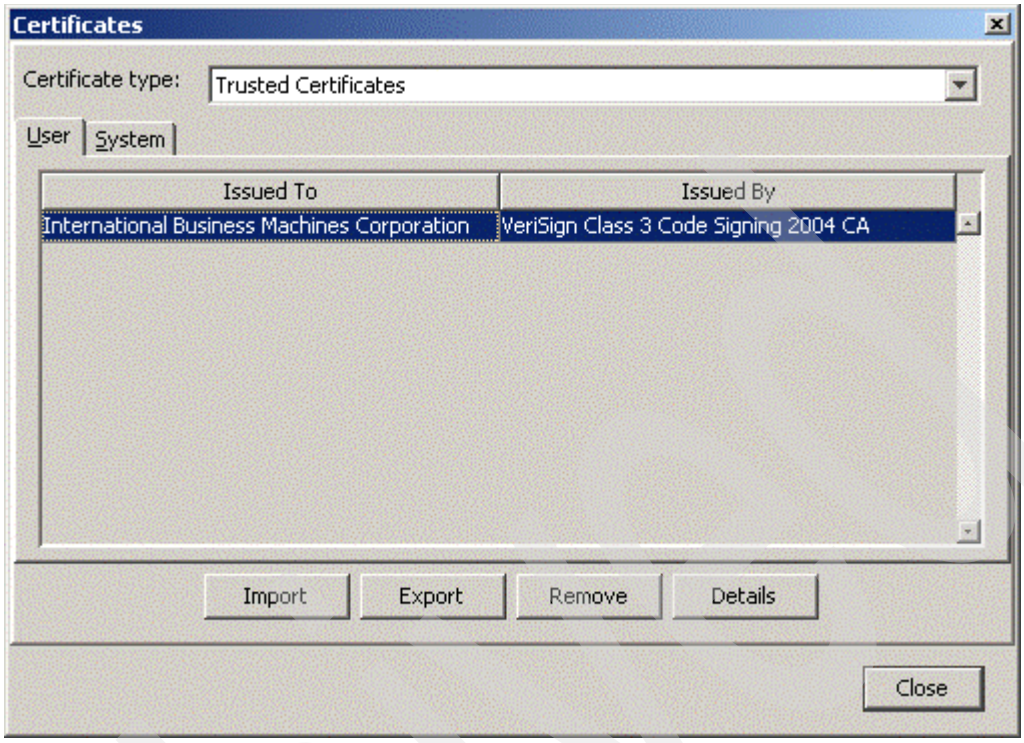



*Figure 2-14 Removing the IBM certificate*

3

# Exploiting configuration information for problem isolation

This chapter provides a scenario that describes the benefits of Tivoli Network Manager and Tivoli Netcool Configuration Manager integration for correlation of network faults and performance indicators to identify the root causes of network problems, including using the launch-in-context feature.

This chapter describes the following topics:

## 3.1 Scenario

This section describes a scenario where we determine the root cause of a network fault in Tivoli Network Manager and take action to resolve the problem in Tivoli Netcool Configuration Manager by launching it through the launch-in-context feature of Tivoli Network Manager.

### 3.1.1 Using configuration change information for problem isolation

Network operations are important for IT organizations, because they provide communication among the services. Without properly working network operations, it is hard to discuss the availability of the service of a business. Indeed, if an organization is a service provider, the importance of network operations is much higher because service availability affects all areas of the service provider's business, so high availability of the network is required. Therefore, there is always a demand for network operations management solutions.

To increase the network operations performance, a monitoring solution that takes action in the shortest possible time is necessary. Integrating Tivoli Network Manager and Tivoli Netcool Configuration Manager lets you use the network monitoring tool to not only determine the root cause of a network problem, but also isolate a possible problem.

This scenario explains how the root cause of a network problem can be identified in Tivoli Network Manager and how the necessary action can be taken in Tivoli Netcool Configuration Manager. The scenario starts with a configuration change performed by a user in Tivoli Netcool Configuration Manager. This change is made by a network operator who monitors the network through Tivoli Network Manager. After making this configuration change, the operator discovers that the change in the configuration of a network device causes a network problem. The operator gathers details about the change from both Tivoli Network Manager and Tivoli Netcool Configuration Manager, and also uses launch-in-context feature that is provided by the integration of these two network tools. As a result, the operator corrects the problem quickly.

In summary, any change in the configuration can be monitored by a network operator, who has a control over the configuration changes in network devices and there shortens the time of resolution.

### 3.1.2 Benefits

The integration of Tivoli Network Manager and Tivoli Netcool Configuration Manager provides the following benefits:

- Integration allows automatic generation of alarms in the Active Event List of Tivoli Network Manager when any change is applied to a network device in Tivoli Netcool Configuration Manager, which provides more control over configuration changes in network devices.
- Automatic alarm generation in Tivoli Network Manager helps operators to make any configuration changes in a network device, and integration of the tools helps operators to check easily whether these changes cause any network problems.
- Using the launch-in-context feature, which results from the integration of Tivoli Netcool Configuration Manager and Tivoli Network Manager, helps the operator to check configuration changes in Tivoli Netcool Configuration Manager and take action in the shortest possible time.

### 3.1.3 Using configuration change information for the problem isolation flow

Figure 3-1 shows the high level operation flow when using configuration change information for problem isolation scenario.

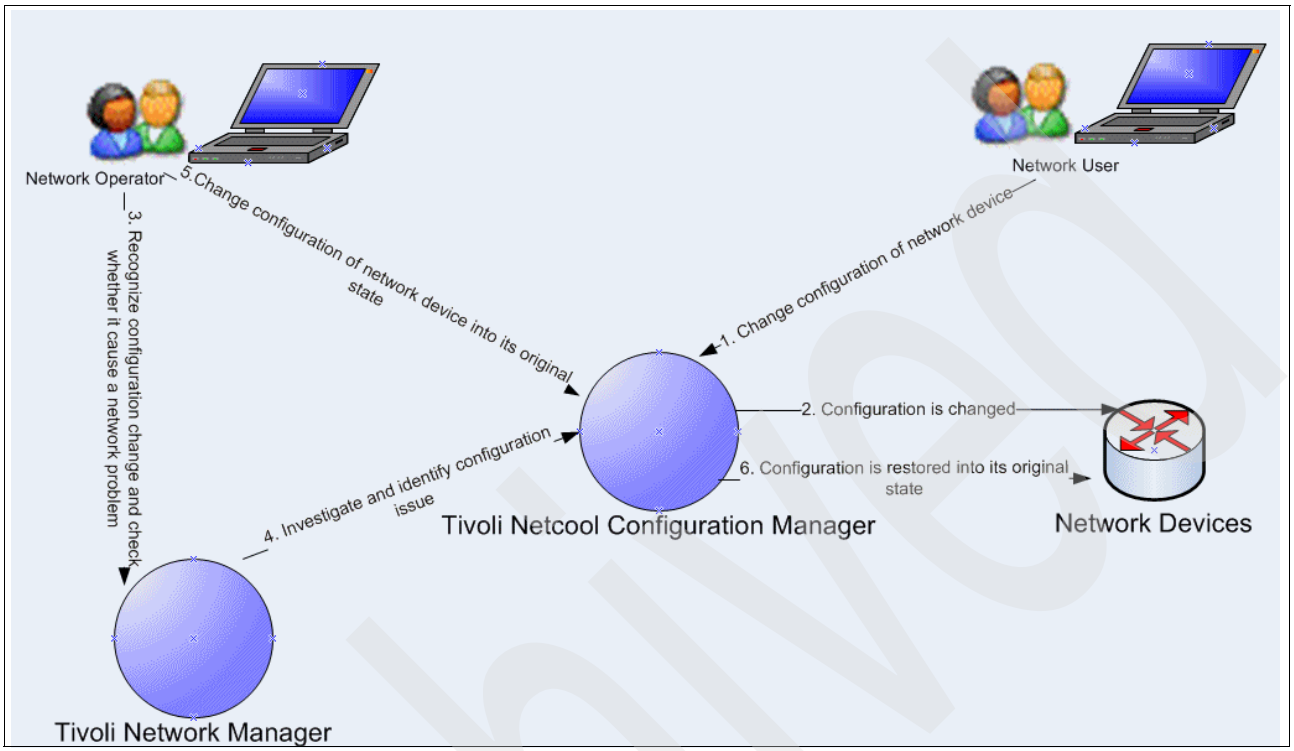



*Figure 3-1 High level flow of the scenario*

## 3.2 Monitoring configuration changes to resolve issues

As described in the previous sections, monitoring with Tivoli Network Manager provides information about the health of the network devices. Integrating Tivoli Network Manager and Tivoli Netcool Configuration Manager provides the ability to monitor configuration changes performed in Tivoli Netcool Configuration Manager in Tivoli Network Manager. This scenario helps network operators not only to recognize the problem as soon as it occurs, but also to become able to understand the root cause of the problem more easily.

In this scenario, a configuration change is performed by UserA in Tivoli Netcool Configuration Manager. The operator sees an alarm in the Active Event List in Tivoli Network Manager. The operator checks the status of the device (that set off the alarm) in the network map. After recognizing the problem, the operator launches a report of unit work summary by using the launch-in-context feature and observes that there is a configuration change in the network device. Then, the operator launches Tivoli Netcool Configuration Manager from Tivoli Network Manager by using the launch-in-context feature and applies the necessary action to correct the problem. Afterwards, the status of that device is checked in Tivoli Netcool Configuration Manager and we note that the problem is resolved.

### 3.2.1 Changing the configuration in Tivoli Netcool Configuration Manager

To make a configuration change on a network device, log in to Tivoli Netcool Configuration Manager by opening a web browser and entering the appropriate address to reach the web console of the application.

For this scenario, Tivoli Netcool Configuration Manager is installed on server with that has the IP address `9.196.131.164` and uses port 7001:

```
http://9.196.131.164:7001
```

Perform the following steps:

1. Enter the credentials to log in to the console, as shown in Figure 3-2, and click **Login**.

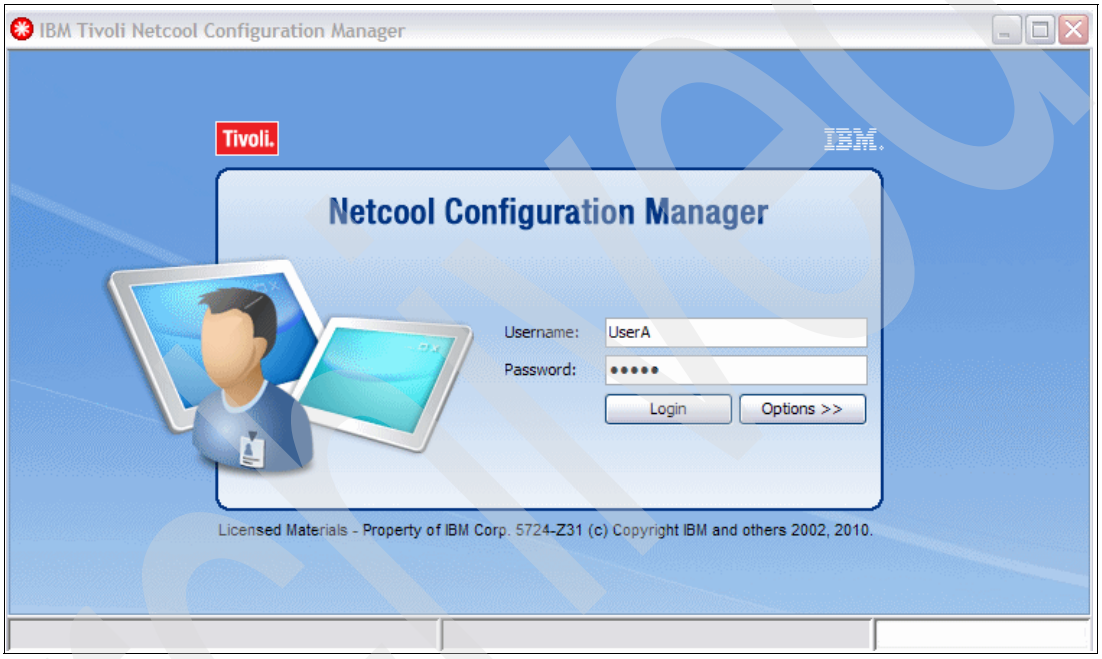



*Figure 3-2 Tivoli Netcool Configuration Manager login window*

2. After entering the credentials, a new page opens, as shown in Figure 3-3. Click **ITNCM Webstart GUI** and enter the credentials again.

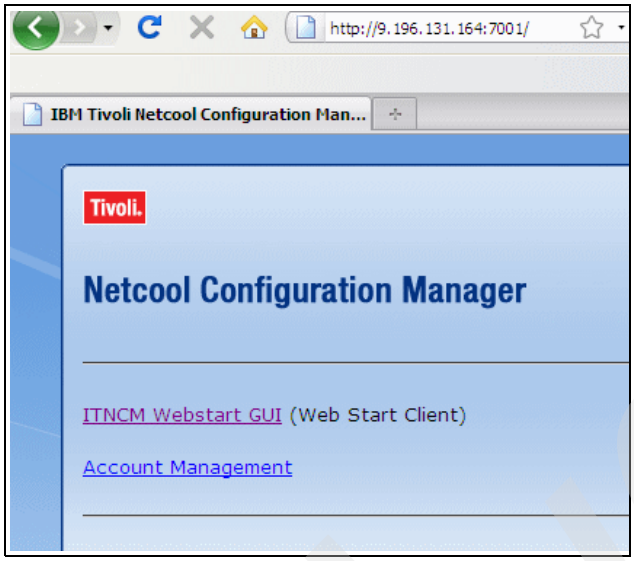



*Figure 3-3 Tivoli Netcool Configuration Manager Webstart GUI (Web Start Client) window*

In this scenario, the Gigabit Ethernet interface of the scotland1-cs35.sco.eu.test.lab integration, which is a Cisco switch, will be shut down. We must change the configuration of the network device by using the Tivoli Netcool Configuration Manager:

3. scotland1-cs35.sco.eu.test.lab is located in SouthBank realm, so expand **Resource Browser** → **ITNCM** → **Southbank**, as shown in Figure 3-4. Click **Southbank**. At the right, all network devices in the Southbank realm are listed. Find scotland1-cs35.sco.eu.test.lab and click it, as shown in Figure 3-4.

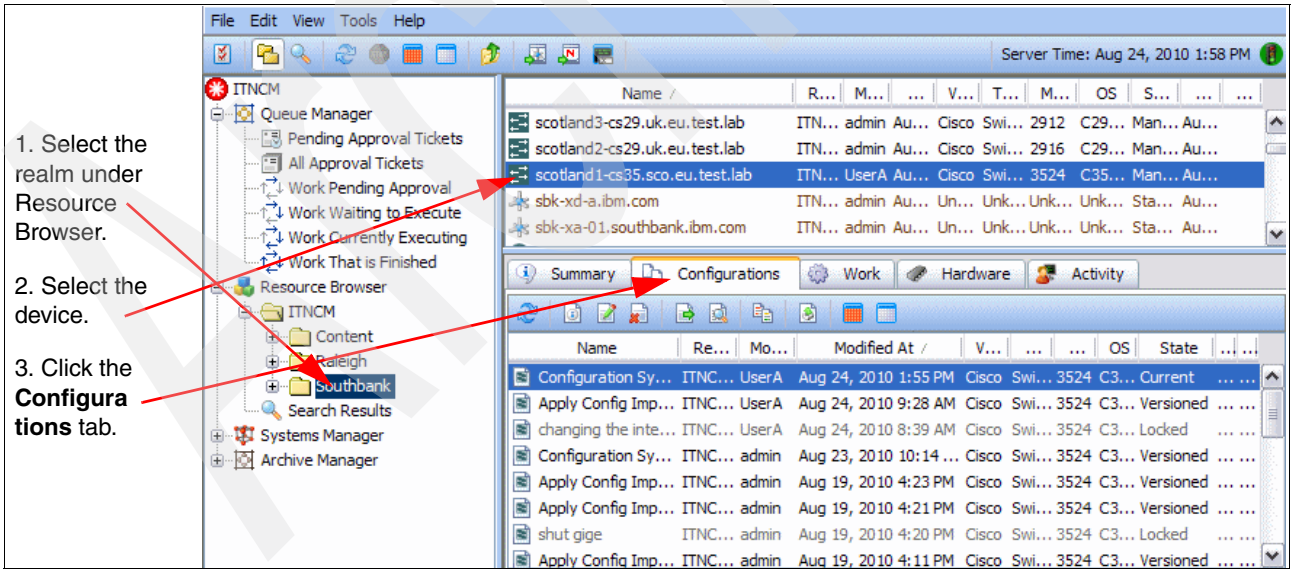



*Figure 3-4 Selecting the device to make a configuration change in Tivoli Netcool Configuration Manager*

4. In the **Configurations** tab, double-click the configuration to open the Configuration Editor.

5. When the Configuration editor window opens, select **interface** → **GigabitEthernet** → **GigabitEthernet 0/1** → **shutdown.** Check the check box to enable the shutdown option (Figure 3-5).

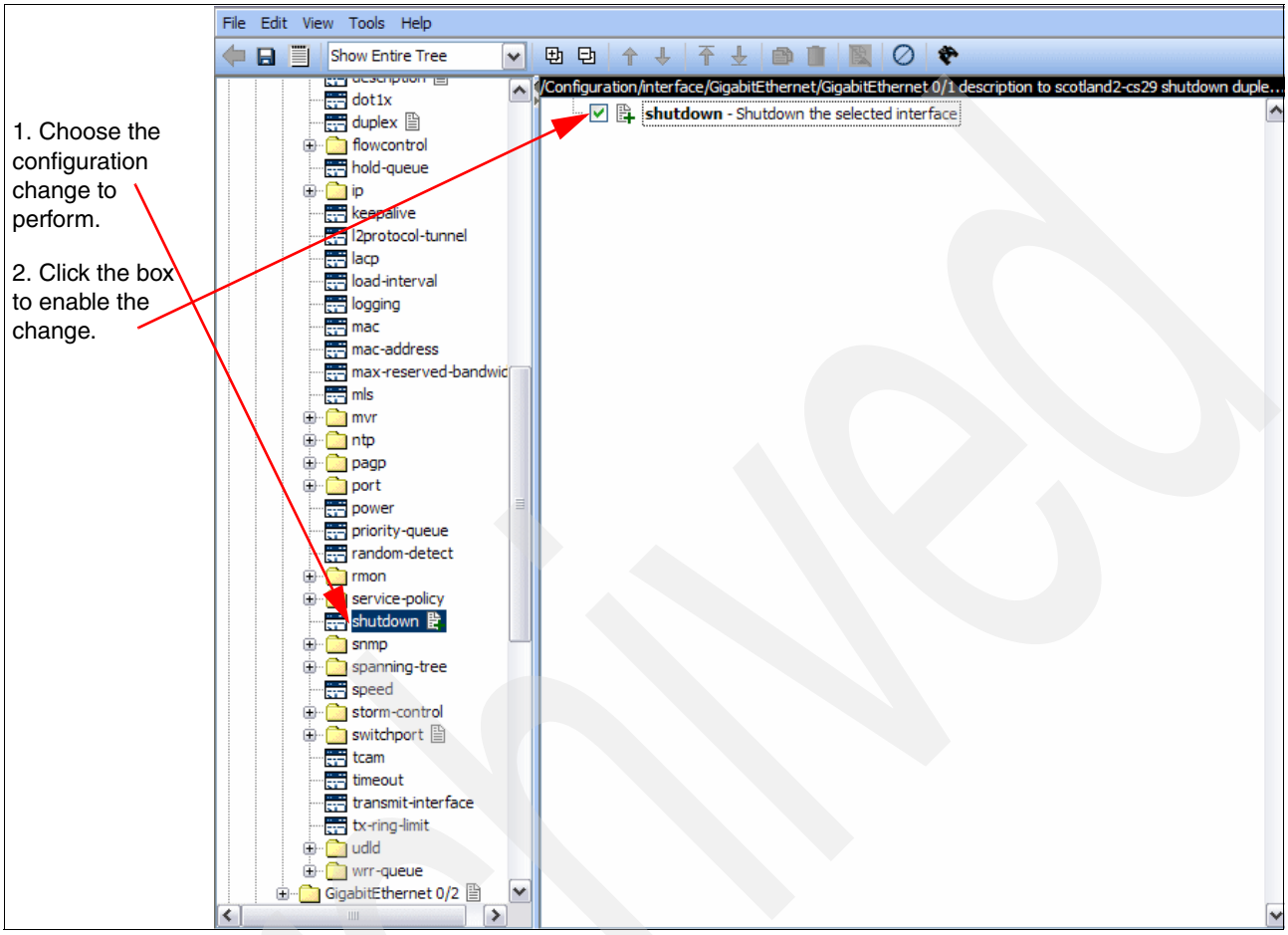



*Figure 3-5 Choosing a configuration change for a selected device in Tivoli Netcool Configuration Manager*

6. Click the **Save** icon ( ).
7. Enter a proper name. (For this scenario, we used “shutdown Gige4”.) Click **OK**.

8. In the Configuration tab, select the created draft configuration and click the **Submit** icon, as shown in Figure 3-6.

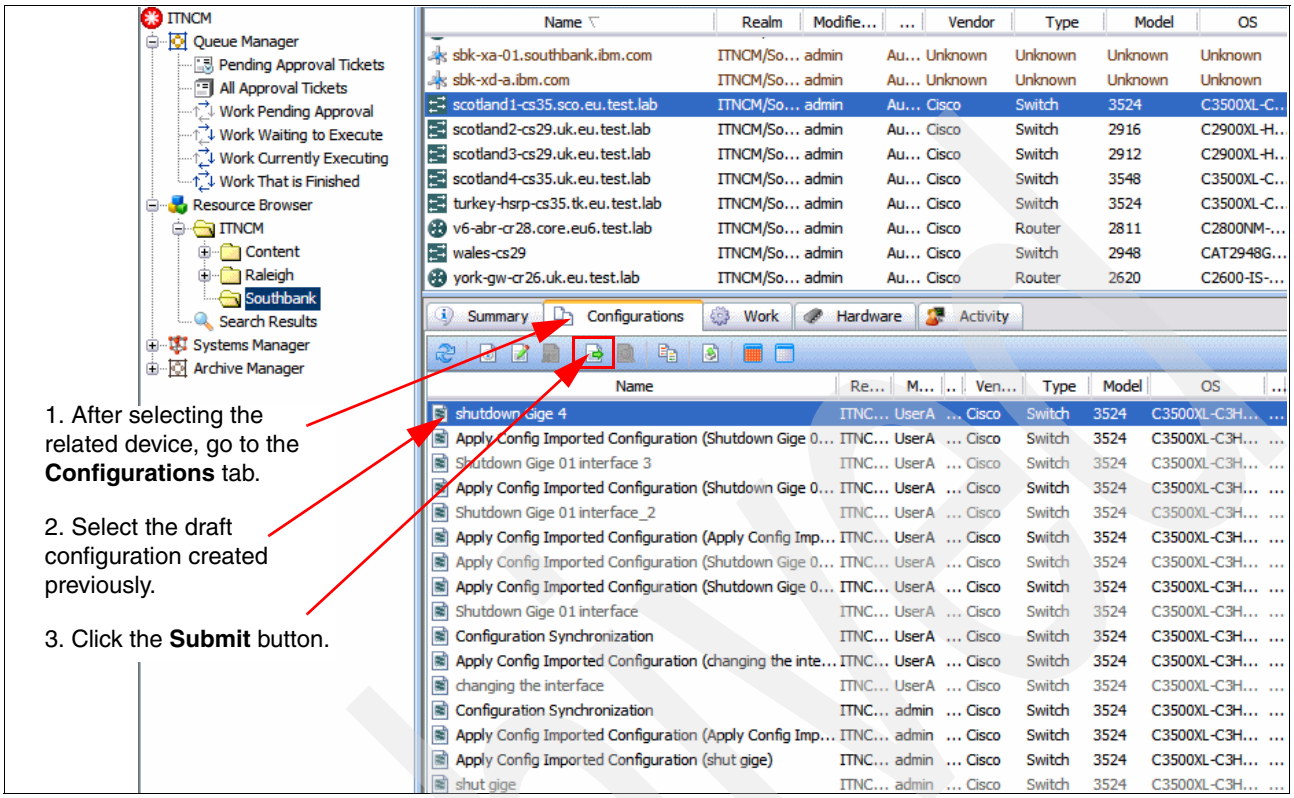



*Figure 3-6 Choosing the draft configuration change and submitting it for execution*

9. In the Password Override window, leave the settings as they are unless the login credentials for a device have changed. Otherwise, the cached credentials are already stored in Tivoli Netcool Configuration Manager. Click **Next**, as shown in Figure 3-7.

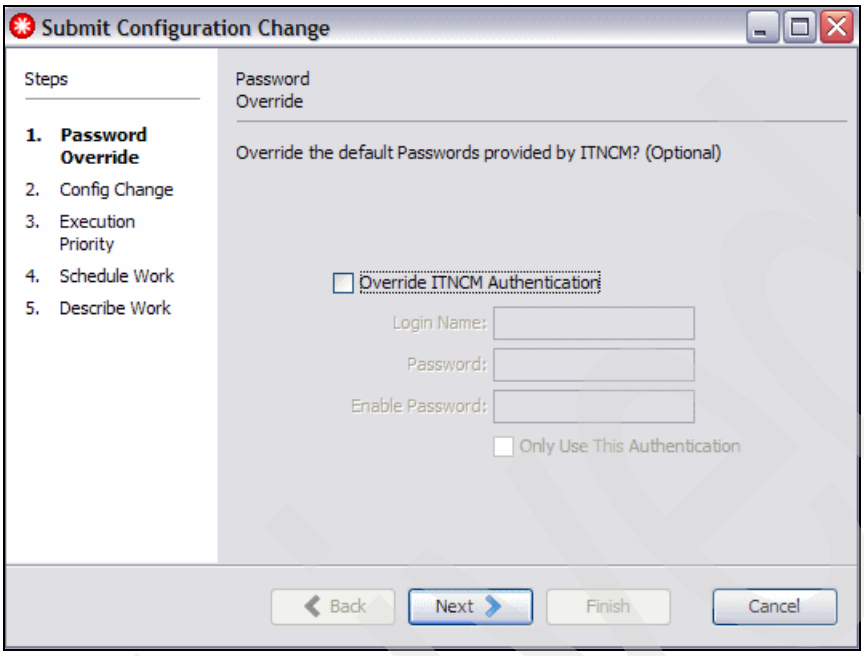



*Figure 3-7 Password Override window*

10. The Config Change window opens (Figure 3-8). Note that we are using a draft version and that the date is indicated in parentheses. Confirm the configuration and click **Next**.

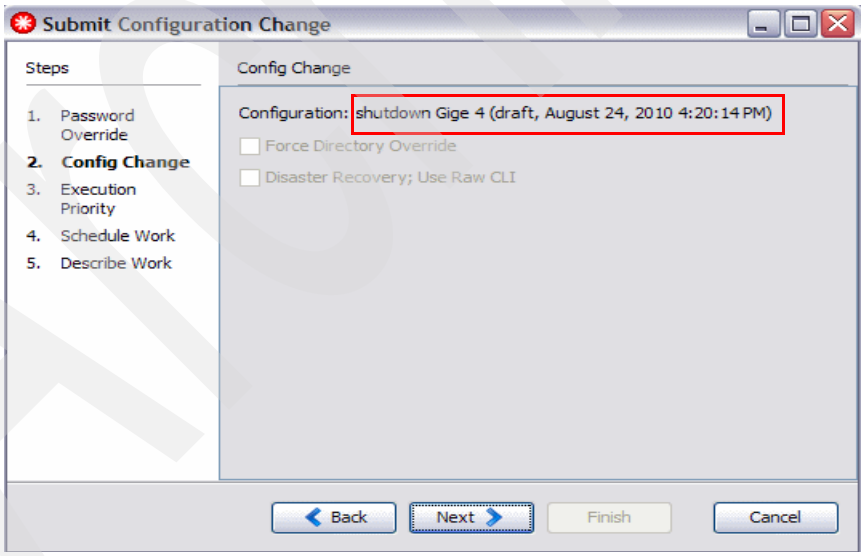



*Figure 3-8 Configuration Change window*

11. Figure 3-9 shows that the execution priority can be set. For this scenario, leave it as Medium and click **Next**.

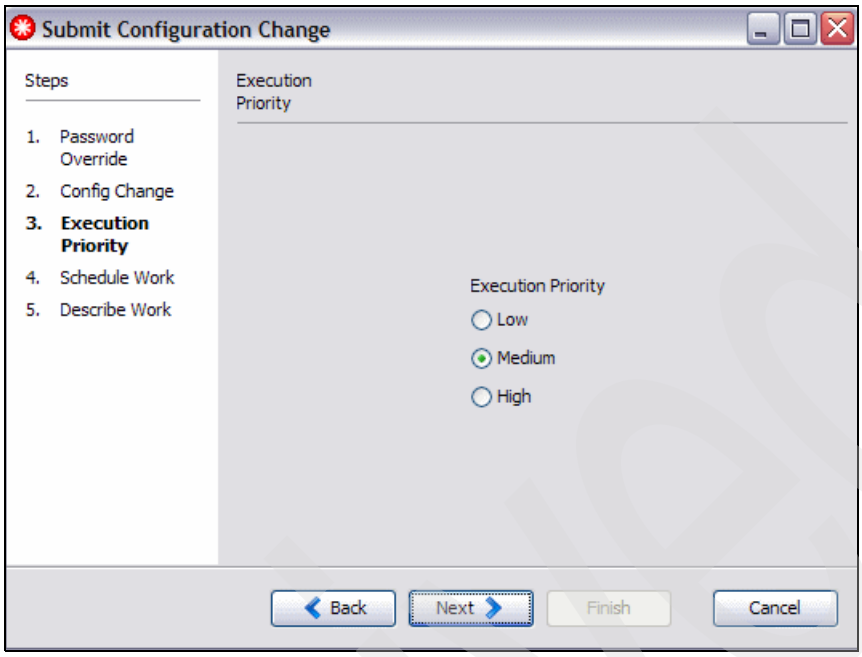



*Figure 3-9 Execution Priority window*

12. In the Schedule Work window (Figure 3-10), there are options for single and recurring schedules. There is also an option for recurring schedules. In this scenario, select **Immediate** to apply the configuration change now, and click **Next**.

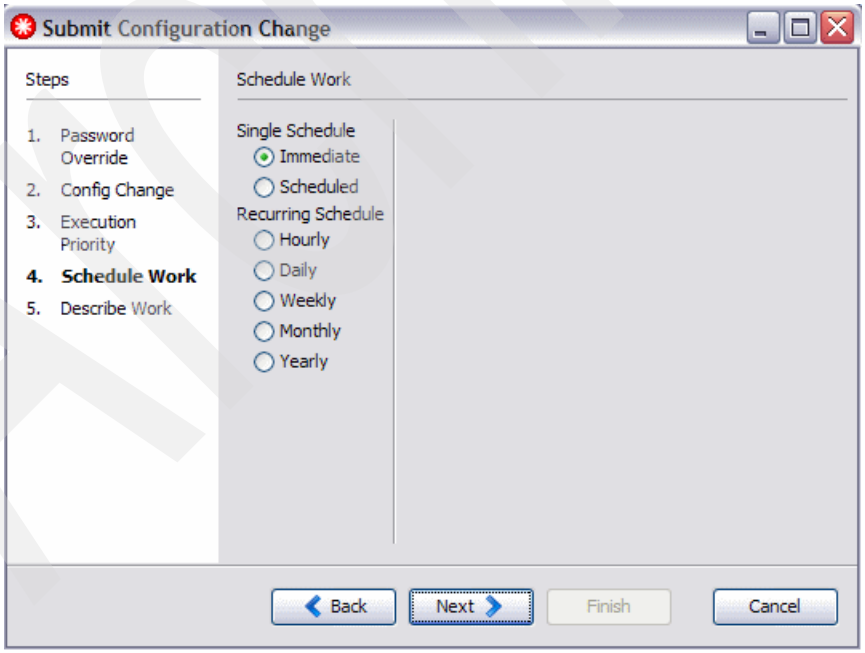



*Figure 3-10 Schedule Work window*

13. In Describe Work window, write a description of the work. For example, in this scenario, we write “Shutdown GigabitEthernet 0/1 interface”, as shown in Figure 3-11.

    Click **Finish** to finalize the configuration change.

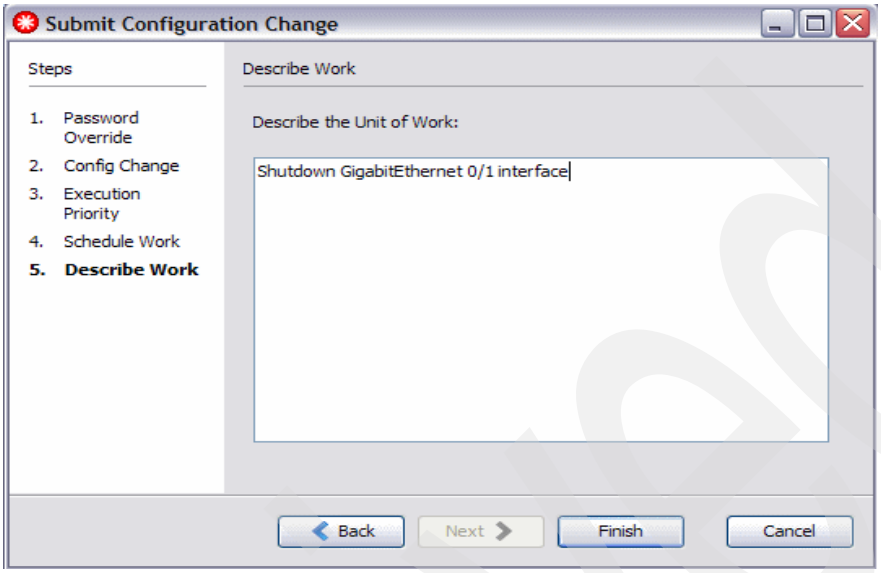



*Figure 3-11 Describe Work window*

14. When the configuration change is submitted, the Unit Of Work (UOW) ID message appears, as shown in Figure 3-12. Note the UOWID, which is #476, as we refer to it in the following sections.

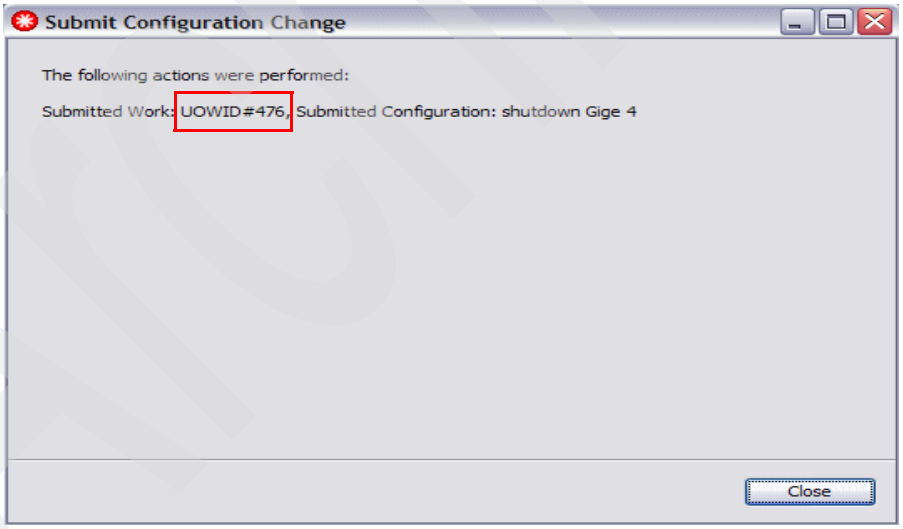



*Figure 3-12 Submission of configuration change message*

By submitting this configuration change, the user “UserA” has shut down an interface of the network device using Tivoli Netcool Configuration Manager. In the following section, we explain how to observe the related alarm in Tivoli Network Manager as an operator.

### 3.2.2 Monitoring Tivoli Network Manager for configuration changes done through Tivoli Netcool Configuration Manager

In this section, a user called “Operator”, who is responsible for monitoring the alarms in Tivoli Network Manager and taking necessary actions, takes note of the configuration change and checks its details by using the launch-in-context feature of Tivoli Network Manager.

For this scenario, Tivoli Network Manager is installed on a server that has the IP address `9.196.131.166`. The link to reach the web console of Tivoli Network Manager is:

```
https://9.196.131.166:16316/ibm/console/logon.jsp
```

As mentioned earlier, web access to Tivoli Network Manager is built on Tivoli Integrated Portal. Log in as the Operator user, as shown in Figure 3-13.

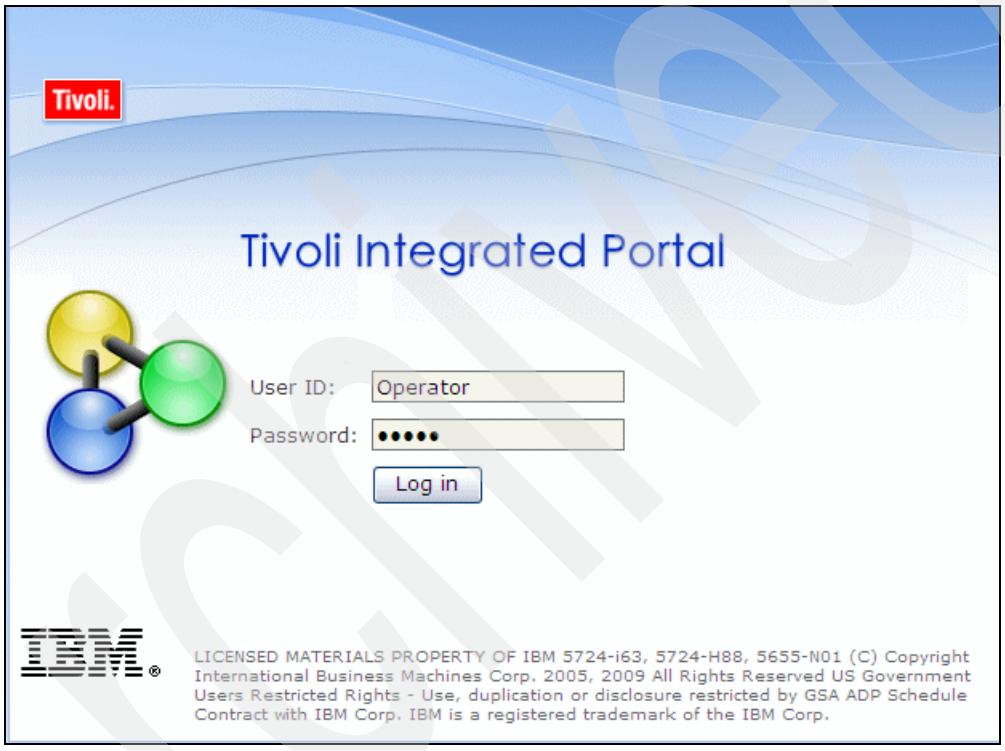



*Figure 3-13 Tivoli Integrated Portal login window used to access Tivoli Netcool Manager*

To monitor and interpret events, perform the following steps:

1. Expand **Availability** → **Events,** and click **Active Event List (AEL)**, as shown in Figure 3-14.

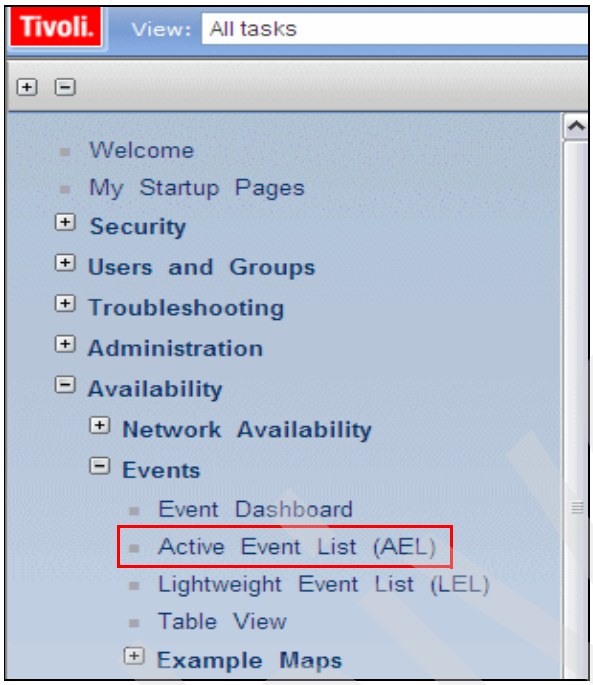



*Figure 3-14 Active Event List (AEL) in Tivoli Network Manager*

The Active Event List is a list of alarms gathered from network devices through probes. As described in 2.4, “Data integration” on page 24, the integration of Tivoli Network Manager and Tivoli Netcool Configuration Manager provides a flow of information about the configuration changes performed in Tivoli Netcool Configuration Manager through the SNMP probe.

Events for configuration change operations performed in Tivoli Netcool Configuration Manager appear in the Active Event List in Tivoli Network Manager with the information “Configuration Changed via Command Line...” written in the Summary field by default. Considering that any change in a configuration does not lead to a problem every time, the severity of these type of events is at the Information level. However, rules may be defined at the probe level for events that come from a specific device on which configuration changes cause errors in the network, and the severity of these type of events can be increased by defining rules in the probe rules file. For further details and all other related product documentation, refer to the Tivoli Netcool/OMNIbus documentation available at the following address:

`http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm`

In this scenario, the default configuration of the probe rules file is used. Therefore the severity of these events is at the Information ( ) level.

2. In the Active Event List, as shown in Figure Figure 3-15, there is a Configuration Change event for node 172.20.98.1.

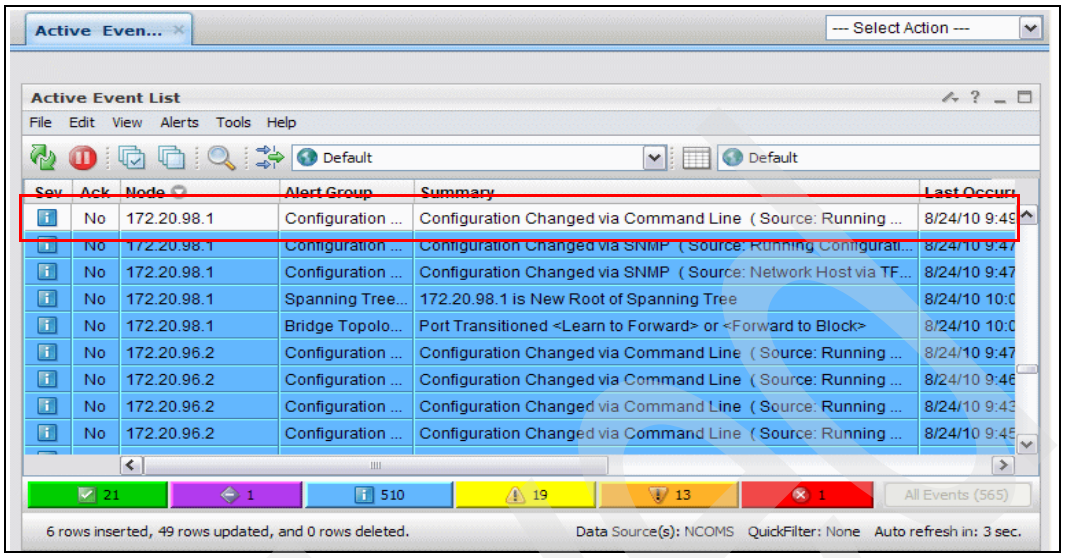



*Figure 3-15 Configuration change event in Active Event List*

This event indicates that there has been a configuration change in device 172.20.98.1. However, the event does not give details about the configuration change. It can be any configuration change, such as changing the access list of an interface of the device or, more severely, shutting down the interface, as is the case in this scenario. To obtain more details, check the status of the device from the network topology map.

