Network Manager IP Edition
Version 3 Release 9

Administration Guide

IBM

Network Manager IP Edition
Version 3 Release 9

Administration Guide

IBM

This edition applies to version 3, modification 9 of IBM Tivoli Network Manager IP Edition (product number 5724-S45) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

IBM Tivoli Network Manager IP Edition provides detailed network discovery, device monitoring, topology visualization, and root cause analysis (RCA) capabilities. Network Manager can be extensively customized and configured to manage different networks. Network Manager also provides extensive reporting features, and integration with other IBM products, such as IBM Tivoli Application Dependency Discovery Manager, IBM Tivoli Business Service Manager and IBM Systems Director.

The *IBM Tivoli Network Manager IP Edition Administration Guide* describes administration tasks for IBM 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 IBM Tivoli Network Manager IP Edition.

Intended audience

This publication is intended for system administrators who are responsible for configuring and administering IBM Tivoli Network Manager IP Edition, and for advanced users who need to query the component databases.

IBM Tivoli Network Manager IP Edition works in conjunction with IBM Tivoli Netcool/OMNIbus; this publication assumes that you understand how IBM Tivoli Netcool/OMNIbus works. For more information on IBM Tivoli Netcool/OMNIbus, see the publications described in "Publications" on page viii.

What this publication contains

This publication contains the following sections:
- Chapter 1, "Starting and stopping Network Manager," on page 1

  Describes how to start and stop IBM Tivoli Network Manager IP Edition and its components.
- Chapter 2, "Administering processes," on page 9

  Describes how to start, stop, check, and troubleshoot processes on UNIX operating systems, and services on Windows operating systems.
- Chapter 3, "Administering logs," on page 25

  Describes how to set up and configure logging for processes.
- Chapter 4, "Administering ports," on page 39

  Describes how to check port usage and define ports.
- Chapter 5, "Administering users," on page 45

  Describes how to set user access to the user interfaces of Network Manager, and to the OQL Service Provider.
- Chapter 6, "Administering system passwords," on page 71

  Describes how to administer the passwords that Network Manager uses for internal processes, and for communicating with the network.
- Chapter 7, "Administering management databases," on page 75

Describes how to use the GUI-based OQL (Object Query Language) workbench, or the OQL Service Provider to access the databases of any Network Manager process.

- Chapter 8, "Administering the NCIM topology database," on page 85

  Describes how to start, stop, and configure the Network and Connectivity Inventory Model (NCIM) database, which holds the topology data, and how to create topology database schemas.

- Chapter 9, "Administering charting," on page 103

  Describes how to build console pages with charts from Tivoli® applications and how to build customized charts.

- Chapter 10, "Administering reports," on page 115

  Describes how to prepare to run reports, how to create and edit reports, and how to configure reporting data sources.

- Chapter 11, "Troubleshooting and support," on page 129

  Describes how to troubleshoot common problems with Network Manager.

- Appendix A, "Command reference," on page 143

  Describes the commands and command-line options that you can use to start Network Manager processes.

- Appendix B, "Web Applications configuration reference," on page 183

  Provides supporting information that you can use to configure Network Manager Web applications.

- Appendix C, "Report reference," on page 197

  Describes the reports available with Network Manager.

- Appendix D, "Entity types," on page 225

  Describes the NCIM topology database entityType table, which contains all the entity types that are available in the NCIM topology database.

- Appendix E, "Scripts," on page 229

  Describes the scripts available in Network Manager

Publications

This section lists publications in the Network Manager library and related documents. The section also describes how to access Tivoli publications online and how to order Tivoli publications.

Your Network Manager library

The following documents are available in the Network Manager library:

- *IBM Tivoli Network Manager IP Edition Release Notes*, GI11-9354-00

  Gives important and late-breaking information about IBM Tivoli Network Manager IP Edition. This publication is for deployers and administrators, and should be read first.

- *IBM Tivoli Network Manager Getting Started Guide*, GI11-9353-00

  Describes how to set up IBM 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, and discover the network. Getting a good network discovery is central to using Network Manager IP Edition successfully. This guide describes how to configure and monitor a first discovery, verify the results of the discovery, configure a production discovery, and how to keep the network topology up to date. Once you have an up-to-date network topology, this guide

describes how to make the network topology available to Network Operators, and how to monitor the network. The essential tasks are covered in this short guide, with references to the more detailed, optional, or advanced tasks and reference material in the rest of the documentation set.

- *IBM Tivoli Network Manager IP Edition Product Overview*, GC27-2759-00

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

- *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*, SC27-2760-00

  Describes how to install IBM 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 IBM Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Administration Guide*, SC27-2761-00

  Describes administration tasks for IBM 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 IBM Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Discovery Guide*, SC27-2762-00

  Describes how to use IBM 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*, SC27-2763-00

  Describes how to use IBM 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 Network Troubleshooting Guide*, GC27-2765-00

  Describes how to use IBM 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*, SC27-2764-00

  Describes how to configure the IBM 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 Management Database Reference*, SC27-2767-00

  Describes the schemas of the component databases in IBM 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 Topology Database Reference*, SC27-2766-00

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

- *IBM Tivoli Network Manager IP Edition Language Reference*, SC27-2768-00

  Describes the system languages used by IBM 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 IBM Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Perl API Guide*, SC27-2769-00

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

- *IBM Tivoli Monitoring for Tivoli Network Manager IP User's Guide*, SC27-2770-00

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

Prerequisite publications

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

- *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 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 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 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 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.

Accessing terminology online

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at the following Web address:

http://www.ibm.com/software/globalization/terminology

Accessing publications online

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center Web site at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File** > **Print** window that allows your PDF reading application to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at the following Web site:

http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss

You can also order by telephone by calling one of these numbers:
- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to the following Web site:

   http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss
2. Select your country from the list and click **Go**. The Welcome to the IBM Publications Center page is displayed for your country.
3. On the left side of the page, click **About this site** to see an information page that includes the telephone number of your local representative.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully.

Accessibility features

The following list includes the major accessibility features in Network Manager:
- The console-based installer supports keyboard-only operation.
- The console-based installer supports screen reader use.
- Network Manager provides the following features suitable for low vision users:
  – All non-text content used in the GUI has associated alternative text.
  – Low-vision users can adjust the system display settings, including high contrast mode, and can control the font sizes using the browser settings.
  – Color is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.
- Network Manager provides the following features suitable for photosensitive epileptic users:

– Web pages do not contain anything that flashes more than two times in any one second period.

The Network Manager Information Center, and its related publications, are accessibility-enabled. The accessibility features of the information center are described in Accessibility and keyboard shortcuts in the information center.

Extra steps to configure Internet Explorer for accessibility

If you are using Internet Explorer as your web browser, you might need to perform extra configuration steps to enable accessibility features.

To enable high contrast mode, complete the following steps:
1. Click **Tools** > **Internet Options** > **Accessibility**.
2. Select all the check boxes in the Formatting section.

If clicking **View** > **Text Size** > **Largest** does not increase the font size, click **Ctrl +** and **Ctrl -**.

IBM® and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education Web site:

http://www.ibm.com/software/tivoli/education

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online
> Go to the IBM Software Support site at http://www.ibm.com/software/ support/probsub.html and follow the instructions.

IBM Support Assistant
> The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install the ISA software, go to http://www.ibm.com/software/support/isa

Conventions used in this publication

This publication uses several conventions for special terms and actions and operating system-dependent commands and paths.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:** and **Operating system considerations:**)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs)
- Words defined in text (example: a nonswitched line is called a *point-to-point* line)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data
- Variables and values you must provide: ... where *myname* represents....

`Monospace`

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

This publication uses environment variables without platform-specific prefixes and suffixes, unless the command applies only to specific platforms. For example, the directory where the Network Manager core components are installed is represented as NCHOME.

When using the Windows command line, preface and suffix environment variables with the percentage sign **%**, and replace each forward slash (*/*) with a backslash (\) in directory paths. For example, on Windows systems, NCHOME is %NCHOME%.

On UNIX systems, preface environment variables with the dollar sign **$**. For example, on UNIX, NCHOME is $NCHOME.

The names of environment variables are not always the same in the Windows and UNIX environments. For example, %TEMP% in Windows environments is equivalent to $TMPDIR in UNIX environments. If you are using the bash shell on

a Windows system, you can use the UNIX conventions.

Chapter 1. Starting and stopping Network Manager

Your options for starting and stopping Network Manager are different depending on how the product has been installed.

Setting environment variables

Before starting any components or working with any configuration files, set the Network Manager environment variables by running the environment script.

The environment script sets the following required environment variables. Other environment variables are set automatically when necessary by Network Manager components.

NCHOME
The Netcool® home location that defaults to `netcool` directory under the installation directory:

- `UNIX` `/opt/IBM/tivoli/netcool`
- `Windows` `C:\IBM\tivoli\netcool`

ITNMHOME and PRECISION_HOME
The Network Manager home location that defaults to `NCHOME/precision` directory under the installation directory:

- `UNIX` `/opt/IBM/tivoli/netcool/precision`
- `Windows` `C:\IBM\tivoli\netcool\precision`

Note: The script also sets PRECISION_HOME. By default, PRECISION_HOME is set to the same location as ITNMHOME, but is used by other parts of the product.

TIPHOME
The Tivoli Integrated Portal home location that defaults to the `tip` directory under the installation directory:

- `UNIX` `/opt/IBM/tivoli/tipv2`
- `Windows` `C:\IBM\tivoli\tipv2`

To set the environment variables, run the appropriate script for your operating system.

- `UNIX` Run the *Installation directory*/netcool/env.sh script.
- `Windows` Run the *Installation directory*\netcool\env.bat batch file.

After you have set the environment variables, start Network Manager and make sure it is running correctly.

Related tasks:

"Starting Network Manager" on page 2
You can start Network Manager, Tivoli Netcool/OMNIbus, and the Tivoli Integrated Portal, together or separately, depending how they are installed.

Starting Network Manager

You can start Network Manager, Tivoli Netcool/OMNIbus, and the Tivoli Integrated Portal, together or separately, depending how they are installed.

Important: Tivoli Netcool/OMNIbus and the topology database must both be started before Network Manager.

Related tasks:

"Setting environment variables" on page 1
Before starting any components or working with any configuration files, set the Network Manager environment variables by running the environment script.

Starting all components on the same server (UNIX only)

If the Tivoli Integrated Portal, Tivoli Netcool/OMNIbus, and Network Manager are installed on the same server, you can start them using the **itnm_start** command.

In the case of Network Manager, the **itnm_start** command starts the master process controller, **ncp_ctrl**, which starts all the Network Manager processes.

Restriction: `Windows` The process control commands are not available on Windows operating systems because the various components are run as services within the Windows environment. On Windows, Network Manager components must be stopped and started from the Windows Services dialog.

To run the **itnm_start** command:

1. If you have not set up the UNIX environment, change to the `$NCHOME/precision/bin` directory.

2. `UNIX` Type the following command: `itnm_start -domain NCOMS`. This command starts all of the Network Manager components that are installed on the server, including the Tivoli Integrated Portal and Tivoli Netcool/OMNIbus, in the example domain NCOMS.

   Note: Informix can only be started by the root user or the informix database administrator user. If you have a non-root Network Manager installation using Informix, and for any reason you need to restart the Informix database, you must log in as the root user and run the following command on Linux and Solaris systems: `/etc/init.d/informix start|stop`; or the following on AIX® systems: `/etc/rc.d/init.d/informix start|stop`. You can also log in as the database administrator and run the **onmode -ky** command to stop the Informix database, and the **oninit** command to start the database.

   For more information, go to the IBM Informix 11.70 Information Center at http://publib.boulder.ibm.com/infocenter/idshelp/v117/index.jsp and search for *Administrator's Reference*.

Related reference:

"itnm_start command-line options" on page 143
Use the **itnm_start** command, with optional advanced arguments, to start Network Manager components.

Starting Network Manager processes using the command console

You can start Network Manager processes by starting the master process controller, **ncp_ctrl**. using the command console.

Before beginning this task, check the following:
- If you want different process dependencies to the defaults, ensure they are configured first.
- Ensure that the UNIX environment is set up.

If you start Network Manager processes using the master process controller, you must start Tivoli Netcool/OMNIbus and the Tivoli Integrated Portal separately.

On Windows, starting the **ncp_ctrl** process using the command console starts it as a process rather than a service.

To start Network Manager using the command console

1. Windows Click **Start** > **Run**.
2. Type the following command:

   ncp_ctrl -domain *DOMAIN* &

   where *DOMAIN* is the domain in which you want to start the core components.

Starting Network Manager processes on Windows

You can start all the processes of Network Manager, not including the Web applications, by starting the master process controller, the **ncp_ctrl** process.

If you start Network Manager processes using the master process controller, you must also start Tivoli Netcool/OMNIbus and the Tivoli Integrated Portal separately.

You can start Network Manager processes in the following ways:
- If you want to start Network Manager processes for the domain that was configured during installation, use the Start menu.
- If you want to start Network Manager processes as Windows services, use the services console.
- If you want to start Network Manager processes as processes, use the command console.

Starting Network Manager processes on Windows using the Start menu

Additional items installed in the Windows Start menu enable you to start Network Manager processes by starting the master process controller, the **ncp_ctrl** process.

These menu items apply only to the domain that was configured during installation.

To start the **ncp_ctrl** process using the Start menu:
1. Click **Start** > **Programs**.
2. To start Network Manager processes as Windows services, click **Start ncp_ctrl -** *initial domain*.
3. To start Network Manager processes as console processes, click **ncp_ctrl (console) -** *initial domain*.

Starting Network Manager processes on Windows using the services console

You can start Network Manager processes as services by starting the master process controller, the `ncp_ctrl` process, as a service.

To start the `ncp_ctrl` process as a Windows service:
1. Click **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Select **ncp_ctrl for domain** *DOMAIN* from the **Services** list.
3. Select **Start** from the **Action** menu.

Starting and stopping the Tivoli Integrated Portal

The Tivoli Integrated Portal Server starts automatically after it has been installed and whenever the computer is started. You can manually stop the server before beginning certain configuration tasks or as needed.

1. In the *tip_home_dir*/profiles/TIPProfile/bin directory, depending on your operating system, enter one of the following commands:

   * **Windows** `stopServer.bat server1`
   * **UNIX** **Linux** `stopServer.sh server1`

   Note: On UNIX and Linux systems, you are prompted to provide an administrator username and password.

2. In the *tip_home_dir*/profiles/TIPProfile/bin directory, depending on your operating system, enter one of the following commands:

   * **Windows** `startServer.bat server1`
   * **UNIX** **Linux** `startServer.sh server1`

Related tasks:

"Setting a trace" on page 132
Enable a trace of the Tivoli Integrated Portal Server when you want to keep a record of activity.

Port assignments

The application server requires a set of sequentially numbered ports.

The sequence of ports is supplied during installation in the response file. The installer checks that the number of required ports (starting with the initial port value) are available before assigning them. If one of the ports in the sequence is already in use, the installer automatically terminates the installation process and you must specify a different range of ports in the response file.

Related tasks:

"Viewing the application server profile" on page 131
Open the application server profile to review the port number assignments and other information.

Starting Tivoli Netcool/OMNIbus

If you have installed Tivoli Netcool/OMNIbus using the Network Manager installation process, you can start the Tivoli Netcool/OMNIbus components by using the `itnm_start` command.

You can also start the Tivoli Netcool/OMNIbus components by using the Tivoli Netcool/OMNIbus commands. For more information about setting up the Tivoli Netcool/OMNIbus components, see the *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Restriction: `Windows` The process control commands are not available on Windows operating systems because the various components are run as services within the Windows environment. On Windows, Network Manager components must be stopped and started from the Windows Services dialog.

To start Tivoli Netcool/OMNIbus using the `itnm_start` command, perform the following steps:

1. On the server where Tivoli Netcool/OMNIbus is installed, change to the `$NCHOME/precision/bin` directory.
2. Enter the following command:

   `UNIX` `itnm_start nco -domain` *domain* This command starts the Tivoli Netcool/OMNIbus components that were configured on this server during installation of Network Manager.

Stopping Network Manager

You can stop Network Manager, Tivoli Netcool/OMNIbus, and the Tivoli Integrated Portal, together or separately, depending how they are installed.

Stopping all components on the same server (UNIX only)

If they are installed on the same server, you can stop the Tivoli Integrated Portal, Tivoli Netcool/OMNIbus, and all Network Manager processes, using the `itnm_stop` command.

On all supported operating systems except Windows, you can use the `itnm_stop` script to stop the following components:

- The Network Manager domain process controller, the `ncp_ctrl` process (which then stops all required processes)
- The Tivoli Integrated Portal
- Tivoli Netcool/OMNIbus

Restriction: The process control commands are not available on Windows operating systems because the various components are run as services within the Windows environment. On Windows, Network Manager components must be stopped from the Windows Services dialog.

To run the `itnm_stop` command, complete the following steps.

1. If you have not already set up the UNIX environment, change to the `$NCHOME/precision/bin` directory.
2. Type the following command: `itnm_stop -domain` *NCOMS*

This command stops all of the Network Manager components that are installed on the server, including the Tivoli Integrated Portal and Tivoli Netcool/OMNIbus, in the example domain NCOMS.

Related reference:

"itnm_stop command-line options" on page 144
Use the `itnm_stop` command, with optional advanced arguments, to stop Network Manager components.

Stopping Network Manager processes using the command console

You can stop all the processes of Network Manager, not including the Tivoli Integrated Portal, by stopping the master process controller, the `ncp_ctrl` process.

If you stop Network Manager processes using the master process controller, you must stop Tivoli Netcool/OMNIbus and the Tivoli Integrated Portal separately.

To stop the `ncp_ctrl` process:

1. Select the console window where the `ncp_ctrl` process is running.
2. Press Ctrl+C.

The `ncp_ctrl` process stops, and also stops all its managed processes.

Stopping Network Manager processes on Windows

You can stop all the processes of Network Manager, not including the Tivoli Integrated Portal, by stopping the master process controller, the `ncp_ctrl` process.

If you stop Network Manager processes using the master process controller, you must stop Tivoli Netcool/OMNIbus and the Tivoli Integrated Portal separately.

You can stop Network Manager processes in the following ways:

- If you want to stop Network Manager processes for the domain that was configured during installation, use the Start menu.
- If you want to stop Network Manager processes running as Windows services, use the services console.
- If you want to start Network Manager processes as processes, use the command console.

Stopping only Network Manager processes using the Start menu

Additional items installed in the Windows Start Menu enable you to stop Network Manager by using the `ncp_ctrl` process.

These menu items only apply to the domain that was set up during installation. You can only stop the `ncp_ctrl` process using the Start menu if the `ncp_ctrl` process was started as a service.

To stop the `ncp_ctrl` process using the Start menu:

1. Click **Start** > **Programs**.
2. To stop the `ncp_ctrl` process, click **Stop ncp_ctrl service - *initial domain***.

Stopping only Network Manager processes from the services console

You can stop Network Manager processes as services by stopping the master process controller, the **ncp_ctrl** process.

To stop the **ncp_ctrl** process, if it is running as a Windows service:
1. Click **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Select **ncp_ctrl for domain** *DOMAIN* from the **Services** list.
3. Select **Stop** from the **Action** menu.

Chapter 2. Administering processes

You can start, stop, and investigate individual Network Manager processes.

About process control

You can check the status of Network Manager processes using the master process controller, the **ncp_ctrl** process.

By default, the **ncp_ctrl** process launches all the Network Manager processes in the appropriate order, in line with configured process dependencies. You can also use the **ncp_ctrl** process to start individual Network Manager processes.

The **ncp_ctrl** process is the only Network Manager component that can start another process. It is also used by other Network Manager processes that need to launch and manage their subprocesses.

The **ncp_ctrl** process is the master process and must be run before all other processes. The **ncp_ctrl** process launches and manages the appropriate processes when their dependencies have been satisfied.

Processes and services on Windows

There are two different ways of running Network Manager processes on Windows: as a process or as a service.

When a process is run as a process from the console, it is run by the current user. If the user has restricted permissions, Network Manager might not function correctly. Use Windows Control Panel to check user permissions.

A service is the Windows equivalent of a background process on UNIX. When Network Manager is installed, the installer creates services for the domain set up as part of the installation process. It is possible to install, or remove, services for additional domains using the ncp_install_services command. You can also start or stop services manually.

The main benefit of running Network Manager processes as services is that an administrator can create domains and services that a standard user can start even if that user does not have adequate permissions to run the application from the command-line.

The main advantage of running processes from the console is that troubleshooting is easier if any problems occur.

When the ncp_ctrl process starts a service, any parameters in the `%NCHOME%/etc/precision/CtrlServices.cfg` take precedence over default service parameters.

Windows services have no STDOUT or STDERR. Therefore they must always log to a file, even if a specific file has not been configured for them in the `CtrlServices.cfg` file. By default, Network Manager processes running as services create log files in `%NCHOME%\log\Precision`, so you must not delete this directory. If you specify a different log file in `CtrlServices.cfg` then that specified file is used

instead.

Network Manager processes

Processes might be referred to in documentation by their executable name (which begins ncp_) or by a descriptive name.

The following table describes the Network Manager processes.

Table 1. Network Manager processes

Executable name	Descriptive name	Description
ncp_brokerd	Really Small Message Broker daemon	Message broker daemon that launches the Really Small Message Broker. Communication between Network Manager core components is managed by Really Small Message Broker. ncp_brokerd starts automatically when any Network Manager process starts.
ncp_class	Active Object Class manager, CLASS	Dynamic library management system responsible for managing the Active Object Classes (AOCs). It is the only component that has direct contact with the AOC definitions, and it distributes these definitions to any component that needs them. You can edit AOCs using a text editor. Stop all Network Manager components before you edit an AOC. **Note:** Ensure that you make a backup of any original AOCs before you edit them. If you overwrite the original copy, the backup copy can be restored.
ncp_config	Network Manager GUI configuration file server, CONFIG	Configuration file server that provides a means for Network Manager GUIs to read from and write to schema files.
ncp_ctrl	Master process controller, CTRL	Master process controller that launches all the Network Manager processes in the appropriate order, in line with configured process dependencies. You can also use the ncp_ctrl process to start individual Network Manager IP Edition processes.
ncp_crypt	Password encryption utility	Utility for manual encryption of passwords.
ncp_disco	Discovery engine	Manages the process of discovering device existence and interconnectivity. The Helper Server process, ncp_d_helpserv, is a subprocess of the discovery engine, ncp_disco. Other subprocesses include the following finder processes, which are responsible for determining device existence: • ncp_df_ping (Ping finder): Makes a simple ICMP echo request for broadcast or multicast addresses, individual IP addresses, or all devices on a subnet • ncp_df_file (File finder): Parses a file, such as /etc/hosts, in order to find devices on the network • ncp_df_collector (Collector finder): Retrieves a list of devices managed by Element Management Systems (EMSs) on the network

Table 1. Network Manager processes (continued)

Executable name	Descriptive name	Description
ncp_dla	Discovery Library Adapter	Collects data on network resources and relationships from Network Manager for import into the Tivoli Change and Configuration Management Database (CCMDB).
ncp_d_helpserv	Helper Server	Helpers retrieve information from the network during a discovery. The Helper Server manages the helpers and stores information retrieved from the network. Discovery agents retrieve their information through the Helper Server to reduce the load on the network. The Helper Server can service the requests directly with cached data or pass on the request to the appropriate helper. The Helper Server manages the following helpers: • ncp_dh_arp (ARP helper): Performs IP address to MAC address resolution • ncp_dh_dns (DNS helper): Performs IP address to device name resolution • ncp_dh_ping (Ping helper): Either pings each device in a subnet, an individual IP address or a broadcast or multicast address • ncp_dh_snmp (SNMP helper): Returns results of an SNMP request such as Get, GetNext and GetBulk • ncp_dh_telnet (Telnet helper): Returns results of a Telnet operation into a specified device • ncp_dh_xmlrpc (Collector helper): Provides communications facilities with EMS collectors using the XML-RPC interface
ncp_g_event	Event Gateway	Provides a bidirectional interface between Network Manager and Tivoli Netcool/OMNIbus. The Event Gateway also forwards events to plug-ins that subscribe to specific types of event and perform further action or further event enrichment based on event data.
ncp_install_services	Domain administration utility for Network Manager on Windows	Use the Windows domain administration utility to install, or remove, services for additional domains when Network Manager is installed on a Windows system. You can also use this utility to start or stop services manually. A service is the Windows equivalent of a background process on UNIX. When Network Manager is installed on Windows, the installer creates services for the domain set up as part of the installation process.
ncp_mib	MIB update administration utility	Use the MIB update administration utility to update your MIB data for use within the SNMP MIB Browser.
ncp_model	Topology manager	Stores the topology data following a discovery and sends the topology data to the topology database (NCIM), where it can be queried using SQL. The topology visualization GUIs retrieve topology data from NCIM to display to network operators.

Table 1. Network Manager processes (continued)

Executable name	Descriptive name	Description
nco_p_ncpmonitor	Probe for Tivoli Netcool/OMNIbus	Enables events generated by the Network Manager polling to be sent to the Tivoli Netcool/OMNIbus ObjectServer. The nco_p_ncpmonitor process converts these events into ObjectServer format.
ncp_poller	Polling engine	Controls network device polling.
ncp_oql	OQL Service Provider	Command-line interface that enables administrators to query and update data in Network Manager databases.
ncp_trapmux	SNMP trap multiplexer	In most networks, traps arrive on a single default port. The SNMP trap multiplexer resolves this problem by listening to a single port and forwarding all the traps it receives to a set of host/socket pairs.
ncp_virtualdomain	Virtual Domain	Virtual Domain is used when running Network Manager with failover. Any connection to this virtual domain is routed to the Network Manager server that is running as the primary server in the failover architecture.
ncp_webtool	Webtools	Provides for the hosting of WebTools on the backend server so that they can be accessed in distributed environments where Topoviz is running on a different server to the Network Manager backend processes and there is a firewall between the two.

Managed and unmanaged processes

The ncp_ctrl process starts two types of process: managed and unmanaged processes.

- *Managed processes* are processes for which the ncp_ctrl process is fully responsible. The ncp_ctrl process not only starts and stops these processes, but also keeps track of their activities and restarts them if they die.

- *Unmanaged processes* are processes that the ncp_ctrl process is only responsible for starting or stopping. The ncp_ctrl process is not responsible for tracking unmanaged processes and makes no attempt to restart these processes if they die.

Although it is entirely up to you to determine which processes are managed and which are unmanaged, it is best practice to ensure that the core Network Manager processes (that is, those responsible for discovery, monitoring, root cause analysis, and topology data) are handled as managed processes. Only processes such as scripts should be launched as unmanaged processes.

About Network Manager domains

A domain is a set of Network Manager processes that work together in a single group. Each domain has a unique name.

Running multiple domains enables you to discover, visualize and monitor multiple network topologies. Multiple Network Manager processes can run independently of each other on the same server if they belong to different domains.

Dividing your network into domains allows you to discover your network in sections. You might want to do this for reasons of scalability: your network might

be too big to be discovered in one piece. Alternatively, you might want to break the network into geographical regions, and make each region correspond to a domain.

By default, Network Manager runs on a single domain.

The domain in which a component runs is determined by the command-line argument -domain, which is compulsory for all components, with the exception of the `ncp_mib` process, which manages the importing of MIBs across all domains using the same Netcool Common Inventory Model (NCIM) database.

Configuration files that are specific to a particular domain have the domain name appended to the file name. For example, the configuration file for the ncp_ctrl process running in domain NCOMS would be `CtrlServicesNCOMS.cfg`

Restriction: Only alphanumeric characters and the underscore (_) character may be used for domain names. Any other characters, for example the hyphen (-) are forbidden.
.

Domain-specific configuration files

If you are running processes in more than one domain, configuration changes should be saved in configuration files with your domain name appended to the filename.

For example, the configuration file for the `ncp_ctrl` process in the domain NCOMS is called `CtrlServices.NCOMS.cfg`.

Although in practice there are some files that you are unlikely to need to alter, in principle all of the following types of files can be made domain-specific:
- Configuration files, that is, all files ending in `.cfg`
- Discovery agent files, that is, all files ending in `.agnt`
- Active Object Class files, that is, all files ending in `.aoc`
- Text-based stitcher files, that is, all files in a `stitchers` directory ending in `.stch`

In the Network Manager documentation, these files are referred to using their default names unless noted otherwise.

Checking process status

You can check the status of IBM Tivoli Netcool/OMNIbus, the Tivoli Integrated Portal, and individual Network Manager processes.

Checking process status by running the itnm_status command

On UNIX operating systems, you can check the status of IBM Tivoli Netcool/OMNIbus, the Tivoli Integrated Portal, and Network Manager by using the `itnm_status` command." steps.

To check the status of all Network Manager components on the current server:
1. Change to the `$NCHOME/precision/bin` directory.
2. Type the following command: `itnm_status`

This command displays the status of all of the Network Manager components that are installed on the server.

Monitoring process status messages

You can view status messages from Network Manager to understand the health and status of the product.

The Network Manager processes send messages to IBM Tivoli Netcool/OMNIbus when they start and stop. You can view these messages to see which processes have started and stopped, and to see failover status.

To view process status messages, complete the following tasks.
1. Add an Active Event List (AEL) portlet to a page.
2. Apply a filter to the AEL so that only events with an `Alert Group` of `ITNM Status` are displayed.

Checking process status by querying ncp_ctrl databases

On all operating systems, you can check the status of individual Network Manager processes by querying the databases of the **ncp_ctrl** process.

The **ncp_ctrl** process must also be running for the domain that you want to interrogate.

Identifying which Network Manager processes are running

To identify the processes that were started by the **ncp_ctrl** process and that are currently running, issue a query to the services.inTray database table.

To identify which processes are running:
1. Log in to the Ctrl service using either the OQL Service Provider or the Management Database Access page:
   - Start the OQL Service Provider by typing a command similar to the following:

     ```
     ncp_oql -domain NCOMS -service Ctrl
     ```

     where *NCOMS* is the domain name. If authentication has been configured for the OQL Service Provider, enter your username and password.
   - Log in to the Management Database Access page and select the Ctrl service.
2. Issue the following command:

   ```
   select serviceName, binaryName, domainName, processId
   from services.inTray
   where serviceState = 4 ;
   go
   ```

The following example output shows that four processes were started by the **ncp_ctrl** process and are currently running:

```
...........
{
              serviceName='ncp_store';
              binaryName='ncp_store';
              domainName='NCOMS';
              processId=7220;
}
{
              serviceName='ncp_model';
              binaryName='ncp_model';
              domainName='NCOMS';
```

```
                    processId=7222;
}
{

                    serviceName='ncp_disco';
                    binaryName='ncp_disco';
                    domainName='NCOMS';
                    processId=7223;
}
{

                    serviceName='ncp_poller(default)';
                    binaryName='ncp_poller';
                    domainName='NCOMS';
                    processId=7223;
}
( 4 record(s) : Transaction complete )
```

Identifying which processes are started automatically

To identify which processes are started automatically by the **ncp_ctrl** process, issue a query to the services.inTray database table.

To identify which processes are started automatically:

1. Log in to the Ctrl service using either the OQL Service Provider or the Management Database Access page:

   • Start the OQL Service Provider by typing a command similar to the following:

   ```
   ncp_oql -domain NCOMS -service Ctrl -username admin
   ```

   where *NCOMS* and *admin* are your domain name and username.

   • Log in to the Management Database Access page and select the Ctrl service.

2. Issue the following command:

   ```
   select * from services.inTray;
   go
   ```

The following example output shows processes configured to be started by the **ncp_ctrl** process:

```
{
        serviceName='ncp_disco';
        binaryName='ncp_disco';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin';
        domainName='NCOMS';
        argList=['-domain','$PRECISION_DOMAIN','-discoOnStartup',
                '0','-latency','100000','-debug','0','-messagelevel',
                'warn'];
        dependsOn=['ncp_d_helpserv','ncp_model'];
        retryCount=5;
        serviceId=4;
        traceLevel=0;
        logLevel='warn';
        serviceKey='ncp_disco_NCOMS';
        serviceState=4;
        interval=10;
        processId=2622;
}
.....
.....
{
        serviceName='ncp_model';
        binaryName='ncp_model';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin';
        domainName='NCOMS';
        argList=['-domain','$PRECISION_DOMAIN','-latency','100000',
                '-debug','0','-messagelevel','warn'];
```

```
        dependsOn=['ncp_config','ncp_store','ncp_class'];
        retryCount=5;
        serviceId=3;
        traceLevel=0;
        logLevel='warn';
        serviceKey='ncp_model_NCOMS';
        serviceState=4;
        interval=10;
        processId=2542;
}
```

Identifying unmanaged processes

To identify which processes are started but not managed by the **ncp_ctrl** process, issue a query to the services.unManaged database.

Insertions into the services.unManaged table are made by other Network Manager components in order to start and stop their subprocesses; for example, the **ncp_disco** process uses the **ncp_ctrl** process to start the finders.

To identify unmanaged processes:

1. Log in to the Ctrl service using either the OQL Service Provider or the OQL Workbench:
   - Start the OQL Service Provider by typing a command similar to the following:

     ncp_oql -domain *NCOMS* -service Ctrl -username *admin*

     where *NCOMS* and *admin* are your domain name and username.
   - Log in to the OQL Workbench and select the Ctrl service.

2. Issue the following command:

   select * from services.unManaged;
   go

The following example output shows that two unmanaged processes have been started by the **ncp_ctrl** process:

```
{
        serviceName='ncp_df_ping';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','LNX39024','-server','ncp_disco.2622'];
        binaryName='ncp_df_ping';
        serviceId=14;
        logLevel='warn';
        traceLevel=0;
        domainName='NCOMS';
        processId=2695;
}
{
        serviceName='ncp_dh_snmp';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','LNX39024'];
        binaryName='ncp_dh_snmp';
        serviceId=19;
        logLevel='warn';
        traceLevel=0;
        domainName='NCOMS';
        processId=4254;
}
( 2 record(s) : Transaction complete )
```

Managing process dependencies

A process cannot start until the processes on which it depends have started. Incorrectly-configured process dependencies can result in problems starting processes.

Listing process dependencies

You can issue a query to the services.inTray database to identify which processes have dependencies on other processes.

To identify process dependencies:

1. Log into the process control databases.
2. Issue the following command:

```
select serviceName, dependsOn
from services.inTray;
go
```

3. The following example output shows that **ncp_class** and **ncp_store** have no dependencies, and that **ncp_model** is dependent on **ncp_class** and **ncp_store**:

```
.....
{
                serviceName='ncp_class';
                dependsOn=[];
}
{
                serviceName='ncp_store';
                dependsOn=[];
}
.....
.....
{
                serviceName='ncp_model';
                dependsOn=['ncp_class', 'ncp_store'];
}
( 4record(s) : Transaction complete )
```

Identifying dependencies for a particular process

To identify the dependencies for a particular process, issue a query to the services.inTray database.

To identify process dependencies for a particular process:

1. Log into the process control databases.
2. Issue the following command:

```
select serviceName, dependsOn
from services.inTray
where serviceName='SERVICE';
go
```

Where *PROCESS* is the name of the process for which you want to query the dependencies; for example, ncp_disco.

The following example output shows that **ncp_model** is dependent on **ncp_class** and **ncp_store:**

```
{
                serviceName='ncp_model';
                dependsOn=['ncp_class', 'ncp_store'];
}
( 1record(s) : Transaction complete )
```

Configuring process dependencies

To configure process dependencies, edit the $NCHOME/etc/precision/
CtrlServices.cfg configuration file.

The process dependencies defined in the CtrlServices.cfg configuration file
specify the order in which the **ncp_ctrl** process starts the processes.

To configure process dependencies:
1. Back up and edit he CtrlServices*DOMAIN*.cfg configuration file for your
   domain, where *DOMAIN* is the name of your domain.
2. Locate the entry for the process whose dependencies you want to configure by
   looking for the following line in the file:

   serviceName='*process_name*';

   where *process_name* is the name of the process.
3. Change the dependencies of the process by adding or removing process names
   to the following line, directly underneath the previous line:

   dependsOn=['*process_name*', '*process_name2*'];
4. Save the **CtrlServices.cfg** configuration file.
5. Restart the master process controller, the **ncp_ctrl** process, for your changes to
   take effect.

List of process dependencies

The Network Manager processes must be started in the correct order.

The process dependencies are shown in the following table:

Table 2. Dependencies of the Network Manager processes

Process	Dependencies
ncp_class	No dependency
ncp_config	No dependency
ncp_ctrl	No dependency
ncp_disco	**ncp_d_helpserv**, **ncp_model**
ncp_d_helpserv	No dependency
ncp_g_event	**ncp_model**, Tivoli Netcool/OMNIbus ObjectServer
ncp_model	**ncp_config**, **ncp_class**, **ncp_store**
ncp_poller	**ncp_g_event**, **nco_p_ncpmonitor**
ncp_oql	The component you want to interrogate
nco_p_ncpmonitor	Netcool/OMNIbus ObjectServer
ncp_trapmux	No dependency
ncp_store	No dependency
ncp_virtualdomain	**ncp_g_event**, **ncp_poller**
ncp_webtool	No dependency

Process control configuration files

Use the following configuration files to configure the ncp_ctrl process.

- $NCHOME/etc/precision/CtrlSchema.cfg contains the definitions for the databases of the ncp_ctrl process. You should not need to edit this file.
- $NCHOME/etc/precision/CtrlServices.cfg contains any necessary inserts into the databases of the ncp_ctrl process to tell the ncp_ctrl process which processes to start and in what order.

In order to configure the ncp_ctrl process to launch and manage the appropriate processes, you must append OQL inserts to the configuration file for the ncp_ctrl process, $NCHOME/etc/precision/CtrlServices.cfg.

Starting and stopping processes

You can start and stop individual processes manually or automatically.

Configuring which processes are started automatically

You can configure which processes are started automatically by the **ncp_ctrl** process by editing the $NCHOME/etc/precision/CtrlServices.cfg file.

Your changes will persist if the **ncp_ctrl** process is stopped and restarted.

You may only want to use a subset of the Network Manager functionality. For example, you might want to use Network Manager to discover your network and visualize the topology only. In this case you can configure the **ncp_ctrl** process so that it does not start the processes that monitor the network and perform root-cause analysis on network events.

To configure which processes are started automatically, perform the following steps:

1. Back up your $NCHOME/etc/precision/CtrlServices.cfg file.
2. Save a copy of the CtrlServices.cfg file with your domain name appended to the filename, for example, CtrlServices.MASTER.cfg.
3. Edit the CtrlServices.MASTER.cfg file. For example, if you want to discover your network and visualize the topology only, you must delete or comment out the entries for the Event Gateway, **ncp_poller**, and **nco_p_ncpmonitor** processes from the CtrlServices.MASTER.cfg file.
4. Start the **ncp_ctrl** process in the domain MASTER.

The **ncp_ctrl** process now starts the limited set of processes in the domain MASTER in the order you specified.

Sample: Starting Network Manager with discovery and visualization functionality only

This sample shows you how to configure the master process controller to start only the processes that perform and support network discovery and visualization.

To ensure that monitoring and event management processes are not started on the current server, you must remove insert statements related to the ncp_g_event, ncp_poller and ncp_virtualdomain processes from the CtrlServices.DOMAIN.cfg file.

Note: The probe for Tivoli Netcool/OMNIbus, nco_p_ncpmonitor, should be left in the `CtrlServices.DOMAIN.cfg` file, as it will still be used to pass Network Manager status events to the ObjectServer.

For the ncp_g_event process, the lines to be removed look similar to the following lines:

```
insert into services.inTray
(
    serviceName,
    binaryName,
    servicePath,
    domainName,
    argList,
    dependsOn,
    retryCount
)
values
(
    "ncp_g_event",
    "ncp_g_event",
    "$NCHOME/preecision/platform/$PLATFORM/bin",
    "DOMAIN",
    [ "-domain" , "DOMAIN", "-latency", "60000" , "-debug", "0", "-messagelevel",
 "warn" ],
    [ "ncp_model" ],
    5
);
```

Starting managed processes

You can start a process as a managed process by making an OQL insert into the `services.inTray` table.

Your changes will be lost if the **ncp_ctrl** process is stopped and restarted.

To start a managed process:
1. Ensure that the **ncp_ctrl** process is running.
2. Log into the process control databases.
3. Issue a command similar to the following:
   ```
   insert into services.inTray
   (
           serviceName,
           binaryName,
           servicePath,
           domainName,
           hostName,
           argList,
           dependsOn,
           retryCount,
           logFile
   )
   values
   (
           "ncp_disco",
           "ncp_disco",
           "NCHOME/precision/platform/$PLATFORM/bin",
           "NCOMS",
           "Felix",
           [ "-domain", "NCOMS", "-debug", "4" ],
           [ "ncp_d_helpserv" ],
           3,
           "$NCHOME/log/precision/disco.log"
   );
   ```

4. The above insert starts **ncp_disco** as a managed process in the NCOMS domain on the host Felix with the arguments "**-domain** NCOMS" and "**-debug** 4", with a dependency on the Helper Server. The **ncp_disco** process will be restarted three times if it stops.

Starting unmanaged processes

You can start a process as an unmanaged process by making an OQL insert into the services.inTray table.

Your changes will be lost if the **ncp_ctrl** process is stopped and restarted.

To start an unmanaged process:
1. Ensure that the **ncp_ctrl** process is running.
2. Log into the process control databases.
3. Issue a command similar to the following:

```
insert into services.unmanaged
(
        serviceName, servicePath, argList
)
values
(
        "user_script",
        "/opt/netcool/precision/solaris2/scripts/",
        [ ]
);
```

The above insert starts a script called user_script, located in the $NCHOME/precision/scripts directory.

Stopping processes

You can stop a managed process that is running by deleting the record in the services.inTray table.

If you delete the record from the services.inTray table, the process is not restarted until the **ncp_ctrl** process is restarted.

To stop a managed process:
1. Ensure that the **ncp_ctrl** process is running.
2. Log into the process control databases.
3. Issue a command similar to the following:

```
delete from services.inTray
where serviceName = 'ncp_model' ;
go
```

The previous command stops the **ncp_model** process.

Managing Network Manager services on Windows

You can manage Network Manager processes in the same way on Windows as you can on UNIX operating systems. Additionally, on Windows you have the option of running processes as services.

Starting a service

You can start a process as a service on Windows using the Services console.

To start a Network Manager process running as a Windows service:
1. Click **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Select the process that you want to start from the **Services** list.
3. Select **Start** from the **Action** menu.

Stopping a service

You can stop a process as a service on Windows using the Services console.

To stop a Network Manager process running as a Windows service:
1. Click **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Select the process that you want to stop from the **Services** list.
3. Select **Stop** from the **Action** menu.

Configuring Network Manager to start automatically

You can configure Network Manager processes to start automatically each time the server is restarted by configuring the `ncp_ctrl` process to start automatically.

To configure the `ncp_ctrl` process to start automatically:
1. Click **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Select **ncp_ctrl for domain** *DOMAIN* from the Services list.
3. Select **Properties** from the **Action** menu.
4. Select the **General** tab.
5. Change the startup type to **Automatic**.
6. Leave all other Network Manager services as manual startups.

The `ncp_ctrl` process will start these Network Manager services when they are required.

Removing services

Windows

You can remove all services for a specified network domain.

To remove all services for a domain:
1. Stop the `ncp_ctrl` process. This prevents services being restarted.
2. Stop all services.
3. Run the following command:
   ```
   ncp_install_services -domain DOMAIN -remove
   ```

   Where *DOMAIN* is the domain for which you want to remove the services.

Changing the user that runs all Network Manager services

You can install all services for a domain to run as a specific user.

To install all services to run as a specific user:
1. From the command line, type the following command:

   `ncp_install_services -domain MASTER -username "IBM\admin"`
2. Type in the password for the admin user.

Services in the domain *MASTER* now run as user admin as opposed to the default LocalSystem.

Running services as a specific user

Windows

You can define the user that a specific service runs as.

When a process is run as a service, it is run by the user configured to run that service, regardless of which user starts it. The default user for services is LocalSystem; in Task Manager, LocalSystem is displayed as SYSTEM.

To define the user that a specific service runs as:
1. Click **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Select the service that you want to configure.
3. Click **ActionProperties**.
4. Click **Log On**.
5. Select **This account**.
6. Enter the details of the user account.

Configuration file differences between Windows and UNIX

You can copy Network Manager configuration files between Windows and UNIX.

The files might lose some formatting when viewed in a text editor due to the different formats for line breaks in text files on Windows and UNIX systems. However, Network Manager is able to read them. When UNIX configuration files are used on Windows, Notepad will not show any line breaks. Wordpad will display UNIX text files correctly, so it is the best application to view configuration files copied from UNIX operating systems. When a Windows configuration file is used on UNIX, vi will show ^M at the end of each line. This is a cosmetic issue and does not affect usability of the file by Network Manager.

Running processes remotely

If you want Network Manager processes on one server to be managed by `ncp_ctrl` on another server, you must configure both instances of `ncp_ctrl`.

To set up processes to be run remotely, complete the following steps.
1. Install Network Manager on both servers.
2. Configure Really Small Message Broker to allow communication between the master server and slave server.
3. On the master server, configure the `CtrlServices.DOMAIN.cfg` file.
   a. Back up and edit the `CtrlServices.DOMAIN.cfg` file.

b. For each process that you want to run on the remote server, set the `hostName` parameter to the host name of the remote server. Make sure the host name is the name as defined on the remote server.

The following example configures the **ncp_store** process to run on the remote server called example.com in domain TARA.

```
insert into services.inTray
(
    serviceName,
    binaryName,
    servicePath,
    domainName,
    hostName,
    argList,
    retryCount
)
values
(
    "ncp_store",
    "ncp_store",
    "/opt/IBM/Tivoli/netcool/precision/platform/linux2x86/bin",
    "TARA",
    "example.com",
    [ "-domain" , "<DOMAIN>" , "-latency" , "100000", "-debug", "0" ],
    5
);
```

4. Start the **ncp_ctrl** process on the remote server in slave mode using the command line argument `-slave`. The following example starts the ncp_ctrl process in slave mode in domain TARA.

```
ncp_ctrl -domain TARA -slave
```

5. Start the **ncp_ctrl** process on the local server in master mode using the normal command line options. The following example starts the ncp_ctrl process in master mode domain TARA.

```
ncp_ctrl -domain TARA
```

The processes that you configured to be run on the slave server are started, and controlled by the **ncp_ctrl** process on the master server. The **ncp_ctrl** process on the master server also starts and controls any processes that it is configured to manage on the master server.

Chapter 3. Administering logs

Network Manager provides logging capabilities for its GUI components and back-end processes. You can set up logging for Network Manager to produce log or trace files that can be used for troubleshooting purposes.

Related tasks:

"Troubleshooting Network Manager" on page 129
Consult these troubleshooting notes to help determine the cause of the problem and what to do about it.

Setting up logging for GUI

You can set up Network Manager to create log or trace files that can be used for troubleshooting GUI issues. You can also adjust the logging level for each component, and the maximum size and number of the log files the systems saves.

GUI component log file overview

Log messages produced by Network Manager GUI components are written to log and trace files.

- Log files provide log information in a standard format that is compatible with IBM's Common Base Event (CBE) format. Messages in CBE format can be used in the IBM Support Assistant Log Analyzer for offline analysis.

  Note: The IBM Support Assistant Log Analyzer is not shipped as part of IBM Tivoli Network Manager IP Edition. You must download and install it separately.

- Trace files capture all messages a log file contains and also additional technical details of operation. Trace files are intended to aid enhanced problem resolution, and are useful to provide to your IBM support contact when requested.

Log message format

GUI log messages are recorded in text format as follows:

```
[<date>T<time>]:<severity>:<message_code_id>:[<thread_id>]:<message>
```

For example:

```
[2010-09-02T04:50:57]:INFO:HNMOB0001I:[Deferrable Alarm : 0]:Initialising
Discovery GUI Server
```

Date and time
> The date and time is in ISO 8601 format.

Severity
> The following severity levels are available:
> - `CONFIG:`
>   Logs all events up to and including configuration changes.
> - `INFO:`
>   Logs only system state changes. This is the default setting.
> - `WARNING:`
>   Logs recoverable system errors.

- SEVERE:

  Logs unrecoverable system errors.

Message code ID

  The message code provides more information on what component of the system the message originates from.

Table 3. Message code IDs

Message code ID	GUI component
HNM T *letter*	Topology visualization components:
HNM T A	Topology client
HNM T B	Topology server
HNM T C	Topology common
HNM N *letter*	MIB GUI components:
HNM N A	MIB browser
HNM N B	MIB grapher
HNM O *letter*	Discovery GUI components:
HNM O A	Discovery configuration GUI
HNM O B	Management Database (formerly called OQL Workbench)
HNM P *letter*	Network polling GUI components:
HNM P A	Network polling configuration (poll policies and definitions)
HNM S *letter*	Structure view components:
HNM S A	Structure browser
HNM X *letter*	Common GUI components:
HNM X A	OQL interface
HNM X B	Others, including: Tools, Filter Builder, Portlets, Entity Search, Expressions, Tree table.
HNM Z *letter*	External product interfaces:
HNM Z A	Tivoli Netcool/OMNIbus Web GUI

Thread ID

  The thread ID indicates the task associated with the function the message originates from.

Message

  The log message itself that provides a description of the event being logged.

Trace message format

Trace messages provide more granular details about operation in the following format:

```
<date> <component_id>\n
<severity>: <message>
```

For example:

```
Aug 24, 2010 3:34:30 AM com.micromuse.precision.disco.server.DiscoConfigLogger
FINE: Received unknown request from the network
```

Trace logs do not provide standardized message format as they are for more enhanced troubleshooting purposes. The severity levels available for trace messages are as follows:

- `FINE:`

  Minimum level of tracing. The majority of stack traces appear at this level already and are written to the trace file. The trace file also includes all log messages.

- `FINER:`

  Medium level of tracing that provides more detailed debug messages.

- `FINEST:`

  Maximum level of tracing that produces very detailed technical information.

Related tasks:

"Changing the logging level for GUIs" on page 28
You can set the level of detail log files contain for GUI components as whole, or specify logging levels on a more granular basis for specific GUI application segments.

Locating GUI log files

All log files generated for GUI components are saved to the `ITNMHOME/profiles/TIPProfile/logs/tnm` directory.

The default name of the log or trace file is `ncp_component_name.number.log` or `ncp_component_name.number.trace`, respectively.

To locate a log file for a component:

1. Go to `ITNMHOME/profiles/TIPProfile/logs/tnm`.

2. Locate the log and trace files that correspond to the GUI component you want to check the log messages for and open the file.

Table 4. GUI component log file mapping

GUI component	Logging properties set in file	.log and .trace file name
Discovery status GUI	`discoconfig.properties`	`ncp_disco.0.log` `ncp_disco.0.trace`
Discovery configuration GUI	`discoconfig.properties`	`ncp_guiconfig.0.log` `ncp_guiconfig.0.trace`
Structure browser	`structurebrowser.properties`	`ncp_structureview.0.log` `ncp_structureview.0.trace`
Topology visualization GUI	`topoviz.properties`	`ncp_topoviz.0.log` `ncp_topoviz.0.trace`
MIB graphing MIB Browser	`itnmgraph.properties`	`ncp_mib.0.log` `ncp_mib.0.trace`

GUI component	Logging properties set in file	.log and .trace file name

Network polling configuration (poll policies and definitions)	`monitorconfig.properties`	`ncp_monitor.0.log`
		
		`ncp_monitor.0.trace`

General settings including database properties for GUI components	`tnm.properties`
	
	Note: This is not to be confused with the log file of the same name located at `ITNMHOME/platform/java/lib/ncp_topoviz/etc/tnm/tnm.properties`. The latter file is used by the Polling engine, `ncp_poller`, to trigger updates to network views, so that poll policy scope is kept up-to-date.
		`ncp_guiconfig.0.log`
		
		`ncp_guiconfig.0.trace`

Management database (formerly called OQL Workbench)	`nmdb.properties`	`ncp_nmdb.0.log`
		
		`ncp_nmdb.0.trace`

Note: Once the log file reaches the specified maximum size limit, it is renamed and a new file is created. The first log file is named `ncp_component_name.0.log`, and the most recent log messages are always in this file. Previous log files are saved with the number increased (for example `ncp_nmdb.1.log`, `ncp_nmdb.2.log`, and so on).

Changing the logging level for GUIs

You can set the level of detail log files contain for GUI components as whole, or specify logging levels on a more granular basis for specific GUI application segments.

Setting logging level for GUI components

You can set the amount of information log files capture for each GUI component. The changes can be made before system startup or during operation. The changes are persistent, and are not affected by system restarts.

To set the logging behavior, you need to modify the corresponding configuration file.

1. Go to `ITNMHOME/profiles/TIPProfile/etc/tnm`.
2. Open the `.properties` file of the GUI component you want to set the logging level for:

Option	Description
`discoconfig.properties`	Discovery configuration GUI
`structurebrowser.properties`	Structure browser
`topoviz.properties`	Topology visualization GUI
`itnmgraph.properties`	MIB graphing MIB Browser
`monitorconfig.properties`	Network polling configuration (poll policies and definitions)
`tnm.properties`	General settings including database properties for GUI components

Option	Description
`nmdb.properties`	Management database (formerly called OQL Workbench)

3. Edit the line *name*`.log.level` to set the message level:

Option	Description
CONFIG	Logs all events up to and including configuration changes.
INFO	Logs only system state changes. This is the default setting.
WARNING	Logs recoverable system errors.
SEVERE	Logs unrecoverable system errors.
FINE	Minimum level of tracing. The majority of stack traces appear at this level already and are written to the trace file. The trace file also includes all log messages. **Note:** When setting the logging level to FINE, FINER, FINEST, or ALL, both log files and trace files will contain information, and the trace files will include all messages from the log files in addition to the more technical details of operation. If any other logging level is set, the trace files remain empty.
FINER	Medium level of tracing that provides more detailed debug messages.
FINEST	Maximum level of tracing that produces very detailed technical information.
ALL	Enables logging and tracing on all levels for the application.
OFF	Disables all logging and tracing for the application.

4. Save and close the `.properties` file.

   Note: The changes take effect immediately if they are made before starting Network Manager. If the changes are made when the system is already running, Network Manager reads the configuration files every 60 seconds and applies any changes immediately.

The following example shows the section of the `structurebrowser.properties` file that determines logging level:

```
structurebrowser.log.filename=ncp_structureview.%g.log
structurebrowser.log.level=INFO
structurebrowser.log.maxsize=10
structurebrowser.log.count=1

structurebrowser.trace.filename=ncp_structureview.%g.trace
structurebrowser.trace.maxsize=10
structurebrowser.trace.count=1
```

The settings here show the default **INFO** setting for the log files. This means log files are populated with information about system state changes, and trace files remain empty.

To change the logging level to have all log messages and enable trace messages, change **INFO** to at least **FINE** (or FINER, or FINEST, depending on the level of detail you require in the trace files). This will mean both log files and trace files will contain information. The following example reflects this change:

```
structurebrowser.log.filename=ncp_structureview.%g.log
structurebrowser.log.level=FINE
structurebrowser.log.maxsize=10
structurebrowser.log.count=1

structurebrowser.trace.filename=ncp_structureview.%g.trace
structurebrowser.trace.maxsize=10
structurebrowser.trace.count=1
```

Setting logging level for application segments

When a specific area requires enhanced troubleshooting, you can enable logging for GUI application segments.

Contact IBM support to identify which application segments require logging to be set for problem determination.

Note: These changes are not persistent. If the system is restarted, all log settings for specific GUI application segments are removed. Logging levels set for the whole GUI component are not affected.

1. In the navigation pane, click **Settings** > **Websphere Administrative Console**.
2. Click **Launch WebSphere administrative console** to start the WebSphere® Application Server console.
3. In the administrative console, click **Troubleshooting** > **Logs and Trace**.
4. In the list, click the name of the server Network Manager is running on.
5. Click **Change Log Detail Levels** and then the **Runtime** tab.
6. Locate the specific application segment name by scrolling down the list and expanding any item as necessary.
7. Click the segment name and select the required logging level from the drop-down menu. Logging and trace level options are the same as for the GUI components.