3. To reach the network topology map, select **Availability** → **Network Availability** → **Hop View.** You can choose only one domain and find the related node by zooming in or, because we know that scotland1-cs35.sco.eu.test.lab is the network device that we want to focus on, you can enter Southbank in the Domain field, scotland1-cs35.sco.eu.test.lab in the Seed field, choose 3 in the Hops field, and click **Submit** ( ).

4. In the Hop view, shown in Figure 3-16, it shows that there is a major event on scotland1-cs35.sco.eu.test.lab. In addition, there are network problems with scotland2-cs29.uk.eu.test.lab and scotland3-cs29.uk.eu.test.lab. This view indicates that ping tests from Tivoli Network Manager failed on both devices.

   Based on the information from the Active Event List that there has been a configuration change on scotland1-cs35.sco.eu.test.lab, and considering that these network devices are related according to the network topology map, the network problems of these three devices might also be related.

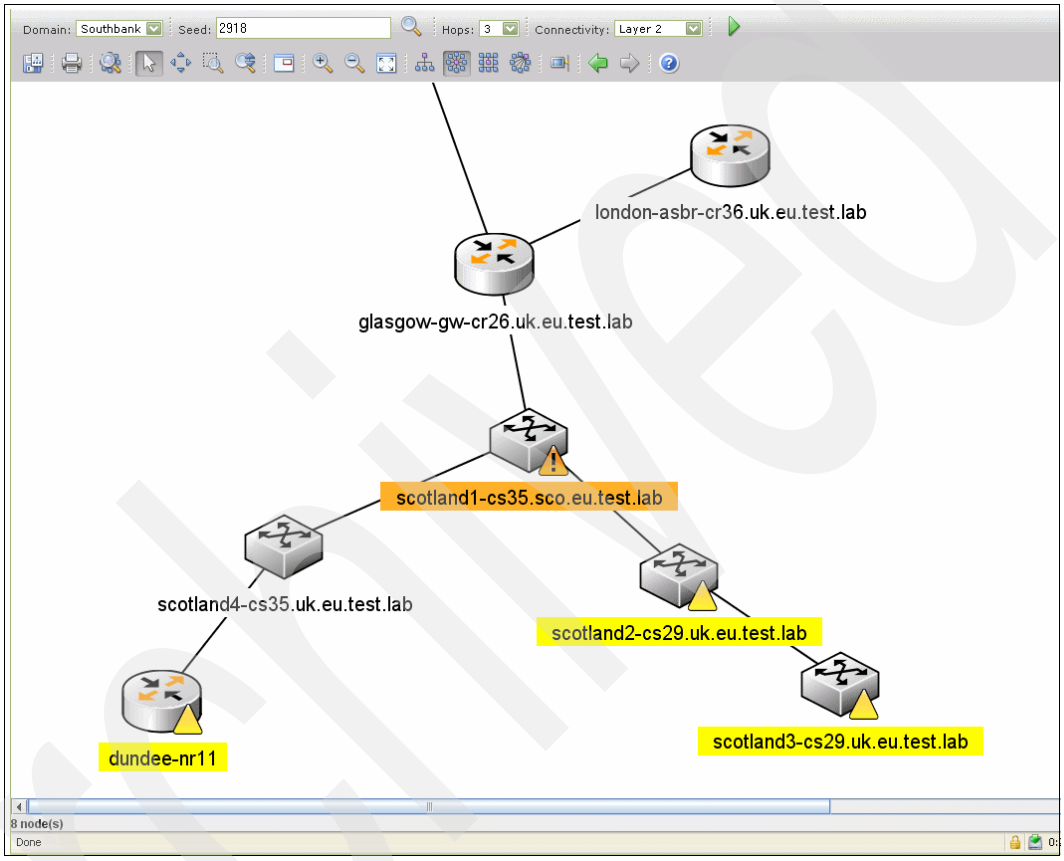



*Figure 3-16 Hop View window showing the health status of the network device*

So far, the Operator user has limited information: There are network problems on these three devices, the event severity level on scotland1-cs35.sco.eu.test.lab is Major, and scotland2-cs29.uk.eu.test.lab" and "scotland3-cs29.uk.eu.test.lab" are not reachable according to ping test results in Tivoli Network Manager. However, the root cause of the network problem is still unknown. In the next section, we explain how to troubleshoot this situation.

## 3.2.3 Troubleshooting

The Unit Of Work (UOW) summary is helpful in obtaining more details about the configuration change. The summary is a brief description of works performed on a network device. It is a property of Tivoli Netcool Configuration Manager, but it can also be launched from Tivoli Network Manager by using the launch-in-context feature.

To use the UOW summary to help you troubleshoot, perform the following steps:

1. To launch “Device Unit Of Work Summary”, right-click the event. Select **Configuration Management** → I**TNCM Reports** → **Device Unit Of Work Summary** in the context menu shown in Figure 3-17.

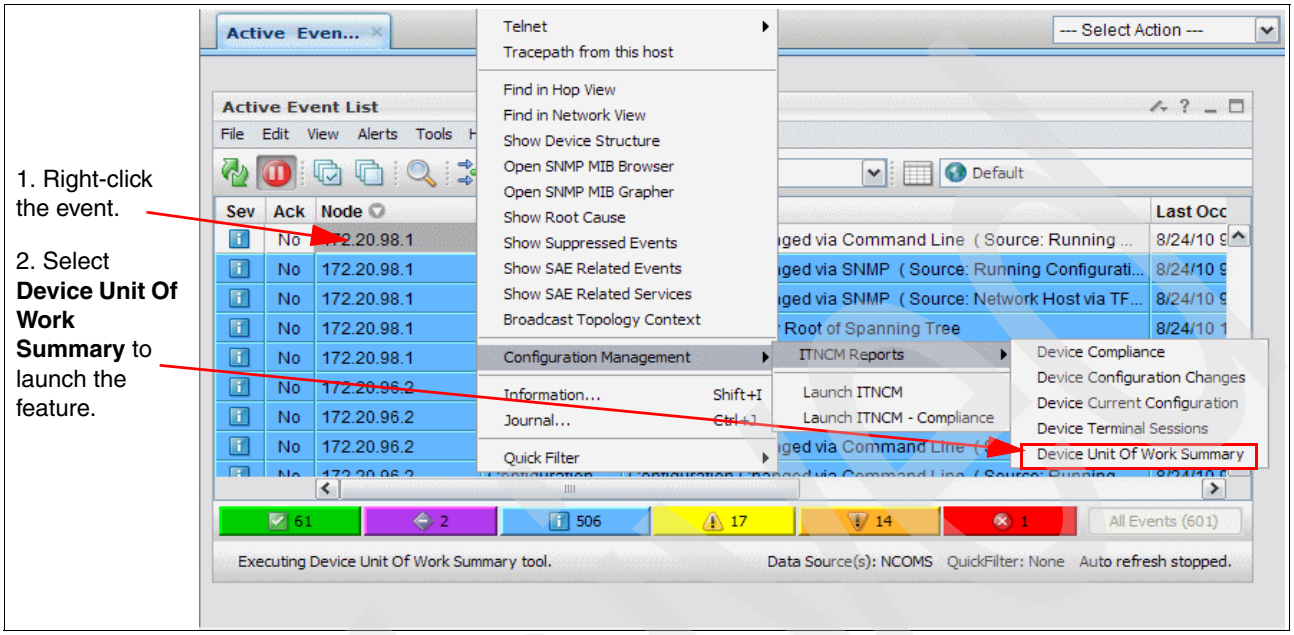



*Figure 3-17 Launching the Device Unit Of Work summary*

The Device Unit Of Work Summary window gives a list of all configuration changes performed in the network device. In this scenario, we are focusing on the network device that has the IP address 172.20.98.1. As shown in Figure 3-18, the latest change is “Shutdown GigabitEthernet 0/1 interface”. This UOW explains the ping failures and network events for the scotland2-cs29.uk.eu.test.lab and scotland3-cs29.uk.eu.test.lab devices discussed in step 4 on page 54 and shown in Figure 3-16 on page 54.

In addition, Figure 3-18 shows when the action was performed and who performed it. Information is also available in the Device Unit Of Work Summary window.

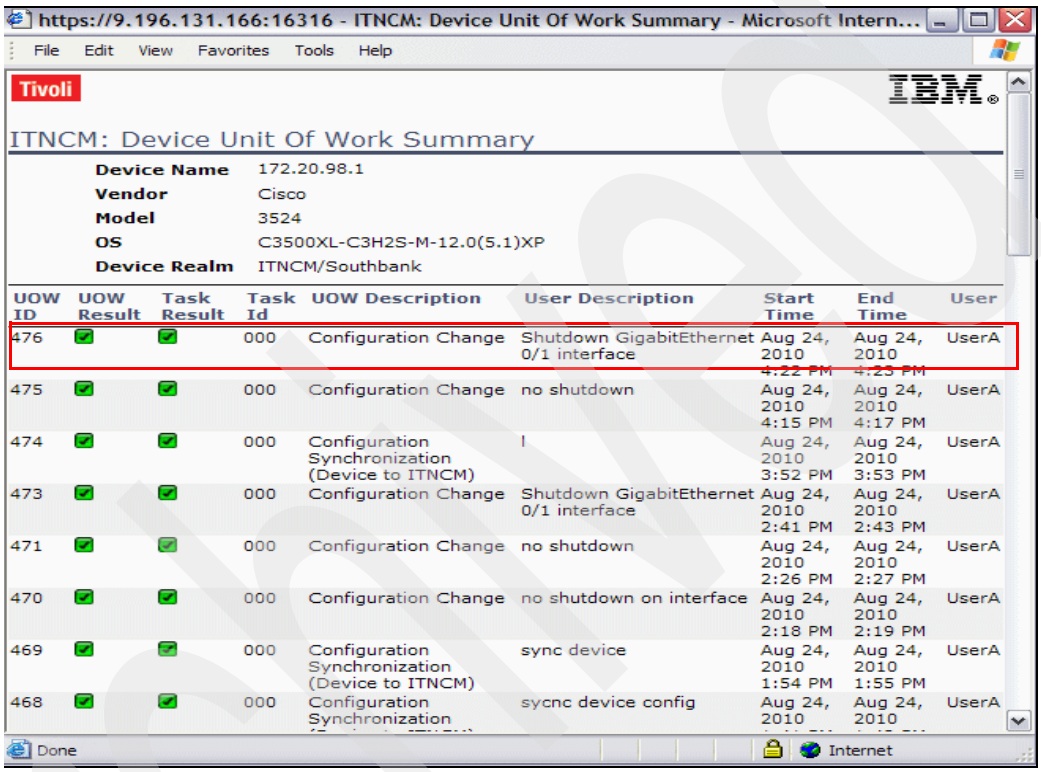



*Figure 3-18 Device Unit of Work Summary window*

Remember that in step 14 on page 50, when UserA submits the configuration change, the UOW ID is provided, which is #476. Note that it is the same as the latest UOW ID in the Device UOW Summary list (Figure 3-18).

2. To verify the change, log in to Tivoli Netcool Configuration Manager through Tivoli Network Manager by using the launch-in-context feature. Right-click the alarm and select **Configuration Manager** → **Launch ITNCM** (Figure 3-19).

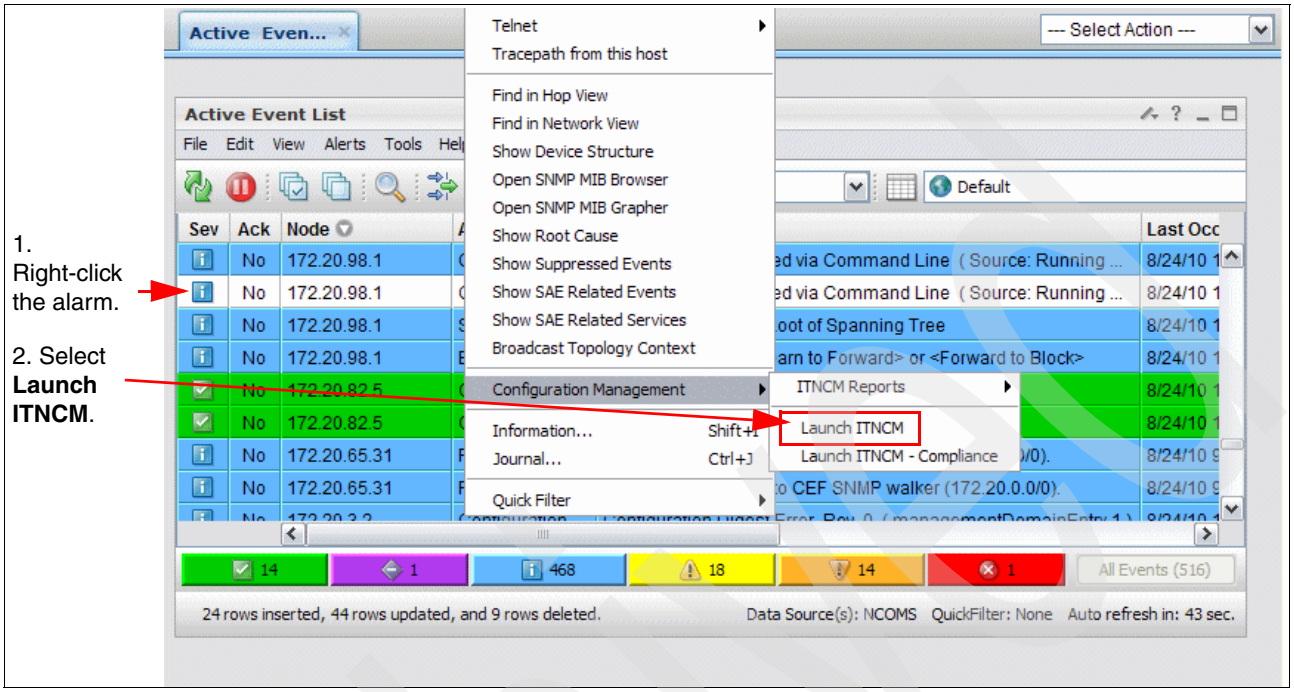



*Figure 3-19 Launch Tivoli Netcool Configuration Manager using the launch-in-context feature*

3. In the login window, enter the login credentials for Tivoli Netcool Configuration Manager (Figure 3-20).


*Figure 3-20 Tivoli Netcool Configuration Manager login window*

4. You can view the finished work in the Queue Manager. You can use the UOW ID to specifically find the finished work. Figure 3-21 shows how to use the Queue Manager to view the finished work.

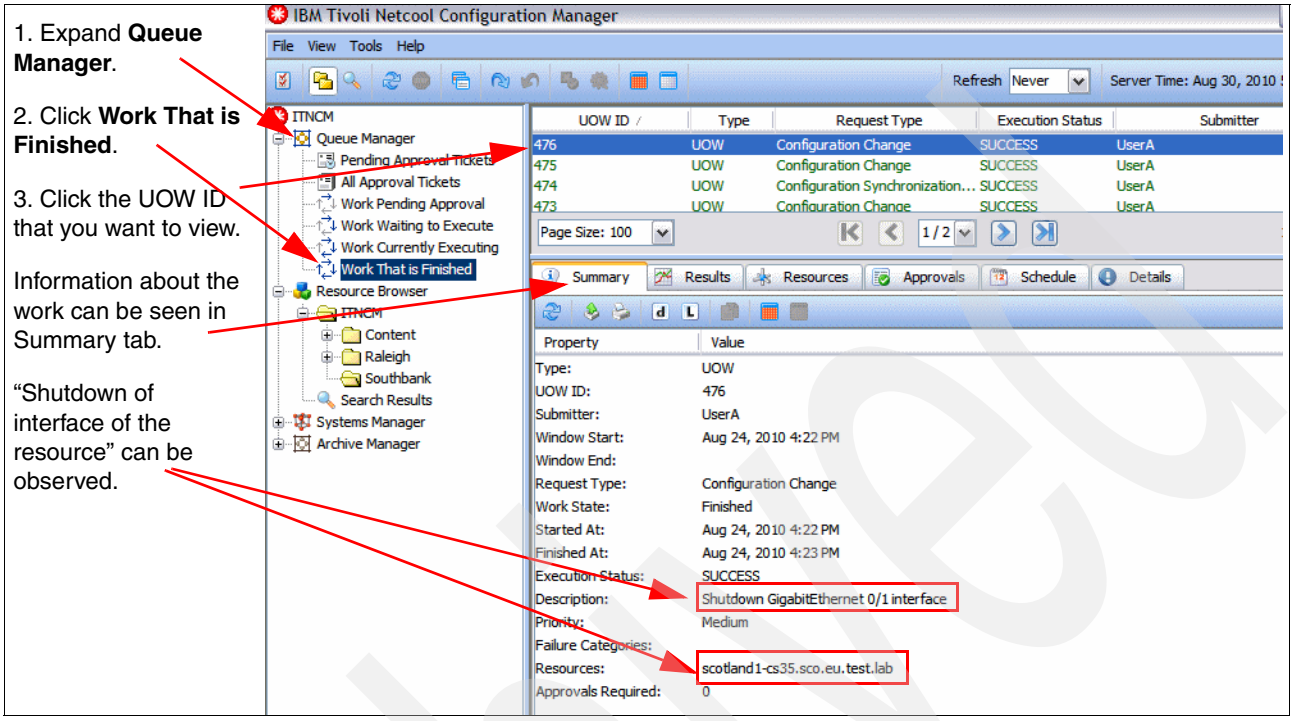



*Figure 3-21 Work That is Finished window in Tivoli Netcool Configuration Manager*

In the list, find the UOW ID (#476) that you found in the Device Unit Of Summary list. Check the information in the Summary tab. Figure 3-21 shows that the UOW ID refers to scotland1-cs35.sco.eu.test.lab.

5. To see the command that is run to change the configuration of the interface, double-click the UOW ID #476 and click the resource. The log (Figure 3-22) reveals that a shutdown command is run on the GigabitEthernet 0/1 interface as observed in configuration change description in the previous step.

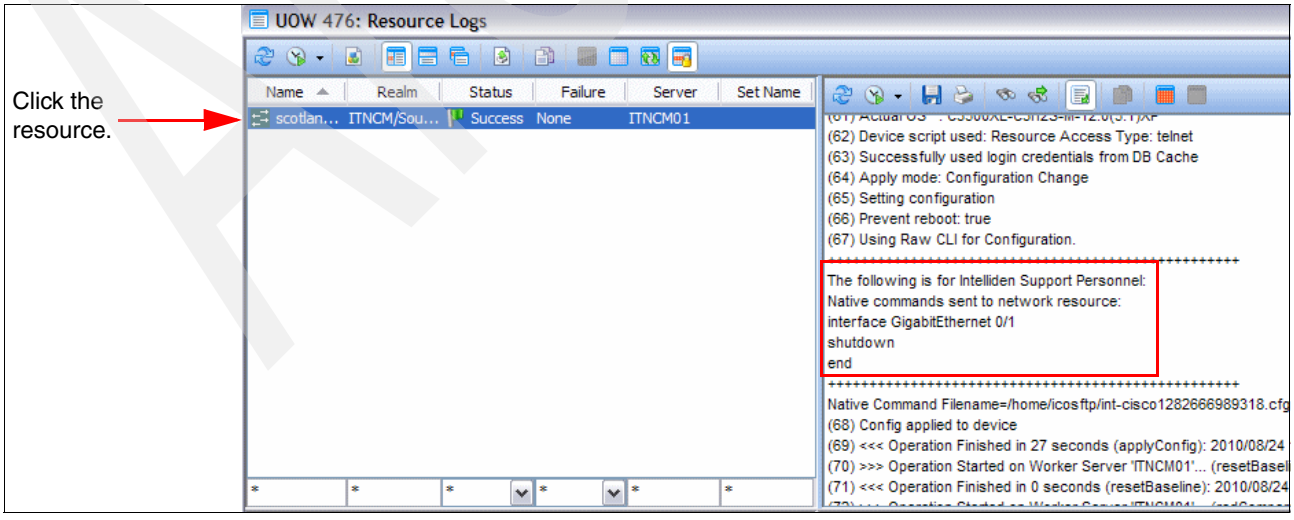



*Figure 3-22 Resource log of unit of work performed to shut down the GigabitEthernet interface of the network device*

Because the change in configuration is identified, the next action by the Operator user is to undo the change, which will correct the problem.

## 3.2.4 Undoing the configuration change

In this section, we explain how to change the interface configuration back to the “no shutdown” configuration.

Perform the following steps:

1. To undo the configuration change performed by UserA, navigate to **Resource Browser** → **Southbank** and click **scotland1-cs35.sco.eu.test.lab** (Figure 3-23). Double-click the **Apply Config ImportedConfiguration (shutdown Gige 4)** configuration, which is the “Current” configuration.

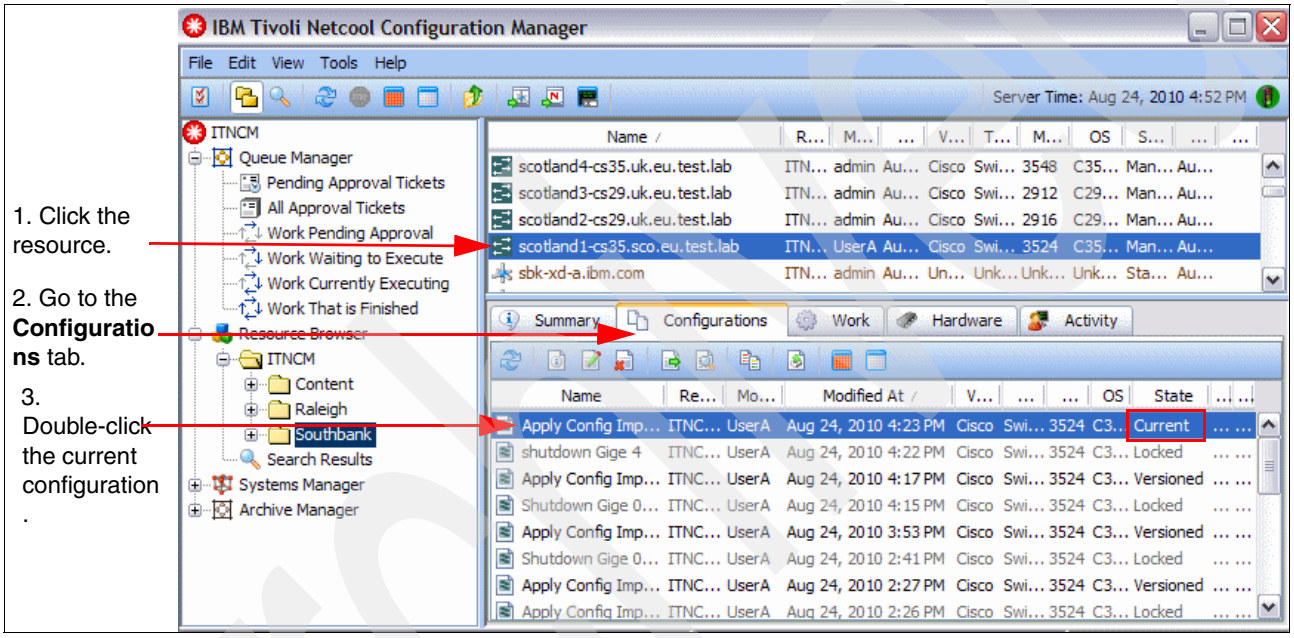



*Figure 3-23 Selecting the current configuration of the network device*

2. Expand **interface** → **GigabitEthernet** → **GigabitEthernet 0/1** and click **shutdown**. Clear the shutdown option check box to undo the shutdown of the interface (Figure 3-24).

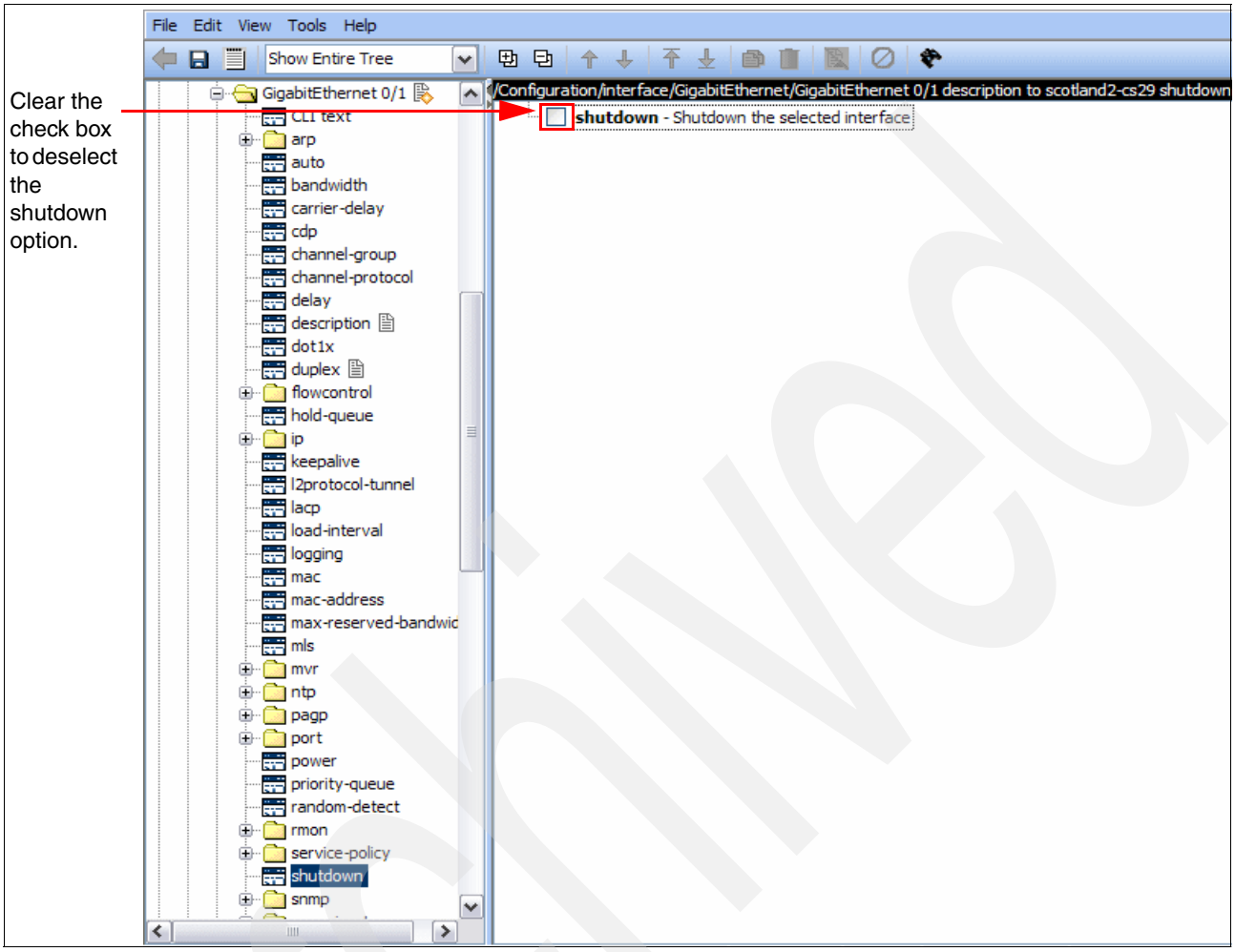



*Figure 3-24 Clear the shutdown check box in the GigabitEthernet 0/1 configuration*

3. To save the change, click **Save** ( ).

   Enter a proper name that describes the configuration change, for example, “Change Gige interface to no shutdown”. Click **OK**.

4. When the draft configuration change is saved, find it in the Configuration tab and submit it (Figure 3-25).

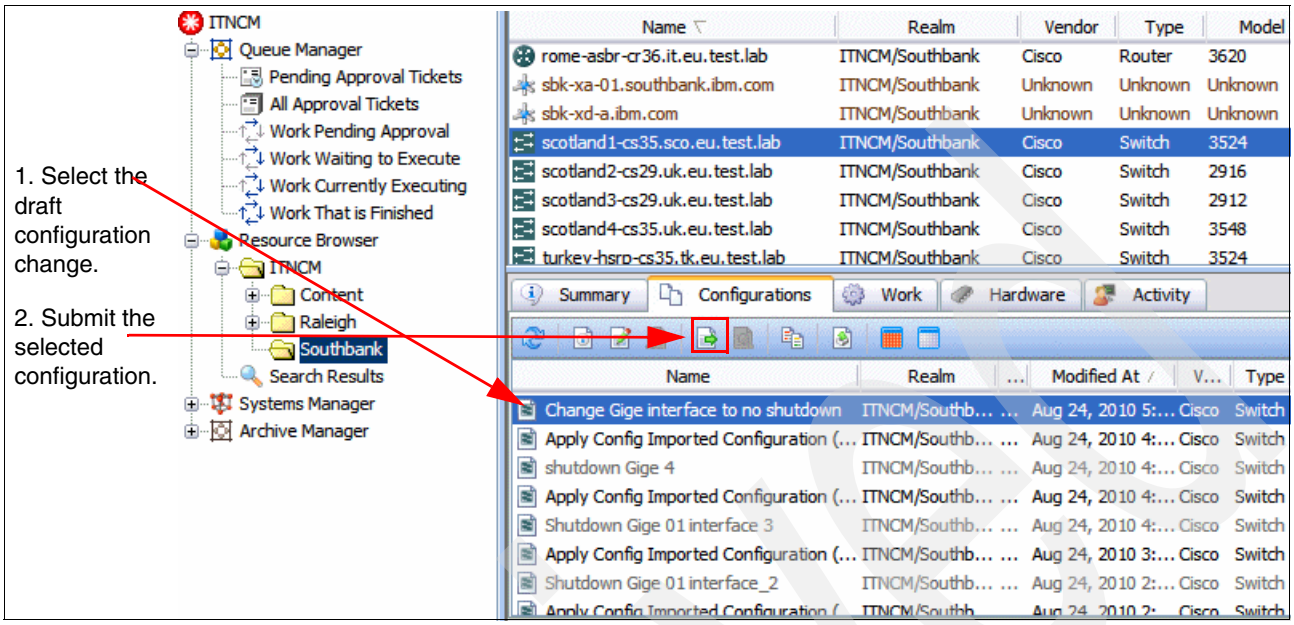



*Figure 3-25 Submitting the undo of the change to no shutdown*

5. When the selected configuration change is submitted, the Submit Configuration Change window opens. The first step is the **Password Override** step, which is described in step 9 on page 48. Use the settings shown in Figure 3-26 for this step and click **Next**.

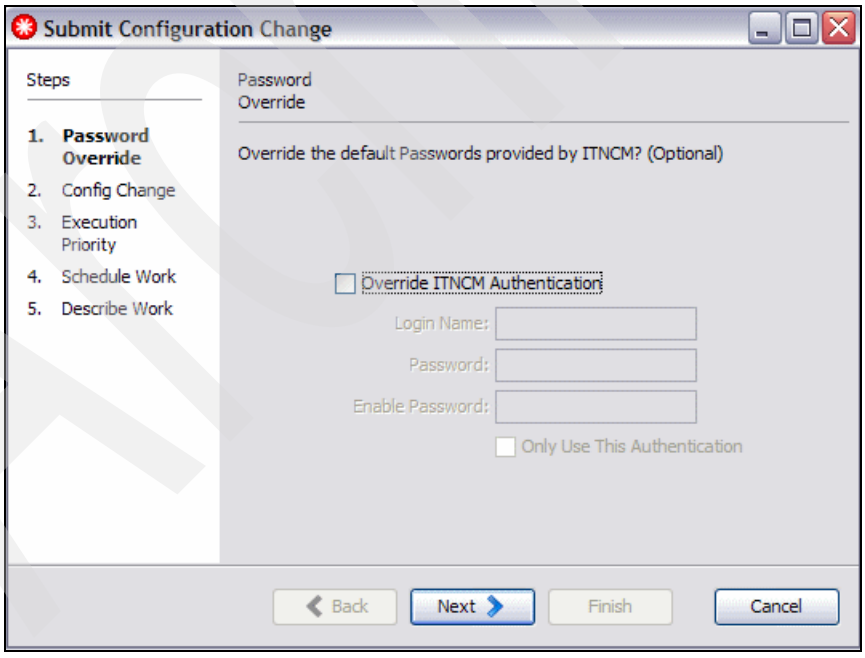



*Figure 3-26 Password Override step*

6. Figure 3-27 shows the Config Change step. Validate the configuration and click **Next.**

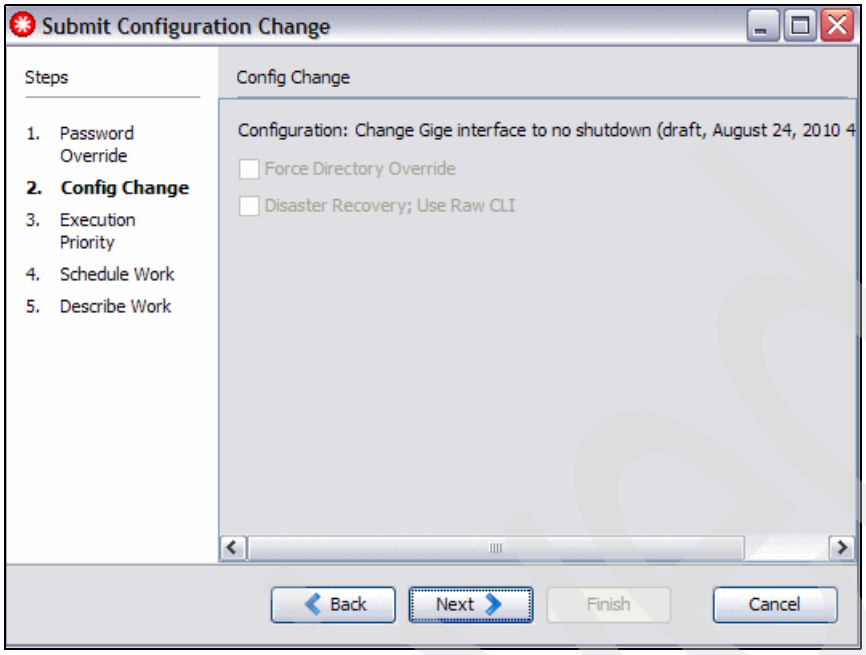



*Figure 3-27 Config Change step*

7. For the Execution Priority step, leave it at Medium and click **Next**.
8. For the Schedule Work step, accept the Immediate setting and click **Next**.
9. In Describe Work step, enter a proper description. We use the “Change the GigabitEthernet 0/1 interface back to no shut down” description in our scenario (Figure 3-28). Click **Finish** to finalize the submission of the change.

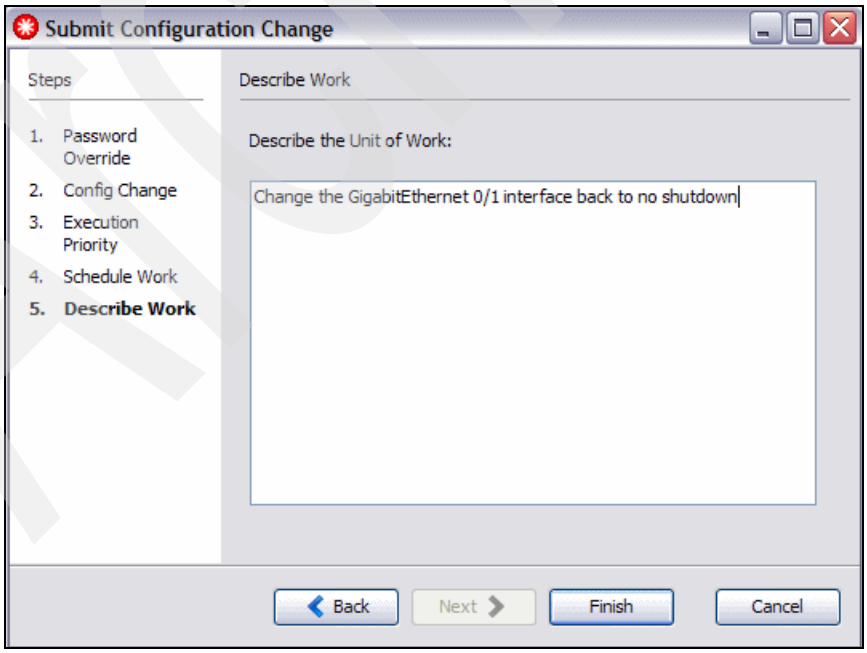



*Figure 3-28 Description of the configuration change for no shutdown*

10. When the configuration change is submitted, the Unit Of Work (UOW) ID message window opens (Figure 3-29). Note that the UOW ID is *#477*.

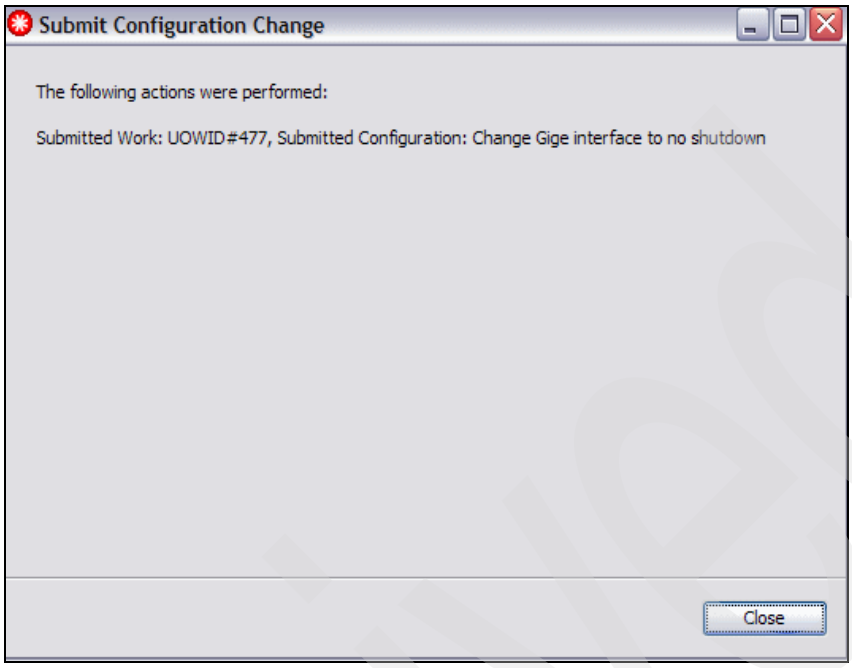



*Figure 3-29 UOW ID information when the "no shutdown interface" configuration change is submitted*

11. To check whether the submitted work has finished successfully, navigate to Queue Manager. As shown in Figure 3-30, select **Work That is Finished**. In the list, look for the UOW ID #477, which is provided when the configuration change is submitted in the previous step.

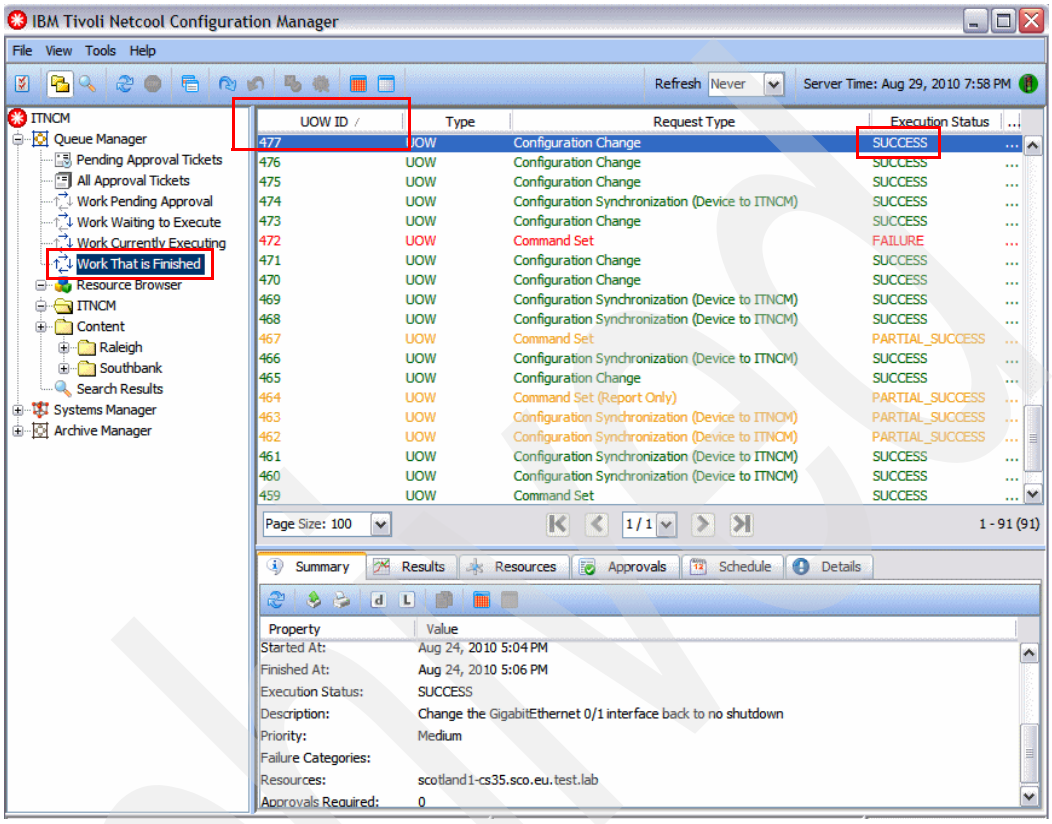



*Figure 3-30 Checking the status of the submitted configuration change for no shutdown*

Figure 3-30 shows that the configuration change for no shutdown has been performed successfully.

12. For more detail about the successfully executed configuration change, check the log. To view the log, double-click the UOW ID #477 and click the resource (Figure 3-31).

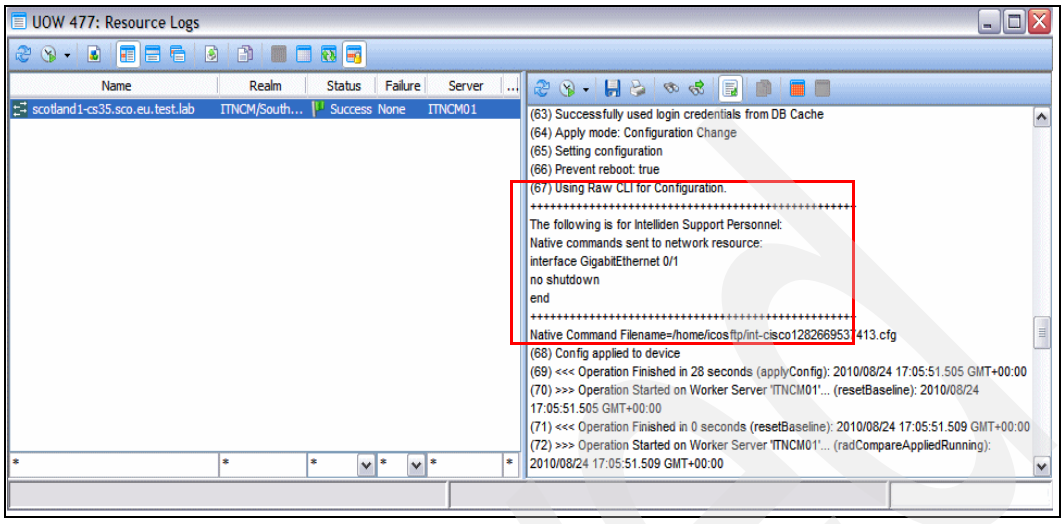



*Figure 3-31 Resource log of configuration change for no shutdown of interface with UOW ID #477*

In the log, note that “no shutdown” is set for interface GigabitEthernet 0/1.

We have undone successfully the configuration change. You can also better validate the configuration change in Tivoli Network Manager.

## 3.2.5 Validating the undo of the change

To validate the undo of the change from Tivoli Network Manager, log in to the Tivoli Network Manager console as the Operator user.

Because the configuration change is performed through Tivoli Netcool Configuration Manager, a configuration change event is generated in Tivoli Network Manager and can be observed in the Active Event List. However, this section focuses on the validation of the change in the device and not its generation., so there is no need to check the event and get the UOW ID. The status of the scotland1-cs35.sco.eu.test.lab network device can be checked directly from the network topology map.

To view the network topology map, select **Availability** → **Network Availability** → **Hop View**. As described in step 3 on page 53, specify **Domain, Seed**, and **Hops** to obtain the map of the network and view the status of the scotland1-cs35.sco.eu.test.lab, scotland3-cs29.uk.eu.test.lab, and scotland2-cs29.uk.eu.test.lab network devices.

As shown in Figure 3-32, the events for scotland2-cs29.uk.eu.test.lab and scotland3-cs29.uk.eu.test.lab are cleared, indicating that the network problem that was caused by a configuration change on the device has been corrected.

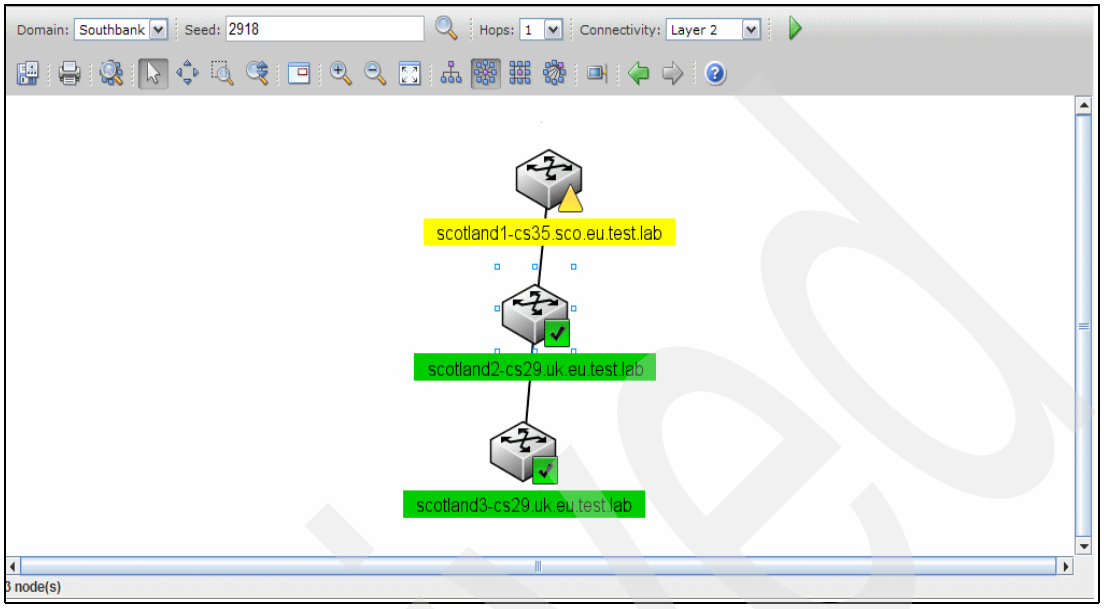



*Figure 3-32 Network map showing that the network problem of the devices has been corrected*

4

# Configuring a rollback after a misconfiguration

This chapter describes a scenario that uses the launch-in-context feature of the integration between Tivoli Network Manager and Tivoli Netcool Configuration Manager to restore a device's configuration to a previous version.

This chapter describes the following topics:

# 4.1 Scenario

The following section provides a brief overview of the scenario for restoring a device's configuration to a network device when an incorrect configuration has been applied.

## 4.1.1 Restoring a device's configuration

Organizations that operate large, complicated, and mission-critical networks require that these networks remain operating at a high level of availability. In the case of service providers, this availability is even more critical, because numerous businesses depend on the service provider for their network. Any network outage caused by a service provider results in a cascading effect across many entities. Because these requirements, organizations deploy network operations centers to maintain, monitor, and repair their networks.

A major responsibility of a network operations center is identifying and resolving problems in the network. In many instances, improperly configured network devices introduce network problems.

Network operators monitor the network for alarm conditions that indicate connectivity issues in the network. Network monitoring tools, such as Tivoli Network Manager, provide monitoring capabilities. However, when a network device configuration change is the root of a network problem, it is difficult to determine the change that was made to the configuration.

This scenario describes how network operators can use the integration between Tivoli Network Manager and Tivoli Netcool Configuration Manager to troubleshoot network problems caused by an incorrect device configuration. Likewise, the scenario demonstrates how a network operator can restore a device configuration to a known good state after a problem has been isolated to a specific device configuration.

The scenario describes the process in two parts:

1. Device configuration troubleshooting
2. Device configuration restoration

## 4.1.2 Benefits

The integration between Tivoli Network Manager and Tivoli Netcool Configuration Manager results in the following benefits:

- This integration provides the ability to launch from Tivoli Network Manager directly into the Tivoli Netcool Configuration Manager.
- Tivoli Netcool Configuration Manager stores historical versions of device configurations, which allows for restoring a device's configuration to a previous state.
- Tivoli Netcool Configuration Manager provides an audit trail of the device's configuration changes that have been made and identifies the users who made the changes.
- Tivoli Netcool Configuration Manager allows for intelligent restoration of a device configuration by determining the differences between the current and historical configuration and only applying the necessary changes to restore a device to a previous state.

### 4.1.3 Restoring a device's configuration scenario operational flow

Figure 4-1 depicts this scenario's high-level operational flow.

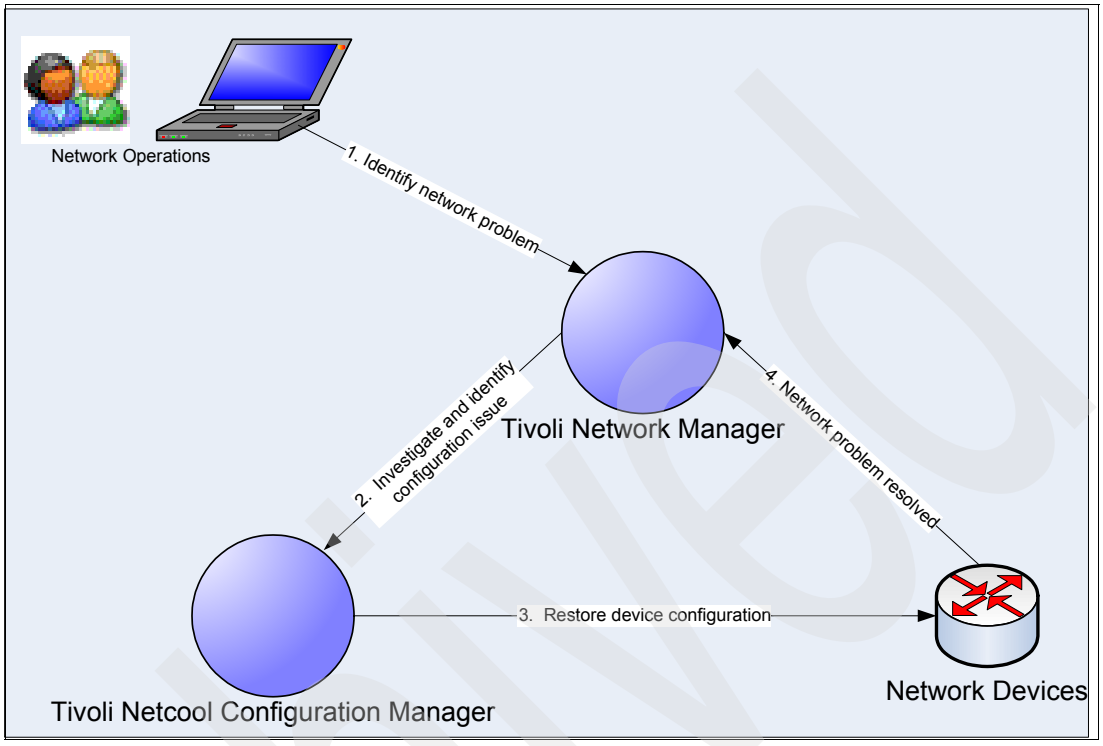



*Figure 4-1 Configuration restoration scenario operational flow diagram*

## 4.2 Device configuration troubleshooting

In this scenario, troubleshooting begins with a network operator monitoring the network with Tivoli Network Manager. The operator monitors both the map of the network and the Active Event List within the application. The network operator uses Tivoli Netcool Configuration Manager during troubleshooting for the analysis of the device's configuration.

### 4.2.1 Identifying a network problem

To begin monitoring a network, log in to Tivoli Network Manager from the Tivoli Integrated Portal. In order to launch the Tivoli Integrated Portal, access a web browser, such as Internet Explorer, and insert the correct server link.

The following link provides access to the lab system that was used for this book:

`http://9.196.131.166:16310/`

Perform the following steps to begin monitoring a network:

1. After the login window opens, enter your User ID and Password in the appropriate fields (Figure 4-2) and click **Log in**.

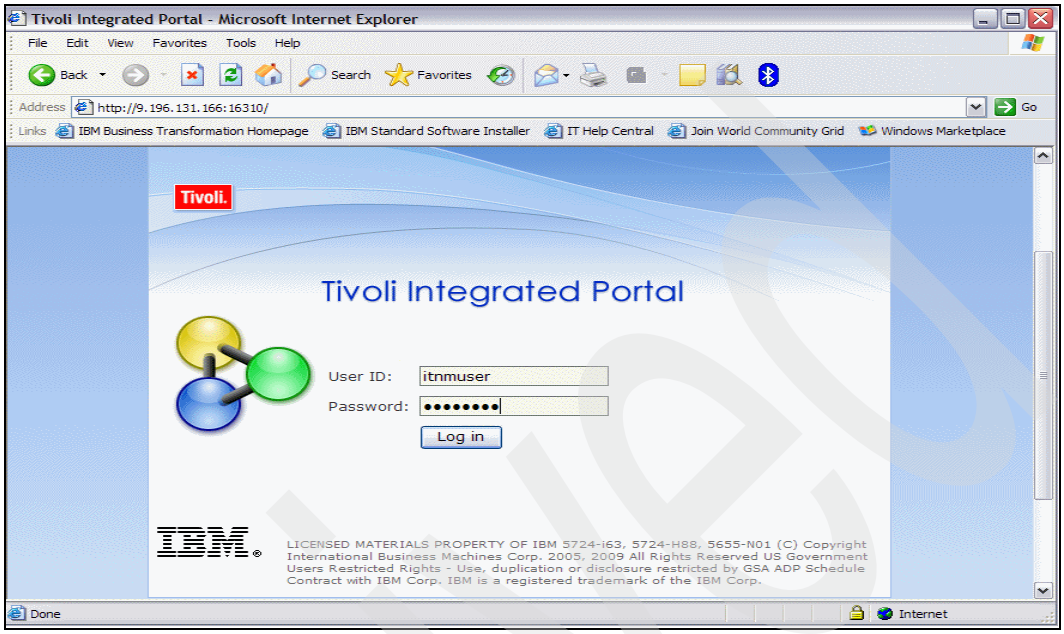



*Figure 4-2 Tivoli Integrated Portal login window*

2. When the Welcome window opens, expand the Availability and Network Availability options in the left pane of the window (Figure 4-3).

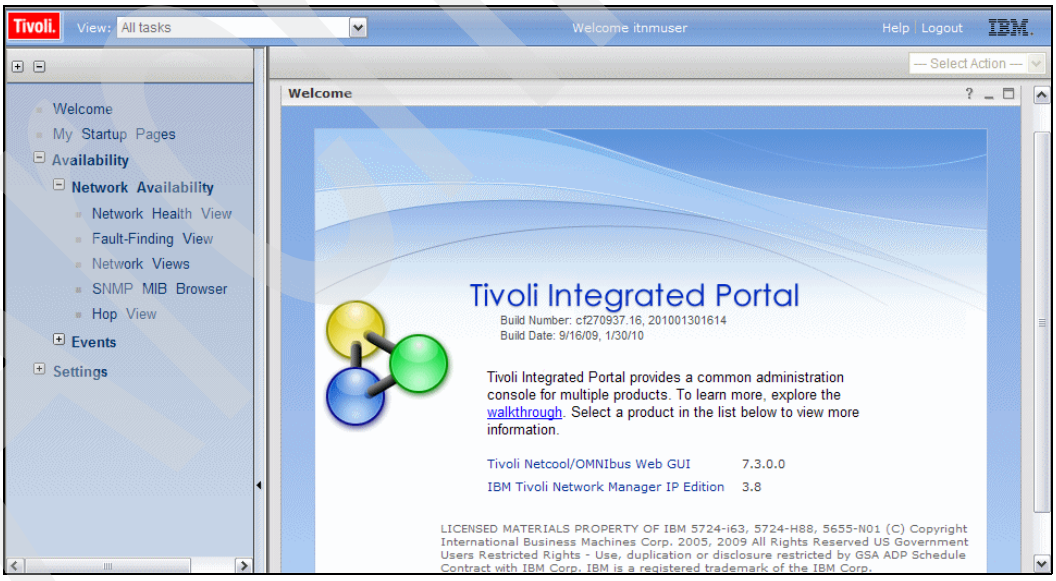



*Figure 4-3 Tivoli Integrated Portal Welcome window*

3. Select **Hop View** to view the network topology map. For this scenario, the monitoring focuses on the scotland1-cs35.sco.eu.test.lab device located in the SouthBank domain. In this view, you see the devices that are in the network and their connections. You also see the state of the devices against which active events have occurred. To narrow the view to the scotland1-cs35.sco.eu.test.lab device, select Southbank in the Domain field, enter

scotland1-cs35.sco.eu.test.lab in the Seed field, select 3 in the Hops field, and click the  icon.

In Figure 4-4, you see that the scotland1-cs35.sco.eu.test.lab device has a major event raised on it. Likewise, the scotland2-cs29.uk.eu.test.lab and scotland3-cs29.uk.eu.test.lab device events indicate an issue. Pings tests to both devices from Tivoli Network Manager have failed. Under this scenario, these events indicate that an incorrect configuration change may have been the trigger.

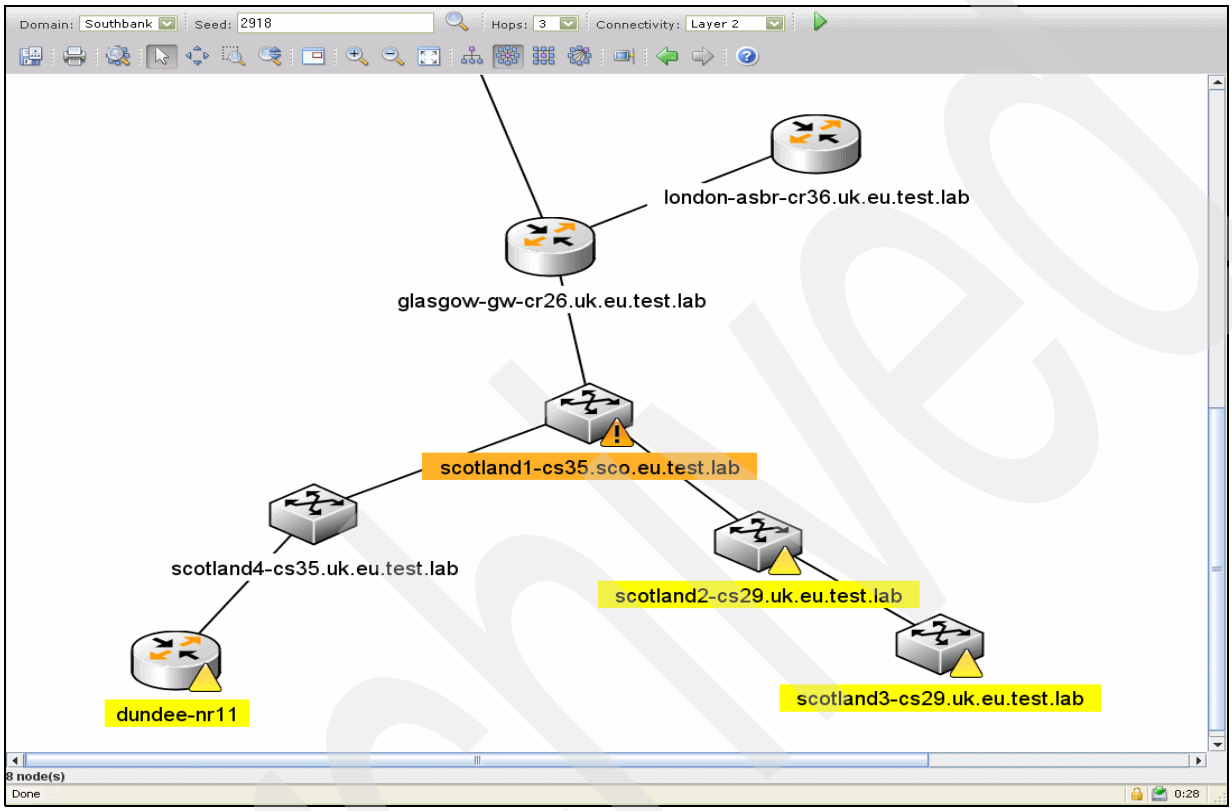



*Figure 4-4 Tivoli Network Manager Hop View window*

4. To determine if configuration changes have occurred, launch the Device Configuration Changes report. To launch the report from Tivoli Network Manager, select the device in Hop View, right-click, and select **Configuration Management → ITNCM Reports → Device Configuration Changes.**

By analyzing the report shown in Figure 4-5, you see that a device configuration change has recently occurred. There is a high probability that the configuration change caused the network problem. We investigate whether configuration changes were made to determine if the changes are the root cause of the problem.

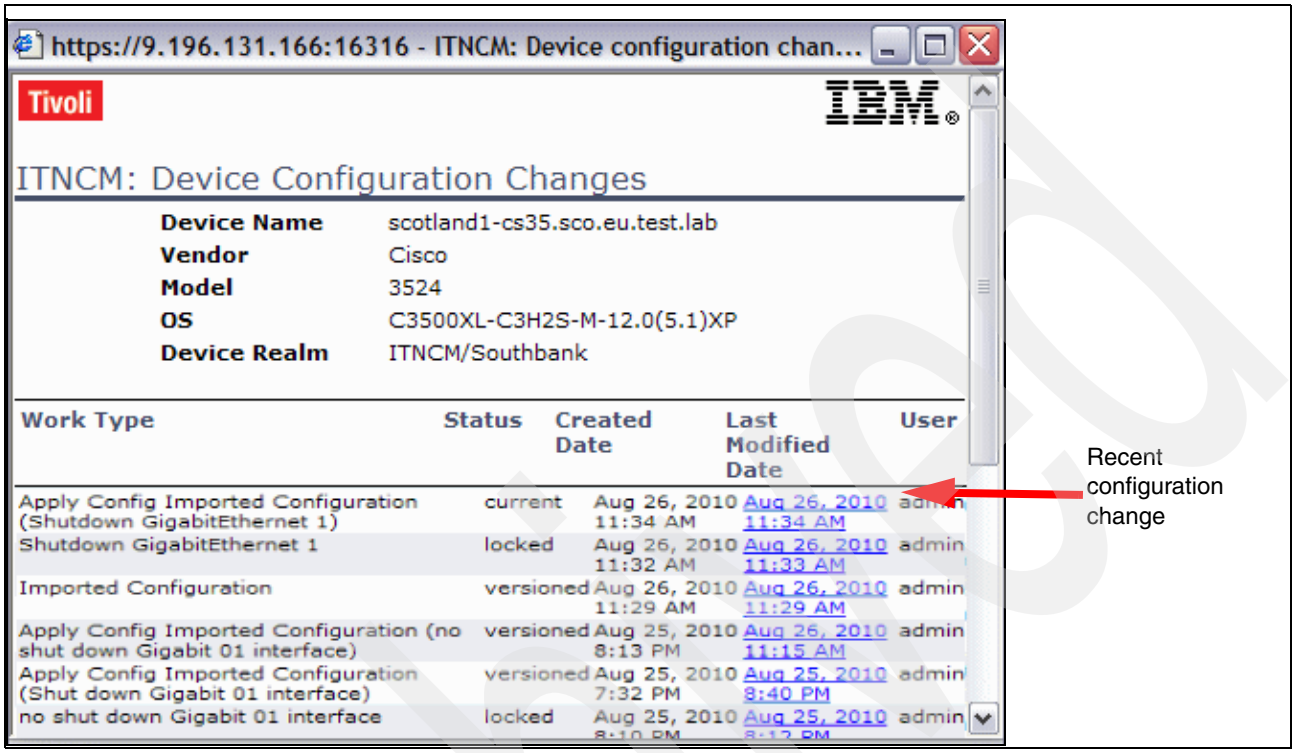



*Figure 4-5 Device Configuration Changes report launched from Tivoli Network Manager*

## 4.2.2 Investigating a device configuration

Now that we have identified a network problem and a device whose configuration must be investigated, we launch from the Tivoli Network Manager to the Tivoli Netcool Configuration Manager to begin the investigation of the device's configurations.

Perform the following steps to investigate a device's configuration:

1. To launch to Tivoli Netcool Configuration Manager from Tivoli Network Manager, select the device in the Hop View, right-click, and select **Configuration Management** → **Launch ITNCM**.

2. After the Tivoli Netcool Configuration Manager login window opens, enter the Username and Password (Figure 4-6).

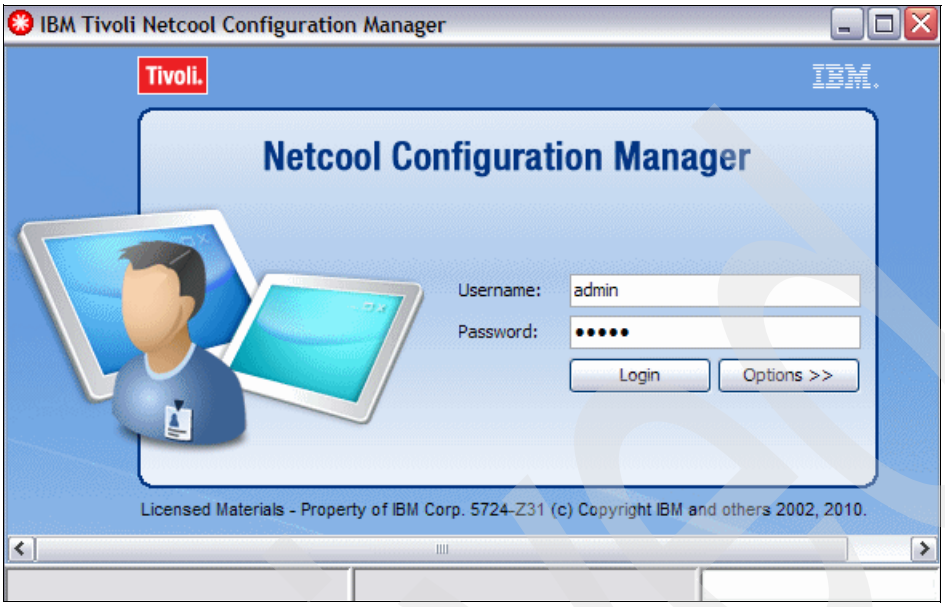



*Figure 4-6 Tivoli Netcool Configuration Manager Login window*

3. In order to determine what has changed in the device's configuration, we use the Show Differences tool in the application. To launch the Show Differences tool, navigate to the realm where the device is located in the Resource Browser section of the graphical user interface (GUI). The scotland1-cs35.sco.eu.test.lab device is in the Southbank realm. Select the **Configurations** tab in the lower pane, the current configuration, and the latest versioned configuration. Right-click and select **Show Differences**.

   Figure 4-7 shows the steps for invoking the Show Differences tool.

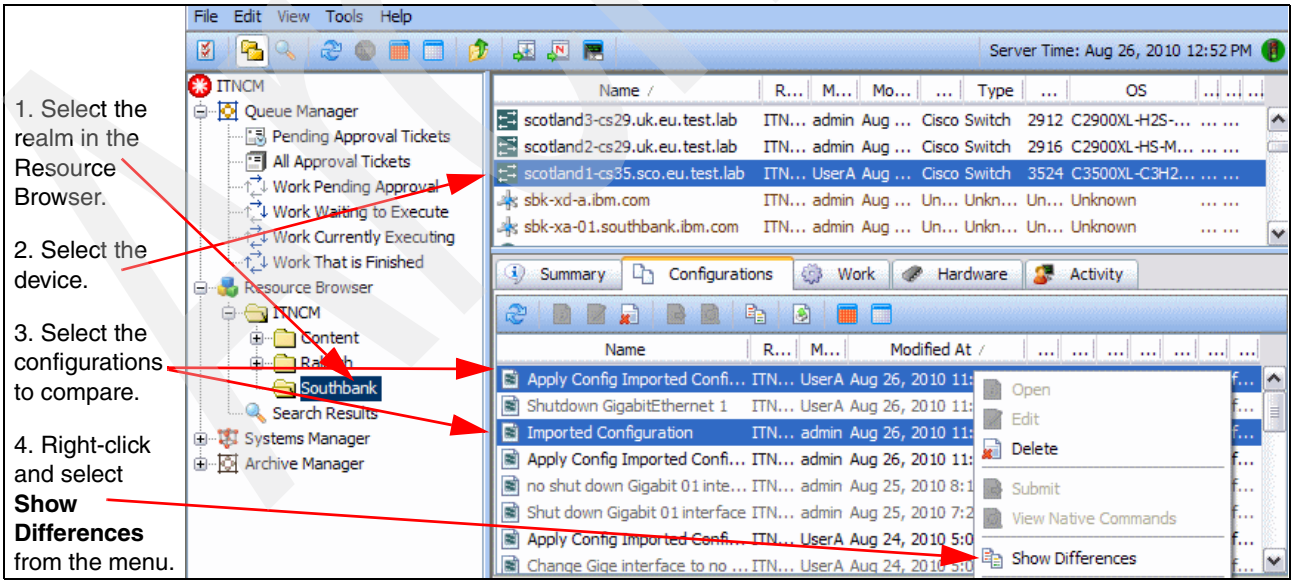



*Figure 4-7 Netcool Configuration Manager main window used to select device configurations for comparison*

4. The Show Differences tool launches. Choose either the Modeled View or the Native View. For this scenario, choose **Native View** and click the **Finish** button. The Native Differences window opens (Figure 4-8).

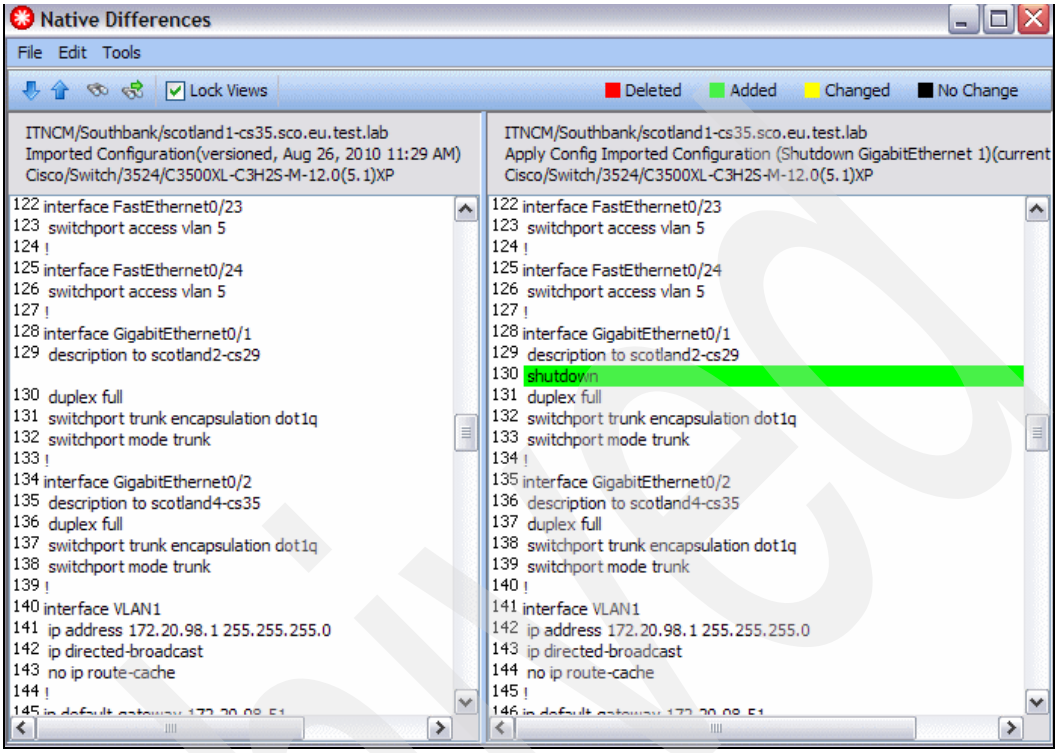



*Figure 4-8 Tivoli Netcool Configuration Manager Native Differences window*

In Figure 4-8, you can see in the current configuration that the **`shutdown`** command was added to the Gigabit Ethernet 0/1 interface in the device configuration. This is the cause of the network problem.

## 4.3 Device configuration restoration

This section of the scenario describes how to restore a device configuration, verify that the configuration is correct, and verify that the network problem is resolved.

### 4.3.1 Correcting the device configuration

Now that network problem is identified, correct it by applying the versioned configuration. Applying the versioned configuration removes the **`shutdown`** command from the device's configuration for the GigabitEthernet 0/1 interface.

Perform the following steps:

1. To apply a versioned configuration to a device, navigate to the realm where the device is located through the Resource Browser section of the GUI. The scotland1-cs35.sco.eu.test.lab device is in the Southbank realm. Select the **Configurations** tab in the lower pane and select the configuration to restore. In this scenario, the correct configuration is dated August 26, 2010 11:29 a.m..

Figure 4-9 shows how to navigate to the desired configuration.

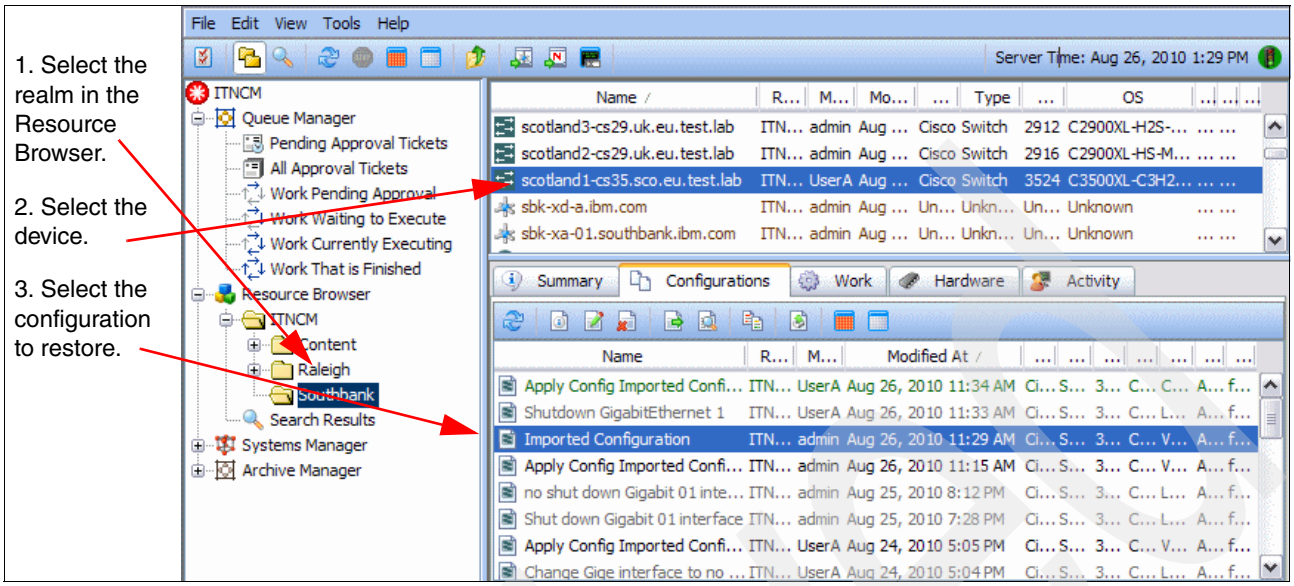



*Figure 4-9 Tivoli Netcool Configuration Manager main window used to select the device configuration for restoration*

2. Right-click and select **Submit** from the menu. You will be presented with a Unit of Work (UOW) workflow that submits a Unit of Work to apply the selected configuration to the device.

   UOWs in Tivoli Netcool Configuration Manager are discrete actions requested by a user to perform a task against a device. UOWs are managed and tracked using the Queue Manager section of the GUI. For detailed documentation about the Queue Manager, including queue descriptions and column descriptions, refer to the *IBM Tivoli Netcool Configuration Manager - Base User Guide*, found at the following address:

   `http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm_pdf_base_usr_61.pdf`

3. The UOW workflow for restoring a versioned configuration begins with the Password Override window (Figure 4-10). This window can be used to change the login credentials for a device if they are different than the cached credentials stored in Tivoli Netcool Configuration Manager. For this scenario, click **Next** to proceed to the next window.

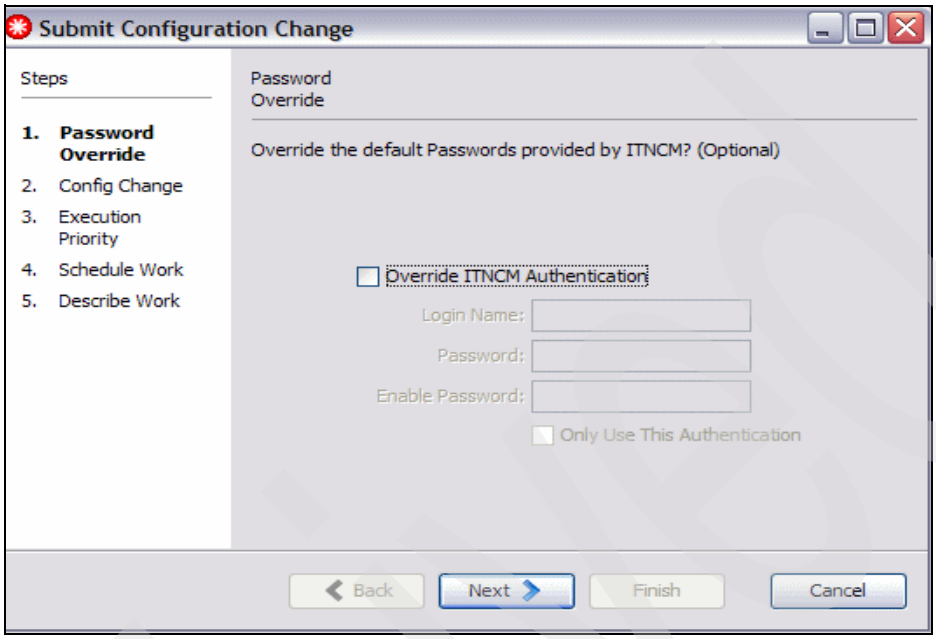



*Figure 4-10 Tivoli Netcool Configuration Manager workflow Password Override window*

4. The Config Change window opens next (Figure 4-11). This window displays the configuration information for the configuration you are restoring. You can verify in this window that you are restoring the correct versioned configuration. As you can see, the configuration is dated August 26, 2010 11:29 a.m., which is correct. The Disaster Recovery option is not used in this scenario. Click **Next** to proceed to the next window.

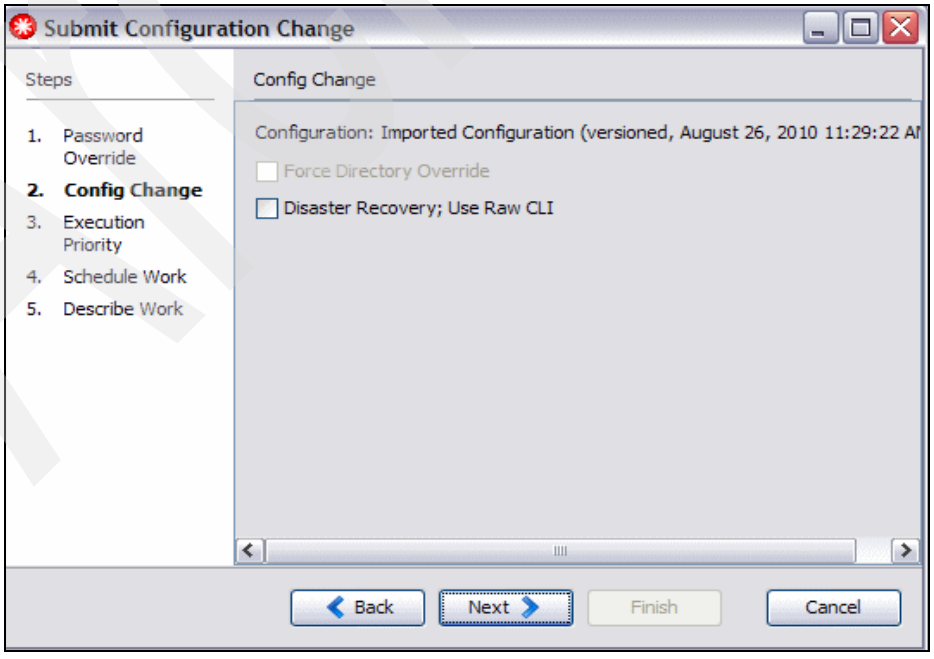



*Figure 4-11 Tivoli Netcool Configuration Manager workflow Config Change window*

5. The Execution Priority window opens next (Figure 4-12). Leave the priority at Medium and click **Next** to proceed to the next window.

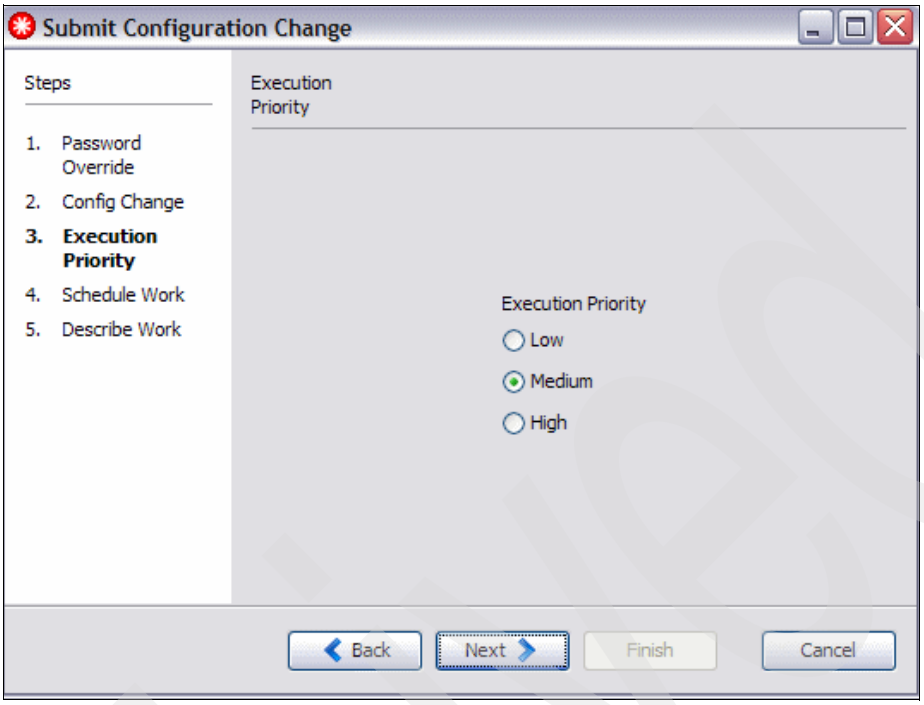



*Figure 4-12 Tivoli Netcool Configuration Manager workflow Execution Priority window*

6. The Schedule Work window opens next (Figure 4-13). This window allows you to schedule a configuration change to execute during a specified time period. Although recurring schedules are displayed as an option, in the case of a configuration restoration, you do not want to schedule the UOW to execute on a recurring basis. For this scenario, select **Immediate**, because we want the change to be applied now to correct the network problem. Click **Next** to proceed to the next window.

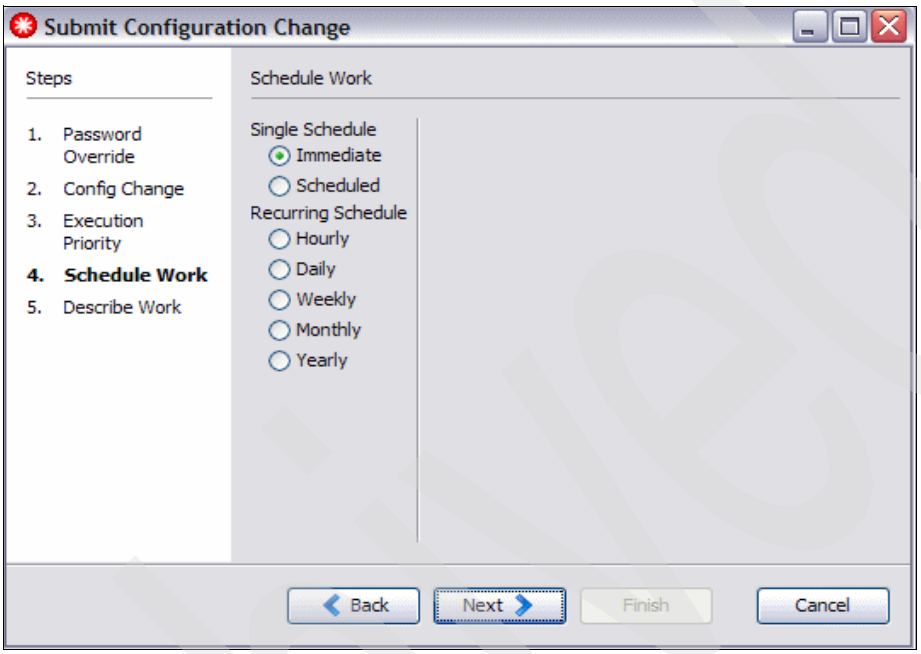



*Figure 4-13 Tivoli Netcool Configuration Manager workflow Schedule Work window*

7. The Description window opens next (Figure 4-14). You must enter a description for the UOW to complete the submission process. Enter your description and click **Finish** to submit the UOW

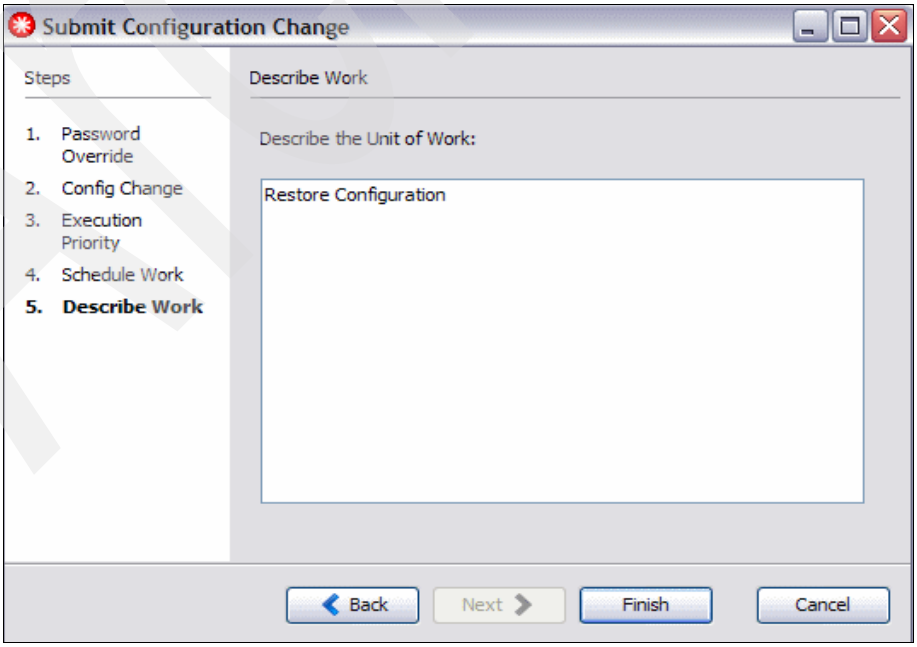



*Figure 4-14 Tivoli Netcool Configuration Manager workflow Describe Work window*

8. After the UOW is submitted, the final workflow window opens (Figure 4-15). The UOW number is identified here, which can be used to track the UOW in the Queue Manager to determine if the configuration change was successful. You can see that we need to view UOW ID #507, which was submitted for our configuration change. Click **Close** to close the window and finish the workflow.