   Note: By default, whatever is set in the GUI component `.properties` file is the default log and trace level for all relevant segments of that GUI component.
8. View the corresponding GUI component log file to check the messages logged for the segment. For example view the `ncp_disco.0.log` or `ncp_disco.0.trace` files for discovery GUI segments.

Related tasks:

"Locating GUI log files" on page 27
All log files generated for GUI components are saved to the `ITNMHOME/profiles/ TIPProfile/logs/tnm` directory.

Setting the log file size

You can set how large a log file can grow in MB, and determine the number of log files the systems keeps.

Follow these steps to set the maximum size of your log files in MB. After the file reaches the maximum size, it is renamed and a new file is created. You can also set the number of files to be stored after the size limit is reached.

1. Go to `ITNMHOME/profiles/TIPProfile/etc/tnm` and open the `.properties` file of the GUI component you want to set the log size for.
2. In the properties file, perform the following steps:
   a. Locate the *component_name*`.log.maxsize` line and set the maximum size a log file can reach in MB. For example, **nmdb.log.maxsizelog=20** means the maximum allowed size of the Management Database log file is 20 MB. The default setting is 10 MB.
   b. Locate the *component_name*`.log.count` line and set the maximum number of files to be stored. For example, **nmdb.log.count=2** means the 2 latest log files will be kept apart from the one being written to at the moment. The default setting is 1, meaning the current and 1 previous file are saved only.

      Note: Once the log file reaches the specified maximum size limit, it is renamed and a new file is created. The first log file is named `ncp_component_name.0.log`, and the most recent log messages are always in this file. Previous log files are saved with the number increased (for example `ncp_nmdb.1.log`, `ncp_nmdb.2.log`, and so on).
3. Perform the same steps for the trace files by locating and editing the *component_name*`.trace.maxsize` and *component_name*`.trace.count` lines.
4. Save the `.properties` file.

Setting up logging for processes

You can troubleshoot processes by looking in the log files for information. You can set up Network Manager to record log or trace files for processes. You can also set the debug level for processes.

Process log file overview

Network Manager can create log and trace files for its processes.

Log files provide information about important process events, such as changes in state, warnings, or errors, in a standard format that is compatible with IBM's Common Base Event (CBE) format. Log files help administrators to monitor their systems and are useful to provide to your IBM Support contact when requested.

Trace files capture low-level system output and technical details. They are intended to aid enhanced problem resolution, and are useful to provide to your IBM Support contact when requested.

Log files can be identified by their .log suffix, and have the following characteristics:

- Log messages have timestamps.
- Log messages are graded by level, such as error, warn, info, and debug.
- Log messages are formatted to be compatible with IBM's Common Base Event format.

- Log files can be deleted and recreated to enable log file rotation.

Trace files can be identified by their .trace suffix. They can capture different levels of detail, referred to as debug levels. Debug level 4 is the most verbose. Trace files set to the higher debug levels can quickly consume disk space, and therefore should be used only when very detailed information is required to solve a problem.

Locating log files for a process

Locate log files for a process to obtain information that might be helpful in troubleshooting the process.

The default name of the log file is the process name followed by the domain name and then the `.log` or `.trace` file extension.

To locate a log file for a process:
1. Navigate to the default location for process log and trace files, `$NCHOME/log/precision`.
2. Locate the log and trace files that correspond to the process name. For example, an instance of the ncp_disco process running on the NCOMS domain generates the following files:

   ncp_disco.*DOMAIN*.log
   ncp_disco.*DOMAIN*.trace

Changing the logging level for processes

Change the logging level of a process before you start the process or while the process is running.

Changing the logging level before starting a process

Change the value of the relevant command-line argument in the configuration file to change the logging level that a process will use when it is started or restarted.

The –debug and –logdir command-line arguments are used for trace information and the -messagelevel and -messagelog command-line arguments are used for log information.

The default message level is `warn`, which means by default the log files do not contain `info` or `debug` messages.

To change the logging level:
1. Navigate to the `CtrlServices.cfg` file. The file is located in the following directory:

   `NCHOME/etc/precision/CtrlServices.`*domain_name*`.cfg`

   The *domain_name* is the name of the domain for which the logging level is to be changed.
2. From the `CtrlServices.cfg` file, change the argument specified in the file to –debug for trace or –messagelevel for logging. The following example shows how the **ncp_webtool** process might be configured in this file.

   ```
   insert into services.inTray
   (
       serviceName,
       binaryName,
       servicePath,
       domainName,
   ```

```
        argList,
        retryCount
    )
    values
    (
        "ncp_webtool",
        "ncp_webtool",
        "$PRECISION_HOME/platform/$PLATFORM/bin",
        "$PRECISION_DOMAIN",
        [ "-domain" , "$PRECISION_DOMAIN" , "-latency" , "100000", "-debug", "0",
    "-messagelevel", "warn"],
        5
    );
```

3. Start, or restart, the **ncp_ctrl** process. The **ncp_ctrl** process is used to stop and start all other processes. You can also restart Network Manager using the `itnm_start ncp` command.

Changing the logging level for a running process

Change the logging level of a running process to provide more detailed log or trace files to aid debugging.

You can change the logging level or trace level (also called the debug level) of a running process by sending a USR1 or USR2 signal to the process. Sending a USR1 signal changes the logging level and sending a USR2 signal changes the trace level. The extra information provided by increasing the logging or trace levels can help you when debugging a problem with a process.

Trace files have five debug levels (0 to 4) that you can cycle through to provide increasing levels of detail about a process. For example, if a process is already at level 3, a USR2 signal will increase the level to 4; if the process is at level 4, a USR2 signal will move it to level 0.

Log files have four message levels that you can cycle through to increase the level of detail that is captured: error, warn, info, and debug.

The following procedure describes how to increase the trace level of a process. To increase the logging level of a process, perform the same procedure using the USR1 signal instead of USR2.

To increase the trace level of a process, perform the following procedure:
1. Find the Process ID (*PID*) of the process you are investigating:
    a. On Unix and Linux operating systems, enter `ps -ef | grep ncp` at the command line.
    b. On Windows operating systems, you can find the *PID* in the **Processes** tab of Windows **Task Manager**.
2. To increase the debug level by one level:
    a. On Unix and Linux operating systems, enter `kill -USR2` *PID* at the command line.
    b. On Windows operating systems, enter `ncp_signal.bat -domain` *domain PID* USR2 at the command prompt.

First Failure Data Capture (FFDC)

Use the First Failure Data Capture (FFDC) tool to collect pertinent data for problem determination if a system failure occurs. The collected data can be sent to Support using the IBM Support Assistant.

The FFDC is a collection of scripts that can be launched with the master command, **ncp_ffdc**. This command is located in the NCHOME/PD/precision directory.

The FFDC tool collects the following information; this information includes log files and cache files:

- Common information that is gathered every time the FFDC tool is used
- Process-specific information that is gathered for a specific process or group of processes
- Default information that is gathered if no processes are specified

When the **ncp_ffdc** command is run, it checks the NCHOME/PD/precision directory for scripts associated with any process or group of processes specified in the command-line options. (These scripts are called ncp_ffdc_*process_name*.) The FFDC then behaves as follows:

- If it finds scripts for the specified process or group of processes, the scripts are executed and the process-specific information is added to the FFDC package, along with the common information and default information.
- If it finds no scripts for the specified process or group of processes, or if no process is specified, default data collection process is performed. Only the default information and common information is added to the FFDC package.

Usage

`UNIX` The following syntax shows how the **ncp_ffdc.sh** command works on UNIX operating systems:

```
ncp_ffdc.sh -p process -g group key -N directory -C directory -f filename
-T directory -vlmktcx -d domain
```

`Windows` The following syntax shows how the **ncp_ffdc.bat** command works on Windows operating systems:

```
ncp_ffdc.bat -p process -N directory -T directory -d domain -v -l -k -x
```

The following table describes the command-line options for the **ncp_ffdc** command on UNIX and Windows operating systems.

Table 5. ncp_ffdc command-line options

Command-line options	Description
-d *domain*	The domain for which to collect data.
-p *process*	The name of the process from which to collect data. If no process name is provided, then information about all processes is collected.

Table 5. ncp_ffdc command-line options (continued)

Command-line options	Description
-g *group key*	A key that denotes a group of processes from which to collect information. Use this command-line option to gather information about operations that invoke multiple processes. For possible options, see Table 6 on page 36. **Restriction:** This command-line option is not supported on Windows operating systems.
-N *directory*	The path to the NCHOME directory.
-C *directory*	The directory to find core files. The process name given by -p is appended to this path. **Restriction:** This command-line option is not supported on Windows operating systems.
-f *filename*	The name of the properties file. **Restriction:** This command-line option is not supported on Windows operating systems.
-T *directory*	Specifies the directory to save the collected data.
-L *logfile*	The fully-qualified path name to the log file.
-l	List sessions.
-m	Print configuration. **Restriction:** This command-line option is not supported on Windows operating systems.
-k	Keep directory; do not remove data collection directory.
-t	Do not remove the temporary files. **Restriction:** This command-line option is not supported on Windows operating systems.
-c	Do not remove the core file. **Restriction:** This command-line option is not supported on Windows operating systems.
-x	Do not create a .tar file. The default is to create a .tar file.
-v	Displays additional information on the screen.

The following table describes the arguments that can be applied to the -g command-line option.

Table 6. Arguments for the -g command-line option of the `ncp_ffdc` *command*

Argument	Description
RCA	Use this option if you are having problems with event processing or root cause analysis. Collects information about the following processes: • ncp_disco • ncp_g_event
FAIL	Use this option if you are having problems with failover. Collects information about the following processes: • ncp_virtualdomain • nco_p_ncpmonitor • ncp_g_event
MON	Use this option if you are having problems with monitoring. Collects information about the following processes: • ncp_poller • ncp_class
GUI	Use this option if you are having problems with the GUI. Collects information about the ncp_GUI process
CONN	Use this option if you are having problems with discovery. Collects information about the ncp_disco process
ALL	Use this option if you are not sure what is causing the problems. Collects information about all core files. This command-line option runs process-specific scripts for the found cores if a script is available.

Log file rotation environment variables

Log file rotation environment variables are used to configure log file rotation for Network Manager. All log files can be rotated, but not all components have log files. Some components have only trace files, which can also be rotated.

If log file rotation environment variables are set, then a new log file is created based on the time specified, and the current log file is renamed.

Important: On UNIX systems, make sure you set these environment variables in the appropriate shell profile files for the account that Network Manager is running. Do not set them in the NCHOME/env.sh file because this is not used when starting Network Manager. On Windows systems, set these variables as system environment variables.

NDE_LOGFILE_MAXSIZE

The NDE_LOGFILE_MAXSIZE environment variable determines the maximum size a log file can reach for a process.

When the log file reaches the maximum size, the ncp_ctrl process renames the log file from *logfilename.log* to *logfilename.log_old* and generates a new log file

named *logfilename.log*. When the new *logfilename.log* file reaches the maximum size, the ncp_ctrl process overwrites *logfilename.log_old*.

The default setting is 1 GB on UNIX systems. On Windows systems, there is no default limit for the maximum size of a log file: you must set a limit if required due to disk space considerations. As a guidance estimate for log files based on the setting of 1 GB per log file and six processes set to full debug level, you would require 24 GB of disk space (6 processes x 4 log or trace files each = 24 log or trace files x 1 GB = 24 GB).

The following example shows how to set the maximum log file size to approximately 2 GB (the setting is in bytes).
```
setenv NDE_LOGFILE_MAXSIZE 2000000000
```

Data type	Integer
Default	1073741824 bytes (1 GB)

Note: If the NDE_LOGFILE_ROTATION_FORMAT environment variable is set, the NDE_LOGFILE_MAXSIZE environment variable is ignored.

NDE_LOGFILE_ROTATION_FORMAT

The NDE_LOGFILE_ROTATION_FORMAT environment variable specifies whether a daily log file rotation is enforced. If this environment variable has a value set, then a daily log file rotation is enforced.

The NDE_LOGFILE_ROTATION_FORMAT environment variable is used in conjunction with the NDE_LOGFILE_ROTATION_TIME environment variable to control the creation of the message log by setting a time of day for log file rotation.

Data type	Specifies the date format that controls how the log files are named.
	For example, `yyyyMMdd-HHmm` generates rotate log files with the year, month, day, hour, and minute added. An example file is `ncp_disco.NCOMS.log_20100430-0000`.
Default	The default is for this value to be undefined.

Note: If the NDE_LOGFILE_ROTATION_FORMAT environment variable is set, the NDE_LOGFILE_MAXSIZE environment variable is ignored.

NDE_LOGFILE_ROTATION_TIME

The NDE_LOGFILE_ROTATION_TIME environment variable specifies the time at which a log file rotation occurs each day. Log files are created at the time set by the NDE_LOGFILE_ROTATION_TIME environment variable.

The NDE_LOGFILE_ROTATION_FORMAT environment variable is used in conjunction with the NDE_LOGFILE_ROTATION_TIME environment variable to control the creation of the message log by setting a time of day for log file rotation.

Data type	Integer
Default	0000

The following example specifies log file rotation at midnight each day:

```
setenv NDE_LOGFILE_ROTATION_FORMAT=yyyyMMdd-HHmm
setenv NDE_LOGFILE_ROTATION_TIME 0000
```

Note: If neither the NDE_LOGFILE_MAXSIZE variable, nor the NDE_LOGFILE_ROTATION_TIME variable is set when Network Manager starts, then the NDE_LOGFILE_MAXSIZE variable is set to the default 1 GB on UNIX systems. On Windows systems, no default is set, and any limit must be set manually as described earlier in this topic.

Chapter 4. Administering ports

If there are conflicts with ports already in use on your system, change some of the default ports.

If you are deploying Network Manager in a secure environment, you might need to know which ports are used by different processes in order to configure a firewall or other security application.

Note: When accessing a Tivoli Netcool/OMNIbus ObjectServer that is protected by a firewall, you must specify an IDUC port and provide access to that port using the firewall.For more information on specifying an ObjectServer IDUC port, see the *IBM Tivoli Netcool/OMNIbus Administration Guide*.

About inter-process communication

Network Manager processes communicate using TCP connections, multicast, and Really Small Message Broker.

About Really Small Message Broker

Communication between Network Manager core components is managed by Really Small Message Broker. To ensure correct operation of Network Manager, Really Small Message Broker must be running at all times.

Various Network Manager core components pass information to other components on the same server, and to any Network Manager core components on different servers. This communication is managed by Really Small Message Broker.

Really Small Message Broker is installed and started automatically by the Network Manager installation process. If you stop Really Small Message Broker while core Network Manager processes such as the Discovery engine, ncp_disco, are running, then the core processes will restart Really Small Message Broker automatically.

Note: Running multiple domains in parallel can overload the message broker on some systems. If you want to run multiple domains under load in parallel then it is good practice to run a separate message broker for each domain.

Related tasks:

"Running a separate message broker for each domain" on page 41
If you want to run multiple domains under load in parallel then it is good practice to run a separate message broker for each domain.

About multicast

Processes that use direct TCP communication first use multicast to locate each other, then set up TCP sockets.

Changing host and port settings for Really Small Message Broker

You can change the host and port settings for Really Small Message Broker by modifying the Really Small Message Broker configuration file and then stopping the broker.

Updating the Really Small Message Broker configuration file

You can configure the host and port for Really Small Message Broker.

Before updating the Really Small Message Broker configuration file (`precision.broker.cfg`), you must stop all ncp processes.

To configure the host and port for Really Small Message Broker, complete the following steps on each server where Network Manager core components are installed.

1. Ensure that all ncp processes have been stopped.
2. Delete the following file:

   `$NCHOME/etc/precision/broker_1883.cfg`

   Important: `Broker_1883.cfg` is automatically generated from `precision.broker.cfg` when the Really Small Message Broker starts. If this file is not deleted before the Really Small Message Broker file is edited, a mismatch can occur between two versions of the file. This can prevent Network Manager from starting.
3. Edit the following file:

   `$NCHOME/etc/precision/Precision.broker.cfg`
4. Locate the following section in the file:

   ```
   broker session =
     {
       'service' = '1883',
       'network' = '127.0.0.1'
     };
   ```

   Note: The `broker session` settings use the IP address of the loopback interface. This ensures that you can only access the broker from the local server. If you want to allow external connections then you must bind to the IP address of the server. Note that allowing external connections to the broker might constitute a security risk.
5. Change the value of `'service'` to the port you want to use. Ensure that it does not conflict with any other ports on your system.
6. Change the value of `'network'` to the address of the current server.
7. Save and close the file.

Stopping Really Small Message Broker

Once you have changed the Really Small Message Broker configuration file, you must stop Really Small Message Broker for your changes to take effect.

To stop Really Small Message Broker, run the following script.

```
$NCHOME/precision/scripts/perl/scripts/stop_broker.pl
```

Any currently running Network Manager core processes such as the Discovery engine, ncp_disco will restart Really Small Message Broker automatically. The new instance of Really Small Message Broker will pick up the configuration changes.

Running a separate message broker for each domain

If you want to run multiple domains under load in parallel then it is good practice to run a separate message broker for each domain.

To run a separate message broker for each domain, proceed as follows.

1. Ensure that all ncp processes have been stopped.
2. Create a domain specific `Precision.broker.cfg` configuration file. Do this by copying the following file: `$NCHOME/etc/precision/Precision.broker.cfg` to a domain-specific copy: `$NCHOME/etc/precision/Precision.broker.DOMAIN_NAME.cfg`

   Where *DOMAIN_NAME* is the name of one of your domains.
3. Locate the following section in the file:

   ```
   broker session =
     {
       'service' = '1883',
       'network' = '127.0.0.1'
     };
   ```
4. Change the value of `'service'` to the port you want to use. Ensure that it does not conflict with any other ports on your system.
5. Save and close the file.
6. Repeat steps 2 to 5 to create a separate message broker for each of your domains.
7. Restart all ncp processes.

Checking port usage

You can check which ports are in use on the current server, to help investigate or prevent port conflicts.

To check which ports are in use on the current server, enter the following command:

```
netstat -a
```

The command returns a list of listening daemons and established connections.

Defining a fixed TCP port

For processes that use TCP socket-based connections, you can define a fixed port instead of using the default randomly assigned port.

To avoid firewall issues or port conflicts, you might have to define a specific TCP port for a process. For example, you might need to do this if the helpers and the Helper Server, `ncp_d_helpserv`, are running on a different host to the Discovery engine, `ncp_disco`, and these hosts are behind a firewall. You might also need to define a fixed TCP port as part of failover configuration.For more information on how to define a fixed TCP port specifically for failover, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

To define a fixed TCP port for a process, complete the following steps:

1. On the first server, start the process.
2. Make a backup copy of the `ServiceData.cfg` file.
3. Edit the `ServiceData.cfg` file and copy the line relevant to the process for which you want to define a port.

   The existing line might resemble the following example:`SERVICE: Helper DOMAIN: DEMO ADDRESS: 192.168.31.8 PORT: 51153 SERVERNAME: britanicus DYNAMIC: YES`

   In this example, `DYNAMIC: YES` shows that the port for the Helper Server has been assigned dynamically.
4. Change the `PORT` setting to the required value.
5. Change the string `DYNAMIC:YES` to `DYNAMIC:NO`. This forces the process to use the same address and port next time it starts.
6. Save the `ServiceData.cfg` file.
7. On the second server, make a backup copy of the `ServiceData.cfg` file.
8. Copy the relevant line from the `ServiceData.cfg` file on the first server to the `ServiceData.cfg` file on the second server.
9. Save the `ServiceData.cfg` file.

Defining a fixed multicast address

You can define which address and port is used by processes for multicast communication by editing the `ServiceData.cfg` configuration file.

If a Network Manager process needs to know what port another process is running on, it looks up the TCP/IP port defined for that process in the `ServiceData.cfg` file. If there is no port defined for a specific service, then the process broadcasts an address request using multicast. You can define the address that is used for this multicast address request.

The multicast address must be the same on all servers that have Network Manager processes that communicate with each other.

To define the address for multicast communication, complete the following steps.

1. Back up and edit the `ServiceData.cfg` file.
2. Edit the line that contains `SERVICE: MulticastService`. Set the ADDRESS and PORT variables.

3. Set the `DOMAIN` to `ANY_PRECISION_DOMAIN`. This means that the service uses the same multicast address for all domains in which it is executed. The line should resemble this example:

```
SERVICE: MulticastService DOMAIN: ANY_PRECISION_DOMAIN
ADDRESS: 224.0.0.108 PORT: 33000
```

4. Save and close the `ServiceData.cfg` file.

List of ports used by the product

Network Manager uses different ports for communication: some fixed, some defined by configuration files, and some assigned by the operating system.

The following table describes the default ports used by Network Manager.

Table 7. Default ports used by Network Manager

Port	Protocol	Description
22	SSH over TCP/IP	If SSH support is enabled, the Telnet Helper uses this port to communicate with network devices.
23	Telnet over TCP/IP	If SSH support is not enabled, the Telnet Helper uses this port to communicate with network devices.
161	SNMP	Port 161 is the default port on network devices to which SNMP queries are sent during the discovery and monitoring processes. Defined in the column m_SnmpPort in the database table snmpStack.verSecurityTable.
162	UDP	Default trap port. Used by the Trap polling agent. If more than one application/process needs access to this port, ncp_trapmux, the SNMP trap multiplexer, can be used to forward traps. The SNMP trap multiplexer, the Trap discovery agent, and the Trap polling agent can all be configured to use a different port.
1521	TCP/IP	Default Oracle database port.
1883	Message Queuing Telemetry Transport (MQTT)	Default port used by Really Small Message Broker for inter-process communication.
3306	TCP/IP	Default MySQL database port. This is used by Topoviz to communicate with the MySQL database.
4100	TCP/IP	Default ObjectServer port. This must be entered at install time. Defined in `interfaces.Arch` on the ObjectServer workstation. This port is used by the `ncp_g_event` process to communicate with the ObjectServer.
7968	TCP/IP	Default port for access to the Network Manager server from Tivoli Integrated Portal. This is used by the Discovery Configuration GUI and it is defined in the `ServiceData.cfg` configuration file. If you want to change this port, edit the `ServiceData.cfg` configuration file and restart the ncp_model process and the ncp_config process using CTRL.
9088	TCP/IP	Default Informix database port.
16310	HTTP	Default port for the Tivoli Integrated Portal. The Tivoli Integrated Portal allocates the next six ports up from this number for its own use. By default, this port redirects to 16316.
16311	HTTPS	Default secure port for the Tivoli Integrated Portal.

Table 7. Default ports used by Network Manager (continued)

Port	Protocol	Description
33000	TCP/IP	By default, the multicast IP address 225.13.13.13 and port 33000 are used to enable the discovery helpers and discovery agents to locate the Helper server. This multicast address is specified in the file `$NCHOME/etc/precision/ServiceData.cfg`. Once a process has located the Helper server, a TCP connection is established on a port assigned by the operating system.
50000	TCP/IP	Default DB2® database port.
OS-assigned	TCP/IP	TCP ports are assigned by the operating system for TCP communication between processes, for example, the communication between discovery agents and the helper server. If this is an issue, you must ensure that your firewall is external to the Network Manager server, and that all discovery processes are run on the same host.

ServiceData configuration file

The `ServiceData` configuration file is a dynamic file that lists TCP and multicast connection information for Network Manager processes.

On startup, every Network Manager service (that is, component or process) that uses a TCP socket adds a line to the ServiceData configuration file. This line contains information about the service. The following information is appended to the configuration file:

- The service name
- The service domain
- The service IP address
- The service port number
- The server on which the process is being run

In the following example configuration file, the first service called MulticastService shows the multicast address and port number. The second service shows that the Helper service is running on the DEMO domain, and includes information about the IP address, port number and the name of the server where the Helper service is running. DYNAMIC: YES means that the port is assigned by the operating system each time the process starts. DYNAMIC: NO defines a fixed port.

```
--
-- Server data file - contains info on servers and the general multicast
-- address to use.
--
SERVICE: MulticastService DOMAIN: ANY_PRECISION_DOMAIN ADDRESS: 225.13.13.13
PORT: 33000

SERVICE: Helper DOMAIN: DEMO ADDRESS: 192.168.31.8 PORT: 51153
SERVERNAME: britanicus DYNAMIC: YES
```

Chapter 5. Administering users

Use the functions of the Web console to provide access to the Web-based interfaces for users, based on the default user roles and user groups. Users and profiles for the OQL Service Provider are managed separately.

About administering users

User administration involves setting user access to the Web applications and the OQL Service Provider.

The user interfaces can be categorized as follows:

Web applications
Network Manager includes the following Web applications:
- Network Discovery GUI
- Network Polling GUI
- Topoviz Hop View
- Topoviz Network Views
- SNMP MIB Browser
- Structure Browser

OQL Service Provider
OQL Service Provider users are managed separately from Web application users.

Default users

Several users are supplied with Network Manager.

Users and their groups

The following table describes users that are present after installation, along with their groups.

Table 8. Users present after installation

User name	Group	Password	Description
tipadmin	None	Defined during installation. The default value for a basic installation is netcool. The administrator should change this password.	The administrator for Tivoli Integrated Portal. In a new installation, this user has permissions to administer users, groups, roles, and pages. Defined in the file-based user repository.

Table 8. Users present after installation (continued)

User name	Group	Password	Description
itnmadmin	Network_Manager_IP_Admin	Defined during installation.	The administrator for Network Manager. In a new installation, this user has permissions to administer all of the Network Manager Web applications. Defined in the user repository chosen during installation. This user also has the following Tivoli Integrated Portal roles by default: • administrator • chartAdministrator • chartCreator
itnmuser	Network_Manager_User	Defined during installation.	An example operator user for Network Manager. Defined in the user repository chosen during installation.
itnmclient	Network_Manager_Client	Defined during installation.	An example guest user for Network Manager. Defined in the user repository chosen during installation.

Related tasks:

"Administering users for Web applications" on page 50
You can perform tasks that help you manage users.

User roles

A role provides users with the ability to perform a predefined set of activities within Web applications.

Access to the Web applications and to functionality within the Web applications depends on the roles assigned to users. Network Manager roles are assigned to users by using groups. Users can also have roles assigned to them from other products.

Note: For information about the user roles you need to view and administer reports using Tivoli Common Reporting, see the Tivoli Common Reporting information center at the following Web address: http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc/tcr_welcome.html.

Important: In addition to the roles assigned to the default user groups, the netcool_rw role is also necessary in order to use the Management Database Access and Network Polling portlets.

Related tasks:

"Administering users for Web applications" on page 50
You can perform tasks that help you manage users.

User roles for charting

Users must have the user IDs assigned to a chart role before they can see and work with the charting functions.

The main administrator (tipadmin) of the application server already has the chartAdministrator role, and can assign users to any of the three chart roles that are available. Logged in users will have no access privileges to the charting features if their user ID has not been assigned to a chart role. These are the capabilities of the chart roles:

chartAdministrator
> Users with this role can create and delete charting connections to data sources, download the BIRT Designer, upload charts, and can clear the charting cache (useful for troubleshooting).

chartCreator
> Users with this role can download the BIRT Designer, upload charts, view, and edit them. They cannot create or delete chart connections nor can they clear the charting cache.

chartViewer
> Users assigned to this role can select and view charts, but cannot modify them or their preferences. They cannot download the BIRT Designer, upload charts, create connections, or clear the charting cache.

Roles are assigned through **Users and Groups > Administrative User Roles**.

User groups

Use groups to organize users into units with common functional goals. Several Network Manager groups are created on installation.

Default user groups

The following groups are supplied with Network Manager. Roles are assigned to these groups during installation.

Network Manager Client
> Assign guest user accounts to this group in order to give the users limited permissions to view the Web applications.

Network Manager IP Admin
> Assign all Network Manager IP Edition administrators to this group in order to give the users administrative permissions for the Network Manager Web applications.

Network Manager User
> Assign all Network Manager IP Edition end users and operators to this group in order to give the users permissions to use the Network Manager Web applications.

Related tasks:

"Administering user groups for Web applications" on page 60
You can perform tasks that help you manage groups.

Roles assigned to the Network_Manager_IP_Admin group

The Network_Manager_IP_Admin group has several user roles assigned to it.

Table 9. Roles for the Network_Manager_IP_Admin_Group

Role	Description
ncp_config	User can save any configuration changes that they have made.
ncp_disco_config	User can view and edit the discovery configuration settings.
ncp_disco_config_alter_domain	User can change the domain for which they are configuring a discovery.
ncp_disco_status	User can view the status of a discovery as it is running.
ncp_disco_status_control	User can start or stop the discovery, or run a discovery with same configuration settings. This role is ineffective without the role Network Manager IP Discovery Status.
ncp_disco_status_alter_domain	User can change the domain from which they are getting discovery status. **Note:** Do not remove this role from discovery administrators.
ncp_mibgraph_default_properties_config	User can change the MIB graph default properties. This role is ineffective without the following Network_Manager_User group roles: ncp_mibgraph_user, ncp_mibgraph_config, ncp_mibbrowser.
ncp_monitor_policy	User can configure poll policies.
ncp_monitor_policy_alter_domain	User can select a domain other than the default for poll policies.
ncp_monitor_template	User can configure poll definitions.
ncp_oql	User can perform and display the results of select type operations using the Management Database Access page.
ncp_oql_update	User can perform and display the results of update type operations using the Management Database Access page.
ncp_manage_unmanage	User can set devices to managed and unmanaged status.
ncp_networkview_admin_global	User can create, edit, partition, and delete Global Views. These are views accessible to all users regardless of the group to which they belong. User can also perform Move operations on network views within the global views.
ncp_networkview_admin_group	User can create, edit, partition, and delete Group Views. These are views assigned to the group or groups that this user belongs to. This role also allows the user to perform Move operations on network views within a group view collection.

Table 9. Roles for the Network_Manager_IP_Admin_Group (continued)

Role	Description
ncp_networkview_admin_all_users	User can create, edit, partition, and delete Private Views. These are private views created by users who have the Network Manager IP Network View - Administer views for user role. This role also allows the user to perform Move operations on network views within a group view collection.
ncp_pathview	User can create, edit, and delete path views.
ncp_topo_mgmt	User can add and remove devices and connections to the topology using the topology management functionality available within the Network Hop View.

Roles assigned to the Network_Manager_User group

The Network_Manager_User group has several user roles assigned to it.

Table 10. Roles for the Network_Manager_User

Role	Description
ncp_hopview	User can access the Hop View.
ncp_networkview	User can access the Network Views and to display any of the following views: • User Views: Network views created by the user. • Group Views: Views assigned to the group or groups that this user belongs to. • Global Views: Views accessible to all users regardless of the group to which they belong.
ncp_networkview_admin_user	User can create, edit, partition, and delete their own set of network views. This role also allows the user to perform Move operations on network views within a user view.
ncp_mibbrowser	User can access the MIB Browser.
ncp_mibbrowser_config	User can access the MIB Browser for configuration purposes.
ncp_mibgraph_config	User can access SNMP MIB Graph for configuration purposes.
ncp_mibgraph_user	User can access SNMP MIB Graph.
ncp_pathview	User can create, edit, and delete path views.
ncp_structurebrowser	User can use the Structure Browser.
ncp_structureview_entitysearch	User can search entities in the Structure Browser.
ncp_structureview_interport_navigation	User can navigate from a port on one device to a port on another device in the Structure Browser.
ncp_webtools	User can use the WebTools.

Table 10. Roles for the Network_Manager_User (continued)

Role	Description
ncw_user	User can view the Tivoli Netcool/OMNIbus Web GUI portlets.

Roles assigned to the Network_Manager_Client group

The Network_Manager_Client group has several user roles assigned to it.

Table 11. Roles for the Network_Manager_Client group

Role	Web Application	Description
ncp_networkview	Network Views	Allows the user to access the Network Views and to display any of the following views: • User Views: Network views created by the user. • Group Views: Views assigned to the group or groups that this user belongs to. • Global Views: Views accessible to all users regardless of the group to which they belong.
ncp_structurebrowser		Allows a user to use the Structure Browser.
ncp_structureview_ entitysearch	Structure Browser	User can search entities in the Structure Browser.
ncp_structureview_interport_ navigation	Structure Browser	User can navigate from a port on one device to a port on another device in the Structure Browser.

Administering users for Web applications

Use the functions of the Web console to administer users for the Network Manager Web applications.

From the left navigation pane, click **Manage Users**. Before you can perform some tasks for users, you must first search for existing users that match the search criteria that you specify. After the search completes, a table displays the users that match your search criteria. To manage users, you can perform these tasks:

Related concepts:

"User roles" on page 46
A role provides users with the ability to perform a predefined set of activities within Web applications.

Related reference:

"Default users" on page 45
Several users are supplied with Network Manager.

Searching for users

You can search for existing users that match the search criteria that you specify.

1. From the navigation pane, click **Manage Users**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more users. For example, select **User ID**.
3. In the **Search for** field, either type the string that you want to search for to limit the set of users, or use the wildcard character (*) to search for all users. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes, a table displays the users that match your search criteria.

   Creating users
   You can create one or more users. The users are added to the registry and a login account for each new user is automatically created. When creating the new user, you can also add the user as a member of one or more groups.

   Deleting users
   You can search for and list the existing users that match your search criteria. After selecting one or more users, you can delete them and remove their user IDs from the user registry.

   Duplicating group assignments for a user
   You can search for users that match your search criteria. After selecting one or more users, these users can be added as members of the same groups that another existing user is already a member of. For example, if all the members of a department need to belong to the same groups as the department manager, you can duplicate the groups that the manager belongs to for all the other users that you choose.

   Customizing search filters for users
   You can create a filtered list of users by specifying the type of filter and the text to be used as part of the search criteria. The filtered list of users is limited to displaying only the users that meet the filter requirements. You can filter users by the letters that the user ID contains or by the letters that the user ID starts or ends with.

   Changing the display options for the list of users
   You can change how the search results are displayed when viewing the list of users. For example, you can change the number of users to be viewed per page or you can display additional details about the users.

Users

A user is an individual who uses a computer. Users can include any user from expert programmers to computer novices.

For example, users might include:

- Users who use a computer product.
- Users who administer the same product and provide their users with access privileges.
- Users who administer users and groups by using a console menu to complete tasks.
- Users who use the same product for development purposes.

An example of a user task might be resetting your own password. An example of an administrator task might be creating new users and groups.

Groups

A group is a collection of *members* that can be used to satisfy specific business needs, such as granting access to a resource.

Membership in a group named Company XYZ can be all the users in a department (Dept 047). A group within another group is referred to as a *nested group*. For example, Dept 047 might be a group within a larger group named Company XYZ Austin.

Members

A member is a *user* or *group* within a group.

For example, membership in a group named Company XYZ can be both an individual user (Harry Jones) as well as all the users in his department (Dept 047).

Customizing search filters for users

You can create a filtered list of users by specifying the type of filter and the text to be used as part of the search criteria. The filtered list of users is limited to displaying only the users that meet the filter requirements. You can filter users by the letters that the user ID contains or by the letters that the user ID starts or ends with.

1. From the navigation pane, click **Manage Users**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more users. For example, select **User ID**.
3. In the **Search for** field, either type the string that you want to search for to limit the set of users, or use the wildcard character (*) to search for all users. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes, a table displays the users that match your search criteria.
6. Click the filter icon.
7. Do one of the following:
   - To create a new filter for an attribute if none exists, click the **[No Filter]** link.
   - To select an existing filter, click on the filter name.
8. If you are creating a new filter, select a filter type from the list. The types of filters are Contains, Starts with, or Ends with.
9. Type the letters that you want to search for in the **Text** field. The wildcard character is not permitted in this field.
10. Click **Apply**.

After you click **Apply**, the name of the filter is listed in the column under the attribute. The filter name matches the letters that were typed in the **Text** field. If no filter has been used for an attribute, the text [No Filter] displays.

The list of users is refreshed, and a filtered list of user IDs is displayed. The filter name and the total number of filtered user IDs are also shown.

Click the ⬇ hide filter icon, or click **Close**, when you have finished working with filters.

Searching for users
You can search for existing users that match the search criteria that you specify.

Changing the display options for the list of users
You can change how the search results are displayed when viewing the list of users. For example, you can change the number of users to be viewed per page or you can display additional details about the users.

Changing the display options for the list of users

You can change how the search results are displayed when viewing the list of users. For example, you can change the number of users to be viewed per page or you can display additional details about the users.

1. From the navigation pane, click **Manage Users**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more users. For example, select **User ID**.
3. In the **Search for** field, either type the string that you want to search for to limit the set of users, or use the wildcard character (*) to search for all users. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes, a table displays the users that match your search criteria.
6. Click the 🖉 options icon.
7. If you want to view more or fewer entries on a page, change the number in the **Entries Per Page** field.
8. If you want to show more details about a user, select one or more check boxes next to the attributes that you want to display additional columns for.
9. If you want to see the user IDs on a different page, type the page number in the field at the bottom of the list, and click **Go** to jump to that page.
10. Click **Apply**.
11. Click the 🖉 hide options icon, or click **Close**, after changing the display options for the list of users.

Searching for users
You can search for existing users that match the search criteria that you specify.

Customizing search filters for users
You can create a filtered list of users by specifying the type of filter and the text to be used as part of the search criteria. The filtered list of users is limited to displaying only the users that meet the filter requirements. You can filter users by the letters that the user ID contains or by the letters that the user ID starts or ends with.

Creating users

You can create one or more users. The users are added to the registry and a login account for each new user is automatically created. When creating the new user, you can also add the user as a member of one or more groups.

1. Complete the steps in "Searching for users" on page 51.

2. Click **Create** to create a new user.

3. In the **User ID** field, type a unique name to identify the user. This user ID will be added to the user registry and also will be used as the login account name. For example, you might type `dlucas`

4. Optional: Click **Group Membership** and then follow the steps in "Changing group membership for a user" to add the user as a member of one or more existing groups.

5. In the **First name** field, type the given or first name of the user. For example, you might type `Diana`

6. In the **Last name** field, type the family or last name of the user. For example, you might type `Lucas`

7. Optional: In the **E-mail** field, type an e-mail address for the user. For example, you might type `dlucas@tivoli.com`

8. In the **Password** field, type a unique password. For example, you might type `d4lucas`.

9. In the **Confirm password** field, type the same password again.

10. Click **Create**. If successful, a message will display that indicates that the user has been created. Also, the user ID and other user information will be added to the user registry, and a new login account will be created for the user.

11. To create another user, click **Create Another**.

12. Repeat the process until all the new users have been created.

    Deleting users
    You can search for and list the existing users that match your search criteria. After selecting one or more users, you can delete them and remove their user IDs from the user registry.

    Duplicating group assignments for a user
    You can search for users that match your search criteria. After selecting one or more users, these users can be added as members of the same groups that another existing user is already a member of. For example, if all the members of a department need to belong to the same groups as the department manager, you can duplicate the groups that the manager belongs to for all the other users that you choose.

Changing group membership for a user

You can search for and list the existing groups that match the search criteria. When creating a new user, you can choose the groups from the search results list in which you want the user to be a member.

1. During the process of "Creating users," click **Group Membership**.

2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more users. For example, select **Group name**.

3. In the **Search for** field, either type the string that you want to search for to limit the set of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.

4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes, the results are displayed in two lists: one list is for groups that matched the search criteria and one list, named **Current Groups**, is for groups that the user is already a member.
6. To add the user to one or more groups, highlight the groups from the matching groups list to select them. For example, you might highlight `ibmaustin01` and `ibmaustin02` and then click **< Add**.
7. Optional: To undo or remove the user as a member, highlight the groups from the **Current Groups** list and then click **Remove >**.
8. Return to the process of "Creating users" on page 54 to complete the steps.

Adding a user to other groups
You can add a user as a member to selected groups.

Changing information about a user
You can change information about a specific user, such as the e-mail address. You can update the e-mail address, change the first or last name information, or set a new password.

Removing a user from other groups
After searching for the groups in which the user is currently a member, you can remove the user from membership in groups that you select.

Viewing information about a user
You can view information about a specific user.

Viewing the groups the group is a member of
You can view a list of existing groups that the specified user is currently a member of.

Viewing information about a user

You can view information about a specific user.
1. From the navigation pane, click **Manage Users**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more users. For example, select **User ID**.
3. In the **Search for** field, either type the string that you want to search for to limit the set of users, or use the wildcard character (*) to search for all users. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes, the users that match your search criteria are displayed as hypertext links.
6. Click on one of the user links to view information about the selected user. You can only view the information, you cannot change it.
7. Click **Cancel** after viewing to return to the previous window.

Changing information about a user
You can change information about a specific user, such as the e-mail address. You can update the e-mail address, change the first or last name information, or set a new password.

Changing group membership for a user
You can search for and list the existing groups that match the search criteria. When creating a new user, you can choose the groups from the search results list in which you want the user to be a member.

Changing information about a user

You can change information about a specific user, such as the e-mail address. You can update the e-mail address, change the first or last name information, or set a new password.

1. From the navigation pane, click **Manage Users**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more users. For example, select **User ID** to locate users by searching by their user IDs.
3. In the **Search for** field, either type the string that you want to search for to limit the set of users, or use the wildcard character (*) to search for all users. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes, the users that match your search criteria are displayed in the column as hypertext links.
6. Click on one of the user links to change information about the user, as needed.
7. In the **First name** and **Last name** fields, enter the new information, if needed.
8. Optional: In the **E-mail** field, enter the new information, if needed.
9. Optional: In the **Password** and **Confirm password** fields , enter the new password, if needed, and confirm the new password.
10. To save the changes, either click **OK** to save and return to the previous window, or click **Apply** to save but remain on the same window.

Changing group membership for a user
You can search for and list the existing groups that match the search criteria. When creating a new user, you can choose the groups from the search results list in which you want the user to be a member.

Viewing information about a user
You can view information about a specific user.

Viewing the groups the user is a member of
You can view a list of existing groups that the specified user is currently a member of.

Viewing the groups the user is a member of

You can view a list of existing groups that the specified user is currently a member of.

1. From the navigation pane, click **Manage Users**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more users. For example, select **User ID**.
3. In the **Search for** field, either type the string that you want to search for to limit the set of users, or use the wildcard character (*) to search for all users. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes, a table displays a list of groups, as hypertext links, that match your search criteria.
6. Click the group name link to see the user properties.

7. Click the **Groups** tab to see the list of groups, in ascending order, that the user is currently a member of.

Adding a user to other groups
You can add a user as a member to selected groups.

Changing group membership for a user
You can search for and list the existing groups that match the search criteria. When creating a new user, you can choose the groups from the search results list in which you want the user to be a member.

Changing information about a user
You can change information about a specific user, such as the e-mail address. You can update the e-mail address, change the first or last name information, or set a new password.

Removing a user from other groups
After searching for the groups in which the user is currently a member, you can remove the user from membership in groups that you select.

Viewing information about a user
You can view information about a specific user.

Adding a user to groups

You can add a user as a member to selected groups.

1. Complete the steps in "Viewing the groups the user is a member of" on page 56
2. Confirm that the user in the **User ID** field is the user that you want to add to more groups.
3. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group name**.
4. In the **Search for** field, either type the string that you want to search for to limit the set of users, or use the wildcard character (*) to search for all users. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
5. In the **Maximum results** field, specify the maximum number of search results that you want to display.
6. Click **Search**. After the search completes, a list is displayed of the groups that match your search criteria.
7. Highlight one or more groups to select them, and click **Add**.

Removing a user from other groups
After searching for the groups in which the user is currently a member, you can remove the user from membership in groups that you select.

Changing group membership for a user
You can search for and list the existing groups that match the search criteria. When creating a new user, you can choose the groups from the search results list in which you want the user to be a member.

Changing information about a user
You can change information about a specific user, such as the e-mail address. You can update the e-mail address, change the first or last name information, or set a new password.

Viewing information about a user
You can view information about a specific user.

Viewing the groups the user is a member of
You can view a list of existing groups that the specified user is currently a member of.

Removing a user from other groups

After searching for the groups in which the user is currently a member, you can remove the user from membership in groups that you select.

1. Complete the steps in "Viewing the groups the user is a member of" on page 56.
2. Confirm that the user in the **User ID** field is the user that you want to remove from other groups.
3. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group name**.
4. In the **Search for** field, either type the string that you want to search for to limit the set of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
5. In the **Maximum results** field, specify the maximum number of search results that you want to display.
6. Click **Search** to begin the search. After the search completes, a table displays the groups that match your search criteria.
7. Select the check boxes next to one or more groups, and then click **Remove**.

   Adding a user to other groups
   You can add a user as a member to selected groups.

   Changing group membership for a user
   You can search for and list the existing groups that match the search criteria. When creating a new user, you can choose the groups from the search results list in which you want the user to be a member.

   Changing information about a user
   You can change information about a specific user, such as the e-mail address. You can update the e-mail address, change the first or last name information, or set a new password.

   Viewing information about a user
   You can view information about a specific user.

   Viewing the groups the group is a member of
   You can view a list of existing groups that the specified user is currently a member of.

Adding more users as members of a group

You can add more users as members of a group.

1. After completing the steps in "Viewing a list of members of a group" on page 66, click **Add Users**.
2. Confirm that the **Group name** field displays the name of the group to which you want to add more users as members.
3. In the **Search by** field, select the attribute from the list that you want to use to search by. For example, select **User ID**.
4. In the **Search for** field, either type the string that you want to search for to limit the set of users or use the wildcard character (*) to search for all users.
5. In the **Maximum results** field, specify the maximum number of search results that you want to display.
6. Click **Search**. After the search is complete, a list displays of the users that matched your search criteria.
7. Highlight one or more users in the list to select them, and then click **Add**.

The users are immediately added to the list of members.

Adding more groups as members of a group
After viewing the list of members in a group that you specify, you can add more groups.

Removing members from a group
After searching for the list of members in a group that you specify, you can remove users and groups as members from the group.

Duplicating group assignments for a user

You can search for users that match your search criteria. After selecting one or more users, these users can be added as members of the same groups that another existing user is already a member of. For example, if all the members of a department need to belong to the same groups as the department manager, you can duplicate the groups that the manager belongs to for all the other users that you choose.

1. Complete the steps in "Searching for users" on page 51.

2. Select the check boxes next to one or more users that you want to assign the same membership as another group.

3. Choose the **Duplicate Group Assignments** action.

4. In the **Search by** field, select the attribute from the list that you want to use to search for one or more users. For example, select **User ID**.

5. In the **Search for** field, either type the string that you want to search for to limit the set of users, or use the wildcard character (*) to search for all users. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.

6. In the **Maximum results** field, specify the maximum number of search results that you want to display.

7. Click **Search**. After the search has been completed, a table displays the users that match your search criteria.

8. Highlight the name of the user whose group membership you want to duplicate for the previously selected users, and click **OK**. The group membership of the user is duplicated for the previously selected users.

Creating users
You can create one or more users. The users are added to the registry and a login account for each new user is automatically created. When creating the new user, you can also add the user as a member of one or more groups.

Deleting users
You can search for and list the existing users that match your search criteria. After selecting one or more users, you can delete them and remove their user IDs from the user registry.

Deleting users

You can search for and list the existing users that match your search criteria. After selecting one or more users, you can delete them and remove their user IDs from the user registry.

1. From the navigation pane, click **Manage Users**.

2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more users. For example, select **User ID**.

3. In the **Search for** field, either type the string that you want to search for to limit the set of users, or use the wildcard character (*) to search for all users. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.

4. In the **Maximum results** field, specify the maximum number of search results that you want to display.

5. Click **Search**. After the search completes, a table displays the users that match your search criteria.

6. Select the check boxes next to the users that you want to delete.

7. Click **Delete**.

8. Click **Delete** again when asked to confirm the deletion. The users are immediately deleted and removed from the user registry. The table that lists the users is refreshed, and the selected users are no longer displayed in the list.

Creating users
You can create one or more users. The users are added to the registry and a login account for each new user is automatically created. When creating the new user, you can also add the user as a member of one or more groups.

Duplicating group assignments for a user
You can search for users that match your search criteria. After selecting one or more users, these users can be added as members of the same groups that another existing user is already a member of. For example, if all the members of a department need to belong to the same groups as the department manager, you can duplicate the groups that the manager belongs to for all the other users that you choose.

Administering user groups for Web applications

Use the functions of the Web console to administer user groups for the Network Manager Web applications.

From the left navigation pane, click **Manage Groups**. Before you can perform some tasks for groups, you must first search for existing groups that match the search criteria that you specify. After the search completes, a table displays the groups that match your search criteria. To manage groups, you can perform these tasks:

Related concepts:

"User groups" on page 47
Use groups to organize users into units with common functional goals. Several Network Manager groups are created on installation.

Creating groups
You can create one or more groups. The group names and descriptions are added to the user registry.

Deleting groups
You can search for and list the existing group names that match the search criteria that you specify. After selecting one or more groups, you can delete them and remove the group names from the user registry.

Duplicating group assignments for a group
You can search for groups that match the search criteria that you specify. After selecting one or more groups, these groups can be members of the same groups as another existing group. For example, if all groups at the Austin site should belong to the same groups as an existing group, you can duplicate the groups that the one group belongs to for all the other groups that you choose.

Customized search filters for groups
You can create a filtered list of groups by specifying the type of filter and the

text to be used as part of the search criteria. The list of groups will be limited because only the groups that meet the extended search criteria will be displayed.

Changing the display options for the list of groups
You can change how the search results are displayed when viewing the list of groups. For example, you can change the number of groups to be viewed per page.

Searching for groups

You can search for existing groups that match the search criteria that you specify.

1. From the navigation pane, click **Manage Groups**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group name**.
3. In the **Search for** field, either type the string that you want to search for to limit the set of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes, a table is displayed that lists the group names that match your search criteria. Descriptions, if any, are also provided.

   Creating groups
   You can create one or more groups. The group names and descriptions are added to the user registry.

   Deleting groups
   You can search for and list the existing group names that match the search criteria that you specify. After selecting one or more groups, you can delete them and remove the group names from the user registry.

   Duplicating group assignments for a group
   You can search for groups that match the search criteria that you specify. After selecting one or more groups, these groups can be members of the same groups as another existing group. For example, if all groups at the Austin site should belong to the same groups as an existing group, you can duplicate the groups that the one group belongs to for all the other groups that you choose.

   Customized search filters for groups
   You can create a filtered list of groups by specifying the type of filter and the text to be used as part of the search criteria. The list of groups will be limited because only the groups that meet the extended search criteria will be displayed.

   Changing the display options for the list of groups
   You can change how the search results are displayed when viewing the list of groups. For example, you can change the number of groups to be viewed per page.

Customizing search filters for groups

You can create a filtered list of groups by specifying the type of filter and the text to be used as part of the search criteria. The list of groups will be limited because only the groups that meet the extended search criteria will be displayed.

1. From the navigation pane, click **Manage Groups**.

2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group name**.

3. In the **Search for** field, either type the string that you want to search for to limit the set of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.

4. In the **Maximum results** field, specify the maximum number of search results that you want to display.

5. Click **Search**. After the search completes, a table displays the groups that match your search criteria.

6. Click the ⊞ filter icon.

7. Do one of the following:

   - To create a new filter for an attribute if none exists, click the **[No Filter]** link.

   - To select an existing filter for an attribute, click on the filter name link.

8. If you are creating a new filter, select a filter type from the list. The types of filters are Contains, Starts with, or Ends with.

9. Type the letters that you want to search for in the **Text** field. The wildcard character is not permitted in this field.

10. Click **Apply**. The list of groups is refreshed and a filtered list of group names displays. The filter name and the total number of filtered group names are also shown.

11. Click the ⊞ hide filter icon, or click **Close**, when you have finished working with filters.

If no filter has been applied for an attribute, the text [No Filter] displays. If you click **Apply**, the name of the filter is listed in the column under the attribute. The filter name matches the letters that were typed in the **Text** field.

Searching for groups
You can search for existing groups that match the search criteria that you specify.

Changing the display options for the list of groups
You can change how the search results are displayed when viewing the list of groups. For example, you can change the number of groups to be viewed per page.

Changing the display options for the list of groups

You can change how the search results are displayed when viewing the list of groups. For example, you can change the number of groups to be viewed per page.

1. From the navigation pane, click **Manage Groups**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group name**.
3. In the **Search for** field, either type the string that you want to search for to limit the set of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes a table displays the groups that match your search criteria.
6. Click the ![icon] options icon.
7. If you want to view more or fewer entries on a page, change the number in the **Entries per page** field, and click **Apply**.
8. If you want to see the group names on a different page, type the page number in the field at the bottom of the list, and click **Go** to jump to that page.
9. Click the ![icon] hide options icon, or click **Close**, after changing the display options for the list of groups.

   Searching for groups
   You can search for existing groups that match the search criteria that you specify.

   Customizing search filters for groups
   You can create a filtered list of groups by specifying the type of filter and the text to be used as part of the search criteria. The list of groups will be limited because only the groups that meet the extended search criteria will be displayed.

Creating groups

You can create one or more groups. The group names and descriptions are added to the user registry.

1. Complete the steps in "Searching for groups" on page 61.
2. Click **Create** to create a new group.
3. In the **Group name** field, type a name to be used to identify the group. This group name will be added to the user registry. For example, you might type `ibm`
4. Optional: In the **Description** field, type a brief description for the group to distinguish this group from other groups. This description will be added to the user registry. The description must be an alphanumeric string with characters that are part of the local code set. For example, `Users and groups, CNC Company Dept 047`
5. Click **Create** to add the group name and the description, if entered, to the user registry. If successful, a message displays indicating that the group has been created.
6. To create another group, click **Create Another**.
7. Repeat the process until all the new groups have been created.

Deleting groups
You can search for and list the existing group names that match the search criteria that you specify. After selecting one or more groups, you can delete them and remove the group names from the user registry.

Duplicating group assignments for a group
You can search for groups that match the search criteria that you specify. After selecting one or more groups, these groups can be members of the same groups as another existing group. For example, if all groups at the Austin site should belong to the same groups as an existing group, you can duplicate the groups that the one group belongs to for all the other groups that you choose.

Viewing information about a group

You can view information about a specific group.

1. From the navigation pane, click **Manage Groups**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group name**.
3. In the **Search for** field, either type the string that you want to search for to limit the set of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes, the groups that match your search criteria are displayed as hypertext links.
6. Click on one of the group name links to view the information about the selected group. You can only view the information, you cannot change it.
7. Click **Cancel** after viewing to return to the previous window.

Adding a group to other groups
Before you can add a group to other groups, you must first search for the groups in which you want the group to be a member.

Changing information about a group
You can change the information about a specific group. You can change the name of the group, add a new description for the group if none exits, or change the existing description.

Viewing the groups the group is a member of
You can view a list of existing groups that the specified group is currently a member of.

Changing information about a group

You can change the information about a specific group. You can change the name of the group, add a new description for the group if none exits, or change the existing description.

1. From the navigation pane, click **Manage Groups**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group name**.
3. In the **Search for** field, either type the string that you want to search for to limit the set of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.

5. Click **Search**. After the search completes, the groups that match your search criteria are displayed in the column as hypertext links.
6. Click on one of the group links to change information about the group, as needed.
7. Optional: In the **Group name** field, enter a different name for the group, if needed.
8. Optional: In the **Description** field, enter a different description that the existing description, or enter a new description if none currently exists, if needed.
9. To save the changes, either click **OK** to save and return to the previous window, or click **Apply** to save but remain on the same window.

   Viewing information about a group
   You can view information about a specific group.

   Viewing the groups the group is a member of
   You can view a list of existing groups that the specified group is currently a member of.

Viewing the groups the group is a member of

You can view a list of existing groups that the specified group is currently a member of.

1. From the navigation pane, click **Manage Groups**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group name**.
3. In the **Search for** field, either type the string that you want to search for to limit theset of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes, a table displays a list of groups, as hypertext links, that match your search criteria.
6. Click the group name link to see the group properties.
7. Click the **Groups** tab to see the list of groups, in ascending order, that the group is currently a member of.

   Adding a group to other groups
   Before you can add a group to other groups, you must first search for the groups in which you want the group to be a member.

   Changing information about a group
   You can change the information about a specific group. You can change the name of the group, add a new description for the group if none exits, or change the existing description.

   Viewing information about a group
   You can view information about a specific group.

   Viewing the members of a group
   You can search for a list of users and groups that are existing members of a specific group.

Adding a group to other groups

Before you can add a group to other groups, you must first search for the groups in which you want the group to be a member.

1. Complete the steps in "Viewing the groups the group is a member of" on page 65.
2. Confirm that the group in the **Group name** field is the group that you want to add to other groups.
3. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group name**.
4. In the **Search for** field, either type the string that you want to search if for to limit the set of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
5. In the **Maximum results** field, specify the maximum number of search results that you want to display.
6. Click **Search** . After the search completes, a list is displayed of the groups that match your search criteria.
7. Highlight one or more groups to select them, and click **Add**.

   Viewing the members of a group
   You can search for a list of users and groups that are existing members of a specific group.

Viewing a list of members of a group

You can search for a list of users and groups that are existing members of a specific group.

1. From the navigation pane, click **Manage Groups**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group names** to locate groups by searching by their group names.
3. In the **Search for** field, either type the string that you want to search for to limit the set of groups, or use the wildcard character (*) to search for all groups.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search is complete, a table displays a list of the groups that match the search criteria.
6. Select the check box next to one group.
7. Click the **Members** tab to view the users and groups that are existing members of the specified group. Icons are used to help distinguish a user ![user icon] from a group ![group icon] member.

   Adding more groups as members of a group
   After viewing the list of members in a group that you specify, you can add more groups.

   Adding more users as members of a group
   You can add more users as members of a group.

   Removing members from a group
   After searching for the list of members in a group that you specify, you can remove users and groups as members from the group.

Removing a user from other groups

After searching for the groups in which the user is currently a member, you can remove the user from membership in groups that you select.

1. Complete the steps in "Viewing the groups the user is a member of" on page 56.
2. Confirm that the user in the **User ID** field is the user that you want to remove from other groups.
3. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group name**.
4. In the **Search for** field, either type the string that you want to search for to limit the set of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
5. In the **Maximum results** field, specify the maximum number of search results that you want to display.
6. Click **Search** to begin the search. After the search completes, a table displays the groups that match your search criteria.
7. Select the check boxes next to one or more groups, and then click **Remove**.

   Adding a user to other groups
   You can add a user as a member to selected groups.

   Changing group membership for a user
   You can search for and list the existing groups that match the search criteria. When creating a new user, you can choose the groups from the search results list in which you want the user to be a member.

   Changing information about a user
   You can change information about a specific user, such as the e-mail address. You can update the e-mail address, change the first or last name information, or set a new password.

   Viewing information about a user
   You can view information about a specific user.

   Viewing the groups the group is a member of
   You can view a list of existing groups that the specified user is currently a member of.

Adding more groups as members of a group

After viewing the list of members in a group that you specify, you can add more groups.

1. After completing the steps in "Viewing a list of members of a group" on page 66, click **Add Groups**.
2. Confirm that the **Group name** field displays the name of the group to which you want to add more groups as members.
3. In the **Search by** field, select the attribute from the list that you want to use to search by. For example, select **Group name**.
4. In the **Search for** field, either type the string that you want to search for to limit the set of groups, or use the wildcard character (*) to search for all groups.
5. In the **Maximum results** field, specify the maximum number of search results that you want to display.
6. Click **Search**. After the search is complete, a list of the groups that matched your search criteria is displayed.

7. Highlight one or more groups in the list to select them, and then click **Add**.

The groups are immediately added to the list of members.

Adding more groups as members of a group
You can add more users as members of a group.

Removing members from a group
After searching for the list of members in a group that you specify, you can remove users and groups as members from the group.

Removing members from a group

After searching for the list of members in a group that you specify, you can remove users and groups as members from the group.

1. Complete the steps in "Viewing a list of members of a group" on page 66.
2. Confirm that the **Group name** field displays the name of the group from which you want to remove members.
3. Select the check boxes next to one or more group members.
4. Click **Remove**.
5. Click **Remove** again when queried to confirm the removal of the selected members from the group. The members are immediately removed and are no longer displayed in the table.

Adding more users as members of a group
You can add more users as members of a group.

Adding more groups as members of a group
After viewing the list of members in a group that you specify, you can add more groups.

Duplicating group assignments for a group

You can search for groups that match the search criteria that you specify. After selecting one or more groups, these groups can be members of the same groups as another existing group. For example, if all groups at the Austin site should belong to the same groups as an existing group, you can duplicate the groups that the one group belongs to for all the other groups that you choose.

1. Complete the steps in "Searching for groups" on page 61.
2. Select the check boxes next to one or more groups that you want to assign the same membership as another group.
3. Choose the **Duplicate Group Assignments** action.
4. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group name**.
5. In the **Search for** field, either type the string that you want to search for to limit the set of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
6. In the **Maximum results** field, specify the maximum number of search results that you want to display.
7. Click **Search**. After the search has been completed, a table displays the groups that match your search criteria.
8. Highlight the name of the group whose group whose group assignment is to be duplicated for the previously selected groups, and click **OK**. The group membership of the group is duplicated for the previously selected groups

Creating groups
You can create one or more groups. The group names and descriptions are added to the user registry.

Deleting groups
You can search for and list the existing group names that match the search criteria that you specify. After selecting one or more groups, you can delete them and remove the group names from the user registry.

Deleting groups

You can search for and list the existing group names that match the search criteria that you specify. After selecting one or more groups, you can delete them and remove the group names from the user registry.

1. From the navigation pane, click **Manage Groups**.
2. In the **Search by** field, select the attribute from the list that you want to use to search for one or more groups. For example, select **Group name**.
3. In the **Search for** field, either type the string that you want to search for a limited set of groups, or use the wildcard character (*) to search for all groups. Whether the search is case sensitive or case insensitive depends on the user registry that you are using.
4. In the **Maximum results** field, specify the maximum number of search results that you want to display.
5. Click **Search**. After the search completes, a table is displayed that lists the group names that match your search criteria. Descriptions, if any, are also provided.
6. Select the check boxes next to the groups that you want to delete.
7. Click **Delete**.
8. Click **Delete** again when asked to confirm the deletion. The groups are immediately deleted and removed from the user registry. The table that lists the groups is refreshed, and the selected groups are no longer displayed in the list.

Creating groups
You can create one or more groups. The group names and descriptions are added to the user registry.

Duplicating group assignments for a group
You can search for groups that match the search criteria that you specify. After selecting one or more groups, these groups can be members of the same groups as another existing group. For example, if all groups at the Austin site should belong to the same groups as an existing group, you can duplicate the groups that the one group belongs to for all the other groups that you choose.

Considerations when changing a user ID

Changing a user ID in the console is equivalent to creating new user that is assigned only the default role of `iscusers`.

You can change a user ID in the Manage Users panel accessed through **Users and Groups** > **Manage Users**. If you change a user ID then it is equivalent to creating new user and the updated user ID is only assigned the default `iscusers` role. Additional roles for the updated user ID can be configured through **Users and Groups** > **User Roles**.

Important: If you change a user ID, any roles that were mapped for it, remain associated with the previous user ID. So if you intend to change or delete a user ID, you should first remove any role mappings that are associated with it. Once

you have made you change, you can re-apply the role mapping to the new user
ID.

Chapter 6. Administering system passwords

In addition to user passwords, Network Manager uses a number of passwords internally and when interacting with the network.

The following topics describe how to administer system passwords.

Note: All password encryption in Network Manager is performed using FIPS 140–2 compliant algorithms.

Encrypting or decrypting a password manually

If you set a password using a configuration file, you must encrypt or decrypt the password manually. By default the **ncp_crypt** command encrypts the password provided. However, if you specify the decrypt option, then the password is decrypted.

Complete these steps to encrypt or decrypt a password from the configuration file.

Note: All password encryption in Network Manager is performed using FIPS 140–2 compliant algorithms.

1. Stop Network Manager.
2. Encrypt or decrypt the required password from the command line using the **ncp_crypt** (**ncp_crypt.bat** on Windows systems) utility in the ITNMHOME/bin directory.

   ```
   ncp_crypt -password password [ -decrypt ] [ -help ] [ -version ]
   ```
3. Configure an insert in the relevant configuration file.
   a. Use the output from the **ncp_crypt** encryption utility.
   b. Set the value of the m_EncryptedPwd field to 1.
4. Restart Network Manager.

To encrypt the password, type the following command.

```
ncp_crypt -password mypassword
```

To decrypt a password you use the same utility that is used to encrypt the password, but with an additional command line argument.

```
ncp_crypt -decrypt -password @44:xXd7WUIC8teZDhLs8RQ1VjArw8HmUtNCwWs/VrVIxqI=@
```

Related tasks:

Chapter 1, "Starting and stopping Network Manager," on page 1
Your options for starting and stopping Network Manager are different depending on how the product has been installed.

Related reference:

"ncp_crypt command-line options" on page 149
Use the ncp_crypt command, with optional advanced arguments, to start ncp_crypt, the password encryption utility.

Changing the encryption key

You can change the encryption key that Network Manager uses when performing password encryption.

Before changing the encryption key, you must first decrypt all the passwords currently used in configuration files using the **ncp_crypt** (**ncp_crypt.bat** on Windows systems) utility in the ITNMHOME/bin directory:

```
ncp_crypt -password password -decrypt
```

Where *password* is the password to decrypt.

During installation of Network Manager, a 128–bit encryption key is generated and is stored in the following location: $NCHOME/etc/security/keys/conf.key. You can change the encryption key using the Tivoli Netcool/OMNIbus utility **nco_keygen**.

To change the encryption key:

1. Use the **nco_keygen** utility to generate a new encryption key. Ensure that you specify the output file as $NCHOME/etc/security/keys/conf.key.
2. Using the new encryption key, reencrypt all the passwords currently used in configuration files using the **ncp_crypt** utility by typing the following command.

   ```
   ncp_crypt -password password
   ```

   Where *password* is the password to encrypt.

Related reference:

"ncp_crypt command-line options" on page 149
Use the ncp_crypt command, with optional advanced arguments, to start ncp_crypt, the password encryption utility.

Deactivating password encryption

You can configure Network Manager to deactivate password encryption. If you do this then passwords entered using the GUIs are written to disk in plain text.

To deactivate password encryption:

1. Edit the **ncp_config** configuration file, ConfigSchema.cfg.
2. Configure the following insert to the config.settings table:

   ```
   insert into config.settings
   (
           m_EncryptPasswords,
           m_EncryptionKeyFile,
   )
   values
   (
           0,
           ""
   );
   ```

   The above insert specifies no encryption (m_EncryptPasswords = 0), and to use the default encryption key

List of passwords in Network Manager

Any password changes should be made using the Network Manager GUIs where possible.

By default, Network Manager encrypts all passwords entered using the Network Manager GUIs. Some passwords cannot be changed using a GUI and can only be changed by configuring insert statements in the relevant configuration file. If you set a password using a configuration file, you must encrypt the password manually.

The following table lists all the passwords in Network Manager, and specifies how to change the password.

Table 12. Network Manager passwords

Access required to	Password type	Description	Change using
Telnet	Privileged mode password	Configured as part of discovery configuration. Network Manager needs this password in order to access a network device using Telnet.	Network Discovery GUI
Telnet	Password	Configured as part of discovery configuration. Network Manager needs this password in order to access a network device using Telnet.	Network Discovery GUI
SNMP	Community string	Configured as part of discovery configuration. Network Manager needs this password in order to access a network device using SNMP.	Network Discovery GUI
SNMP	Version 3 Authentication password	Configured as part of discovery configuration. Network Manager needs this password in order to access a network device using SNMP.	Network Discovery GUI
SNMP	Version 3 Private password	Configured as part of discovery configuration. Network Manager needs this password in order to access a network device using SNMP.	Network Discovery GUI
NCIM Database	Password for command-line access to topology database	Provides access to the NCIM topology database.	The `$NCHOME/etc/ precision/ DbLogins. DOMAIN.cfg` and `$NCHOME/etc/ precision/ MibDbLogin.cfg` configuration files.

Table 12. Network Manager passwords (continued)

Access required to	Password type	Description	Change using
NCIM Database	Access settings used by Network Manager Web applications	You need the NCIM topology database password in order to use GUIs that query the NCIM database.	Database Access Configuration GUI
Tivoli Netcool/OMNIbus ObjectServer	ObjectServer secure password	The Event Gateway needs this password in order to access the ObjectServer for event enrichment activities.	Configuration file insert
Web applications	`tnm.properties` password	Allows GUI access to the NCIM database.	Web applications

Chapter 7. Administering management databases

Use either the GUI-based Management Database Access page or the OQL Service Provider to access the databases of any process.

Querying management databases using the Management Database Access page

Use the Management Database Access page to perform queries on Network Manager component databases.

Logging into the Management Database Access page

To log in to the Management Database Access page:
1. Log in to the Tivoli Integrated Portal.
2. Click **Administration** > **Network** > **Management Database Access**.

Issuing a query using the Management Database Access page

Use the Management Database Access page to issue simple and complex queries against Network Manager databases.

To issue a database query using the Management Database Access page:
1. Click **Administration** > **Network** > **Management Database Access**.
2. Specify a value for the following fields.

   Domain
   > Select the domain in which to issue the OQL query.

   Service
   > Select the service that you want to query.

3. To issue a single-line query, type the query in the **Query** field and click **Go**

   .

4. To issue a multiple-line query:

   a. Click **Advanced OQL Query** .
   b. Type the query in the **OQL Command** field and click **OK**.

   c. Click **Go** .

   Tip: To skip step 4c, append `;go` to multiple-line queries.

Listing the databases and tables of the current service

You can explore the databases of a service, the tables of those databases, and the columns of those tables.

Listing the databases of a service using the OQL Workbench

To display a list of the databases of the service you are logged into, use the **show databases** command.

To list the databases of a service:

1. Click **Administration** > **Network** > **Management Database Access**.
2. Specify a value for the following fields.

   Domain
   > Select the domain in which to issue the OQL query.

   Service
   > Select the service that you want to query.

3. Click **Advanced OQL Query** . In the **OQL Command** field, type the following query:

   ```
   show databases;
   go
   ```

Sample output

The following example output shows the databases of the ncp_model service:

```
{
        databases = [ 'dbModel', 'master', 'model', 'ncimCache' ]
}
```

Listing the tables of a database using the Management Database Access page

To display a list of the tables of a database, use the **show tables from** command.

To list the tables of a database:

1. Click **Administration** > **Network** > **Management Database Access**.
2. Specify a value for the following fields.

   Domain
   > Select the domain in which to issue the OQL query.

   Service
   > Select the service that you want to query.

3. Click **Advanced OQL Query** . In the **OQL Command** field, type the following query:

   ```
   show tables from
   database_name;
   go
   ```

Sample output

The following example output shows the tables of the master database:

```
{
        tables = [ 'entityByName', 'entityByNeighbor', 'containers' ]
}
```

Listing the columns of a database table using the Management Database Access page

You can display a list of the columns of a database table using the **show table** command.

To list the columns of a database table:

1. Click **Administration** > **Network** > **Management Database Access**.
2. Specify a value for the following fields.

   Domain
   > Select the domain in which to issue the OQL query.

   Service
   > Select the service that you want to query.

3. Click **Advanced OQL Query** ▫▫▫ . In the **OQL Command** field, type the following query:

   ```
   show table
   database_name.table_name;
   go
   ```

   database_name is the name of the database, and *table_name* is the name of the required table.

Sample output

The following example output shows the columns of the master.entityByName database:

```
{
        schema = {
            ObjectID = {
                DataType = 'long';
                NotNull = 'Y';
                PrimaryKey = 'Y';
                Indexed = 'N';
                Unique = 'Y';
                }
            EntityName = {
                Datatype = 'text';
                NotNull = 'Y';
                PrimaryKey = 'Y';
                Indexed = 'N';
                Unique = 'Y';
                };
.....
.....
        };
}
```

Querying management databases from the command line

You can use the OQL Service Provider to perform queries on Network Manager component databases.

Once you have logged into the OQL Service Provider, you can issue OQL statements to act on the databases of the service that you are logged into. You must terminate statements with a semi-colon (;) and the **go** keyword. You can also use the **send** keyword instead of **go**.

You can configure the OQL Service Provider to require authentication against NCIM or the ObjectServer. For more information, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Starting the OQL Service Provider

Start the OQL Service Provider in order to log into the databases of a given Network Manager process.

Type the following command:

```
ncp_oql -domain DOMAIN_NAME -service SERVICE_NAME [-username USERNAME ] [-password
 PASSWORD ] [ -latency LATENCY ]
```

In this command:
- *DOMAIN_NAME* is name of the domain to query.
- *SERVICE_NAME* is the name of the Network Manager process to query.
- *USERNAME* is the username to authenticate with. This argument is only required if the OQL Service Provider has been configured to require authentication.
- *PASSWORD* is the password to authenticate with. This argument is only required if the OQL Service Provider has been configured to require authentication.
- *LATENCY* is the maximum time in milliseconds (ms) that the service provider waits to connect to another Network Manager process using the messaging bus. This option is useful for large and busy networks where the default settings can cause processes to assume that there is a problem when in fact the communication delay is a result of network traffic. The default value is 3000 (equivalent to 3 seconds). You might want to increase this value as the default value might not be long enough to get a response from a large or busy OQL database.

Listing the databases and tables of the current service using the OQL Service Provider

You can explore the databases of a service, the tables of those databases, and the columns of those tables.

Listing the databases of a service using the OQL Service Provider

To display a list of the databases of the service you are logged into, use the **show databases** command.

To list the databases of a service using the OQL Service Provider
1. Start the OQL Service Provider.
2. Type the following query:

```
show databases;
go
```

Sample output

The following example output shows the databases of the ncp_model service:

```
{
        databases = [ 'master', 'translations' ]
}
```

Related tasks:

"Starting the OQL Service Provider" on page 78
Start the OQL Service Provider in order to log into the databases of a given Network Manager process.

Listing the tables of a database using the OQL Service Provider

To display a list of the tables of a database, use the **show tables from** command.

To list the tables of a database using the OQL Service Provider:
1. Start the OQL Service Provider.
2. Type the following query:

```
show tables from
database_name;
go
```

Sample output

The following example output shows the tables of the master database:

```
{
        tables = [ 'entityByName', 'entityByNeighbor', 'containers' ]
}
```

Related tasks:

"Starting the OQL Service Provider" on page 78
Start the OQL Service Provider in order to log into the databases of a given Network Manager process.

Listing the columns of a database table using the OQL Service Provider

You can list the columns of a database table using the **show table** command.

To issue a database table query using the OQL Service Provider:
1. Start the OQL Service Provider.
2. Type the following query:

```
show table
database_name.table_name;
go
```

database_name is the name of the database, and *table_name* is the name of the
required table.

Sample output

The following example output shows the columns of the master.entityByName
database:

```
{
        schema = {
            ObjectID = {
                DataType = 'long';
                NotNull = 'Y';
                PrimaryKey = 'Y';
                Indexed = 'N';
                Unique = 'Y';
                }
            EntityName = {
                Datatype = 'text';
                NotNull = 'Y';
                PrimaryKey = 'Y';
                Indexed = 'N';
                Unique = 'Y';
                };
.....
.....
        };
}
```

Related tasks:

"Starting the OQL Service Provider" on page 78
Start the OQL Service Provider in order to log into the databases of a given
Network Manager process.

Using OQL queries in scripts

You can launch the service provider in a special mode that executes a single
specified query and disconnects from the service provider.

This allows OQL queries to be used in scripts.

The following example shows the -query option in use.

```
ncp_oql -domain NCOMS -service Disco -query "select * from disco.status;"
```

The above example performs a single query on the disco.status database table
and disconnects from the OQL Service Provider. In order to perform this query, the
ncp_disco process would have to be running in the NCOMS domain, and the
specified user name and password combination would have to be valid.

Any acceptable OQL query can be specified with the -query option. The query
must be terminated with a semi-colon but not the **go** keyword.

Exiting the OQL Service Provider

When you have finished issuing OQL queries, exit the OQL Service Provider.

To exit the service provider, type the following command:
```
quit;
```

OQL Service Provider tips

OQL Service Provider provides a number of commands to facilitate interaction
with the command line.

Restriction: These commands only work in the OQL Service Provider. They do not
work in the Management Database Access page.

Show history of commands

Use the `hist` command to show the most recent commands.

Using the `hist` command, you can display up to the thousand (1,000) most recent
commands.

Sample

This sample shows how to use the `hist` command:
```
history

        1:      select * from services.unManaged;
        2:      select * from services.unManaged where serviceName like 'dh';
        3:      select count(*) from services.unManaged;
```

Execute a previous command

Use the ! command together with a number from the command history list to
repeat a recent command. Use the !! command to repeat the most recent
command.

Sample

This sample shows how to use the ! command:
```
history

        1:      select * from services.unManaged;
        2:      select * from services.unManaged where serviceName like 'dh';
        3:      select count(*) from services.unManaged;

!2
```

This executes the second command in the history list and produces the following
output:
```
{
        serviceName='ncp_dh_dns';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=23;
        processId=10734;
}
{
        serviceName='ncp_dh_snmp';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
```

```
                argList=['-domain','NCOMS'];
                serviceId=24;
                processId=10750;
        }
        {
                serviceName='ncp_dh_arp';
                servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
                argList=['-domain','NCOMS'];
                serviceId=25;
                processId=10872;
        }
        {
                serviceName='ncp_dh_telnet';
                servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
                argList=['-domain','NCOMS'];
                serviceId=52;
                processId=11424;
        }
        {
                serviceName='ncp_dh_ping';
                servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
                argList=['-domain','NCOMS'];
                serviceId=67;
                processId=13399;
        }
( 5 record(s) : Transaction complete )
```

Turn on tabular display mode

Use the `tabon` command to turn on tabular display mode.

Sample

This sample shows how to use the `tabon` command:

```
tabon
select * from services.unManaged where serviceName like 'dh';
go
```

This produces the following output:

```
+--------------+---------------------------------------+--------------------
| serviceName  | servicePath                           | argList
+--------------+---------------------------------------+--------------------
| ncp_dh_dns   | $PRECISION_HOME/platform/$PLATFORM/bin/ | ['-domain','NCOMS']
| ncp_dh_snmp  | $PRECISION_HOME/platform/$PLATFORM/bin/ | ['-domain','NCOMS']
| ncp_dh_arp   | $PRECISION_HOME/platform/$PLATFORM/bin/ | ['-domain','NCOMS']
| ncp_dh_telnet | $PRECISION_HOME/platform/$PLATFORM/bin/ | ['-domain','NCOMS']
| ncp_dh_ping  | $PRECISION_HOME/platform/$PLATFORM/bin/ | ['-domain','NCOMS']
+--------------+---------------------------------------+--------------------

----+----------+----------+
    | serviceId | processId |
----+----------+----------+
    | 23        | 10734     |
    | 24        | 10750     |
    | 25        | 10872     |
    | 52        | 11424     |
    | 67        | 13399     |
----+----------+----------+

( 5 record(s) : Transaction complete )
```

Turn off tabular display mode

Use the taboff command to turn off tabular display mode.

Sample

This sample shows how to use the tabon command:

```
taboff
select * from services.unManaged where serviceName like 'dh';
go
```

This produces the following output:

```
{
        serviceName='ncp_dh_dns';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=23;
        processId=10734;
}
{
        serviceName='ncp_dh_snmp';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=24;
        processId=10750;
}
{
        serviceName='ncp_dh_arp';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=25;
        processId=10872;
}
{
        serviceName='ncp_dh_telnet';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=52;
        processId=11424;
}
{
        serviceName='ncp_dh_ping';
        servicePath='$PRECISION_HOME/platform/$PLATFORM/bin/';
        argList=['-domain','NCOMS'];
        serviceId=67;
        processId=13399;
}
( 5 record(s) : Transaction complete )
```

OQL service names for processes

Each process that has associated databases has an OQL service name, which you use to log into the databases of the process.

To list all services, run **ncp_oql** with the -options option.

The following table lists all the OQL service names for the Network Manager processes.

Table 13. Processes and their OQL service names

Process	OQL service name
ncp_class	Class

Table 13. Processes and their OQL service names (continued)

Process	OQL service name
`ncp_config`	Config
`ncp_ctrl`	Ctrl
`ncp_disco`	Disco
`ncp_d_helpserv`	Helper
`ncp_g_event`	EventGateway
`ncp_g_event (RCA plugin)`	Amos
`ncp_model`	Model
`ncp_poller(default)`	SnmpPoller
`ncp_df_ping`	DiscoPingFinder
`ncp_dh_snmp`	SnmpHelper
`ncp_trapmux`	TrapMux
`ncp_virtualdomain`	VirtualDomain
`ncp_webtool`	WebTool
Service for the NCIM database **Restriction:** You cannot query ncim from the Management Database Access page.	ncim
Service for the ObjectServer **Restriction:** You cannot query ncim from the Management Database Access page.	ObjectServer

Chapter 8. Administering the NCIM topology database

Network topology information is held in the NCIM database.

Changing the hostname, port, or database name

If you change the details of the NCIM database, you might need to perform some configuration tasks to enable Network Manager to connect to the database.

Configuring GUI access to the topology database

If you have changed the NCIM settings, you must configure access for the Network Manager Web applications.

You only need to configure topology database access settings if the default settings configured by the installation process are not sufficient, for example, if you have changed the topology database.

To configure topology database access settings:
1. Click **Administration** > **Network** > **Database Access Configuration**. The Configure NCIM Database Access and the Configure Historical Polling Database Access portlets are displayed.
2. Enter the host that the database is installed on in the **Database Host** field. By default, this is the same host that Network Manager is installed on.
3. Enter the port used by the database in the **Database Port** field.
4. Enter the user name that was entered during installation of the database in the **Username** field.
5. Enter the password that was entered during installation of the database in the **Password** field.
6. Confirm the password.

Related reference:

"Topoviz screen is blank" on page 138
If Topoviz fails to start, or starts with a blank screen, refresh the browser window. If the Network Manager splash screen does not appear, check the topology database access settings.

Re-creating network views

If you create a new NCIM database schema and want your Network Manager GUI to use the new schema, you must configure the GUI to access the new database and you also need to re-create your network views.

Ensure you have configured GUI access to the new topology database.

Network views are auto-provisioned by the `default.xml` and `itnmuser.xml` files when installing Network Manager, and are then created in the database. However, if you do not create the topology database schemas during installation, or subsequently change your database, then you need to re-create your views.

To re-create network views:
1. Go to `NCHOME/precision/profiles/TIPProfile/etc/tnm/autoprovision`.

2. Rename the files called *filename*`.xml.processed` to *filename*`.xml`.
3. Save and close the files.

Changing NCIM details on DB2

If you change the hostname, port, or database name of the NCIM database on DB2, you must uncatalog and recatalog the database. Otherwise you will not be able to access the GUI.

See your DB2 documentation for instructions on configuring DB2.

To uncatalog and recatalog the database:

1. Uncatalog the database using the following command: UNIX

   `$NCHOME\precision\scripts\sql\db2\uncatalog_db2_database.sh` *database_name*

   Windows

   `%NCHOME%\precision\scripts\sql\db2\uncatalog_db2_database.bat` *database_name*

   where *database_name* is the name of the NCIM database.
2. Catalog the database using the following command:

   `%ITNMHOME%\scripts\sql\db2\catalog_db2_database.bat` *database_name host port*

   where *database_name* is the name of the NCIM database, *host* is the hostname of the server where NCIM is installed, and *port* is the port on which the NCIM database is running.

Creating the topology database schemas

You can set up the topology database during installation. If you need to set up a database after installation for an existing Network Manager, then you can do this manually using the scripts provided.

You must create the topology database before you can use Network Manager.

For information about creating the topology databases, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Creating Informix topology database schemas on UNIX

UNIX

You can use scripts provided by Network Manager to create the topology database schemas in an Informix database on UNIX.

To create the topology database:

1. Make sure you have followed the prerequisites for installing Informix, and install and configure the Informix database.
2. Optional: If you installed the Informix database on a different host from Network Manager, copy the `$ITNMHOME/scripts/sql/informix/create_informix_database.sh` script to the remote host where you installed Informix.
3. If you installed the Informix database on the same host as Network Manager, change to the `$ITNMHOME/scripts/sql/informix` directory.
4. Run the following script to create the databases:
   `./create_informix_database.sh` *database_name user_name*

where:

database_name
>Specifies the name of the database.

user_name
>Specifies the name of the database user that will be used to connect to the database.

>**Important:** This user must not be the administrative user. This user must be an existing operating system user.

For example, to create an Informix database called "NCIM" for the Informix user "ncim", type `./create_informix_database.sh NCIM ncim`.

5. Go to the machine where you have Network Manager installed and change to the `$ITNMHOME/scripts/sql` directory.

6. If your database is on a remote host, run the **create_all_schemas.sh** command as the administrative user as follows: `./create_all_schemas.sh` *database_type database_name host user_name password port*

   where:

   database_type
   >Identifies the type of database to create. In this case, it is `informix`.

   database_name
   >Specifies the name of the database. For Informix the format must be *server_name.database_name*, where the *server_name* is the name of the Informix server and not the host name.

   host   Specifies the server host name or IP address where the database is installed.

   user_name
   >Identifies the user that will be used to connect to the database.

   password
   >Provides the password for the user.

   port   Specifies the port used by the database.

7. If your database is on the same host as Network Manager, go to `$ITNMHOME/scripts/sql/informix` and run the following script to populate the databases:

   `./populate_informix_database.sh` *database_name* `> populate.log 2>&1`

8. Examine the `populate.log` file for any errors.

9. Run the `$ITNMHOME/bin/ncp_mib` command to ensure that the ncmib database is fully populated with SNMP data from the MIBs before a discovery is run.

10. If you want your Network Manager GUI to use the database schema you created, then you need to configure access to the new topology database schema and re-create your network views (see related tasks later in this section).

Related tasks:

"Configuring GUI access to the topology database" on page 85
If you have changed the NCIM settings, you must configure access for the
Network Manager Web applications.

"Re-creating network views" on page 85
If you create a new NCIM database schema and want your Network Manager GUI
to use the new schema, you must configure the GUI to access the new database
and you also need to re-create your network views.

Creating Informix topology database schemas on Windows

Windows

You can use scripts provided by Network Manager to create the topology database
schemas in an Informix database on Windows.

To create the topology database:

1. Make sure you have followed the prerequisites for installing Informix, and
   install and configure the Informix database.
2. Optional: If you installed the Informix database on a different host from
   Network Manager, copy the `%ITNMHOME%\scripts\sql` directory and its contents
   from the Network Manager server to the remote host where you installed
   Informix.
3. On the host where the database is installed, open a command prompt and
   change to the `%ITNMHOME%\scripts\sql\informix` directory.
4. Run the following script to create the databases: `create_informix_database.bat`
   `database_name user_name`

   where:

   database_name
   > Specifies the name of the database.

   user_name
   > Specifies the name of the database user that will be used to connect to
   > the database.
   >
   > **Important:** This user must not be the administrative user. This user
   > must be an existing operating system user.

   For example, to create a Informix database called "NCIM" for the Informix user
   "ncim", type `create_informix_database.bat NCIM ncim`.
5. Run the following script to populate the databases::

   `populate_informix_database.bat` `database_name` `> populate.log 2>&1`
6. Examine the `populate.log` file for any errors.
7. Run the `%ITNMHOME%\bin\ncp_mib` command to ensure that the ncmib database
   is fully populated with SNMP data from the MIBs before a discovery is run.
8. If you want your Network Manager GUI to use the database schema you
   created, then you need to configure access to the new topology database
   schema and re-create your network views (see related tasks later in this
   section).

Related tasks:

"Configuring GUI access to the topology database" on page 85
If you have changed the NCIM settings, you must configure access for the
Network Manager Web applications.

"Re-creating network views" on page 85
If you create a new NCIM database schema and want your Network Manager GUI
to use the new schema, you must configure the GUI to access the new database
and you also need to re-create your network views.

Creating DB2 topology database schemas on UNIX

> UNIX

You can use scripts provided by Network Manager to create the topology database
schemas in a DB2 database on UNIX.

To create the topology database:
1. Make sure you have followed the prerequisites for installing DB2, and install
   and configure the DB2 database.
2. Optional: If you installed the DB2 database on a different host from Network
   Manager, copy the `$ITNMHOME/scripts/sql/db2/create_db2_database.sh` script
   to the remote host where you installed DB2.
3. If you installed the DB2 database on the same host as Network Manager,
   change to the `$ITNMHOME/scripts/sql/db2` directory.
4. Run the script as the DB2 administrative user by typing the following
   command: `./create_db2_database.sh` *database_name user_name* `-force`

   where:

   database_name
   > Is the required name of the database

   user_name

   > Is the DB2 user that will be used to connect to the database

   > **Important:** This user must not be the administrative user. This user
   > must be an existing operating system and DB2 user.

   -force Is an optional argument that forces any DB2 users off the instance
   before the database is created.

   For example, to create a DB2 database called "NCIM" for the DB2 user
   "ncim", type:

   `./create_db2_database.sh NCIM ncim`
5. Go to the machine where you have Network Manager installed and change to
   the `$ITNMHOME/scripts/sql` directory.
6. If your database is on a remote host, run the **create_all_schemas.sh**
   command as the administrative user as follows: `./create_all_schemas.sh`
   database_type database_name host user_name password port

   where:

   database_type
   > Identifies the type of database to create. In this case, it is `db2`.

   database_name
   > Specifies the name of the database.

host	Specifies the server host name or IP address where the database is installed.

user_name
Identifies the DB2 user that will be used to connect to the database.

Important: This user must not be the administrative user. This user must be an existing operating system and DB2 user.

password
Provides the password for the user.

port	Specifies the port used by the database.

7. If your database is on the same host as Network Manager, go to `$ITNMHOME/scripts/sql/db2` and run the following script to populate the databases:

    `./populate_db2_database.sh` *database_name user_name password* `> db2.log 2>&1`

8. Examine the `db2.log` file for any errors.

9. Login as the DB2 administrator on the DB2 client running on the Tivoli Integrated Portal server.

10. Run the following script to catalog the database: `$ITNMHOME/scripts/sql/db2/` `catalog_db2_database.sh` *database_name host port*

    where:

    database_name
    Is the name of the NCIM database

    host	Is the host name of the server where NCIM is installed.

    port	Is the port on which the NCIM database is running.

    The following command shows an example usage of the script:

    `./catalog_db2_database.sh ITNM db2server.ibm.com 50000`

11. Run the `$ITNMHOME/bin/ncp_mib` command to ensure that the ncmib database is fully populated with SNMP data from the MIBs before a discovery is run.

12. If you want your Network Manager GUI to use the database schema you created, then you need to configure access to the new topology database schema and re-create your network views (see related tasks later in this section).

Related tasks:

"Configuring GUI access to the topology database" on page 85
If you have changed the NCIM settings, you must configure access for the Network Manager Web applications.

"Re-creating network views" on page 85
If you create a new NCIM database schema and want your Network Manager GUI to use the new schema, you must configure the GUI to access the new database and you also need to re-create your network views.

Creating DB2 topology database schemas on Windows

You can use scripts provided by Network Manager to create the topology database schemas in a DB2 database on Windows.

To create the topology database:

1. Make sure you have followed the prerequisites for installing DB2, and install and configure the DB2 database.
2. Optional: If you installed the DB2 database on a different host from Network Manager, copy the `%ITNMHOME%\scripts\sql` directory and its contents from the Network Manager server to the remote host where you installed DB2.
3. On the host where the database is installed, open a command prompt and change to the `%ITNMHOME%\scripts\sql\db2` directory.
4. Run the following script as an administrative user to create the databases:
   `create_db2_database.bat` *database_name user_name* `-force`
   where:

   database_name
   > Is the required name of the database

   user_name

   > Is the DB2 user that will be used to connect to the database

   > **Important:** This user must not be the administrative user. This user must be an existing operating system and DB2 user.

   -force Is an optional argument that forces any DB2 users off the instance before the database is created.

   For example, to create a DB2 database called "NCIM" for the DB2 user "ncim", type:

   `create_db2_database.bat NCIM ncim`.

5. Run the following script to populate the databases:
   `populate_db2_database.bat` *database_name user_name password* `> db2.log 2>&1`
6. Examine the `db2.log` file for any errors.
7. Login as the DB2 administrator on the DB2 client running on the Tivoli Integrated Portal server.
8. Run the following script to catalog the database: `catalog_db2_database.bat` *database_name host port*
   where:

   database_name
   > Is the name of the NCIM database

   host Is the host name of the server where NCIM is installed.

   port Is the port on which the NCIM database is running.

   The following command shows an example usage of the script:

   `catalog_db2_database.bat ITNM db2server.ibm.com 50000`

9. Run the `%ITNMHOME%\bin\ncp_mib` command to ensure that the ncmib database is fully populated with SNMP data from the MIBs before a discovery is run.

10. If you want your Network Manager GUI to use the database schema you created, then you need to configure access to the new topology database schema and re-create your network views (see related tasks later in this section).

Related tasks:

"Configuring GUI access to the topology database" on page 85
If you have changed the NCIM settings, you must configure access for the Network Manager Web applications.

"Re-creating network views" on page 85
If you create a new NCIM database schema and want your Network Manager GUI to use the new schema, you must configure the GUI to access the new database and you also need to re-create your network views.

Creating MySQL topology database schemas on UNIX

UNIX

You can use scripts provided by Network Manager to create the topology database schemas in a MySQL database on UNIX.

To create the topology database:

1. Make sure you have followed the prerequisites for installing MySQL, and install and configure the MySQL database.
2. Optional: If you installed the MySQL database on a different host from Network Manager, copy the `$ITNMHOME/scripts/sql/mysql/create_mysql_database.sh` script to the remote host where you installed MySQL.
3. If you installed the MySQL database on the same host as Network Manager, change to the `$ITNMHOME/scripts/sql/mysql` directory.
4. Run the following script to create the databases and grant permissions to the `ncim` user to access them:

   `./create_mysql_database.sh root password prefix`

   You can also specify an optional *prefix* value here that applies a prefix to schema names. This is useful when creating multiple sets of NCIM schemas in the same database. If you use prefixes, you must also update the following files to include the prefix for each schema name reference; unless otherwise stated, update the following files after base or fix pack installations:
   - `tnm.properties`
   - `ncpolldata.properties` (no update needed for fix packs)
   - `DbLogins.DOMAIN.cfg`
   - `MibDbLogins.cfg` (no update needed for fix packs or if only GUI components are installed)

   For example, when you have several domains and you use the prefix `abc` to determine the schema for a particular domain, you must then update the schema name references with the `abc` prefix for that domain, as shown for each `*schema*` property in the following sample from the `tnm.properties` file (the `abc` prefix highlighted in bold):

   ```
   tnm.trace.maxsize=10
   tnm.database.schema.ncmib=abcncmib
   tnm.trace.count=1
   tnm.graph.missedViewRefreshIntervals=20
   tnm.trace.filename=ncp_guiconfig.%g.trace
   tnm.log.count=1
   ```

```
tnm.database.type=oracle
tnm.oql.response.poll.timeout=120000
tnm.oql.response.poll.delay=100
tnm.database.schema.ncim=abcncim
tnm.graph.maxFailedRequests=15
tnm.fips.key.location=encryption/keys/crypt.key
tnm.graph.poller=DEFAULT_POLLER
tnm.database.schema.ncpgui=abcncpgui
tnm.database.port=1521
tnm.database.schema.ncmonitor=abcncmonitor
tnm.graph.viewRefreshInterval=15000
tnm.fips.mode=false
tnm.database.host=cb1v2
tnm.log.maxsize=10
tnm.log.filename=ncp_guiconfig.%g.log
tnm.database.dbname=ITNMIP39
tnm.graph.historicalViewRefreshInterval=30000
tnm.database.password=abcncim
tnm.log.level=INFO
tnm.database.password.encrypted=false
tnm.oql.timeout=30000
tnm.database.username=abcncim
```

5. Go to the machine where you have Network Manager installed and change to the $ITNMHOME/scripts/sql directory.

6. If your database is on a remote host, run the **create_all_schemas.sh** command as the administrative user as follows: **./create_all_schemas.sh** *database_type database_name host user_name password port prefix*

   where:

   database_type
   : Identifies the type of database to create. In this case, it is mysql.

   database_name
   : Specifies the name of the database.

   host Specifies the server host name or IP address where the database is installed.

   user_name
   : Identifies the user that will be used to connect to the database.

   password
   : Provides the password for the user.

   port Specifies the port used by the database.

   prefix Is an optional argument that if specified applies a prefix to schema names. This is useful when creating multiple sets of NCIM schemas in the same database. If used, the value must be the same prefix as the one set when running the **create_mysql_database.sh** script.

7. If your database is on the same host as Network Manager, go to $ITNMHOME/scripts/sql/mysql and run the following script to create the tables within the databases:

   ```
   ./populate_mysql_database.sh root password
   ```

8. Run the $ITNMHOME/bin/ncp_mib command to ensure that the ncmib database is fully populated with SNMP data from the MIBs before a discovery is run.

9. If you want your Network Manager GUI to use the database schema you created, then you need to configure access to the new topology database schema and re-create your network views (see related tasks later in this section).

Related tasks:

"Configuring GUI access to the topology database" on page 85
If you have changed the NCIM settings, you must configure access for the
Network Manager Web applications.

"Re-creating network views" on page 85
If you create a new NCIM database schema and want your Network Manager GUI
to use the new schema, you must configure the GUI to access the new database
and you also need to re-create your network views.

Creating MySQL topology database schemas on Windows

Windows

You can use scripts provided by Network Manager to create the topology database
schemas in a MySQL database on Windows.

To create the topology database:

1. Make sure you have followed the prerequisites for installing MySQL, and
   install and configure the MySQL database.
2. Optional: If you installed the MySQL database on a different host from
   Network Manager, copy the `%ITNMHOME%\scripts\sql` directory and its contents
   from the Network Manager server to the remote host where you installed
   MySQL.
3. On the host where the database is installed, open a command prompt and
   change to the `%ITNMHOME%\scripts\sql\mysql` directory.
4. Run the script to create the databases and grant permissions to the `ncim` user to
   access them using the following commands:

   `create_mysql_database.bat root `*`password prefix`*

   You can also specify an optional *prefix* value here that applies a prefix to
   schema names. This is useful when creating multiple sets of NCIM schemas in
   the same database. If you use prefixes, you must also update the following files
   to include the prefix for each schema name reference; unless otherwise stated,
   update the following files after base or fix pack installations:

   - `tnm.properties`
   - `ncpolldata.properties` (no update needed for fix packs)
   - `DbLogins.`*`DOMAIN`*`.cfg`
   - `MibDbLogins.cfg` (no update needed for fix packs or if only GUI components
     are installed)

   For example, when you have several domains and you use the prefix `abc` to
   determine the schema for a particular domain, you must then update the
   schema name references with the `abc` prefix for that domain, as shown for each
   `*schema*` property in the following sample from the `tnm.properties` file (the
   `abc` prefix highlighted in bold):

   ```
   tnm.trace.maxsize=10
   tnm.database.schema.ncmib=abcncmib
   tnm.trace.count=1
   tnm.graph.missedViewRefreshIntervals=20
   tnm.trace.filename=ncp_guiconfig.%g.trace
   tnm.log.count=1
   tnm.database.type=oracle
   tnm.oql.response.poll.timeout=120000
   tnm.oql.response.poll.delay=100
   tnm.database.schema.ncim=abcncim
   tnm.graph.maxFailedRequests=15
   ```

```
tnm.fips.key.location=encryption/keys/crypt.key
tnm.graph.poller=DEFAULT_POLLER
tnm.database.schema.ncpgui=abcncpgui
tnm.database.port=1521
tnm.database.schema.ncmonitor=abcncmonitor
tnm.graph.viewRefreshInterval=15000
tnm.fips.mode=false
tnm.database.host=cb1v2
tnm.log.maxsize=10
tnm.log.filename=ncp_guiconfig.%g.log
tnm.database.dbname=ITNMIP39
tnm.graph.historicalViewRefreshInterval=30000
tnm.database.password=abcncim
tnm.log.level=INFO
tnm.database.password.encrypted=false
tnm.oql.timeout=30000
tnm.database.username=abcncim
```

5. Run the script to create the tables within the databases using the following commands:

   ```
   populate_mysql_database.bat root password
   ```

6. Run the `%ITNMHOME%\bin\ncp_mib` command to ensure that the ncmib database is fully populated with SNMP data from the MIBs before a discovery is run.

7. If you want your Network Manager GUI to use the database schema you created, then you need to configure access to the new topology database schema and re-create your network views (see related tasks later in this section).

Related tasks:

"Configuring GUI access to the topology database" on page 85
If you have changed the NCIM settings, you must configure access for the Network Manager Web applications.

"Re-creating network views" on page 85
If you create a new NCIM database schema and want your Network Manager GUI to use the new schema, you must configure the GUI to access the new database and you also need to re-create your network views.

Creating Oracle topology database schemas on UNIX

UNIX

You can use scripts provided by Network Manager to create the topology database schemas in an Oracle database on UNIX.

To create the topology database:

1. Make sure you have followed the prerequisites for installing Oracle, and install and configure the Oracle database.

2. Optional: If you installed the Oracle database on a different host from Network Manager, copy the `$ITNMHOME/scripts/sql/oracle/create_oracle_database.sh` script to the remote host where you installed Oracle.

3. If you installed the Oracle database on the same host as Network Manager, change to the `$ITNMHOME/scripts/sql/oracle` directory.

4. Run the following script to create the databases: `./create_oracle_database.sh user_name password prefix`

   where:

user_name

> Specifies the name of the database user that will be used to connect to the database.

password

> Specifies the password of the database user.

prefix

> You can also specify an optional *prefix* value here that applies a prefix to schema names. This is useful when creating multiple sets of NCIM schemas in the same database. If you use prefixes, you must also update the following files to include the prefix for each schema name reference; unless otherwise stated, update the following files after base or fix pack installations:
>
> - `tnm.properties`
> - `ncpolldata.properties` (no update needed for fix packs)
> - `DbLogins.DOMAIN.cfg`
> - `MibDbLogins.cfg` (no update needed for fix packs or if only GUI components are installed)
>
> For example, when you have several domains and you use the prefix abc to determine the schema for a particular domain, you must then update the schema name references with the abc prefix for that domain, as shown for each `*schema*` property in the following sample from the `tnm.properties` file (the abc prefix highlighted in bold):
>
> ```
> tnm.trace.maxsize=10
> tnm.database.schema.ncmib=abcncmib
> tnm.trace.count=1
> tnm.graph.missedViewRefreshIntervals=20
> tnm.trace.filename=ncp_guiconfig.%g.trace
> tnm.log.count=1
> tnm.database.type=oracle
> tnm.oql.response.poll.timeout=120000
> tnm.oql.response.poll.delay=100
> tnm.database.schema.ncim=abcncim
> tnm.graph.maxFailedRequests=15
> tnm.fips.key.location=encryption/keys/crypt.key
> tnm.graph.poller=DEFAULT_POLLER
> tnm.database.schema.ncpgui=abcncpgui
> tnm.database.port=1521
> tnm.database.schema.ncmonitor=abcncmonitor
> tnm.graph.viewRefreshInterval=15000
> tnm.fips.mode=false
> tnm.database.host=cb1v2
> tnm.log.maxsize=10
> tnm.log.filename=ncp_guiconfig.%g.log
> tnm.database.dbname=ITNMIP39
> tnm.graph.historicalViewRefreshInterval=30000
> tnm.database.password=abcncim
> tnm.log.level=INFO
> tnm.database.password.encrypted=false
> tnm.oql.timeout=30000
> tnm.database.username=abcncim
> ```

5. Go to the machine where you have Network Manager installed and change to the `$ITNMHOME/scripts/sql` directory.

6. If your database is on a remote host, run the **create_all_schemas.sh** command as the administrative user as follows: `./create_all_schemas.sh` *database_type database_name host user_name password port prefix*

   where:

database_type
> Identifies the type of database to create. In this case, it is `oracle`.

database_name
> Specifies the name of the database. For Oracle, this must be the SID.

host Specifies the server host name or IP address where the database is installed.

user_name
> Identifies the user that will be used to connect to the database.

password
> Provides the password for the user.

port Specifies the port used by the database.

prefix Is an optional argument that if specified applies a prefix to schema names. This is useful when creating multiple sets of NCIM schemas in the same database. If used, the value must be the same prefix as the one set when running the **create_oracle_database.sh** script.

7. If your database is on the same host as Network Manager, go to `$ITNMHOME/scripts/sql/oracle` and run the following script to populate the databases:

   `./populate_oracle_database.sh` *database_user_name password* `> oracle.log 2>&1`

8. Examine the `oracle.log` file for any errors.

9. Run the `$ITNMHOME/bin/ncp_mib` command to ensure that the ncmib database is fully populated with SNMP data from the MIBs before a discovery is run.

10. If you want your Network Manager GUI to use the database schema you created, then you need to configure access to the new topology database schema and re-create your network views (see related tasks later in this section).

Related tasks:

"Configuring GUI access to the topology database" on page 85
If you have changed the NCIM settings, you must configure access for the Network Manager Web applications.

"Re-creating network views" on page 85
If you create a new NCIM database schema and want your Network Manager GUI to use the new schema, you must configure the GUI to access the new database and you also need to re-create your network views.

Creating Oracle topology database schemas on Windows

Windows

You can use scripts provided by Network Manager to create the topology database schemas in an Oracle database on Windows.

To create the topology database:

1. Make sure you have followed the prerequisites for installing Oracle, and install and configure the Oracle database.

2. Optional: If you installed the Oracle database on a different host from Network Manager, copy the `%ITNMHOME%\scripts\sql` directory and its contents from the Network Manager server to the remote host where you installed Oracle.

3. On the host where the database is installed, open a command prompt and change to the `%ITNMHOME%\scripts\sql\oracle` directory.

4. Run the following command to create the databases: `sqlplus`
   database_user_name password `< create_oracle_database.sql`

   where:

   database_user_name
   > Specifies the name of the database user that will be used to connect to the database.

   password
   > Specifies the password of the database user.

   prefix

   > You can also specify an optional *prefix* value here that applies a prefix to schema names. This is useful when creating multiple sets of NCIM schemas in the same database. If you use prefixes, you must also update the following files to include the prefix for each schema name reference; unless otherwise stated, update the following files after base or fix pack installations:
   > - `tnm.properties`
   > - `ncpolldata.properties` (no update needed for fix packs)
   > - `DbLogins.DOMAIN.cfg`
   > - `MibDbLogins.cfg` (no update needed for fix packs or if only GUI components are installed)

   > For example, when you have several domains and you use the prefix abc to determine the schema for a particular domain, you must then update the schema name references with the abc prefix for that domain, as shown for each `*schema*` property in the following sample from the `tnm.properties` file (the abc prefix highlighted in bold):

   ```
   tnm.trace.maxsize=10
   tnm.database.schema.ncmib=abcncmib
   tnm.trace.count=1
   tnm.graph.missedViewRefreshIntervals=20
   tnm.trace.filename=ncp_guiconfig.%g.trace
   tnm.log.count=1
   tnm.database.type=oracle
   tnm.oql.response.poll.timeout=120000
   tnm.oql.response.poll.delay=100
   tnm.database.schema.ncim=abcncim
   tnm.graph.maxFailedRequests=15
   tnm.fips.key.location=encryption/keys/crypt.key
   tnm.graph.poller=DEFAULT_POLLER
   tnm.database.schema.ncpgui=abcncpgui
   tnm.database.port=1521
   tnm.database.schema.ncmonitor=abcncmonitor
   tnm.graph.viewRefreshInterval=15000
   tnm.fips.mode=false
   tnm.database.host=cb1v2
   tnm.log.maxsize=10
   tnm.log.filename=ncp_guiconfig.%g.log
   tnm.database.dbname=ITNMIP39
   tnm.graph.historicalViewRefreshInterval=30000
   tnm.database.password=abcncim
   tnm.log.level=INFO
   tnm.database.password.encrypted=false
   tnm.oql.timeout=30000
   tnm.database.username=abcncim
   ```

5. Run the following script to populate the databases:

   `populate_oracle_database.bat` *database_user_name password* `> oracle.log 2>&1`

6. Examine the `oracle.log` file for any errors.

7. Run the `%ITNMHOME%\bin\ncp_mib` command to ensure that the ncmib database is fully populated with SNMP data from the MIBs before a discovery is run.
8. If you want your Network Manager GUI to use the database schema you created, then you need to configure access to the new topology database schema and re-create your network views (see related tasks later in this section).

Related tasks:

"Configuring GUI access to the topology database" on page 85
If you have changed the NCIM settings, you must configure access for the Network Manager Web applications.

"Re-creating network views" on page 85
If you create a new NCIM database schema and want your Network Manager GUI to use the new schema, you must configure the GUI to access the new database and you also need to re-create your network views.

Removing a domain from the topology database

When a domain is no longer required, it can be removed from the NCIM topology database using the `domain_drop.pl` script.

This will remove the entire topology for the domain from NCIM, along with any poll policies for the domain. Note that this script does not remove configuration information for the domain, and the cache of the topology will be unaffected.

To remove the domain from the topology database
1. Change to the following directory:
   `$NCHOME/precision/scripts/perl/scripts`
2. Run the following command:
   `NCHOME/precision/bin/ncp_perl domain_drop.pl -domain obsoletedomain -password password`
3. For further options, run the **domain_drop.pl** script with the `-help` command-line option.

Removing the topology database

You can remove the topology database if it is no longer required.

Before removing the topology database, you must stop all processes that connect to the database.

Removing a MySQL topology database on UNIX

UNIX

You can remove the MySQL database on UNIX using a script.

To remove the database:
1. Change to the scripts directory using the following command:
   `cd $NCHOME/precision/scripts/sql/mysql`
2. Execute the script using the following command:
   `drop_mysql_database.sh root password`

Removing a MySQL topology database on Windows

`Windows`

You can remove the MySQL database on Windows using a script.

To remove the database:
1. Change to the scripts directory using the following command:
   ```
   cd %NCHOME%\precision\scripts\sql\mysql
   ```
2. Execute the script using the following command:
   ```
   drop_mysql_database.bat root password
   ```

Removing a DB2 topology database on UNIX

`UNIX`

You can remove the DB2 database on UNIX using a script.

To remove a DB2 database, complete the following steps:
1. Change to the scripts directory using the following command:
   ```
   cd $NCHOME/precision/scripts/sql/db2
   ```
2. Execute the script using the following command:
   ```
   drop_db2_database.sh NCIM [ force ]
   ```

If you use the optional force option, the script forces any existing DB2 users off the instance before attempting to drop the database.

Removing a DB2 topology database on Windows

`Windows`

You can remove the DB2 database on Windows using a script.

To remove a DB2 database, complete the following steps:
1. Change to the scripts directory using the following command:
   ```
   cd %NCHOME%\precision\scripts\sql\db2
   ```
2. Execute the script using the following command:
   ```
   drop_db2_database.bat NCIM [ force ]
   ```
   If you use the optional force option, the script forces any existing DB2 users off the instance before attempting to drop the database.

Removing an Informix topology database on UNIX

`UNIX`

You can remove the Informix database on UNIX using a script.

To remove an Informix database, complete the following steps:
1. Change to the scripts directory using the following command:
   ```
   cd $NCHOME/precision/scripts/sql/informix
   ```
2. Execute the script using the following command:
   ```
   drop_informix_database.sh database
   ```
   where *database* is the required name of the database to drop.

Removing an Informix topology database on Windows

You can remove the Informix database on Windows using a script.

To remove an Informix database, complete the following steps:

1. Change to the scripts directory using the following command:

   `cd %NCHOME%\precision\scripts\sql\informix`

2. Execute the script using the following command:

   `drop_informix_database.bat` *database*

   where *database* is the required name of the database to drop.

Removing an Oracle topology database on UNIX

You can remove the Oracle database on UNIX using a script.

To remove an Oracle database, complete the following steps:

1. Ensure that you are logged in as the `system` user.
2. Change to the scripts directory using the following command:

   `cd $NCHOME/precision/scripts/sql/oracle`

3. Execute the script using the following command:

   `sqlplus system/password < drop_oracle_database.sql`

If you use the optional force option, the script forces any existing Oracle users off the instance before attempting to drop the database.

Removing an Oracle topology database on Windows

You can remove the Oracle database on Windows using a script.

To remove an Oracle database, complete the following steps:

1. Ensure that you are logged in as the `system` user.
2. Change to the scripts directory using the following command:

   `cd %NCHOME%\precision\scripts\sql\oracle`

3. Execute the script using the following command:

   `sqlplus system/password < drop_oracle_database.sql`

If you use the optional force option, the script forces any existing Oracle users off the instance before attempting to drop the database.