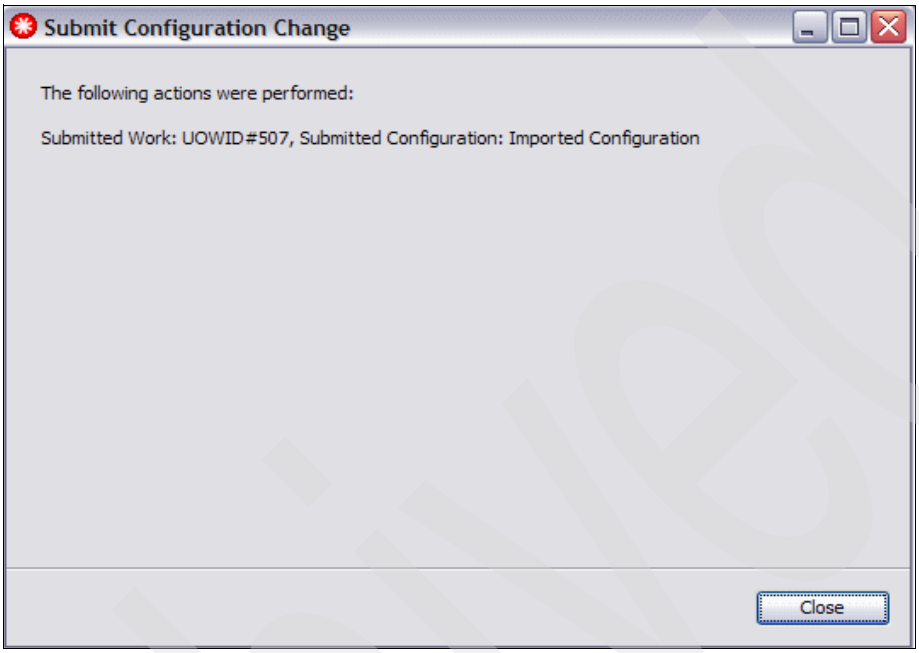



*Figure 4-15 Tivoli Netcool Configuration Manager workflow completion window*

## 4.3.2 Verifying the configuration change

Perform the following steps to verify the configuration change:

1. To verify that the configuration change was successful, navigate to the Queue Manager in the GUI and select the **Work That is Finished** queue. Search for the UOW ID #507 in the list of UOWs. You can see from the list of UOWs that the UOW ID #507 completed successfully, as noted by the Execution Status and the green color. However, we need to view the UOW log to ensure that the correct change was applied to the device configuration.

2. Select the UOW (Figure 4-16), right-click, and select **Log** to view the UOW log.

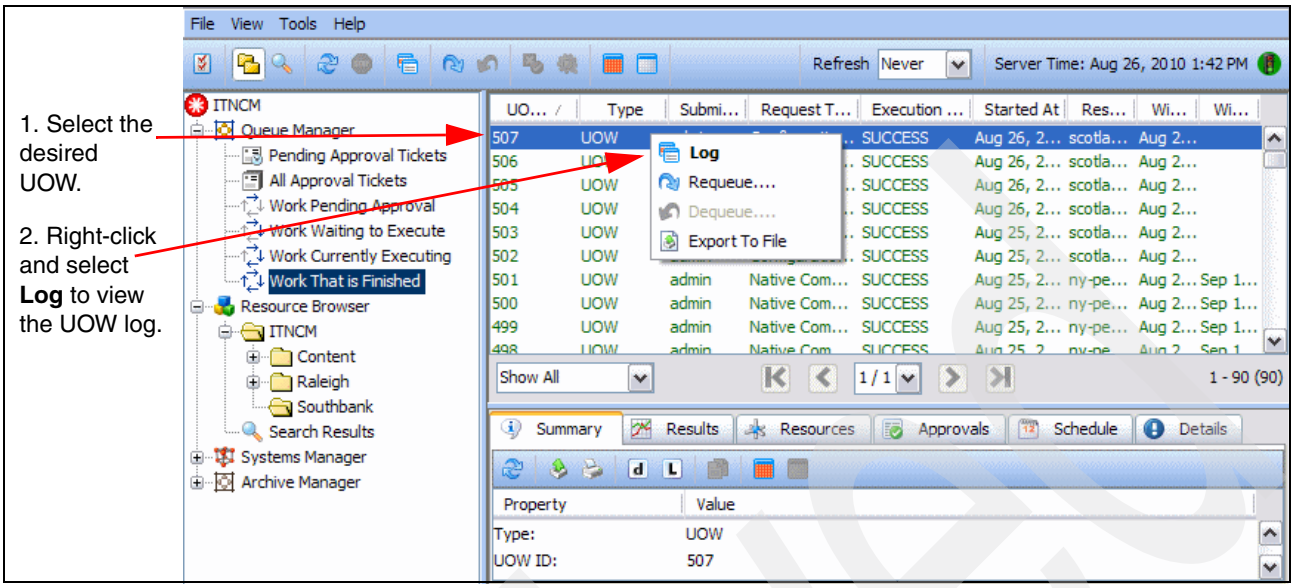



*Figure 4-16 Tivoli Netcool Configuration Manager Queue Manager list window*

3. The UOW log window for UOW ID #507 opens (Figure 4-17). The double pane shows the summary UOW data on the left and the UOW log on the right.

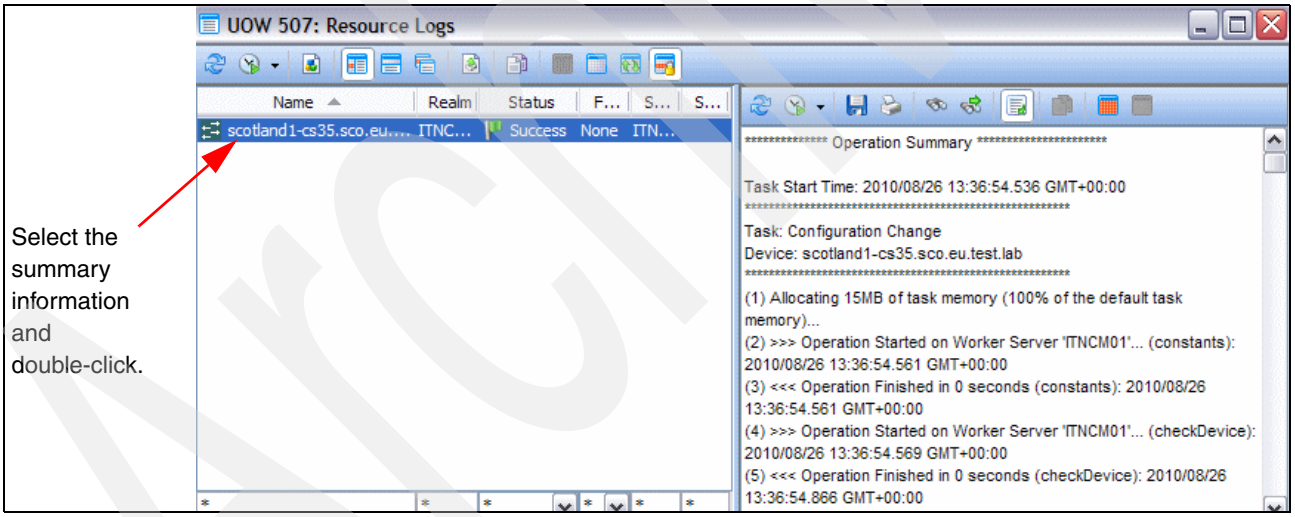



*Figure 4-17 Tivoli Netcool Configuration Manager Resource Logs window*

4. Double-click the UOW summary in the left pane of the window. This launches the log in a separate window for easier viewing (Figure 4-18).

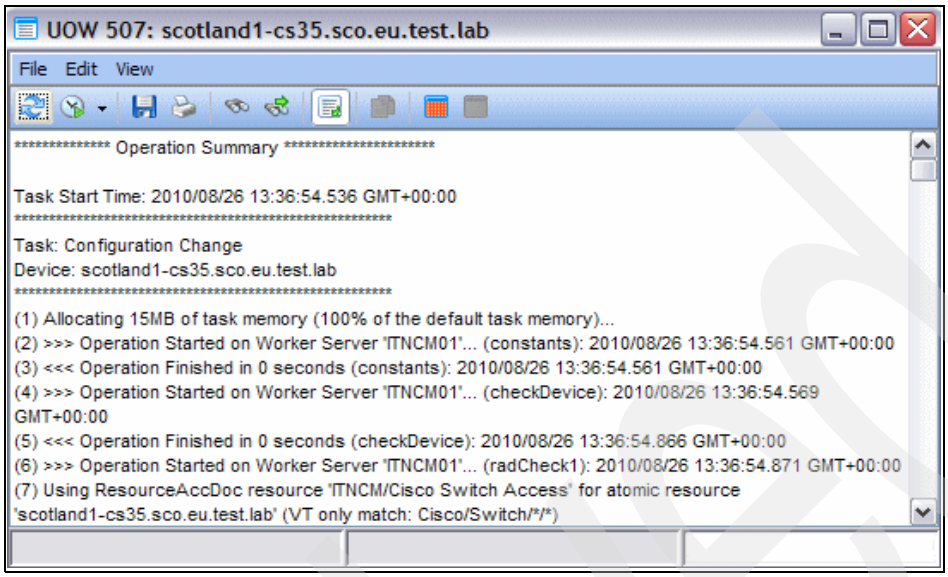



*Figure 4-18 Tivoli Netcool Configuration Manager detailed UOW log window*

The following section (Example 4-1) from the UOW log for UOW ID #507 shows that **no shutdown** was issued on the GigabitEthernet 0/1 interface and a new version of the configuration was imported and stored in Tivoli Netcool Configuration Manager. For this scenario, this is the correct command to bring the interface back up and correct our network problem, so applying the historical configuration resolved the issue.

*Example 4-1 UOW log data that identifies the configuration applied to the device*

```
Native commands sent to network resource:
interface GigabitEthernet 0/1
no shutdown
end
++++++++++++++++++++++++++++++++++++++++++++++++++
Native Command Filename=/home/icosftp/int-cisco1282829869673.cfg
(92) Config applied to
device
```

5. As an additional verification, select the realm for the device in the Resource Browser section of the GUI and select the device. Click the **Configurations** tab. Double-click the current device configuration in the list of configurations. Figure 4-19 displays the steps for viewing the current configuration.

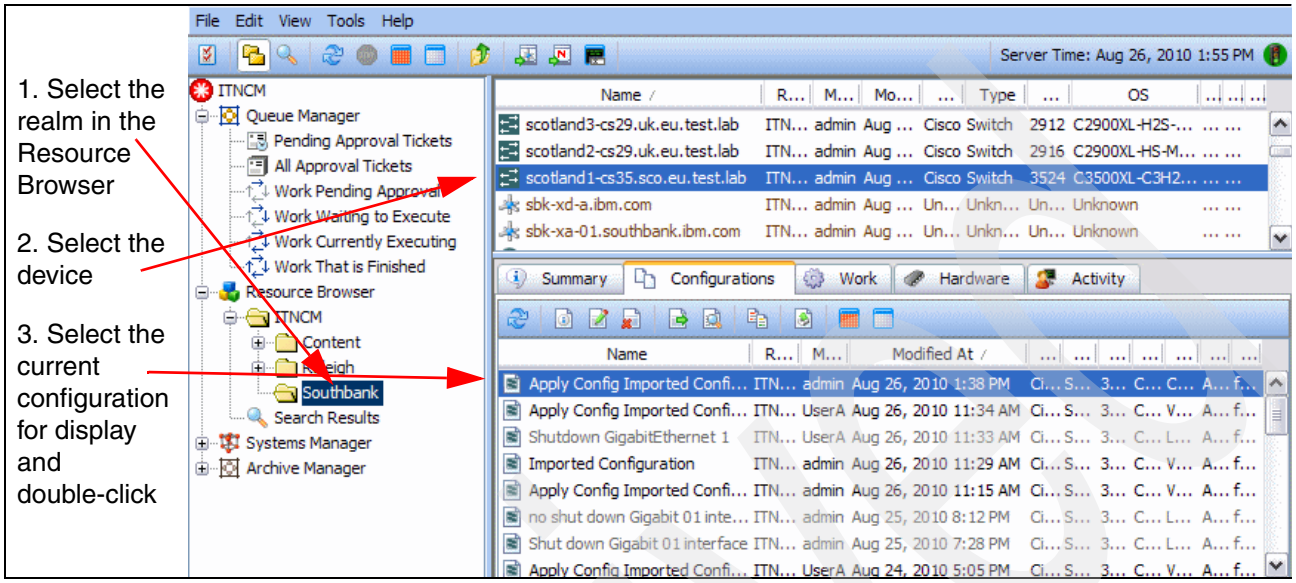



*Figure 4-19 Tivoli Netcool Configuration Manager configurations list window*

6. The Configuration Editor window opens (Figure 4-20). This is a GUI representation of the device configuration. To view sub-commands within the tree, expand **+** to the left of the command. Commands that are configured for the device are noted by .

   Figure 4-20 displays the GigabitEthernet 0/1 interface configuration. As you can see, shutdown is no longer enabled on the interface.

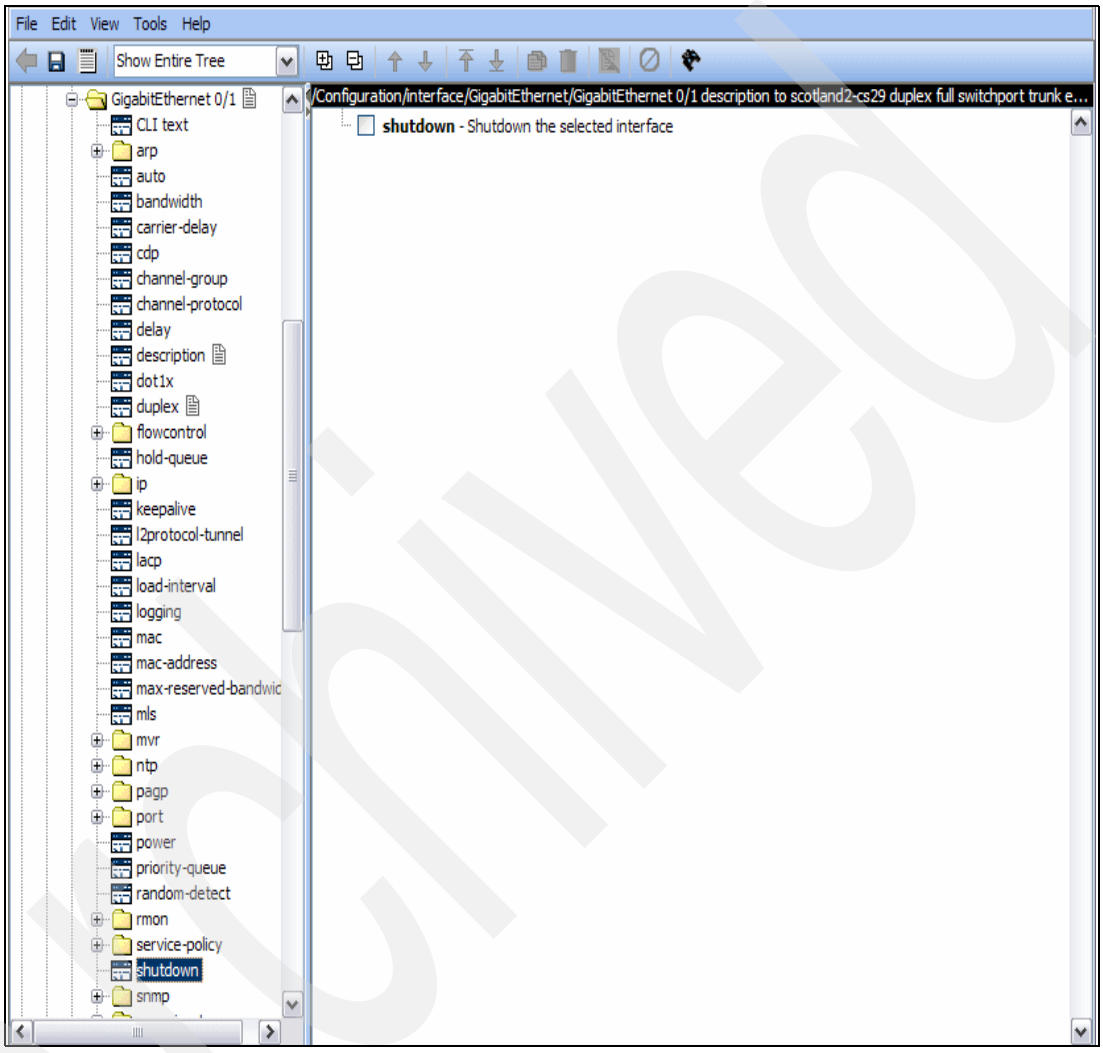



*Figure 4-20 Tivoli Netcool Configuration Manager configuration editor window*

7. As an alternative to viewing the configuration in the GUI mode, Tivoli Netcool Configuration Manager allows you to view the configuration in native command mode. This view displays the commands as they would be displayed on the actual device. For our scenario, using a Cisco switch, this view is like having run **show running-configuration** on the actual device. Launch the native command view from the Configuration Editor window by selecting **File** → **Tools** → **View Native Commands**.

   Figure 4-21 shows the device configuration in the native command mode. Notice again that shutdown is no longer enabled on the device.


*Figure 4-21 Tivoli Netcool Configuration Manager native command view window*

## 4.3.3 Network problem resolved

To determine whether or not the network problem has been resolved, we need to return to Tivoli Network Manager. Following the steps outlined in 4.2.1, “Identifying a network problem” on page 69, return to the Hop View option to view the network topology map. Navigate to the Hop View for scotland1-cs35.sco.eu.test.lab.

As shown in Figure 4-22, the scotland2-cs29.uk.eu.test.lab and scotland3-cs29.uk.eu.test.lab events are clear, which indicates the success of ping tests to both devices from Tivoli Network Manager and that the interface from scotland1-cs35.sco.eu.test.lab to scotland2-cs29.uk.eu.test.lab is restored.

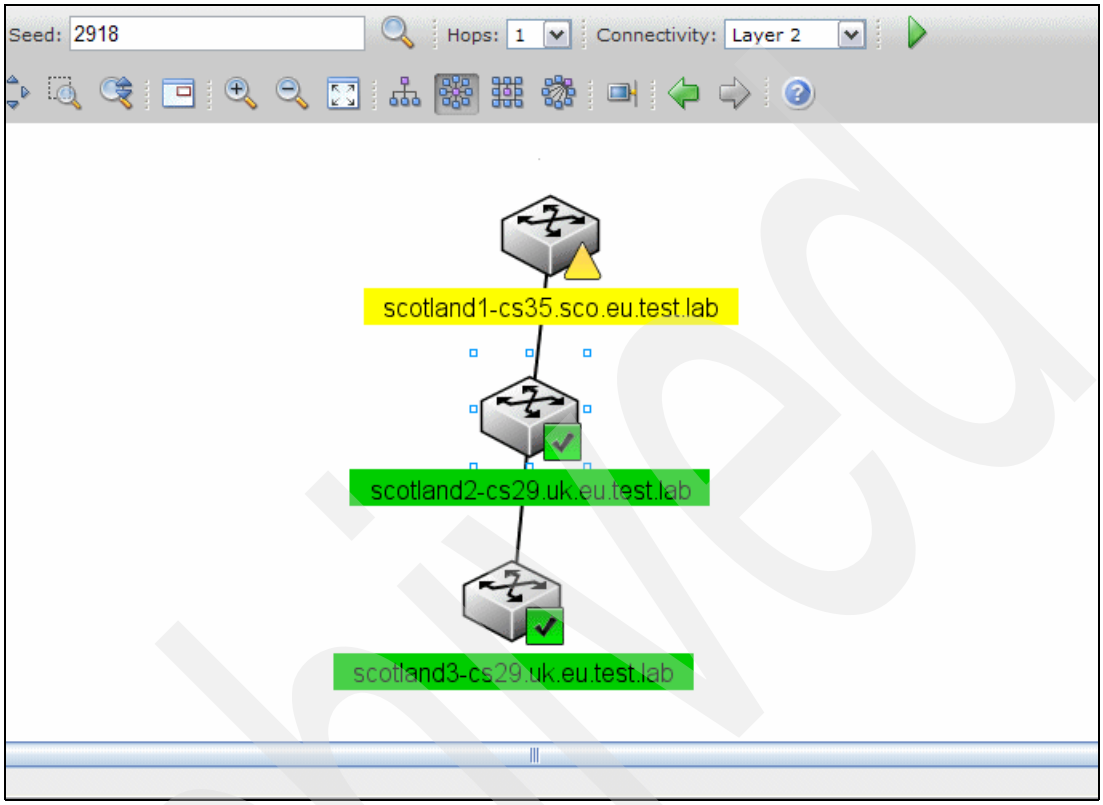



*Figure 4-22 Tivoli Network Manager Hop View window*

5

# Implementing a new network configuration standard

This chapter discusses how to implement a new network configuration standard across multiple devices using the launch-in-context features of the integration between Tivoli Network Manager and Tivoli Netcool Configuration Manager.

This chapter describes the following topics:

## 5.1 Scenario

Networks in large organizations are rarely static. Often, there is a need to change many network devices at once to ensure uniformity across the network environment. Regardless of the reason, whether to apply an operating system patch, to change access permissions, or roll out new configurations, making these changes can be a timely process and prone to errors. In this chapter, we examine the ways to update the configuration of many devices across the network at once.

### 5.1.1 Forwarding traps from network devices to mttrapd probe server

This scenario describes a situation where you have just implemented a new network management solution, including Tivoli Network Manager, Tivoli Netcool/OMNIbus, and mttrapd probe, and integrated the solution with Tivoli Netcool Configuration Manager. The mttrapd probe allows traps to be received from network devices and forwarded to Tivoli Netcool/OMNIbus and Tivoli Network Manager for root cause analysis, alerts, and topological representation of failures. In order for this process to be effective, the devices in the network must have their SNMP trap forwarding address set to the address of the mttrapd probe. This scenario demonstrates how to push this hardware configuration change out to multiple devices simultaneously by using Tivoli Netcool Configuration Manager, and verifying the success by observing that traps have been received by Tivoli Netcool/OMNIbus and are visible in the Active Event List (AEL).

The scenario shows examples of making changes through both the modelled and the native command sets in Tivoli Netcool Configuration Manager.

### 5.1.2 Benefits

The benefits demonstrated within this scenario are:

- Changes can be applied to many devices at one time.
- The changes are accurate and uniform.
- The time-to-value for the full implementation of your network management solution is reduced.

## 5.2 Using Tivoli Netcool Configuration Manager to apply a configuration through a modelled command set

In this section, we demonstrate how to use the modelled command set to create a configuration change to be applied to multiple devices. For our example, we are going to use a group of Cisco devices and apply the correct command for adding the mttrapd server's IP address into the configuration for trapd forwarding.

### 5.2.1 Creating the command set

Here are the steps required to create a command set to add the snmp-server host information, so that traps will be forwarded to our mttrapd server. Perform the following steps:

1. Launch the Tivoli Netcool Configuration Manager application. We perform this action from our Tivoli Integration Portal (TIP) console (Figure 5-1).

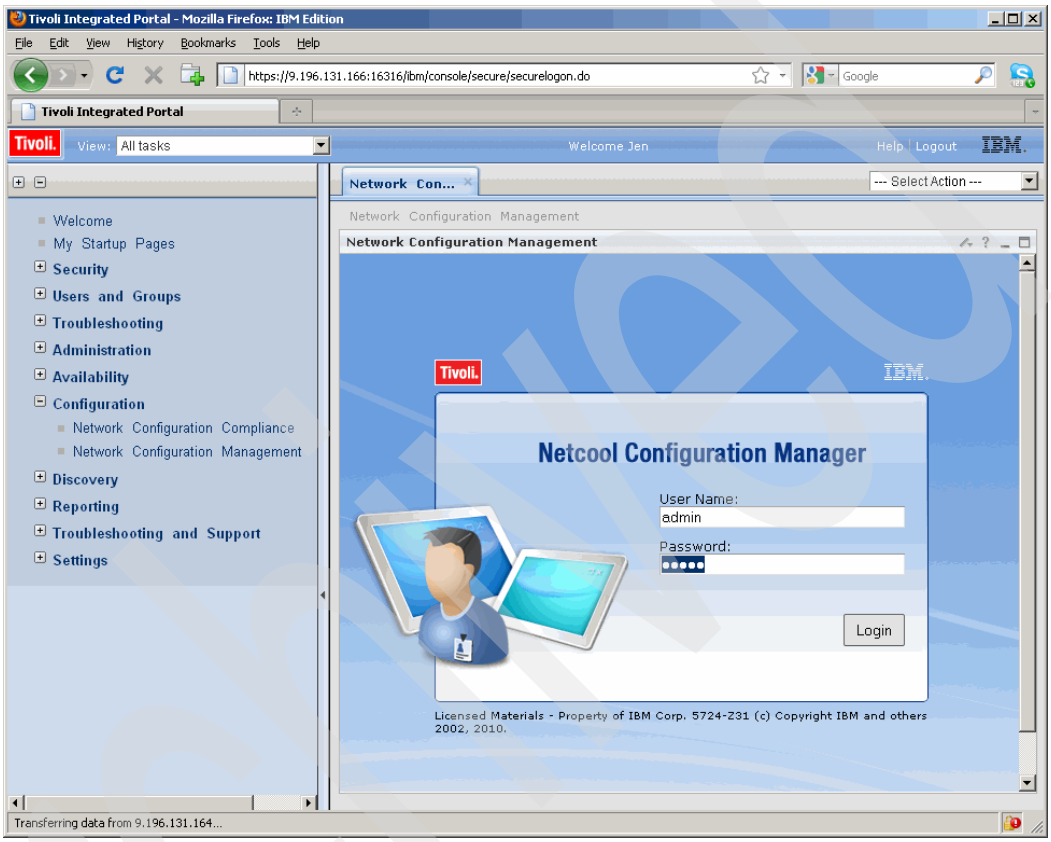



*Figure 5-1 Tivoli Netcool Configuration Manager login*

2. In Tivoli Netcool Configuration Manager, navigate to Resource Browser and the top level realm, which is Tivoli Netcool Configuration Manager in our environment (Figure 5-2).

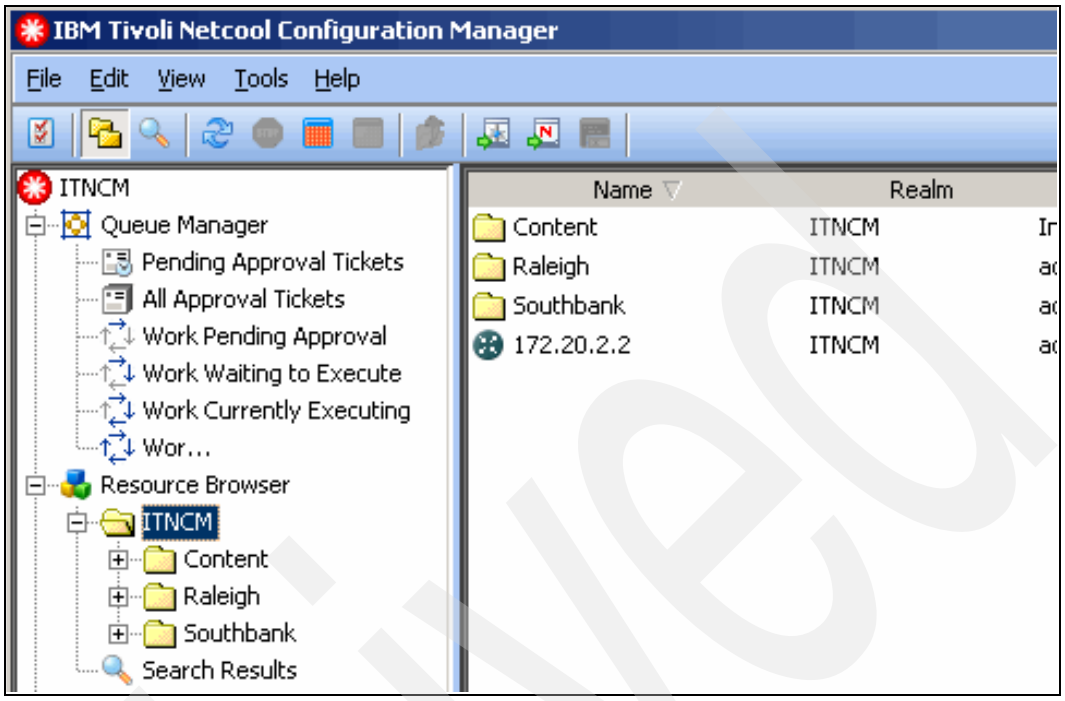



*Figure 5-2 Tivoli Netcool Configuration Manager*

3. From the File menu, select **New** → **Command Set** (Figure 5-3).

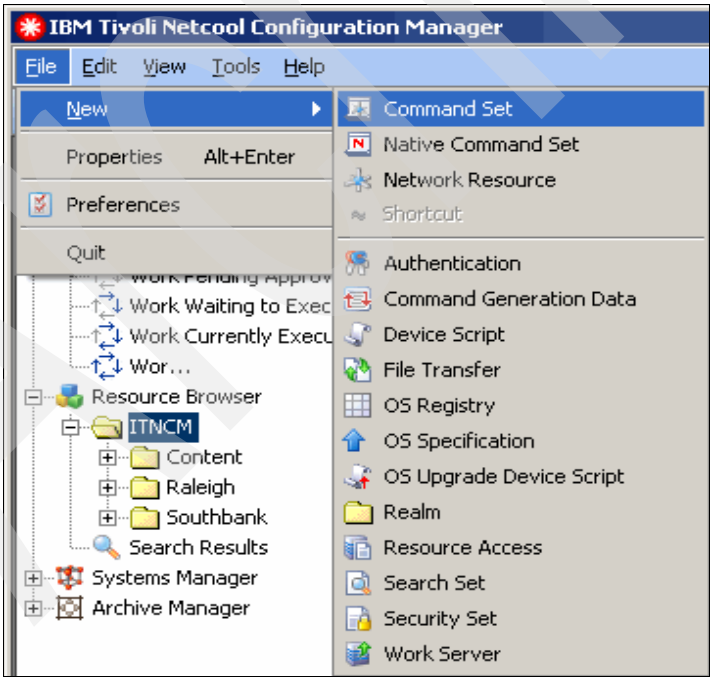



*Figure 5-3 Command set*

4. In the next window that opens (Figure 5-4), provide a unique name for your command set and information regarding Vendor, Type, Model, and Operating System (VTMOS). For our example, we used the following values:

| | |
|---|---|
| **Name** | Cisco Trap Forwarding (Modelled) |
| **Vendor** | Cisco |
| **Type** | Router |
| **Model** | 26* |
| **OS** | *12.3* |

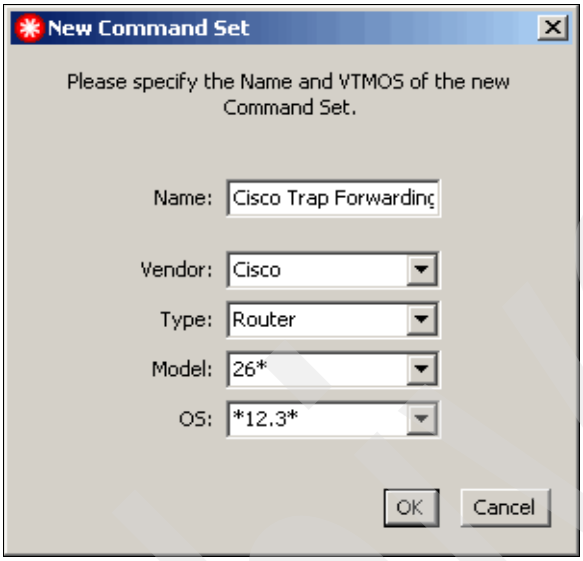



*Figure 5-4 New command set*

**Note:** Even though we are choosing a specific VTMOS during creation, when the command set is applied, because Cisco IOS based devices generally use the same command to set the value for trap forwarding, we can choose a broader range of any device of the same Vendor.

5. Back in the Tivoli Netcool Configuration Manager Resource Browser, we see we now have a new command set named “Cisco Trap Forwarding (Modelled)”. Right-click this command set and choose **Edit** to provide the configuration information (Figure 5-5).

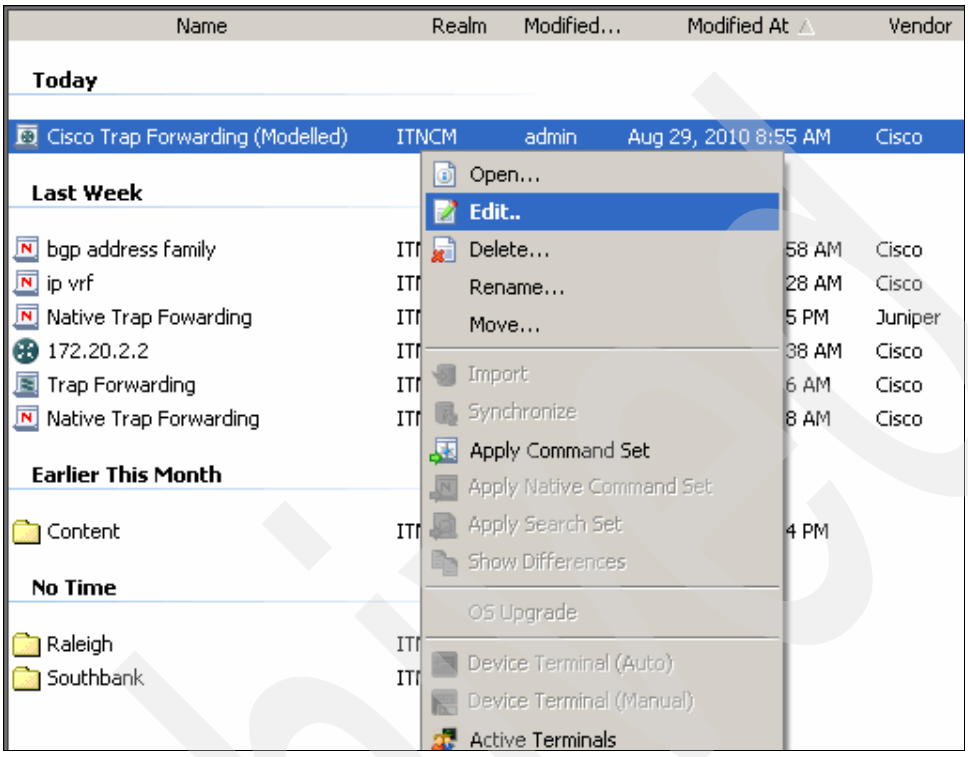



*Figure 5-5 Cisco Trap Forwarding (Modelled) command set*

6. We now see the modelled view of the configuration. From here, we want to navigate the tree to locate **snmp-server** → **host**, as shown by numbers 1 and 2 in Figure 5-6. Ensure that you have changed from Match mode to Replace mode by toggling the button that looks like two triangles stacked on top of one another, and verify the mode, as shown by numbers 3 and 4 of Figure 5-6. Click the **+** symbol for **Add host**, as shown by number 5 of Figure 5-6.

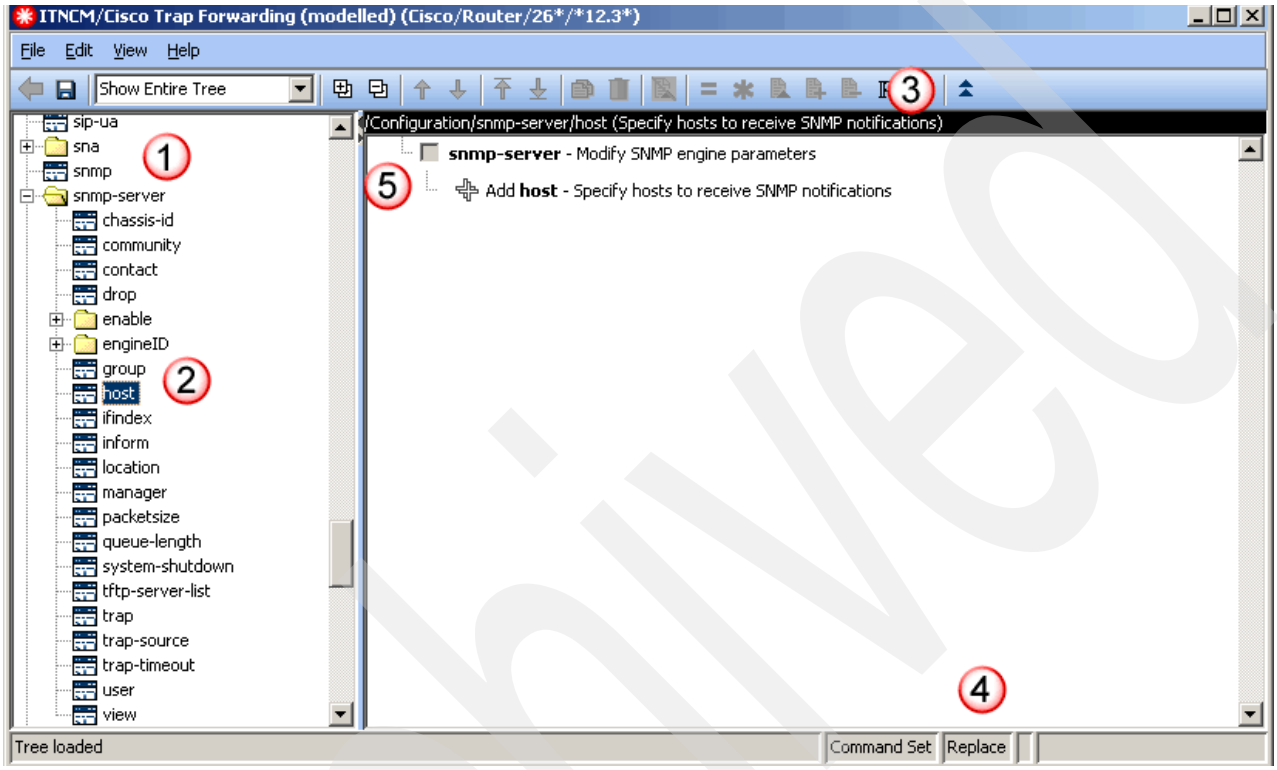



*Figure 5-6 Modelled view of the configuration*

**Note:** For more information about the use of Match Mode versus Replace Mode, see Chapter 10, “Configuration Editor”, of the *IBM Tivoli Netcool Configuration Manager 6.1 - Base User Guide*.

7. Expand the resulting blank host line (Figure 5-7).

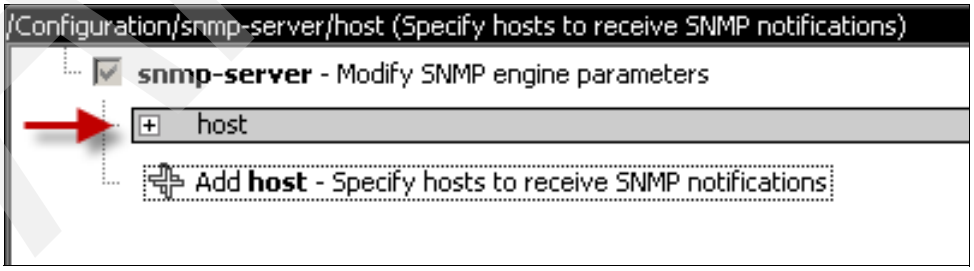



*Figure 5-7 Host line*

The required fields will be highlighted in red and with an asterisk next to them (Figure 5-8).

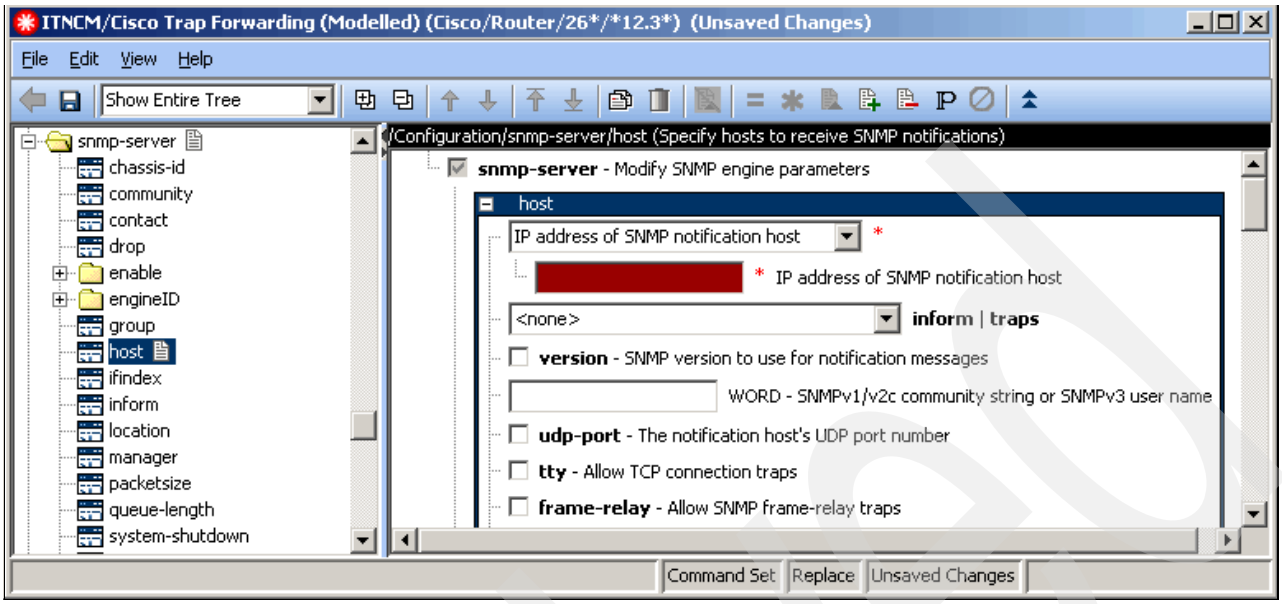



*Figure 5-8 Required fields*

8. Complete the fields with the values required, noted by the number 1. You might prefer for some values to be configurable at the time of the application of the command set. For example, we want to add in the SNMP Community String when we apply the command set, because we might be using different Community Strings for different devices. To configure these values, select the field for the Community String, as indicated by the number 2. Then click the **Parameter** button, the stylize “P”, as indicated by number 3 (Figure 5-9).