Chapter 9. Administering charting

The Charting feature enables you to retrieve data from IBM Tivoli applications such as Tivoli Monitoring and Tivoli Business Service Manager and from custom charts that were designed with the Eclipse Business Intelligence and Reporting Tools Designer.

Use the charting features to build console pages with charts from Tivoli applications and customized charts created using the Business Intelligence and Reporting Tools Designer.

Related reference:

"Chart errors" on page 134
Consult this list of possible causes of charting errors and suggested solutions.

User roles for charting

Users must have the user IDs assigned to a chart role before they can see and work with the charting functions.

The main administrator (tipadmin) of the application server already has the chartAdministrator role, and can assign users to any of the three chart roles that are available. Logged in users will have no access privileges to the charting features if their user ID has not been assigned to a chart role. These are the capabilities of the chart roles:

chartAdministrator
> Users with this role can create and delete charting connections to data sources, download the BIRT Designer, upload charts, and can clear the charting cache (useful for troubleshooting).

chartCreator
> Users with this role can download the BIRT Designer, upload charts, view, and edit them. They cannot create or delete chart connections nor can they clear the charting cache.

chartViewer
> Users assigned to this role can select and view charts, but cannot modify them or their preferences. They cannot download the BIRT Designer, upload charts, create connections, or clear the charting cache.

Roles are assigned through **Users and Groups > Administrative User Roles**.

Modifying chart properties

You can change the directory where chart files are located or to fine tune the timing of chart refreshes.

After a chart has been added to a console page, it is automatically refreshed with new data at intervals. The refresh rate is adjusted based on the response time of the Tivoli Integrated Portal Server. This ensures that the server is not overloaded with data requests and that it remains responsive. The algorithm for calculating the next refresh interval uses three parameters from the chart properties:

> Minimum refresh interval

Maximum refresh interval

Response time multiplier

You can adjust the balance of chart refresh rate and server performance by using a tipcli command:

1. On the command-line interface, change to the *install_dir*/profiles/ TIPProfile/bin/ directory.

2. Run the following command declaring the chart property that you want to modify and its new value:

   `Windows` `tipcli.bat ChartProperties --[name parameter_name --value --parameter_value] --username user_name --password user_password`

   `UNIX` `Linux` `tipcli.sh ChartProperties --[name parameter_name --value --parameter_value] --username user_name --password user_password`

   The following list provides details on the arguments and parameters shown:

   parameter_name
   > The chart property that you want to modify. The following parameters can be modified:
   >
   > - UPDATE_MAXIMUM_INTERVAL (Default value = 60)
   >
   >   The default maximum interval between data refreshes is 60 seconds unless the server response time multiplied by the UPDATE_MULTIPLIER value is longer. Consider raising this number if the calculated interval often exceeds the maximum.
   >
   > - REPORT_OUTPUT_DIR (Default value = install_dir/temp/report)
   >
   > - AXIS_TIMEOUT (Default value = 9000)
   >
   >   If the system times out or an error message is displayed while importing an Tivoli Monitoring chart, it is typically because the Tivoli Enterprise Portal Server is unavailable. You can extend the time period before the time out by increasing this value.
   >
   > - REPORT_INPUT_DIR (Default value = install_dir/report)
   >
   > - DBTABLE_VERSION (Default value = 1.1.1)
   >
   > - UPDATE_MINIMUM_INTERVAL (Default value = 30)
   >
   >   The default shortest interval between data refreshes is 30 seconds unless the server response time multiplied by the UPDATE_MULTIPLIER value is lower. Consider raising this number if the calculated interval is often lower than the minimum.
   >
   > - UPDATE_MULTIPLIER (Default value = 10)

   parameter_value
   > The value that you want to set for the declared property.

   user_name
   > The user name of the Tivoli Integrated Portal user.

   user_password
   > The password for the Tivoli Integrated Portal user.

   For example:

   `Windows` `tipcli.bat ChartProperties --[name UPDATE_MAXIMUM_INTERVAL --value --120] --username tipuser1 --password tipuserpassw0rd`

Configuring multiple ITM Web Services

Use this procedure if you want to display charts from more than one Tivoli Managed Network.

During an advanced installation that includes the charting feature, you can also identify an ITM Web Service for retrieving attribute values into charts. In environments that have multiple managed networks, you can configure an additional ITM Web Service for each Tivoli Enterprise Portal Server. Follow this procedure to manually add another ITM Web Service to the same server instance.

1. Copy the `ITMWebServiceEAR.ear` directory branch to a temporary location (such as `c:\temp`): from *tip_home_dir*`/profiles/TIPProfile/installedApps/TIPCell/`.

2. Rename the Web service in `application.xml`:

   a. At the command line, change to the temporary directory.

   b. In the temporary directory, open `application.xml` from *tip_home_dir*`/profiles/TIPProfile/installedApps/TIPCell/ITMWebServiceEAR.ear/META-INF/` in a text editor.

   c. Change the name `<display-name>ITMWebServiceEAR</display-name>` to `<display-name>ITMWebService2EAR</display-name>`.

   d. Change the name `<context-root>ITMWebService</context-root>` to `<context-root>ITMWebService2</context-root>`.

3. Rename the Web service in `webservice.properties.readme`:

   a. At the command line, change to the temporary directory.

   b. In the temporary directory, open `webservice.properties.readme` from *tip_home_dir*`/profiles/TIPProfile/installedApps/TIPCell/ITMWebServiceEAR.ear/resources` in a text editor.

   c. Change `WEBSERVICE.NAME=ITMWebService` to `WEBSERVICE.NAME=ITMWebService2`.

   d. Save the file as `webservice.properties`.

4. Rename the `ITMWebServiceEAR.ear` directory to `ITMWebService2EAR.ear` in the temporary directory.

5. Use the following example to guide you and create a script called `installwebservice.jacl` in the temporary directory :

```
installwebservice.jacl:
$AdminApp install c:/temp/ITMWebService2EAR.ear [ list -usedefaultbindings
-defaultbinding.virtual.host default_host -MapRolesToUsers
{{"chartViewer" No Yes "" ""}}]

set deployment [$AdminConfig getid /Deployment:ITMWebService2EAR/]
set deployedObject [$AdminConfig showAttribute $deployment deployedObject]
set classloader [$AdminConfig showAttribute $deployedObject classloader]

$AdminConfig showall $classloader
$AdminConfig modify $classloader {{mode PARENT_FIRST}}

$AdminConfig showall $classloader

$AdminConfig save
```

6. Use the following example to guide you and in the temporary directory create a script called `installwebservice.cmd` that will used to deploy the Web service:

```
installwebservice.cmd:
echo Installing Web Service
```

```
    set TIP="c:\ibm\tivoli\tip"
    set PROFILE=TIPProfile
    set TIPTOOLS=c:\tiptools
    set USERNAME=tipadmin
    set PASSWORD=tippass

    cd %TIP%\profiles\%PROFILE%\bin
    call wsadmin -f %TIPTOOLS%\installwebservice.jacl -username %USERNAME%
    -password %PASSWORD%

    echo All Done!
```

7. Run the `installwebservice.cmd` script to deploy the Web service.

8. Run these **tipcli** commands in *tip_home_dir*/bin/ to configure the username and password for the new Web service, adding the Web service name at the end of the command line: `tipcli.bat ITMLogin --hostname localhost --port 1920 --username sysadmin --password sysadm1n --servicename ITMWebService2`

9. Stop and then restart the Tivoli Integrated Portal Server.

10. Add to the list of Web services in the Charting portlet, using the exact information as the default Web service, and changing only the Service Name.

Configuring for localized or customized Tivoli Monitoring charts

National Language Version (NLV) text or customer-specific resource bundles from IBM Tivoli Monitoring applications are not displayed correctly in Charting. To include such resource bundles, you need to copy some files to your Tivoli Integrated Portal Server installation.

This procedure involves copying the product resource jar files from the Tivoli Enterprise Portal Server to the application server and referencing them in the class path used by the ITM Web Service.

1. Locate the `*_resources.jar` files on the computer where the Tivoli Enterprise Portal Server is installed:

   - `Windows` *itm_install_dir*\CNB\classes

   - `UNIX` `Linux` *itm_install_dir*/arch/cw/classes

2. On the computer where the Tivoli Integrated Portal Server is installed, copy the `*_resources.jar` files to *BIRTExtension*/lib.

3. Add the `*_resources.jar` file names to the class path in the `MANIFEST.MF` file of `ITMWebService.jar`:

   a. Copy `ITMWebService.jar` from *tip_home_dir*/profiles/TIPProfile/installedApps/TIPCell/ITMWebServiceEAR.ear to a temporary directory.

   b. Decompress the file with this command: `jar xvf ITMWebService.jar`

   c. In a text editor, open `MANIFEST.MF` from the `META-INF` directory.

   d. Add the file names of the new jar files to the Class-Path entry, while being careful of file formatting:

```
META-INF/MANIFEST.MF:
Manifest-Version: 1.0
Created-By: 2.3 (IBM Corporation)
Class-Path: browser.jar cnp.jar cnp_vbjorball.jar ka4_resources.jar
kfw_resources.jar kjrall.jar knt_resources.jar koq_resources.jar
kor_resources.jar koy_resources.jar kp5_resources.jar kph_resources.jar
kpk_resources.jar kpv_resources.jar kpx_resources.jar kqr_resources.jar
```

```
kqv_resources.jar kqx_resources.jar kto_resources.jar kud_resources.jar
kul_resources.jar kum_resources.jar kux_resources.jar kva_resources.jar
ksy_resources.jar khd_resources.jar tap_cli.jar util.jar workspace.jar
resources/ my_new_resources.jar
```

   e. Save and close MANIFEST.MF.
4. From the temporary directory, compress the file with the following command
   and replace the old ITMWebService.jar with the updated file:

   `jar cfm ITMWebService.jar META-INF\MANIFEST.MF com org`

5. If you are logged on to the portal, log off, and then complete the next two steps
   to restart the Tivoli Integrated Portal Server.
6. In the *tip_home_dir*/profiles/TIPProfile/bin directory, depending on your
   operating system, enter one of the following commands:

   - **Windows**   `stopServer.bat server1`

   - **UNIX**   **Linux**   `stopServer.sh server1`

     Note: On UNIX and Linux systems, you are prompted to provide an
     administrator username and password.

7. In the *tip_home_dir*/profiles/TIPProfile/bin directory, depending on your
   operating system, enter one of the following commands:

   - **Windows**   `startServer.bat server1`

   - **UNIX**   **Linux**   `startServer.sh server1`

Importing or exporting charts and chart customizations

You can import or export charts and chart customizations at the command line.

To import or export a chart, or a chart customization:

1. On the command-line interface, change to the *tip_home_dir*/profiles/
   TIPProfile/bin/ directory.
2. Run the following command to export chart data:
   `tipcli.bat|.sh ChartExport --dir output_directory --type`
   `all|customcharts|page [--pageID page_ID | --pageName page_name]`
   `--username tip_username --password tip_user_password`

   Export command options
   > Use the Export command to create the specified directory (`dir`) and
   > export the chart data to that directory.

Table 14. ChartExport command arguments

Parameter and arguments	Description
`--dir output_directory`	Mandatory parameter. The directory where the exported data is saved. If the directory does not exist, it is created.
`--type all|customcharts|page`	Mandatory parameter. If you set the `--type` to `all`, then all charts are exported. If you set it to `customcharts`, then only customized charts are exported. If you set it to `page`, then you can use either the `--pageID` or the `--pageName` parameter to specify the page for which you want to export chart data.

Table 14. ChartExport command arguments (continued)

Parameter and arguments	Description
[--pageID *page_ID* | --pageName *page_name*]	Optional parameter. If you set the --type parameter to page, then you can use either the --pageID or the --pageName parameter to specify the page for which you want to export chart data.
--username *tip_username*	Mandatory parameter. The user name for a user with either the chartAdministrator or chartCreator role.
--password *tip_user_password*	Mandatory parameter. The password for the specified user name.

3. Run the following command to import chart data:
   tipcli.bat|.sh ChartImport --dir *source_directory* --username *tip_username* --password *tip_user_password*

   Import command options
   ChartImport is used to import chart data from a specified directory.

Table 15. ChartImport command arguments

Parameter and arguments	Description
--dir *source_directory*	Mandatory parameter. The directory where the data to imported is located. BIRT Designer file format is .rptdesign.
--username *tip_username*	Mandatory parameter. The user name for a user with either the chartAdministrator or chartCreator role.
--password *tip_user_password*	Mandatory parameter. The password for the specified user name.

Tivoli charts

You can display charts with data from IBM Tivoli Monitoring and other Tivoli products.

When you create a page with the Charting portlet, it opens with choices for chart sources and chart customization. Use the Tivoli Charts source to display a chart of data selected from supported Tivoli applications such as Tivoli Monitoring and Tivoli Business Service Manager.

Opening a chart from a Tivoli application

You can retrieve real-time data from Tivoli applications to render in a chart portlet.

A page created with the Charting portlet gives you a choice of displaying a chart with data retrieved from a Tivoli product or one that was created with the BIRT Designer. These instructions are for data sources accessed through a Tivoli application's Web service (J2EE application for using the chart and table queries from Tivoli monitoring and analytics products).

1. Create a new page (**Settings** > **Page Management** > **New Page**), provide a page name and click **Save**. Select the **Charting** portlet entity, and click **OK** and select

Tivoli Charts. The Charting title bar has several tools for editing the portlet, getting help, personalizing the display, and minimizing or maximizing the display.

2. In the Charting portlet, click **Tivoli Charts** to open a table of defined connections to chart sources. If the chart services for IBM Tivoli Monitoring were enabled during installation, details are displayed with the name ITM.

3. Select a Tivoli application row from the list and click **Next**.

4. Select an information group from the **Groups** ☑ list. The Web service identifies the available chart types for that group and displays them in the list. If the list is empty, ask your administrator for help or review the troubleshooting topic for charts.

5. Select the chart type to open and click **Finish**. The query is passed through the Tivoli servers to the monitoring agent (or agents) and data samplings are returned based on the chart that was requested.

6. If you would like to save the page, click **Save** and complete the fields. Select Client Side page persistence to ensure the best performance and behavior of charting portlets.

The chart is rendered as specified by the view query. To share the chart with others who view the same page, click **Share Preferences**. You must have the chartAdministrator or chartCreator role to be able to share preferences.

Hover the mouse over a chart point to see the value it represents or switch to the table view to see all the values. If the chart toolbar is hidden, click ⬇ to open it. You can ↻ **Refresh** the data, manipulate and refine the chart, publish the chart for sharing with other users, or click ↩ **Return to chart selector** and select a different chart.

Defining a Web service connection

The Charting portlet enables you to retrieve data from Tivoli data sources that have been defined there. The definition includes the application server address and the Web service name.

Before a connection can be established for a Web service, that service and its data sources must be configured. Web service connections are usually created during the product installation, so it is rare that an administrator needs to create a new connection. The chartAdministrator role is required to create or delete connections.

In particular for IBM Tivoli Monitoring Web Service connections, the optional BIRTExtension component must be installed and single sign-on (SSO) must be configured between the Tivoli Integrated Portal Server and the Tivoli Monitoring instance.

Create a connection definition for the Tivoli applications from which you want to retrieve chart data.

1. Create a new page (**Settings** > **Page Management** > **New Page**), provide a page name and click **Save**. Select the **Charting** portlet entity, and click **OK** and select **Tivoli Charts**. The Charting title bar has several tools for editing the portlet, getting help, personalizing the display, and minimizing or maximizing the display.

2. In the Charting portlet, click **Tivoli Charts** to open a table of defined connections to chart sources. If the chart services for IBM Tivoli Monitoring were enabled during installation, details are displayed with the name ITM.

3. Click ⬜ **New**. If you do not see this tool, click ⬜ to display the chart toolbar.

4. In the window that opens, complete the fields to identify the Charting Web service:

   a. Enter a **Name** of up to 32 characters for the connection.

   b. From the **Type** list select a service type, for example, `Web Service`.

   c. From the **Protocol** list, select the non-secure HTTP or secure HTTPS. For example, for an Tivoli Monitoring Web Service connection, select `HTTP`.

   d. Enter the fully qualified **Hostname** of the application server.

   e. Enter a **Port** number for the application server. The default port is 16310 for HTTP and 16311 for HTTPS. However, the port number used depends on the product you are connecting to, for example, an Tivoli Monitoring Web Service connection normally uses port `15200`. Consult your administrator or the product documentation for the port to use.

   f. In the **Service Name** field, provide a service name for the connection. The service name depends on the application you are connecting to (such as `TIPWebServiceHttpRouter` for Tivoli Monitoring). Refer to your product documentation for the correct Web Service Name to use.

   g. Select a render format for the connection, that is, either BIRT or Dojo. For example, for an Tivoli Monitoring Web Service connection select **BIRT**.

   h. Select the authentication method to be used and if you do not select the single sign-on (SSO) option, provide log in credentials. For a IBM Tivoli Monitoring Web Service connection, select the SSO option.

5. Click **Create** to add the Web service definition to the list.

6. To configure the connection in relation to the relevantTivoli Enterprise Portal Server, carry out the following steps at the command line:

   a. Change directory to `install_dir/profiles/TIPProfile/bin`.

   b. To configure the connection, depending on the platform enter:

   `Windows` `./tipcli.sh ITMLogin --hostname` *host_name* `--port` *port_num* `--servicename` *service_name*

   `UNIX` `Linux` `./tipcli.sh ITMLogin --hostname` *host_name* `--port` *port_num* `--servicename` *service_name*

   Where:

   hostname is the name that you provided in the Connection Properties dialog.

   service_name is the exact service name that you provided in the Connection Properties dialog.

   port_num is the port number that is to be used for the Tivoli Enterprise Portal Server connection (normally 1920).

If you need to modify a definition, delete it and then create a new connection.

Repeat these steps on any other application servers that you intend to import Tivoli charts from.

Custom charts

The charts portlet enables you to display charts created with the Eclipse Business Intelligence and Reporting Tools Designer.

A page created with the Charting portlet opens with choices for chart source and chart customization. You can open charts that were created with the BIRT Designer. BIRT is an Eclipse-based open source reporting system that is available for downloading and using with your product.

Your product contains a special version of the BIRT Designer with plug-ins to connect to Tivoli applications hosting a custom Web service interface.

Opening a chart created in the BIRT Designer

You can retrieve charts that were created with the Business Intelligence and Reporting Tools.

A page created with the Charting portlet gives you a choice of displaying a chart with data retrieved from a Tivoli product or one that was created with the BIRT Designer. These steps are for opening a BIRT chart.

1. Create a new page (**Settings** > **Page Management** > **New Page**), provide a page name and click **Save**. Select the **Charting** portlet entity, and click **OK** and select **Tivoli Charts**. The Charting title bar has several tools for editing the portlet, getting help, personalizing the display, and minimizing or maximizing the display.
2. In the Charting portlet, click **Custom Charts** to open a list of BIRT charts. If no charts are listed, you need to upload them.
3. Select the chart to display and click **Finish**.

The chart and the data it specifies are displayed.

Uploading a BIRT chart

You can retrieve charts that were created with the Business Intelligence and Reporting Tools (BIRT) Designer.

You need to identify the BIRT report file to the Charting portlet to make it accessible for display.

1. Create a new page (**Settings** > **Page Management** > **New Page**), select **Charting** portlet entity, then click **Add Portlet**.
2. In the Charting portlet, click **Custom Charts** to open a list of BIRT charts.
3. Click ⬆ **Upload**.
4. Click **Browse** to locate and open the report design file, then click ⬆ **Upload** to add it to the list of BIRT charts. Charts are created in the BIRT Designer workspace directory with a `.rptdesign` extension.

After uploading the report design, you can open the uploaded BIRT chart in a chart portlet.

Chart or table creation with the BIRT Designer

Use the Business Intelligence and Reporting Tools Designer to create custom charts and tables that can be saved and uploaded to a charting portlet.

Here is a brief overview of the basic steps to create a chart or table.

After downloading the BIRT Designer, you need to download and extract it. The BIRT Designer that comes with Tivoli Integrated Portal runs only on Windows.

1. Select **Custom Charts** from the page that was created with the Charting portlet.
2. Select the ⬇ BIRT Designer link.
3. When prompted, save the birt-designer compressed file, then decompress it.
4. In the birt-designer directory, start `birt.exe`.

After installing and starting the BIRT Designer, create your first chart.

1. Create a new report in the BIRT Designer with **File** > **New** > **New Report**.
2. Click the **Data Explorer** tab to open the Data Explorer view.
3. Right-click **Data Sources** and click **New Data Source**, with either `IBM Tivoli Data Query Web Service` or `JDBC Data Source` as the type, depending on what kind of data sources are available. (Do not select the sample data database because the number of data rows returned might exceed the charting 10,000 row limit.) Follow the screens and enter the information as necessary.
   - When `IBM Tivoli Data Query Web Service` is the type of Data Source, a connection is made to the Web Service. You can securely connect to a Web service by choosing HTTPS as the protocol. For the port, increment the port number you chose at install time by 1 (such as 16311). You must also enter a username and password for the administrative console. You will receive another prompt to accept the SSL certificate from the server. Accept the certificate to connect.
   - When `JDBC Data Source` is the data source, you might need to add the driver to the BIRT Designer and the application server. The DB2 JDBC driver is included with both the stand-alone BIRT Designer and the one that is included with your product. Copy the JDBC drivers to the these directories and then restart the BIRT Designer and the application server: `<BIRT Designer>\plugins\ org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919\drivers;` `<install_dir>\systemApps\isclite.ear\TIPChartPortlet.war\WEB-INF\ platform\plugins\ org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919\drivers.`
4. Create a new Data Set and select the data source you just created. A data set provides data to a chart or table. Follow the screens and enter information as necessary.
5. Drop a Chart from the Palette view of BIRT onto your report, then configure the chart with the Chart Wizard using the Data Set created in the previous step. To create a table, drag the Data Set onto the report. A table containing the data set is created for you. The report design you create in the BIRT Designer should contain a single data set and a single chart or table only.
6. After you finish creating the chart, save your changes, and click the **Preview** tab to render the chart. Each report design file can contain one chart or table. Use the **Reporting** module if you want to multiple charts or tables in the same report.

7. Return to the administrative console, create a new page with the Charting portlet, save it, click **Custom Charts**, then choose **Upload**, and navigate to the `mychartname.rptdesign` location. The chart was saved in the `workspace` directory of the BIRT Designer.

Note: The sample database charts that are provided with the BIRT Designer can consume a large amount of hard disk space. Use the sample data base only for testing and practice.

Chart tools

After creating or opening a page from one of the chart sources, you can adjust it.

While a chart is displayed, click any of these tools to manipulate it. If the charting toolbar is collapsed, click ⬇ to expand. You can also right-click a chart data point to see and select a chart tool from the pop-up menu.

Tool	Purpose
Refresh	Refresh the current chart with new data. You can also refresh the design, which reads the chart definition from the source application and is useful if the definition has been edited. However, it slows down the chart rendering, so use it only when you know or think that the chart definition has changed.
Preferences	Change the appearance and behavior of the chart.
Toggle Table	Switch the chart to a table format. You can drag the column borders to adjust the widths.
Toggle Chart	Switch the table to a chart format. If this tool is unavailable, the table cannot be rendered as a chart.
Return to chart selector	Go back to the previous view and select another chart type or design.
Print Preview	Open a printable view of the chart or table. You can then use the browser's print function to print the page.
Save to File	Save the chart or table in the PNG (Portable Network Graphics) image format.

Tool	Purpose
Publish	Publish this portlet to make it available to other chart users. Select one of the following: **Share Preferences** to save the current chart selection and customization for this portlet to share with others. **Clear Shared Preferences** to reset the preference settings to their defaults for this portlet. Users will see the chart selector instead of a specific chart. Specify will not remove specific user preferences; other users will still see their selections if they have changed them. **Clear User Preferences** to reset only the preferences that the current user might have set in this portlet. If default preferences exist, the user will see the chart and customization for the defaults. Otherwise, the chart selector is displayed.

Chapter 10. Administering reports

You can create new reports, modify existing reports, and configure user access to reports.

Creating and editing reports

You can edit existing reports and create your own reports using the Tivoli Common Reporting tools.

You can create new reports using the Cognos® Query Studio, which is described in the *Query Studio User Guide*, available from the **Help** menu in the **Reporting** > **Common Reporting** portlet.

You can edit existing reports using the Cognos Report Studio, which is described in the *Report Studio Professional Authoring User Guide*, available from the **Help** menu in the **Reporting** > **Common Reporting** portlet.

Restriction: You can edit existing reports using the Cognos Report Studio only if they are based on the Cognos data model. The reference information for each individual report describes which data model the report is based on. If you want to modify a BIRT-based report, you can use the Cognos Query Studio to create a similar report using the old report as a guide, and modify the report if necessary later using the Cognos Report Studio.

If you create or edit custom Cognos-based reports, then the report creation or editing procedure will require selection of IBM Common Data Model (CDM) views and attributes. For more information on the CDM views, see the *IBM Tivoli Network Manager IP Edition Topology Database Reference*.

Creating a URL to run reports

You can construct a URL to open a report directly in a browser window. These URLs can be used by other applications to run reports.

To construct a URL to open a report, complete the following steps.
1. Locate the report that you want to use and note which parameters are required.
2. Construct a URL similar to the following:

   ```
   https://hostname:port/tarf/servlet/component?b_action=cognosViewer&ui.action=run
   &ui.object=/content/package[@name='Network Manager']/
   folder[@name='report_group_name']
   /report[@name='report_name']&ui.name=report_name&run.outputFormat=HTML&
   domainName=AUTO&report_parameter="value"
   ```

   Where
   - *hostname* is the name of the server where the Tivoli Integrated Portal is installed.
   - *port* is the port number for the Tivoli Integrated Portal.
   - *report_group_name* is the name of the group to which the report belongs.
   - *report_name* is the name of the report that you want to open.
   - *report_parameter* is a parameter to be passed to the report.
   - *value* is the value of the parameter.

The following example URL opens the IP Routing Info report, which belongs to the Path Views Reports report group, showing path 3323 and device 13.

```
https://10:10:10:108:9999/tarf/servlet/component?b_action=cognosViewer&ui.action
=run&ui.object=/content/package[@name='Network Manager']
/folder[@name='Path Views Reports']/report[@name='IP Routing Info']&ui.name
=IP Routing Info&run.outputFormat=HTML&domainName
=AUTO&pathEntityId=3323&entityId=13
```

Configuring data sources for reporting

Data sources for reporting are set during installation. If the database details change, configure the data source again.

For example, if you change the username and password used to connect to NCIM, or move the NCIM database to another server, you need to configure the data sources.

If you want to use Tivoli Data Warehouse as the data source for reports, you need to configure the appropriate data sources to connect to the Tivoli Data Warehouse.

Configuring data sources for BIRT

If you use reports based on the BIRT data model, you must configure data sources from the Report Data Sources window. If you also use reports based on the Cognos data model, you must configure Cognos data sources separately.

If you are not using Tivoli Data Warehouse, configure NCIM as the data source. If you want to use Tivoli Data Warehouse as the data source, obtain the database and connection details from the database administrator before starting this task.

To define the data sources for all reports based on the BIRT data model, complete the following steps.

Tip: The reference documentation for each report shows you which data model the report uses.

1. Change to the following directory (the following path is the default location):/opt/IBM/tivoli/tipv2Components/TCRComponent/bin.

2. Run the following command: **UNIX**

```
trcmd.sh -modify -dataSources -reports -username tip_username -password
tip_password -dataSource name=data_source_name -setDatasource odaURL=
JDBC_database_URL odaDriverClass=JDBC_driver_class
odaUser=database_user odaPassword=database_user_password
```

Windows

```
trcmd.bat -modify -dataSources -reports -username tip_username -password
tip_password -dataSource name=data_source_name -setDatasource odaURL=
JDBC_database_URL odaDriverClass=JDBC_driver_class
odaUser=database_user odaPassword=database_user_password
```

Replace the variables in the command using the following definitions:

- *tip_username* is the username of the administrative user for the Tivoli Integrated Portal, for example `tipadmin`.
- *tip_password* is the password for this user.
- *data_source_name* is the name of the data source you want to configure. Allowed values are:
  - NCIM for reports using topology information.

- – PARAMETERS for reports using the NCPOLLDATA database or the NCPOLLDATA schema for report parameters.
  - – NCPOLLDATA for reports using polling data.
- *JDBC_database_URL* is the URL for the JDBC database. The URL depends on the platform and other variables. To construct the URL, refer to the following list:
-

JDBC URL

> **IDS** **Informix**®
>> ```
>> jdbc:informix-sqli://hostname:port/database_name
>> :INFORMIXSERVER=server;
>> DELIMIDENT=YIFX_LOCK_MODE_WAIT=-1
>> ```
>
> **Oracle** **Oracle**
>> ```
>> jdbc:oracle:thin:@hostname:port:database_name
>> ```
>
> **MySQL** **MySQL**
>> ```
>> jdbc:mysql://hostname:port/database_name
>> ```
>
> **DB2** **DB2**
>> ```
>> "jdbc:db2://hostname:port/
>> database_name:currentSchema=NCIM;"
>> ```

Using the following values:

hostname
> The name of the host where the NCIM or TDW database is installed.

port The port on which to connect to the NCIM or TDW database. The default for DB2 databases is 50000, for Oracle databases is 1521, for Informix databases is 9088, and for MySQL is 3306.

database_name
> By default, the name of the NCIM database is `ncim`. The default name of the TDW database is WAREHOUS.

server The name of the Informix server.

The following examples show JDBC connection URLs for each of the different database platforms.

> **IDS** **Informix**
>> jdbc:informix-sqli://192.168.1.2:9088/
>> itnm:INFORMIXSERVER=demo_on;
>> DELIMIDENT=Y; IFX_LOCK_MODE_WAIT=-1
>
>> This example URL connects to an Informix database with the following properties:
>> - – The database server host IP address is 192.168.1.2.
>> - – The database is running on port 9088. This is the default port for Informix.
>> - – The Informix database name is itnm.
>> - – The Informix server instance name is demo_on.

> **Oracle** **Oracle**
>> jdbc:oracle:thin:192.168.1.2:1521:itnm

This example URL connects to an Oracle database with the following properties:

– The database server host IP address is 192.168.1.2.

– The database is running on port 1521. This is the default port for Oracle.

– The Oracle database name is itnm.

`MySQL` **MySQL**

jdbc:mysql://192.168.1.2:3306/ncim

This example URL connects to a MySQL database with the following properties:

– The database server host IP address is 192.168.1.2.

– The database is running on port 3306. This is the default port for MySQL.

– The name of the topology database schema name is ncim.

`DB2` **DB2**

jdbc:db2://192.168.1.2:50000/itnm:NCIM

This example URL connects to a DB2 database with the following properties:

– The database server host IP address is 192.168.1.2.

– The database is running on port 50000. This is the default port for DB2.

– The DB2 database name is itnm.

– The name of the topology database schema name, in uppercase, is NCIM.

- *jdbc_driver_class* is the class name of the JDBC driver. The following values show the class names for different platforms.

-

JDBC Driver

`IDS` **Informix**

```
com.informix.jdbc.IfxDriver
```

`Oracle` **Oracle**

```
oracle.jdbc.driver.OracleDriver
```

`MySQL` **MySQL**

```
com.mysql.jdbc.Driver
```

`DB2` **DB2**

```
com.ibm.db2.jcc.DB2Driver
```

- *database_user* is the name of a user that has read permissions in the target database.

- *database_user_password* is the password of this user.

Example commands to set data sources for NCIM and for Tivoli Data Warehouse

- Example command to set a Tivoli Data Warehouse data source on Oracle:

The following command sets the NCPOLLDATA data source for historical reporting to the Tivoli Data Warehouse:`trcmd.sh -modify -dataSources -reports -username tipadmin -password admin`

```
-dataSource name=NCPOLLDATA -setDatasource odaURL="jdbc:thin://
myserver.abc.com:1521/WAREHOUS"
odaDriverClass="oracle.jdbc.driver.OracleDriver" odaUser=itmuser
odaPassword=itmuser
```

- Example commands to set an NCIM data source on DB2:

  The following command sets the NCIM data source:`trcmd.sh -modify`
  `-dataSources -reports -username tipadmin -password netc00l`
  `-dataSource name=NCIM -setDatasource odaURL="jdbc:db2://`
  `myserver.abc.com:50000`
  `/ITNM:currentSchema=NCIM;" odaDriverClass="com.ibm.db2.jcc.DB2Driver"`
  `odaUser=ncim odaPassword=ncim`

  The following command sets the PARAMETERS data source:`trcmd.sh -modify`
  `-dataSources -reports -username tipadmin -password netc00l`
  `-dataSource name=PARAMETERS -setDatasource odaURL="jdbc:db2://`
  `myserver.abc.com:50000`
  `/ITNM:currentSchema=NCPOLLDATA;"`
  `odaDriverClass="com.ibm.db2.jcc.DB2Driver"`
  `odaUser=ncim odaPassword=ncim`

  The following command sets the NCPOLLDATA data source to connect to an
  NCIM database on DB2:`trcmd.sh -modify -dataSources -reports -username`
  `tipadmin -password netc00l`
  `-dataSource name=NCPOLLDATA -setDatasource odaURL="jdbc:db2://`
  `myserver.abc.com:50000`
  `/ITNM:currentSchema=NCPOLLDATA;"`
  `odaDriverClass="com.ibm.db2.jcc.DB2Driver"`
  `odaUser=ncim odaPassword=ncim`

Configuring data sources for Cognos

If you use reports based on the Cognos data model, you must configure data
sources for the reports. If you also use reports based on the BIRT data model, you
must configure BIRT data sources separately.

Network Manager defines a data source for each Network Manager database
schema used by Cognos. The reports require the following data sources: NCIM,
NCMONITOR, NCPGUI, NCPOLLDATA, PARAMETERS, and IBM_TRAM.

Configuring a DB2 data source

To configure a DB2 data source for Cognos reports, follow these configuration
steps.

Complete the following tasks to configure a DB2 data source.

1. Click **Reporting** > **Common Reporting** > **Network Manager**. Select
   Administration from the **Launch** menu. Click the **Configuration** tab.
2. Click the data source that you want to configure. Network Manager reports
   require the following data sources to be configured:
   - NCIM
   - NCMONITOR
   - NCPGUI
   - NCPOLLDATA
   - PARAMETERS

   Do not edit the data source IBM_TRAM.
3. Click **Connection**.

4. Select **DB2** as the connection type. Leave the other settings at the defaults. Click **OK**.

5. Follow the onscreen instructions to set up the connection. Ensure that you include the following Network Manager-specific information:

   User for database signon

   Ensure that you enter a username and password combination that has access to the NCIM schemas used by the reports you want to use. For example, the default data source NCPOLLDATA uses the NCPOLLDATA NCIM schema, and the DB2 configuration scripts give the user `ncpolldata` access to this schema.

   Click **Help** in the wizard for information about specific fields.

6. When you have finished configuring the data source, configure the connection associated with the data source.

   a. Click the name of the data source.

   b. Click the **Set Properties** icon in the Actions column.

   c. Click **Connections**.

   d. Click **Set...** next to **Open Session Commands**.

   e. Enter the following code, replacing *schema_name* with the name of the appropriate schema.

   Tip: The schemas have the same name as the data sources, except the PARAMETERS data source, which uses the NCPOLLDATA schema.

   ```
   <commandBlock>
    <commands>
     <sqlCommand>
          <sql>SET CURRENT SCHEMA = schema_name</sql>
     </sqlCommand>
    </commands>
   ```

   f. Apply the changes.

   g. Verify the signon properties of the connection.

      1) Test the connection using the **Signon** option. If the test is not successful, first verify that the username and password are correct by testing the connection using the **User ID and password** option, and then verify that the database details are correct.

      2) If necessary, edit the signon properties of the connection. Enter the username and password of a database user with access permissions to the database tables used by this data source. The default username is `itmuser`, with the password `netcool`.

7. Repeat these steps for each data source that you want to configure.

Configuring an Oracle data source

To configure an Oracle data source for Cognos reports, follow these configuration steps.

Complete the following tasks to configure an Oracle data source.

1. Click **Reporting** > **Common Reporting** > **Network Manager**. Select **Administration** from the **Launch** menu. Click the **Configuration** tab.

2. Click the data source that you want to configure. Network Manager reports require the following data sources to be configured:

   • NCIM

   • NCMONITOR

   • NCPGUI

- NCPOLLDATA
- PARAMETERS

Do not edit the data source IBM_TRAM.

3. Click **Connection**.
4. Select **Oracle** as the connection type. Leave the other settings at the defaults. Click **OK**.
5. Follow the onscreen instructions to set up the connection. Ensure that you include the following Network Manager-specific information:

   User for database signon
   > Ensure that you enter a username and password combination that has access to the NCIM schemas used by the reports you want to use. For example, the default data source NCPOLLDATA uses the NCPOLLDATA NCIM schema, and the Oracle configuration scripts give the user `ncpolldata` access to this schema.

   SQL *Net connect string
   > This string must match the string defined in the `$ORACLE_HOME/network/admin/tnsnames.ora` file.

   Click **Help** in the wizard for information about specific fields.
6. When you have finished configuring the data source, configure the connection associated with the data source.
   a. Click the name of the data source.
   b. Click the **Set Properties** icon in the Actions column.
   c. Click **Connections**.
   d. Click **Set...** next to **Open Session Commands**.
   e. Enter the following code, replacing *schema_name* with the name of the appropriate schema.

      Tip: The schemas have the same name as the data sources, except the PARAMETERS data source, which uses the NCPOLLDATA schema.

      ```
      <commandBlock>
       <commands>
        <sqlCommand>
             <sql>ALTER SESSION SET CURRENT_SCHEMA=schema_name</sql>
        </sqlCommand>
       </commands>
      </commandBlock>
      ```
   f. Apply the changes.
   g. Verify the signon properties of the connection.
      1) Test the connection using the **Signon** option. If the test is not successful, first verify that the username and password are correct by testing the connection using the **User ID and password** option, and then verify that the database details are correct.
      2) If necessary, edit the signon properties of the connection. Enter the username and password of a database user with access permissions to the database tables used by this data source. The default username is `itmuser`, with the password `netcool`.
7. Repeat these steps for each data source that you want to configure.

Configuring an Informix data source on AIX, Solaris, and Windows

To configure an Informix data source for Cognos reports on AIX, Solaris, and Windows, follow these configuration steps.

Complete the following tasks to configure an Informix data source.

1. Click **Reporting** > **Common Reporting** > **Network Manager**. Select **Administration** from the **Launch** menu. Click the **Configuration** tab.
2. Click the data source that you want to configure. Network Manager reports require the following data sources to be configured:
   - NCIM
   - NCMONITOR
   - NCPGUI
   - NCPOLLDATA
   - PARAMETERS

   Do not edit the data source IBM_TRAM.
3. Click **Connection**.
4. Select **Informix** as the connection type. Leave the other settings at the defaults. Click **OK**.
5. Follow the onscreen instructions to set up the connection. Ensure that you include the following Network Manager-specific information:

   User for database signon
   > Ensure that you enter a username and password combination that has access to the NCIM schemas used by the reports you want to use. For example, the default data source NCPOLLDATA uses the NCPOLLDATA NCIM schema, and the Informix configuration scripts give the user `ncpolldata` access to this schema.

   Informix database name
   > The default is `itnm`.

   Server name
   > The default is `ITNM`.

   Service
   > The default is `9088`.

   Click **Help** in the wizard for information about specific fields.
6. When you have finished configuring the data source, you can configure the connection associated with the data source. You must configure the connection if you have changed the username or password used to connect to the database.
   a. Click the name of the data source.
   b. Click the **Set Properties** icon in the Actions column.
   c. Verify the signon properties of the connection.
      1) Test the connection using the **Signon** option. If the test is not successful, first verify that the username and password are correct by testing the connection using the **User ID and password** option, and then verify that the database details are correct.
      2) If necessary, edit the signon properties of the connection. Enter the username and password of a database user with access permissions to the database tables used by this data source. The default username is `itmuser`, with the password `netcool`.

7. Repeat these steps for each data source that you want to configure.

Configuring an Informix data source on Linux and Linux for zSeries

To configure an Informix data source for Cognos reports on Linux and Linux for zSeries®, follow these configuration steps.

Complete the following tasks to configure an Informix data source.

1. Click **Reporting** > **Common Reporting** > **Network Manager**. Select **Administration** from the **Launch** menu. Click the **Configuration** tab.
2. Click the data source that you want to configure. Network Manager reports require the following data sources to be configured:
   - NCIM
   - NCMONITOR
   - NCPGUI
   - NCPOLLDATA
   - PARAMETERS

   Do not edit the data source IBM_TRAM.
3. Click **Connection**.
4. Copy the connection string.
5. Select **Other Type** as the connection type.
6. Paste the string into the **Connection string** box.
7. Leave the other settings at the defaults. Click **OK**.
8. Follow the onscreen instructions to set up the connection. Ensure that you include the following Network Manager-specific information:

   User for database signon
   Ensure that you enter a username and password combination that has access to the NCIM schemas used by the reports you want to use. For example, the default data source NCPOLLDATA uses the NCPOLLDATA NCIM schema, and the Informix configuration scripts give the user `ncpolldata` access to this schema.

   Informix database name
   The default is `itnm`.

   Server name
   The default is `ITNM`.

   Service
   The default is `9088`.

   Connection string

   Enter a string like the following:`^User ID:^?Password:;LOCAL;OD;driver=IBM INFORMIX ODBC DRIVER;host=`*hostname*`;server=`*server_name*`;database=`*database_name*`; service=`*service*`;protocol=olsoctcp;DELIMIDENT=Y;UID=%s;PWD=%s`

   Where:
   - *hostname* is the name of the server where Informix is installed.
   - *server_name* is the name of the server. By default, this is ITNM.
   - *database_name* is the name of the database. By default, this is `itnm`.
   - *service* is the name of the port. The default is 9088.

   Click **Help** in the wizard for information about specific fields.

9. When you have finished configuring the data source, you can configure the connection associated with the data source. You must configure the connection if you have changed the username or password used to connect to the database.

   a. Click the name of the data source.

   b. Click the **Set Properties** icon in the Actions column.

   c. Verify the signon properties of the connection.

      1) Test the connection using the **Signon** option. If the test is not successful, first verify that the username and password are correct by testing the connection using the **User ID and password** option, and then verify that the database details are correct.

      2) If necessary, edit the signon properties of the connection. Enter the username and password of a database user with access permissions to the database tables used by this data source. The default username is `itmuser`, with the password `netcool`.

10. Repeat these steps for each data source that you want to configure.

Configuring a MySQL data source

To configure a MySQL data source for Cognos reports, follow these configuration steps.

Complete the following tasks to configure a MySQL data source.

1. Click **Reporting** > **Common Reporting** > **Network Manager**. Select **Administration** from the **Launch** menu. Click the **Configuration** tab.

2. Click the data source that you want to configure. Network Manager reports require the following data sources to be configured:
   - NCIM
   - NCMONITOR
   - NCPGUI
   - NCPOLLDATA
   - PARAMETERS

   Do not edit the data source IBM_TRAM.

3. Click **Connection**.

4. Copy the connection string.

5. Select **Other Type** as the connection type.

6. Paste the string into the **Connection string** box.

7. Leave the other settings at the defaults. Click **OK**.

8. Follow the onscreen instructions to set up the connection. Ensure that you include the following Network Manager-specific information:

   User for database signon

   Ensure that you enter a username and password combination that has access to the NCIM schemas used by the reports you want to use. For example, the default data source NCPOLLDATA uses the NCPOLLDATA NCIM schema, and the MySQL configuration scripts give the user `ncpolldata` access to this schema.

   Connection string

   Enter a string like the following:`^User ID:^?Password:;LOCAL;OD;driver=MySQL;SERVER=hostname;DATABASE=database_name;PORT=port;OPTION=4096;UID=%s;PWD=%s`

Where:
- *hostname* is the name of the server where MySQL is installed.
- *database_name* is the name of the database. By default, this is `itnm`.
- *port* is the port on which MySQL is running.

Click **Help** in the wizard for information about specific fields.

9. When you have finished configuring the data source, you can configure the connection associated with the data source. You must configure the connection if you have changed the username or password used to connect to the database.

   a. Click the name of the data source.
   b. Click the **Set Properties** icon in the Actions column.
   c. Verify the signon properties of the connection.

      1) Test the connection using the **Signon** option. If the test is not successful, first verify that the username and password are correct by testing the connection using the **User ID and password** option, and then verify that the database details are correct.
      2) If necessary, edit the signon properties of the connection. Enter the username and password of a database user with access permissions to the database tables used by this data source. The default username is `itmuser`, with the password `netcool`.

10. Repeat these steps for each data source that you want to configure.

Changing the data source isolation level

The default isolation level for the Cognos ODBC data source is set to read committed. If you have multiple domains or have many polls running, or both, you might need to change the isolation level to read uncommitted for performance reasons and to avoid table locks that trigger errors.

To set the isolation level to read uncommitted, change the NCPOLLDATA data source settings as follows:

1. Click **Reporting** > **Common Reporting** > **Network Manager**. Select **Administration** from the **Launch** menu. Click the **Configuration** tab.
2. Click NCPOLLDATA.
3. Click the **Set properties** icon and then select the **Connection** tab.
4. Select **Read uncommitted** from the **Specify a value** drop down menu.

   Note: Some database vendors use different names for the isolation levels. See the Tivoli Common Reporting help and search for "isolation levels" for information on the levels available and their corresponding names on different database types.

5. Click **OK**.

Configuring BIRT reports to store database passwords using JNDI

For FIPS 140-2 compliance you can configuring BIRT reports to store NCIM passwords using the Java™ Naming and Directory Interface (JNDI).

To configuring BIRT reports to store NCIM passwords using JNDI, perform the following steps.

Restriction: The `setupITNMDatasources.jy` script only works for DB2 and Oracle.

1. 1. Remove the DB access information from the Birt reports.

   a. Edit the file `$NCHOME/../tipv2Components/TCRComponent/data/resource/ITNM39/itnm/lib/itnm_data_source.rptlibrary`.

   b. Remove the following properties for each datasource: `odaURL`, `odaUser`, and `odaPassword`.but leave the The lines to remove look similar to the following code snippet:

   ```
   <property name="odaURL">jdbc:db2://hostname:port/database_name</property>
   <property name="odaUser">root</property>
   <encrypted-property name="odaPassword" encryptionID="base64">
   encrypted_password</encrypted-property>
   ```

   Note: Do not remove the datasource `odaJndiName` property.

2. Run the `setupITNMDatasources.jy` script to create JNDI names for data sources.

   Note: Tivoli Integrated Portal must be running in order to use this script.

   The `$NCHOME/precision/bin/setupITNMDatasources.jy` script defines two sets of JNDI datasources for DB2 and Oracle, one for NCIM and one for NCPOLLDATA. These JNDI datasources are used by BIRT reports. The `setupITNMDatasources.jy` script is required in FIPS 140-2 installations where the encrypted database password must not be stored in the Tivoli Common Reporting `rptlibrary` file.

   The syntax for running the script is as follows:

   ```
   /opt/IBM/tivoli/tipv2/profiles/TIPProfile/bin/wsadmin.sh -lang jython -username
    tip_user_name -password tip_password -f setupITNMDatasources.jy
    -createDB2|-createOracle  all db_user_name db_user_password
    db_server_hostname db_database_name path_to_db2_jdbc_jar
   |path_to_oracle_jdbc_jar db_port
   ```

   Here is an example for a DB2 database: DB2

   ```
   /opt/IBM/tivoli/tipv2/profiles/TIPProfile/bin/wsadmin.sh -lang jython -username
    tipadmin -password netcool -f setupITNMDatasources.jy
    -createDB2  all db2inst1 netcool db2hostserver.ibm.com ITNM
   /opt/IBM/tivoli/tipv2Components/BIRTExtension/platform/plugins/
   org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers 50000
   ```

   Here is an example for an Oracle database: DB2

   ```
   /opt/IBM/tivoli/tipv2/profiles/TIPProfile/bin/wsadmin.sh -lang jython -username
    tipadmin -password netcool -f setupITNMDatasources.jy
    -createOracle  all ncim ncim oraclehostserver.ibm.com orcl
   /opt/IBM/tivoli/tipv2Components/TCRComponent/lib/birt-runtime-2_2_2
   /ReportEngine/plugins/
   org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers 1521
   ```

   Note: To modify an existing JNDI datasource, you must first delete the datasource and then create it again. For example, you must do this if the database password changes.

3. 3. Stop and and then restart Tivoli Integrated Portal.

setupITNMDatasources script

Use the setupITNMDatasources script to manage JNDI datasources.

Running the script

The script uses the following syntax.

Restriction: The setupITNMDatasources.jy script only works for DB2 and Oracle.

```
DB2
```

```
/opt/IBM/tivoli/tipv2/profiles/TIPProfile/bin/wsadmin.sh -lang jython -username
 tip_user_name -password tip_password -f
 setupITNMDatasources.jy [ -createDB2|-createOracle  all db_user_name
db_user_password db_server_hostname db_database_name
 path_to_db2_jdbc_jar|path_to_oracle_jdbc_jar db_port]
 [ -display ] [ -delete ]
```

Command-line options

The following table describes the command-line options for the setupITNMDatasources script.

Table 16. setupITNMDatasources command-line options

Command-line option	Description
-createDB2	Creates a DB2 datasource.
-createOracle	Creates an Oracle datasource.
-display	Displays all current datasources.
-delete	Removes all current datasources.

Chapter 11. Troubleshooting and support

Use this information to help you resolve problems with the product.

Troubleshooting Network Manager

Consult these troubleshooting notes to help determine the cause of the problem and what to do about it.

Related tasks:

Chapter 3, "Administering logs," on page 25
Network Manager provides logging capabilities for its GUI components and back-end processes. You can set up logging for Network Manager to produce log or trace files that can be used for troubleshooting purposes.

Troubleshooting Tivoli Integrated Portal

Consult these troubleshooting notes to help determine the cause of the problem and what to do about it.

Login errors
Anything from an unassigned user role to a loss of connectivity with the user repository can cause a login error. Read the TIPProfile logs for help in diagnosing the cause.

Harmless authentication messages:

Certain sign-on messages are routine and might not indicate that a problem has occurred.

For installations that have been configured to use the Tivoli Integrated Portal authentication service, it is possible that an authentication client receives CTGES1504E and CTGES1505E messages. These messages are generated when an unused single sign-on LTPA token is discarded, and might be insignificant.

An authentication client attempts to use all single sign-on tokens provided to it when authenticating to an authentication service. Some of these tokens might not apply to the configured authentication service, causing CTGES1504E and CTGES1505E messages to be generated on the client and CTGES1089E on the server. When not accompanied by other CTGES0008E authentication client errors, these messages indicate only that a particular single sign-on token was discarded.

Already logged in:

Read this topic if you closed your work session and then tried to log in again, but received a message that the user ID was already logged in.

If you are logged in to the portal and close the browser window, you might not be logged out. Because you closed the browser, though, you need to log in again to start another work session. If, while logging in, you get a message that the user ID is already logged in and do you want to log out the other user, accept the request.

No user role assigned:

Users cannot log in to the console if they do not have user roles assigned.

If you have a valid user ID and password but get a message that the login failed and to try again (even after successive retries), ask your administrator to review your role assignments.

Every user ID must be assigned the minimum roles necessary to log in to the application server: Monitor, Configurator, Operator, Deployer, or Administrator. Users should also have the minimum required product level roles or they might not see the contents of their default product pages after logging in.

Slow network response:

Performance issues can cause an unresponsive script message to display after login.

If, immediately after logging in, you get a message about an unresponsive script and you are asked whether to continue or cancel opening the Web page, click **Continue**. After a short time, the welcome page for the console is displayed.

Such messages can indicate a slow network link between your computer and the application server. Ping the server computer to see the round trip response time. Use response times of 40 ms or better.

Try using a remote desktop connection to a computer that has a better response time with the application server and logging in from there.

Consider using a caching HTTP proxy to improve speed and reduce network traffic.

Viewing TIPProfile logs for login errors:

In the event of a login error, review the system outage and system error logs to help determine the cause.

Follow these steps to open the system outage and system error logs:
1. At the command line, change to the `tip_home_dir`/profiles/TIPProfile/logs/ server1 directory.
2. Open `SystemOut.log` and `SystemErr.log` in a text editor. On Windows, for example, the command `notepad systemout.log` opens the log in Windows Notepad.
3. Review the errors.
4. If the cause and solution to your login error is not apparent, send the `SystemOut.log` and `SystemErr.log` from this directory and the `server1_exception.log` (and any other files that were modified within a few minutes of this one) from the sibling `ffdc` directory to your security administrator for further examination.

Related tasks:

Open the application server profile to review the port number assignments and other information.

Viewing the application server profile

Open the application server profile to review the port number assignments and other information.

The profile of the application server is available as a text file on the computer where it is installed.

1. Locate the *tip_home_dir*/profiles/TIPProfile/logs directory.
2. Open AboutThisProfile.txt in a text editor.

This is the profile for an installation on in a Windows environment as it appears in *tip_home_dir*\profiles\TIPProfile\logs\AboutThisProfile.txt:

```
Application server environment to create: Application server
Location: C:\IBM\tivoli\tip\profiles\TIPProfile
Disk space required: 200 MB
Profile name: TIPProfile
Make this profile the default: True
Node name: TIPNode Host name: tivoliadmin.usca.ibm.com
Enable administrative security (recommended): True
Administrative consoleport: 16315
Administrative console secure port: 16316
HTTP transport port: 16310
HTTPS transport port: 16311
Bootstrap port: 16312
SOAP connector port: 16313
Run application server as a service: False
Create a Web server definition: False
```

If you want to see the complete list of defined ports on the application server, you can open *tip_home_dir*/properties/TIPPortDef.properties in a text editor:

```
#Create the required WAS port properties for TIP
#Mon Oct 06 09:26:30 PDT 2008
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=16323
WC_adminhost=16315
DCS_UNICAST_ADDRESS=16318
BOOTSTRAP_ADDRESS=16312
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=16321
SOAP_CONNECTOR_ADDRESS=16313
ORB_LISTENER_ADDRESS=16320
WC_defaulthost_secure=16311
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=16322
WC_defaulthost=16310
WC_adminhost_secure=16316
```

Related tasks:

"Viewing TIPProfile logs for login errors" on page 130
In the event of a login error, review the system outage and system error logs to help determine the cause.

Editing a properties file

Properties files describe the environment and their settings are usually predefined or added during installation. You do not need to change these files unless instructed by IBM Software Support.

The properties files are on the computer where the Tivoli Integrated Portal Server is installed.

1. Locate the *tip_home_dir*/properties directory. For example, C:\IBM\tivoli\tipv2\properties is the default installation path on Windows; /opt/IBM/tivoli/tipv2/ is the default installation path on Linux or UNIX.
2. Open the desired properties file in a text editor.

3. Edit the file as needed, and then save and close it.
4. Stop the application server, and then restart it.

Setting a trace

Enable a trace of the Tivoli Integrated Portal Server when you want to keep a record of activity.

The portal has a Troubleshooting Logs and Trace option for enabling a trace.

Follow these steps to set a trace that will record the Tivoli Integrated Portal Server actions in a log file: `tip_home_dir`/profiles/TIPProfile/logs/`server`/trace.log.

1. In the portal, click **Troubleshooting > Logs and Trace**.
2. Select the Tivoli Integrated Portal Server name (such as server1) in the Logging and Tracing portlet.
3. In the **Configuration** tab, click **Change Log Detail Levels**.
4. In the **Groups** list, expand **com.ibm.tivoli.*** and click **com.ibm.tivoli.tip.***.
5. Select a log level (such as **All Messages and Traces**) and click **OK** or **Apply**.
6. When prompted to save the configuration, click **Save**.
7. Stop and restart the Tivoli Integrated Portal Server:
   a. In the `tip_home_dir`/profiles/TIPProfile/bin directory, depending on your operating system, enter one of the following commands:
      - `Windows` `stopServer.bat server1`
      - `UNIX` `Linux` `stopServer.sh server1`

      Note: On UNIX and Linux systems, you are prompted to provide an administrator username and password.
   b. In the `tip_home_dir`/profiles/TIPProfile/bin directory, depending on your operating system, enter one of the following commands:
      - `Windows` `startServer.bat server1`
      - `UNIX` `Linux` `startServer.sh server1`

After the server has been stopped and restarted, trace entries are saved to the `tip_home_dir`/profiles/TIPProfile/logs/server1/trace.log file.

Related tasks:

"Starting and stopping the Tivoli Integrated Portal" on page 4
The Tivoli Integrated Portal Server starts automatically after it has been installed and whenever the computer is started. You can manually stop the server before beginning certain configuration tasks or as needed.

Checking hostname settings

The value of the Hostname property in the `tip_home_dir`/properties/ `tip.properties` file is used by Tivoli Integrated Portal to convert incoming browser requests (for example, http://<*SystemName*>:16310) to the appropriate Tivoli Integrated Portal non-secure access (for example, http://<*HostnameValue*>:16315)/ ibm/console), which is then converted to the Tivoli Integrated Portal secure access (for example, https://<*HostnameValue*>:16316/ibm/console/login.jsp).

The Hostname property should contain the fully qualified hostname. This is required if the web browser being used to access Tivoli Integrated Portal is running on a machine in a different DNS domain to the Tivoli Integrated Portal Server (application server).

The value of the *tip_home_dir*/properties/tip.properties file's Hostname entry is set during installation by a routine built into Java that checks the /etc/hosts (or %WinDir%\system32\drivers\etc\hosts) entry for the system; if the fully qualified domain name (FQDN) is not set in /etc/hosts, the Java routine returns either the short name or the IP address of the machine, depending on the type of operating system (all but AIX).

Therefore, before the Network Manager installer is run, ensure that a line exists in /etc/hosts of the following form:

IP address FQDN shortname
For example: 9.10.11.12 yourserver.domainname.com yourserver

This line ensures that the FQDN is set as the Hostname entry at install time in *tip_home_dir*/properties/tip.properties.

If you try to connect to the application server and the URL conversion to the non-secure access appears to be working incorrectly, you should check Hostname property entry in tip.properties.

1. Open the *tip_home_dir*/properties/tip.properties file in a text editor.
2. Check the Hostname property and make sure the value can be correctly resolved by the web browser being used to access the application server.
3. Edit the Hostname entry to the FQDN of the application server and save the changes.
4. Stop and restart the application server. The changes take effect when the application server is restarted.

Increasing memory for the Java Virtual Machine

This task describes how to increase the amount of memory available to the Tivoli Integrated Portal.

To increase the amount of memory available to the Java Virtual Machine (JVM), carry out the following steps:

1. Manually stop the application server.
2. Change to the *tip_home_dir*/profiles/TIPProfile/bin directory.
3. Use the **wsadmin** command to increase the heap size for the JVM, as follows:
   wsadmin.sh -lang jython -conntype NONE
4. At the wsadmin> prompt, issue the following commands, where *xxx* is the new heap size value, in megabytes.

   ```
   jvm=AdminConfig.list("JavaVirtualMachine")

   AdminConfig.modify(jvm, '[[initialHeapSize xxx]]')
   AdminConfig.modify(jvm, '[[maximumHeapSize xxx]]')
   AdminConfig.save()

   exit
   ```
5. Clean the server1 and tnm logs and restart the Tivoli Integrated Portal Server. The changes take effect when the Tivoli Integrated Portal Server is restarted.

Attention: If you attempt to start the Tivoli Integrated Portal Server with a maximum heap size that is too large, error messages that are similar to the following are generated in the *tip_home_dir*/profiles/TIPProfile/logs/server1/native_stderr.log file:

```
JVMJ9GC019E -Xms too large for -Xmx
JVMJ9VM015W Initialization error for library j9gc23(2): Failed to initialize
Could not create the Java virtual machine.
```

Chart errors

Consult this list of possible causes of charting errors and suggested solutions.

BIRT report design format is not valid
> The report designs that you create in the BIRT Designer should contain a single data set and a single chart or table and nothing else. Other items in the report might cause the error,
>
> ```
> TIPCH0005E The design format for the chart or table is not valid
> ```
>
> If you receive this error, modify your chart .rptdesign, upload it again, and open it in a chart portlet.

Chart does not render or is very slow to render because the amount of data is too large
> When you open a BIRT designed chart that has a large amount of data, it is possible to exceed the capacity of the application server. If this happens, you will get an error message. Try pre-filtering the data so that only values of interest get retrieved.
>
> Also, be sure to single-click pages that have chart portlets in them. The page might not display correctly or render the chart when it is double-clicked from the navigation tree.

Chart portlet might not display in portlet list
> While working in with a charting portlet, you can change the type of chart by selecting another one from a list of available charts. Although it is unlikely, it is possible for the list to not populate with the available charts. If this happens, log out of the portal, restart your browser, and log in again.

Cannot copy and add the charting portlet to a new page
> When copying the Charting portlet and adding it to a new page, you might get this message:
>
> ```
> CWLAA6003 Could not display the portlet,
> the portlet may not be started. Check the error logs
> ```
>
> If this happens, ensure the charting role that your user ID is assigned to has the Editor access level assigned.

Error messages while using the Charting portlet
> While using the charting portlet, you could get this error message:
>
> ```
> TIPMSG1003E  An error occurred while making the server request.
> Error: 'dojo.byId(...)' is null or not an object
> ```
>
> Alternatively, it might be an EOF (End Of File) exception that appears. If either of these errors occurs, close the error message window and proceed. Most of the time the chart will load; if it does not, you can either click ⟳ **Refresh** in the portlet or reload the chart from the selection.

Many users are loading to the same page that has charting portlets
> This error can be displayed if too many users attempt to open a chart in the same page at the same time:

```
TIPCH0006E An error occurred while collecting data for the chart,
check the web service data source.
Cannot set the string value () to parameter 1 java.rmi.RemoteException:
KFWITM220E Request failed during execution;
nested exception is: KFWITM220E Request failed during execution.
```

This error can happen when the system is overloaded with requests. Close the error message window, then click ⟳ **Refresh** in the chart portlet.

Closing many chart portlet pages in quick succession gives an error

When running the portal in the Firefox browser, you might get this error if you quickly close many pages that have chart portlets:

```
TIPMSG1003E  An error occurred while making the server request.
Error: dojo.byId(this.namespace + "chartNameH") has no properties
```

If this happens, close the error message window and proceed. The pages will eventually close without error.

Cannot get the result set metadata from the ITM Web Service

When you connect to the ITM Web Service from the BIRT Designer to create a custom chart, you might receive an error message, `Cannot get the result set metadata` while creating a chart. Here are some possible causes to review with your Tivoli Monitoring administrator:

- The IBM Tivoli Monitoring agent (or agents) is stopped or has connectivity problems.
- The query is not supported by the Charting portlet or BIRT Designer. The Charting portlet uses the view's definition, including any filters applied. The BIRT Designer enables you to modify the query. You can check the BIRT Designer log file at `<BIRTDesigner>\workspace\ .metadata\.log` for exception details. If you see this exception, the query might not be supported in this release:

  ```
  Caused by: org.apache.axis2.AxisFault: java.rmi.RemoteException:
  KFWITM220E Request failed during execution.
  ```

  In the Tivoli Enterprise Portal, click ❓ **Query editor** and look for the query in the navigation tree. If the query is not listed, it will not be available to the BIRT Designer or Charting portlet. Ask your administrator to check the log files.

- If this is long-term historical data that is being retrieved, the Tivoli Data Warehouse Proxy agent is stopped or has connectivity problems. These are examples of errors that can occur when a view type is chosen that queries historical data, but no data exists to return.

  ```
  TIPCH0006E An error occurred while collecting data for the chart:
  Cannot get the result set metadata.java.rmi. RemoteException:
  KFWITM220E Request failed during execution; nested exception is:
  KFWITM220E Request failed during execution.
  ```

  Historical data queries require that historical data collection be configured and started for the attribute groups and that sufficient data bas been gathered to render a historical view. Furthermore, summarized historical data requires that the Summarization and Pruning agent also be configured and the process completed at least once before querying summarized and pruned data.

Timeout or message about not connecting to the server

If the system times out or an error message is displayed while importing an Tivoli Monitoring chart, it is typically because the Tivoli Enterprise

Portal Server is unavailable for some reason. Check that the portal server is online and start it if it is not. Then try importing the chart again. If the error is

```
TIPMSG1000E Detail: AxisFault
```

open *<install_dir>*/properties/charts.properties in a text editor and increase the value of this parameter (180000 is 3 minutes):
```
AXIS_TIMEOUT=180000.
```

Unable to view Tivoli Monitoring charts after installing the Web GUI followed by Tivoli Business Service Manager
This error can be displayed when you attempt to load a chart from the ITM Web Service:

```
Axis Fault: Error initializing ITM Import Manager
```

The ITM Web Service needs to be configured with the login ID for the Tivoli Enterprise Portal Server. Use the ITMLogin command as described in the "Additional commands" on page 179.

Loading a chart from an ITM Web Service continues indefinitely
This error can happen in a saved chart page when the administrative console is running in the Firefox browser and the **Page persistence** setting in the General properties is set to **None**. You can click **Refresh** in the browser toolbar. You can also change **Page persistence** to **Client**, and then **Save** the page with this setting.

Avoid double-clicking pages in the navigation tree. If you double-click a page that contains a charting portlet, the page might not display correctly or render the chart. A single click is all you need to do.

Problems loading a page after changing to another ITM Web Service
After adding the ITM Web Service and populating charts with data from Tivoli Enterprise Monitoring Agents and OMEGAMON XE agents, do not switch to a different ITM Web Service because there is no guarantee that the same charts and queries will be available and there might be problems loading the page.

Use the chart selector from the chart toolbar to load a different chart. In addition, the ITM Web Service must be installed in the same instance as the application server.

Cannot connect to an ITM Web Service from a remote Tivoli Integrated Portal Server Connection to an ITM Web Service from a remote application server will not be successful and is not supported in this release. The remote server must define its own Web service connection to be able to import charts from that Web service.

Imported charts are inconsistent with their Tivoli Monitoring counterpart
Many of the Tivoli Enterprise Portal workspaces are designed for showing data from all the managed systems within the enterprise. When these charts are imported into the console, users might notice that some of the charts show data for all managed systems, without grouping data under each managed system name.

To view a subset of the data for the chart, right-click the chart portlet and click **Preferences**. Specify the managed system name in the **Parameters** tab. The result will be a chart showing data for only the managed system name that was specified. Ensure that the text entered matches the managed system name as it appears in the Tivoli Enterprise Portal client, such as `myhostname:NT`.

Tivoli Business Service Manager users can import Tivoli Monitoring resources into the Service Component Registry using the Xmltoolkit. Whenever the service is clicked in the service tree, the charting portlet automatically receives the managed system name as context (no need to specify the name in Preferences > Parameters).

Too many active report queries

When importing charts from a Tivoli Enterprise Portal Server that is at Version 6.2 (not Version 6.2 Fix Pack 1 or later), the portal server might get a message about too many active report queries. If this happens, add the following environment variable to the portal server environment file:

```
KFW_REPORT_REQUEST_LIMIT=100
```

where 100 is the maximum number of outstanding requests that the portal server will allow from each agent. The default value for IBM Tivoli Monitoring V.6.2 is 15. The environment file is opened in a text editor through Manage Tivoli Monitoring Services or the command line:

Windows   `<itm_install_dir>\cnps\kfwenv`

Linux   `<itm_install_dir>/config/cq.ini`

UNIX   `<itm_install_dir>/config/cq.ini`

After editing the environment file, and recycling the Tivoli Enterprise Portal Server, try importing charts again. Adjust the report request limit if you continue to get the same error.

Related concepts:

Chapter 9, "Administering charting," on page 103
The Charting feature enables you to retrieve data from IBM Tivoli applications such as Tivoli Monitoring and Tivoli Business Service Manager and from custom charts that were designed with the Eclipse Business Intelligence and Reporting Tools Designer.

Tivoli Enterprise Portal Server is offline:

You need connectivity with the Tivoli Enterprise Portal Server when installing the ITM chart feature and when importing Tivoli monitoring agent data for rendering charts.

Importing a Tivoli Monitoring chart

To retrieve Tivoli Monitoring agent attribute values for rendering in a chart, a query is sent to the Tivoli Enterprise Portal Server. If the portal server is unavailable for some reason, the message number **TIPMSG1000E** is displayed. Check that the server is online and start it if it is not.

Disabling Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration is an option that is provided in Windows Server 2003 operating systems and above. To use Network Manager in Tivoli Integrated Portal, you must disable Internet Explorer Enhanced Security Configuration.

Follow these steps to disable Internet Explorer Enhanced Security Configuration:
1. Close all instances of Internet Explorer.
2. Click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
3. If a User Account Control dialog is displayed, click **Continue**.

4. Under **Security Summary**, click **Configure IE ESC**.

5. Under **Administrators**, click **Off**.

6. Under **Users**, click **Off**.

7. Click **OK**.

Internet Explorer Enhanced Security Configuration is disabled.

Troubleshooting Web Applications

Use this troubleshooting information to help you resolve common problems that might occur when you administer the Web applications.

Device not found

A `Device Not Found` error might occur when you right-click an event in the Tivoli Netcool/OMNIbus Web GUI and click **Find in Hop View**.

This error appears for one of the following reasons:

- There is no corresponding device in the topology. If this is the case, you should check that:
  - You have configured the scope of the discovery so that it includes this device.
  - You have run the appropriate Discovery Agent to discover this device.
  - The device is a supported network device.
  - The device has been discovered, as it may have recently come online and need to be discovered.
- The event came from a probe that has not been configured to include the fields that Network Manager requires to locate the device. This is the most likely cause of the error if the device is in the topology.

Topoviz screen is blank

If Topoviz fails to start, or starts with a blank screen, refresh the browser window. If the Network Manager splash screen does not appear, check the topology database access settings.

Related tasks:

"Configuring GUI access to the topology database" on page 85
If you have changed the NCIM settings, you must configure access for the Network Manager Web applications.

Unable to access domain

If the **Domain** drop-down list does not show the expected domain, check your topology database access settings. Also check the `$TIPHOME/profiles/TIPProfile/logs/server1/SystemOut.log` and `$TIPHOME/profiles/TIPProfile/logs/server1/SystemErr.log` files for relevant information.

Unable to execute right-click tools in AEL

If the **Show Root Cause** or **Show Suppressed Events** context menu options fail to execute and return an error message, this might be because the CGI scripts, which are run when you select these menu options, are unable to find the path to Perl.

If you have installed Perl in a nonstandard location, ensure that you have specified the correct path to Perl in all CGI scripts.

Device in Topoviz appears as generic node

If a device is known to be a switch or router but appears in the Network Hop View or in the Network Views as a generic node icon, then the device may not be correctly mapped to an icon in its active object class (AOC) file.

Cause

Device was discovered correctly and is mapped to an AOC file. One way to check this is to make sure that in the Network Views, the device can be located in one of the Device Class network views.

Resolving the problem

Certain AOC files do not give a visual icon but rather use the statement `visual_icon = ' ';`. In this case the AOC file (and the corresponding device) takes the visual_icon from the super_class of the AOC.

Example

An example is the Extreme.aoc and ExtremeSummit.aoc file. The super_class for Extreme.aoc is Device.aoc file, which uses the 'Device' icon. If you would like any device instantiated as an Extreme.aoc to be seen in Network Hop View or in the Network Views as a switch or router, edit the AOC file and use the statement `visual_icon = 'Switch';`; or `visual_icon = 'Router;` in place of `visual_icon = ' ';`.

Unable to copy network view

If you get an error message while trying to copy a network view from one user to another or you notice that certain network views are blank, and the NCIM topology database in use is Informix, then the database might be missing a dbspace file.

To check whether the error condition is caused by a missing dbspace file in the Informix database, perform the following check:

- Open the `ITNMHOME/profiles/TIPProfile/logs/tnm/ncp_topoviz.0.log` log file.
- Look for the following text:`Caused by: java.sql.SQLException: Smart-large-object error`

  If you find this text, it means that the error is caused by the missing Informix dbspace file.

To resolve this error, use the Informix `onspaces` command-line utility to create an ncimsbspace dbspace. For more information on this procedure, see the information on installing and configuring the Informix database in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Troubleshooting reporting

If you have problems with Tivoli Common Reporting, check the troubleshooting information.

Polled data reports contain null values

If reports on polled data contain null values, you might need to run the drop_polldata.pl script.

Over time, with the addition and removal of entities, the ncmonitor.monitoredInstance table can contain instances of entityIds that have since been removed from the ncim.entity table. This can result in polled data reports containing null information. Complete the following steps to fix this problem:

1. Run the following command to determine whether your database contains null values:

   ```
   select count(*) from ncpolldata.monitoredInstance where
   instanceType = 'ifIndex' and entityId is null; select count(*) from
    ncpolldata.monitoredInstance where
   instanceType = 'ifIndex' and entityId not in (select entityId
   from ncim.interface);
   ```

2. If any values are returned from the above query, run the following script to delete the polled data for a domain:

   ```
   perl drop_polldata.pl -domain domain
   ```

   Where *domain* is the domain for which you want to delete polled data.

Viewing reporting log files

You can view the log files for Tivoli Common Reporting to check for problems.

The log files for Tivoli Common Reporting are in the following locations

- `TIPHOME/logs`
- `tipv2/profiles/TIPProfile/logs`
- `tipv2Components/TCRCompoenents/cognos/logs/`
- `tipv2Components/TCRCompoenents/cognos/contentstore/`
- `tipv2Components/TCRCompoenents/logs/`
- `tipv2/logs/`

Changing the logging level for reporting

You can increase the logging level to help debug problems.

To change the logging level for a reporting process, complete the following steps.

1. Log into the Tivoli Integrated Portal.
2. Click **Troubleshooting** > **Logs and Trace**.
3. Change the logging level for processes beginning `com.ibm.tivoli.reporting`. For information about how to use the Logging and Tracing window, see the online help.

Troubleshooting database access

In the event of problems with access to the topology database, historical polling database, or polling database, run the ncp_db_access.pl script. This script checks database setup and determines whether access to the databases is being prevented by firewalls.

The **ncp_db_access.pl** script checks database setup and firewall issues for the following databases:

- NCIM topology database
- NCMONITOR polling database
- MIB historical polling database

1. Before running the script, check that the password of the user that connects to the database has not expired.
2. Change to the $NCHOME/precision/scripts/perl/scripts directory and locate the ncp_db_access.pl program.
3. Issue the following command.
   perl ncp_db_access.pl -domain *domain_name*
   Where:

   - *domain_name* is the name of the required domain.

   For each database the script indicates whether connection is in order or if there are access problems.

Troubleshooting unresponsive portlets

If portlets in the GUI that use Java become unresponsive, try increasing Java memory options.

Sometimes, pages containing Hop view or Network view portlets stop responding. A java.lang.OutOfMemoryError error message might be received in the Java console. If this happens, increasing the applet memory might solve the issue. To increase the applet memory, complete the following steps.

1. Open the Java control panel.

   a. � Windows ▏ Click **Start** > **Control Panel** > **Java Control Panel** > **Java** > **Java Applet Runtime Settings** > **View**.

   b. ▏ UNIX ▏ Open the control panel in $JAVA_HOME/bin/ControlPanel.

2. Type the following in the Java Runtime Parameter field: **-Xms256M -Xmx512M**. The -Xms option specifies the initial amount of memory, in MB. The -Xmx option specifies the maximum amount of memory, in MB, and can be increased up to 1024MB. The values you specify depend on your system and on the number of devices or events you are trying to view.

Appendix A. Command reference

Use this information to understand which commands to use to start Network Manager processes. It is good practice to configure the master process controller, ncp_ctrl, to launch and manage Network Manager processes. You can also start processes manually using the command-line options described here.

For further information on databases related to Network Manager processes, see the *IBM Tivoli Network Manager IP Edition Management Database Reference*.

itnm_status command-line options

Use the **itnm_status** command, with optional advanced arguments, to retrieve information about whether the individual components or all components are running.

The **itnm_status** script is started by using the following command line; optional arguments are shown enclosed in square brackets. `itnm_status` *components* `-verbose -help`

The following table describes the command-line options for **itnm_status**.

Table 17. itnm_status command-line options

Command-line options	Description
components	Optional; one or more component abbreviations. If no component is specified, the status of all components is reported. The following component abbreviations are possible: **IBM Tivoli Netcool/OMNIbus** nco **Network Manager** ncp **Tivoli Integrated Portal** tip
`-verbose`	Optional; provides more information on the screen.
`-help`	Optional; displays help on screen.

itnm_start command-line options

Use the **itnm_start** command, with optional advanced arguments, to start Network Manager components.

The **itnm_start** script is started by using the following command line; optional arguments are shown enclosed in square brackets.

`itnm_start [ `*components*` ] -domain `*precision_domain*` [ -verbose ] [ -help ]`

The following example starts the core components in domain NCOMS:

`itnm_start ncp -domain NCOMS`

The following table describes the command-line options for **itnm_start**.

Table 18. itnm_start command-line options

Command-line options	Description

components	Optional; one or more component abbreviations. If no component is specified, all components are started. The following component abbreviations are possible:
	
	IBM Tivoli Netcool/OMNIbus
	    nco
	
	Network Manager
	    ncp
	
	Tivoli Integrated Portal
	    tip

-domain *DomainName*	Optional; applies to the Network Manager domain. If not used, then the default domain is used (the one specified during install).
-verbose	Optional; provides more information on the screen.
-help	Optional; displays help on screen.

Related tasks:

"Starting all components on the same server (UNIX only)" on page 2
If the Tivoli Integrated Portal, Tivoli Netcool/OMNIbus, and Network Manager are installed on the same server, you can start them using the **itnm_start** command.

itnm_stop command-line options

Use the **itnm_stop** command, with optional advanced arguments, to stop Network Manager components.

The **itnm_stop** script is started by using the following command line; optional arguments are shown enclosed in square brackets.

```
itnm_stop [ components ] -domain precision_domain [ -verbose ] [ -help ]
```

The following example stops the core components in domain NCOMS:

```
itnm_stop ncp -domain NCOMS
```

The following table describes the command-line options for **itnm_stop**.

Table 19. itnm_stop command-line options

Command-line options	Description

components	Optional; one or more component abbreviations. If no component is specified, all components are stopped. The following component abbreviations are possible:
	
	IBM Tivoli Netcool/OMNIbus
	    nco
	
	Network Manager
	    ncp
	
	Tivoli Integrated Portal
	    tip

Table 19. itnm_stop command-line options (continued)

Command-line options	Description
-domain *DomainName*	Optional; applies to the Network Manager domain. If not used, then the default domain is used (the one specified during install).
-verbose	Optional; provides more information on the screen.
-help	Optional; displays help on screen.

Related tasks:

"Stopping all components on the same server (UNIX only)" on page 5
If they are installed on the same server, you can stop the Tivoli Integrated Portal, Tivoli Netcool/OMNIbus, and all Network Manager processes, using the **itnm_stop** command.

ncp_class command-line options

Use the ncp_class command, with optional advanced arguments, to start the Active Object Class manager.

It is best practice to configure the ncp_ctrl process, the master process controller, to launch and manage the ncp_class process.

Attention: If you are using Network Manager IP Edition with failover, you must start CLASS using the ncp_ctrl process. The ncp_ctrl process checks the status of the ncp_class process and uses this information to generate the Health Check events used by the failover process.

Prequisites

For CLASS to run, it requires access to the NCIM database. The connection and access to the database is performed automatically, you do not need to do anything.

The AOC files define the class hierarchy. There is a copy of this hierarchy in the entityClass NCIM database table. If changes are made to the AOC files, CLASS updates the entityClass database table when it connects to the NCIM database to reflect any changes to the AOC hierarchy.

Note: If you create a new AOC file, you should also add a new insert to the class.classIds database table in the ClassSchema.cfg configuration file.

Command

To manually start CLASS, run the ncp_class command.

The command line options for ncp_class are:
```
ncp_class -domain DOMAIN_NAME [ -cachesize SIZE_IN_MB ][ -cachepercent
PERCENTAGE_OF_CACHE_IN_MEMORY ]
[ -debug DEBUG ][ -messagelevel MESSAGELEVEL ]
[-messagelog PATHTOLOGFILE][ -help ][ -latency LATENCY ]
[ -read_aocs_from DIRECTORY_NAME ][ -version ]
```

The following table describes the command-line options of the ncp_class command.

Table 20. `ncp_class` command-line options

Option	Explanation
`-cachesize SIZE_IN_MB`	Specifies the size of the cache in megabytes (MB).
`-cachepercent PERCENTAGE_OF_CACHE_IN_MEMORY`	Enables you to specify the ratio of the cache that is resident in memory to the cache that is resident on the hard disk. The ratio that you specify depends on the amount of memory that exists on the host machine and the number of processes it is running. The default value is 100% cache.
`-domain DOMAIN_NAME`	The name of the domain under which to run CLASS.
`-debug DEBUG`	The level of debugging output (1-4, where 4 represents the most detailed output).
`-messagelevel MESSAGELEVEL`	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
`-messagelog PATH_TO_LOGFILE`	The path to the message log file.
`-help`	Displays the command line options. Does not start the component even if used in conjunction with other arguments.
`-latency LATENCY`	The maximum time in milliseconds (ms) that CLASS waits to connect to another Network Manager IP Edition process by means of the messaging bus. This option is useful for large and busy networks where the default settings can cause processes to assume that there is a problem when in fact the communication delay is a result of network traffic.
`-read_aocs_from DIRECTORY_NAME`	The full path of the directory from which to read the AOC definitions.
`-version`	Displays the version number of the component. Does not start the component even if used in conjunction with other arguments.

When CLASS is launched it obtains the AOC definitions either from a directory of AOC files or from the cache files contained in `NCHOME/var/precision`.

You can control the location of the source AOC definitions using the command line options. The possible combinations are as follows:

- If you omit the `-read_aocs_from` argument from the command line, CLASS automatically reads the cache files from `NCHOME/var/precision` if they are present. If there are no valid cache files, CLASS uses the definitions in `NCHOME/precision/aoc`.
- If you specify a directory using the `-read_aocs_from` option, CLASS initializes itself with the AOCs located in the specified directory. CLASS automatically moves any existing cache files to a backup directory.

Regardless of the options specified, CLASS generates a warning if the files within the `NCHOME/precision/aoc` directory are more recent than the cache files contained within the `NCHOME/var/precision` directory.

For more information about failover, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

ncp_config command-line options

Use the ncp_config command, with optional advanced arguments, to start the
Network Manager GUI configuration file server.

The ncp_config process provides a means for the configuration GUIs to read from
and write to schema files.

It is started and stopped automatically by the shell scripts that launch the GUIs
and so in general need not be manually started.

You can also start the `ncp_config` process manually using the following command
line—optional arguments are shown enclosed in square brackets.

```
ncp_config –domain DOMAIN_NAME [ -debug DEBUG ] [ -latency LATENCY ]
[ -messagelevel MESSAGELEVEL] [ -messagelog PATHTOLOGFILE] [ -query QUERY ]
[ -read_schemas_from DIRECTORY_NAME ] [ -write_schemas_to DIRECTORY_NAME ]
[ -logdir ] [ -nologdir DIRNAME ] [ -help ] [ -version ]
```

Command line options for the ncp_config process are explained in the following
table:

Table 21. Explanation of Command Line Options

Option	Explanation
-domain *DOMAIN_NAME*	The name of the domain under which to run the ncp_config process. Data saved in the GUI is saved to the domain name that you specify here.
-debug *DEBUG*	The level of debugging output (1-4, where 4 represents the most detailed output).
-latency *LATENCY*	The maximum time in milliseconds (ms) that the ncp_config process waits to connect to another Network Manager process using the messaging bus. This option is useful for large and busy networks where the default settings can cause processes to assume that there is a problem when in fact the communication delay is a result of network traffic.
-messagelevel *MESSAGELEVEL*	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
-messagelog *PATHTOLOGFILE*	The path to the message log file.
-query *QUERY*	A query statement to pass to the OQL Service Provider. This option is designed to run the `ncp_config` process in batch mode. In batch mode, `ncp_config` processes the OQL query statement against the requested database, writes the schema files, and exits.

Table 21. Explanation of Command Line Options　(continued)

Option	Explanation
-read_schemas_from *DIRECTORY_NAME*	The full path of the directory from which the ncp_config process reads the schema files. This command line option can only be used when starting the ncp_config process manually. If this option is not specified, NCHOME/etc/precision is used as a default.
-write_schemas_to *DIRECTORY_NAME*	The full path to which the ncp_config process writes the schema files. This command line option can only be used when starting the ncp_config process manually. If no path is specified, the ncp_config process updates the files in the source directory, saving a backup of the existing schema.
-help	Displays the command line options. Does not start the component even if used in conjunction with other arguments.
-version	Displays the version number of the component. Does not start the component even if used in conjunction with other arguments.

ncp_ctrl command-line options

Use the ncp_ctrl command, with optional advanced arguments, to start the master process controller.

The ncp_ctrl process is started by using the following command line; optional arguments are shown enclosed in square brackets.

```
ncp_ctrl –domain DOMAIN_NAME [ -debug DEBUG ]
[ -messagelevel MESSAGELEVEL ] [ -messagelog PATHTOLOGFILE ]
[ -help ] [ -version ] [ -latency LATENCY ]
[ -logdir DIRNAME ] [ -slave ] [ -nologdir ]
```

Command line options for the ncp_ctrl process are explained in the following table:

Table 22. Explanation of Command Line Options

Option	Explanation
-domain *DOMAIN_NAME*	The name of the domain under which to run the ncp_ctrl process.
-debug *DEBUG*	The level of debugging output (1-4, where 4 represents the most detailed output).
-help	Displays the command line options. Does not start the component even if used in conjunction with other arguments.
-latency *LATENCY*	The maximum time in milliseconds (ms) that the ncp_ctrl process waits to connect to another Network Manager process using the messaging bus. This option is useful for large and busy networks where the default settings can cause processes to assume that there is a problem when in fact the communication delay is a result of network traffic.

Table 22. Explanation of Command Line Options   (continued)

Option	Explanation
-logdir *DIRNAME*	Specifies the directory where log files are to be added and directs log messages for each process started by the ncp_ctrl process to a separate file in the specified directory.
-messagelevel *MESSAGELEVEL*	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
-messagelog *PATHTOLOGFILE*	The path to the message log file.
-nologdir	Turns off log file writing and prints log messages on screen.
-slave	Indicates that this instance of the ncp_ctrl process is to be run in slave mode. The slave ncp_ctrl process must have the same domain name as the master ncp_ctrl process. When running in slave mode, ncp_ctrl accepts requests from the master process to launch services. The slave mode can be used to distribute processes.
-version	Displays the version number of the component. Does not start the component even if used in conjunction with other arguments.

ncp_crypt command-line options

Use the ncp_crypt command, with optional advanced arguments, to start ncp_crypt, the password encryption utility.

The password encryption utility, the ncp_crypt process, is started manually using the following command line; optional arguments are shown enclosed in square brackets.

Note: All password encryption in Network Manager is performed using FIPS 140–2 compliant algorithms.

```
ncp_crypt -password password [ -decrypt ] [ -help ] [ -version ]
```

By default this command encrypts the password provided. However, if you specify the -decrypt option then the password is decrypted.

Command line options for the ncp_crypt process are explained in the following table:

Table 23. Explanation of Command Line Options

Option	Explanation
-password	Specifies the password to encrypt or decrypt. By default the password is encrypted.

Table 23. Explanation of Command Line Options (continued)

Option	Explanation
-decrypt	Overrides the default and instructs ncp_crypt to decrypt the password.
-help	Displays the command line options. Does not start the component even if used in conjunction with other arguments.
-version	Displays the version number of the component. Does not start the component even if used in conjunction with other arguments.

ncp_disco command-line options

Use the ncp_disco command, with optional advanced arguments, to start the Discovery engine.

It is best practice to configure the ncp_ctrl process, the master process controller, to launch and manage the ncp_disco process.

The master process controller, ncp_ctrl, must be running in order for ncp_disco to launch and manage its subprocesses.

The ncp_disco process is started by using the following command line; optional arguments are shown enclosed in square brackets.

```
ncp_disco [ -activeOnBackupDomain ] [ -cachesize SIZE_IN_MB ] [
-cachepercent PERCENTAGE_OF_CACHE_IN_MEMORY ] —domain DOMAIN_NAME [
-discoOnStartup {0 | 1} ] [ -debug DEBUG ] [ -help ] [ -latency LATENCY ]
[-messagelevel MESSAGELEVEL ] [ -messagelog PATHTOLOGFILE ] [ -version ]
```

Command-line options for the ncp_disco process are explained in the following table:

Table 24. Explanation of command-line options

Option	Explanation
-activeOnBackupDomain	Specifies whether to have a discovery active on the backup domain of a failover pair. **Attention:** This option is provided for non-standard Network Manager configurations only and must not be set if you are running a standard Network Manager failover configurations. Standard failover will not work if this flag is set. Do not set this flag if you are running the ncp_virtualdomain process.
-cachesize *SIZE_IN_MB*	Specifies the size of the cache in megabytes (MB).
-cachepercent *PERCENTAGE_OF_CACHE_IN_MEMORY*	Enables you to specify the ratio of the cache that is resident in memory to the cache that is resident on the hard disk. The ratio that you specify depends on the amount of memory that exists on the host machine and the number of processes it is running. The default value is 100% cache.
-domain *DOMAIN_NAME*	The name of the domain under which to run the ncp_disco process.

Table 24. Explanation of command-line options (continued)

Option	Explanation
`-discoOnStartup {0 | 1}`	Specifies whether to have a new discovery start automatically when ncp_disco starts up. The options are: • 0 – discovery does not start automatically when ncp_disco starts up • 1 – discovery starts automatically when ncp_disco starts up By default, a new discovery does not start automatically.
`-debug DEBUG`	The level of debugging output (1-4, where 4 represents the most detailed output).
`-help`	Displays the command-line options. Does not start the component even if used in conjunction with other arguments.
`-latency LATENCY`	The maximum time in milliseconds (ms) that the ncp_ctrl process waits to connect to another Network Manager process using the messaging bus. This option is useful for large and busy networks where the default settings can cause processes to assume that there is a problem when in fact the communication delay is a result of network traffic.
`-messagelevel MESSAGELEVEL`	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
`-messagelog PATHTOLOGFILE`	The path to the log file.
`-version`	Displays the version number of the component. Does not start the component even if used in conjunction with other arguments.

The `-cachesize` and `-cachepercent` options can be used to reduce the memory required when the process responds to OQL queries that result in large numbers of records being returned.

When a value for `-cachesize` is specified, a fixed size of records is cached in core memory with the remaining records being flushed to disk. When a value for `-cachepercent` is specified, that percentage of the data is cached in core memory with the remainder being flushed to disk. These command-line options are not intended to be used for permanent data storage as the cache is cleared when the process exits.

ncp_d_helpserv command-line options

Use the ncp_d_helpserv command, with optional advanced arguments, to start the Helper Server.

It is good practice to configure the Helper Server to be started automatically by CTRL at the appropriate time, by making the appropriate OQL insertion into the services.inTray table of CTRL. Alternatively, you can start the Helper Server manually using the command line.

Optional arguments are shown enclosed in square brackets.

```
ncp_d_helpserv -domain DOMAIN_NAME [ -debug DEBUG ]   [ -help ]
 [ -messagelevel MESSAGELEVEL ] [ -messagelog PATHTOLOGFILE ] [ -version ]
```

Table 25. Explanation of command-line options

Option	Explanation
-domain *DOMAIN_NAME*	The name of the domain under which to run the Helper Server.
-debug *DEBUG*	The level of debugging output (1-4, where 4 represents the most detailed output).
-errorlevel *ERRORLEVEL*	The types of error to be printed: • 1: print only fatal errors • 2: print fatal errors and warnings • 3: print fatal errors, warnings, and informational messages
-help	Displays the command line options. Does not start the component even if used in conjunction with other arguments.
-messagelevel *MESSAGELEVEL*	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
-messagelog *PATHTOLOGFILE*	The path to the message log file.
-version	Displays the version number of the component. Does not start the component even if used in conjunction with other arguments.

Starting helpers

Provided that the Helper Server is launched by CTRL, the individual helpers are automatically started as and when they are required.

The only situation in which you might need to configure an insert for an individual helper into the disco.managedProcesses table would be if you wanted to start that helper on a remote machine (that is, a machine other than the one that is running the Helper Server). In this situation, you would insert the required helper into the disco.managedProcesses table, specifying the appropriate remote host in the m_Host field.

ncp_g_event command line options

Use the **ncp_g_event** command, with optional advanced arguments, to start the Event Gateway.

Usage considerations

It is best practice to configure the **ncp_ctrl** process, the master process controller, to launch and manage the **ncp_g_event** process.

Attention: If you are using Network Manager with failover, you must start the Event Gateway using the **ncp_ctrl** process. The **ncp_ctrl** process checks the status of the Event Gateway component and uses this information to generate the health check events used by the failover process.

For more information about failover, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Syntax

The following example shows the syntax of the **ncp_g_event** command:

```
ncp_g_event –domain DOMAIN_NAME [-debug DEBUG] [-help] [-latency LATENCY]
[ -messagelevel MESSAGELEVEL ] [ -messagelog PATHTOMSGLOGFILE ] [ -logdir
PATHTOLOGFILE] [-version]
```

The following table describes the command-line options of the **ncp_g_event** command.

Table 26. ncp_g_event command-line options

Option	Description
-domain DOMAIN_NAME	The name of the domain under which to run **ncp_g_event**.
-debug DEBUG	The level of debugging output (1-4), where 4 represents the most detailed output.
-help	Prints out the command-line options for **ncp_g_event** then exits.
-latency LATENCY	The maximum time in milliseconds (ms) that **ncp_g_event** waits for a response to a query of another Network Manager IP Edition process. This option is useful for large and busy networks where the default settings can cause processes to assume that there is a problem when in fact the communication delay is a result of network traffic. The default value is 10000. If you specify a lower value on the command line, it is increased to 10000. For large topologies, make sure you set a value of at least a few minutes.

Table 26. ncp_g_event command-line options (continued)

Option	Description
-messagelevel *MESSAGELEVEL*	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
-messagelog *PATHTOMSGLOGFILE*	The path to the message log file.
-server *OBJECTSERVER*	The name of the ObjectServer to connect to. This defaults to NCOMS if no server is specified. **Tip:** The $NCHOME/etc/precision/ ConfigItnm.cfg file provides a simpler, efficient alternative for configuring failover. Use this file instead of the -server command-line option, to specify the ObjectServer name.
-logdir *PATHTOLOGFILE*	The directory to write log files to.
-primaryDomain *PRIM_DOMAIN_NAME*	The name of the primary domain. **Tip:** The $NCHOME/etc/precision/ ConfigItnm.cfg file provides a simpler, efficient alternative for configuring failover. Use this file instead of the -primaryDomain command-line option, to specify the primary domain name.
-version	Prints the version number of **ncp_g_event** then exits.

ncp_install_services command-line options

Use the ncp_install_services command, with optional advanced arguments, to start the ncp_install_services process. This process installs or removes services for additional Windows domains.

The ncp_install_services process is started by using the following command line; optional arguments are shown enclosed in square brackets.

```
ncp_install_services —domain DOMAIN_NAME [ -debug DEBUG ] [ -help ] [ -install ]
[ -messagelevel MESSAGELEVEL ] [-messagelog PATHTOLOGFILE][ -remove ]
[ -username ] [ -password ] [ -version ]
```

Table 27. Explanation of Command Line Options

Option	Explanation
-domain *DOMAIN_NAME*	The name of the domain for which services will be set up or removed.
-debug *DEBUG*	The level of debugging output (1-4, where 4 represents the most detailed output).
-help	Displays the command line options. Does not start the component even if used in conjunction with other arguments.

Table 27. Explanation of Command Line Options   (continued)

Option	Explanation
-install	Installs services for the selected domain. **Note:** You must not specify both -install and -remove at the same time. If you do this, ncp_install_services performs no action. If you specify neither -install nor -remove, then the -install option is assumed.
-messagelevel *MESSAGELEVEL*	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
-messagelog *PATHTOLOGFILE*	The path to the message log file.
-remove	Removes services for the selected domain.
-username	Name of the user that the services are set up to run as. If this option is omitted then services are set up to run as the LocalSystem user (which appears as SYSTEM on the task manager).
-password	Password for the user specified using the -username option. If the -username option is not specified, then the -password option should not be speciofied either, as no password is required to run services as the LocalSystem user. If the -username option is specified but the -password option is not then ncp_install_services prompts for a password. **Note:** This is a more secure approach if you are being overlooked while you are entering the command, because what you type at the prompt will not be echoed to the screen, whereas what you type on the command line will be echoed.
-version	Displays the version number of the component. Does not start the component even if used in conjunction with other arguments.

ncp_mib command-line options

Use the **ncp_mib** command, with optional advanced arguments, to start the MIB update administration utility. You do not need to configure the ncp_ctrl process to start **ncp_mib**. You need to start **ncp_mib** only after you have added new MIBs.

Note: All MIBs must be valid in order to be parsed correctly.

There is only one ncp_mib process for all domains. So, there is no -domain option for **ncp_mib**. There are also no process dependencies for this command.

After you run the **ncp_mib** command, you can verify that a MIB has loaded successfully by querying the NCIM database table ncmib.mib_modules with a command similar to the following example (the example assumes the NCIM database is running on MySQL):

```
mysql> select * from ncmib.mib_modules where moduleName ='RFC1213-MIB';
```

If the MIB loaded, a table is displayed containing a moduleName of RFC1213-MIB.

You can also verify that MIBs are loaded by running the **ncp_mib** command with the -messagelevel info option. A message similar to the following informs you that the MIBs are being processed:

```
09/10/08 12:41:08: Information: I-MIB-001-013: [1096571552t]
Resolving references for module 'RFC1213-MIB'
```

When processing completes, a message states that the MIBs have been committed to the database.

The **ncp_mib** command takes the following command-line options.

```
ncp_mib [ -db ] [ -debug debug level ] [-diff ] [ -dryrun ] [ -emtpydb ]
[ -force ] [ -help ] [ -logdir ] [ -messagelevel message level ]
[-messagelog] [ -override ] [ -showcontents ] [ -version ]
```

Command line options are explained in Table 28.

Table 28. Explanation of Command Line Options

Option	Explanation
-db	Specifies the MIB Database ID, as defined in MibDbLogin.cfg. The default value is MIB.
-debug *debug level*	The level of debugging output (1-4, where 4 represents the most detailed output).
-diff	Compares the list of MIBs in files with those in the SQL DB and show difference.
-dryrun	Shows what would be done by issuing the command but does not alter the SQL database in any way.
-emtpydb	Removes all the MIB data from the database and exits.
-force	Attempts to resolve and insert all parsed MIB objects, regardless of whether all dependencies are met. This option allows the insertion of a partially resolved MIB module, inserting those MIB objects which have their dependencies satisfied while leaving out those MIB objects which do not.
-help	Displays the command line options. Does not start the component even if used in conjunction with other arguments.
-logdir	Specifies the directory into which log files are written.
-messagelevel *message level*	Specifies the message level to use for log files: • Debug • Info • Warn • Error • Fatal The default is Warn.
-messagelog	Specifies the path to the message log.
-override	Empties the database and then attempts to import all the MIBs. If there are errors, such as unresolved MIB modules, the transaction is rolled back and the original state of the database is restored.

Table 28. Explanation of Command Line Options (continued)

Option	Explanation
-showcontents	Displays a list of the MIB modules that are contained in the MIB files and states which ones are resolved.
-version	Displays the version number of the component.

ncp_model command-line options

Use the **ncp_model** command, with optional advanced arguments, to start the topology manager.

It is best practice to configure the **ncp_ctrl** process, the master process controller, to launch and manage the **ncp_model** process. You can also start the **ncp_model** process by using the following command-line syntax; optional arguments are shown enclosed in square brackets.

```
ncp_model —domain DOMAIN_NAME
[ -backup ] [ -debug DEBUG ] [ -help ]
[ -latency LATENCY ] [ -messagelevel MESSAGELEVEL ]
[ -messagelog PATHTOLOGFILE ] [ -version ]
```

Command-line options for the **ncp_model** process are explained in the following table.

Table 29. ncp_model command-line options

Option	Explanation
-domain DOMAIN_NAME	The name of the domain under which to run the **ncp_model** process.
-backup	Set this option when running in failover mode without NCIM replication. When running with the -backup command-line option, the **ncp_model** process will not attempt to update the Network Connectivity and Inventory Model (NCIM) database with topology data. **Tip:** The $NCHOME/etc/precision/ConfigItnm.cfg file provides a simpler, efficient alternative for configuring failover. Use this file instead of the -backup command-line option, to indicate that the **ncp_model** process should not update the NCIM database.
-primaryDomain	Set this option when running in failover mode with NCIM replication. Specifies the name of the primary domain in the failover pair. This name must match the -domain value on the primary server. **Tip:** The $NCHOME/etc/precision/ConfigItnm.cfg file provides a simpler, efficient alternative for configuring failover. Use this file instead of the -primaryDomain command-line option, to indicate that the **ncp_model** process should not update the NCIM database.
-debug DEBUG	The level of debugging output (1-4, where 4 represents the most detailed output).
-help	Displays the command line options. Does not start the component even if used in conjunction with other arguments.

Table 29. ncp_model command-line options   (continued)

Option	Explanation
-latency *LATENCY*	The maximum time in milliseconds (ms) that the **ncp_model** process waits to connect to another Precision Server process by means of the messaging bus. This option is useful for large and busy networks where the default settings can cause processes to assume that there is a problem when in fact the communication delay is a result of network traffic.
-messagelevel *MESSAGELEVEL*	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
-messagelog *PATHTOLOGFILE*	The path to the message log file.
-version	Displays the version number of the component. Does not start the component even if used in conjunction with other arguments.

ncp_oql command-line options

Use the ncp_oql command, with optional advanced arguments, to start ncp_oql, the OQL Service Provider. The OQL Service Provider is the command-line interface that enables administrators to query and update data in Network Manager management databases.

To launch the OQL Service Provider, use the following command line; optional arguments are shown enclosed in square brackets:

```
ncp_oql —domain DOMAIN_NAME -service SERVICE_NAME [ -username USERNAME] [ -password
 PASSWORD] [ -poller ] [ -schema PATH_TO_SCHEMA_FILE ] [ -debug DEBUG ]
[ -messagelevel MESSAGELEVEL ] [ -help ] [ -history HISTORY_SIZE ] [ -latency
LATENCY ] [ -oqldump ] [ -query QUERY ] [ -updates ] [ -snoop ] [ -tabular ]
[ -options ] [ -dbId DATABASE_ID ] [ -version ]
```

Table 30. Explanation of Command Line Options

Option	Explanation
-dbId *DATABASE_ID*	This option is only valid when used in conjunction with the ncim service. Choose the database from DbLogins to connect to. The default value is NCIM.
-debug *DEBUG*	The level of debugging output (1-4, where 4 represents the most detailed output).
-domain *DOMAIN_NAME*	The name of the relevant domain. Ensure that the process whose databases you wish to query is running.
-help	All Network Manager components have a special -help option that displays the command line options. The component is not started even if —help is used in conjunction with other arguments.
-history *HISTORY_SIZE*	The size of the command line history.

Table 30. Explanation of Command Line Options (continued)

Option	Explanation
`-latency LATENCY`	The maximum time in milliseconds (ms) that the service provider waits to connect to another Network Manager process using the messaging bus. This option is useful for large and busy networks where the default settings can cause processes to assume that there is a problem when in fact the communication delay is a result of network traffic. The default value is 3000 (equivalent to 3 seconds). You might want to increase this value as the default value might not be long enough to get a response from a large or busy OQL database.
`-messagelevel MESSAGELEVEL`	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
`-oqldump`	Using this argument results in the databases from the application being converted into OQL create and insert statements. This can be a useful means of recording the internal state of a component for debugging or analysis at a later date.
`-password PASSWORD`	The password to access the OQL Service Provider. This argument is only required if the OQL Service Provider is in authentication mode. This feature is provided for use in conjunction with the `-query` option, to enable OQL queries to be placed in scripts. For security reasons you must use this option carefully, as other users may be able to see your password. You can also enter your password when prompted rather than at the command line.
`-query QUERY`	A query to pass to the OQL Service Provider, designed to allow OQL statements in scripts (used in conjunction with `-password`).
`-options`	Displays the list of options allowed as query services.
`-poller`	Specifies a poller instance to connect to.
`-schema PATH_TO_SCHEMA_FILE`	This option is only valid when used in conjunction with the ncp_config service. Specifies a schema file to use.
`-server SERVER_NAME`	This option is valid only with the ObjectServer service. It defaults to the current ObjectServer given in the ConfigItnm file.
`-service SERVICE_NAME`	The service you wish to interrogate. Run **ncp_oql** with the `-options` command line option to list all available services.
`-snoop`	Shows queries made on the service.
`-tabular`	Toggles tabular results display format.

Table 30. Explanation of Command Line Options (continued)

Option	Explanation
`-updates`	Shows updates made on the service.
`-username` *USERNAME*	The username to use to log into the service provider. This argument is only required if the OQL Service Provider is in authentication mode.
`-version`	All Network Manager components have a special `-version` option that displays the version number of the component. The component is not started even if –version is used in conjunction with other arguments.

nco_p_ncpmonitor command-line options

On UNIX operating systems, use the **nco_p_ncpmonitor** command, with optional advanced arguments, to start the Probe for Tivoli Netcool/OMNIbus, and to configure how the probe works.

Usage considerations

Use this command only to troubleshoot IBM Tivoli Network Manager IP Edition.

The **nco_p_ncpmonitor** command starts the Probe for Tivoli Netcool/OMNIbus independently of the domain process controller CTRL. If you are using Network Manager IP Edition with failover, you must start the Probe for Tivoli Netcool/OMNIbus using CTRL. The CTRL process checks the status of the Probe for Tivoli Netcool/OMNIbus and uses this information to generate the Health Check events used by the failover process.

There are no dependencies for starting the Probe for Tivoli Netcool/OMNIbus.

Syntax

The following example shows the syntax of the **nco_p_ncpmonitor** command.

```
nco_p_ncpmonitor -domain DOMAIN_NAME [ -buffer ] [ -buffersize ] [ -capturefile ]
 [ -debug DEBUG ] [ –help ] [ -latency LATENCY ] [ -manager ]
[ -messagelevel ] [ -messagelog ] [ -name ] [ -nobuffer ] [ -noraw ] [ -propsfile ]
[ -raw ] [ -rulesfile ] [ -server ] [ -version ]
```

The following table describes the command-line options of the **nco_p_ncpmonitor** command.

Table 31. nco_p_ncpmonitor command-line options

Option	Explanation
`-autosaf`	Enable automatic store and forward mode.
`-buffer`	Allows you to turn on alert buffering.
`-buffersize`	The size of the alert buffer to use.
`-capturefile`	Raw capture file to write to.
`-debug` *DEBUG*	The level of debugging output (1-4, where 4 represents the most detailed output).
`-domain` *DOMAIN_NAME*	The name of the domain under which Network Manager IP Edition processes are running.

Table 31. nco_p_ncpmonitor command-line options (continued)

Option	Explanation
—help	Prints out a synopsis of all command line options for the component. If specified, the component is *not* started.
-latency *LATENCY*	The maximum time in milliseconds (ms) that the component waits to connect to another Network Manager IP Edition process via the messaging bus. This option is useful for large and busy networks where the default settings can cause the process to assume that there is a problem when in fact the communication delay is a result of network traffic.
-manager	Manager name.
-messagelevel *MESSAGELEVEL*	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
-messagelog *PATHTOLOGFILE*	The path to the message log file.
-name	Name of probe.
-noautosaf	Disable automatic store and forward mode.
-nobuffer	Allows you to turn off alert buffering.
-noraw	Allows you to turn off raw capture mode.
-nosaf	Disable store and forward mode.
-propsfile	Properties file to use.
-raw	Allows you to turn on raw capture mode.
-rulesfile	Rules file to use.
-saf	Enable store and forward mode.
-server	The name of the ObjectServer to connect to. **Tip:** The $NCHOME/etc/precision/ConfigItnm.cfg file provides a simpler, efficient alternative for configuring failover. Use this file instead of the -server command-line option, to specify the ObjectServer name.
-version	Prints the version number of the component. If specified, the component is *not* started even if -version is used in conjunction with other arguments.

ncp_poller command-line options

Use the **ncp_poller** command, with optional advanced arguments, to start the network polling engine.

It is best practice to configure the **ncp_ctrl** process, the master process controller, to launch and manage the **ncp_poller** process.

Attention: If you are using Network Manager with failover, you must start the **ncp_poller** process by using the **ncp_ctrl** process. The **ncp_ctrl** process checks the status of the **ncp_poller** process and uses this information to generate the health check events used by the failover process.

Prerequisites

Before you manually start the **ncp_poller** process, the following Network Manager IP Edition processes must be running:

- MODEL must be running in order to pass the network topology to the polling subsystem.
- The Probe for Tivoli Netcool/OMNIbus must be running to transfer events to the ObjectServer.

Command

To manually start the **ncp_poller** process, run the **ncp_poller** command.

The command-line syntax for **ncp_poller** is:

```
ncp_poller [-admin] -domain DOMAIN_NAME [-debug DEBUG] [ -deregister ]
 [-errorlevel ERRORLEVEL] [ -force ] [ -help ] [ -latency LATENCY]
[ -messagelevel MESSAGELEVEL ] [ -messagelog PATHTOLOGFILE ]
[ -name ] [ -primaryDomain PRIMARY_DOMAIN_NAME ] [ -readsnmpconfig ]
[ -register ] [-version] [-logdir]
```

The following table describes the command-line options for **ncp_poller**.

Table 32. **ncp_poller** *command-line options*

Option	Explanation
-admin	If you are using one poller, this option is mandatory. If you are using multiple pollers, one of the pollers must be started with this option. The poller that is started with the -admin option updates the views and purges the poll data. If the poller is running as a backup, it updates the device access credentials in the snmpKeyChain table. For performance reasons, the poller with the smallest polling load is usually started with this option.
-debug DEBUG	The level of debugging output (1-4, where 4 represents the most detailed output).
-deregister	Deregisters a poller. Any polls assigned to a poller that is not registered will not run.
-domain DOMAIN_NAME	The name of the domain under which to run the **ncp_poller** process.

Table 32. `ncp_poller` command-line options (continued)

Option	Explanation
-errorlevel *ERRORLEVEL*	The types of error to be printed: • 1: Print only fatal errors • 2: Print fatal errors and warnings • 3: Print fatal errors, warnings, and informational messages
-force	Forces deregistration of the poller. Deletes all polling policies assigned to the named poller.
-help	Prints out a synopsis of all command-line options for **ncp_poller** then exits.
-latency *LATENCY*	The maximum time in milliseconds (ms) that the **ncp_poller** process waits for a response to a query of another Network Manager IP Edition process. This option is useful for large and busy networks where the default settings can cause the process to assume that there is a problem when in fact the communication delay is a result of network traffic. For large topologies, make sure you set a value of at least a few minutes.
-messagelevel *MESSAGELEVEL*	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
-messagelog *PATHTOLOGFILE*	The path to the message log file.
-name	Run as a named poller. Only polls assigned to this poller will be run.
-primaryDomain *PRIMARY_DOMAIN_NAME*	Configures the **ncp_poller** process to operate in backup mode. **Tip:** The $NCHOME/etc/precision/ConfigItnm.cfg file provides a simpler, efficient alternative for configuring failover. Use this file instead of the -primaryDomain command-line option, to configure the poller to operate in backup mode.
-readsnmpconfig	Instructs the poller to read the configuration from the SnmpStackSecurityInfo.cfg file and write it to the configuration database.
-register	Registers the poller. Pollers must be registered before polls can be assigned to them.
-version	Prints the version number of **ncp_poller** then exits.

For more information on failover, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

ncp_store command-line options

Use the ncp_store command, with optional advanced arguments, to start the ncp_store process.