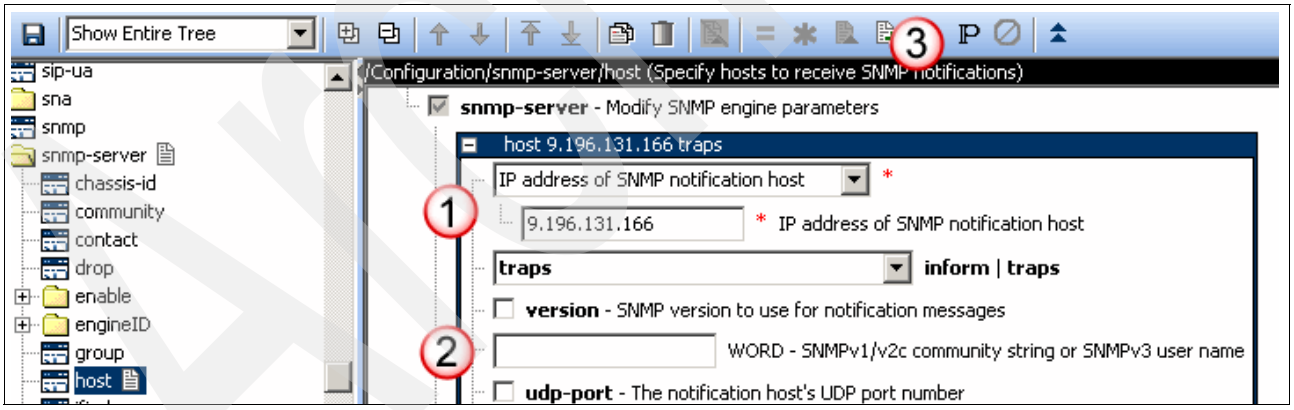



*Figure 5-9 Configuration changes*

9. A window opens and prompts you for the name of the parameter (Figure 5-10). We use SNMP Community String for the name of this parameter. Click **OK**.

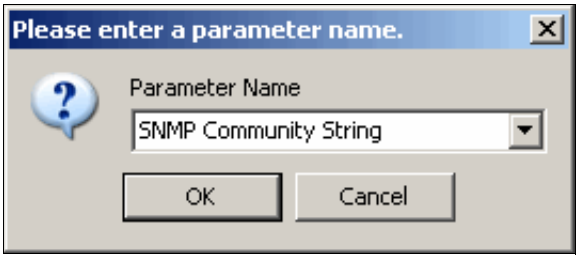



*Figure 5-10 Enter a parameter*

10. After you enter the completed parameters of all the values you want populated, click the **Save** button to save changes, as indicated by the number 1, then close the window by clicking the X in the upper right corner, indicated by the number 2 (Figure 5-11).

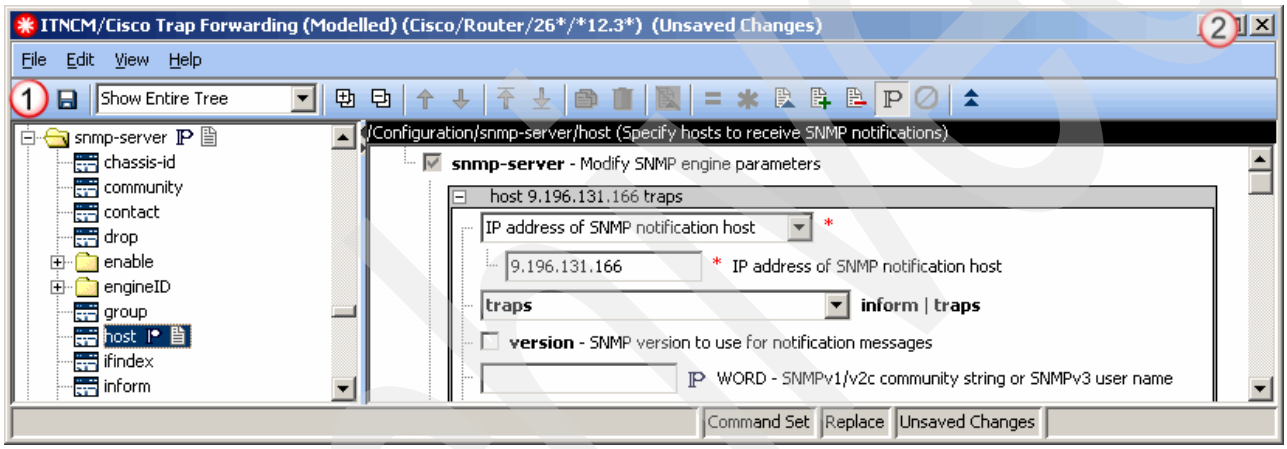



*Figure 5-11 Unsaved changes*

You have now created and populated a modelled command set intended to add the IP address of the new mttrapd probe system to your Cisco devices.

## 5.2.2 Applying the command set

This section describes the process for applying the new command set to add the snmp-server host information, so that traps are forwarded to our mttrapd server. We apply this command set to all Cisco devices within our environment.

Perform the following steps:

1. From the Tivoli Netcool Configuration Manager Resource Browser, right-click and click **Apply Command Set** (Figure 5-12).

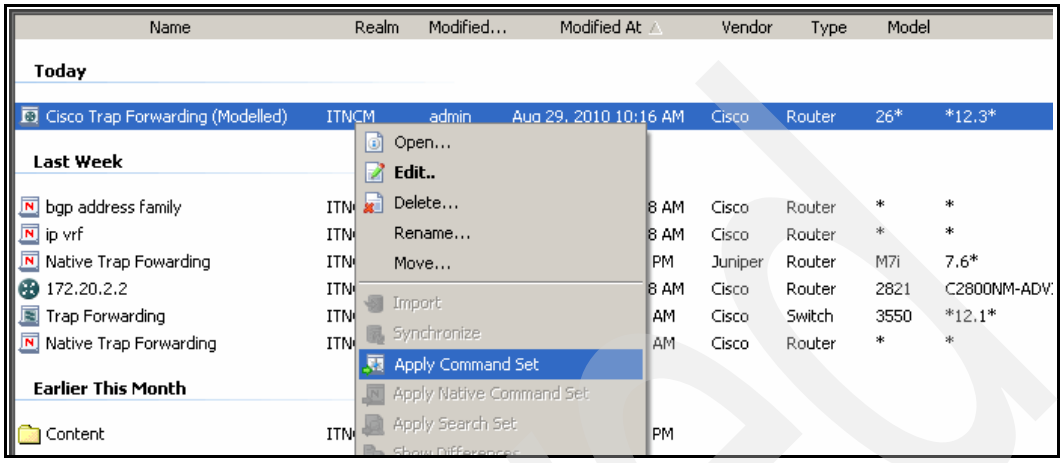



*Figure 5-12 Apply Command Set*

2. Because we chose a specific command set to apply, the Cisco Trap Forwarding (Modelled) command set is already selected. Click **Next** (Figure 5-13).

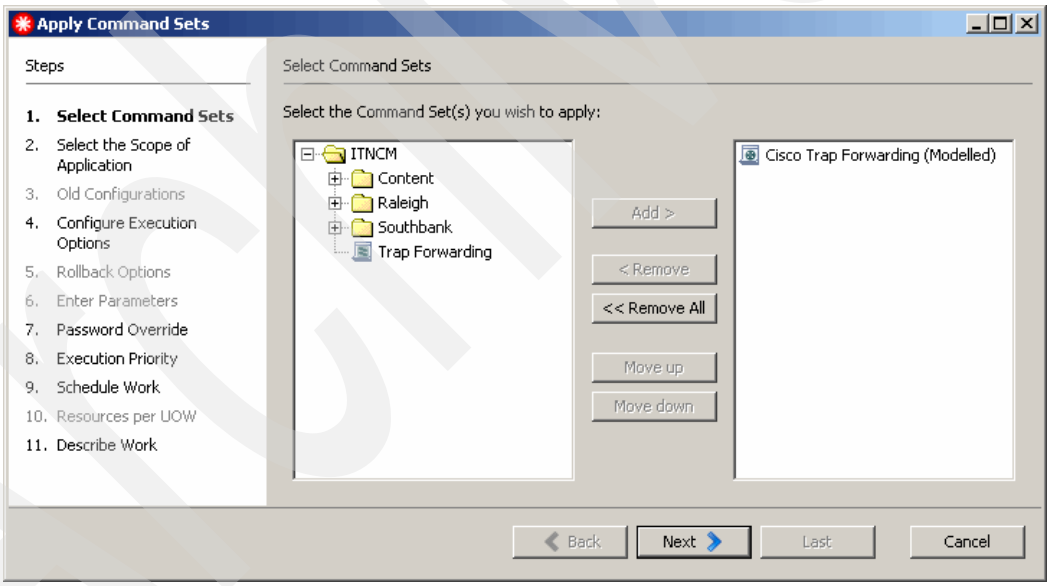



*Figure 5-13 Cisco Trap Forwarding (Modelled) command set*

3. Next, we configure the scope for the application of the command set. The first option allows us to attempt to apply this command set to all devices of a specific VTMOS for an entire realm. The second option allows you to select individual devices, one at a time. For this example, we are using the first option. Click **Next (**Figure 5-14).

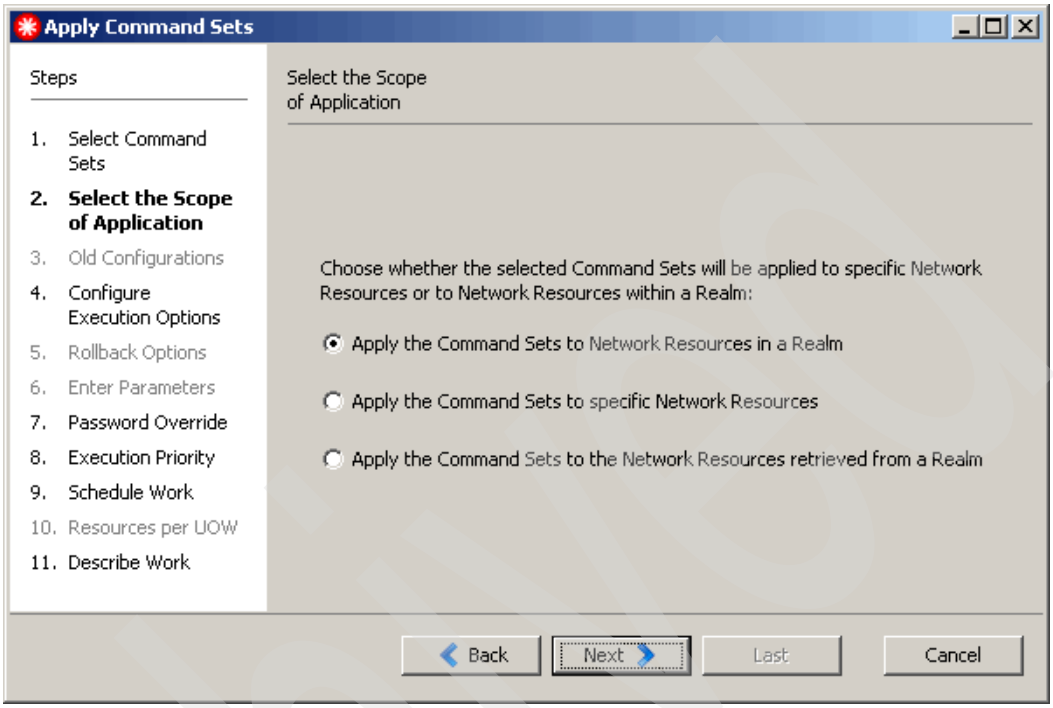



*Figure 5-14 Scope for the application of the command set*

4. In the next window, we have the options to select a realm and a VTMOS. In our example, we want to apply to both the Raleigh and the Southbank realms. To do this task, we select the **ITNCM realm**, and check the **Include Sub-realms** check box. For the VTMOS option, we want to apply to all Cisco devices, which is our default selection. Click **Next** (Figure 5-15).

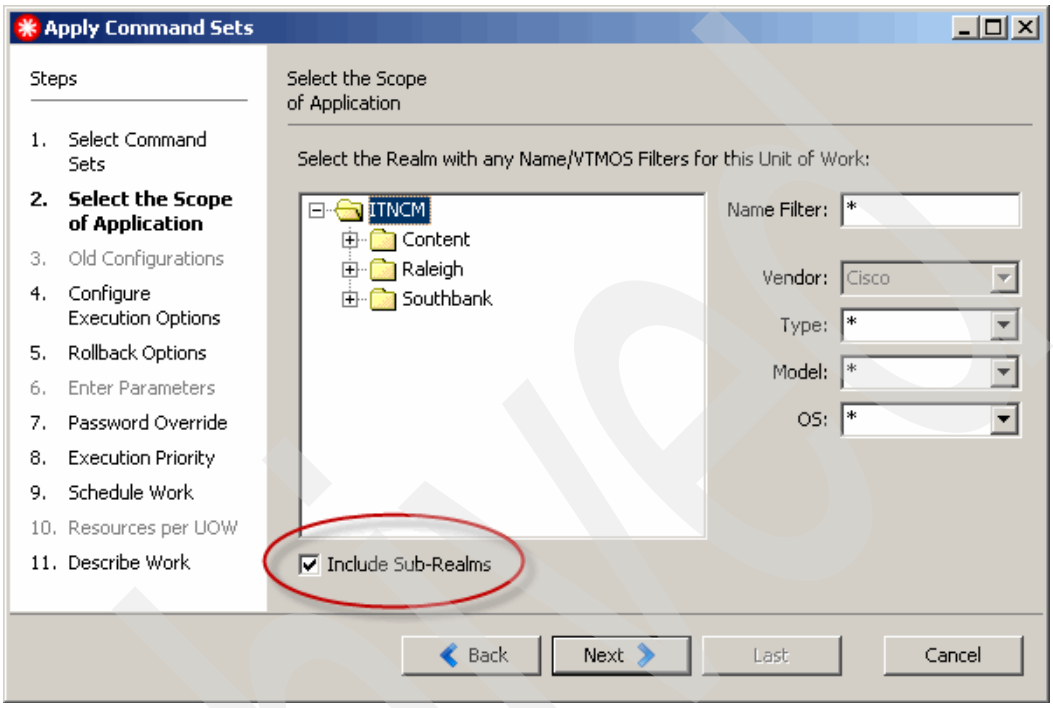



*Figure 5-15 Select the Scope of Application*

**Note:** As noted previously, the flexibility of Tivoli Netcool Configuration Manager allows us to apply this configuration change to all Cisco devices, despite the fact that it was created specifically for the Cisco 26* Routers with IOS *12.3*.

5. In the next window, you configure the execution options. Because we are applying a modelled command set, you may select either **Execute Mode** or **Report Only Mode**. For our example, to avoid duplication of steps, we run in Execute Mode. For all of the other options, choose the default values. Click **Next** (Figure 5-16).

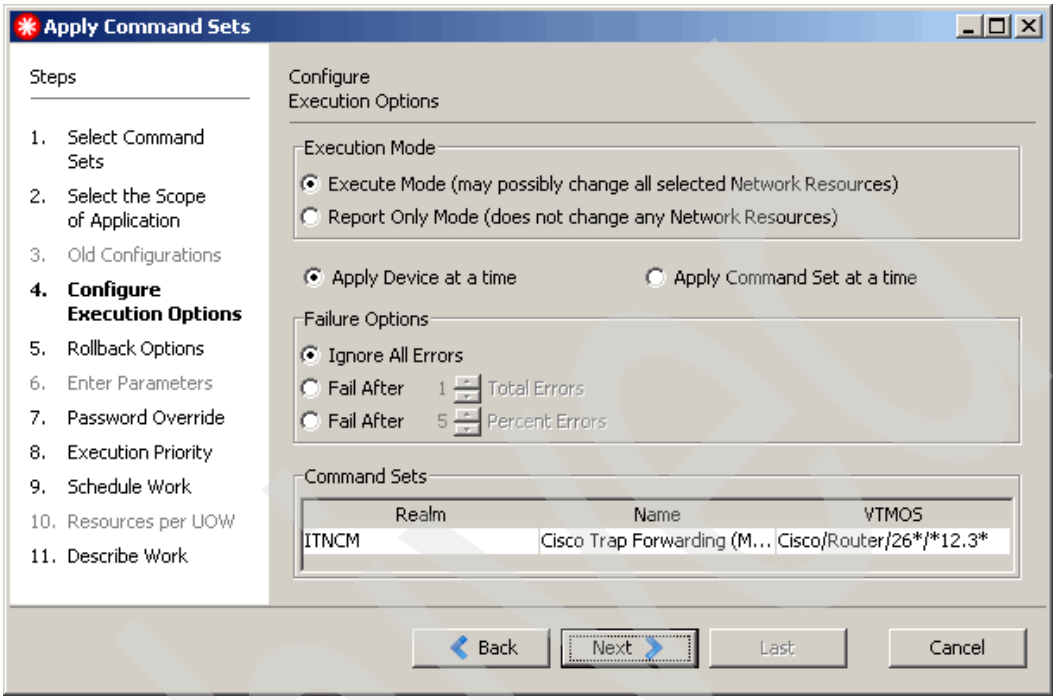



*Figure 5-16 Configure Execution Options*

**Note:** The best practice for modelled configuration changes is to select the **Report Only Mode** first. This mode shows what changes would occur if run against the devices you have selected, based on the configuration information stored in Tivoli Netcool Configuration Manager. This is not an option when doing a Native Command Set.

6. Because we are adding a command, instead of changing or deleting one, we do not need to worry about a rollback if the configuration change fails. Thus, the Rollback Options can be safely skipped for our example. Note that if you have chosen **Report Only Mode** in the previous window, this window will not open. Click **Next** (Figure 5-17).

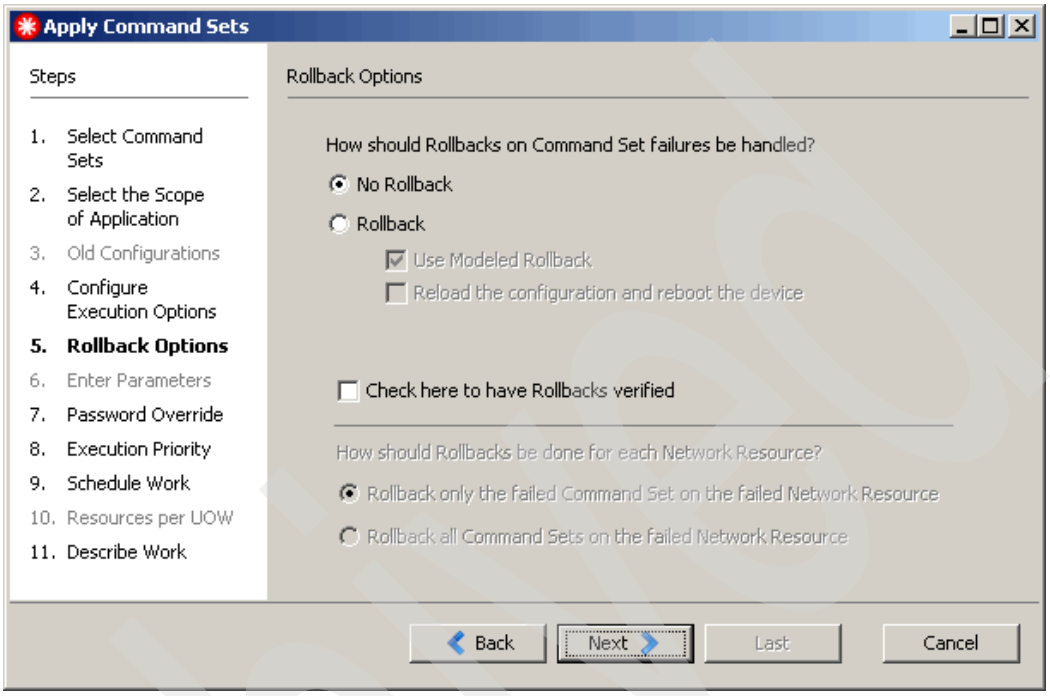



*Figure 5-17 Rollback Options*

7. Because we added some parameters, the next windows prompt us with questions about those parameters. First, we are prompted about how we want to modify the parameters. For more detailed information about the parameters and how they can be used, see Chapter 7, “Command Sets”, of the *IBM Tivoli Netcool Configuration Manager 6.1 - Base User Guide*, which can be found at the following address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm_pdf_base_usr_61.pdf

For our example, we select **Local**. Click **Next** (Figure 5-18).

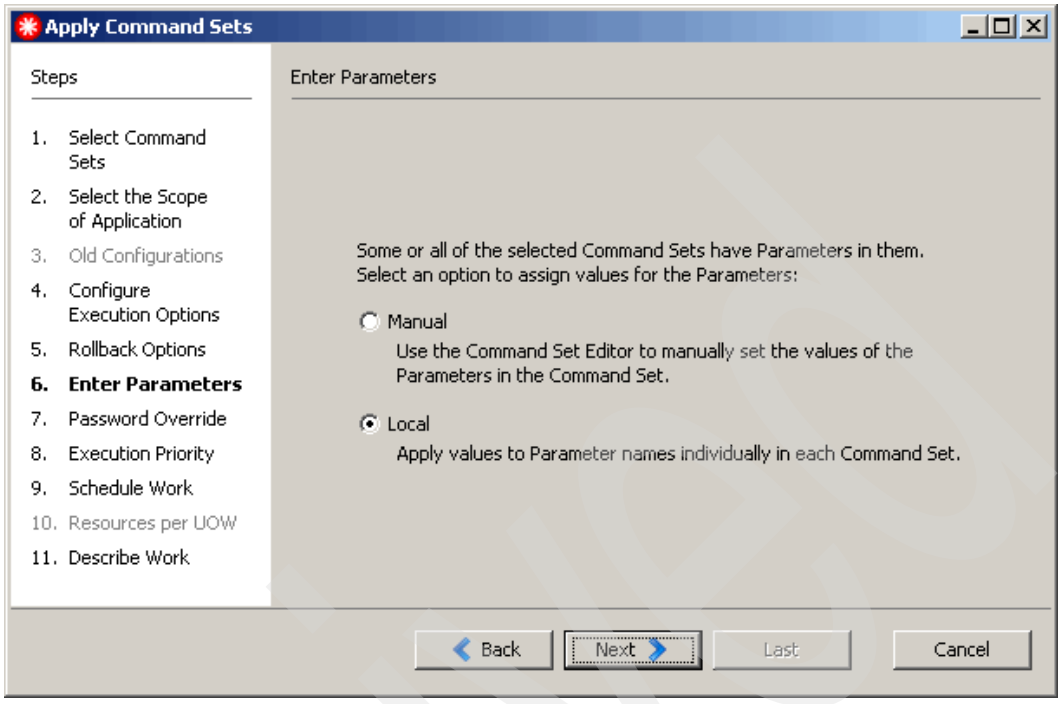



*Figure 5-18 Select Local*

8. The next window allows you to add in your parameter value. First, click the line with the parameter you want to modify, as indicated by the number 1. Then, where indicated by the number 2, enter the value you want to apply. Click **Next** (Figure 5-19).

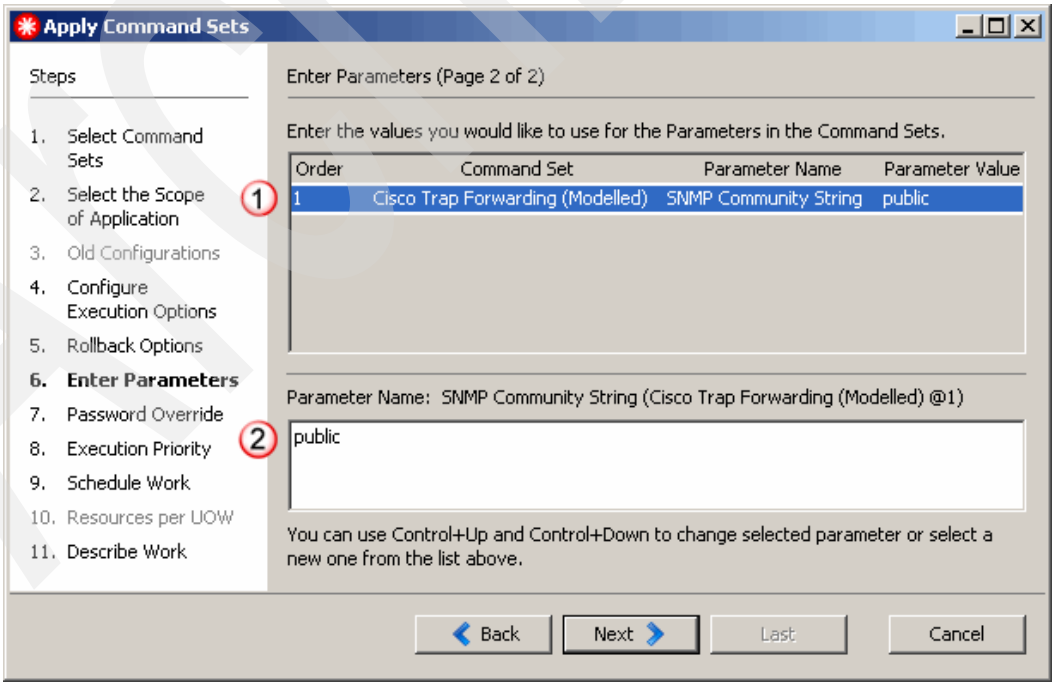



*Figure 5-19 Add in your parameter value*

9. The next window allows you to change the login details for the devices. You may want to use this menu if you have used a different set of credentials to discover the devices than to the set of credentials that might be used to modify the device's configuration. Click **Next** (Figure 5-20).

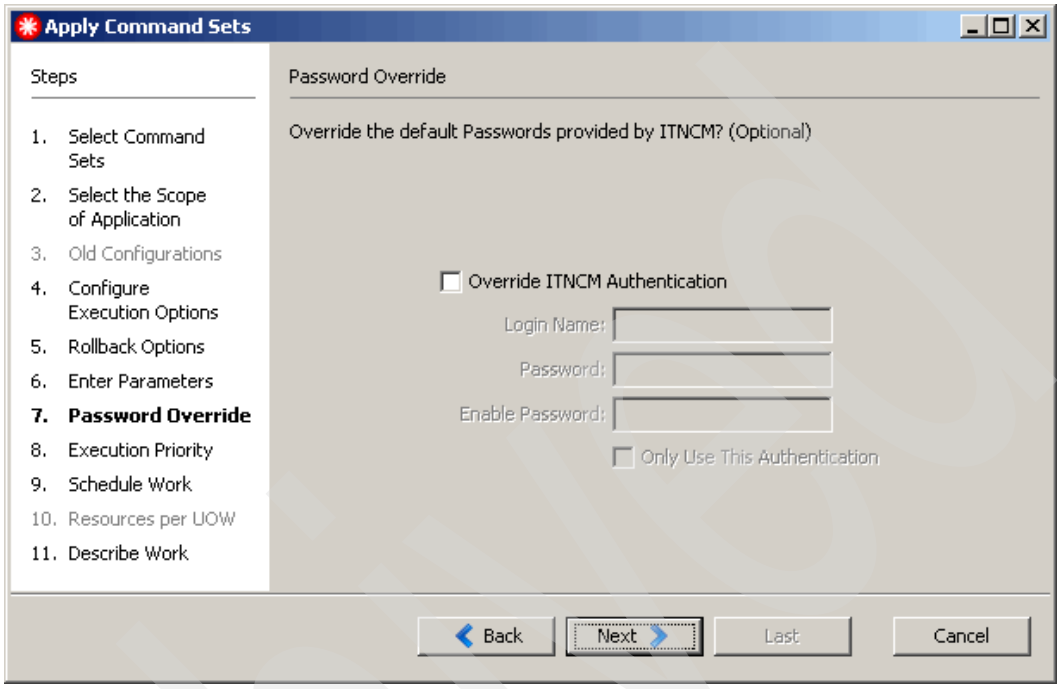



*Figure 5-20 Password Override*

10. The next window is about the priority of this change in comparison to any other Unit Of Work (UOW) that may be queued. In our case, the default priority of Medium is acceptable. Click **Next** (Figure 5-21).

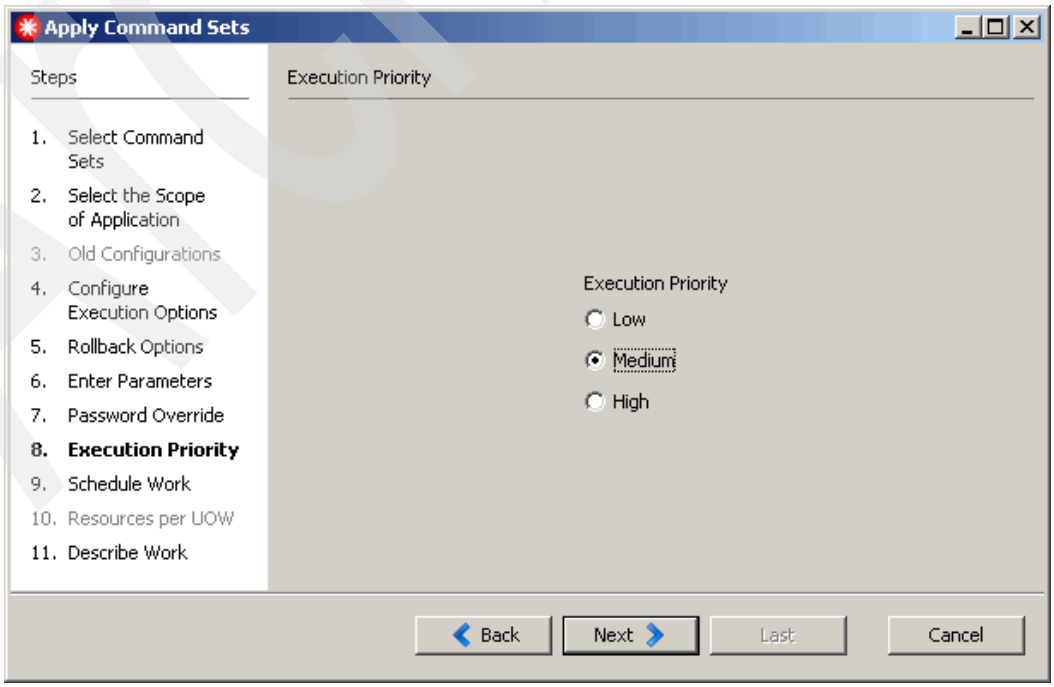



*Figure 5-21 Execution Priority*

11. The next window prompts you to schedule the UOW. We want to execute it immediately, so we accept the default setting. Click **Next** (Figure 5-22).

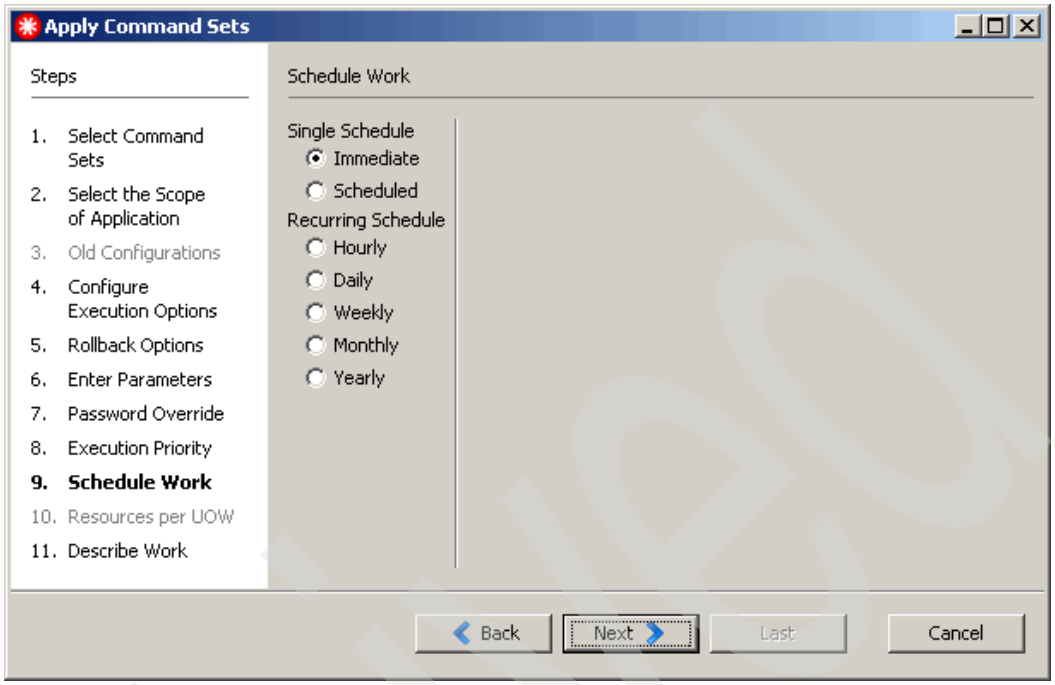



*Figure 5-22 Schedule Work*

12. The next window prompts you for a short description of the UOW. This is a mandatory field, but can be any type of description you want. Click **Next** (Figure 5-23).

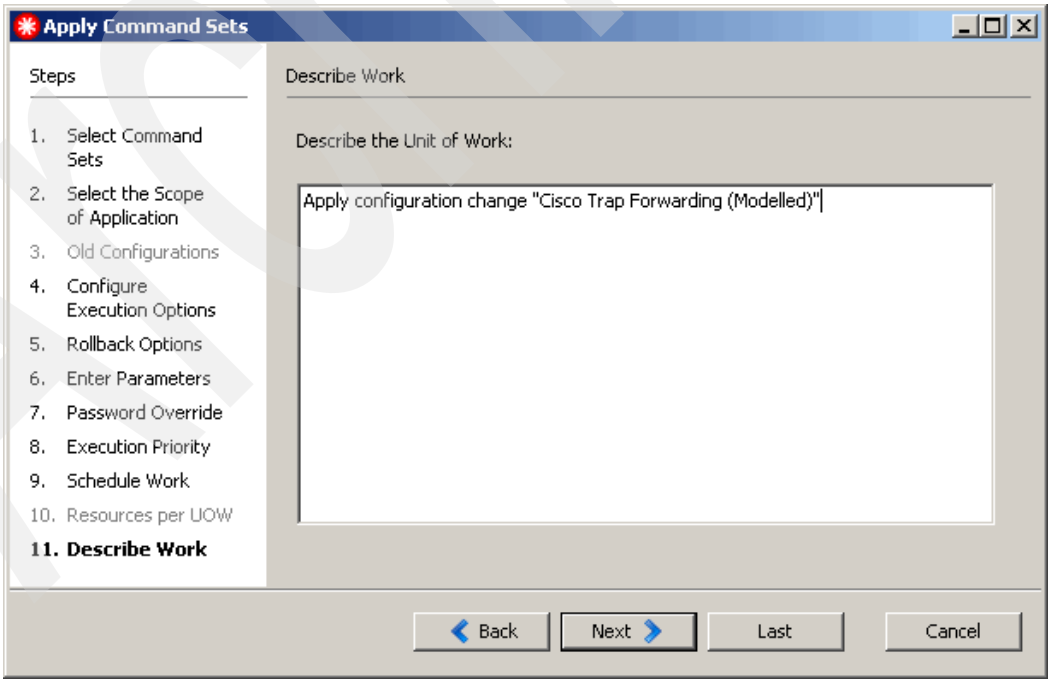



*Figure 5-23 Describe Work*

13. The last window is a summary of the UOW of the actions to be taken. Notice that because we chose Execution Mode instead of Report Only Mode, the Mode field has highlighted, in red, the fact that devices will be modified. Click **Finish** to open the final window (Figure 5-24).

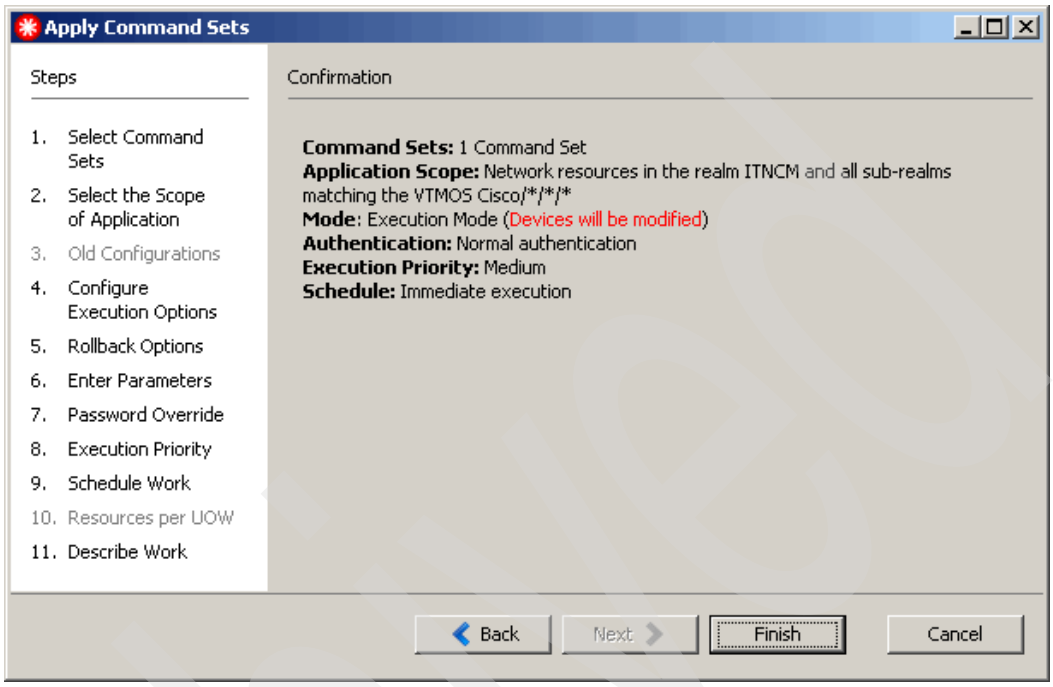



*Figure 5-24 Summary of the UOW*

14. A final window opens and informs you that the UOW was successfully submitted and provides you with the UOW ID number. Click **Close**.

After the UOW has been completed, you may review the logs in Tivoli Netcool Configuration Manager. For more information about how to review the Resource Logs, see Chapter 5. “Queue Manager”, of the *IBM Tivoli Netcool Configuration Manager 6.1 - Base User Guide*, found at the following address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_configurationmgr.doc_6.1.0/ncm_pdf_base_usr_61.pdf

## 5.3 Using Tivoli Netcool Configuration Manager to apply a configuration through the native command set

In this section, we demonstrate how to use the native command set to create a configuration change to be applied to multiple devices. For this example, we use a group of Juniper devices and apply the correct command to add.

### 5.3.1 Creating the command set

To create the native command set, perform the following steps:

1. As shown in Figure 5-1 on page 89 and Figure 5-2 on page 90, log in to the Tivoli Netcool Configuration Manager Base GUI and navigate to the top-level ITNCM realm.
2. From the File menu, select **New** → **Native Command Set** (Figure 5-25).

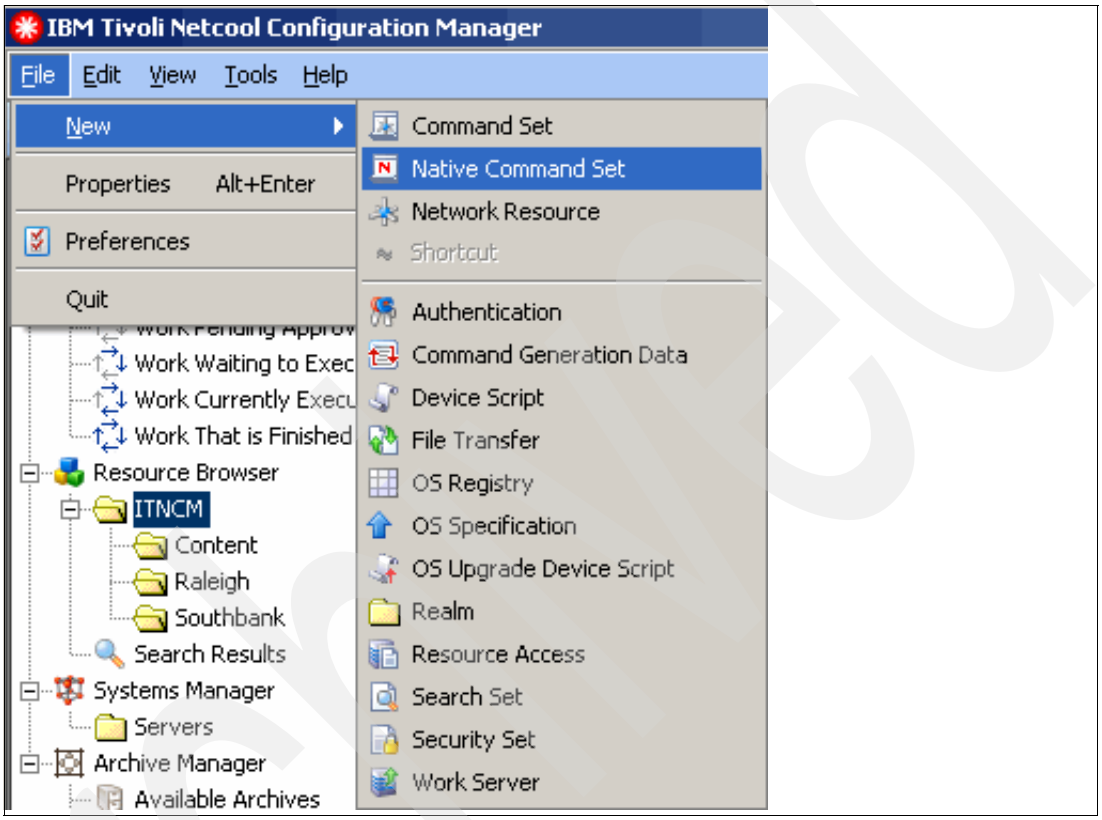



*Figure 5-25 Native Command Set*

3. When prompted, provide a unique name for this command set and supply the VTMOS information (Figure 5-26). In our example, we used the following values:

**Name** Juniper Trap Forwarding (Native)
**Vendor** Juniper
**Type** Router
**Model** M*
**OS** *

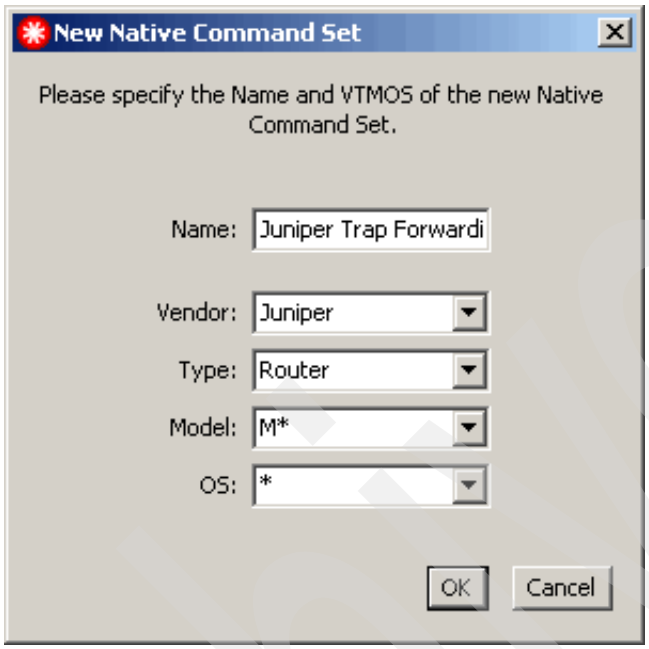



*Figure 5-26 Native Command Set*

4. Return to the Tivoli Netcool Configuration Manager GUI, locate the new native command set in the list, right-click, and select **Edit** (Figure 5-27).

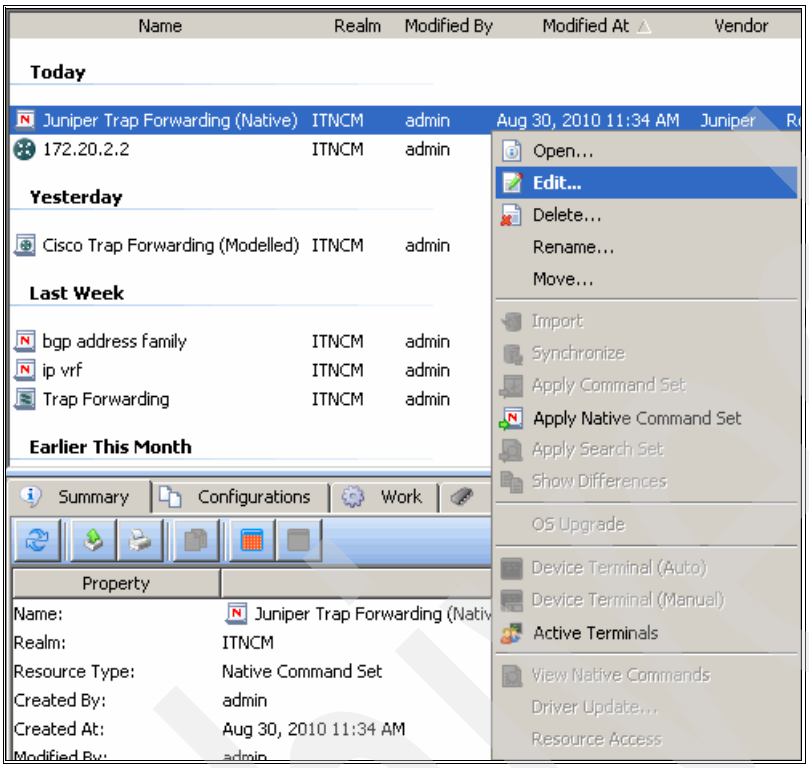



*Figure 5-27 New native command set*

5. In the window that opens next, in the area indicated by the number 1, enter the command that should be executed on the device. Click the **Save** button, indicated by the 2, and close the window by clicking the X in the upper right corner, indicated by the 3. (Figure 5-28).

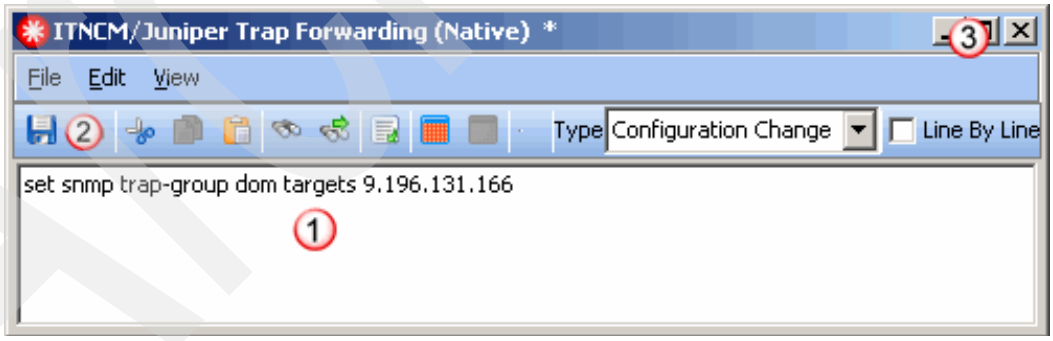



*Figure 5-28 Trap Forwarding*

We have completed the creation of the new native command set.

## 5.3.2 Applying the native command set

This section describes the process used to apply the native command set to a single Juniper device by choosing that device.

Perform the following steps:

1. In the Resource Browser, navigate to a realm containing the device you want to modify. Right-click the device and select **Apply Native Command Set** (Figure 5-29).

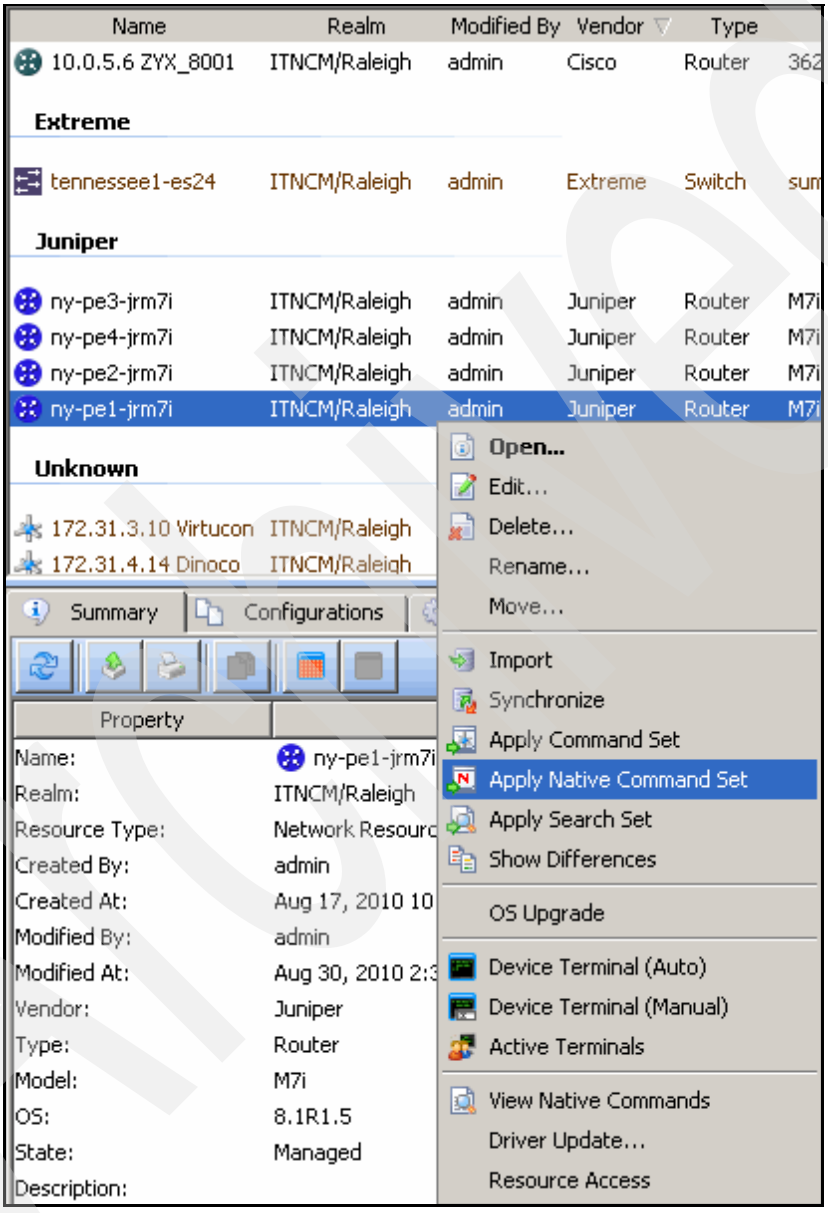



*Figure 5-29 Apply Native Command Set*

2. Highlight the native command set you want to apply, as indicated by the number 1, then click the **Add** button, indicated by the number 2, to move it over to the list of command sets to apply. Click **Next** (Figure 5-30).

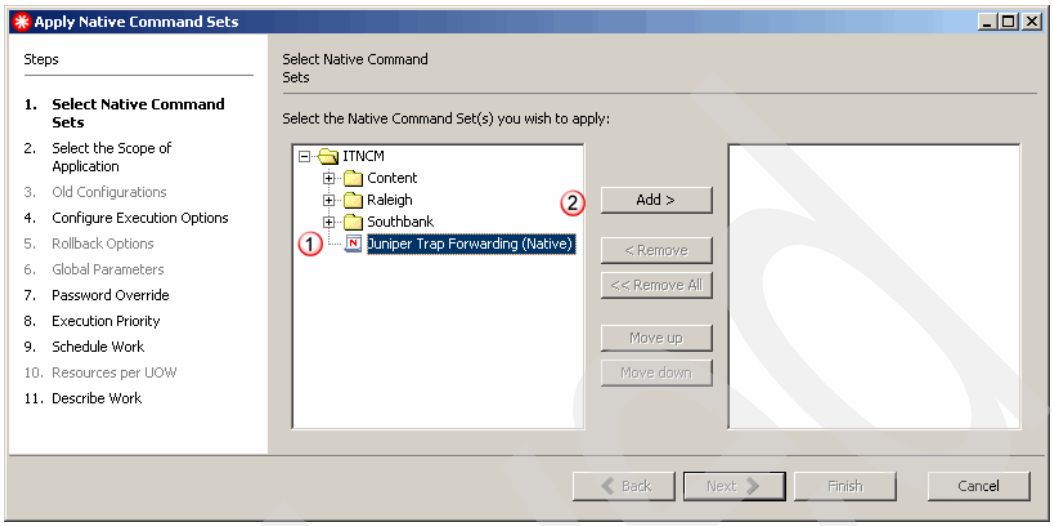



*Figure 5-30 Click the Add button*

3. In the next window, you are prompted for the scope to which the native command set should be applied. We only want to apply to specific resource in this case. Click **Next** (Figure 5-31).

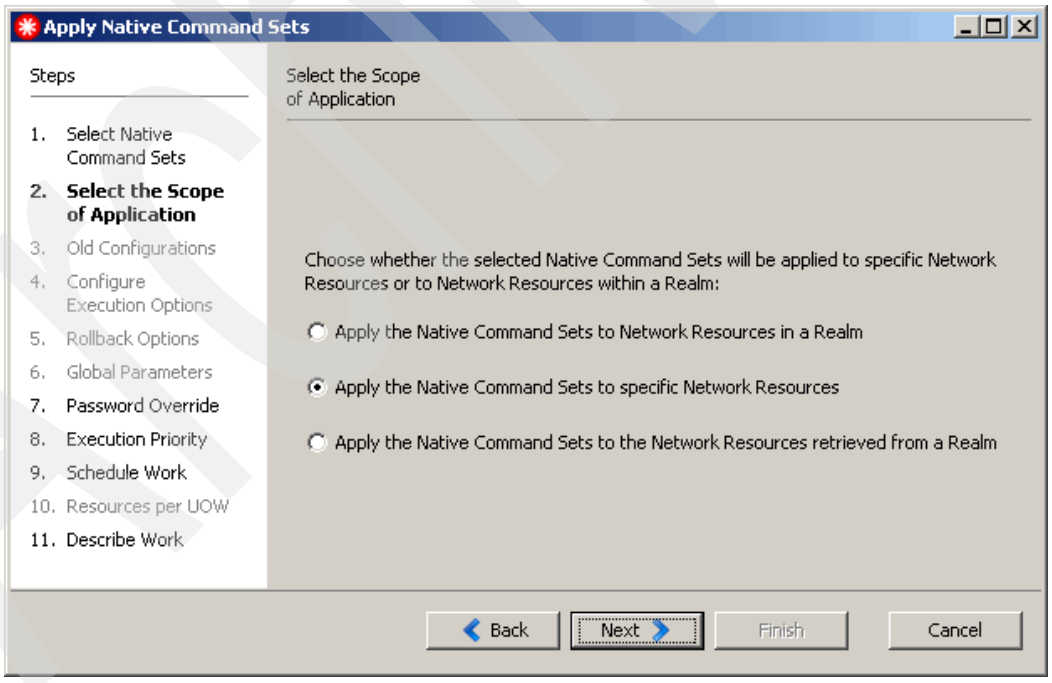



*Figure 5-31 Select the Scope*

4. The next window allows you to select the specific devices to which you want the configuration to be applied. Because we already selected the ny-pe1-jrm7i device, the selection has already been made. Click **Next** (Figure 5-32).

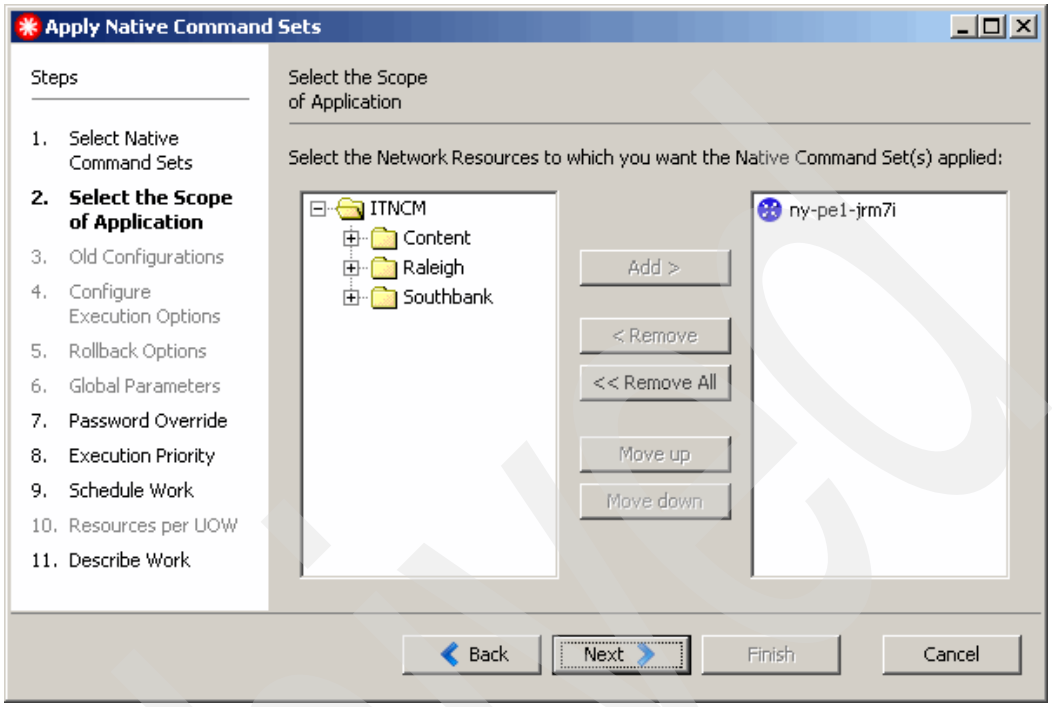



*Figure 5-32 Select the Scope of Application*

5. As before, we have the ability to roll back the change in case of failure, but we will not configure any rollback options. Click **Next** (Figure 5-33).

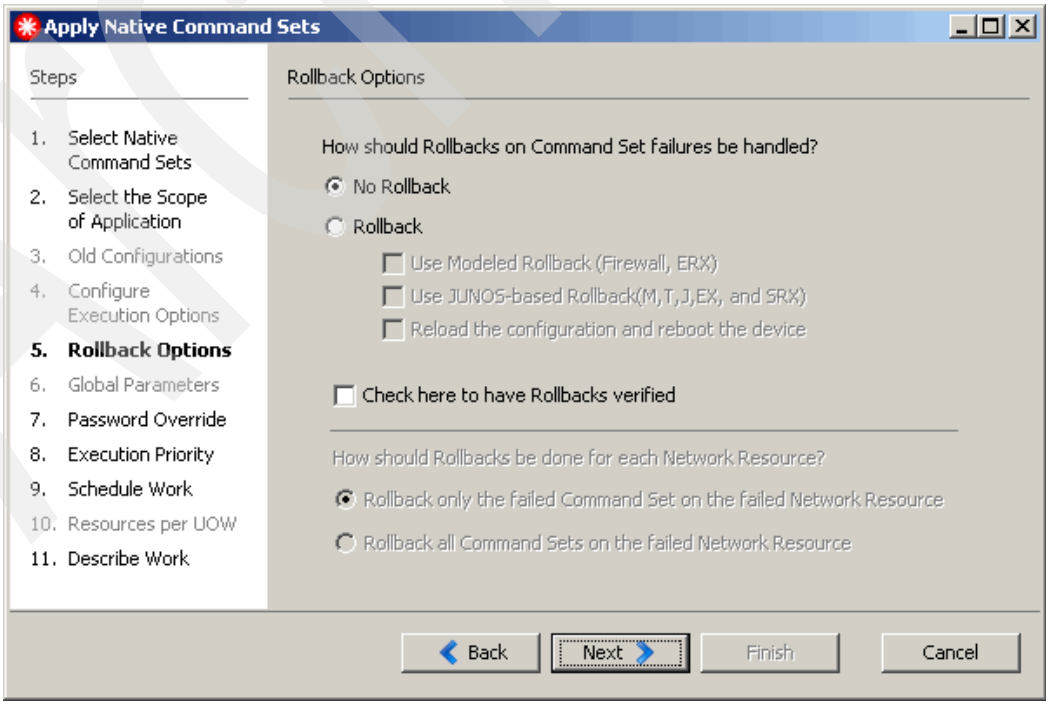



*Figure 5-33 Rollback Options*

6. As before, we are prompted about overriding the default login details for the device. We leave these details unchanged. Click **Next** (Figure 5-34).

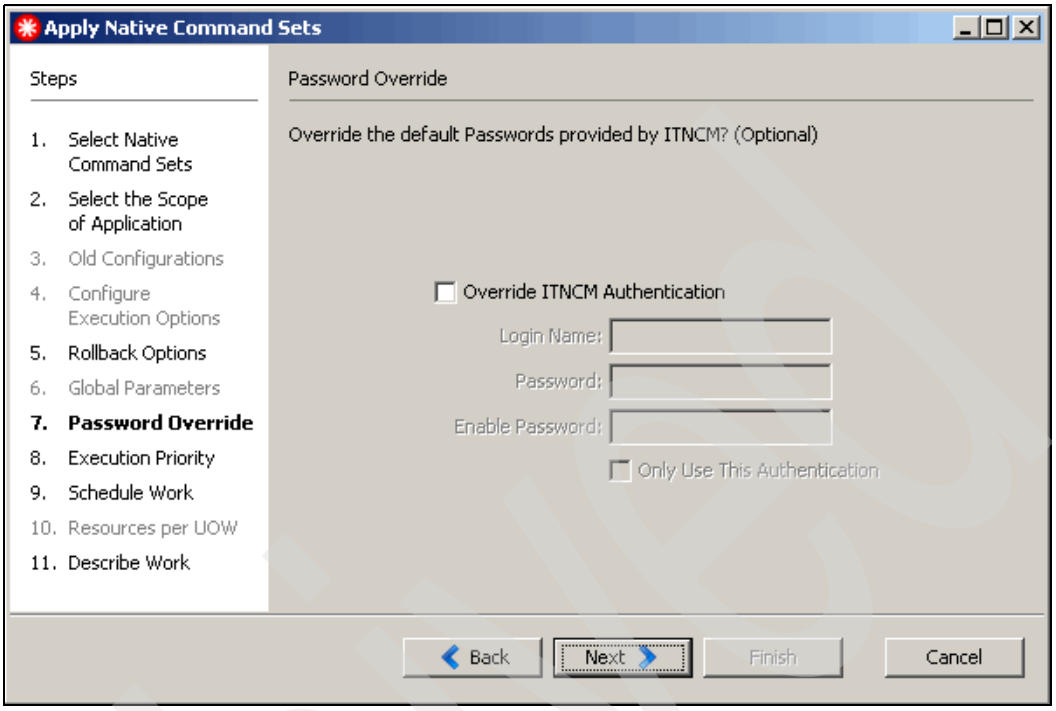



*Figure 5-34 Password Override*

7. The next window is used to set the execution priority. We accept the default of Medium. Click **Next** (Figure 5-35).

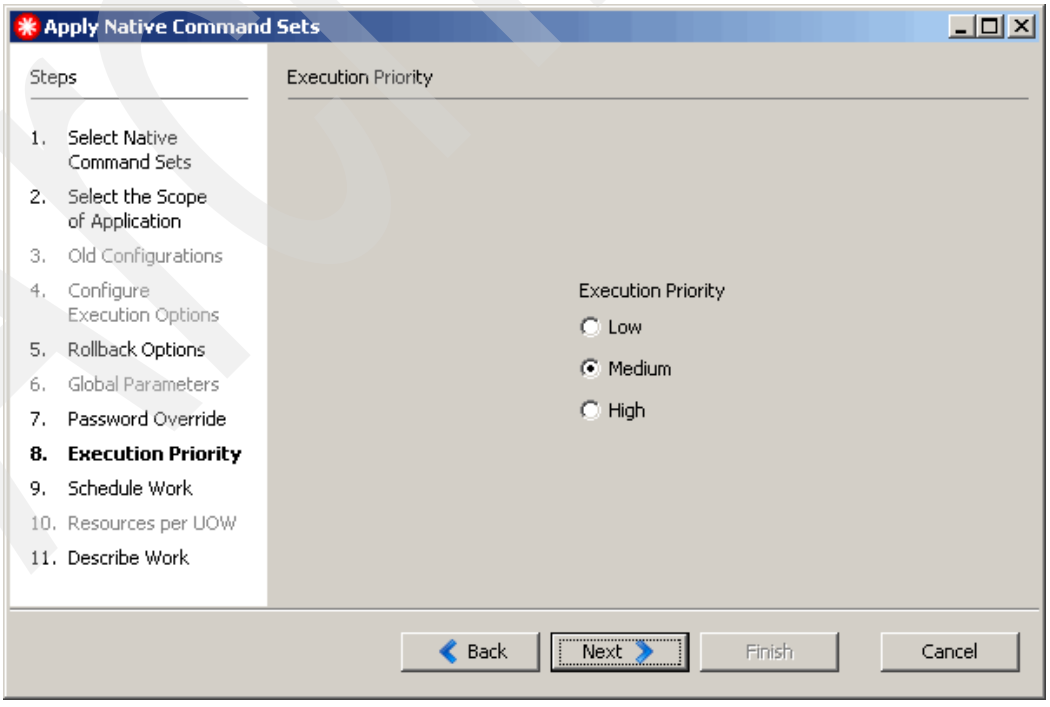



*Figure 5-35 Execution Priority*

8. The next window prompts you to schedule this UOW. In this example, we accept the default, which is to execute it immediately (Figure 5-36).

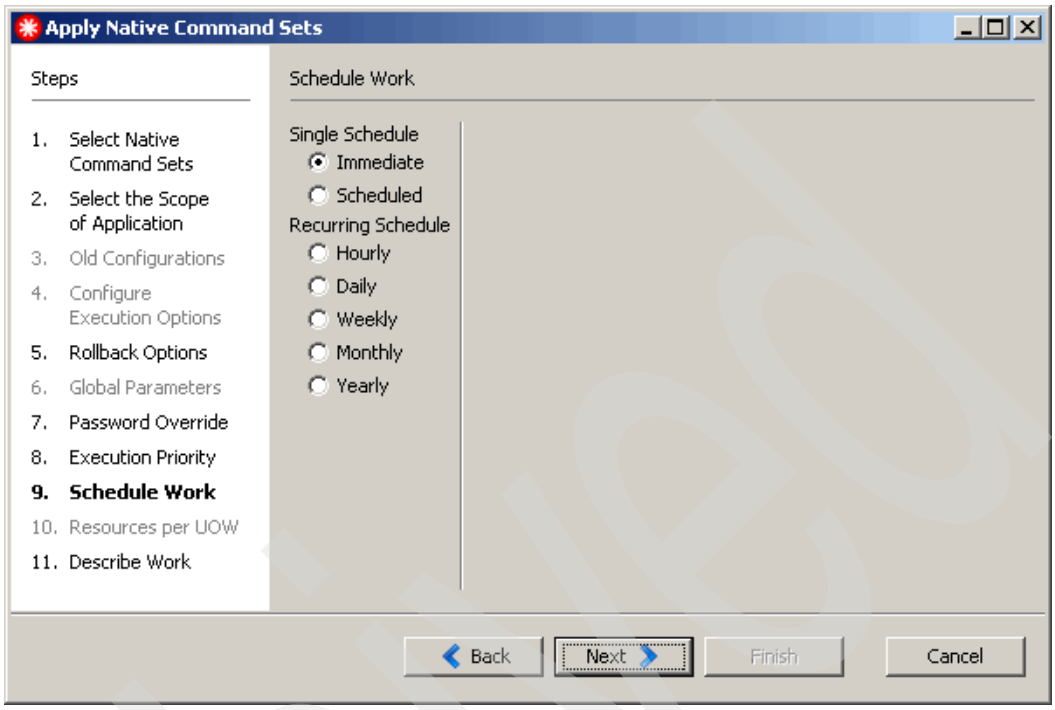



*Figure 5-36 Schedule Work*

9. The last window shows the description of work. Again, enter a description that describes the UOW. Click **Finish** to see the UOW ID number assigned (Figure 5-37).

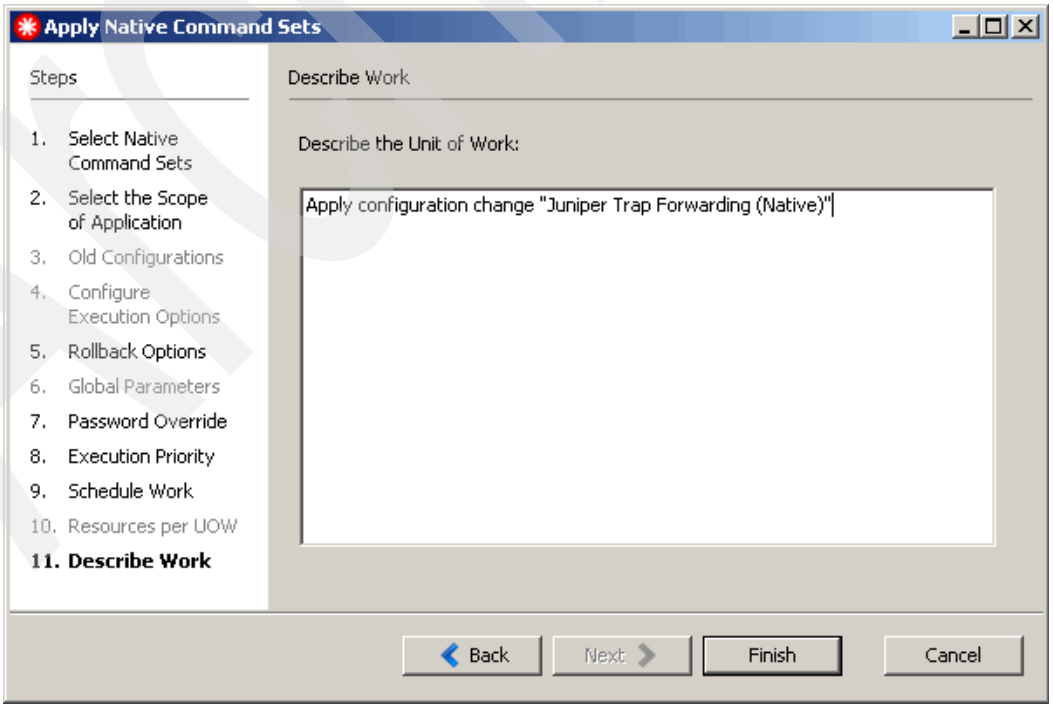



*Figure 5-37 Describe Work*

The UOW is placed in the queue and executed in turn. Review the Resource Logs for the status of the UOW.

## 5.4 Results of these configuration changes

To observe the results of these changes, take a look in the Active Event List (AEL) to see traps received from these devices. For example, we now have a trap from a Cisco device that we configured in 5.3.2, “Applying the native command set” on page 108. We can see that it is a Cisco Catalyst and that the mttrapd probe received and processed this trap (Figure 5-38).

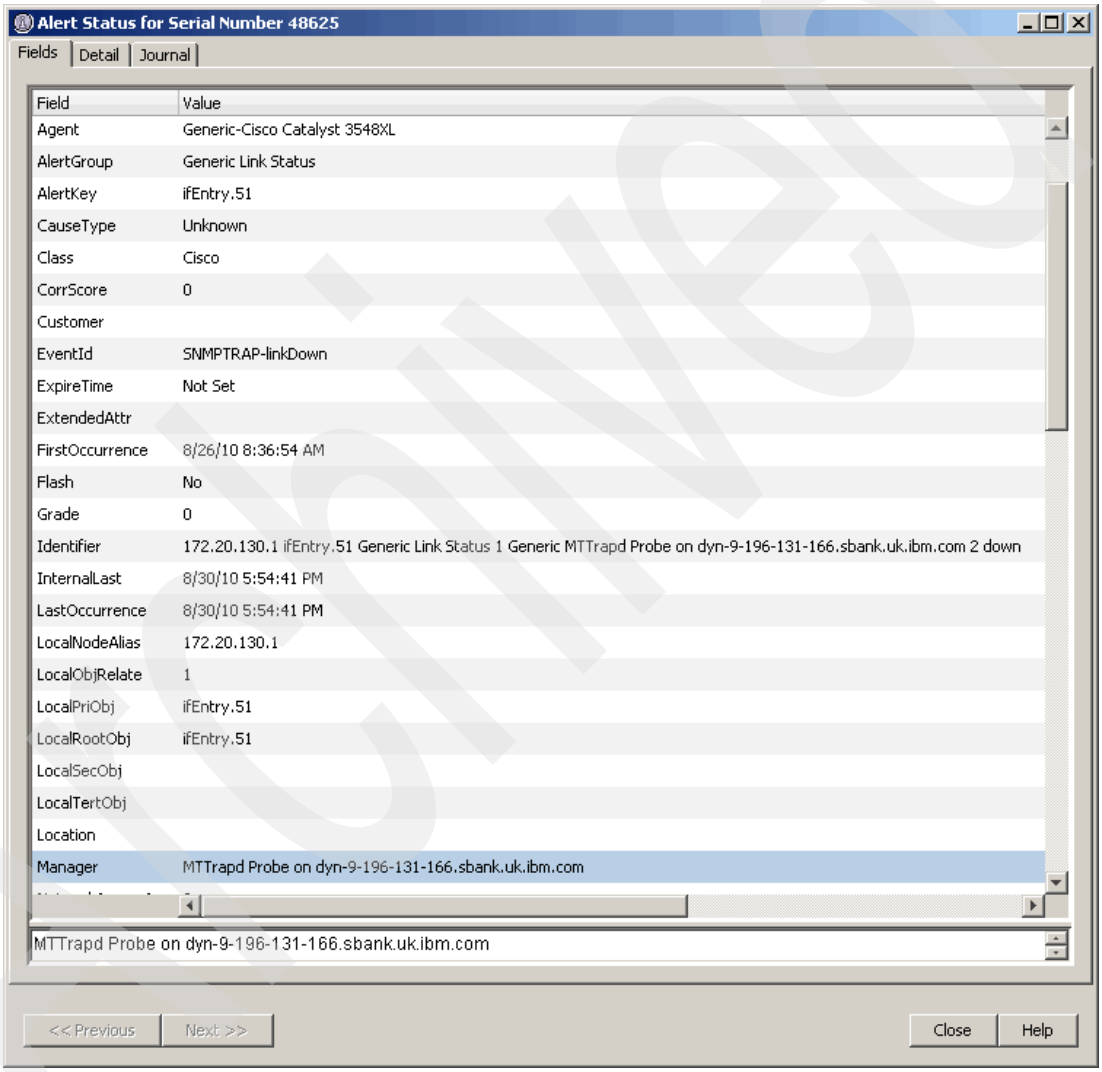



*Figure 5-38 Results of these configuration changes*

6

# Ensuring that a configuration is appropriate for supporting a new network service

This scenario outlines how we can use Tivoli Netcool Configuration Manager compliance policies to ensure that a configuration is consistent across a subset of managed routers. Tivoli Network Manager is used to decide to which devices to apply the compliance policy. We verify that the policy has been set by using both Tivoli Network Manager and within Tivoli Netcool Configuration Manager.

This chapter describes the following topics:

## 6.1 Scenario

A service provider receives a request to provide a layer 3 MPLS Virtual Private Network (VPN) for a new customer named ZYX Industries. The service provider uses Tivoli Network Manager to select ZYX's office facing PE routers and apply an MPLS L3 VPN compliance policy to these devices.

There are three steps to create a new layer 3 MPLS VPN within a Cisco router. We use a compliance policy to apply two of these steps: Creating the customer's ip vrf definition and creating a new customer named bgp address-family.

The following scenario describes how to create an ip vrf definition, remedial-action, rule, and policy. A new process is created that applies both the ip vrf and ip address-family policies to the PE routers. If the policy fails, the remedial action is applied to add the ip vrf and bgp address-family configurations to the routers.

There are several items that must be created to create a compliance policy within Tivoli Netcool Configuration Manager - Compliance:

1. A *command set* is the set of commands that are applied to the router. The command set can include variables. We use global variables for the BGP domain AS number and for the customer name. This single policy can then be used again and again for each new customer.
2. To determine if a router configuration contains a particular command set, we need a *definition* containing the most fundamental part of the command set.
3. We create a *remedial action* to provide details about what needs to be done if the definition is not satisfied and a configuration change is necessary.
4. We create a *rule* that determines how the definition and remedial action can be applied.
5. We create a *policy* to define the set rules run by a process.
6. We create a *process* to define which devices to run and to determine when to run a set of policies.

# 6.2 Creating an ip vrf command set

Perform the following steps to create an ip vrf command set:

1. Create two new global parameters named CUST and AS. In the Netcool Configuration Compliance Manager, select **Parameters** → **Parameter Administration** to open the Parameter Administration window. Select **New** to create a new parameter. Enter a description and a value for the parameter and select **Apply** (Figure 6-1).

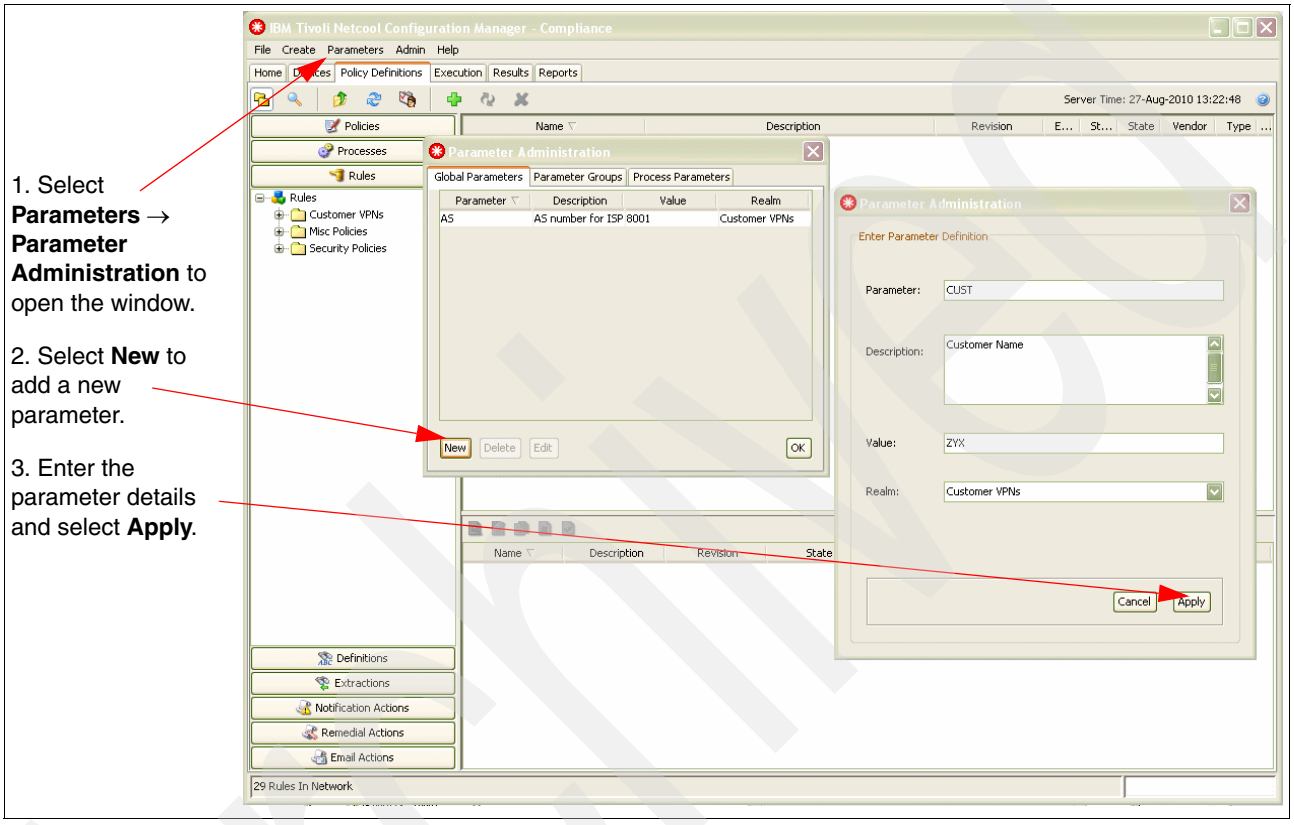



*Figure 6-1 Creating global parameters*

2. To create a new native command set, from the Tivoli Netcool Configuration Manager, select **File** → **New** → **Native Command Set**. Enter a name for the native command set enter Cisco in the Vendor field and Router in the Type field, and select **OK** (Figure 6-2).

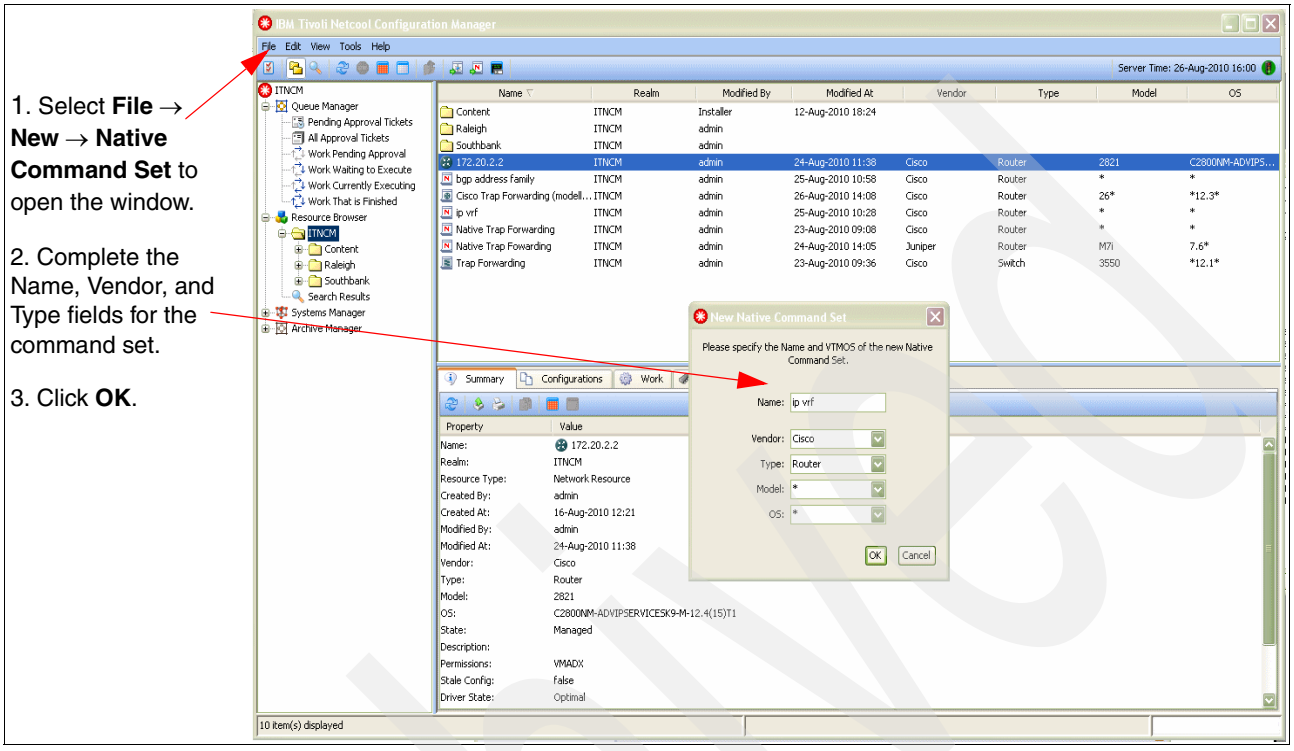



*Figure 6-2 Creating a new ip vrf command set*

3. Add the ip vrf command set. Enclose the AS and CUST parameters between '$' signs (Figure 6-3).

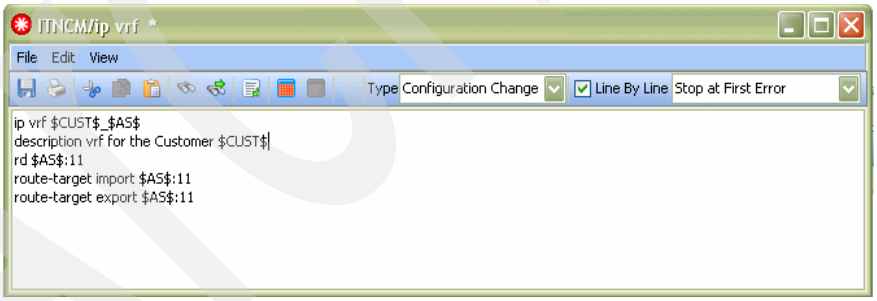



*Figure 6-3 Adding the ip vrf command set*

4. Add the ip address-family command set in a similar way (Figure 6-4).

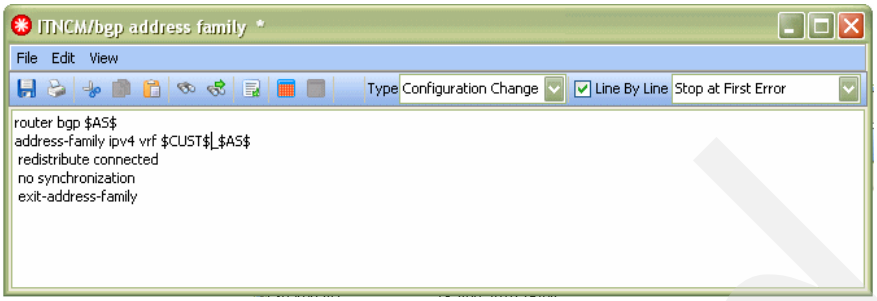



*Figure 6-4 Adding the bgp address-family command set*

## 6.3 Creating the ip vrf definition

The following steps describe how to create a definition within the Tivoli Netcool Configuration Manager Compliance Manager. The text in the ip vrf ZYX definition is compared with the text in the configuration file to confirm that the ip vrf ZYX command set has been applied to the selected devices. A similar definition needs to be created for the bgp address-family policy.

Perform the following steps:

1. Within Tivoli Netcool Configuration Manager Compliance Manager, navigate to the **Policy Definitions** tab. Select **Definitions** from the drop-down tabs on the left side. Select **Create Definition** either from the Create drop-down menu or by selecting the green plus symbol (Figure 6-5).