It is best practice to configure the ncp_ctrl process, the master process controller, to launch and manage the ncp_store process. You can also start the ncp_store process using the following command line; optional arguments are shown enclosed in square brackets.

```
ncp_store –domain DOMAIN_NAME [ -cachesize SIZE_IN_MB ] [ -cachepercent
PERCENTAGE_OF_CACHE_IN_MEMORY ] [ -debug DEBUG ]
[ -help ] [ -version ] [ -latency LATENCY ] [ -logdir PATHTOLOGFILE]
[ -messagelevel MESSAGELEVEL ] [ -messagelog PATHTOMSGLOGFILE ]
```

Command line options for the ncp_store process are explained in the following table:

Table 33. Explanation of Command Line Options

Option	Explanation
-domain *DOMAIN_NAME*	The name of the domain under which to run the ncp_store process.
-cachesize *SIZE_IN_MB*	Specifies the size of the cache in megabytes (MB).
-cachepercent *PERCENTAGE_OF_CACHE_IN_MEMORY*	Specifies the ratio of the cache that is resident in memory to the cache that is resident on the hard disk. The ratio that you specify depends on the amount of memory that exists on the host machine and the number of processes it is running. The default value is 0% cache. This ensures that ncp_store has a smaller memory footprint, as all its databases are stored on disk and not in memory. For large topologies setting -cachepercent 100 can make ncp_store start up faster. This setting has a larger memory footprint.
-debug *DEBUG*	The level of debugging output (1-4, where 4 represents the most detailed output).
-help	Displays the command line options. Does not start the component even if used in conjunction with other arguments.
-latency *LATENCY*	The maximum time in milliseconds (ms) that the ncp_store process waits to connect to another Network Manager process by means of the messaging bus. This option is useful for large and busy networks where the default settings can cause processes to assume that there is a problem when in fact the communication delay is a result of network traffic.
-logdir *PATHTOLOGFILE*	The directory to write log files to.

Table 33. Explanation of Command Line Options (continued)

Option	Explanation
-messagelevel *MESSAGELEVEL*	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
-messagelog *PATHTOMSGLOGFILE*	The path to the message log file.
-version	Displays the version number of the component. Does not start the component even if used in conjunction with other arguments.

ncp_trapmux command-line options

Use the **ncp_trapmux** command, with optional advanced arguments, to start the SNMP trap multiplexer.

To start the **ncp_trapmux** process, use the following command line, where optional arguments are shown enclosed in square brackets.

```
ncp_trapmux -domain DOMAIN_NAME [ -debug DEBUG ] [ -help ] [ -latency
LATENCY ] [ -messagelevel MESSAGELEVEL ] [ -messagelog PATHTOLOGFILE ] [
-version ]
```

Command line options for the ncp_trapmux process are explained in the following table:

Table 34. Explanation of Command Line Options

Option	Explanation
-domain *DOMAIN_NAME*	The name of the domain under which to run the trap multiplexer.
-debug *DEBUG*	The level of debugging output (1-4, where 4 represents the most detailed output).
-help	Displays the command line options. Does not start the component even if used in conjunction with other arguments.
-latency *LATENCY*	The maximum time in milliseconds (ms) that the ncp_trapmux process waits to connect to another Network Manager process by means of the messaging bus. This option is useful for large and busy networks where the default settings can cause processes to assume that there is a problem when in fact the communication delay is a result of network traffic.
-messagelevel *MESSAGELEVEL*	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal

Table 34. Explanation of Command Line Options   (continued)

Option	Explanation
-messagelog *PATH_TO_LOGFILE*	The path to the message log file.
-version	Displays the version number of the component. Does not start the component even if used in conjunction with other arguments.

ncp_virtualdomain command-line options

Use the `ncp_virtualdomain` command, with optional advanced arguments, to start the Virtual Domain component.

Virtual Domain is used when running Network Manager with failover.

It is best practice to configure the `ncp_ctrl` process, the master process controller, to launch and manage Virtual Domain. The command-line syntax for Virtual Domain is:

```
ncp_virtualdomain -domain DOMAIN_NAME -virtualDomain VIRTUAL_DOMAIN_NAME
[-backupDomain BACKUP_DOMAIN_NAME] [-debug DEBUG] [-help] [-latency
LATENCY] [ -messagelevel MESSAGELEVEL ] [ -messagelog PATH_TO_LOGFILE ] [
-primaryDomain PRIMARY_DOMAIN_NAME] [-version]
```

The following table describes the command-line options for `ncp_virtualdomain`.

Table 35. `ncp_virtualdomain` command-line options

Option	Description
-backupDomain *BACKUP_DOMAIN_NAME*	The name of the backup domain. Only add this command-line option on the primary Network Manager server. The name must match the -domain value on the backup Network Manager server. **Tip:** The $NCHOME/etc/precision/ConfigItnm.cfg file provides a simpler, efficient alternative for configuring failover. Use this file instead of the -backupDomain command-line option, to specify the backup domain name.
-debug *DEBUG*	The level of debugging output (1-4, where 4 represents the most detailed output).
-domain *DOMAIN_NAME*	The name of the domain under which the Network Manager component is running. This name must be different for the primary and backup Network Manager servers.
-help	Prints out a synopsis of all command-line options for the component. If specified, the component is not started even if -help is used in conjunction with other arguments.
-latency *LATENCY*	The maximum time in milliseconds (ms) that the Virtual Domain component waits to connect to another Network Manager process using the messaging bus.

Table 35. `ncp_virtualdomain` command-line options (continued)

Option	Description
-messagelevel *MESSAGELEVEL*	The level of messages to be logged (the default is warn): • debug • info • warn • error • fatal
-messagelog *PATH_TO_LOGFILE*	The path to the message log file.
-primaryDomain *PRIMARY_DOMAIN_NAME*	The name of the primary domain. Only add this command-line option on the backup Network Manager server. The name must match the -domain value on the primary Network Manager server. **Tip:** The $NCHOME/etc/precision/ConfigItnm.cfg file provides a simpler, efficient alternative for configuring failover. Use this file instead of the -primaryDomain command-line option, to specify the primary domain name.
-version	Prints the version number of the component. If specified, the component is not started even if -version is used in conjunction with other arguments.
-virtualDomain *VIRTUAL_DOMAIN_NAME*	The name of the virtual domain that any external application is to connect to. This name must be the same for the primary and backup Network Manager servers. **Tip:** The $NCHOME/etc/precision/ConfigItnm.cfg file provides a simpler, efficient alternative for configuring failover. Use this file instead of the -virtualDomain command-line option, to specify the virtual domain name.

ncp_webtool command-line options

Use the **ncp_webtool** command to run the Web tools on the backend server.

The ncp_webtool process transfers the running of the Web tools to the backend server in environments where Topoviz is running on a different server to the Network Manager backend processes and there is a fire wall between the two. This transfer makes the Web tools available across such distributed environments.

You do not need to interact directly with ncp_webtool process, as it is a sever-time application that runs without user input.

It is best practice to configure the ncp_ctrl process, the master process controller, to launch and manage the ncp_webtool process. However, you can start the ncp_webtool process manually by entering the command, **ncp_webtool**, on the command line.

The **ncp_webtool** command takes these options.

```
ncp_webtool -domain [ -debug debug level ] [ -help ] [ -latency ] [ -messagelevel
message level ] [ -messagelog ] [ -version ]
```

Command line options are explained in Table 36.

Table 36. Explanation of Command Line Options

Option	Explanation
-debug *debug level*	Specifies the level of debugging output (1-4, where 4 represents the most detailed output).
-domain	Specifies the domain.
-help	Displays the command line options.
-latency	Specifies the network timeout value to use (in milliseconds).
-messagelevel *message level*	Specifies the message level to use for log files: • Debug • Info • Warn • Error • Fatal The default is Warn.
-messagelog	Displays the path to the message log file.
-version	Displays the version number of the component.

Command reference for Tivoli Integrated Portal

Use the Tivoli Integrated Portal command line interface *tipcli* commands for writing scripts for passing information between applications.

The `tipcli` commands are entered in the *tip_home_dir*/profiles/TIPProfile/bin directory, for example, `C:\IBM\tivoli\tip\profiles\TIPProfile\bin\tipcli.bat` on Windows or `/opt/IBM/tivoli/tip/profiles/TIPProfile/bin/tipcli.sh` on Linux or UNIX.

The `tipcli` component provides help for its various commands:

Help [--command *command_name***]**
> Access help for all commands or optionally you can use the `command` argument to return detailed help for a specific command.

The following returns help for the `AddUpdatePreferenceProfile` command:

```
tipcli.bat Help --command AddUpdatePreferenceProfile
Help
----
AddUpdatePreferenceProfile --username <TIPusername> --password <passwordForUser>
 --profileName <profileName> [--newProfileName <newProfileName>] [--themeDir <th
emeDir>] [--showNavTree <true|false>] [--componentDir <default|ltr|rtl>] [--text
Dir <default|contextual|ltr|rtl>] [--views <viewList>] [--roles <roleList>] [--d
efaultView <defaultView>]
where
  <TIPusername> is the username on TIP that has iscadmins role.
  <passwordForUser> is the password for the user.
  <profileName> is profile name which will be created or updated.
  <newProfileName> is the new name for the existing preference profile.
  <themeDir> is the directory name of the installed theme. Example: TIPLight
  <showNavTree> specify if show navigation tree by default after login the conso
le.
```

```
  <componentDir> specify component direction for the console.
  <textDir> specify text direction for the console.
  <viewList> is views assignment for the preference profile.
  <roleList> is roles assignment for the preference profile.
  <defaultView> specify which view is displayed by default after login the conso
le.

CTGWA4017I The command completed successfully.
```

Working with roles

`tipcli` commands for working with roles.

ListRoles
> List all roles.

AddRole --username *tip_username* **--password** *tip_user_password* **--roleName**
role_name
> Add the specified role. Console users are granted access to resources based on the role to which they have been assigned. All roles that are created have a resource type of `Custom`.
>
> **Note:** Arguments to the `role_name` parameter should not include spaces.

UpdateRole --username *tip_username* **--password** *tip_user_password* **--roleName**
role_name **--newRoleName** *new_role_name*
> Change the name of a specified role to the supplied new role name.
>
> **Note:** Arguments to the `role_name` and `newRoleName` parameters should not include spaces.

DelRole --username *tip_username* **--password** *tip_user_password* **--roleName**
role_name
> Delete the specified role.
>
> **Note:** Arguments to the `role_name` parameter should not include spaces.

ListRolesFromGroup --username *tip_username* **--password** *tip_user_password*
--groupID *group_ID*
> List all roles associated with a specified user group.

MapRolesToGroup --username *tip_username* **--password** *tip_user_password*
--groupID *group_ID* **--roleList** *role_name1, role__name2*
> Associate a comma separated list of roles with a particular user group.

RemoveRolesFromGroup --username *tip_username* **--password** *tip_user_password*
--groupID *group_ID* **--roleList** *role_name1, role__name2*
> Disassociate a comma separated list of roles from a particular user group.

ListRolesForPage --pageUniqueName *page_unique_name*
> List all roles associated with a specified page.

MapRolesToPage --username *tip_username* **--password** *tip_user_password*
--pageUniqueName *page_unique_name* **--roleList** *role_name1, role__name2*
--accessLevelList *level1, level2*
> Associate a comma separated list of roles with a particular page and set the access level to the page for each role.

RemoveRolesFromPage --username *tip_username* **--password** *tip_user_password*
--pageUniqueName *page_unique_name* **--roleList** *role_name1, role__name2*
> Disassociate a comma separated list of roles from a particular page.

ListRolesForPortletEntity --portletEntityUniqueName
portlet_entity_unique_name
> List all roles associated with a specified portlet.

MapRolesToPortletEntity --username *tip_username* **--password**
tip_user_password **--portletEntityUniqueName** *portlet_entity_unique_name*
--roleList *role_name1,* *role__name2* **--accessLevelList** *level1,* *level2*
> Associate a comma separated list of roles with a particular portlet and set
> the access level to the portlet for each role.

RemoveRolesFromPortletEntity --username *tip_username* **--password**
tip_user_password **--portletEntityUniqueName** *portlet_entity_unique_name*
--roleList *role_name1,* *role__name2*
> Disassociate a comma separated list of roles from a particular portlet.

ListRolesFromUser --username *tip_username* **--password** *tip_user_password*
--userID *user_ID*
> List all roles associated with a specified user ID.

MapRolesToUser --username *tip_username* **--password** *tip_user_password*
--userID *user_ID* **--roleList** *role_name1,* *role__name2*
> Associate a comma separated list of roles with a particular user ID.

RemoveRolesFromUser --username *tip_username* **--password** *tip_user_password*
--userID *user_ID* **--roleList** *role_name1,* *role__name2*
> Disassociate a comma separated list of roles from a particular user ID.

ListRolesForView --viewUniqueName *view_name*
> List all roles associated with a specified view.

MapRolesToView --username *tip_username* **--password** *tip_user_password*
--viewUniqueName *view_name* **--roleList** *role_name1,* *role__name2*
--accessLevelList *level1,* *level2*
> Associate a comma separated list of roles with a particular view and set
> the access level for the view for each role.

RemoveRolesFromView --username *tip_username* **--password** *tip_user_password*
--viewUniqueName *view_name* **--roleList** *role_name1,* *role__name2*
> Disassociate a comma separated list of roles from a particular view.

Working with views

tipcli commands for working with views.

The tipcli commands are entered in the *tip_home_dir*/profiles/TIPProfile/bin
directory, for example, C:\IBM\tivoli\tip\profiles\TIPProfile\bin\tipcli.bat
on Windows or /opt/IBM/tivoli/tip/profiles/TIPProfile/bin/tipcli.sh on
Linux or UNIX.

ListViews
> List all views.

AddViewMembers --username *tip_username* **--password** *tip_user_password* **--view**
view_unique_name **[--members** *members1,* *member2***] [--launchMembers**
launch_member1, *launch_member2***]**
> Add members or launch members for a specified view.

ListViewsForRole --roleName *role_name*
> List the views associated with a specified role.

MapViewsToRole --username *tip_username* **--password** *tip_user_password*
--roleName *role_name* **--viewList** *view_unique_name1,* *view_unique_name2*

--accessLevelList *level1,* *level2*
> Associate a comma separated list of views with a particular role and set the access level for the role for each view.

RemoveViewsFromRole --username *tip_username* **--password** *tip_user_password*
--roleName *role_name* **--viewList** *view_unique_name1,* *view_unique_name2*
> Disassociate a comma separated list of views from a particular role.

Working with users

tipcli commands for working with users.

ListUsersFromRole --roleName *role_name*
> List the users associated with a specified role.

MapUsersToRole --username *tip_username* **--password** *tip_user_password*
--roleName *role_name* **--usersList** *user_ID1:user_ID2*
> Associate a colon (:) separated list of user IDs with a particular role.
>
> **Note:** Arguments to the usersList parameter should not include a colon (:).

RemoveUsersFromRole --username *tip_username* **--password** *tip_user_password*
--roleName *role_name* **--usersList** *user_ID1:user_ID2*
> Disassociate a colon (:) separated list of user IDs from a particular role.

Working with preference profiles

tipcli commands for working with preference profiles.

DeletePreferenceProfile --username *tip_username* **--password**
tip_user_password **--profileName** *profile_name*
> Delete the specified preference profile.

ListPreferenceProfiles [--name *profile_name*]
> Return a list of console preference profiles. Optionally, you can specify a comma separated lists of preference profiles, to return their unique names.

ShowPreferenceProfile --uniqueName *profile_unique_name*
> List all the attributes for a specified profile preference.

AddUpdatePreferenceProfile --username *tip_username* **--password**
tip_user_password **--profileName** *profile_name* [**--newProfileName**
new_profile_name] [**--themeDir** *theme_dir*] [**--showNavTree** true|false]
[**--componentDir** default|ltr|rtl] [**--textDir** default|contextual|ltr|rtl]
[**--views** *view_unique_name1,* *view_unique_name2*] **--roles** *role_name1,*
role_name2] [**--defaultView** *view_unique_name*]
> Use the AddUpdatePreferenceProfile command to create a new profile preference or update an existing profile.

Table 37. AddUpdatePreferenceProfile command arguments

Parameter and arguments	Description
--username *tip_username*	Mandatory parameter. A user with the iscadmins role.
--password *tip_user_password*	Mandatory parameter. The password for the user with the iscadmins role.
--profileName *profile_name*	Mandatory parameter. The name of the profile that is to be created or modified.
[--newProfileName *new_profile_name*]	Optional parameter. The new name for the specified profile.

Table 37. AddUpdatePreferenceProfile command arguments (continued)

Parameter and arguments	Description
[--themeDir *theme_dir*]	Optional parameter. Used to specify the directory for the theme that you want to apply.
[--showNavTree true|false]	Optional parameter. Used to specify whether or not you want the navigation pane to be displayed for preference profile.
[--componentDir default|ltr|rtl]	Optional parameter. Used to specify component display direction, that is, whether you want items to display left-to-right, right-to-left, or to use the default browser settings.
[--textDir default|ltr|rtl]	Optional parameter. Used to specify text direction, that is, whether you want text to display left-to-right, right-to-left, or to use the default browser settings.
[--views *view_unique_name1, view_unique_name2*]	Optional parameter. Used to specify the views that you want to assign to the preference profile. Comma separated list.
--roles *role_name1, role_name2*]	Optional parameter. Used to specify the roles that you want to assign to the preference profile. Comma separated list.
[--defaultView *view_unique_name*]	Optional parameter. Used to specify the view that you want displayed when a user logs into the portal.

Working with portlets

`tipcli` commands for working with portlets.

The `tipcli` commands are entered in the *tip_home_dir*/profiles/TIPProfile/bin directory, for example, `C:\IBM\tivoli\tip\profiles\TIPProfile\bin\tipcli.bat` on Windows or `/opt/IBM/tivoli/tip/profiles/TIPProfile/bin/tipcli.sh` on Linux or UNIX.

ListPortletEntitiesForRole --roleName *role_name*]
>   List the portlets entities associated with a specified role.

MapPortletEntitiesToRole --username *tip_username* **--password** *tip_user_password* **--roleName** *role_name* **--portletEntityList** *portletEntity_unique_name1, portletEntity_unique_name2* **--accessLevelList** *level1, level2*
>   Associate a comma separated list of portlets with a particular role and set the access level for the role for each portlet.

RemovePortletEntitiesFromRole --username *tip_username* **--password** *tip_user_password* **--roleName** *role_name* **--portletEntityList** *portletEntity_unique_name1, portletEntity_unique_name2*
>   Disassociate a comma separated list of portlets with from particular role.

Working with pages

tipcli commands for working with pages.

ListPages [--viewList *view_unique_name1,* *view_unique_name2***]**
[--customizePages true|false]
>   List all pages. You can optionally filter the list by using the viewlist
>   parameter and providing a comma separated list of views. You can also
>   use the customizePages (set totrue) to return a list of custom pages only.

ListPagesForRole --roleName *role_name*
>   List the pages associated with a specified role.

MapPagesToRole --username *tip_username* **--password** *tip_user_password*
--roleName *role_name* **--pageList** *page_unique_name1,* *page_unique_name2*
--accessLevelList *level1,* *level2*
>   Associate a comma separated list of pages with a particular role and set
>   the access level for the role for each page.

RemovePagesFromRole --username *tip_username* **--password** *tip_user_password*
--roleName *role_name* **--pageList** *page_unique_name1,* *page_unique_name2*
>   Disassociate a comma separated list of pages from a particular role.

Working with user groups

tipcli commands for working with user groups.

The tipcli commands are entered in the *tip_home_dir*/profiles/TIPProfile/bin
directory, for example, C:\IBM\tivoli\tip\profiles\TIPProfile\bin\tipcli.bat
on Windows or /opt/IBM/tivoli/tip/profiles/TIPProfile/bin/tipcli.sh on
Linux or UNIX.

ListGroupsFromRole --roleName *role_name*
>   List the user groups associated with a specified role.

MapGroupsToRole --username *tip_username* **--password** *tip_user_password*
--roleName *role_name* **--groupsList** *group_name1:* *group_name2*
>   Associate a colon (:) separated list of groups with a particular role.

>   **Note:** Arguments to the groupsList parameter should not include a colon
>   (:).

RemoveGroupsFromRole --username *tip_username* **--password** *tip_user_password*
--roleName *role_name* **--groupsList** *group_name1:* *group_name2*
>   Disassociate a colon (:) separated list of groups from a particular role.

Charting tipcli commands

tipcli commands for working with charting.

ListCharts --username *tip_username* **--password** *tip_user_password*
>   Use ListCharts to review the charts that are configured in the
>   environment.

ChartConnection --action *action* **[--name** *name***] [--protocol** *protocol*
--hostname *hostname* **--port** *port* **-- serviceName** *serviceName* **--username**
username **--password** *password***--renderFormat** *render_format*
--Datasource_Username *datasource_username* **--credentialType** *credential_type***]**
--username *tip_username* **--password** *tip_user_password*
>   ChartConnection is used to configure a connection to any IBM Tivoli
>   Charting Web Service. The ITM Web Service is just one example.

ChartExport --dir *output_directory* **--type all|customcharts|page [--pageID** *page_ID* **| --pageName** *page_name*] **--username** *tip_username* **--password** *tip_user_password*

ChartExport is used to export chart data.

Table 38. ChartExport command arguments

Parameter and arguments	Description
--dir *output_directory*	Mandatory parameter. The directory where the exported data is saved. If the directory does not exist, it is created.
--type all|customcharts|page	Mandatory parameter. If you set the --type to all, then all charts are exported. If you set it to customcharts, then only customized charts are exported. If you set it to page, then you can use either the --pageID or the --pageName parameter to specify the page for which you want to export chart data.
[--pageID *page_ID*	--pageName *page_name*]	Optional parameter. If you set the --type parameter to page, then you can use either the --pageID or the --pageName parameter to specify the page for which you want to export chart data.
--username *tip_username*	Mandatory parameter. The user name for a user with either the chartAdministrator or chartCreator role.
--password *tip_user_password*	Mandatory parameter. The password for the specified user name.

ChartImport --dir *source_directory* **--username** *tip_username* **--password** *tip_user_password*

ChartImport is used to import chart data from a specified directory.

Table 39. ChartImport command arguments

Parameter and arguments	Description
--dir *source_directory*	Mandatory parameter. The directory where the data to be imported is located. BIRT Designer file format is .rptdesign.
--username *tip_username*	Mandatory parameter. The user name for a user with either the chartAdministrator or chartCreator role.
--password *tip_user_password*	Mandatory parameter. The password for the specified user name.

ChartProperties [--name *property_name* **--value** *property_value*] **--username** *tip_username* **--password** *tip_user_password*

ChartProperties is used to view or modify properties for charting. If you only provide username and password details and no other arguments, then the current properties are listed. It is useful to run this command first so that you can review the current property names and values before you decide to make updates.

Table 40. ChartProperties command arguments

Parameter and arguments	Description
`--name` *property_name* `--value` *property_value*	Optional parameter. The name of the property that you want to update and the value that you want to set. For example, to set the timeout value to 10,000,000 milliseconds, enter `--name AXIS_TIMEOUT --value 10000000`.
`--username` *tip_username*	Mandatory parameter. The user name for a user with the `chartAdministrator` role.
`--password` *tip_user_password*	Mandatory parameter. The password for the specified user name.

ListRestoreTimestamp

Use the `ListRestoreTimestamp` command to return a list of charting store backups by timestamp.

RestoreChartStore --BackupTimestamp *backup_timestamp* **--username** *tip_username* **--password** *tip_user_password*

Use the `RestoreChartStore` command to restore a chart store by timestamp.

Table 41. RestoreChartStore command arguments

Parameter and arguments	Description
`RestoreChartStore --BackupTimestamp`	Mandatory parameter. The timestamp of the charting store backup.
`--username` *tip_username*	Mandatory parameter. The user name for a user with the `chartAdministrator` role.
`--password` *tip_user_password*	Mandatory parameter. The password for the specified user name.

Export `tipcli` commands

`tipcli` commands for exporting Tivoli Integrated Portal data.

Note: If you specify additional parameters for the `tipcli.bat|.sh` Export and make a typing error, that is, if you type a parameter incorrectly, or use the incorrect case, then the commands runs as if no parameters were specified and no warning message is displayed.

ListExportPlugins

Use the `ListExportPlugins` command to list all plugins that can be exported.

Export [--includePlugins|--excludePlugins *plugin1*,*plugin2*] **[--settingFile** *setting_file*] **--username** *tip_username* **--password** *tip_user_password*

Use the `Export` command to export customization data for an instance of Tivoli Integrated Portal. If you provide no parameters to the `Export` command, all custom data is exported by default.

Table 42. Export command arguments

Parameter and arguments	Description
[`--includePlugins`|`--excludePlugins` *plugin1*,*plugin2*]	Optional parameter. You can choose to include or exclude a list of plugins when you run the `Export` command.

Table 42. Export command arguments (continued)

Parameter and arguments	Description
`[--settingFile setting_file]`	Optional parameter. You can specify your export requirements in properties file instead of specifying your requirements using separate parameters at the command line. Provide a path to the settings file as the argument to the `settingFile` parameter. On systems running Windows you must use double backslashes characters (\\) when specifying the path to your settings file, for example, `C:\\tmp\\export.properties`. Command line parameters take precedence over entries in the settings file.
`--username tip_username`	Mandatory parameter. The user name for a user with the `iscadmin` role.
`--password tip_user_password`	Mandatory parameter. The password for the specified user name.

Export [--exportFile *export_file*] **[--pages ALL|NONE|***page1*,*page2*] **[--views ALL|NONE|***view1*,*view2*] **[--roles ALL|NONE|REQUIRED|***role1*,*role2*] **[--exportPagesInViews true|false] [--userPreferences ALL|NONE|REQUIRED|***user_ID1*,*user_ID2*] **[--consolePreferenceProfiles ALL|NONE|***pref_ID1*,*pref_ID2*] **[--includeEntitiesFromApp** *war1*,*war2*] **[--includeCustomData true|false] [--includeCredentialData true|false] [--includeMytasks true|false] [--includeMyStartupPages true|false] [--includeTransformations true|false] --username** *tip_username* **--password** *tip_user_password*

Table 43. ExportPagePlugin command arguments

Parameter and arguments	Description
`[--exportFile export_file]`	Optional parameter. Specifies the path and file name for the exported data, for example, `c:/tmp/extest.zip`.
`[--pages ALL|NONE|page1,page2]`	Optional parameter. If you do not use the `pages` parameter, the default setting is ALL unless either `exportPagesInViews` or `includeEntitiesFromApp` is defined, then the default setting is NONE. You can also provide a list of pages that you want to export.
`[--views ALL|NONE|view1,view2]` `--exportpageinviews [true|false]`	Optional parameter. If you do not use the `views` parameter, the default setting is ALL. You can also provide a list of views that you want to export and optionally specify that you want to export all pages associated with the specified views. **Note:** Whether the optional parameter `exportpageinviews` is set to `true` or `false`, if a view has a default node in the navigation pane associated with it, then the page associated with the node is always exported. This is also true, even if you specify NONE as the argument to the `--pages` parameter.

Table 43. ExportPagePlugin command arguments (continued)

Parameter and arguments	Description
[--roles ALL|NONE|REQUIRED|*role1*,*role2*]	Optional parameter. You can export no roles, all roles, or a specific list of roles. The default setting is ALL unless the pages parameter or the includeEntitiesFromApp parameter is specified. Then, the default setting is set to REQUIRED.
[--exportPagesInViews true|false]	Optional parameter. Use this parameter, set to true, to export the pages associated with an exported view. The default value is false.
[--userPreferences ALL|NONE|REQUIRED|*user_ID1*,*user_ID2*]	Optional parameter. You can export preferences for all users, no users, or for a specified list of users by user ID. The default setting is ALL. This parameter overrides the includeMytasks and includeMyStartupPages parameters.
[--consolePreferenceProfiles ALL|NONE|*pref_ID1*,*pref_ID2*]	Optional parameter. You can export no preference profile data, all preference profile data, or data for a specific list of preference profiles. The default setting is ALL. **Note:** If a console preference profile has a custom view as its default view, then that view is automatically exported. If the exported view has a default node in the navigation pane, then the associated page is automatically exported with the view.
[--includeEntitiesFromApp *war1*,*war2*]	Optional parameter. You can provide a list of WARs to export pages that contain portlets associated with the listed WARs.
[--includeCustomData true|false]	Optional parameter. The default value is true. If is set to false, no customization data is exported.
[--includeCredentialData true|false]	Optional parameter. The default value is true. If is set to false, no credential data is exported.
[--includeMytasks true|false]	Optional parameter. The default setting is true. This parameter only applies when the includeEntitiesFromApp parameter is also specified.
[--includeMyStartupPages true|false]	Optional parameter. The default setting is true. This parameter only applies when the includeEntitiesFromApp parameter is also specified.
[--includeTransformations true|false]	Optional parameter. The default setting is true.
--username *tip_username*	Mandatory parameter. The user name for a user with the iscadmins role.
--password *tip_user_password*	Mandatory parameter. The password for the specified user name.

Export [--includeCharts ALL|NONE|*page_ID1*,*page_ID2***] --username** *tip_username*
--password *tip_user_password*

Table 44. ChartExportPlugin commands

Parameter and arguments	Description
[--includeCharts ALL|NONE|*page_ID1*,*page_ID2*]	Optional parameter. You can export all charts, no charts, or specify a list of charts to be exported. The default setting is ALL. **Note:** If you run the Export command using the --includeCharts parameter, it must be run by the same user that started the Tivoli Integrated Portal Server.
--username *tip_username*	Mandatory parameter. The user name for a user with the chartAdministrator role.
--password *tip_user_password*	Mandatory parameter. The password for the specified user name.

Import `tipcli` commands

tipcli commands for importing Tivoli Integrated Portal data.

Note: If you specify additional parameters for the tipcli.bat|.sh Import and make a typing error, that is, if you type a parameter incorrectly, or use the incorrect case, then the commands runs as if no parameters were specified and no warning message is displayed.

ListImportPlugins
> Use the ListImportPlugins command to list all plugins that are available to be imported.

Import [--includePlugins|--excludePlugins *plugin1*,*plugin2*] **[--settingFile** *setting_file*] **[--backupDir backup_dir] --username** *tip_username* **--password** *tip_user_password*
> Use the Import command to import customization data into a Tivoli Integrated Portal environment. If you provide no parameters to the Import command, all custom data is imported by default.

Table 45. Import command arguments

Parameter and arguments	Description
[--includePlugins|--excludePlugins *plugin1*,*plugin2*]	Optional parameter. You can choose to include or exclude a list of plugins when you run the Import command.
[--settingFile *setting_file*]	Optional parameter. You can specify your import requirements in properties file instead of specifying your requirements using separate parameters at the command line. Provide a path to the settings file as the argument to the settingFile parameter. On systems running Windows you must use double backslashes characters (\\) when specifying the path to your settings file, for example, C:\\tmp\\import.properties. Command line parameters take precedence over entries in the settings file.
[--backupDir backup_dir]	You can specify a directory to save the backup data during an import operation so that if it is required you can subsequently restore settings.

Table 45. Import command arguments (continued)

Parameter and arguments	Description
`--username tip_username`	Mandatory parameter. The user name for a user with the `iscadmin` role.
`--password tip_user_password`	Mandatory parameter. The password for the specified user name.

Import [--importFile *import_file***] [--rollback ALL] [--haSupport both|true|false] --username** *tip_username* **--password** *tip_user_password*

Table 46. ImportPagePlugin command arguments

Parameter and arguments	Description
`[--importFile import_file]`	Optional parameter. Specifies the path and file name for the data to be imported, for example, `c:/tmp/extest.zip`.
`[--rollback ALL]`	Optional parameter. Use the `rollback` parameter if you want to restore a Tivoli Integrated Portal environment to its pre-import state. You can only roll back an import if you have made no changes to the environment since you performed the import.
`[--haSupport both|true|false]`	Optional parameter. You can set this parameter to `both`, `true`, or `false`. The setting indicates whether to include load balancing data, the default value is `both`. If you set it to `false`, only non-load balancing data is imported, that is, transformations. If is set to `true`, only load balancing base data is imported. When it is set to `both`, both types of data are imported. This parameter can also be used in non-load balanced environments. If is set to `true`, only base data is imported. If you set it to `false`, only non-base data is imported, that is, transformations.

Additional commands

Additional `tipcli` commands.

cmsUpdateRemoteEntries [--username *username* **--password** *password***] (-toremote | -fromremote | -deleteremote) [-force]**
   Save system information in the file specified.

Table 47. cmsUpdateRemoteEntries command arguments

Parameter and arguments	Description
`[--username username --password password]`	Optional parameters. User name and password for a Tivoli Integrated Portal user. If you do not provide user name and password details at the command line, you must enter the user name and password in an interactive mode.

Table 47. cmsUpdateRemoteEntries command arguments (continued)

Parameter and arguments	Description
-toremote	Optional parameter. Indicates that the update is to occur to the remote data store, that is, the local information is to be written to the remote database.
-fromremote	Optional parameter. Indicates that the update is to occur from the remote data store. Any information saved locally is downloaded and updated from the remote database.
-deleteremote	Optional parameter. Indicates that the launch entries provided by this Tivoli Integrated Portal instance to the remote database is to be deleted from the database. Additionally, this command prevents any further updates from being sent to the remote database. On execution, the cmsUpdateRemoteEntries command with the toremote and force options updates the database and re-enables automatic updates to the remote database. **Note:** There is no difference between deleteremote with the force option and deleteremote without the force option.
-force	Optional parameter. Indicates that any caching or optimization mechanisms for the data should be ignored and that the data should be updated regardless of the state.Any existing cached information is discarded. All data in the database is refreshed for the toremote case, including the resource bundles.

Version
> List the versions of the products and components installed in the environment.

SystemInfo [--outputFile *outputFile***]**
> Save system information in the file specified.

ITMLogin --hostname *hostname* **--port** *port* **--username** *username* **--password** *password* **[--servicename]**
> ITMLogin is used to configure the ITM Web Service to connect to the Tivoli Enterprise Portal Server. For example, this command in Windows configures the username and password for a new ITM Web Service to be added to the application server instance.
>
> ```
> C:\IBM\tivoli\tip\bin\tipcli.bat ITMLogin --hostname
> localhost --port 1920 --username sysadmin --password
> sysadm1n --servicename ITMWebService2
> ```
>
> You can use the ITMLogin command to change the hostname, port, username, and password of an existing Tivoli Enterprise Portal Server instance. Changing a configured ITM Web Service to a different Tivoli Enterprise Portal Server is not supported, because the two portal servers may have different configurations. If you need to use a different portal

server, you can install another instance of the ITM Web Service and use this command (along with the -serviceName option) to configure.

TADDMLogin --hostname *hostname* **[--port** *port***] --username** *username* **--password** *password*

Log in to the Tivoli Application Dependency Discovery Manager.

Appendix B. Web Applications configuration reference

Use this information to support configuration of web applications.

Web application configuration files

There are separate configuration files for the Network Manager web applications and for Topoviz. This section explains how to change configuration settings in these files.

There are two configuration files. These files are located at `ITNMHOME/profiles/TIPProfile/etc/tnm/`. These files contain all the settings used by the web applications. The configuration files are the following:

- `topoviz.properties`: Contains settings used by Topoviz.
- `status.properties`: Contains status display settings for Topoviz and the Structure Browser.
- `tnm.properties`: Contains settings used by all the other Network Manager web applications.

To change any of the settings in these files, edit the appropriate file.

Note: `ITNMHOME` is the environment variable that contains the path to the Network Manager installation directory.

Backup copies of both of these files, containing default settings, are held at the following location:`ITNMHOME/profiles/TIPProfile/etc/tnm/default`

Note: The `tnm.properties`, `status.properties`, and `topoviz.properties` files are monitored every 60 seconds for changes, so these changes are automatically detected by Topoviz.

Topoviz configuration files

The configuration files for IBM Tivoli Network Manager IP Edition Web applications and Topoviz contain all the settings that are used by each application.

The configuration files are located at `ITNMHOME/profiles/TIPProfile/etc/tnm`. The files are as follows:

- `topoviz.properties`: Contains settings used by Topoviz.
- `status.properties`: Contains status display settings for Topoviz and the Structure Browser.
- `tnm.properties`: Contains settings used by all the other Network Manager IP Edition Web applications.

To change any of the settings in these files, edit the appropriate file.

Backup copies of both of these files, containing default settings, are stored at the following location: `ITNMHOME/profiles/TIPProfile/etc/tnm/default`.

The `tnm.properties`, `status.properties`, and `topoviz.properties` files are monitored every 60 seconds for changes, so that these changes are automatically detected by Topoviz.

WebTools configuration files

Each web tool has its own XML configuration file.

These configuration files are held at the following locations: `ITNMHOME/profiles/TIPProfile/etc/tnm/tools` and `ITNMHOME/precision/scripts/webtools/etc`.

Table 44 lists the configuration files.

Table 48. WebTool Configuration Files

Type of Tool	Name of Tool	Name of Associated Configuration File
General Diagnostic and Information Retrieval Tools	Advanced Ping Tool	`AdvancedPing.xml`
	Advanced Subnet Ping Tool	`AdvancedSubnetPing.xml`
	Advanced Traceroute Tool	`AdvancedTraceroute.xml`
	Whois Lookup Tool	`WhoisLookup.xml`
	DNS Lookup Tool	`DNSLookup.xml`
Cisco Information Retrieval Tools	Cisco Information Tool	`CiscoBGPInfo.xml`
		`CiscoInterfaceList.xml`
		`CiscoISISInfo.xml`
		`CiscoMBGPInfo.xml`
		`CiscoMPLSInfo.xml`
		`CiscoOSPFInfo.xml`
		`CiscoRoutingInfo.xml`
		`CiscoVRFList.xml`
Cisco Diagnostic Tools	Cisco Route Information Tool	`CiscoShowRoute.xml`
	Cisco VRF Information Tool	`CiscoVRFInfo.xml`
	Cisco Ping Tool	`CiscoPing.xml`
	Cisco LSP Ping Tool	`CiscoLSPPing.xml`
	Cisco VRF Ping Tool	`CiscoVRFPing.xml`
	Cisco Traceroute Tool	`CiscoTraceroute.xml`
	Cisco LSP Traceroute Tool	`CiscoLSPTraceroute.xml`
	Cisco VRF Traceroute Tool	`CiscoVRFTraceroute.xml`
Juniper Information Retrieval Tools	Juniper Information Tool	`JuniperBGPInfo.xml`
		`JuniperInterfaceList.xml`
		`JuniperISISInfo.xml`
		`JuniperMPLSInfo.xml`
		`JuniperOSPFInfo.xml`
		`JuniperRoutingInfo.xml`
		`JuniperVRFList.xml`

Table 48. WebTool Configuration Files (continued)

Type of Tool	Name of Tool	Name of Associated Configuration File
Juniper Diagnostic Tools	Juniper Route Information Tool	`JuniperShowRoute.xml`
	Juniper Ping Tool	`JuniperPing.xml`
	Juniper Traceroute Tool	`JuniperTraceroute.xml`

WebTools configuration files define all parameters used by WebTools. You should not normally need to change these parameters.

The only parameters that you might be required to configure are the Telnet login details for the Cisco and Juniper tools, as described in "Configuring Telnet Login Details".

Note: Passwords specified in the WebTools configuration files are plain-text. If you configure Telnet login details within these files, then it is recommended that you apply appropriate security measures to the WebTools directories, `ITNMHOME/profiles/TIPProfile/etc/tnm/tools` and `ITNMHOME/precision/scripts/ webtools/etc`.

Structure Browser configuration files

The appearance and tools of the Structure Browser are controlled through configuration files.

The following configuration files control the appearance of the Structure Browser window. Both files are located in `ITNMHOME/profiles/TIPProfile/etc/tnm`.
- The `structurebrowser.properties` file controls settings that are only related to the Structure Browser window.
- The `status.properties` file controls all status indicator settings for both the Topoviz views and the Structure Browser window.
- The `ncp_structurebrowser_menu.xml` file controls what tools are available in through the Structure Browser.

Note: The `structurebrowser.properties`,`status.properties`, and `ncp_structurebrowser_menu.xml` files are monitored every 60 seconds for changes, so these changes are automatically detected by the Structure Browser.

The managed status column can be hidden or displayed, and the managed and unmanaged icons are customizable also. You can set whether the column appears in the **Device Structure Tree** and change the icons for the managed and unmanaged states in the `structurebrowser.properties` file.

URL parameters

Use URL parameters to construct a URL to launch any of the Network Manager Web applications directly from a Web browser. For example, you can construct a URL to launch the Hop View containing a predefined network map.

These parameters can be typed directly into the address bar of your browser. Alternatively, you could write a Tivoli Netcool/OMNIbus Web GUI tool to pass column values for an event to a CGI script. The script could then call the relevant Web application with these parameters.

Default windows composed of multiple Web applications, such as the Network Health View, cannot be opened using a URL. The following table lists the Network Manager Web applications that can be opened using URLs.

Table 49. GUI windows that can be opened with URLs

Window	URL	Takes parameters
Hop View	https://host:port/ibm/console/ncp_topoviz/HopView.do	Yes
MIB Browser	https://host:port/ibm/console/ncp_mibbrowser/Launch.do	Yes
MIB Grapher	https://host:port/ibm/console/ncp_mibbrowser/pages/mib_graph/mibgraphview_servlet.jsp	Yes
Network Discovery Configuration	https://host:port/ibm/console/ncp_disco/DiscoConfig.do	No
Network Discovery Status	https://host:port/ibm/console/ncp_disco/DiscoStatus.do	No
Network Views	https://host:port/ibm/console/ncp_topoviz/NetworkView.do	Yes
Path Views	https://host:port/ibm/console/ncp_topoviz/PathViewNewPath.do	Yes
Web Tools	https://host:port/ibm/console/ncp_webtools/pages/ncp_wt_index.jsp?	Yes

The following topics explain the URL parameters to use for the different Web applications.

Hop View URL parameters

Use this information to understand how to construct a URL to display layer 2 and layer 3 connectivity maps in the Hop View.

URL parameters

The following table shows the URL parameters that you can pass to the Hop View to display layer 2 or layer 3 connectivity maps.

Table 50. URL parameters for Hop View maps

Parameter	Description	Required?
seed	An identifier for the seed device. This may be the `EntityName`, `IPAddress` or `ObjectId` of the required seed device. This corresponds to the **Seed** field in the Hop View toolbar.	Yes
domain	The name of the Network Manager domain. This corresponds to the **Domain** field in the Hop View toolbar.	Yes
hops	This is the number of hops from the seed device. This corresponds to the **Hops** field in the Hop View toolbar.	No
layout	This can be any of the following: • hierarchical • symmetrical • orthogonal • circular	No
endNodes	This can take one of the following values: • `true`: Show end nodes in the map. • `false`: Do not show end nodes in the map.	No
connectivity	This can take one of the following values: • `layer1` • `layer2` • `layer3` • `ipsubnets` This corresponds to the **Connectivity** field in the Hop View toolbar.	No

Example 1: URL for layer 2 connectivity map

The following example shows the format of a Topoviz URL for a layer 2 connectivity map. Note that Topoviz URLs are case-sensitive.

```
https://host:port/ibm/console/ncp_topoviz/HopView.do?domain=MPLSTEST&type=layer2
&layout=hierarchical&seed=lon-core-cis-h.ibm.com&hops=2&endNodes=true
```

Example 2: URL for layer 3 connectivity map

The following example shows the format of a Topoviz URL for a layer 3 map. Note that Topoviz URLs are case-sensitive.

```
https://host:port/ibm/console/ncp_topoviz/HopView.do?domain=MPLSTEST&type=layer3
&layout=symmetric&seed=lon-core-cis-h.ibm.com&HOPS=2&endNodes=true
```

Network Views URL parameters

Use this information to understand how to construct a URL to display specific maps in the network views.

Each saved network view has a unique ID. To find out the ID of a particular view, hover the cursor over the name of the view in the navigation tree. The ID is displayed in the status bar at the bottom of the browser window, and as a tooltip.

Passing a network view ID in the URL to Network Views opens that network view. The view is shown without the navigation tree.

URL for a saved network view

The following example shows the format of a Network Views URL containing the parameter `id`. Note that Topoviz URLs are case-sensitive.

`https://`*`host:port`*`/ibm/console/ncp_topoviz/NetworkView.do?`**`id=10690`**

MIB Browser URL Reference

You can launch the MIB Browser directly from a web browser. The URL required to launch an empty MIB Browser is as follows:

`https://`*`host:port`*`/ibm/console/ncp_mibbrowser/Launch.do`

In this URL:
* *host* is the IP address of the host on which the Tivoli Integrated Portal server is running.
* *port* is the port to access on the host on which the Tivoli Integrated Portal server is running. By default this is `16316`.

This URL opens the MIB Browser with the **Domain** option menu set to the first value in the list, and no **Host** or **OID** values set in the SNMP Query toolbar.

URL Parameters

You can supply the following optional parameters when you launch the MIB Browser:
* `domain`: name of the Network Manager domain to use to obtain the MIB and SNMP data. The value of this parameter is used to set the **Domain** option menu in the Configuration Toolbar.

  If you are writing a tool to launch the MIB Browser from the AEL, then you may wish to specify the name of the ObjectServer rather than the name of the Network Manager domain. Do this by supplying the parameter `$selected_rows.ServerName`, where `ServerName` is the field in the AEL event that specifies the name of the ObjectServer.
* `host`: IP address of the target device to be queried for SNMP data. This value is used to populate the **Host** field in the SNMP Query Toolbar.
* `variable`: the MIB object to query. This value can be the OID of the MIB object, such as `1.3.6.1.2.1.1.3` or it can be the name of the MIB object, such as `sysUpTime`. This value is used to populate the **OID** field in the SNMP Query Toolbar.
* `resultsOnly`: takes one of the values `true` or `false`.
  - If `true`, then the MIB Browser is launched in full mode.
  - If `false`, then the MIB Browser is launched in results-only mode.

If you supply the *domain,* *host,* and *variable* parameters, then the MIB Browser launches, automatically performs the SNMP query specified by these parameters, and then displays the results in the SNMP Query Results Area. The type of SNMP query performed varies depending on the value of the *variable* parameter:

- If the *variable* parameter is a single MIB object in the MIB tree then the MIB Browser performs an SNMP `Get` query on startup.
- If the *variable* parameter is a table in the MIB tree then the MIB Browser performs an SNMP `Get Table` query on startup.
- In all other cases, the MIB Browser performs an SNMP `Walk` query on startup.

Examples of URLs

Some examples of URLS to launch the MIB Browser are shown below:

- `https://host:port/ibm/console/ncp_mibbrowser/Launch.do`

  The MIB Browser opens up with the **Domain** option menu set to the first value. No host or OID values are set in the SNMP Query Toolbar.

- `https://host:port/ibm/console/ncp_mibbrowser/Launch.do?domain=NCOMS`

  The MIB Browser opens up with the **Domain** option menu set to the specified domain.

- `https://host:port/ibm/console/ncp_mibbrowser/Launch.do?domain=NCOMS&host=198.162.3.4`

  The MIB Browser opens up with the **Domain** option menu set to the specified domain and the Host field set to 198.162.3.4.

- `https://host:port/ibm/console/ncp_mibbrowser/Launch.do?domain=NCOMS&host=198.162.3.4&variable=ifTable`

  The MIB Browser opens up with the **Domain** option menu, the **Host** and **OID** fields set accordingly. In addition, an SNMP `Get Table` query will automatically be issued for the MIB object `ifTable`. The results will be displayed in the SNMP Query Results Area.

- `https://host:port/ibm/console/ncp_mibbrowser/Launch.do?domain=NCOMS&host=198.162.3.4&variable=sysUpTime&resultsOnly=true`

  The MIB Browser opens up with the **Domain** option menu, the **Host** and **OID** fields set accordingly. In addition, an SNMP `Get` query will automatically be issued for the MIB object `sysUpTime`. The MIB Browser opens in results-only mode and contains only the results showing the value of sysUpTime for the network device with IP address 198.162.3.4.

MIB Grapher URL Reference

You can graph MIB variables for a node or interface by specifying a URL in your Web browser.

The following table shows the parameters for the MIB Grapher.

Table 51. URL parameters for the MIB Grapher

Parameter	Description	Required?
domain	The name of the Network Manager domain.	Yes
host	The hostname of the node or interface for which you want to graph MIB variables.	Yes
init	Required to be set to `true` for launching this window.	Yes

Example: URL to graph MIB variables for a device

https://host:port/ibm/console/ncp_mibbrowser/pages/mib_graph/
mibgraphview_servlet.jsp?init=true&domain=NCOMS&host=192.168.0.2

Web Tools URL reference

You can also launch WebTools by specifying a URL in your web browser to call up a form-based interface. This is useful if you want to gain access to WebTools without logging into Topoviz.

To launch WebTools using a URL:

1. Open a supported web browser and enter the following URL:

   ```
   https://host:port/ibm/console/ncp_webtools/pages/ncp_wt_index.jsp?
   domain=domain name
   ```

   In this URL:

   - *host* is the IP address of the host on which the Tivoli Integrated Portal server is running.
   - *port* is the port to access on the host on which the Tivoli Integrated Portal server is running. By default this takes the value of 16311.
   - *domain* is the domain you want to access with the tools.

   For example,

   ```
   https://test.itnm.com:16311/ibm/console/ncp_webtools/pages/ncp_wt_index.jsp?
   domain=NCOMS
   ```

   The Tivoli Integrated Portal Login page appears in the web browser.

2. Enter your username and password.

   Note: Usernames and passwords are case-sensitive.

3. Click the **Log In** button.
   The main **WebTools** menu appears. This provides access to the following web tools:

   - General tools
   - Cisco-specific tools
   - Juniper-specific tools

Note: It is also possible to launch a web tool from a third-party application, such as a web page. To do this, launch the desired web tool in Topoviz, copy the URL that Topoviz generates in the **Address** field of your browser, and paste this URL to the third-party application.

Path Views URL parameters

You can create a new Path View or find a device in an existing Path View by specifying a URL in your Web browser.

The following table shows the parameters for Path Views.

Table 52. URL parameters for Path Views

Parameter	Description	Required?
domain	The name of the Network Manager domain.	Yes, to create a path.
entityID	The ID of the entity to find in a path.	Yes

Example: URL to create a new path

https://host:port/ibm/console/ncp_topoviz/
PathViewNewPath.do?domain=MPLSTEST&entityId=10690

Example: URL to find a device in a path

https://host:port/ibm/console/ncp_topoviz/FindPathView.do?entityId=10690

Cisco and Juniper WebTools commands

Use this information to determine which commands are executed by the Cisco and Juniper WebTools.

The following topics list the relevant commands.

Cisco information tools

Use this information to determine which commands are executed by the WebTools that retrieve information from Cisco devices.

The following table shows the commands executed by the Cisco information tools, and specifies how to launch each web tool from a network map within the Hop View or Network Views, and from the main WebTools menu.

Table 53. Cisco Information Tools Reference

Web Tool	Commands executed	Right-click menu option	Menu option in the main WebTools menu

Cisco Information Tool – BGP	`show ip bgp summary`
	
	`show ip bgp flap-statistics`
	
	`show ip bgp dampened-paths`
	
	`show ip bgp inconsistent-as`
	
	`show ip bgp neighbors`
		Webtools > Information Tools > View BGP Information	**Cisco Information Tool > BGP information**

Cisco Information Tool – Interface	`show ip interface brief`	**Webtools > Information Tools > View Interfaces**	**Cisco Information Tool > Interface information**

Cisco Information Tool – ISIS	`show isis neighbors`
	
	`show isis topology`
		Webtools > Information Tools > View ISIS Information	**Cisco Information Tool > ISIS information**

Cisco Information Tool – MBGP	`show ip bgp vpn all flap-statistics`
	
	`show ip bgp vpn all dampened-paths`
	
	`show ip bgp vpn all neighbors`
	
	`show ip bgp vpn all paths`
		Webtools > Information Tools > View MBGP Information	**Cisco Information Tool > MBGP information**

Cisco Information Tool – MPLS	`show ip rsvp interface`
	
	`show ip vrf detail`
	
	`show mpls l2transport vc`
	
	`show mpls forwarding-table`
		Webtools > Information Tools > View MPLS Information	**Cisco Information Tool > MPLS information**

Table 53. Cisco Information Tools Reference (continued)

Web Tool	Commands executed	Right-click menu option	Menu option in the main WebTools menu

Cisco Information Tool – MPLS TE	`show mpls traffic-eng tunnels brief`
	
	`show mpls traffic-eng autoroute`
		Webtools > Information Tools > View MPLS TE Information	**Cisco Information Tool > MPLS TE Tunnel information (general)**

Cisco Information Tool – MPLS TE (filtered)	`show mpls traffic-eng tunnels source` *source* `show mpls traffic-eng tunnels destination` *destination* `show mpls traffic-eng tunnels` *tunnelInterface* `show mpls traffic-eng tunnels role [all|head|middle|remote |tail]`	**Webtools > Information Tools > View MPLS TE Information (filtered)**	Not available

Cisco Information Tool – MPLS TE Link Management	`show mpls traffic-eng link-management summary`
	
	`show mpls traffic-eng link-management interfaces [`*interface*`]`
		Webtools > Information Tools > View MPLS TE Link Management Information	Not available

Cisco Information Tool – OSPF	`show ip ospf`
	
	`show ip ospf interface`
	
	`show ip ospf neighbor`
	
	`show ip ospf border-routers`
	
	`show ip ospf statistics`
		Webtools > Information Tools > View OSPF Information	**Cisco Information Tool > OSPF Information**

Cisco Information Tool – Routing Summary	`show ip protocols`
	
	`show ip route summary`
	
	`show ip route static`
	
	`show ip route eigrp`
	
	`show ip route ospf`
	
	`show ip route isis`
		Webtools > Information Tools > View Routing Summary Information	**Cisco Information Tool > Routing summary**

Cisco Information Tool – VRF List	`show ip vrf list`
	
	`show ip vrf interfaces`
		Webtools > Information Tools > View VRF Information	**Cisco Information Tool > VRF list**

Cisco diagnostic tools

Use this information to determine which commands are executed by the WebTools that perform diagnosis on Cisco devices.

The following table shows the commands executed by the Cisco diagnostic tools, and specifies how to launch each web tool from a network map within the Hop View or Network Views, and from the main WebTools menu.

Table 54. Cisco and Juniper WebTools Reference

Web Tool	Commands Executed	Menu Option	Menu Option in the main WebTools menu
Cisco Route Information Tool	`show ip route target`	**Cisco Tools... Diagnostic Tools... View a Route...**	**Cisco Routing Information**
Cisco VRF Information Tool	`show ip route vrf vrf_name target`	Not available	**Cisco VRF Information**
Cisco Ping Tool	`ping target`	**Cisco Tools...** **Diagnostic Tools...** **Ping from this device...**	**Cisco Ping**
Cisco LSP Ping Tool	`ping mpls ipv4 target verbose`	**Cisco Tools...** **Diagnostic Tools...** **LSP Ping from this device...**	**Cisco LSP Ping**
Cisco VRF Ping Tool	`ping vrf vrf_name ip target`	**Cisco Tools...** **Diagnostic Tools...** **VRF Ping from this device...**	**Cisco VRF Ping**
Cisco Traceroute Tool	`traceroute target`	**Cisco Tools...** **Diagnostic Tools...** **Traceroute from this device...**	**Cisco Traceroute**
Cisco LSP Traceroute Tool	`traceroute mpls ipv4 target verbose`	**Cisco Tools...** **Diagnostic Tools...** **LSP Traceroute from this device...**	**Cisco LSP Traceroute**
Cisco VRF Traceroute Tool	`traceroute vrf vrf_name ip target`	**Cisco Tools...** **Diagnostic Tools...** **VRF Traceroute from this device...**	**Cisco VRF Traceroute**

Juniper information tools

Use this information to determine which commands are executed by the WebTools that retrieve information from Juniper devices.

The following table shows the commands executed by the Juniper information tools, and specifies how to launch each web tool from a network map within the Hop View or Network Views, and from the main WebTools menu.

Table 55. Cisco and Juniper WebTools Reference

Web Tool	Commands Executed	Menu Option	Menu Option in the main WebTools menu

Juniper Information Tool – BGP	`show ip bgp summary`
	
	`show ip bgp flap-statistics`
	
	`show ip bgp dampened-paths`
	
	`show ip bgp inconsistent-as`
	
	`show ip bgp neighbors`
		Juniper Tools...
		