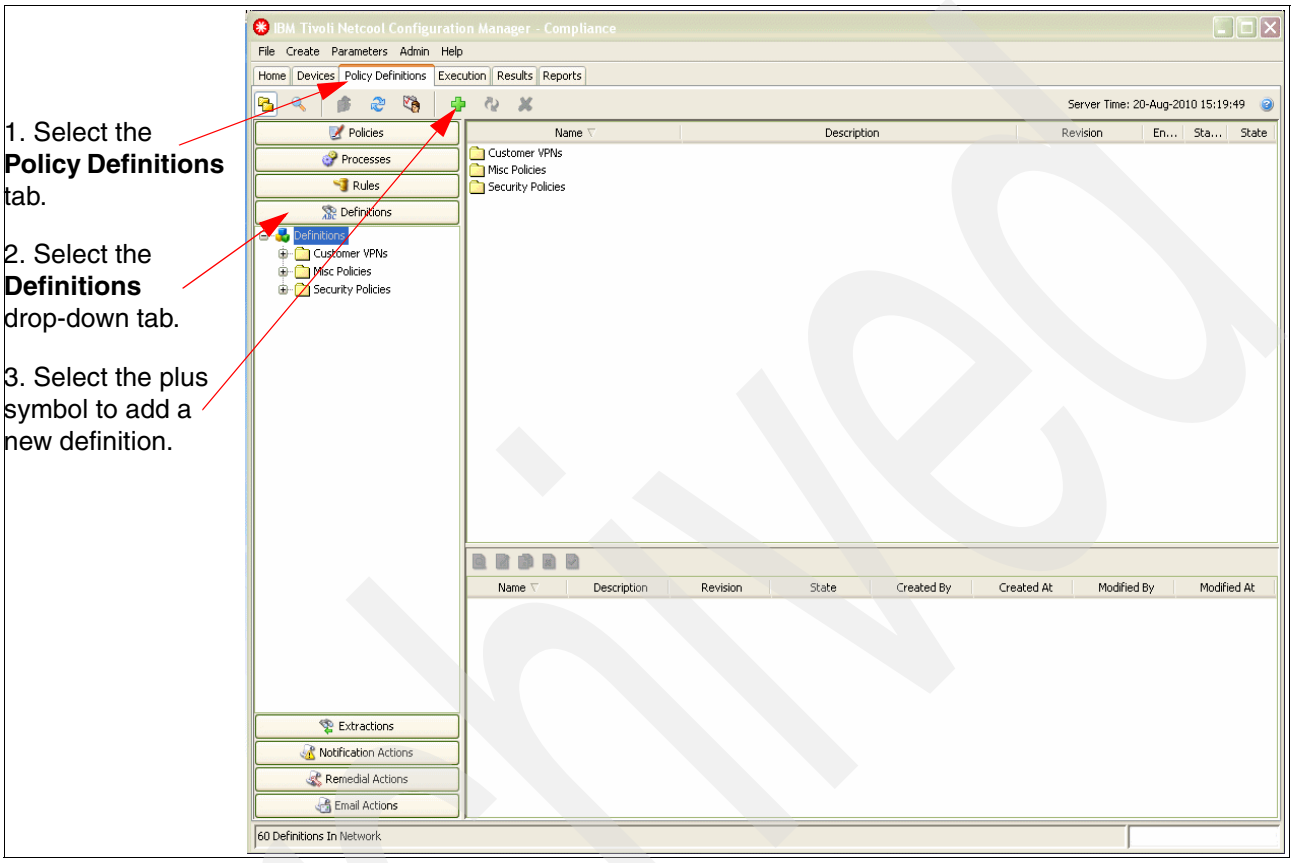



*Figure 6-5 Tivoli Netcool Configuration Manager - Compliance Definitions tab*

2. Enter a name and description for the definition. Select the **Create compliance definition using CLI configuration lines** radio button and select **Next** (Figure 6-6).

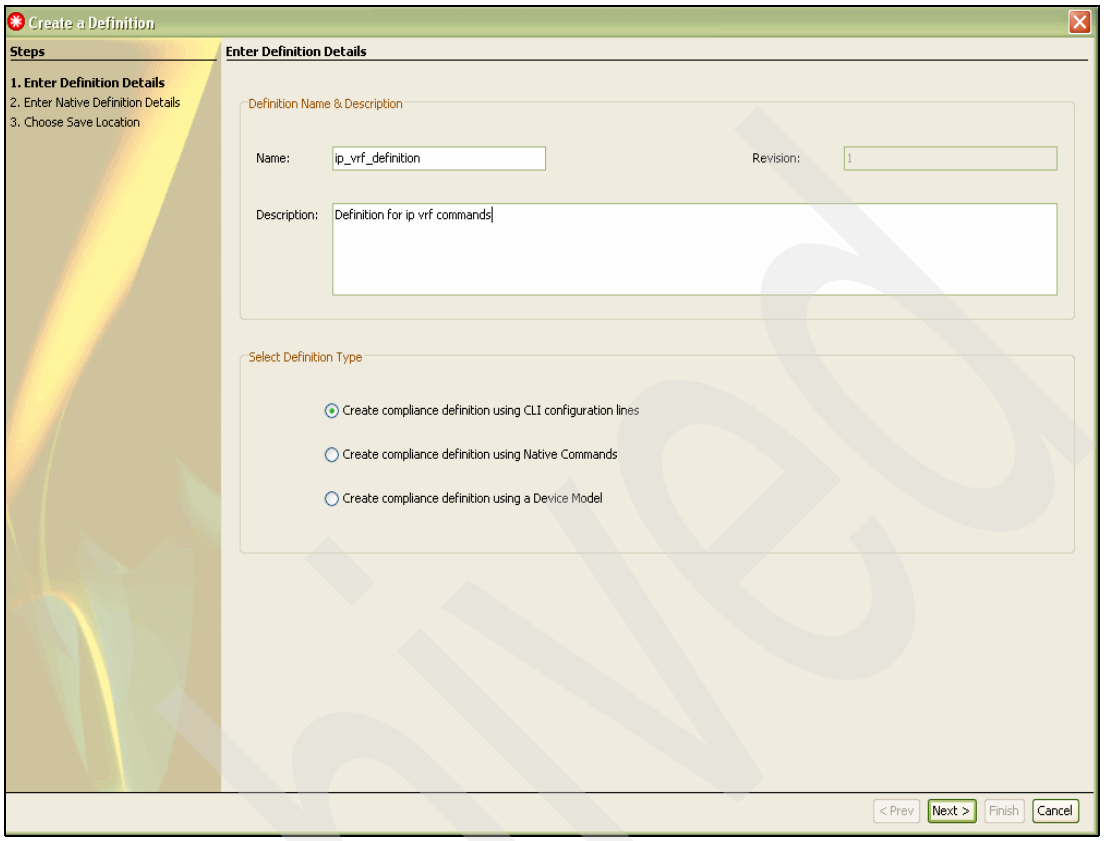



*Figure 6-6 Defining the ip vrf compliance definition*

3. Enter the evaluation definition details. We want to check that the configuration has been created for a new ip vrf. Enter the text “ip vrf:” and select the AS and CUST Global Parameters by clicking the **Insert Parameter** button. Click the **Add** button to add this command to the Evaluation List and select **Next** (Figure 6-7).

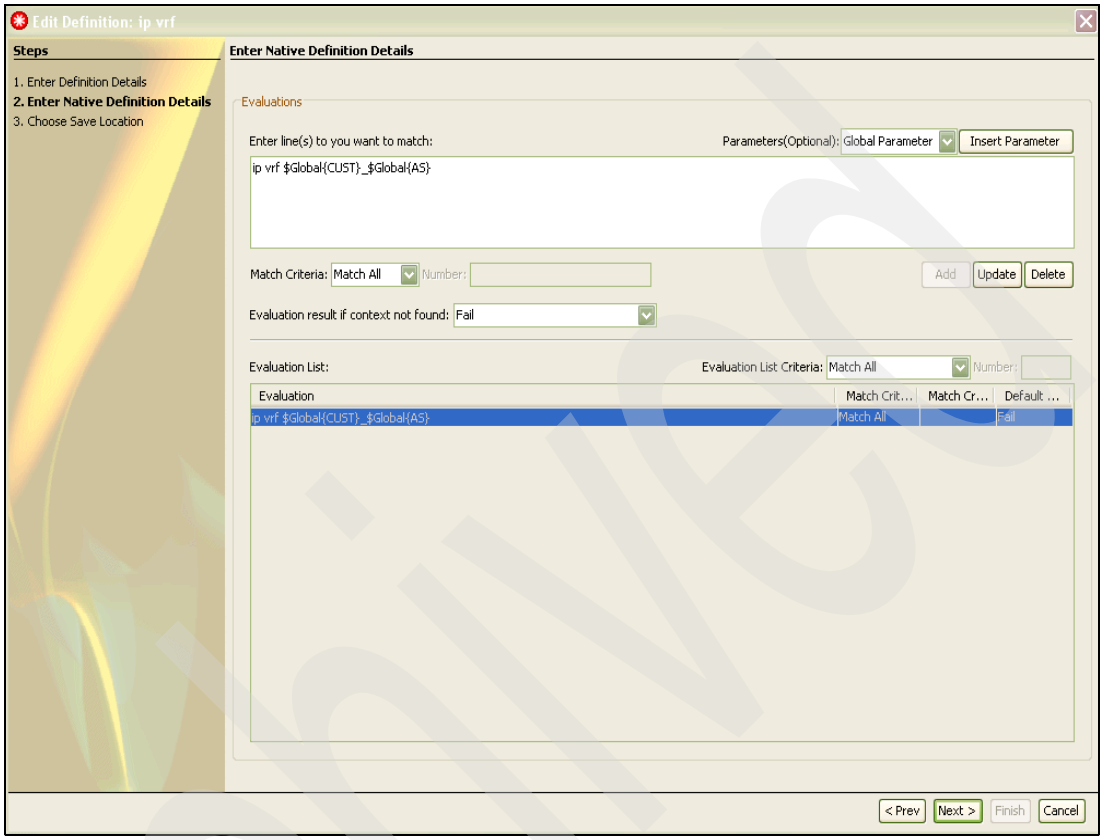



*Figure 6-7 Entering the ip vrf evaluation definition*

4. Select a location to which you save the new definition. It maybe useful to create a new realm to which you add all new configurations. Select **Finish** (Figure 6-8).

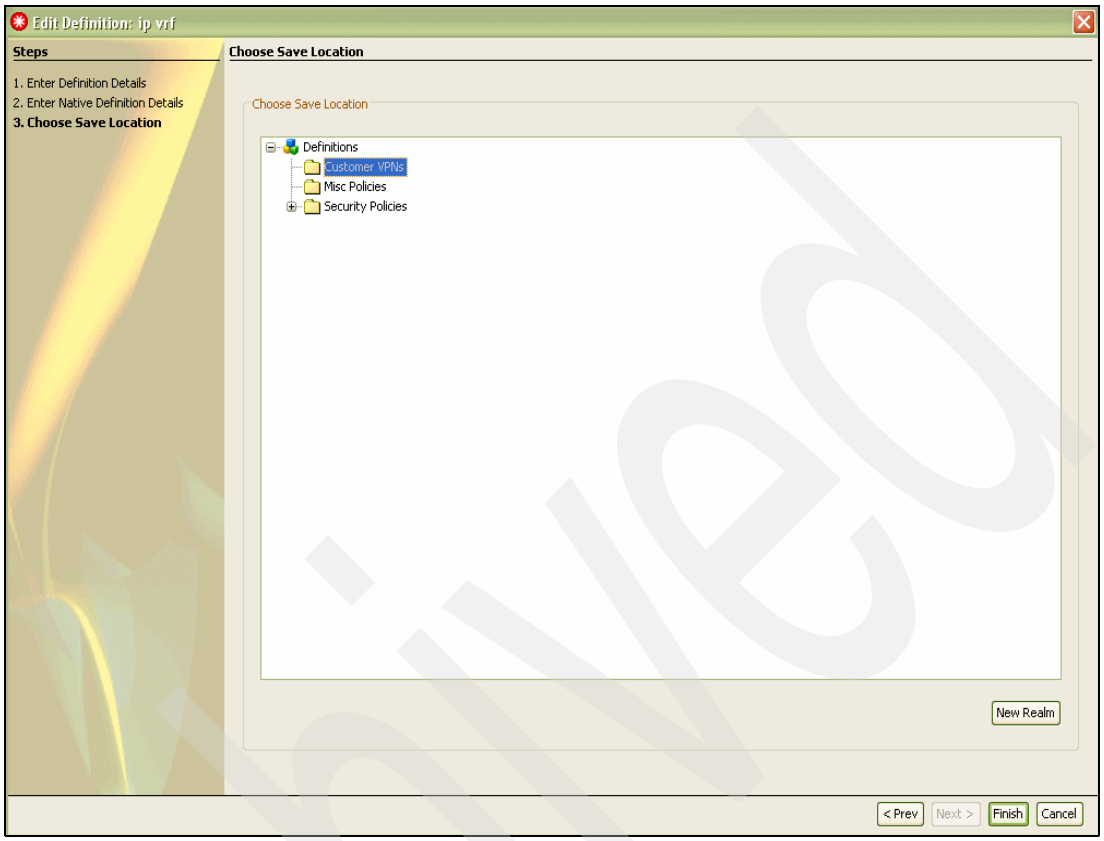



*Figure 6-8 Selecting a location to which you save the new ip vrf definition*

## 6.4 Creating an ip vrf remedial action

When we run a rule, it compares the router configuration with the definition created in 6.3, “Creating the ip vrf definition” on page 119. If the configuration comparison fails, we need to define a remedial action that can be used to correct it. In this case, the remedial action is to run the command set to create a new ip vrf.

Perform the following steps:

1. Within Tivoli Netcool Configuration Manager Compliance Manager, navigate to the **Policy Definitions** tab. Select **Remedial actions** from the drop-down tabs on the left side. Select **Create Remedial action** either from the Create drop-down list or by selecting the green plus symbol (Figure 6-9).

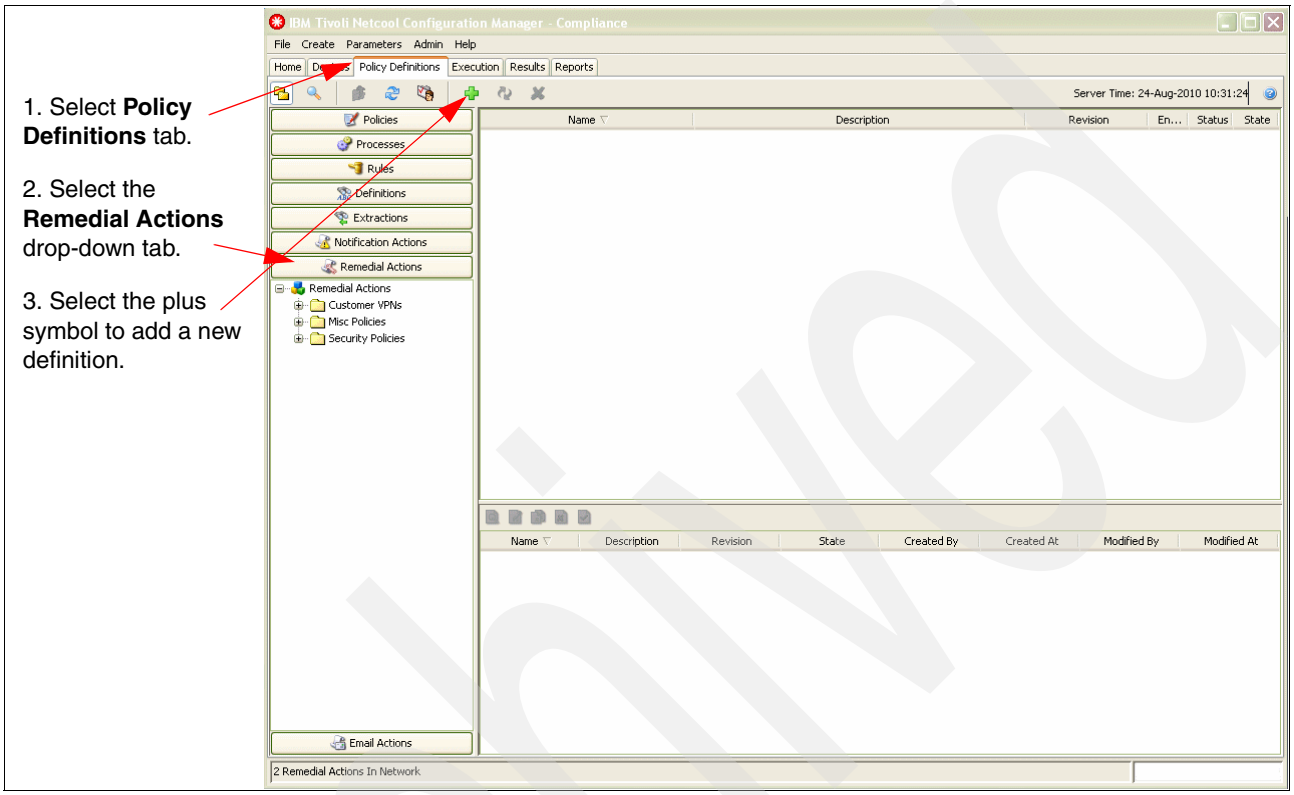



*Figure 6-9 Tivoli Netcool Configuration Manager - Compliance Remedial Actions tab*

2. Enter a name and description for the remedial action. Select the **Remedial Action** radio button. Select **Next** (Figure 6-10).

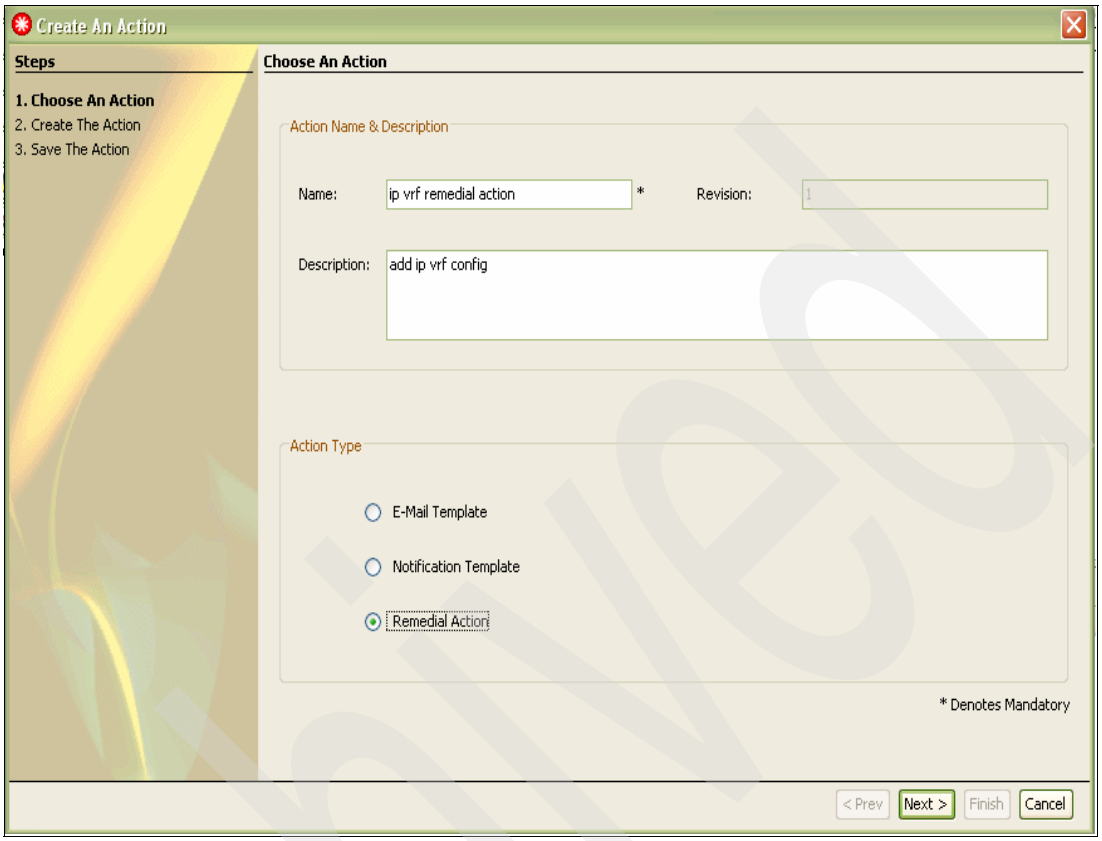



*Figure 6-10 Defining the ip vrf remedial action*

3. Select the command set to run as the remedial action, in this case, the ip vrf command set (Figure 6-11). Select **Next**.

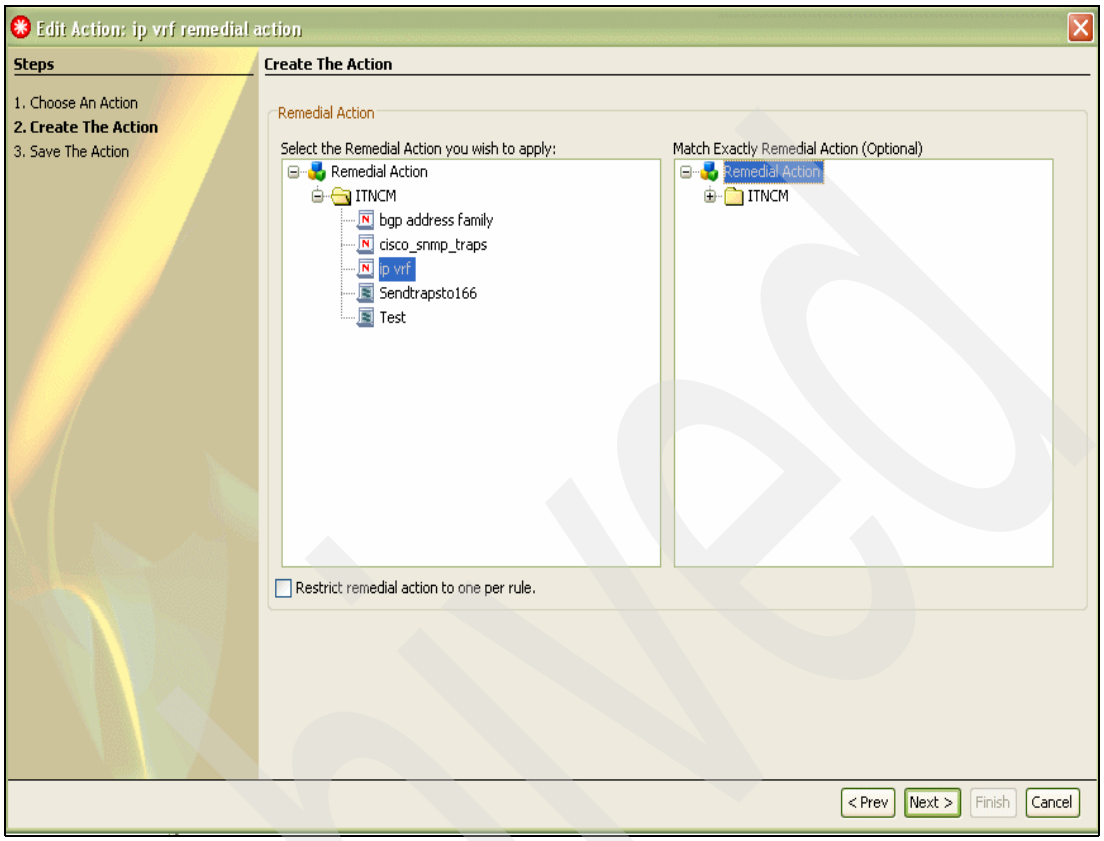



*Figure 6-11 Selecting the ip vrf command set for the remedial action*

4. Select a location to save the remedial action (Figure 6-12). Click **Finish**.

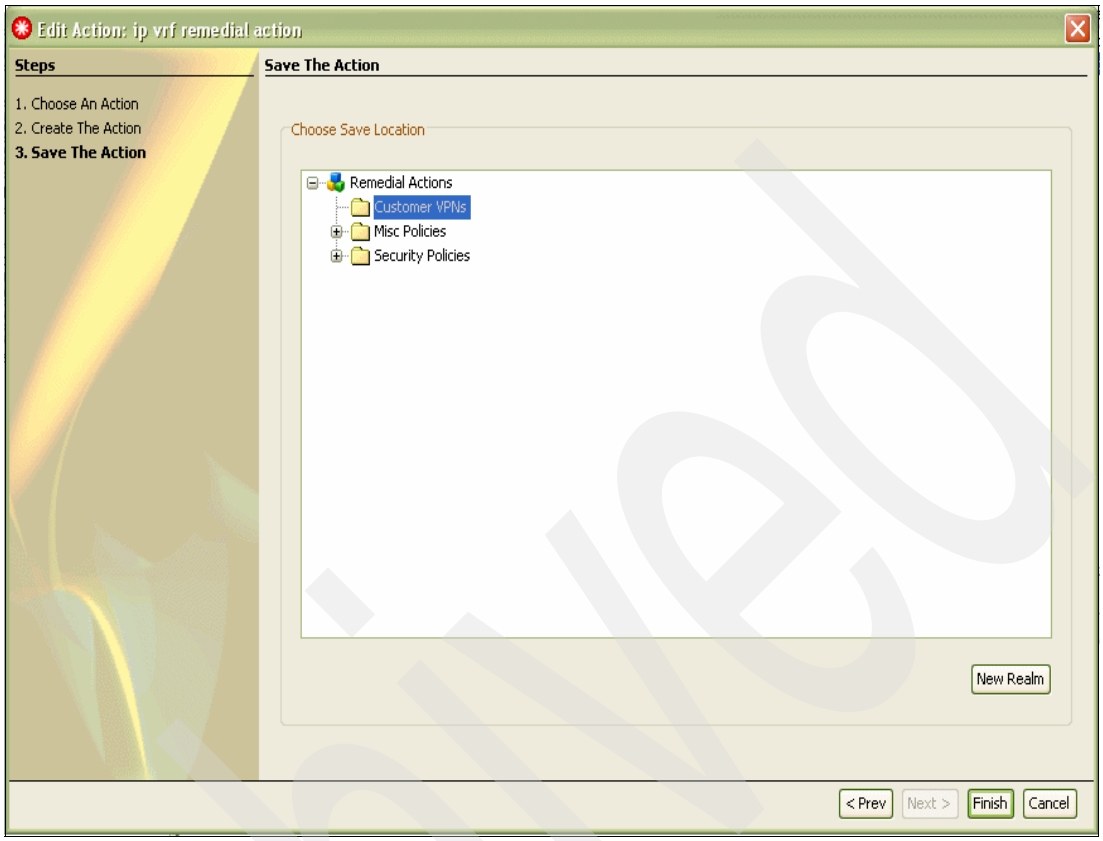



*Figure 6-12 Selecting a location to save the new remedial action*

## 6.5 Creating an ip vrf rule

Now that the definition and remedial action have been created, it is necessary to link these together using a rule.

Perform the following steps:

1. From the Tivoli Netcool Configuration Manager Compliance home page, click the **Rule** tab and create a new rule by selecting the green plus symbol.

2. Enter a name and description for the rule. Select **cisco** and **router** from the Application Device Filter (Figure 6-13). Select **Next**.

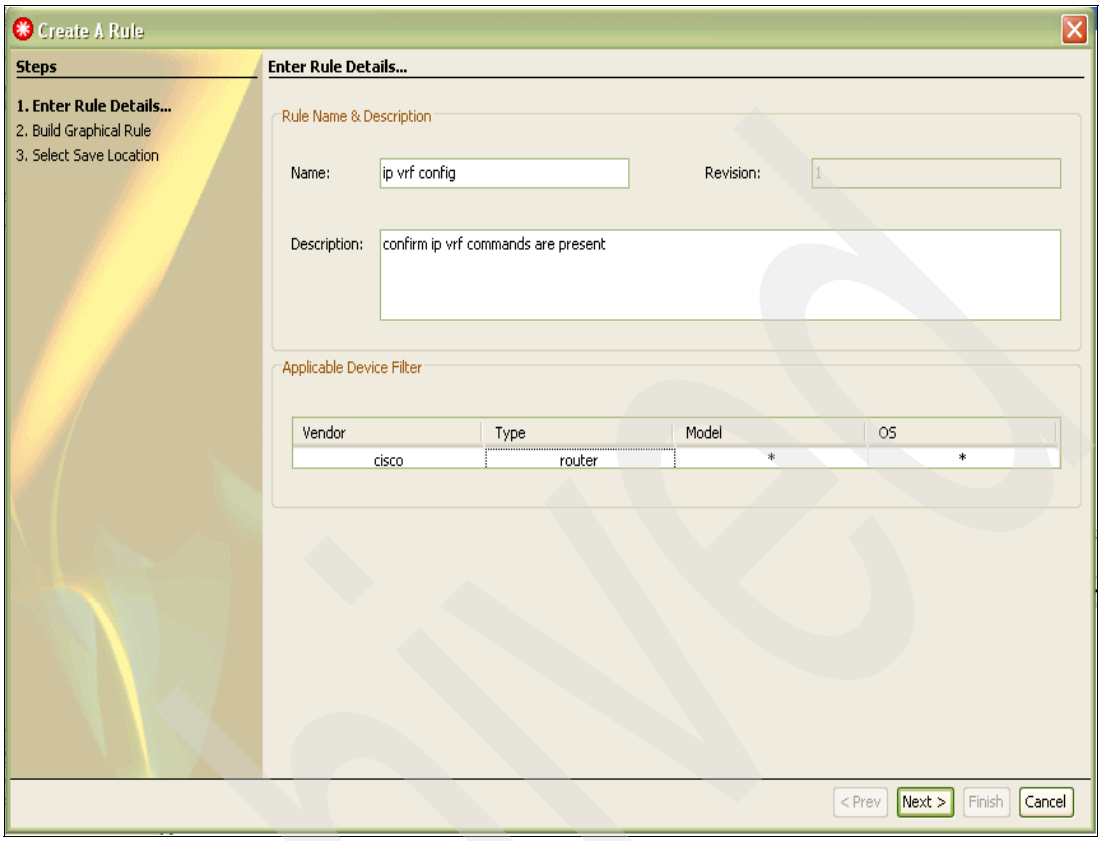



*Figure 6-13 Defining the new ip vrf configuration rule*

Using the tools on the left hand side, build a graphical rule (Figure 6-14). Drag a Start ( )and Compliant ( ) icon into the empty space on the right side. When you drag a definition ( ) icon into the space, a select definition window opens (Figure 6-15 on page 130). This window is used to select the actual definition you want to use.

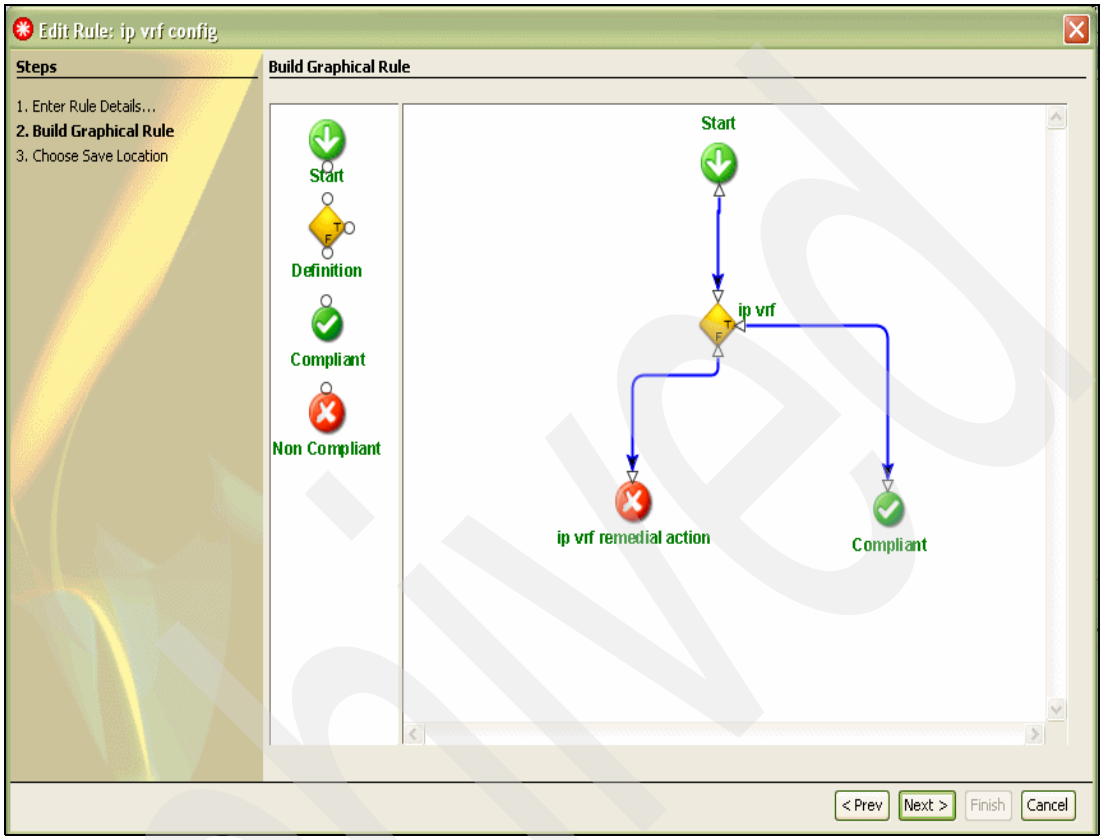



*Figure 6-14 Building an ip vrf graphical rule*

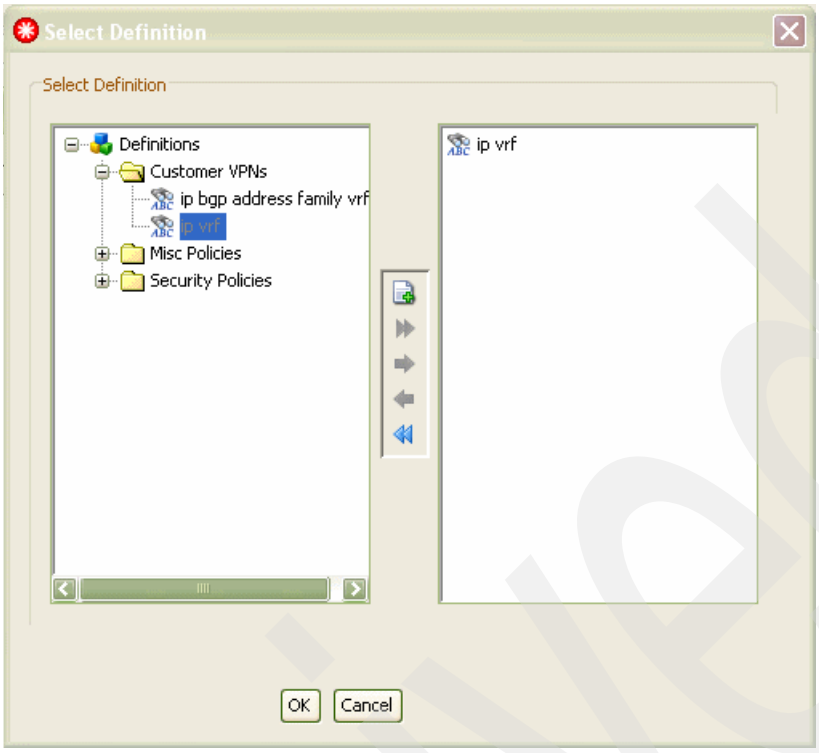



*Figure 6-15 Selecting a definition for the rule to use*

Back in the Edit Rule window (Figure 6-14 on page 129), drag the Non Compliant X icon on to the white space. A Select Remedial action window opens. Select the ip vrf remedial action. Connect the icons together with arrows by clicking the small circles and dragging the arrow connections to another icon.

3. Save the rule in a suitable location and click **Finish**.

## 6.6 Creating a new ip vrf policy

You can create a new ip vrf policy by performing the following steps:

1. From the Tivoli Netcool Configuration Manager Compliance home page, click the **Policies** tab and create a new policy by selecting the green plus symbol.

2. Enter a name and description for the policy. Select **Cisco** and **Router** from the Application Device Filter and include the ip vrf configuration rule from the Rules Included section (Figure 6-16). Select **Next**.

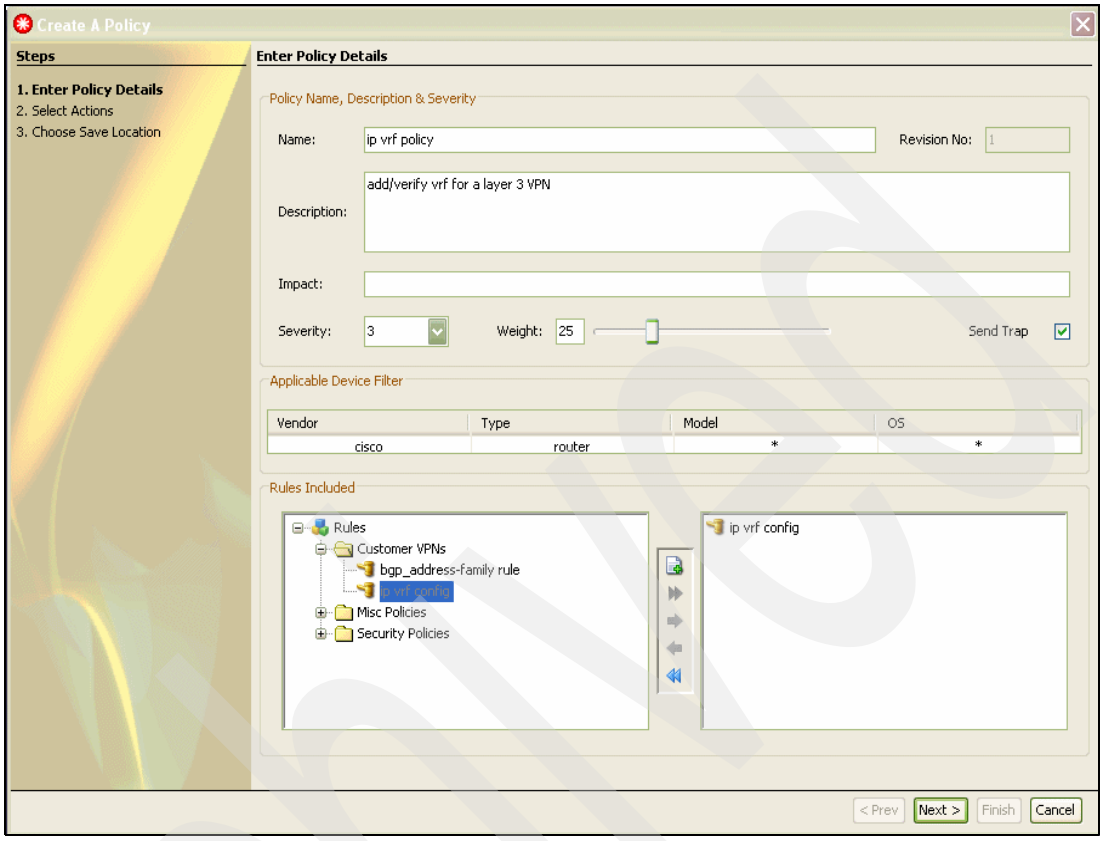



*Figure 6-16 Defining the ip vrf policy*

3. Select the **No Action** radio button and click **Next** (Figure 6-17).

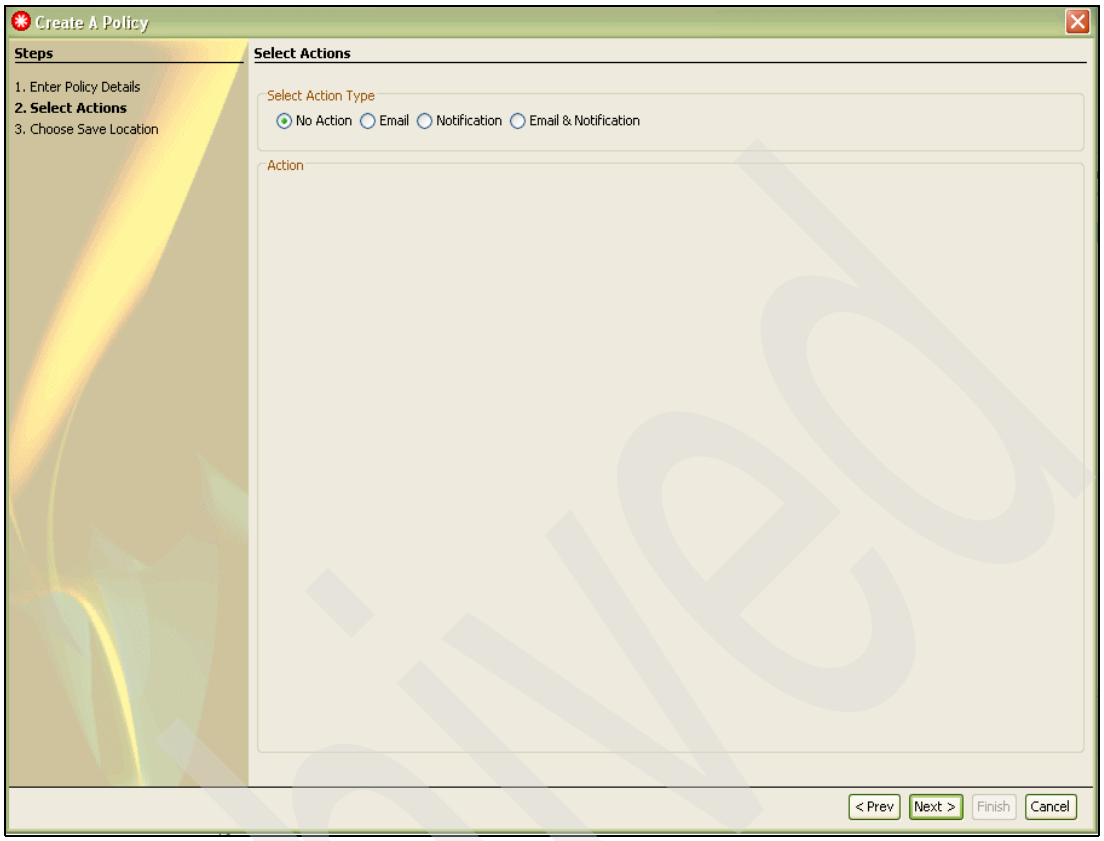



*Figure 6-17 Selecting the ip vrf policy action*

4. Save the new policy in a suitable location and click **Finish**.

## 6.7 Creating a new layer 3 VPN process

To create a new layer 3 VPN process that includes the ip vrf and the bgp address-family policies, perform the following steps:

1. From the Tivoli Netcool Configuration Manager Compliance home page, create a new process by selecting the green plus symbol.

2. Enter a name and description for the layer 3 VPN process. Add both the ip vrf policy and the bgp address-family policy to the process (Figure 6-18). Select **Next**.

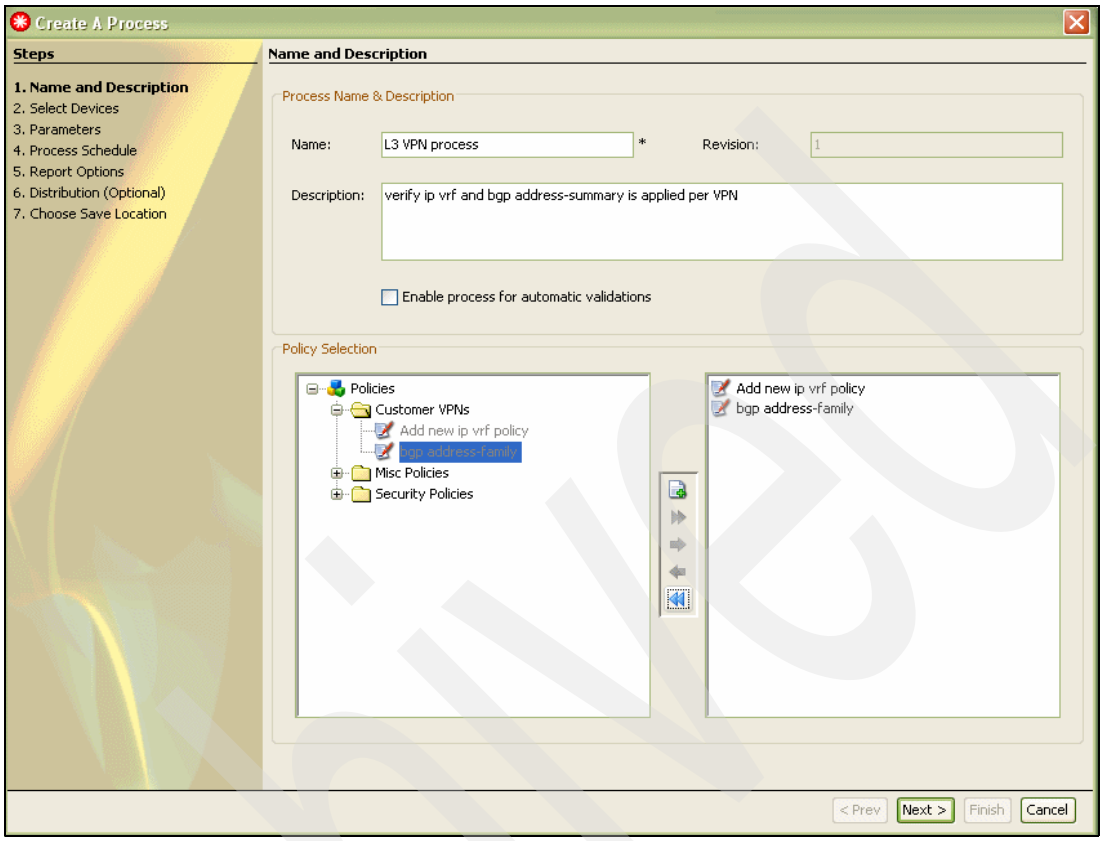



*Figure 6-18 Defining a new process*

3. From the Network views within Tivoli Network Manager IP Edition, select the **MPLS Core view** and from determine the PE routers that are connected to the ZYX's customer environment (Figure 6-19).