		Information Tools...
		
		View BGP Information...
			Juniper Information Tool

Juniper Information Tool – Interfaces	`show ip interface brief`	**Juniper Tools...** **Information Tools...** **View Interfaces...**	**Juniper Information Tool**

Juniper Information Tool – ISIS	`show isis neighbors`
	
	`show isis topology`
		Juniper Tools...
		
		Information Tools...
		
		View ISIS Information...
			Juniper Information Tool

Juniper Information Tool – MPLS	`show ip rsvp interface`
	
	`show ip vrf detail`
	
	`show mpls l2transport vc`
	
	`show mpls forwarding-table`
		Juniper Tools...
		
		Information Tools...
		
		View MPLS Information...
			Juniper Information Tool

Juniper Information Tool – OSPF	`show ip ospf`
	
	`show ip ospf interface`
	
	`show ip ospf neighbor`
	
	`show ip ospf border-routers`
	
	`show ip ospf statistics`
		Juniper Tools...
		
		Information Tools...
		
		View OSPF Information...
			Juniper Information Tool

Table 55. Cisco and Juniper WebTools Reference (continued)

Web Tool	Commands Executed	Menu Option	Menu Option in the main WebTools menu

Juniper Information Tool – Routing Summary	`show ip protocols`
	
	`show ip route summary`
	
	`show ip route static`
	
	`show ip route eigrp`
	
	`show ip route ospf`
	
	`show ip route isis`
		Juniper Tools...
		
		Information Tools...
		
		View Routing Summary Information...
			Juniper Information Tool

Juniper Information Tool – VRF List	`show ip vrf list`
	
	`show ip vrf interfaces`
		Juniper Tools...
		
		Information Tools...
		
		View VRF Information...
			Juniper Information Tool

Juniper diagnostic tools

Use this information to determine which commands are executed by the WebTools that perform diagnosis on Cisco devices.

The following table shows the commands executed by the Juniper diagnostic tools, and specifies how to launch each web tool from a network map within the Hop View or Network Views, and from the main WebTools menu.

Table 56. Juniper Diagnostic Tools

Web Tool	Commands Executed	Menu Option	Menu Option in the main WebTools menu
Juniper Route Information Tool	`show route` *`target`*	**Juniper Tools...** **Diagnostic Tools...** **View a Route...**	**Juniper Routing Information**
Juniper Ping Tool	`ping` *`target`*	**Juniper Tools...** **Diagnostic Tools...** **Ping from this device...**	**Juniper Ping**
Juniper Traceroute Tool	`traceroute` *`target`*	**Juniper Tools...** **Diagnostic Tools...** **Traceroute from this device...**	**Juniper Traceroute**

Appendix C. Report reference

Network Manager reports are grouped by their function. Use this reference to understand the typical uses, prerequisites, and other properties of each report.

Network Manager data model

Each product that uses the Cognos data model provides namespaces, which contain query subjects to use to build up reports.

Namespaces

The Network Manager data model provides the following namespaces for designing reports.

Event The Event namespace contains query subjects to create Current® Status reports.

Monitoring Data
>   The Monitoring Data namespace contains query subjects to create Performance reports. The polled data timestamp has a time dimension relationship to allow time dimension reports. The data for the Monitoring Data namespace comes from the NCPOLLDATA database.

Network
>   The Network namespace contains query subjects to create Asset and Troubleshooting reports. The data for the Network namespace comes from the NCIM database.

Network Views
>   The Network Views namespace contains query subjects to create reports about network views and policies updating views. The data for the Network Views namespace comes from the NCPGUI and NCMONITOR databases.

Path Views
>   The Path Views namespace contains query subjects to create Path Views reports.

Shared
>   The Shared namespace contains query subjects that can be shared to prevent query subject duplicates.

Asset reports

Asset reports provide views on the discovered attributes of the network devices for inventory information.

To access the Asset reports, click **Reporting** > **Common Reporting** > **Network Manager**. Then click **Asset Reports**.

Card Detail by Card Type report

Displays the results of card discovery operations performed by the Entity MIB and Entity Discovery agents. The report is organized by card type and is based on the data extracted from the entPhysicalVendorType entity MIB table.

Report properties

The following table describes the Card Detail by Card Type report.

Table 57. Properties of the Card Detail by Card Type report

Property	Description
Typical uses	Use this report to locate the devices housing a specific card type.
Prerequisites	None
Data model	BIRT

Card Detail by Device Type report

Displays the results of device discovery operations performed by the entity MIB agent. The report is organized by device type and is based on the data extracted from the entPhysicalVendorType entity MIB table.

Report properties

The following table describes the Card Detail by Device Type report.

Table 58. Properties of the Card Detail by Device Type report

Property	Description
Typical uses	Use this report identify the card details within a device.
Prerequisites	This report requires the Entity MIB and Entity discovery agents to be enabled.
Data model	BIRT

Discovery Drilldown report

Displays the results of the network discovery organized by device vendor. The report displays a list of vendor names. It lists device classes for each vendor.

Report properties

The following table describes the Discovery Drilldown report.

Table 59. Properties of the Discovery Drilldown report

Property	Description
Typical uses	Use this report to look up interface details on a device, such as spare ports, or MAC and IP addresses.
Prerequisites	None
Data model	BIRT

Hardware MAC Vendor report

Displays information on equipment vendors with registered MAC addresses.

Report properties

The following table describes the Hardware MAC Vendor report.

Table 60. Properties of the Hardware MAC Vendor report

Property	Description
Typical uses	Use this report to lookup interface details, including ifAlias, on devices sorted by vendor.
Prerequisites	None
Data model	BIRT

Interface Availability report

Displays a table of interface types and statuses broken down by vendor, class name and device. The report also displays the count of each interface type on the network and the status of those interfaces (up or down). One report is displayed for each selected domain.

Report properties

The following table describes the Interface Availability report.

Table 61. Properties of the Interface Availability report

Property	Description
Typical uses	Use this report to determine the counts of each interface type, both functioning and non-functioning.
Prerequisites	None
Data model	Cognos

IP Addressing Summary report

Displays information on the IP addresses used in the network grouped according to CIDR notations.

Report properties

The following table describes the IP Addressing Summary report.

Table 62. Properties of the IP Addressing Summary report

Property	Description
Typical uses	Use this report to identify IPv4 subnets with spare IP addressing capacity or those subnets over a specific threshold of allocated IP addresses.
Prerequisites	None
Data model	Cognos

Operating System by Device report

Displays information on the operating systems running on the various devices in your network. This report only shows information for Cisco and Juniper devices.

Report properties

The following table describes the Operating System by Device report.

Table 63. Properties of the Operating System by Device report

Property	Description
Typical uses	Use this report to show operating system details by device and vendor. For example, you can locate devices with a certain operating system that has a newly released security update.
Prerequisites	The OSInfo agent must be run during discovery in order for the information required for this report to be available.
Data model	Cognos

Summary By Device Class report

Displays a bar graph with the number of devices on your network displayed by class name.

Report properties

The following table describes the Summary By Device Class report.

Table 64. Properties of the Summary By Device Class report

Property	Description
Typical uses	Use this report to show a quick count of devices by Active Object Class (AOC) groups. For instance, how many Cisco 3750 devices are in use.
Prerequisites	None
Data model	BIRT

Vendor and Device Availability report

Displays class names and device counts grouped by vendor. The report also displays the count and percentage of devices for each vendor broken down by device type.

Report properties

The following table describes the Vendor and Device Availability report.

Table 65. Properties of the Vendor and Device Availability report

Property	Description
Typical uses	Use this report to show a quick count of devices by vendor and device model.
Prerequisites	None

Table 65. Properties of the Vendor and Device Availability report (continued)

Property	Description
Data model	BIRT

Current Status reports

Current Status reports provide useful status on any outstanding problems. They list the work queue and the waiting queue in terms of the devices affected, and are sorted by age of the events.

To access the Current Status reports, click **Reporting** > **Common Reporting** > **Network Manager**. Then click **Current Status Reports**.

Acknowledged Events by First Occurrence report

Displays a list of acknowledged events with severity higher than "Warning", sorted by event severity and age of event.

Report properties

The following table describes the Acknowledged Events by First Occurrence report.

Table 66. Properties of the Acknowledged Events by First Occurrence report

Property	Description
Typical uses	This report presents shift leaders with a quick status of the incident queue. This report looks at acknowledged events and shows incidents being worked on.
Prerequisites	None.
Data model	BIRT

Unacknowledged Events by First Occurrence report

Displays a list of unacknowledged events with severity higher than "Warning", sorted by event severity and age of event.

Report properties

The following table describes the Unacknowledged Events by First Occurrence report.

Table 67. Properties of the Unacknowledged Events by First Occurrence report

Property	Description
Typical uses	This report presents shift leaders with a quick status of the incident queue. This report looks at unacknowledged events and shows incidents that are waiting to be assigned.
Prerequisites	None.
Data model	BIRT

Monitoring reports

Monitoring reports provide a list of devices being polled under each monitoring policy to help you verify that you are polling the correct devices for the correct information.

To access the Monitoring reports, click **Reporting** > **Common Reporting** > **Network Manager**. Then click **Monitoring Reports**.

Monitoring Device Details report

Displays detailed information about the monitoring policies enabled for a device.

Report properties

The following table describes the Monitoring Device Details report.

Table 68. Properties of the Monitoring Device Details report

Property	Description
Typical uses	You would run this report to verify how a particular device is being monitored by Network Manager by listing all the policies whose scope matches this device.
Prerequisites	None
Data model	BIRT

Monitoring Policy Details report

Displays detailed information about a selected monitoring policy.

Report properties

The following table describes the Monitoring Policy Details report.

Table 69. Properties of the Monitoring Policy Details report

Property	Description
Typical uses	Run this report to verify the list of devices being monitored by this policy.
Prerequisites	None
Data model	BIRT

Monitoring Policies Report

Also known as the Monitoring Policies report, if it is launched as a right-click report. Displays all the enabled policies and for each policy all the devices and interfaces that match the scope.

Report properties

The following table describes the Monitoring Summary report.

Table 70. Properties of the Monitoring Summary report

Property	Description
Typical uses	You can run this report to archive the monitoring configuration for your network, or use it for reference purposes offline.
Prerequisites	None
Data model	BIRT

Network Technology reports

Network Technology reports provide insight into the states of BGP, OSPF, and VLAN networks based on information gathered during discovery.

To access the Network Technology reports, click **Reporting** > **Common Reporting** > **Network Manager**. Then click **Network Technology Reports**.

BGP Details report

Displays detailed information about BGP Sessions and Autonomous Systems.

Report properties

The following table describes the BGP Details report.

Table 71. Properties of the BGP Details report

Property	Description
Typical uses	Run this report to see the members of each BGP session and its state for each Autonomous System. View the details of any route reflectors and their clients and the state of each member of the Autonomous Systems.
Prerequisites	None
Data model	BIRT

BGP Summary report

Displays charts and tables with BGP Session and Autonomous System Summary information.

Report properties

The following table describes the BGP Summary report.

Table 72. Properties of the BGP Summary report

Property	Description
Typical uses	Run this report to see a quick count of the elements in the BGP environment including the Autonomous Systems, inter-AS, and sessions per state.
Prerequisites	None
Data model	BIRT

Device Connectivity report

The Device Connectivity report lists all interfaces that a device is connected to.

Report properties

The following table describes the Device Connectivity report.

Table 73. Properties of the Device Connectivity report

Property	Description
Typical uses	Run this report to understand the various physical and logical connections from the ports or interfaces on a specific device, including the remote ports or interfaces.
Prerequisites	None
Data model	BIRT

MPLS VPN Details report

Displays detailed information about discovered MPLS VPNs including VRFs, Route Distinguishers, Route Targets, and VPWS.

Report properties

The following table describes the MPLS VPN Details report.

Table 74. Properties of the MPLS VPN Details report

Property	Description
Typical uses	Run this report to see details of the MPLS VPNs discovered in this domain. See details of the VRF Route Targets including import/export mismatches, membership details of VPN and VPWS, as well as PE/CE connections and PE/P connections.
Prerequisites	None
Data model	BIRT

MPLS VPN Summary report

Displays charts and tables with MPLS VPN summary information.

Report properties

The following table describes the MPLS VPN Summary report.

Table 75. Properties of the MPLS VPN Summary report

Property	Description
Typical uses	Run this report to see a quick list and count of the VPNs, VPWS devices, and associated PE/CE devices.
Prerequisites	None
Data model	BIRT

OSPF Details report

Displays charts and tables with detailed OSPF Session and Area information.

Report properties

The following table describes the OSPF Details report.

Table 76. Properties of the OSPF Details report

Property	Description
Typical uses	Run this report to see the routers and their roles in the OSPF areas, the session states and costs on each interface, the Type 2 LSA origination routers and connections.
Prerequisites	None
Data model	BIRT

OSPF Summary report

Displays charts and tables with OSPF Session and Area summary information.

Report properties

The following table describes the OSPF Summary report.

Table 77. Properties of the OSPF Summary report

Property	Description
Typical uses	Run this report to see a quick list of the OSPF areas and the counts for the various router types and states.
Prerequisites	None
Data model	BIRT

VLAN Details report

Displays detailed information about VLANs and trunk ports.

Report properties

The following table describes the VLAN Details report.

Table 78. Properties of the VLAN Details report

Property	Description
Typical uses	Run this report to see a list of VLAN IDs on each interface of a VLAN supported device, or a list of interfaces in each VLAN ID.
Prerequisites	None
Data model	BIRT

VLAN Membership report

Displays information on device and interface VLAN membership.

Report properties

The following table describes the VLAN Membership report.

Table 79. Properties of the VLAN Membership report

Property	Description
Typical uses	Run this report to see the interface details of the members of a specific VLAN ID.
Prerequisites	None
Data model	BIRT

VLAN Summary report

Displays charts and tables with VLAN summary information.

Report properties

The following table describes the VLAN Summary report.

Table 80. Properties of the VLAN Summary report

Property	Description
Typical uses	Run this report to see counts of VLAN operational interfaces per VLAN ID, counts of trunk ports and lists of VLAN IDs per device.
Prerequisites	None
Data model	BIRT

VTP Summary report

Displays charts and tables with VTP summary information.

Report properties

The following table describes the VTP Summary report.

Table 81. Properties of the VTP Summary report

Property	Description
Typical uses	Run this report to see a list of the VTP domains and count of interfaces, including a breakdown of the VTP modes.
Prerequisites	Requires the CiscoVTP discovery agent.
Data model	BIRT

Network Views reports

These reports show details about network views.

To access the Network Views reports, click **Reporting** > **Common Reporting** > **Network Manager**. Then click **Network Views Reports**.

Monitored Network Views report

Displays the poll definitions, policies, and entities that are being monitored for each network view.

Report properties

The following table describes the Monitored Network Views report.

You can drill down from this report to see the devices and interfaces monitored by an individual poll definition in the Monitored Network Views Drilldown report.

Table 82. Properties of the Monitored Network Views report

Property	Description
Typical uses	Run this report to see the poll definitions, policies, and entities that are being monitored.
Prerequisites	None
Data model	Cognos

Path Views reports

Path Views reports allow you to view device and routing information for IP and MPLS TE paths.

To access the Path Views reports, in the Tivoli Common Reporting portlet, click **Reporting** > **Common Reporting** > **Network Manager**. Then click **Path Views Reports**.

IP Path Detail report

Displays the devices and interfaces for the IP path.

Report properties

The following table describes the IP Path Detail report.

Table 83. Properties of the IP Path Detail report

Property	Description
Typical uses	Use this report to view and check ingress and egress interface details of each hop for a selected user created path. This report can also be generated from the IP Path Summary report.
Prerequisites	None
Data model	Cognos

IP Path Summary report

Displays all the IP Paths configured.

Report properties

The following table describes the IP Path Summary report.

Table 84. Properties of the IP Path Summary report

Property	Description
Typical uses	Use this report to view a list of all user created paths showing ingress and egress information of the path, status, and path changes. From this report drill down into any of the paths to check ingress and egress interface details of each hop.
Prerequisites	None
Data model	Cognos

IP Routing Info report

Displays the device and routing information for a specific device or multiple devices on the path.

Report properties

The following table describes the IP Routing Info report.

Table 85. Properties of the IP Routing Info report

Property	Description
Typical uses	Generate this report from a member device of a user-created path on a topology map to see details of the ingress and egress interfaces of the device for this path.
Prerequisites	None
Data model	Cognos

MPLS TE Path Detail report

Displays the devices and interfaces for the MPLS TE path.

Report properties

The following table describes the MPLS TE Path Detail report.

Table 86. Properties of the MPLS TE Path Detail report

Property	Description
Typical uses	Use this report to view and check ingress and egress interface details of each hop for a selected MPLS-TE tunnel. This report can also be generated from the MPLS-TE Path Summary report.
Prerequisites	None
Data model	Cognos

MPLS TE Path Summary report

Displays all the MPLS TE Tunnels that were discovered in the network.

Report properties

The following table describes the MPLS TE Path Summary report.

Table 87. Properties of the MPLS TE Path Summary report

Property	Description
Typical uses	Use this report to view a list of all MPLS-TE tunnels showing ingress and egress information of the tunnel, status, and path changes. From this report drill down into any of the tunnels to check ingress and egress interface details of each hop.
Prerequisites	None
Data model	Cognos

MPLS TE Routing Info report

Displays the device and routing information for a specific device or multiple devices on the tunnel.

Report properties

The following table describes the MPLS TE Routing Info report.

Table 88. Properties of the MPLS TE Routing Info report

Property	Description
Typical uses	Generate this report from a member device of a MPLS-TE tunnel on any topology map to see details of the ingress and egress interfaces of the device for this tunnel.
Prerequisites	None
Data model	Cognos

Performance reports

Performance reports allow you to view any historical performance data that has been collected by the monitoring system for diagnostic purposes. View trend and topN charts for data to gain insight on short term behaviors.

To access the Performance reports, click **Reporting** > **Common Reporting** > **Network Manager**. Then click **Performance Reports**.

Note: The amount of historical data that the system can store and, consequently, the amount of historical data that the Performance reports can display, is restricted by default to preserve report performance. You can increase the storage limit for historical performance data; however, this can lead to a degradation in the performance of the Performance reports.

Bandwidth Top N report

Displays the bandwidth of the top N devices.

Report properties

The following table describes the Bandwidth Top N report.

Table 89. Properties of the Bandwidth Top N report

Property	Description
Typical uses	Use this report to identify interfaces with the heaviest bandwidth use, and drill down to see the usage over time.
Prerequisites	None
Data model	BIRT

Bandwidth Utilization report

Displays the bandwidth utilization of a device.

Report properties

The following table describes the Bandwidth Utilization report.

Table 90. Properties of the Bandwidth Utilization report

Property	Description
Typical uses	Use this report to see the bandwidth use of selected devices, and drill down to see the usage over time per interface.
Prerequisites	None
Data model	Cognos

Composite Trending report

Displays a composite chart that contains data for two poll definitions.

Report properties

The following table describes the Composite Trending report.

Table 91. Properties of the Composite Trending report

Property	Description
Typical uses	Use this report to show a list of selected devices and drill down to see the trend of up to six data items.
Prerequisites	None
Data model	BIRT

Device Summarization report

Displays summarization data for devices. This report uses the Tivoli Data Warehouse KNP_POLL_DATA_COLLECTION hourly and daily summarization tables.

Report properties

The following table describes the Device Summarization report.

Table 92. Properties of the Device Summarization report

Property	Description
Typical uses	Use this report to see device level data collected and summarized over a longer period of time.
Prerequisites	You must have Tivoli Data Warehouse installed and configured for with Network Manager to use this report.
Data model	BIRT

Generic Top or Bottom N report

Displays the top or bottom N devices with drilldown to a chart according to device or interface.

Report properties

The following table describes the Generic Top or Bottom N report.

Table 93. Properties of the Generic Top or Bottom N report

Property	Description
Typical uses	Use this report to identify the best or worst performers, by average value, for any collected SNMP metric, and drill down to see the trend over time.
Prerequisites	None
Data model	BIRT

Generic Trend Analysis report

Displays the device summary with drilldown to a chart according to device or interface.

Report properties

The following table describes the Generic Trend Analysis report.

Table 94. Properties of the Generic Trend Analysis report

Property	Description
Typical uses	Use this report to see the average values collected for of a list of selected devices and drilldown to see the trend over time for that data item.
Prerequisites	None
Data model	Cognos

Generic Quick View report

Displays the device list with drilldown to a chart according to device or interface.

Report properties

The following table describes the Generic Quick View report.

Table 95. Properties of the Generic Quick View report

Property	Description
Typical uses	Use this report to quickly list a set of selected devices to be used as an index to drill down to see a trend graph over time.
Prerequisites	None
Data model	BIRT

Interfaces Summarization report

Displays summarization data for interfaces. This report uses the Tivoli Data Warehouse KNP_POLL_DATA_COLLECTION hourly and daily summarization tables.

Report properties

The following table describes the Interfaces Summarization report.

Table 96. Properties of the Interfaces Summarization report

Property	Description
Typical uses	Use this report to see interface level data collected and summarized over a longer period of time.
Prerequisites	You must have Tivoli Data Warehouse installed and configured for with Network Manager to use this report.
Data model	BIRT

System Availability Summary report

Displays availability summary for devices with drilldown to a chart according to device. This report is based on the sysUptime data.

Report properties

The following table describes the System Availability Summary report.

Table 97. Properties of the System Availability Summary report

Property	Description
Typical uses	Use this report to see availability statistics as defined by collected sysUptime data.
Prerequisites	None
Data model	BIRT

Summary reports

Summary reports allow you to view historical performance data that has been collected by the monitoring system in a dashboard style presentation.

The Summary reports have automatic refresh, which makes these reports ideal as a dashboard.

To access the Summary reports, click **Reporting** > **Common Reporting** > **Network Manager**. The click **Summary Reports**.

Note: The amount of historical data available for the Summary reports to display is set low by default to preserve report performance. You can increase the storage limit for historical performance data; however, this can lead to degradation in the performance of the Summary reports.

Device Availability Summary report

Displays information on the availability history of the selected devices.

Report properties

The following table describes the Device Availability Summary report.

Table 98. Properties of the Device Availability Summary report

Property	Description
Typical uses	Use this report to verify device availability using their SysUpTime and response time. Drill down to identify patterns of behavior for packet response times and packet loss.
Prerequisites	The chassis ping and sysUpTime poll policies must be enabled, with the Store Poll Data option enabled.
Data model	BIRT

Device Egress Traffic Health Summary report

Displays indicators for network output from a device such as snmpOutBandwidth, ifOutDiscards, ifOutErrors.

Report properties

The following table describes the Device Egress Traffic Health Summary report.

Table 99. Properties of the Device Egress Traffic Health Summary report

Property	Description
Typical uses	Use this report to see general health trends for outgoing traffic on interfaces using data from ifoutErrors, ifOutDiscards, and bandwidth.
Prerequisites	None
Data model	BIRT

Device Ingress Traffic Health Summary report

Displays indicators for network input to a device such as snmpInBandwidth, ifInDiscards, and ifInErrors.

Report properties

The following table describes the Device Ingress Traffic Health Summary report.

Table 100. Properties of the Device Ingress Traffic Health Summary report

Property	Description
Typical uses	Use this report to see general health trends for incoming traffic on interfaces using data from ifInErrors, ifInDiscards, and bandwidth.
Prerequisites	None

Table 100. Properties of the Device Ingress Traffic Health Summary report (continued)

Property	Description
Data model	BIRT

Router Health Summary report

Displays summary and performance information for a specified router.

Report properties

The following table describes the Router Health Summary report.

Table 101. Properties of the Router Health Summary report

Property	Description
Typical uses	The Router Health Summary report can be used to monitor recent changes in a key router. It can also be used to monitor a bottleneck in the network.
Prerequisites	To use this report, you must enable the ciscoMemoryPctUsage, cpuBusyPoll, and Default Chassis polls with the Store Poll Data option enabled.
Data model	BIRT

Troubleshooting reports

Troubleshooting reports help you identify problems while optimizing the discovery of the network as well as help identify possible problems discovered in the network such as duplex mismatches.

To access the Troubleshooting reports, click **Reporting** > **Common Reporting** > **Network Manager**. Then click **Troubleshooting Reports**.

Connected Interface Duplex Mismatch report

Displays a list of connections where one end of the connection is half-duplex and the other end is full-duplex.

Report properties

The following table describes the Connected Interface Duplex Mismatch report.

Table 102. Properties of the Connected Interface Duplex Mismatch report

Property	Description
Typical uses	Diagnosing performance or availability issues. **Tip:** The duplex value for the interfaces are learned at discovery time from the dot3StatsDuplexStatus value in the EtherLike-MIB.mib. This MIB defines the values for dot3StatsDuplexStatus as: unknown(1); halfDuplex(2); and fullDuplex(3). A value of unknown means that Network Manager cannot determine the duplex status based on the available MIB information.
Prerequisites	None
Data model	BIRT

Devices Pending Delete on Next Discovery report

Displays information on devices to be deleted from the topology if they are not found during the next discovery cycle.

Report properties

The following table describes the Devices Pending Delete on Next Discovery report.

Table 103. Properties of the Devices Pending Delete on Next Discovery report

Property	Description
Typical uses	If device has been removed from the network, it will remain in the topology for x more discoveries, where x is the value of the LingerTime variable for the device in the topology database. This report can show devices that you do not expect to be deleted from the topology, and you can investigate why they were not discovered.
Prerequisites	None
Data model	BIRT

Devices With No Connections report

Displays information on devices on which no connections terminate or originate.

Report properties

The following table describes the Devices With No Connections report.

Table 104. Properties of the Devices With No Connections report

Property	Description
Typical uses	This report shows devices for which connectivity was not discovered properly. You can then investigate why connectivity was not discovered properly for these devices. For example, the correct agents might not have been run.
Prerequisites	None
Data model	BIRT

Devices with no SNMP Access report

Displays those devices to which the discovery could not get SNMP access.

Report properties

The following table describes the Devices with no SNMP Access report.

Table 105. Properties of the Devices with no SNMP Access report

Property	Description
Typical uses	Troubleshooting devices for which no connectivity information was discovered. There might be a number of reasons why the discovery agents could not get SNMP access to these devices, for example, incorrect SNMP community strings.
Prerequisites	None
Data model	Cognos

Devices with Unclassified SNMP Object IDs report

Displays those devices with SNMP Object IDs (OIDs) that have not been assigned to specific classes.

Report properties

The following table describes the Devices with Unclassified SNMP Object IDs report.

Table 106. Properties of the Devices with Unclassified SNMP Object IDs report

Property	Description
Typical uses	This report shows devices that could not be classified properly by analyzing the ncim.mappings table to check whether the sysObjectId is recognized. You can then investigate whether the Active Object Classes (AOCs) need to be modified to be able to classify devices with these OIDs. For example, the correct agents might not have been run.
Prerequisites	None
Data model	BIRT

Devices with Unknown SNMP Object IDs report

Displays those devices with unknown SNMP Object IDs (OIDs).

Report properties

The following table describes the Devices with Unknown SNMP Object IDs report.

Table 107. Properties of the Devices with Unknown SNMP Object IDs report

Property	Description
Typical uses	Use this report to identify devices with sysObjectId that were not recognized. For example, Network Manager might recognize the sysObjectID as belonging to a specific vendor, but not the specific model. Such devices are collected in the class NetworkDevice. Update both the AOC files and the ncim.mappings table in order to correctly classify the device.
Prerequisites	None
Data model	BIRT

Incompletely Configured Devices report

Displays all devices with no system contact or location, and all interfaces with no ifAlias, grouped by Vendor and main node.

Report properties

The following table describes the Incompletely Configured Devices report.

Table 108. Properties of the Incompletely Configured Devices report

Property	Description
Typical uses	Use this report to identify custom context information, such as Contact, Location, and ifAlias learned from the device. This information can be archived, or used to check compliance for management purposes.
Prerequisites	None

Table 108. Properties of the Incompletely Configured Devices report (continued)

Property	Description
Data model	BIRT

Interface Status Distribution report

Displays a scatter chart that indicates the distribution of operational and non-operational interfaces and the number of devices with each type of interface.

Report properties

The following table describes the Interface Status Distribution report.

Table 109. Properties of the Interface Status Distribution report

Property	Description
Typical uses	Use this report to understand how many devices have broken or spare interfaces, or how many devices have large numbers of operational interfaces.
Prerequisites	None
Data model	BIRT

Network Device Configuration Errors report

Displays devices with duplex mismatches, BGP sessions down, route target import/export mismatches.

Report properties

The following table describes the Network Device Configuration Errors report.

Table 110. Properties of the Network Device Configuration Errors report

Property	Description
Typical uses	Use this report to find devices that need to be reconfigured.
Prerequisites	None
Data model	BIRT

Utility reports

Utility reports display all discovered devices and their interfaces in different views.

To access the Utility reports, click **Reporting** > **Common Reporting** > **Network Manager**. Then click **Utility Reports**.

Discovered Nodes and Interfaces Flat File List report

Displays all discovered devices and interfaces.

Report properties

The following table describes the Discovered Nodes and Interfaces Flat File List report.

Table 111. Properties of the Discovered Nodes and Interfaces Flat File List report

Property	Description
Typical uses	Use this report to archive discovered devices and interfaces, or to export to a third party tool such as a spreadsheet or database.
Prerequisites	None
Data model	BIRT

Tier Summary by Device Type report

Displays all devices according to what license tier they belong to.

Report properties

The following table describes the Tier Summary by Device Type report.

Table 112. Properties of the Tier Summary by Device Type report

Property	Description
Typical uses	Use this report to identify devices in terms the type of ports. This report should not be used to verify IBM license compliance requirements.
Prerequisites	None
Data model	BIRT

Context reports

Context reports show information related to the selected device.

To access context reports, right-click a device in the topology view and select **Reports** > *Report name*.

Bandwidth In Utilization report

Displays the SNMP in bandwidth utilization of a device.

Report properties

This is the Bandwidth Utilization report using snmpInBandwidth poll policy. The following table describes the Bandwidth In Utilization report.

Table 113. Properties of the Bandwidth In Utilization report

Property	Description
Typical uses	Use this report to see the bandwidth in use of selected.

Table 113. Properties of the Bandwidth In Utilization report (continued)

Property	Description
Prerequisites	To use this report, you must enable the snmpInBandwidth poll policy with the Store Poll Data option enabled.
Data model	Cognos

IfInDiscards report

Displays the ifInDiscards of the device.

Report properties

This is the Cognos Generic Trend Analysis report using ifInDiscards poll policy. The following table describes the IfInDiscards report.

Table 114. Properties of the IfInDiscards report

Property	Description
Typical uses	Use this report to see the trend of the discarded packets of an interface on a device.
Prerequisites	To use this report, you must enable the ifInDiscards poll policy with the Store Poll Data option enabled.
Data model	Cognos

Memory usage report

Displays the memory usage of a device.

Report properties

This is the Cognos Generic Trend Analysis report using ciscoMemoryPool poll policy. The following table describes the Memory usage report.

Table 115. Properties of the Memory usage report

Property	Description
Typical uses	Use this report to see the trend of the memory usage of a device.
Prerequisites	To use this report, you must enable the ciscoMemoryPool poll policy with the Store Poll Data option enabled.
Data model	Cognos

CPU Usage report

Displays the CPU usage of the device.

Report properties

This is the Cognos Generic Trend Analysis report using cpuBusyPoll poll policy. The following table describes the CPU Usage report.

Table 116. Properties of the CPU Usage report

Property	Description
Typical uses	Use this report to see a history of the CPU usage of a device.
Prerequisites	To use this report, you must enable the cpuBusyPoll poll policy with the Store Poll Data option enabled.
Data model	Cognos

Router Health Summary report

Displays summary and performance information for a specified router.

Report properties

The following table describes the Router Health Summary report.

Table 117. Properties of the Router Health Summary report

Property	Description
Typical uses	The Router Health Summary report can be used to monitor recent changes in a key router. It can also be used to monitor a bottleneck in the network.
Prerequisites	To use this report, you must enable the ciscoMemoryPctUsage, cpuBusyPoll, and Default Chassis polls with the Store Poll Data option enabled.
Data model	BIRT

Monitoring Policies Report

Also known as the Monitoring Policies report, if it is launched as a right-click report. Displays all the enabled policies and for each policy all the devices and interfaces that match the scope.

Report properties

The following table describes the Monitoring Summary report.

Table 118. Properties of the Monitoring Summary report

Property	Description
Typical uses	You can run this report to archive the monitoring configuration for your network, or use it for reference purposes offline.
Prerequisites	None

Table 118. Properties of the Monitoring Summary report (continued)

Property	Description
Data model	BIRT

Appendix D. Entity types

The entityType table contains all the entity types that are available in the NCIM topology database.

The following table lists the entity types available in the topology database.

Table 119. Summary of the information in the entityType table

Value (entityType)	Entity type name (typeName)	Category (metaClass)
0	Unknown	Element
1	Chassis	Element
2	Interface	Element
3	Logical Interface	Element
4	Local VLAN	Element
5	Module	Element
6	PSU	Element
7	Logical Collection	Collection
8	Daughter Card	Element
9	Fan	Element
10	Backplane	Element
11	Slot	Element
12	Sensor	Element
13	Virtual Router	Element
15	Subnet	Collection
16	Global VLAN	Collection
17	VPN	Collection
18	HSRP Group	Collection
19	Stack	Element
20	VRF	Element
21	OSPF Routing Domain	Collection
22	OSPF Service	Service
23	OSPF Area	Collection
24	VTP Domain	Collection
25	Other	Element
26	BGP Service	Service
27	BGP AS (Autonomous System)	Collection
28	BGP Route	Attribute
29	BGP Cluster	Collection
30	BGP Network	Collection
31	ISIS Service	Service

Table 119. Summary of the information in the entityType table (continued)

Value (entityType)	Entity type name (typeName)	Category (metaClass)
32	ISIS Level	Collection
33	OSPF Pseudo-Node	Element
34	ITNM Service	Collection
35	MPLS TE Service	Service
36	MPLS TE Tunnel	Element
37	MPLS TE Resource	Element
38	MPLS LSP	Element
40	IP Connection	Element
41	PIM Service	Service
42	PIM Network	Collection
43	IPMRoute Service	Service
44	IPMRoute Upstream	Element
45	IPMRoute Downstream	Element
46	IPMRoute MDT	Collection
47	IPMRoute Source	Element
48	IPMRoute Group	Element
49	IP Path	Collection
50	IP Endpoint	Protocol Endpoint
51	VLAN Trunk Endpoint	Protocol Endpoint
52	Frame Relay Endpoint	Protocol Endpoint
53	OSPF Endpoint	Protocol Endpoint
54	ATM Endpoint	Protocol Endpoint
55	VPWS Endpoint	Protocol Endpoint
56	BGP End Point	Protocol Endpoint
57	ISIS End Point	Protocol Endpoint
58	MPLS Tunnel End Point	Protocol Endpoint
59	TCP/UDP End Point	Protocol Endpoint
60	PIM End Point	Protocol Endpoint
61	IPMRoute End Point	ProtocolEndPoint
62	IGMP End Point	ProtocolEndPoint
70	Topology	Topology
72	Layer 2 Topology	Topology
73	Layer 3 Meshed Topology	Topology
75	MPLS TE Topology	Topology
77	Pseudo Wire Topology	Topology
78	OSPF Topology	Topology
79	BGP Topology	Topology
80	IP Path Topology	Topology
81	PIM Topology	Topology

Table 119. Summary of the information in the entityType table (continued)

Value (entityType)	Entity type name (typeName)	Category (metaClass)
82	Local VLAN Topology	Topology
83	IPMRoute Topology	Topology
84	VPLS Pseudo Wire Topology	Topology
110	Generic Collection	Collection
120	IGMP Service	Service
121	IGMP Groups	Collection
122	VSI (Virtual Switch Instance)	Element

Appendix E. Scripts

Use the supplied Perl, shell, or SQL scripts to perform administration, discovery configuration, product upgrade, or troubleshooting tasks.

Perl scripts

Use the supplied Perl scripts to perform administration, discovery configuration, product upgrade, or troubleshooting tasks.

Running Perl scripts

To run Perl scripts on Windows, use `%NCHOME%\precision\bin\ncp_perl.bat`. To run Perl scripts on UNIX, use `$NCHOME/precision/bin/ncp_perl`.

Note: Some discovery agents are implemented using Perl scripts, and include the following discovery agents. All of these agents are located in `$NCHOME/precision/disco/agents/perlAgents`. For more information on Perl discovery agents, see the *IBM Tivoli Network Manager IP Edition Discovery Guide*.

- AlcatelVRRP.pl
- Entity.pl
- NATTextFileAgent.pl
- ASAgent.pl
- iprouting_inperl.pl
- NortelPassport.pl
- CiscoSwitchInPerl.pl
- IPv6Interface.pl
- OSInfo.pl
- NATGatewayAgent.pl

Administration scripts

Use these scripts to administer domains, manage nodes, query processes, and perform actions on the topology.

AddNode.pl

Use the **AddNode.pl** Perl script to add devices to your network topology.

Description

You might want to add a device to your network topology if you know it has been added since the last discovery.

When you add a device, a partial discovery is triggered to add the device to the network topology. Full topology connectivity is not displayed for the device until after the next full discovery is completed.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/AddNode.pl -domain
NCOMS -latency 10000 -debug 4 -verbose 192.168.10.8
```

UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/AddNode.pl -domain
NCOMS -file mynodes.txt
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\AddNode.pl -domain
NCOMS -file mynodes.txt
```

Command-line options

The following table describes the command-line options for the **AddNode.pl** script.

Table 120. AddNode.pl command-line options

Command-line option	Description
-domain *DomainName*	Mandatory; the name of the domain you want to add the node to.
-latency *MessageLatency*	Optional; the maximum time in milliseconds to wait between attempts to send a message. This is needed for busy networks.
-debug *DebugLevel*	Optional; the level of detail the debugging output provides. Values are 1 to 4, where 4 represents the most detailed output.
-file *FileName*	Optional; file containing the list of nodes to be added to the network topology. Add one IP address or host name per line in the file. **Note:** You must provide the names of the nodes either in a file or by entering them in the command line, as described in *host* below.
-verbose	Optional; provides more information on the screen.
host	Optional; the name of the node to be added. You can add any number of nodes this way, separated by spaces. The information entered for a node can be either the IP address or the host name. If you do not provide a host name, then the -file option must be used.

domain_create.pl

Use the **domain_create.pl** Perl script to migrate discovery configuration and existing poll policies from an existing domain to a newly created domain.

Description

If your deployment requires additional network domains, you must configure process control for the domains and register the domains with the NCIM topology database. Once you have done this, you can then use the **domain_create.pl** Perl script to migrate the configuration and network polls from an existing domain to the new domain. You must use one instance of ncp_ctrl to run and manage each domain. The script does not migrate the topology from the original domain.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts
/perl/scripts/domain_create.pl -domain NCOMS2 -password password
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts
\perl\scripts\domain_create.pl -domain NCOMS2 -password password
```

Command-line options

The following table describes the command-line options for the script.

Table 121. domain_create.pl command-line options

Command-line option	Description
-newdomain *Domain*	Mandatory; the name of the domain you have created, for example NCOMS2. **Restriction:** Only alphanumeric characters and the underscore (_) character may be used for domain names. Any other characters, for example the hyphen (-) are forbidden.
-password *Password*	Mandatory; the password for the domain.
-verbose	Optional; provides more information on the screen.
-help	Optional; provides help on this command

domain_drop.pl

Use the `domain_drop.pl` Perl script to remove a network domain from the NCIM topology database. This removes the entire topology for the domain from NCIM, along with any poll policies for that domain. Note that this script does not remove configuration information for the domain, and the cache of the topology will be unaffected.

Description

This script removes the entire topology for the specified domain from NCIM, along with any poll policies for the domain. Note that this script does not remove configuration information for the domain, and the cache of the topology is unaffected.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts
/perl/scripts/domain_drop.pl -domain obsoletedomain -password
password
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
domain_drop.pl -domain obsoletedomain -password password
```

Command-line options

The following table describes the command-line options for the script.

Table 122. domain_drop.pl command-line options

Command-line option	Description
-domain *Domain*	Mandatory; name of the domain to remove.
-password *Password*	Optional; password of the domain to remove.

itnm_pathTool.pl

Use the itnm_pathTool.pl script to trace a path between a source and destination device. The script determines the interfaces and physical ports used along the path.

Usage

The script displays the path in ASCII format providing the path is not asymmetric or load-balanced. If the path is asymmetric or load-balanced, the path data is displayed in raw format.

Tracing a path

The following example command line traces a path from IPv4 address 172.16.254.1 to IPv4 address 172.16.2.3. `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/webtools/bin/
itnm_pathTool.pl -domain NCOMS -from 172.16.254.1 -to 172.16.2.3
```

Command-line options

The following table describes the command-line options for the script.

Table 123. itnm_pathTool.pl command-line options

Command-line option	Description
-domain *DomainName*	Mandatory. The network domain in which to perform the path trace.
-from	Specifies the source IPv4 address, from which to perform the trace.
-to	Specifies the target IPv4 address, to which to perform the trace.
-delete	Deletes the specified path from the NCIM topology database.
-outofband	You can trace a path between an interface inside your domain and one outside, and this option is referred to as an out-of-band trace. This command-line option forces the use of discovered access IP addresses, if available. **Note:** This reduces ingress accuracy.
-ping	Pings each next-hop address to verify it is reachable from the management platform.
-store	Stores or updates the retrieved path information in the NCIM topology database.

Table 123. itnm_pathTool.pl command-line options (continued)

Command-line option	Description
-return	Instructs the path trace to additionally retrieve the return path, from the target device back to the source device. Specifying -from A -to B -return is the same as specifying -from A -to A -via B. Therefore the command-line options -return and -via cannot be specified together.
-timeout	Override the default 30 second timeout per prerequisite check.
-via	Optional IPv4 address to perform the path trace through. This command-line option cannot be used with the option -return.
-debug *debug*	The level of debugging output (0-4, where 4 represents the most detailed output).
-help	Displays the command line options. Does not start the component even if used in conjunction with other arguments.

ITNMIP_Listener.pl

Use the **ITNMIP_Listener.pl** script to listen to messages being passed between processes on the message bus.

Usage

Many Network Manager processes communicate through a message bus. For example, **ncp_model** broadcasts topology updates on the message bus. Each process broadcasts on a different subject. For example, **ncp_model** broadcasts on the subject MODEL. The **ITNMIP_Listener.pl** script listens to messages on the message bus and prints them to screen.

Listening for topology change notifications

The following example command line listens for topology change notifications on the NCOMS domain. `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
ITNMIP_Listener.pl -domain NCOMS -process Model -messageClass NOTIFY
```

Listening for discovery status updates

The following example listens for updates on discovery status updates on the NCOMS domain on Windows. `Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
ITNMIP_Listener.pl -domain NCOMS -subject
/ITNM/DISCO/UPDATE
```

Listening for Network Manager status events

The following example listens for events regarding the status of the Network Manager product. `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
ITNMIP_Listener.pl -domain NCOMS -process ITNMSTATUS -messageClass NOTIFY
```

Command-line options

The following table describes the command-line options for the script.

Table 124. ITNMIP_Listener.pl command-line options

Command-line option	Description
-debug *debug*	The level of debugging output (0-4, where 4 represents the most detailed output).
-domain *DomainName*	Mandatory. The discovery domain on which to listen.
-help	Displays the command line options. Does not start the component even if used in conjunction with other arguments.
-subject	The specific subject to listen to. If you specify a subject, the -domain argument is ignored, and the script listens on all domains. If you specify a subject you do not need to specify a messageClass and process. All subjects begin \'ITNM/\' and have the domain appended. For example, the **ncp_model** notify subject for domain *TESTDOMAIN* is /ITNM/MODEL/NOTIFY/TESTDOMAIN.
-process	The process to listen to. Valid options are: • Model - ncp_model • Class - ncp_class • Config - ncp_config • Ctrl - ncp_ctrl • Disco - ncp_disco • PingFinder - ncp_f_ping • ITNMSTATUS - status events If you specify a messageClass and process you do not need to specify a subject.
-messageClass	The class of messages to listen for. Not all processes support all classes. Classes are: • NOTIFY • QUERY • STATUS If you specify a messageClass and process you do not need to specify a subject.

ManageNode.pl

Use the **ManageNode.pl** perl script to set the status of one or more unmanaged devices back to managed state following a period of maintenance.

Description

You can set the status of one or more unmanaged devices back to managed state following a period of maintenance.

This is useful when a device is in unmanaged state and you want to set it to managed state again to receive alerts that are not tagged unmanaged and are used for root cause analysis.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/ManageNode.pl
-domain NCOMS -user root -pwd fruit -verbose -file mynodes.txt
```

`UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/ManageNode.pl
-domain NCOMS -user root -pwd fruit -verbose neptune.ibm.com 192.168.0.6
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\ManageNode.pl
-domain NCOMS -user root -pwd fruit -verbose -file mynodes.txt
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\ManageNode.pl
-domain NCOMS -user root -pwd fruit -verbose neptune.ibm.com 192.168.0.6
```

Command-line options

The following table describes the command-line options for the script.

Table 125. ManageNode.pl command-line options

Command-line option	Description
-domain *DomainName*	Mandatory; the name of the domain where the unmanaged node resides.
-user *username*	Mandatory; the name of the database user.
-pwd *password*	Mandatory; the password for the database user.
-file *FileName*	Optional; file containing the list of nodes to be set to managed state. Add one IP address or host name per line in the file. **Note:** You must provide the names of the nodes either in a file or by entering them in the command line, as described in *host* below.
-verbose	Optional; provides more information on the screen.
host	Optional; the name of the node to be set to managed state. You can specify any number of nodes this way, separated by spaces. The information entered for a node can be either the IP address or the host name. If you do not provide a host name, then the -file option must be used.

read_ncp_cfg.pl

Use the **read_ncp_cfg.pl** Perl script to query the Master Domain Controller process, ncp_ctrl, and extract the current service state of the processes that ncp_ctrl has been configured to run.

Description

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/read_ncp_cfg.pl
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\read_ncp_cfg.pl
```

Command-line options

The following table describes the command-line options for the script.

Table 126. read_ncp_cfg.pl command-line options

Command-line option	Description
-domain *DomainName*	Mandatory; the name of the domain where the Master Domain Controller process resides.

RemoveNode.pl

Use the **RemoveNode.pl** perl script to remove specified devices from the network topology. It does this by setting the device to unmanaged state and marking the device to be removed during the next full discovery.

Description

This script sets the specified device to unmanaged state and marks the device to be removed during the next full discovery. This is useful when you have removed a device from the network, and you want to remove it from your network topology as soon as possible, instead of waiting for three full discovery cycles. The script marks the nodes and all associated objects for deletion. The next full discovery removes the nodes and all objects from the databases.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/RemoveNode.pl
-domain NCOMS -user root -pwd fruit -verbose -file mynodes.txt
```

`UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/RemoveNode.pl
-domain NCOMS -user root -pwd fruit -verbose neptune.ibm.com 192.168.0.6
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\RemoveNode.pl
-domain NCOMS -user root -pwd fruit -verbose -file mynodes.txt
```

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\RemoveNode.pl
-domain NCOMS -user root -pwd fruit -verbose neptune.ibm.com 192.168.0.6
```

Command-line options

The following table describes the command-line options for the script.

Table 127. ManageNode.pl command-line options

Command-line option	Description
-domain *DomainName*	Mandatory; the name of the domain where the unmanaged node resides.
-latency *MessageLatency*	Optional; the maximum time in milliseconds to wait between attempts to send a message. This is needed for busy networks.
-debug *DebugLevel*	Optional; the level of detail the debugging output provides. Values are 1 to 4, where 4 represents the most detailed output.
-user *username*	Mandatory; the name of the database user.
-pwd *password*	Mandatory; the password for the database user.
-file *FileName*	Optional; file containing the list of nodes to be removed from the network topology. Add one IP address or host name per line in the file. **Note:** You must provide the names of the nodes either in a file or by entering them in the command line, as described in *host* below.
-verbose	Optional; provides more information on the screen.
-force	Optional; when used, you are not prompted to confirm the removing of a node.
host	Optional; the name of the node to be removed. You can specify any number of nodes in this way, separated by spaces. The information entered for a node can be either the IP address or the host name. If you do not provide a host name, then the -file option must be used.

UnmanageNode.pl

Use the `UnmanageNode.pl` Perl script to set one or more devices to unmanaged state so that engineers can work on these devices without generating network events. Unmanaged devices are not polled by Network Manager. Events for these devices from other sources are tagged in the **Active Event List (AEL)** to indicate they are from an unmanaged device.

Description

If you set a device to unmanaged, polling is suspended for the unmanaged node. In the **Active Event List (AEL)**, all alerts are tagged to indicate they are from an unmanaged device, and are not used for root cause analysis. You can also unmanage individual devices or groups of devices from the topology map views.

There is also an option to set individual components of a device to unmanaged state using the Structure Browser.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/UnmanageNode.pl
-domain NCOMS -user root -pwd fruit -verbose -file mynodes.txt
```

`UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/UnmanageNode.pl
-domain NCOMS -user root -pwd fruit -verbose neptune.ibm.com 192.168.0.6
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\UnmanageNode.pl
-domain NCOMS -user root -pwd fruit -verbose -file mynodes.txt
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\UnmanageNode.pl
-domain NCOMS -user root -pwd fruit -verbose neptune.ibm.com 192.168.0.6
```

Command-line options

The following table describes the command-line options for the script.

Table 128. UnmanageNode.pl command-line options

Command-line option	Description
`-domain` *DomainName*	Mandatory; the name of the domain where the node to be unmanaged resides.
`-user` *username*	Mandatory; the name of the database user.
`-pwd` *password*	Mandatory; the password for the database user.
`-file` *FileName*	Optional; file containing the list of nodes to be unmanaged. Add one IP address or host name per line in the file. **Note:** You must provide the names of the nodes either in a file or by entering them in the command line, as described in *host* below.
`-verbose`	Optional; provides more information on the screen.
host	Optional; the name of the node to be unmanaged. You can specify any number of nodes this way, separated by spaces. The information entered for a node can be either the IP address or the host name. If you do not provide a host name, then the `-file` option must be used.

Discovery scripts

Use these scripts to query and control the discovery.

audit.pl

Use the `audit.pl` script to generate a status report for the Discovery engine, ncp_disco. The output is in html format and reports information about discovery, agents and stitchers. You can set the frequency at which the status report is generated. The default is 500 seconds.

Description

Running the script

To run the script, use a command line similar to the following: **UNIX**

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/audit.pl
-domain NCOMS [ frequency ]
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
audit.pl -domain NCOMS  [ frequency ]
```

Command-line options

The following table describes the command-line options for the script.

Table 129. audit.pl command-line options

Command-line option	Description
-domain *DomainName*	Mandatory; the name of the domain on which the discovery was run.
frequency	Optional; the frequency, in seconds, at which the report generated by the audit script is run. The default is 500 seconds.
-verbose	Optional; provides more information on the screen.
-help	Optional; provides help on this command

BuildSeedList.pl

Use the `BuildSeedList.pl` Perl script to write a list of seeds to a file.

Description

The `BuildSeedList.pl` Perl script retrieves the list of hostnames and IP addresses discovered during the discovery and writes this list to a file. The script also provides the insert that can be used in the file finder to use this list to seed the discovery. The use of a fully populated seed list for discovery speeds up discovery time.

Running the script

To run the script, use a command line similar to the following: **UNIX**

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
BuildSeedList.pl
```

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
BuildSeedList.pl
```

Command-line options

The following table describes the command-line options for the `BuildSeedList.pl` script.

Table 130. BuildSeedList.pl command-line options

Command-line option	Description
`-domain` *DomainName*	Mandatory; the name of the domain for which the discovery is running.
`-verbose`	Optional; provides more information on the screen.
`-help`	Optional; provides help on this command

discoAgentsUsed.pl

Use the `discoAgentsUsed.pl` script to determine which discovery agents were used to discover the most recently discovered devices in the current domain. Results are presented in an HTML file for viewing using a Web browser.

Description

Note: The Discovery engine, ncp_disco, must be running when you run this script.

Running the script

To run the script, use a command line similar to the following: **UNIX**

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
discoAgentsUsed.pl -domain NCOMS [reportFileName]
```

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
discoAgentsUsed.pl -domain NCOMS [reportFileName]
```

Command-line options

The following table describes the command-line options for the script.

Table 131. discoAgentsUsed.pl command-line options

Command-line option	Description
`-domain` *DomainName*	Mandatory; the name of the domain where the discovery is running.
reportFileName	Optional; the name of the HTML file to contain the list of discovery agents used to discover the most recently discovered devices in the specified domain. If no name is supplied for the report file, the default name of agentList.html is used.
`-verbose`	Optional; provides more information on the screen.
`-help`	Optional; provides help on this command

disco_profiling_data.pl

Use the `disco_profiling_data.pl` script to output summary data of all the discoveries run on a domain or extracted from a given profiling cache. This script includes data on how long it took to transfer discovery profiling data to the NCIM topology database.

Description

The script is run using the following command line. Optional arguments are shown enclosed in square brackets. UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
disco_profiling_data.pl -domain domain_name  [ -fromcache ]
[ -discocachefile discovery_cache_filename ] [ -
modelcachefile model_cache_filename ]
[ -debug debug_level ] [ -help ]
```

 Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
disco_profiling_data.pl -domain domain_name  [ -fromcache ]
[ -discocachefile discovery_cache_filename ] [ -
modelcachefile model_cache_filename ]
[ -debug debug_level ] [ -help ]
```

The script reads data from the Topology manager database table, model.profilingData. For more information on this table see the *IBM Tivoli Network Manager IP Edition Discovery Guide*.

Running the script

To retrieve data from a specified domain, use a command line similar to the following: UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
disco_profiling_data.pl -domain NCOMS
```

 Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
disco_profiling_data.pl -domain NCOMS
```

To retrieve data from cache files, use a command line similar to the following:
 UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
disco_profiling_data.pl -domain NCOMS -fromcache
```

 Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
disco_profiling_data.pl -domain NCOMS -fromcache
```

To retrieve data from discovery and model caches, use a command line similar to the following: UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
disco_profiling_data.pl -domain NCOMS
discocachefile Disco.Cache.disco.profilingData.NCOMS
-modelcachefile Model.Cache.model.profilingData.NCOMS
```

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
disco_profiling_data.pl -domain NCOMS
discocachefile Disco.Cache.disco.profilingData.NCOMS
-modelcachefile Model.Cache.model.profilingData.NCOMS
```

Command-line options

The following table describes the command-line options for the script.

Table 132. disco_profiling_data.pl command-line options

Command-line option	Description
-domain *DomainName*	Mandatory; the name of the domain to retrieve data from.
-fromcache	Optional; instructs the script to retrieve data from the cache files. IN this case the Discovery engine, ncp_disco, and the Topology manager, ncp_model, do not need to be running.
-discocachefile *discovery_cache_filename*	Optional; name of a discovery cache file to extract disco profiling data from. This setting overrides the -fromcache setting.
-modelcachefile *model_cache_filename*	Optional; name of a model cache file to extract model profiling data from. This setting overrides -fromcache setting.
-debug *debug_level*	Optional; specifies required debug level.
-help	Optional; provides help on this command

Output

Running the script retrieves output similar to the following:

```
--------------------------------------------------------------------------------
Domain          Date_of_discovery     collection  processing  transfer    total
--------------------------------------------------------------------------------

NCOMS           2012-08-24T23:00:00   00:33:26    00:18:02    00:00:00    00:00:00
NCOMS           2012-09-30T23:00:04   00:30:36    00:16:04    00:11:04    00:57:44
NCOMS           2012-09-31T23:00:07   00:28:53    00:16:36    00:10:59    00:56:28
--------------------------------------------------------------------------------


---------------------------------------------------------------
entities  devices  access  interfaces  discoMem  modelMem
---------------------------------------------------------------

194328    352      347     93620       729.58    0.00
194925    352      348     93948       729.01    726.38
194997    352      348     93996       725.57    728.89
---------------------------------------------------------------
```

Table 133. Output columns

Column	Description
Domain	Domain name.
Date_of_discovery	Start date and time of the discovery.
collection	Length of time spent collecting data. This is the sum of time spend in discovery phases 1-3.

Table 133. Output columns (continued)

Column	Description
processing	Length of time spent in the final processing phase of discovery.
transfer	Length of time taken for the Topology manager, ncp_model, to update NCIM following the discovery.
total	Total time taken for the discovery. This is the sum of collection, processing and transfer.
entities	Total number of entities discovered as reported by the Discovery engine, ncp_disco.
devices	Number of devices discovered as reported by the Discovery engine, ncp_disco.
access	Number of entities to which ncp_disco reported SNMP access interfaces.
interfaces	Number of interfaces discovered as reported by the Discovery engine, ncp_disco.
discoMem	Memory usage of the the ncp_disco process in MB.
modelMem	Memory usage of the ncp_model process in MB.

itnm_disco.pl

Use the **itnm_disco.pl** script to start and stop network discoveries, and display status of a running discovery.

Display the current status of network discovery

To run the script to display the current status of network discovery, use a command line similar to the following. UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/itnm_disco.pl
-domain NCOMS -status -delay 5
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\itnm_disco.pl
-domain NCOMS -status -delay 5
```

Start a network discovery

To run the script to start a network discovery, use a command line similar to the following. UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/itnm_disco.pl
-domain NCOMS -start
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\itnm_disco.pl
-domain NCOMS -start
```

Note: If the **ncp_disco** process is running, then running the **itnm_disco.pl** script with the *-start* option starts a discovery. If the **ncp_disco** process is not running, then running the **itnm_disco.pl** script with the *-start* option only starts the **ncp_disco** process, and does not start a discovery.

Stop a network discovery

To run the script to stop a network discovery, use a command line similar to the following. `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/itnm_disco.pl
-domain NCOMS -stop
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\itnm_disco.pl
-domain NCOMS -stop
```

Command-line options

The following table describes the command-line options for the script.

Table 134. itnm_disco.pl command-line options

Command-line option	Description
-domain *DomainName*	Mandatory; the name of the domain where you want to start, stop, or display status of a discovery.
-status	Optional; instructs the scripts to display status of a discovery.
-start	Optional; instructs the scripts to start a discovery.
-stop	Optional; instructs the scripts to stop a discovery.
-delay	Optional; count in seconds to delay
-v	Optional; provides more information on the screen.

listEntities.pl

Use the `listEntities.pl` script to retrieve device information from the master.EntityByName OQL database table and output the information in HTML format.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
listEntities.pl -domain NCOMS [ level_of_detail ]
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
listEntities.pl -domain NCOMS [ level_of_detail ]
```

Command-line options

The following table describes the command-line options for the script.

Table 135. listEntities.pl command-line options

Command-line option	Description
-domain *DomainName*	Mandatory; the name of the domain where the discovery was run.
level_of_detail	Optional; a numerical value that indicates the level of detail to capture in the HTML file: • 0: Show just the types of device on the network • 1: Show each main node (each individual device) • 2: Show every entity from the master.entityByName table including interfaces

restart_disco_process.pl

Use the `restart_disco_process.pl` script to stop the currently running discovery process and start a new instance. The running discovery process must have been started by ncp_ctrl for the script to take effect.

Description

The script stops the current discovery process by removing its entry from ncp_ctrl's services.inTray table. The script then inserts the entry into services.inTray again using the original argument list, triggering the process to restart. The `-startDiscovery` optional argument determines whether or not the script should wait for the discovery process to start and then initiate a new full discovery.

Running the script

The script is usually called from the RestartDiscoProcess discovery stitcher. However, you can run the script directly using the command line, for example:

UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
restart_disco_process.pl -domain NCOMS -startDiscovery 1
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
restart_disco_process.pl -domain NCOMS -startDiscovery 1
```

Command-line options

The following table describes the command-line options for the script.

Table 136. restart_disco_process.pl command-line options

Command-line option	Description
-domain *DomainName*	Mandatory, the name of the domain on which to restart the discovery process.

Table 136. restart_disco_process.pl command-line options (continued)

Command-line option	Description
`-debug 0-4`	Sets the debug level, where 0 is no logging and 4 is trace level logging.
`-help`	Displays command-line options help.
`-latency` *latency in seconds*	Time to wait for processing data in seconds.
`-startDiscovery 1│0`	Optional. If set to 1, then the script triggers a new full discovery after the new discovery process is running.

scheduleDiscovery.pl

Use the `scheduleDiscovery.pl` script to display when the next full discovery is scheduled. You can also use this script to schedule full discoveries.

Display the current discovery schedule

To display the current discovery schedule, use a command line similar to the following: **UNIX**

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/
scheduleDiscovery.pl -domain NCOMS -display -v
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\
scheduleDiscovery.pl -domain NCOMS -display -v
```

Set a daily time for discovery

To set a daily time for discovery, use a command line similar to the following:
UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/
scheduleDiscovery.pl -domain NCOMS -time 24_hour_time -v
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\
scheduleDiscovery.pl -domain NCOMS -time 24_hour_time -v
```

Set a weekly schedule for discovery

To set a weekly schedule for discovery, use a command line similar to the following: **UNIX**

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/
scheduleDiscovery.pl -domain NCOMS -day 0..6 -time 24_hour_time -v
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\
scheduleDiscovery.pl -domain NCOMS -day 0..6 -time 24_hour_time -v
```

Set a monthly schedule for discovery

To set a monthly schedule for discovery, use a command line similar to the following: **UNIX**

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/
scheduleDiscovery.pl -domain NCOMS -date 0..31 -time 24_hour_time -v
```

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\
scheduleDiscovery.pl -domain NCOMS -date 0..31 -time 24_hour_time -v
```

Set the discovery schedule to occur at a specified interval

To set the discovery schedule to occur at a specified interval, use a command line similar to the following: UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/bin/
scheduleDiscovery.pl -domain NCOMS -interval number_of_hours_between_discovery -v
```

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\bin\
scheduleDiscovery.pl -domain NCOMS -interval number_of_hours_between_discovery -v
```

Command-line options

The following table describes the command-line options for the script.

Table 137. scheduleDiscovery.pl command-line options

Command-line option	Description
-domain *DomainName*	Mandatory; the name of the domain on which to schedule the discovery or query the discovery schedule.
-time *24_hour_time*	Optional; the time, in 24-hour clock format, at which to run to run discovery.
-day *day(s) of the week*	Optional; one or more days in a week to run discovery, where 0 is Sunday and 6 is Saturday.
-date *date(s) in the month*	Optional; one or more dates in the month when discovery must be run. If the date value is greater than 28, discovery might not execute in certain months.
-interval *number_of_hours_between_discovery*	Optional; number of hours between discovery.
-v	Turn on Verbose mode.

Polling scripts

Use these scripts to control and diagnose network polling,

get_policies.pl

Use the `get_policies.pl` Perl script to move poll policies and associated data between domains. This script can also be used to back up all poll policies to file or to load poll policies from a file into a specified domain. You can also move a subset of poll policies.

Description

Running the script

To run the script to copy policies from one domain to another, use a command line similar to the following: UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
get_policies.pl -from domain=SOURCE -to domain=DESTINATION -
ncim_password NCIM_password
 -ncmonitor_password NCMONITOR_password
```

 Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
get_policies.pl -from domain=SOURCE -to domain=DESTINATION -
ncim_password NCIM_password
 -ncmonitor_password NCMONITOR_password
```

To run the script to copy policies from one domain to a file, use a command line similar to the following: UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
get_policies.pl -from domain=SOURCE -to file=exportedData.xml
```

 Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
get_policies.pl -from domain=SOURCE -to file=exportedData.xml
```

Command-line options

To view all the available command line options, use the command line help to display a list. Type `get_policies.pl -help`.

itnm_poller.pl

Use this script to enable, disable, or check the status of poll policies. This script also shows the polling status of a given entity.

Description

Use the itnm_poller.pl script to perform any of the following activities:
- Enabling one or more poll policies.
- Disabling one or more poll policies.
- Triggering the refresh of a policy configuration and its entity list.
- Displaying the status of poll policies.
- Displaying polling status of given IP address, or of all IP addresses being monitored.

For more information on the NCMONITOR polling status tables, including the ncmonitor.expectedIps table, see the *IBM Tivoli Network Manager IP Edition Management Database Reference*.

For more information on the procedure to ensure that the important IP addresses in your network are being polled as expected by Network Manager, see the *IBM Tivoli Network Manager IP Edition Event Management Guide.*

Enabling one or more poll policies

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
itnm_poller.pl -domain NCOMS -enable 10
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
itnm_poller.pl -domain NCOMS -enable 10
```

Disabling one or more poll policies

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
itnm_poller.pl -domain NCOMS -disable 10
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
itnm_poller.pl -domain NCOMS -disable 10
```

Triggering the refresh of a policy configuration and its entity list

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
itnm_poller.pl -domain NCOMS -refresh 10
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
itnm_poller.pl -domain NCOMS -refresh 10
```

Displaying the status of all poll policies

To run the script, use a command line similar to the following. This also provides the poll policy ID for each poll policy listed and this is useful if you need to subsequently use the itnm_poller.pl script to perform another action on a specific poll policy; for example, enabling or refreshing a policy. `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
itnm_poller.pl -domain NCOMS -status all
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
itnm_poller.pl -domain NCOMS -status all
```

Displaying polling status of a chassis ping poller with specified IP address

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
itnm_poller.pl -domain NCOMS -chassis 10.101.10.10
```

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
itnm_poller.pl -domain NCOMS -chassis 10.101.10.10
```

Command-line options

The following table describes the command-line options for the script.

Table 138. itnm_poller.pl command-line options

Command-line option	Description
-domain *DOMAIN_NAME*	Mandatory; the domain that contains the poll policies of interest.
-enable *POLICY_ID*	Optional; enables the poll policy with the specified ID. Run the itnm_poller.pl script with the -status option first in order to retrieve the desired poll policy ID.
-disable *POLICY_ID*	Optional; disables the poll policy with the specified ID. Run the itnm_poller.pl script with the -status option first in order to retrieve the desired poll policy ID.
-status *POLICY_SET*	Optional; displays the status of the specified policies. The parameter *POLICY_SET* can take one of the following values: • all • static • realtime If no value is specified for *POLICY_SET*, then the value defaults to static. The output of the script when run with the -status option also lists the ID of each poll policy.
-refresh *POLICY_ID* | all	Optional; refreshes the policy configuration and its entity list for a single policy or all active policies. Run the itnm_poller.pl script with the -status option first in order to retrieve the desired poll policy ID.
-chassis *CHASSIS_IP*	Optional; displays the polling status of a chassis ping poller with specified IP address.
-interface *INTERFACE_IP*	Optional; displays the polling status of an interface ping poller with specified IP address.
-help	Optional; provides help on this command

ncp_ping_poller_snapshot.pl

The ncp_ping_poller_snapshot.pl script takes a snapshot of the current ping polling status within a specified network domain. The retrieved data is stored and can be used to generate reports on the polling status using the ncp_polling_exceptions.pl script.

Description

Use the ncp_ping_poller_snapshot.pl script to ensure that important IP addresses in your network are being polled as expected by Network Manager and, if not, to provide information to resolve the problem.

For more information on ensuring that the important IP addresses in your network are being polled as expected by Network Manager, see the *IBM Tivoli Network Manager IP Edition Event Management Guide*.

Prerequisites for this script are as follows:

- The pollLog and pollLogSummary tables must have been created in the NCMONITOR schema.
- The DbLogins file must be usable for the given domain.
- The domain must exist in the NCIM topology database.
- The Polling engine, **ncp_poller**, must be running in the given domain.
- There must be at least one active ping poll in the current domain.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
ncp_ping_poller_snapshot.pl -domain DOMAIN_NAME -password PASSWORD
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
ncp_ping_poller_snapshot.pl -domain DOMAIN_NAME -password PASSWORD
```

Command-line options

The following table describes the command-line options for the script.

Table 139. ncp_ping_poller_snapshot.pl command-line options

Command-line option	Description
-domain *DOMAIN_NAME*	Mandatory; the name of the relevant domain.
-password *PASSWORD*	Optional; the database password used to access the NCIM and NCMONITOR schemas. This is required only if the password is encrypted in the DbLogins configuration file.
-logdir*LOGFILENAME*	Optional; a log file called ncp_ping_poller_snapshot.pl.*DOMAIN_NAME*.log is generated that can be checked if there are any problems accessing the database. It is generated in the current directory by default if this option is not given.
-help	Optional; provides help on this command

ncp_polling_exceptions.pl

Use this script to print a report of the status of entities currently being polled or not being polled by the Network Manager Polling engine, ncp_poller.

Description

Use the ncp_polling_exceptions.pl script as part of the procedure to ensure that the important IP addresses in your network are being polled as expected by Network Manager and, if not, to provide information to resolve the problem.

For more information on the procedure to ensure that the important IP addresses in your network are being polled as expected by Network Manager, see the *IBM Tivoli Network Manager IP Edition Event Management Guide*.

Running the script

To run the script, use a command line similar to the following: UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
ncp_polling_exceptions.pl -domain DOMAIN_NAME -format LIST | REPORT
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
ncp_polling_exceptions.pl -domain DOMAIN_NAME -format LIST | REPORT
```

Command-line options

The following table describes the command-line options for the script.

Table 140. ncp_polling_exceptions.pl command-line options

Command-line option	Description
-domain *DOMAIN_NAME*	Mandatory; the name of the relevant domain.
-notpolled	Optional; outputs a list of IP addresses that are not polled as compared with the list of expected IP addresses. This output is in LIST format only.
-format LIST | REPORT	Optional; determines the output format. This can be report format or a list of IP addresses.
-help	Optional; provides help on this command

ncp_upload_expected_ips.pl

The ncp_upload_expected_ips.pl script parses a plain text file of IP addresses, and loads these addresses to the ncmonitor.expectedIps table. Any data already in the table is removed. The list should contain IP addresses of interest within the given domain, and will allow the ping polling of these addresses to be monitored.

Description

Use the ncp_upload_expected_ips.pl script as part of the procedure to ensure that the important IP addresses in your network are being polled as expected by Network Manager and, if not, to provide information to resolve the problem.

Any existing IP addresses for the current domain will be removed from the ncmonitor.expectedIps table by this script before uploading the new file contents.

For more information on the NCMONITOR polling status tables, including the ncmonitor.expectedIps table, see the *IBM Tivoli Network Manager IP Edition Management Database Reference*.

For more information on the procedure to ensure that the important IP addresses in your network are being polled as expected by Network Manager, see the *IBM Tivoli Network Manager IP Edition Event Management Guide*.

Prerequisites for this script are as follows:
- expectedIps table must have been created in the NCMONITOR schema.
- The DbLogins file must be usable for the given domain.
- The domain must exist in the NCIM topology database.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
ncp_upload_expected_ips.pl -domain DOMAIN_NAME -file FILENAME -password PASSWORD
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
ncp_upload_expected_ips.pl -domain DOMAIN_NAME -file FILENAME -password PASSWORD
 -logdir LOGFILENAME
```

Command-line options

The following table describes the command-line options for the script.

Table 141. ncp_upload_expected_ips.pl command-line options

Command-line option	Description
-domain *DOMAIN_NAME*	Mandatory; the domain that contains the IP addresses for which you want to check polling status.
-file *FILENAME*	Mandatory; a plain text file of IP addresses, separated by whitespace (for example, one IP address per line). The script accepts IPv4 addresses only. The file is expected to contain just IP addresses in standard dot notation.
-password *PASSWORD*	Optional; the database password used to access the NCIM and NCMONITOR schemas. This is required only if the password is encrypted in the DbLogins configuration file.
-logdir*LOGFILENAME*	Optional; a log file called ncp_upload_expected_ips.*DOMAIN_NAME*.log is generated that can be checked if there are any problems accessing the database. It is generated in the current directory by default if this option is not given.
-help	Optional; provides help on this command

Example scripts

Use the example OQL and SNMP scripts as a starting point for creating your own scripts.

oql_example.pl

This script provides examples of Perl-scripted queries into the OQL databases. Use these examples as a starting point when writing your own script that uses the OQL extensions provided by ncp_perl.

Running the script

To run the script, use a command line similar to the following: **UNIX**

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
oql_example.pl
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
oql_example.pl
```

Command-line options

There are no command-line options for this script.

snmp_example.pl

This script provides examples of Perl-scripted SNMP queries into a specified device. Use this example script as a starting point when writing your own script that uses the SNMP extensions provided by ncp_perl.

Running the script

To run the script, use a command line similar to the following: **UNIX**

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
snmp_example.pl -node <Device>
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
snmp_example.pl -node <Device>
```

Command-line options

The following table describes the command-line options for the script.

Table 142. snmp_example.pl command-line options

Command-line option	Description
-node *Device*	Mandatory; IP address or hostname for which the SNMP query.

Troubleshooting scripts

Use these scripts to perform troubleshooting tasks.

GetDiscoCache.pl

To generate discovery cache files for a recent discovery as if it had been run in failover mode, use the GetDiscoCache.pl Perl script. Failover cache files help IBM Support and Development teams to troubleshoot discovery.

Running the script

After a discovery has finished, you can run the GetDiscoCache.pl script to generate cache files for that discovery. The ncp_disco process must still be running. If the ncp_disco process has been stopped or restarted since the discovery finished, you cannot use the GetDiscoCache.pl script to generate cache files for that discovery. You must either run another discovery in failover mode or run another discovery normally and then run the GetDiscoCache.pl script.

The script stores the cache files in `ITNMHOME/var/precision` as `PerlStore.`*`timestamp`*`.Cache.`*`DatabaseName`*`.`*`TableName`*`.`*`DomainName`*`,` so that they are ready to send to IBM Support for troubleshooting purposes. To run the script, use a command line similar to the following: **UNIX**

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
GetDiscoCache.pl -domain DomainName
```

Note: On UNIX systems only, the script also compresses the cache files into a `.tar` file by default. For more information, see option `-buildtar` in the following table.

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
GetDiscoCache.pl  -domain DomainName
```

Command-line options

The following table describes the command-line options for the `GetDiscoCache.pl` script.

Table 143. AddNode.pl command-line options

Command-line option	Description
`-domain` *DomainName*	Mandatory; the name of the domain you want to retrieve discovery tables for and build a copy of the cache files.
`-debug` *DebugLevel*	Optional; the level of detail the debugging output provides. Values are 1 to 4, where 4 represents the most detailed output.
`-latency` *MessageLatency*	Optional; the maximum time in milliseconds to wait between attempts to send a message. This is needed for busy networks.
`-help`	Optional; displays help for command line options on screen.

Table 143. AddNode.pl command-line options (continued)

Command-line option	Description
`-buildtar 0	1`	On UNIX systems only; sets whether the copy of the cache files is compressed into a `.tar` file in the current directory. The file is called *service.timestamp.DomainName*.tar, where *service* is the name of the process from which to retrieve the data. The default setting is 1, meaning the files are compressed. Set it to 0 to turn off the creation of compressed `.tar` files.
`-service`	Optional. You can specify the name of the service to retrieve the cache data from. The default is `Disco` for the discovery process.
`-dbName`	Optional; specifies the discovery database to cache (for example, `Details`).
`-tblName`	Optional; specifies the discovery table to cache. Only used if `-dbName` is set (for example, `-dbName IpRoutingTable -tblName returns`).

The following is an example of using the command-line options for
GetDiscoCache.pl on a UNIX system: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
GetDiscoCache.pl -domain NCOMS -service Disco -buildtar 1
```

ncp_db_access.pl

Checks database setup and determines whether access to the databases is being prevented by firewalls. This script accesses the topology database, historical polling database, and the distributed polling database.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
ncp_db_access.pl -domain NCOMS
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
ncp_db_access.pl  -domain NCOMS
```

Command-line options

The following table describes the command-line options for the script.

Table 144. ncp_db_access.pl command-line options

Command-line option	Description
`-domain` *Domain*	Mandatory; the domain in which to check database access.

PrintCacheFile.pl

Takes a specified cache file and prints out the ROMP contents of the file in a human-readable format. This is mostly useful for scripting and debugging purposes.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
PrintCacheFile.pl -domain domain cache_file
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
PrintCacheFile.pl -domain domain cache_file
```

Command-line options

The following table describes the command-line options for the script.

Table 145. PrintCacheFile.pl command-line options

Command-line option	Description
-domain *domain*	The domain in which you want the script to run. This option is mandatory.
cache_file	The name of the cache file. This option is mandatory.

snmp_walk.pl

Troubleshoots discovery connection and topology issues and produces .mimic and .snmpwalk output files for further investigation.

Description

By default the script performs an SNMP or mimic walk of the entire device, starting at the 'internet' MIB node.

This script accesses devices through the Helper System. Community strings for the devices are defined in $NCHOME/etc/precision/SnmpStackSecurityInfo.*DOMAIN*.cfg.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
snmp_walk.pl -domain NCOMS2 1.2.3.4 ifIndex @vlan2
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
snmp_walk.pl -domain NCOMS2 1.2.3.4 ifIndex @vlan2
```

Command-line options

The following table describes the command-line options for the script.

Table 146. snmp_walk.pl command-line options

Command-line option	Description
`-domain` *Domain*	Mandatory; the domain containing the device on which to perform the SNMP walk.
Node	IP address or hostname of the device on which to perform the SNMP walk
OID_or_MIB_variable	Optional; the MIB node from which to begin the SNMP walk. The node can be expressed as an OID (for example, 1.3.6.1.2.1.2.2.1.1), or as a MIB variable (for example, ifIndex). By default the script performs an SNMP or mimic walk of the entire device, starting at the 'internet' MIB node.
SNMP_community_string	Optional; community string to enable access to the device.
`-verbose`	Optional; provides more information on the screen.
`-help`	Optional; provides help on this command

Upgrade scripts

The upgrade Perl scripts are used as part of the process of upgrading and migrating from previous Network Manager versions.

ITNMDataExport.pl

This script exports Network Manager configuration files.

Running the script

To run the script, use a command line similar to the following: **UNIX**

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/
upgrade/ITNMDataExport.pl
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\
upgrade\ITNMDataExport.pl
```

Command-line options

The following table describes the command-line options for the script.

Table 147. ITNMDataExport.pl command-line options

Command-line option	Description
-export	Exports configuration data.
-help	Displays usage information.

ITNMDataImport.pl

This script imports Network Manager configuration files.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/
upgrade/ITNMDataImport.pl
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\
upgrade\ITNMDataImport.pl
```

Command-line options

The following table describes the command-line options for the script.

Table 148. ITNMDataImport.pl command-line options

Command-line option	Description
-import	Imports configuration data.
-help	Displays usage information.
-simulate	Simulates a data import. Shows what would be done, without importing data.

ITNMExportNetworkViews.pl

This script exports and imports network views and filter data.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/
upgrade/ITNMExportNetworkViews.pl
```

`Windows`

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\
upgrade\ITNMExportNetworkViews.pl
```

Command-line options

The following table describes the command-line options for the script.

Table 149. ITNMExportNetworkViews.pl command-line options

Command-line option	Description
-export	Required. Exports network views.
-import	Required. Imports network views.
-server	Required. The type of database. Allowed values are: mysql, oracle, db2, informix.
-dbname	Required. The name of the database, Oracle SID, or Informix servername.dbname.
-host	Required. The host name of the database server.

Table 149. ITNMExportNetworkViews.pl command-line options (continued)

Command-line option	Description
-username	Required. Username for accessing the database.
-password	Required. Password for accessing the database.
-port	Optional. Database port (if not using the default).
-ncimSchema	Optional. The name of the NCIM database schema (if not using the default).
-ncpguiSchema	Optional. The name of the ncpgui database schema (if not using the default).
-mysql_socket	Optional. The location of the MySQL socket, if using a MySQL database.
-help	Optional. Displays help information for the script.
-domain	Optional. The domain to import the views into. The default is NCOMS.
-fromDomain	Optional. When exporting views, the domain to export from.
-toDomain	Optional. When exporting views, the domain to import to.
-allocateNewEntityIds	Optional. Allocate new entity IDs for devices. If not specified, entity IDs are preserved.

ncp_ncim_diff.pl

This script identifies the differences between your previous installation's NCIM database schema and the new installation's NCIM schema. This is useful if you are upgrading to a later version of Network Manager and you have made custom changes to the previous NCIM database schema. Once the script has identified these differences, you can manually update the NCIM schema.

Description

If your deployment requires additional network domains, you must configure process control for the domains and register the domains with the NCIM topology database. Once you have done this, you can then use the **domain_create.pl** Perl script to migrate the configuration and network polls from an existing domain to the new domain. You must use one instance of ncp_ctrl to run and manage each domain. The script does not migrate the topology from the original domain.

Running the script

To run the script, use a command line similar to the following: UNIX

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/perl/scripts/
ncp_ncim_diff.pl -domain NCOMS2
```

Windows

```
%NCHOME%\precision\bin\ncp_perl.bat %NCHOME%\precision\scripts\perl\scripts\
ncp_ncim_diff.pl -domain NCOMS2
```

Command-line options

The following table describes the command-line options for the script.

Table 150. ncp_ncim_diff.pl command-line options

Command-line option	Description
-domain *Domain*	Mandatory; the previous domain whose NCIM structure you want to compare to the new installation's schema.
-verbose	Optional; provides more information on the screen.
-help	Optional; provides help on this command

Shell and batch scripts

Use the supplied shell and batch scripts to perform administration tasks.

The following scripts must not be modified. These scripts are used by the itnm_start, itnm_stop, and itnm_status commands to start, stop, and check the status of Network Manager processes:

- itnm_control.sh
- itnm_control_functions.sh
- nco_control.sh
- ncp_control.sh
- tip_control.sh
- tip_server.sh

create_db2_database

Use this script to create the back end NCIM relational database schemas in a DB2 database.

Running the script

Run this script as the DB2 administrative user.

To run the script, use a command line similar to the following: **UNIX**

```
$NCHOME/precision/scripts/sql/db2/create_db2_database.sh database_name user_name
 [ -force ]
```

Windows

```
%NCHOME%\precision\scripts\sql\db2\create_db2_database.bat database_name user_name
 [ -force ]
```

Command-line options

The following table describes the command-line options for the **create_db2_database** script.

Table 151. create_db2_database.sh and create_db2_database.bat command-line options

Command-line option	Description
database_name	Mandatory; the name of the database.

Table 151. create_db2_database.sh and create_db2_database.bat command-line options (continued)

Command-line option	Description
user_name	Mandatory; the name of the database user that will be used to connect to the database. **Important:** This user must not be the administrative user. This user must be an existing operating system and DB2 user.
-force	Optional; instructs the script to force any existing DB2 users off the instance before attempting to drop the database

create_informix_database

Use this script to create the back end NCIM relational database schemas in an Informix database.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/scripts/sql/informix/create_informix_database.sh database_name
 user_name
```

`Windows`

```
%NCHOME%\precision\scripts\sql\informix\create_informix_database.bat database_name
 user_name
```

Command-line options

The following table describes the command-line options for the `create_informix_database` script.

Table 152. create_informix_database.sh and create_informix_database.bat command-line options

Command-line option	Description
database_name	Mandatory; the name of the database.
user_name	Mandatory; the name of the database user.

create_mysql_database

Use this script to create the back end NCIM relational database schemas in a MySQL database.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/scripts/sql/mysql/create_mysql_database.sh admin_username
admin_password [ prefix ]
```

`Windows`

```
%NCHOME%\precision\scripts\sql\mysql\create_mysql_database.bat admin_username
admin_password [ prefix ]
```

Command-line options

The following table describes the command-line options for the
`create_mysql_database` script.

Table 153. create_mysql_database.sh and create_mysql_database.bat command-line options

Command-line option	Description
admin_username	Mandatory; the use name of the database administrator.
admin_password	Mandatory; the password for the database administrator.
prefix	Optional;

create_oracle_database

Use this script to create the back end NCIM relational database schemas in an
Oracle database.

Running the script

To run the script, use a command line similar to the following: **UNIX**

```
$NCHOME/precision/scripts/sql/oracle/create_oracle_database.sh database_name
user_name [ -force ]
```

Windows

```
%NCHOME%\precision\scripts\sql\oracle\create_oracle_database.bat database_name
user_name [ -force ]
```

Command-line options

The following table describes the command-line options for the
`create_oracle_database` script.

Table 154. create_oracle_database.sh and create_oracle_database.bat command-line options

Command-line option	Description
database_name	Mandatory; the name of the database.
user_name	Mandatory; the name of the database user.
-force	Optional; instructs the script to force any existing DB2 users off the instance before attempting to drop the database

drop_db2_database

Use this script to remove the back end NCIM relational database implemented using DB2.

Running the script

To run the script, use a command line similar to the following: `UNIX`

`$NCHOME/precision/scripts/sql/db2/drop_db2_database.sh` *database_name* `[ -force ]`

`Windows`

`%NCHOME%\precision\scripts\sql\db2\drop_db2_database.bat` *database_name* `[ -force ]`

Command-line options

The following table describes the command-line options for the **drop_db2_database** script.

Table 155. drop_db2_database.sh and drop_db2_database.bat command-line options

Command-line option	Description
database_name	Mandatory; the name of the database.
-force	Optional; instructs the script to force any existing DB2 users off the instance before attempting to drop the database

drop_informix_database

Use this script to remove the back end NCIM relational database implemented using Informix.

Running the script

To run the script, use a command line similar to the following: `UNIX`

`$NCHOME/precision/scripts/sql/informix/drop_informix_database.sh` *database_name*

`Windows`

`%NCHOME%\precision\scripts\sql\informix\drop_informix_database.bat` *database_name*

Command-line options

The following table describes the command-line options for the **drop_informix_database** script.

Table 156. drop_informix_database.sh and drop_informix_database.bat command-line options

Command-line option	Description
database_name	Mandatory; the name of the database.

drop_mysql_database

Use this script to remove the back end NCIM relational database implemented using MySQL.

Running the script

To run the script, use a command line similar to the following: ▌ UNIX ▐

```
$NCHOME/precision/scripts/sql/mysql/drop_mysql_database.sh database_name
[ -force ]
```

▌ Windows ▐

```
%NCHOME%\precision\scripts\sql\mysql\drop_mysql_database.bat database_name
[ -force ]
```

Command-line options

The following table describes the command-line options for the **drop_mysql_database** script.

Table 157. drop_mysql_database.sh and drop_mysql_database.bat command-line options

Command-line option	Description
database_name	Mandatory; the name of the database.
-force	Optional; instructs the script to force any existing DB2 users off the instance before attempting to drop the database

drop_oracle_database

Use this script to remove the back end NCIM relational database implemented using Oracle.

Running the script

To run the script, use a command line similar to the following: ▌ UNIX ▐

```
$NCHOME/precision/scripts/sql/oracle/drop_oracle_database.sh database_name
[ -force ]
```

▌ Windows ▐

```
%NCHOME%\precision\scripts\sql\oracle\drop_oracle_database.bat database_name
[ -force ]
```

Command-line options

The following table describes the command-line options for the **drop_oracle_database** script.

Table 158. drop_oracle_database.sh and drop_oracle_database.bat command-line options

Command-line option	Description
database_name	Mandatory; the name of the database.
-force	Optional; instructs the script to force any existing DB2 users off the instance before attempting to drop the database

populate_db2_database

Use this script to populate the back end NCIM relational database schemas in a DB2 database. You usually run this script after having created the NCIM relational database using the shell or batch script create_db2_database.

Running the script

To run the script, use a command line similar to the following: UNIX

```
$NCHOME/precision/scripts/sql/db2/populate_db2_database.sh database_name user_name
 [ -force ]
```

 Windows

```
%NCHOME%\precision\scripts\sql\db2\populate_db2_database.bat database_name user_name
 [ -force ]
```

Command-line options

The following table describes the command-line options for the `populate_db2_database` script.

Table 159. populate_db2_database.sh and populate_db2_database.bat command-line options

Command-line option	Description
database_name	Mandatory; the name of the database.
user_name	Mandatory; the name of the database user.
-force	Optional; instructs the script to force any existing DB2 users off the instance before attempting to drop the database

populate_informix_database

Use this script to populate the back end NCIM relational database schemas in an Informix database. You usually run this script after having created the NCIM relational database using the shell or batch script create_informix_database.

Running the script

To run the script, use a command line similar to the following: UNIX

```
$NCHOME/precision/scripts/sql/informix/populate_informix_database.sh database_name
 user_name
```

 Windows

```
%NCHOME%\precision\scripts\sql\informix\populate_informix_database.bat database_name
 user_name
```

Command-line options

The following table describes the command-line options for the `populate_informix_database` script.

Table 160. populate_informix_database.sh and populate_informix_database.bat command-line options

Command-line option	Description
database_name	Mandatory; the name of the database.
user_name	Mandatory; the name of the database user.

populate_mysql_database

Use this script to populate the back end NCIM relational database schemas in a MySQL database. You usually run this script after having created the NCIM relational database using the shell or batch script `create_mysql_database`.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/scripts/sql/mysql/populate_mysql_database.sh database_name
 user_name [ -force ]
```

`Windows`

```
%NCHOME%\precision\scripts\sql\mysql\populate_mysql_database.bat database_name
 user_name [ -force ]
```

Command-line options

The following table describes the command-line options for the `populate_mysql_database` script.

Table 161. populate_mysql_database.sh and populate_mysql_database.bat command-line options

Command-line option	Description
database_name	Mandatory; the name of the database.
user_name	Mandatory; the name of the database user.
-force	Optional; instructs the script to force any existing users off the instance before attempting to drop the database

populate_oracle_database

Use this script to populate the back end NCIM relational database schemas in an Oracle database. You usually run this script after having created the NCIM relational database using the shell or batch script `create_oracle_database`.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/scripts/sql/oracle/populate_oracle_database.sh database_name
 user_name [ -force ]
```

`Windows`

```
%NCHOME%\precision\scripts\sql\oracle\populate_oracle_database.bat database_name
 user_name [ -force ]
```

Command-line options

The following table describes the command-line options for the
`populate_oracle_database` script.

*Table 162. populate_oracle_database.sh and populate_oracle_database.bat command-line
options*

Command-line option	Description
database_name	Mandatory; the name of the database.
user_name	Mandatory; the name of the database user.
-force	Optional; instructs the script to force any existing users off the instance before attempting to drop the database

register_all_agents

During normal installation, the installation process should register all agents with
the ncp_disco process. If for any reason this fails to happen, the script
`register_all_agents` is provided so that the user can reregister the installed agent
set. It should only be necessary to use this script on rare occasions.

Running the script

To run the script, use a command line similar to the following: UNIX

`$NCHOME/precision/scripts/register_all_agents.sh`

 Windows

`%NCHOME%\precision\scripts\register_all_agents.bat`

Command-line options

This script has no command-line options.

restrict_oracle_privileges.sh

This script applies to NCIM databases created using Oracle as RDBMS. This script
revokes the broad set of privileges the NCIM database user was initially given
when the NCIM database schema was created. Following this, the script grants
finer-grained privileges on the objects which were created in the other schemas.
The script must be run as a user with system privileges.

Running the script

To run the script, use a command line similar to the following: UNIX

`$NCHOME/precision/scripts/sql/oracle/restrict_oracle_privileges.sh` *user_name*
 password [*prefix*]

 Windows

`%NCHOME%\precision\scripts\sql\oracle\restrict_oracle_privileges.bat` *user_name*
 password [*prefix*]

Command-line options

The following table describes the command-line options for the
`restrict_oracle_privileges.sh` script.

Table 163. restrict_oracle_privileges.sh command-line options

Command-line option	Description
user_name	Mandatory; the name of the database user. This must be a user with system privileges.
password	Mandatory; pasword of the database user.
prefix	Optional; adds a prefix to the database name.

setup_run_as_root.sh

Certain processes in Network Manager must be run as root. If you installed
Network Manager as a non-root user, you can use the `setup_run_as_root.sh` script
to alter permissions so that you can run the back end processes while logged on as
the root user.

Running the script

To run the script, use a command line similar to the following: █ UNIX █

```
$NCHOME/precision/scripts/setup_run_as_root.sh
```

Command-line options

This script has no command-line options.

setup_run_as_setuid_root.sh

Certain processes in Network Manager must be run as root. If you installed
Network Manager as a non-root user, you can use this script to alter permissions
so that you can run Network Manager while logged on as the non-root user who
installed the product, or another user in the same group. The processes that must
be run as root will have their `setuid` permission changed so that they execute as
root even when invoked by a non-root user.

In order for this script to work correctly, you must be logged on as root when you
run it.

Note: Due to the way this script has to make certain shared libraries trusted, only
one installation per machine can be set up to be run by a non-root user. If you have
multiple installations of Network Manager on the same server, you will have to
run all but one of them as root.

Running the script

To run the script, use a command line similar to the following: █ UNIX █

```
$NCHOME/precision/scripts/setup_run_as_setuid_root.sh
```

Command-line options

This script has no command-line options.

uncatalog_db2_database

Use this script to uncatalog a DB2 database if you have changed the hostname, port, or database name.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/scripts/sql/db2/uncatalog_db2_database.sh database_name
```

`Windows`

```
%NCHOME%\precision\scripts\sql\db2\uncatalog_db2_database.bat database_name
```

Command-line options

The following table describes the command-line options for the `uncatalog_db2_database` script.

Table 164. uncatalog_db2_database command-line options

Command-line option	Description
database_name	Mandatory; the name of the database to uncatalog.

unsetup_run_as_setuid_root.sh

You can use this script to reverse the effects of the `setup_run_as_setuid_root.sh` script.

In order for this script to work correctly, you must be logged on as root when you run it.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/precision/scripts/unsetup_run_as_setuid_root.sh
```

Command-line options

This script has no command-line options.

SQL scripts

Use the supplied SQL scripts to perform setup tasks on the Tivoli Netcool/OMNIbus ObjectServer.

create_itnm_triggers.sql

Use this script to set up a Tivoli Netcool/OMNIbus ObjectServer to support the setting of event severity based on the value of the NmosCauseType field. For example, if NmosCauseType has the value 1 (root cause), then running this script will cause the event severity to be set to Critical.

Running the script

To run the script, use a command line similar to the following: UNIX

```
$NCHOME/omnibus/bin/nco_sql -server objectserver_name -user user_name -password
 password < $NCHOME/precison/scripts/create_itnm_triggers.sql
```

Windows

```
%NCHOME%\omnibus\bin\nco_sql -server objectserver_name -user user_name -password
 password < %NCHOME%\precison\scripts\create_itnm_triggers.sql
```

Command-line options

The following table describes the command-line options for the create_itnm_triggers.sql script.

Table 165. create_itnm_triggers.sql command-line options

Command-line option	Description
objectserver_name	Mandatory; the name of the database.
user_name	Mandatory; the name of the database user.
password	Mandatory; the password of the database user.

create_sae_automation.sql

Use this script to set up the Tivoli Netcool/OMNIbus ObjectServer with automations and right-click tools to support the generation of service-affected events.

Running the script

To run the script, use a command line similar to the following: UNIX

```
$NCHOME/omnibus/bin/nco_sql -server objectserver_name -user user_name -password
 password < $NCHOME/precison/scripts/create_sae_automation.sql
```

Windows

```
%NCHOME%\omnibus\bin\nco_sql -server objectserver_name -user user_name -password
 password < %NCHOME%\precison\scripts\create_sae_automation.sql
```

Command-line options

The following table describes the command-line options for the create_sae_automation.sql script.

Table 166. create_sae_automation.sql command-line options

Command-line option	Description
objectserver_name	Mandatory; the name of the database.

Table 166. create_sae_automation.sql command-line options (continued)

Command-line option	Description
user_name	Mandatory; the name of the database user.
password	Mandatory; the password of the database user.

drop_itnm_triggers.sql

Use this script to set up a Tivoli Netcool/OMNIbus ObjectServer to remove support for setting of event severity based on the value of the NmosCauseType field. After running this script, the value of NmosCauseType (for example 1,root cause) has no effect on event severity.

Running the script

To run the script, use a command line similar to the following: UNIX

```
$NCHOME/omnibus/bin/nco_sql -server objectserver_name -user user_name -password
 password < $NCHOME/precison/scripts/drop_itnm_triggers.sql
```

Windows

```
%NCHOME%\omnibus\bin\nco_sql -server objectserver_name -user user_name -password
 password < %NCHOME%\precison\scripts\drop_itnm_triggers.sql
```

Command-line options

The following table describes the command-line options for the **drop_itnm_triggers.sql** script.

Table 167. drop_itnm_triggers.sql command-line options

Command-line option	Description
objectserver_name	Mandatory; the name of the database.
user_name	Mandatory; the name of the database user.
password	Mandatory; the password of the database user.

drop_sae_automation.sql

Use this script to remove from the Tivoli Netcool/OMNIbus ObjectServer the automations and right-click tools to support the generation of service-affected events.

Running the script

To run the script, use a command line similar to the following: UNIX

```
$NCHOME/omnibus/bin/nco_sql -server objectserver_name -user user_name -password
 password < $NCHOME/precison/scripts/drop_sae_automation.sql
```

Windows

```
%NCHOME%\omnibus\bin\nco_sql -server objectserver_name -user user_name -password
 password < %NCHOME%\precison\scripts\drop_sae_automation.sql
```

Command-line options

The following table describes the command-line options for the
drop_sae_automation.sql script.

Table 168. drop_sae_automation.sql command-line options

Command-line option	Description
objectserver_name	Mandatory; the name of the database.
user_name	Mandatory; the name of the database user.
password	Mandatory; the password of the database user.

ncp_configure_omnibus.sql

This script is used to set up versions of Tivoli Netcool/OMNIbus prior to Version
7.3.1 by adding additional fields required by Network Manager.

This script is automatically run by the Network Manager installer.

Running the script

To run the script, use a command line similar to the following: `UNIX`

```
$NCHOME/omnibus/bin/nco_sql -server objectserver_name -user user_name -password
 password < $NCHOME/precison/scripts/ncp_configure_omnibus.sql
```

`Windows`

```
"%NCHOME%\omnibus\bin\isql.bat" -S objectserver_name -U user_name -P password
-i < %NCHOME%\precison\scripts\ncp_configure_omnibus.sql
```

Command-line options

The following table describes the command-line options for the
ncp_configure_omnibus.sql script.

Table 169. ncp_configure_omnibus.sql command-line options

Command-line option	Description
objectserver_name	Mandatory; the name of the database.
user_name	Mandatory; the name of the database user.
password	Mandatory; the password of the database user.

Appendix F. Network Manager glossary

Use this information to understand terminology relevant to the Network Manager product.

The following list provides explanations for Network Manager terminology.

AOC files
> Files used by the Active Object Class manager, `ncp_class` to classify network devices following a discovery. Device classification is defined in AOC files by using a set of filters on the object ID and other device MIB parameters.

active object class (AOC)
> An element in the predefined hierarchical topology of network devices used by the Active Object Class manager, `ncp_class`, to classify discovered devices following a discovery.

agent See, discovery agent.

class hierarchy
> Predefined hierarchical topology of network devices used by the Active Object Class manager, `ncp_class`, to classify discovered devices following a discovery.

configuration files
> Each Network Manager process has one or more configuration files used to control process behaviour by setting values in the process databases. Configuration files can also be made domain-specific.

discovery agent
> Piece of code that runs during a discovery and retrieves detailed information from discovered devices.

Discovery Configuration GUI
> GUI used to configure discovery parameters.

Discovery engine (ncp_disco)
> Network Manager process that performs network discovery.

discovery phase
> A network discovery is divided into four phases: Interrogating devices, Resolving addresses, Downloading connections, and Correlating connectivity.

discovery seed
> One or more devices from which the discovery starts.

discovery scope
> The boundaries of a discovery, expressed as one or more subnets and netmasks.

Discovery Status GUI
> GUI used to launch and monitor a running discovery.

discovery stitcher
> Piece of code used during the discovery process. There are various discovery stitchers, and they can be grouped into two types: data collection stitchers, which transfer data between databases during the data collection

phases of a discovery, and data processing stitchers, which build the network topology during the data processing phase.

domain
: See, network domain.

entity A topology database concept. All devices and device components discovered by Network Manager are entities. Also device collections such as VPNs and VLANs, as well as pieces of topology that form a complex connection, are entities.

event enrichment
: The process of adding topology information to the event.

Event Gateway (ncp_g_event)
: Network Manager process that performs event enrichment.

Event Gateway stitcher
: Stitchers that perform topology lookup as part of the event enrichment process.

failover
: In your Network Manager environment, a failover architecture can be used to configure your system for high availability, minimizing the impact of computer or network failure.

Failover plug-in
: Receives Network Manager health check events from the Event Gateway and passes these events to the Virtual Domain process, which decides whether or not to initiate failover based on the event.

Fault Finding View
: Composite GUI view consisting of an **Active Event List (AEL)** portlet above and a Network Hop View portlet below. Use the Fault Finding View to monitor network events.

full discovery
: A discovery run with a large scope, intended to discover all of the network devices that you want to manage. Full discoveries are usually just called discoveries, unless they are being contrasted with partial discoveries. See also, partial discovery.

message broker
: Component that manages communication between Network Manager processes. The message broker used byNetwork Manager is called Really Small Message Broker. To ensure correct operation of Network Manager, Really Small Message Broker must be running at all times.

NCIM database
: Relational database that stores topology data, as well as administrative data such as data associated with poll policies and definitions, and performance data from devices.

ncp_disco
: See, Discovery engine.

ncp_g_event
: See, Event Gateway.

ncp_model
: See, Topology manager.

ncp_poller
> See, Polling engine.

network domain
> A collection of network entities to be discovered and managed. A single Network Manager installation can manage multiple network domains.

Network Health View
> Composite GUI view consisting of a Network Views portlet above and an **Active Event List (AEL)** portlet below. Use the Network Health View to display events on network devices.

Network Hop View
> Network visualization GUI. Use the Network Hop View to search the network for a specific device and display a specified network device. You can also use the Network Hop View as a starting point for network troubleshooting. Formerly known as the Hop View.

Network Polling GUI
> Administrator GUI. Enables definition of poll policies and poll definitions.

Network Views
> Network visualization GUI that shows hierarchically organized views of a discovered network. Use the Network Views to view the results of a discovery and to troubleshoot network problems.

OQL databases
> Network Manager processes store configuration, management and operational information in OQL databases.

OQL language
> Version of the Structured Query Language (SQL) that has been designed for use in Network Manager. Network Manager processes create and interact with their databases using OQL.

partial discovery
> A subsequent rediscovery of a section of the previously discovered network. The section of the network is usually defined using a discovery scope consisting of either an address range, a single device, or a group of devices. A partial discovery relies on the results of the last full discovery, and can only be run if the Discovery engine, `ncp_disco`, has not been stopped since the last full discovery. See also, full discovery.

Path Views
> Network visualization GUI that displays devices and links that make up a network path between two selected devices. Create new path views or change existing path views to help network operators visualize network paths.

performance data
> Performance data can be gathered using performance reports. These reports allow you to view any historical performance data that has been collected by the monitoring system for diagnostic purposes.

Polling engine (ncp_poller)
> Network Manager process that polls target devices and interfaces. The Polling engine also collects performance data from polled devices.

poll definition
> Defines how to poll a network device or interface and further filter the target devices or interfaces.

poll policy
Defines which devices to poll. Also defines other attributes of a poll such as poll frequency.

Probe for Tivoli Netcool/OMNIbus (nco_p_ncpmonitor)
Acquires and processes the events that are generated by Network Manager polls and processes, and forwards these events to the ObjectServer.

RCA plug-in
Based on data in the event and based on the discovered topology, attempts to identify events that are caused by or cause other events using rules coded in RCA stitchers.

RCA stitcher
Stitchers that process a trigger event as it passes through the RCA plug-in.

root-cause analysis (RCA)
The process of determining the root cause of one or more device alerts.

SNMP MIB Browser
GUI that retrieves MIB variable information from network devices to support diagnosis of network problems.

SNMP MIB Grapher
GUI that displays a real-time graph of MIB variables for a device and usse the graph for fault analysis and resolution of network problems.

stitcher
Code used in the following processes: discovery, event enrichment, and root-cause analysis. See also, discovery stitcher, Event Gateway stitcher, and RCA stitcher.

Structure Browser
GUI that enables you to investigate the health of device components in order to isolate faults within a network device.

Topology Manager (ncp_model)
Stores the topology data following a discovery and sends the topology data to the NCIM topology database where it can be queried using SQL.

WebTools
Specialized data retrieval tools that retrieve data from network devices and can be launched from the network visualization GUIs, Network Views and Network Hop View, or by specifying a URL in a web browser.

Notices

This information applies to the PDF documentation set for IBM Tivoli Network Manager IP Edition 3.9.

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 grant 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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

> IBM World Trade Asia Corporation
> Licensing
> 2-31 Roppongi 3-chome, Minato-ku
> Tokyo 106-0032, Japan

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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

>   IBM Corporation
>   958/NH04
>   IBM Centre, St Leonards
>   601 Pacific Hwy
>   St Leonards, NSW, 2069
>   Australia
>   IBM Corporation
>   896471/H128B
>   76 Upper Ground
>   London
>   SE1 9PZ
>   United Kingdom
>   IBM Corporation
>   JBF1/SOM1 294
>   Route 100
>   Somers, NY, 10589-0100
>   United States of America

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

The terms in Table 170 are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Table 170. IBM trademarks

AIX	iSeries	RDN
ClearQuest	Lotus	SecureWay
Cognos	Netcool	solidDB
Current	NetView	System z
DB2	Notes	Tivoli
developerWorks	OMEGAMON	WebSphere
Enterprise Storage Server	PowerVM	z/OS
IBM	PR/SM	z/VM
Informix	pSeries	zSeries

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

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

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Index

Special characters

! command   81

A

about this profile   131
accessibility   xi
adding a user to groups   55
adding more groups as members of a
   group   68
adding more users as members of a
   group   59
adding users to a group   57
AddNode.pl script   229, 230, 231, 234,
   236, 237, 239, 240, 243, 244, 246, 248
administration
   users   45
application server
   ports   4
   profile   131
Asset reports   197
authentication
   client messages   129

B

back up
   server settings   133
BIRT charts   111
BIRT Designer
   steps to create a chart   112
BIRT reports
   and FIPS 140-2   126
   configuring to store NCIM passwords
      using JNDI   126
BuildSeedList.pl script   239

C

cache files   255
Card Detail by Device Type   198
changing display options for a group   63
changing display options for a user   53
changing host and port settings
   for Really Small Message Broker   40
changing user information   56, 65
chart
   connection to a Tivoli Web
      service   109
   errors   134
   opening a BIRT   111
   roles   47, 103
   Tivoli application   108
   tools   113
   troubleshooting
      chart errors   134
   uploading a BIRT   111
charts
   BIRT overview   111

charts *(continued)*
   exporting   107
   importing   107
cloning
   server settings   133
command line options
   ncp_class   145
   ncp_g_event   153
command-line commands
   ncp_mib   155
commands
   ncp_poller   162
components
   binary names   18
configuration files   183, 184, 185
   differences, Windows and UNIX   23
   domain-specific   13
   for Topoviz   183
   ServiceData   44
configure logging level of a process   32
configuring
   BIRT reports to store NCIM
      passwords using JNDI   126
   Structure Browser   185
   web applications   183
   WebTools   184
context menus
   in the Web GUI   138
Context reports   220
conventions, typeface   xiii
creating filters   52, 62
creating users   54
CTGES1504E and CTGES1505E   129
Current Status reports   201

D

DB2
   uncatalog   86
debug level   31
default   45
deleting groups   69
deleting users   60
dependencies
   configuring, process   18
   identifying specific, process   17
   identifying, process   17
   processes start order   18
disco_profiling_data.pl script   241
domain MIB Browser URL
   parameter   188
domains
   processes   12
drop_polldata.pl   140
duplicating group assignments for
   groups   69
duplicating group assignments for
   users   59

E

editing
   properties files   131
education
   see Tivoli technical training   xii
environment variables   1
   log files   36
environment variables, notation   xiii
errors
   device not found   138
   domain not found   138
   screen blank   138
   unable to execute right-click
      tools   139
execute previous commands   81
exporting
   charts   107

F

filtering a list of groups   62
filtering a list of users   52
FIPS 140-2
   and BIRT reports   126
First Failure Data Capture (FFDC)   34

G

glossary   275
groups   45
   adding more as members of a
      group   68
   changing information about   65
   changing viewing options   63
   creating filters   62
   deleting   69
   duplicating group assignments   69
   filtering a list of   62
   managing   60
   Network_Manager_IP_Admin
      roles   48
   removing members from   68
   searching for   61, 65, 69
   viewing group information   65
   viewing membership of   66
GUI
   locating log files   27

H

Helper Server
   starting   152
Helper System
   command line   152
   starting   152
helpers
   starting   152
hist command   81

host and port settings
  changing for Really Small Message
    Broker 40
host MIB Browser URL parameter 188
hostname 132

I

ID
  network view 188
identifying
  network view 188
importing
  charts 107
Internet Explorer Enhanced Security
  Configuration 137
IP path
  detailed report 208
  summary report 208
IP routing
  report 209
itnm_pathTool.pl script 232
ITNMIP_Listener.pl script 233

J

JNDI datasources
  managing using script 127

L

load balancing
  charting
    database tables for load
      balancing 103
    charting tables 103
log file
  GUI component 25
  location for GUI logs 27
  location for process logs 32
  process 31
log files
  environment variables 36
  rotating 36
log size 31
logging 25
logging in GUI 25
logging level
  application segments 30
  changing before starting a process 32
  changing for a running process 32,
    33
  changing for GUI components 28
  debug level 28, 32, 33
  GUI components 28
  log files 28
  troubleshooting 28
login
  errors 129
  must have roles 130
  slow response 130
  troubleshooting 130
  users 130
logs
  administering 25
  setting up 25

M

maintenance tools
  FFDC 34
managing groups 60
managing users 50
manuals viii
maps
  opening using URL parameters 186
  saved, in Network Views 188
message broker 39
  changing host and port settings 40
  running separate broker for each
    domain 41
MIB Browser
  URL parameters 188
MIB Grapher
  URL parameters 189
MIB tree
  sysUpTime scalar object 188
micro broker
  stopping 41
monitoring reports 202
MPLS TE path
  detailed report 209
  summary report 209
MPLS TE routing
  report 210
multicast 40
  changing the address 42

N

NCHOME 1
NCIM
  uncatalog, on DB2 86
ncp_class command line options 145
ncp_ctrl 9
  slave mode 23
ncp_g_event
  command line options 153
ncp_mib command 155
ncp_model
  command line options 157
ncp_ping_poller_snapshot.pl 251
ncp_poller command 162
ncp_polling_exceptions.pl 252
ncp_store
  command line options 164
ncp_upload_expected_ips.pl 252
Network Manager glossary 275
Network Technology reports 203
network views
  identifying 188

O

online publications viii
OQL Service Provider
  ! command 81
  execute previous commands 81
  hist command 81
  taboff command 83
  tabon command 82
  tips 81
ordering publications viii

P

pages 173
Path Views
  URL parameters 190
Performance reports 208, 210
Perl scripts
  for polling 247
polling scripts 247
port
  numbers 131
port assignments 4
ports
  changing defaults 39
  checking usage 41
  defaults 43
  defining fixed multicast address 42
  defining fixed TCP 42
  inter-process communication 40
  inter-process communication
    overview 39
process control
  configuration files 19
  overview 9
process control configuration files
  dependencies 19
processes
  changing logging level before
    starting 32
  changing logging level when
    running 32, 33
  changing user, services 23
  checking status 13
  configuration files 19
  configuring automatic
    sample 19
  configuring automatic start 19
  configuring automatic start, Windows
    services 22
  configuring dependencies 18
  dependencies, start order 18
  domains 12
  identifying 14
  identifying automatic 15
  identifying dependencies 17
  identifying specific dependencies 17
  identifying unmanaged 16
  list 10
  locating log files 32
  managed, overview 12
  multicast 40
  ncp_ctrl 9
  removing services 22
  running as specific user, Windows
    services 23
  ServiceData configuration file 44
  starting as a service 22
  starting managed 20
  starting unmanaged 21
  stopping 21
  stopping as a service 22
  TCP communication 40
  unmanaged, overview 12
  Windows services 9
properties
  editing files 131
publications viii

IBM ®

Printed in the Republic of Ireland