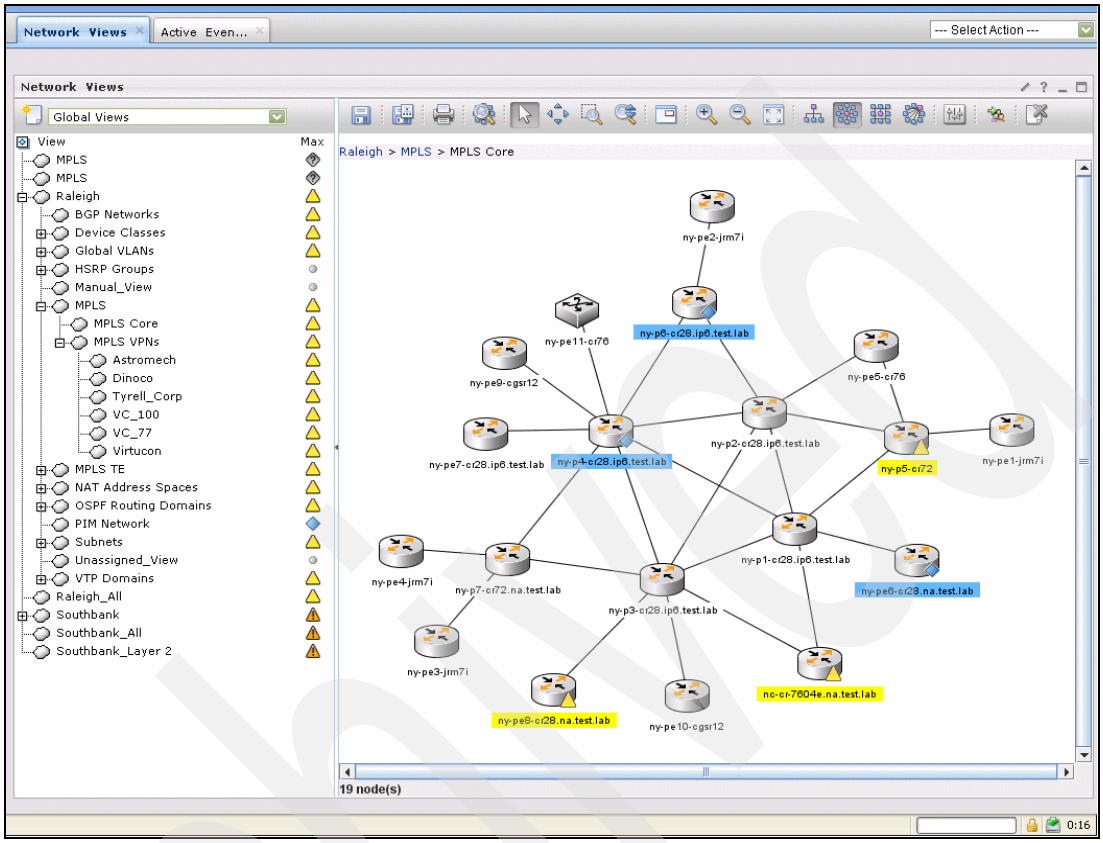



*Figure 6-19 MPLS Core Network view from Tivoli Network Manager*

4. From within the Tivoli Netcool Configuration Manager Compliance process view, select the ZYX's customer-facing PE routers determined by Tivoli Network Manager (Figure 6-20). Select **Next**.

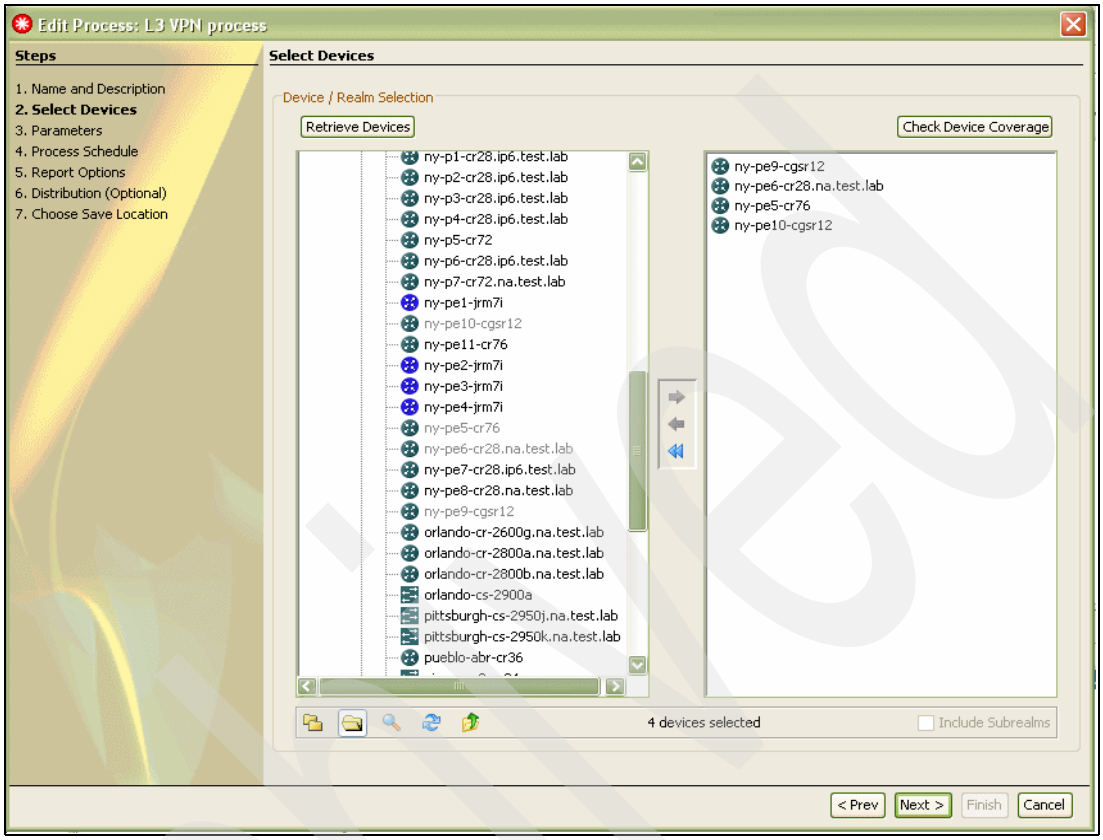



*Figure 6-20 Selecting PE routers connected to the customer network*

5. The next window provides options to add and edit the parameters for this process. Leave the parameters as the defaults and select **Next**.
6. It is possible to define a schedule for the process to run from the next window. Leave the definition as the default and select **Next**.
7. There are report options defined in the next window. Leave the options as the defaults and select **Next**.
8. It is possible to store or email reports from the next window. Leave the options as the defaults and select **Next**.
9. Choose a suitable place to save the new process and click **Finish**.

# 6.8 Executing the process

Now that we have created the process, we can execute it to determine if the commands are present or not. Perform the following steps:

1. From the Tivoli Netcool Configuration Manager - Compliance home page, select the **Execute** tab and the **By Process** drop-down table. Select the L3 VPN process just created and execute the process by pressing the **Execute** button. Click **Yes** in the dialog box that opens (Figure 6-21).

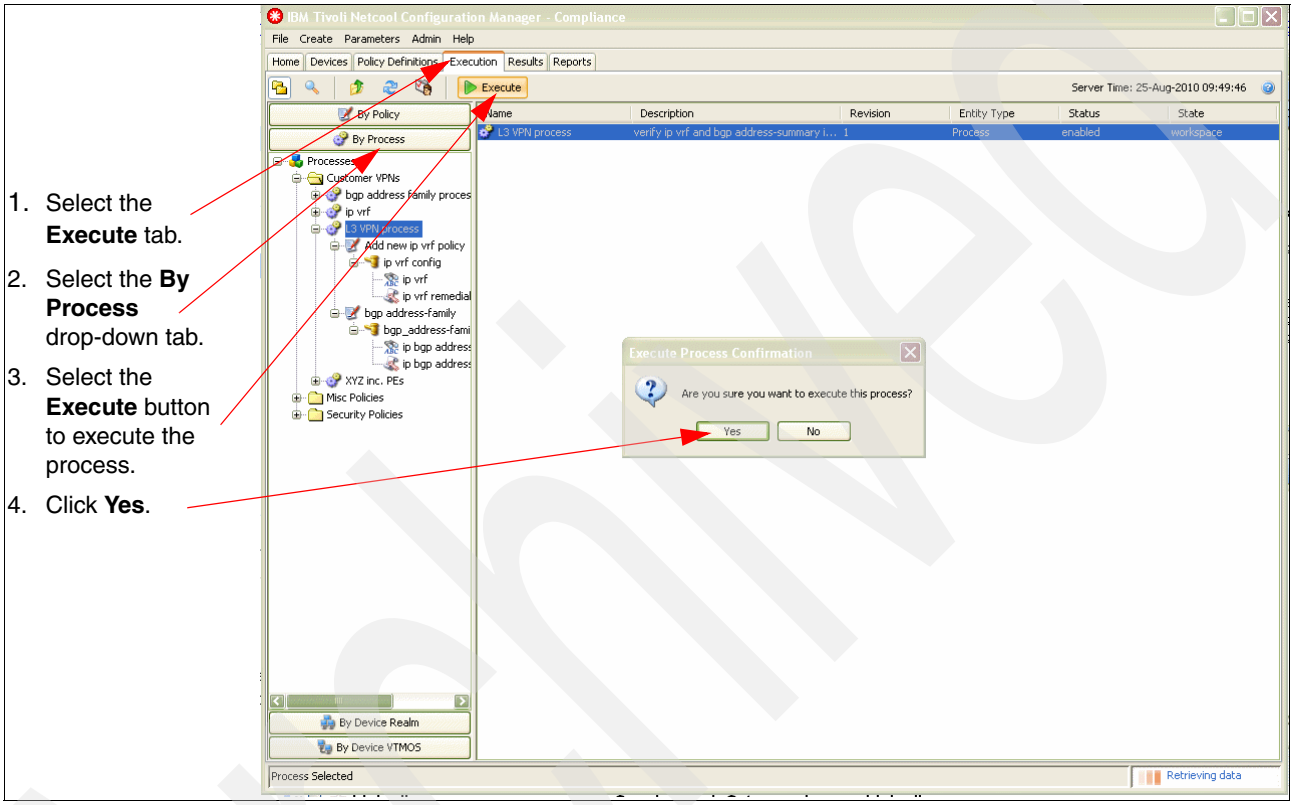



*Figure 6-21 Executing the L3 VPN process*

5. Select the latest Process in the Process Execution Summary pane. The Policy Validation Summary is displayed. In this case, all eight rules failed (four for each policy).

6. Select one of the policies and select the **Details** button to discover why it failed (Figure 6-22).

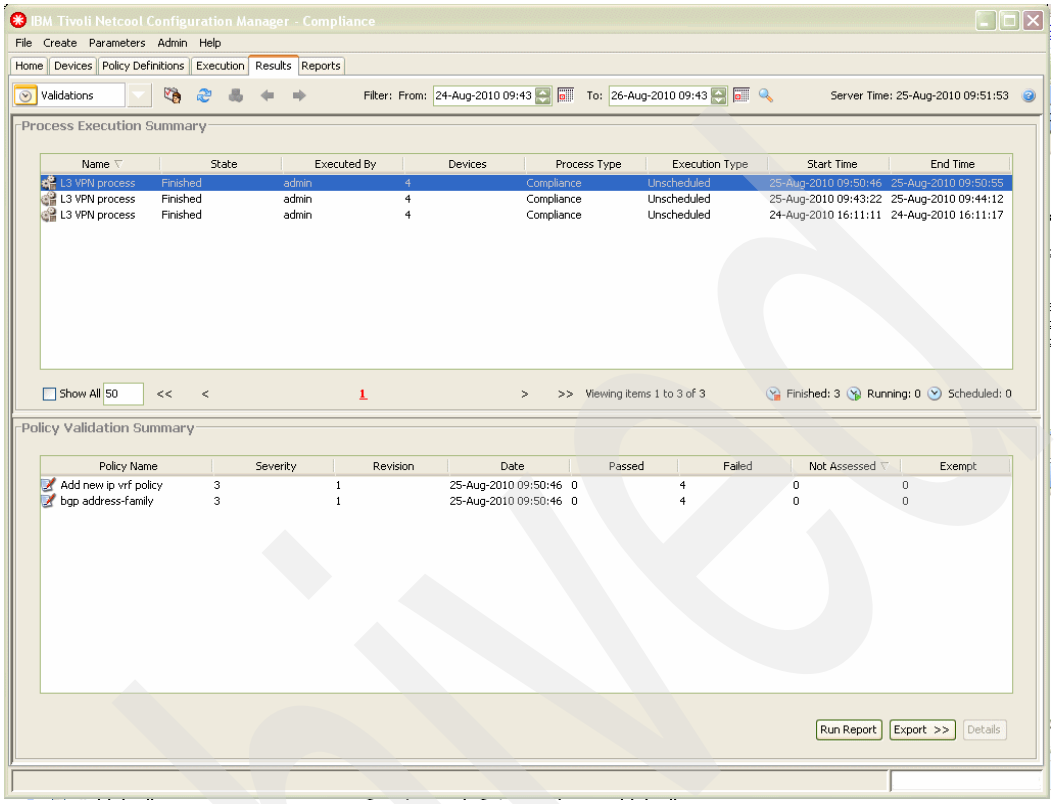



*Figure 6-22 Process Execution and Policy Validation Summary page*

7. This window displays all the devices against which the process was run. Select a device to display details about why it failed. Here you can see that a match for the ip vrf was not found (Figure 6-23).

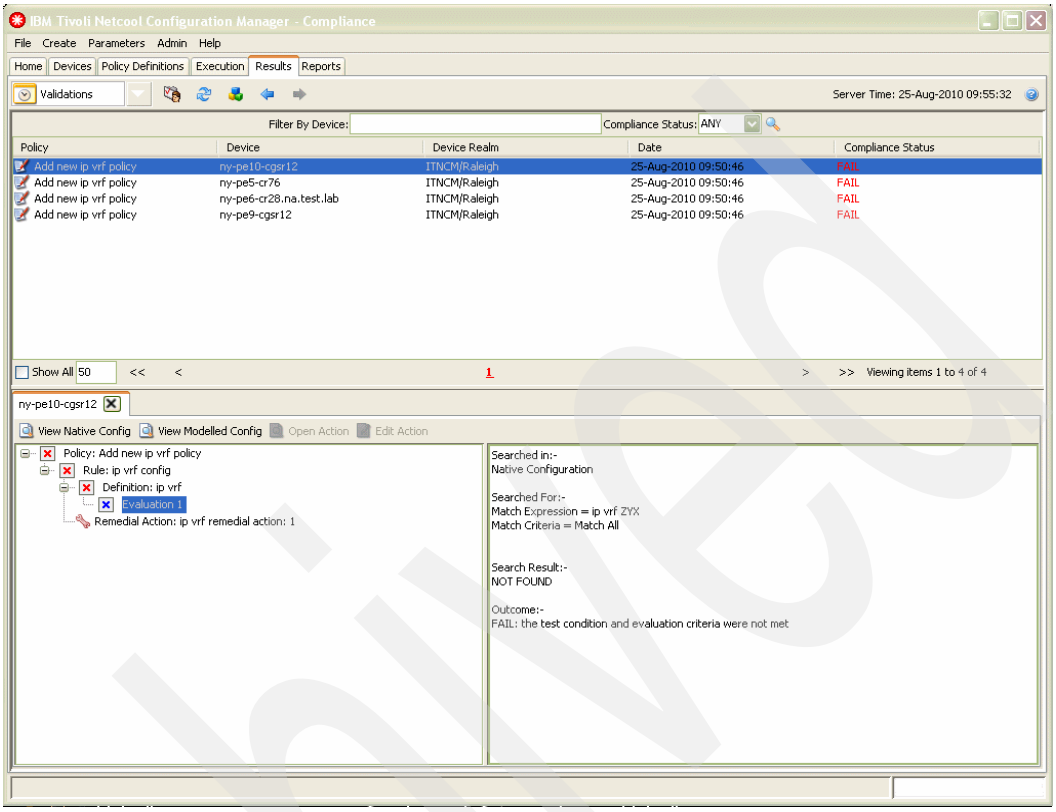



*Figure 6-23 Policy results Search Result: NOT FOUND*

8. Select the **Remedial Action spanner** icon to discover the status of the remedial action. You see that the Remedial Action Status is Pending Approval (Figure 6-24).

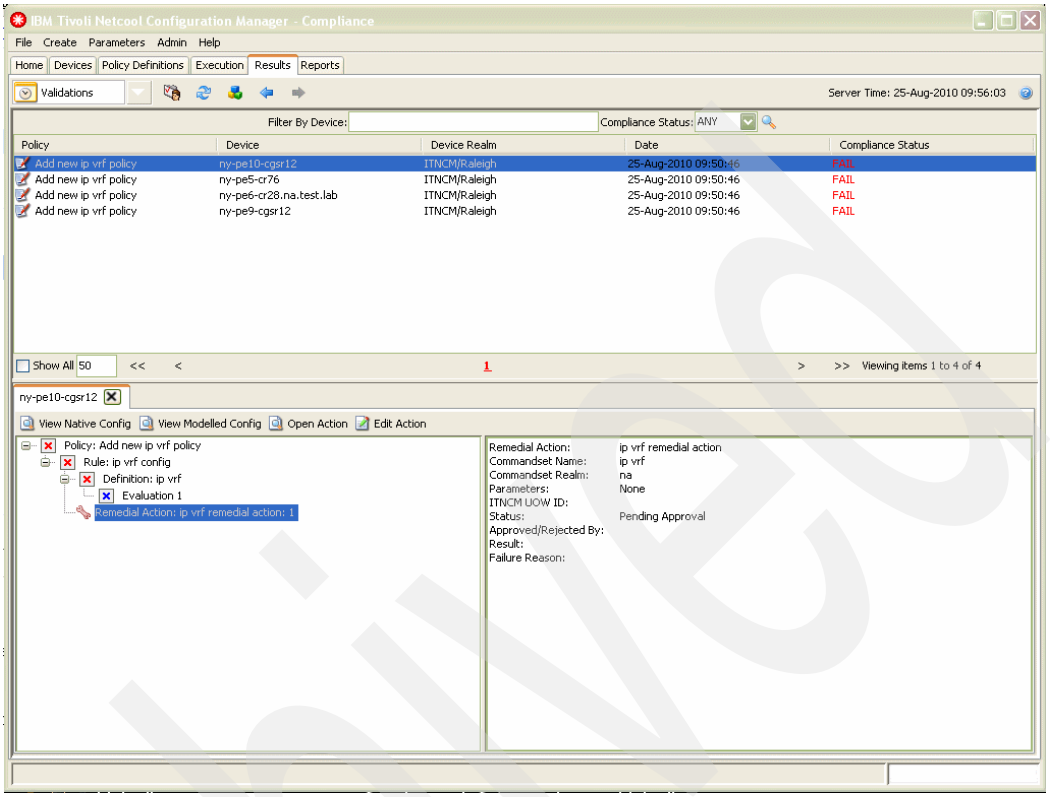



*Figure 6-24 Remedial Action status view Status: Pending Approval*

9. Select the **Remedial Action Queue** drop-down menu to display the remedial actions for each device. Right-click each device to approve each remedial action (Figure 6-25).

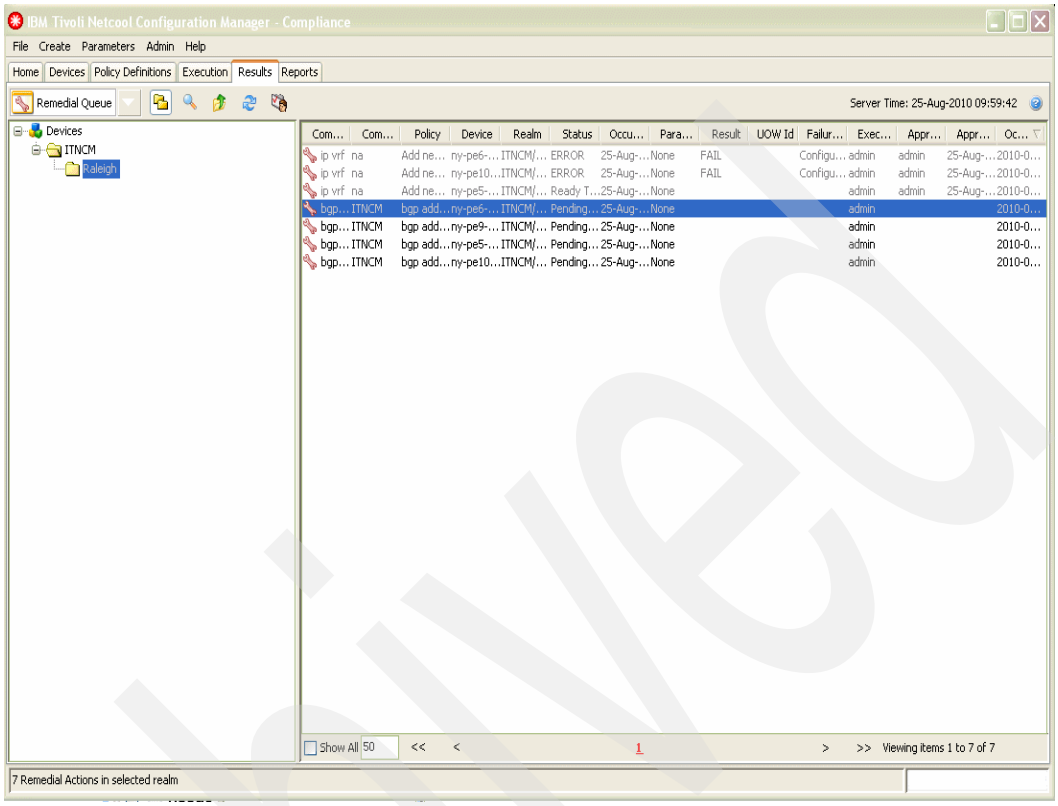



*Figure 6-25 Remedial actions results view*

10. Open Tivoli Netcool Configuration Manager. Identify the UOW that applies to the ip vrf command set so you can confirm that the command set has been applied successfully (Figure 6-26).

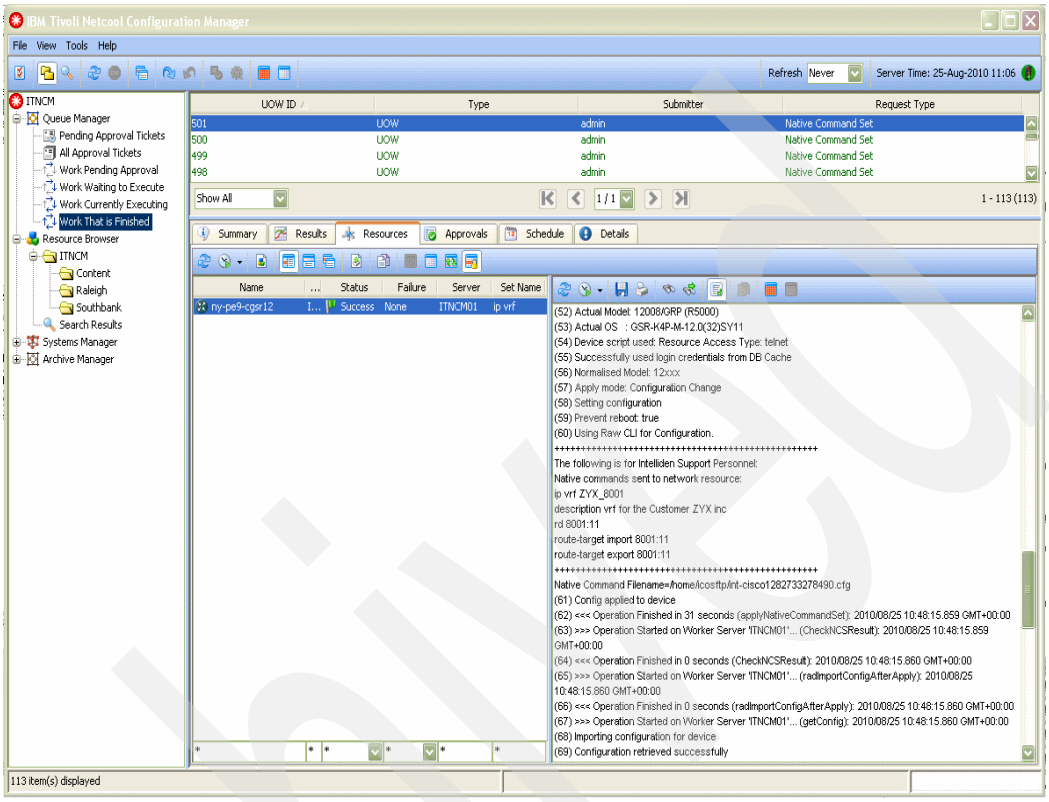



*Figure 6-26 Tivoli Netcool Configuration Manager UOW native command set applied successfully*

11. Re-execute the L3 VPN Process. This time, the ip vrf policy rule is successful (Figure 6-27).

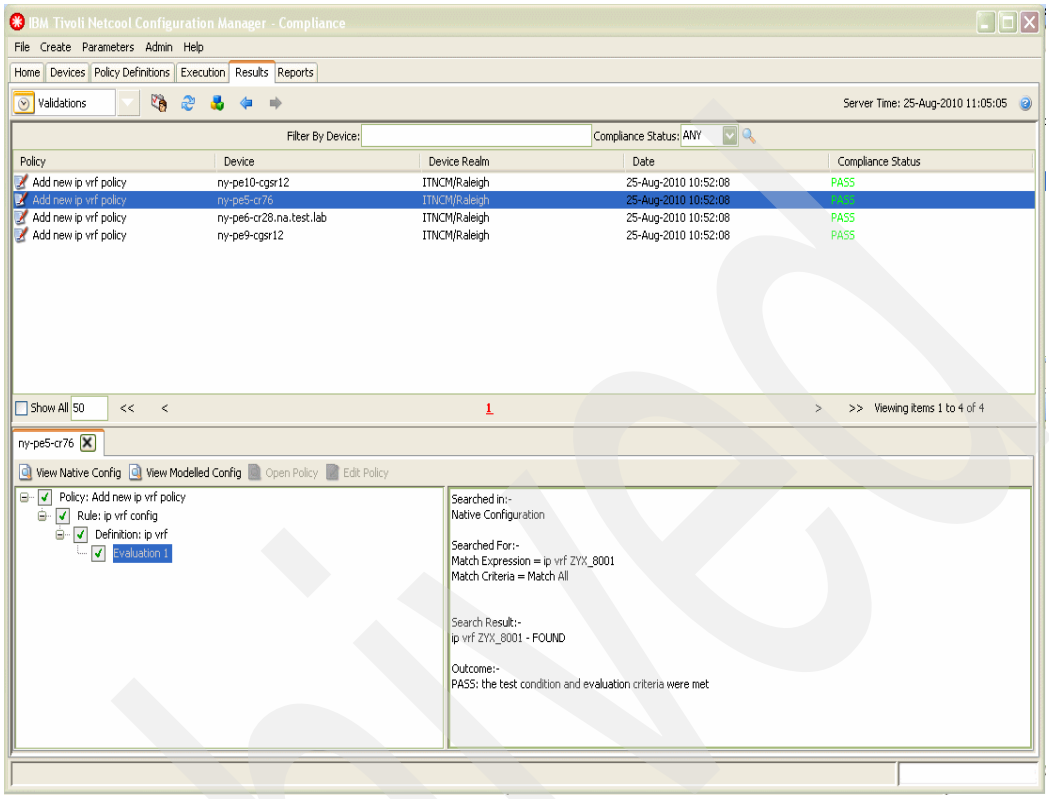



*Figure 6-27 Policy results Search Result: FOUND*

12. There are three steps to create a layer 3 MPLS VPN:

    a. Add a new customer ip vrf.

    b. add a new customer bgp address family.

    c. Apply the ip vrf to the customer facing interface. It is possible to use a policy to apply the ip vrf as well, although it might be simpler to log in to the relevant PE routers and apply the command manually or through Tivoli Netcool Configuration Manager.

13. After performing a full/partial rediscovery through Tivoli Network Manager, you can see the VPN environment configured on the 4x ZXY-facing PE routers (Figure 6-28).

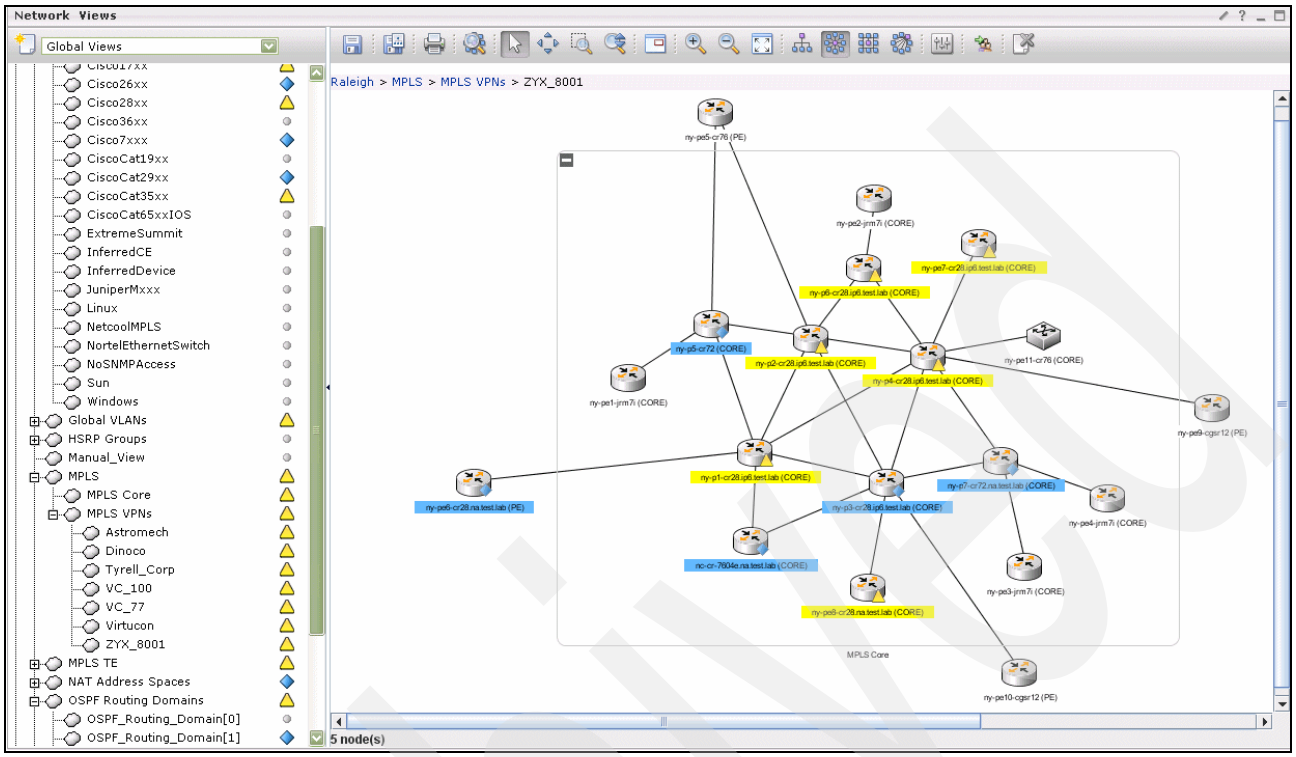



*Figure 6-28 MPLS VPN network view showing the routers participating in the ZYX layer 3 VPN*

# Glossary

**AEL** Active Event List. A list of events in Tivoli Netcool/OMNIbus.

**ATM** Asynchronous transfer mode. A cell-based switching technique that uses asynchronous time division multiplexing. It encodes data into small fixed-sized cells (cell relay) and provides data link layer services that run over OSI Layer 1 physical links.

**domain** Partitioning of devices in Tivoli Network Manager, which is typically based on geography, but can be based on any criteria required. The devices may exist in multiple domains simultaneously.

**command set** Snippets of resource configurations that can be applied across multiple network resources in Tivoli Netcool Configuration Manager.

**native command set** A command set that allows the user to send native (command-line interface (CLI)) commands to one or more network resource at a time in Tivoli Netcool Configuration Manager.

**MPLS** Multiprotocol Label Switching. A mechanism in high-performance telecommunications networks that directs and carries data from one network node to the next. MPLS makes it easy to create “virtual links” between distant nodes. It can encapsulate packets of various network protocols.

**realm** Partitioning of devices within Netcool Configuration Manager, which can be based on geography, device type, or any other criteria required. The devices may not exist in more than one realm.

**UOW** Unit Of Work. Any action to be taken by Tivoli Netcool Configuration Manager.

**UOW ID** Unit Of Work ID. A unique number assigned to each unit of work submitted in Tivoli Netcool Configuration Manager.

**VLAN** Virtual local area network. A group of hosts with a common set of requirements that communicate as though they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch.

**VPN** Virtual private network. A network that uses a public telecommunication infrastructure and its technology, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

**SNMP** Simple Network Management Protocol. A UDP-based network protocol that is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

# Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

## Other publications

These publications are also relevant as further information sources.

### Tivoli Netcool Configuration Manager publications

The following documents are available in the Tivoli Netcool Configuration Manager library:

- *IBM Tivoli Netcool Configuration Manager API Guide*

  Describes the architecture and installation procedures for APIs. Explains the API terminology, and provides structured API examples and workarounds for known issues.

- *IBM Tivoli Netcool Configuration Manager Auto-Discovery Guide*

  Describes the various utilities and procedures needed to maintain and support Auto-Discovery.

- *IBM Tivoli Netcool Configuration Manager - Base Installation and Configuration Guide*

  Describes installation, configuration, and uninstallation procedures for Tivoli Netcool Configuration Manager- Base.

- *IBM Tivoli Netcool Configuration Manager - Base System Admin Guide*

  Describes how to set up user accounts and configure Tivoli Netcool Configuration Manager - Base.

- *IBM Tivoli Netcool Configuration Manager - Base User Guide*

  Provides general usage information for Tivoli Netcool Configuration Manager - Base, including use of Preferences, Searching, Realms, Queue Manager, Resource Browser, and Command Sets.

- *IBM Tivoli Netcool Configuration Manager - Compliance Installation and Upgrade Guide*

  Describes installation, configuration, and uninstallation procedures for Tivoli Netcool Configuration Manager - Compliance.

- *IBM Tivoli Netcool Configuration Manager - Compliance System Admin Guide*

  Provides information about Tivoli Netcool Configuration Manager - Compliance utilities, database and policy exports and imports, housekeeping, and security.

- *IBM Tivoli Netcool Configuration Manager - Compliance User Guide*

  Provides general usage information for Tivoli Netcool Configuration Manager - Compliance, including use of devices, compliance entities, runtime execution, results, security, and reporting.

- *IBM Tivoli Netcool Configuration Manager Drivers Installation and Configuration Guide*

  Describes driver installation, postinstallation, and uninstallation procedures.

- *IBM Tivoli Netcool Configuration Manager IDT Guide*

  Describes the architecture and configuration of the Device Terminal.

- *IBM Tivoli Netcool Configuration Manager Integration Guide*, SC14-7615

  Describes how to integrate Netcool Configuration Manager with Tivoli Netcool/OMNIbus and Tivoli Network Manager.

- *IBM Tivoli Netcool Configuration Manager OOBC Installation Guide*

  Describes how to install and configure the Tivoli Netcool Configuration Manager OOBC.

- *IBM Tivoli Netcool Configuration Manager OS Manager Guide*

  Explains how to create and manage the OS registry, OS specification resources, and OS upgrade requests.

- *IBM Tivoli Netcool Configuration Manager Reporting Manager Guide*

  Describes how to access reports, and explains reporting types and reporting utilities.

- *IBM Tivoli Netcool Configuration Manager Reporting Manager Installation Guide*

  Describes a number of installation procedures, including postinstallation tasks and uninstallation tasks for the Reporting Manager.

- *IBM Tivoli Netcool Configuration Manager Silent Installation Guide*

  Describes procedures for performing a silent installation of Tivoli Netcool Configuration Manager.

All these documents can be accessed at the following address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.tivoli.nam.doc/welcome_itncm.htm

## Tivoli Network Manager IP Edition publications

To use the information in this book effectively, you must have some prerequisite knowledge, which you can obtain from the following Tivoli Network Manager publications:

- *IBM Tivoli Monitoring for Tivoli Network Manager IP Edition User's Guide*, SC27-2770

  Provides information about installing and using IBM Tivoli Monitoring for Tivoli Network Manager IP Edition. This publication is for system administrators who install and use IBM Tivoli Monitoring for Tivoli Network Manager IP Edition to monitor and manage Tivoli Network Manager IP Edition resources.

- *IBM Tivoli Network Manager Getting Started Guide,* GI11-9353

  Describes how to get started using Tivoli Network Manager IP Edition. After you have installed the product, this guide describes how to start the product, make sure it is running correctly, log in, and start setting up the product to discover, view, and poll the network.

- *IBM Tivoli Network Manager IP Edition Administration Guide*, SC27-2761

  Describes administration tasks for Tivoli Network Manager IP Edition, such as how to administer processes, query databases, and start and stop the product. This publication is for administrators who are responsible for the maintenance and availability of Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Discovery Guide*, SC27-2762

  Describes how to use Tivoli Network Manager IP Edition to discover your network. This publication is for administrators who are responsible for configuring and running network discovery.

- *IBM Tivoli Network Manager IP Edition Event Management Guide*, SC27-2763

  Describes how to use Tivoli Network Manager IP Edition to poll network devices, to configure the enrichment of events from network devices, and to manage plug-ins to the Tivoli Netcool/OMNIbus Event Gateway, including configuration of the RCA plug-in for root-cause analysis purposes. This publication is for administrators who are responsible for configuring and running network polling, event enrichment, root-cause analysis, and Event Gateway plug-ins.

- *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*, SC27-2760

  Describes how to install Tivoli Network Manager IP Edition. It also describes necessary and optional post-installation configuration tasks. This publication is for administrators who need to install and set up Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Language Reference*, SC27-2768

  Describes the system languages used by Tivoli Network Manager IP Edition, such as the Stitcher language, and the Object Query Language. This publication is for advanced users who need to customize the operation of Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Management Database Reference*, SC27-2767

  Describes the schemas of the component databases in Tivoli Network Manager IP Edition. This publication is for advanced users who need to query the component databases directly.

- *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide*, GC27-2765

  Describes how to use Tivoli Network Manager IP Edition to troubleshoot network problems identified by the product. This publication is for network operators who are responsible for identifying or resolving network problems.

- *IBM Tivoli Network Manager IP Edition Network Visualization Setup Guide*, SC27-2764

  Describes how to configure the Tivoli Network Manager IP Edition network visualization tools to give your network operators a customized working environment. This publication is for product administrators or team leaders who are responsible for facilitating the work of network operators.

- *IBM Tivoli Network Manager IP Edition Perl API Guide*, SC27-2769

  Describes the Perl modules that allow developers to write custom applications that interact with the Tivoli Network Manager IP Edition. Examples of custom applications include Polling and Discovery Agents. This publication is for advanced Perl developers who need to write such custom applications.

- *IBM Tivoli Network Manager IP Edition Product Overview*, GC27-2759

  Gives an overview of Tivoli Network Manager IP Edition. It describes the product architecture, components and functionality. This publication is for anyone interested in Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Topology Database Reference*, SC27-2766

  Describes the schemas of the database used for storing topology data in Tivoli Network Manager IP Edition. This publication is for advanced users who need to query the topology database directly.

All these documents can be accessed at the following address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.tivoli.nam.doc/welcome_nmip.htm

### Tivoli Netcool/OMNIbus publications

To use the information in this book effectively, you must have some prerequisite knowledge, which you can obtain from the following Tivoli Netcool/OMNIbus publications:

- *IBM Tivoli Netcool/OMNIbus Administration Guide*, SC23-9681

  Describes how to perform administrative tasks using the Tivoli Netcool/OMNIbus Administrator GUI, command-line tools, and process control. The publication also contains descriptions and examples of ObjectServer SQL syntax and automations.

- *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*, SC23-9680

  Includes installation and upgrade procedures for Tivoli Netcool/OMNIbus, and describes how to configure security and component communications. The publication also includes examples of Tivoli Netcool/OMNIbus architectures and describes how to implement them.

- *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide*, SC23-9684

  Contains introductory and reference information about probes and gateways, including probe rules file syntax and gateway commands.

- *IBM Tivoli Netcool/OMNIbus User's Guide*, SC23-9683

  Provides an overview of the desktop tools and describes the operator tasks related to event management using these tools.

- *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide*, SC23-9682

  Describes how to perform administrative and event visualization tasks using the Tivoli Netcool/OMNIbus Web GUI.

All these documents can be accessed at the following address:

`http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.tivoli.nam.doc/welcome_ob.htm`

## Online resources

These websites are also relevant as further information sources:

- IBM Tivoli Netcool Configuration Manager documentation:

  `http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.tivoli.nam.doc/welcome_itncm.htm`

- IBM Tivoli Network Manager IP Edition documentation:

  `http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.tivoli.nam.doc/welcome_nmip.htm`

- IBM Tivoli Netcool/OMNIbus documentation:

  `http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.tivoli.nam.doc/welcome_ob.htm`

## How to get Redbooks

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks publications, at this website:

**ibm.com**/redbooks

# Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

# Index

## U



## V

# Integration Guide for IBM Tivoli Netcool/OMNIbus, IBM Tivoli Network Manager, and IBM Tivoli Netcool Configuration Manager

**Implement an integrated network and configuration management solution**

**Experiment with real-life scenarios and use cases**

**Learn about integration best practices**

This IBM Redbooks publication covers the integration scenarios for IBM Tivoli Network Manager, IBM Tivoli Netcool/OMNIbus, and IBM Tivoli Netcool Configuration Manager. These three products working together provide a comprehensive solution for network and event management, and network configuration management, within the context of service availability and performance management.

Tivoli Network Manager and Tivoli Netcool/OMNIbus are long established products in the IBM portfolio. Tivoli Netcool Configuration Manager (from the Intellident acquisition) is a new product in the portfolio and provides a comprehensive network configuration and change management solution and a policy-based network compliance solution for managing network devices in complex, rapidly changing environments.

This book describes practical examples and use cases where these products work together to address network configuration management and event management requirements.

IT architects and IT specialists working on integrating these Tivoli products in real life environments will benefit from this book.

**INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION**

**BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE**

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

**For more information:**
**ibm.com**/redbooks

SG24-7893-00 ISBN 0738434833